190037

Protecting Children Online

National Criminal Justice Reference Service (NCJRS)
Box 6000
Rockville, MD 20849-6000

Performed Under Contract
Fox Valley Technical College
Criminal Justice Department
Appleton, Wisconsin

If you have issues viewing or accessing this file, please contact us at NCJRS.gov.

Acknowledgments

The *Protecting Children Online* training program was jointly developed by the United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, the National Center for Missing and Exploited Children and Fox Valley Technical College, Appleton, Wisconsin.

Contributors

Daniel Armagh
Director of Legal Education
National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314
703-837-6337
darmagh@ncmec.org

Peter Banks
Director of Training and Outreach
National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314
703-837-6209
pbanks@ncmec.org

Philip Condu
OJJDP Program Coordinator
Fox Valley Technical College
Criminal Justice Department
1825 North Bluemound Drive
Appleton, WI 54914
800-648-4966
condu@foxvalley.tec.wi.us

Sergeant James Doyle
New York City Police Department
Computer Investigations & Technology Unit
One Police Plaza, Room 1110D
New York, NY 10038
212-374-4247
jrdoyle@ix.netcom.com

Detective Robert Farley
Cook County Sheriff's Police Department
Child Exploitation Unit
1401 S. Maybrook Drive
Maywood, IL 60153
708-865-4875
rhfarley@hotmail.com

J. Patrick Finley
OJJDP Program Manager
Fox Valley Technical College
Criminal Justice Department
1825 North Bluemound Drive
Appleton, WI 54914
800-648-4966
76065.463@compuserve.com

Kathy Free
Project Manager
Exploited Child Unit
National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314
703-837-6307
kfree@ncmec.org

Michael Geraghty
Network Intrusion Detection Manager
Corporate Computer and Network Security
Lucent Technologies
101 Crawford Corner Road
Room 2C605
Holmdel, NJ 07733
732-949-1044
mgeraghty@lucent.com

Robert Kreisa
President
Criminal Justice Associates
3180 Dans Drive
Stevens Point, WI 54481
715-342-4872
cja@coredcs.com

Ronald Laney
Director
Missing and Exploited Children's Program
Office of Juvenile Justice and Delinquency Prevention
810 7th Street NW
Washington, DC 20531
202-616-3637
laney@ojp.usdoj.gov

Michael Medaris
Program Manager
Missing and Exploited Children's Program
Office of Juvenile Justice and
Delinquency Prevention
810 7th Street NW
Washington, DC 20531
202-616-3637
medarism@ojp.usdoj.gov

Sergeant Gary O'Connor
Lower Gwynedd Township Police Department
1130 North Bethlehem Pike
Spring House, PA 19477
215-646-5303
sargeoc@aol.com

Detective Wayne Promisel
Fairfax County Police
10600 Page Avenue
Fairfax, VA 22030
703-246-7813
promisel@aol.com

John Rabun
Vice President and Chief Operating Officer
National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314
703-837-6216
jrabun@ncmec.org

Ruben Rodriguez
Director
Exploited Child Unit
National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314
703-837-6261
rrodriguez@ncmec.org

Chief Bradley Russ
Portsmouth Police Department
3 Junkins Avenue
Portsmouth, NH 03801
603-427-1500
bruss@pd.cityofportsmouth.com

Lieutenant Bill Walsh
Dallas Police Department
Youth & Family Crimes Division
106 S. Harwood Street, Room 225
Dallas, TX 75201
214-670-5936
bwalsh4122@hotmail.com

PROTECTING CHILDREN ONLINE

Agenda

Day One

8:30 a.m. - 8:45 a.m. **Welcome & Overview of Course**
Student Introductions

8:45 a.m. –12:00 noon **Computer Crimes Against Children**

This module of instruction will provide students with information regarding the growing problem of computer crimes against children. The presentation will provide an overview of the issues of the sexual abuse and exploitation of children and the impact of computer technology as a tool used by sex offenders to facilitate their sexual victimization of children. Participants will be provided with information regarding the child victim, offender typology, child pornography and child erotica, the dynamics of the crime of sexual abuse and exploitation, the uses of computers by offenders to victimize children, and the complex legal, jurisdictional, technical, and investigative problems encountered in these investigations. Case examples will be used to illustrate how computers are used to store, manufacture and distribute child pornography and to solicit children for sexual contact.

12:00 noon - 1:00 p.m. **Lunch Break**

1:00 p.m. - 4:30 p.m. **Orientation to Computer Technology**

This module will provide investigators with a fundamental understanding of computer technology and communications as a foundation for the remainder of the course. Computer hardware, software, and networks will be explained and defined. The Internet and how it works is discussed and demonstrated, with particular attention to how the Internet is used to exploit children. Computer equipment commonly used to create and distribute child pornography is demonstrated.

Day Two

8:30 a.m. - 12:00 noon **The Investigation: Technical Aspects**

This module is designed for the responding officer and investigator of child exploitation violations that occur involving the Internet. The primary emphasis is focused on initiating and conducting this fairly new and somewhat technical investigation. Utilizing judicial subpoenas and search warrants, the student will realize the critical elements to request from Internet service providers. Online access by the instructor will take the student through fundamental tracking methods that are necessary to identifying the electronic suspect. Online undercover methodologies and operations will also be demonstrated.

12:00 noon- 1:00 p.m. **Lunch Break**

1:00 p.m. - 4:30 p.m. **The Investigation: Technical Aspects (continues)**

Day Three

8:30 a.m. -12:00 noon **Legal Issues: Winning in Court**

This module is designed to provide students with a comprehensive overview of privacy issues, search and seizure issues, and legal exposure attendant with the investigation and prosecution of computer assisted sexual exploitation of children. Students will be instructed on the most recent court rulings in relevant cases and what the legal analysis means for the investigation protocol for law enforcement. Classic and evolving defenses will be examined and instruction on how to rebut these defenses in and out of court will be discussed. Jurisdiction and partnering will be addressed to empower local and state law enforcement to successfully investigate and prosecute computer exploitation cases.

12:00 noon - 1:00 p.m. **Lunch Break**

1:00 p.m. - 4:30 p.m. **Legal Issues: Winning in Court (continues)**

Day 4

8:30 a.m. - 12:00 noon **Conducting the Child Exploitation Investigation**

This module will provide the student from the large or small police department with a practical, non-technical approach to conducting an online child exploitation investigation. The module will be divided into several sections, each of which utilizes illustrations from actual online child exploitation investigations. Procedures will be identified that can be utilized by law enforcement from the time of the initial complaint, to the arrest of the molester, and the forensic review of the computer system.

12:00 noon - 1:00 p.m. **Lunch Break**

1:00 p.m. - 4:30 p.m. **Resources and Prevention**

This module will identify and explain the many resources that can be utilized in the successful investigation of computer crimes against children, including presentations from representatives from the National Center for Missing and Exploited Children's Exploitation Child Unit, the FBI, U.S. Postal Service, and U.S. Customs Service.

Day 5

8:30 a.m. - 9:30 a.m. **Resources and Prevention (continued)**

9:30 a.m. – 11:45 a.m. **Practical Exercises**

11:45 a.m. - 12:00 noon **Evaluations and Certificates**

PROTECTING CHILDREN ONLINE

Table of Contents

1. Computer Crimes Against Children

2. Orientation to Computer Technology

3. The Investigation: Technical Aspects

4. Legal Issues: Winning in Court

5. Conducting the Child Exploitation Investigation

6. Resources and Prevention

7. Appendix

PROTECTING CHILDREN ONLINE

Mission Statement

The purpose of this training program is to provide law enforcement with the information necessary to properly understand, recognize, and investigate computer crimes against children.

Computer Crimes Against Children

OJJDP

Welcome to

Fox Valley Technical COLLEGE
Knowledge That Works

Protecting Children Online

sponsored by
Office of Juvenile Justice and Delinquency Prevention,
The National Center for Missing and Exploited Children and
Fox Valley Technical College

Please complete following items (located in the front of your training manual) before class begins:

1. **Fox Valley Technical College registration form**
   (Complete the top two sections and sign the bottom)
2. **Fox Valley Technical College waiver (1/2 sheet of paper)**
3. **NCMEC Survey**
   Place in box on table in back of room by end of first break
4. **Fox Valley Technical College Table Tent (Place on your table)**

PCO-CCAC-Walsh-1

COMPUTER CRIMES AGAINST CHILDREN

PROTECTING CHILDREN ON-LINE

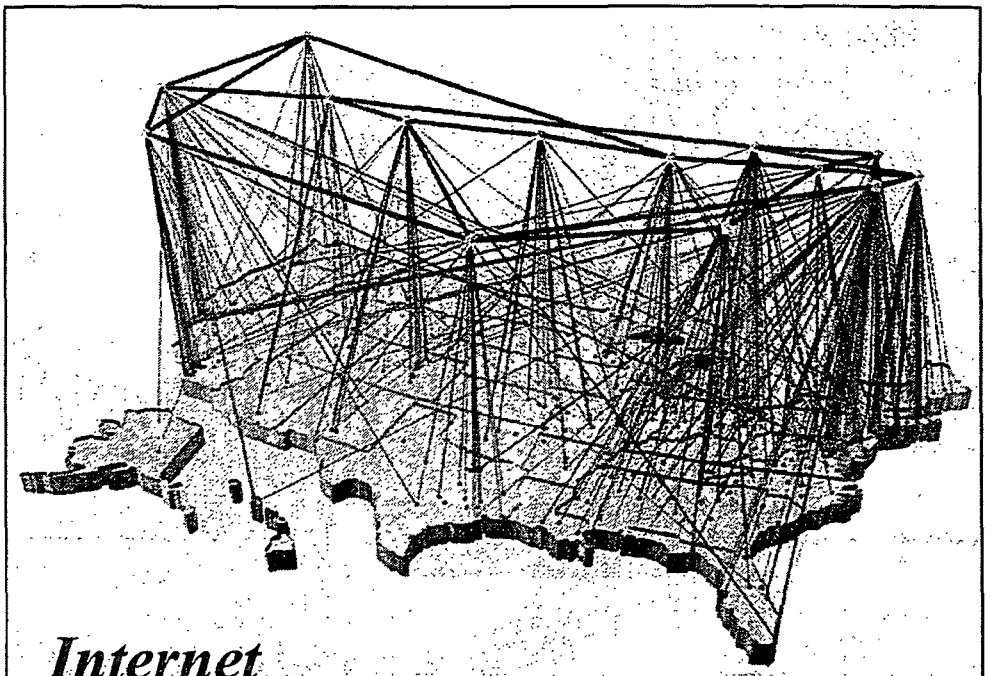
Presented by

Lt. Bill Walsh

Youth and Family Crimes Division

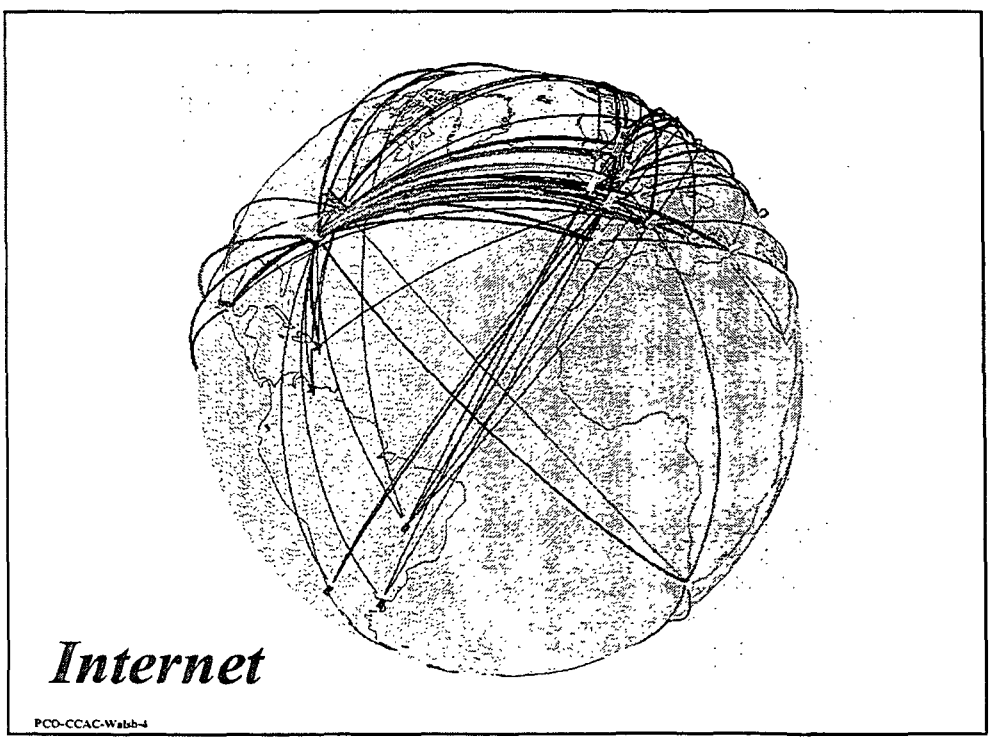
Dallas Police Department

PCO-CCAC-Walsh-2



Internet

PCO-CCAC-Walsh-3

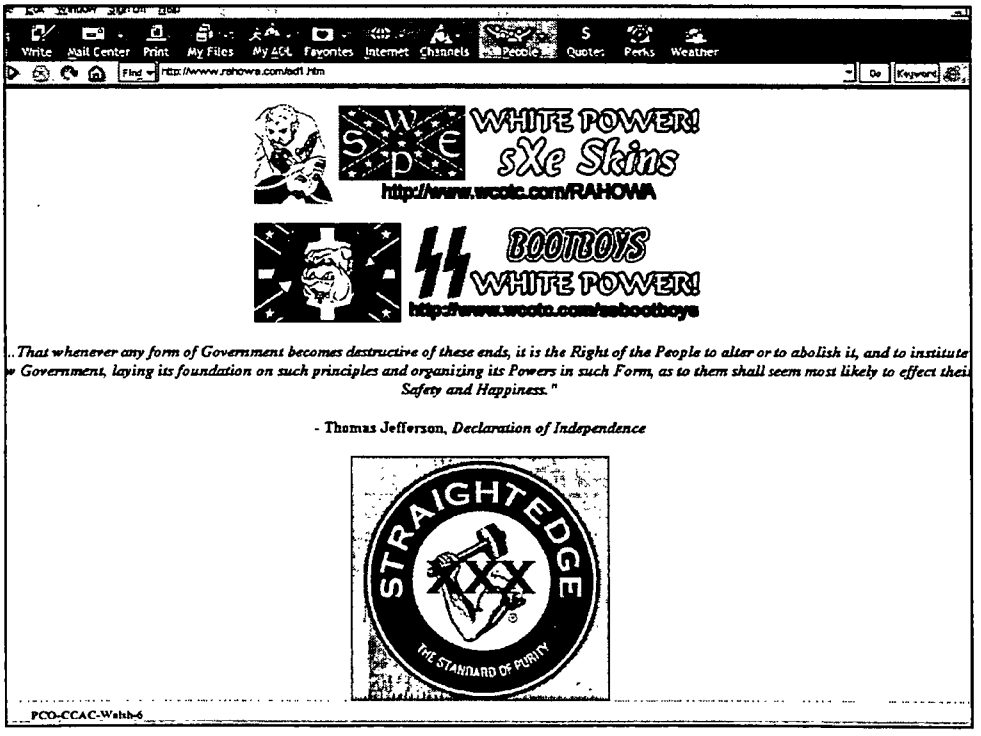


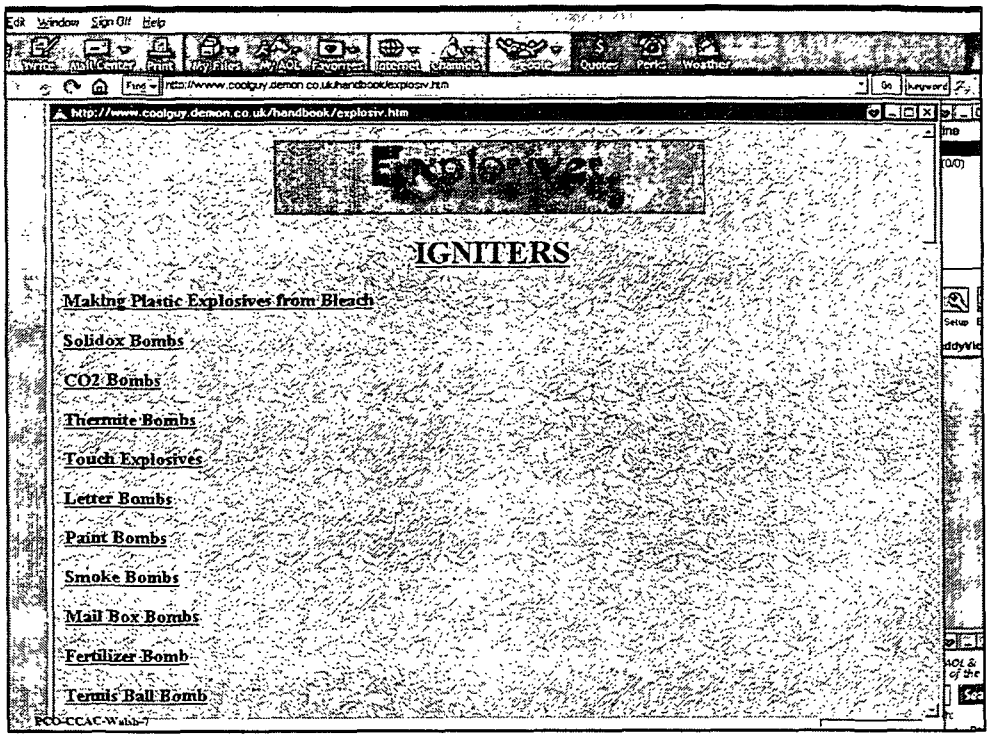
Internet

PCO-CCAC-Walsh-4

Risks to Children on the Internet

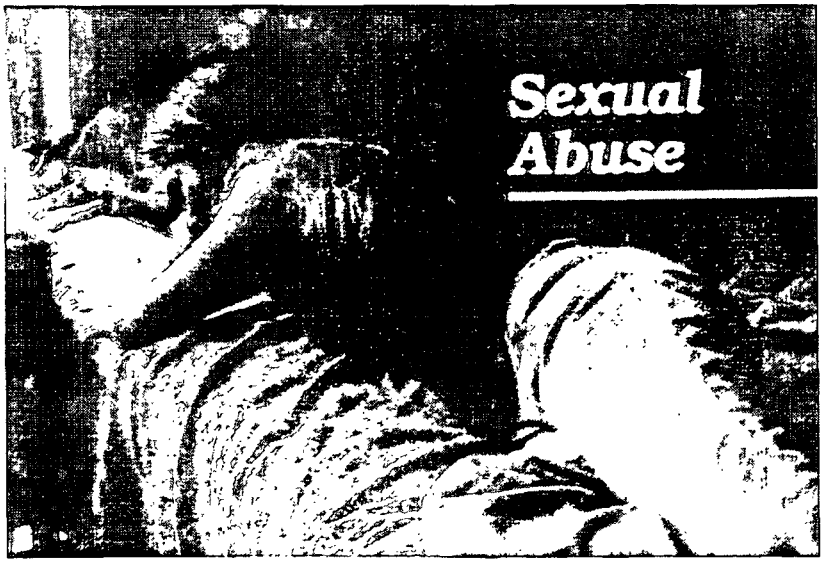
- Exposure to inappropriate material
  - extremist groups
  - pornography
- Sexual Exploitation
  - online solicitation
  - exposure to child pornography
- Harassment
- Other




http://www.coolguy.demon.co.uk/handbook/explosiv.htm
IGNITERS
Making Plastic Explosives from Bleach
Solidox Bombs
CO2 Bombs
Thermite Bombs
Touch Explosives
Letter Bombs
Paint Bombs
Smoke Bombs
Mail Box Bombs
Fertilizer Bomb
Tennis Ball Bomb
PCO-CCAC-Webb-7


KITTY FOXX
The Grandmom of Porn
I know all you horny guys want to see me in action!
Take a peek at these free sample photos from some of my xxx-movies
DID YOU LIKE MY SAMPLES?
IF YOU WANT TO GET A REAL BIG "WOODY"
THEN GO GET A FRESH BOX OF TISSUES AND
CLICK BELOW.
Kitty's Free Pics
XXX Video
Order Form
Fan Club
Kitty Bio
Sex Links
Back Home
PCO-CCAC-Webb-8

PCO-CCAC-Walsh-9



PCO-CCAC-Walsh-10

Flower Mound doctor arrested on child porn charge

F.B.I. Reports Cracking a Child Smut Network on America Online

Court upholds law on child-sex images

Man accused of using Internet in bid to arrange rape of woman

Officer charged with distributing obscene material on Internet

On-line child pornography ring busted

Abilene man gets six years in computer child porn case

Constable may be jailed in Internet porn case

Seized child porn was set to go on-line

FBI, police confiscate material in Dallas area

Trooper charged in child porn case

PCO-CCAC-Walsh-11

Question:

How many of your agencies have had a case involving the computer related sexual abuse and exploitation of children or trafficking in child pornography?

PCO-CCAC-Walsh-12

Question:

When were computers first used to facilitate the sexual abuse and exploitation of children ?

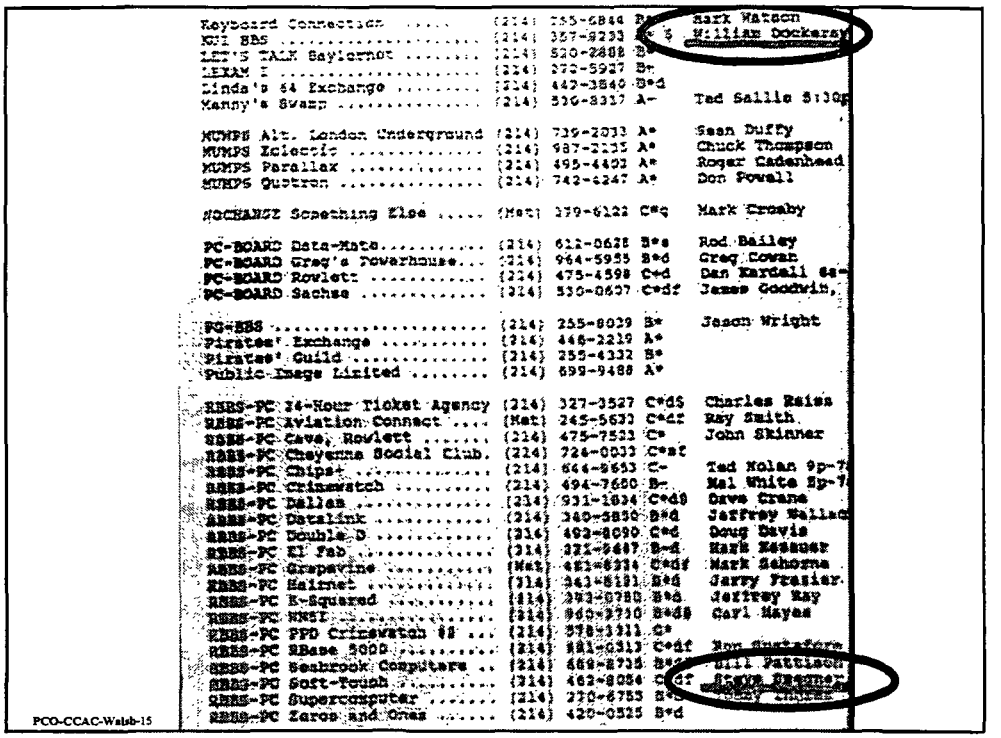
Metropolitan

December 3, 1987 The Dallas Morning News

How about some sugar? Ugh, yuk

Child-porn inquiry implicates 3

Doctor arrested; educator suspended



```
Keyboard Connection  .....  (214) 755-6844 B*    Mark Watson
KUI BBS ..................  (214) 357-9233 A* $  William Dockery
LET'S TALK Saylornot .....  (214) 520-2808 B*
LEXAN I ..................  (214) 270-5927 B*
Linda's 64 Exchange ......  (214) 442-3840 B*d
Manny's Swamp ............  (214) 530-8317 A-    Ted Sallis 8:30p

MUMPS Alt. London Underground (214) 739-2033 A*   Sean Duffy
MUMPS Eclectic ...........  (214) 987-2135 A*    Chuck Thompson
MUMPS Parallax ...........  (214) 495-4402 A*    Roger Cadenhead
MUMPS Quatren ............  (214) 742-6247 A*    Don Powell

#OCHANZZ Something Else ...  (Met) 379-6122 C*q   Mark Crosby

PC-BOARD Data-Mate........  (214) 612-0628 B*s   Rod Bailey
PC-BOARD Greg's Powerhouse.. (214) 964-5935 B*d   Greg Cowan
PC-BOARD Rowlett .........  (214) 475-4598 C*d   Dan Kardell 6a-
PC-BOARD Sachse ..........  (214) 530-0607 C*df  James Goodwin,

PG-BBS ...................  (214) 255-8029 B*    Jason Wright
Pirates' Exchange ........  (214) 446-2219 A*
Pirates' Guild ...........  (214) 255-4332 B*
Public Image Limited .....  (214) 699-9488 A*

RBBS-PC 24-Hour Ticket Agency (214) 327-3527 C*dS  Charles Reiss
RBBS-PC Aviation Connect ... (Met) 245-5632 C*df  Ray Smith
RBBS-PC Cave, Rowlett ....  (214) 475-7523 C*    John Skinner
RBBS-PC Cheyenne Social Club. (214) 724-0033 C*st
RBBS-PC Chips+ ...........  (214) 644-8653 C-    Ted Nolan 9p-7
RBBS-PC Crimewatch .......  (214) 494-7680 B-    Mal White 5p-7
RBBS-PC Dallas ...........  (214) 931-1034 C*dS  Dave Crane
RBBS-PC Datalink .........  (214) 340-5850 B*d   Jeffrey Wallac
RBBS-PC Double D .........  (214) 492-8090 C*d   Doug Davis
RBBS-PC El Fab ...........  (214) 321-9447 B-d   Mark Kessner
RBBS-PC Grapevine ........  (Met) 481-6234 C*df  Mark Sahorna
RBBS-PC Helmet ...........  (214) 343-8181 B*d   Jerry Frasier
RBBS-PC R-Squared ........  (214) 283-0780 B*d   Jeffrey Ray
RBBS-PC RMSI .............  (214) 960-2710 B*dS  Carl Hayes
RBBS-PC PPD Crimewatch #1 ... (214) 578-1211 C*
RBBS-PC RBase 5000 .......  (214) 881-0313 C*df  Ron Gustafson
RBBS-PC Seabrook Computers .. (214) 669-8705 B*d   Bill Pattison
RBBS-PC Soft-Touch .......  (214) 462-8056 C*df  Steve Brenner
RBBS-PC Supercomputer ....  (214) 270-6753 B*d   Gary Shiers
RBBS-PC Zeros and Ones ...  (214) 420-0525 B*d
```

PCO-CCAC-Walsh-15

Question:

What kind of person would use a computer to facilitate the sexual abuse and exploitation of children?

PCO-CCAC-Walsh-16

James Fox

Computer Crimes Against Children

1. Sexual abuse and exploitation of children
2. Impact of computer technology

Sexual Abuse

- Sexual abuse is a crime of violence committed against minor victims.

Sexual Abuse

- Sexual abuse is a crime of violence committed against minor victims.

Child Sexual Abuse

- 61% of all rape victims are under 18 yrs. old
- Girls 12-15 are victims of violent crime at a rate 84 % higher than the general public
- While victimization can occur at any age, the ages between 7 and 13 years represent the peak period of vulnerability
- 40% of imprisoned sex offenders reported that their victims were less than 12 yrs. old.

Unique Problems Encountered with Sexual Abuse Investigations

- Child victims
- Dynamics of sexual abuse
- Disclosure process
- Forensic interviews of children
- Sex offenders
- Requires multi-disciplinary response

Child Victims

Children are not only victims of sexual abuse & exploitation,

Child Victims

Children are not only victims of sexual abuse & exploitation, they are usually *Perfect Victims*

Child Victims

- They are often too trusting
- They often desire attention and affection
- They often desire material things
- They are often curious about sex
- They are often not viewed as credible witnesses

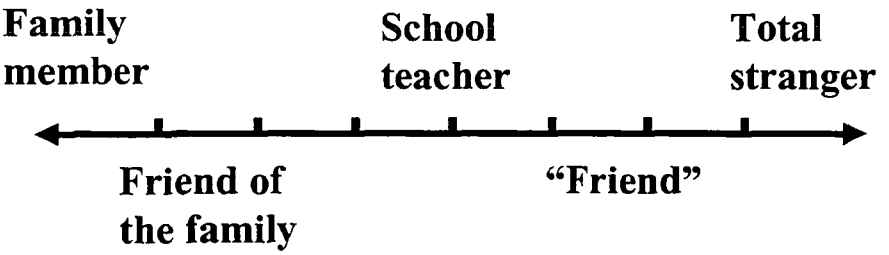
Dynamics of Sexual Abuse

- In the majority of cases, there is no medical evidence
- In most cases, child "knows" the offender
- Child may not want the offender punished
- Almost always occurs in private

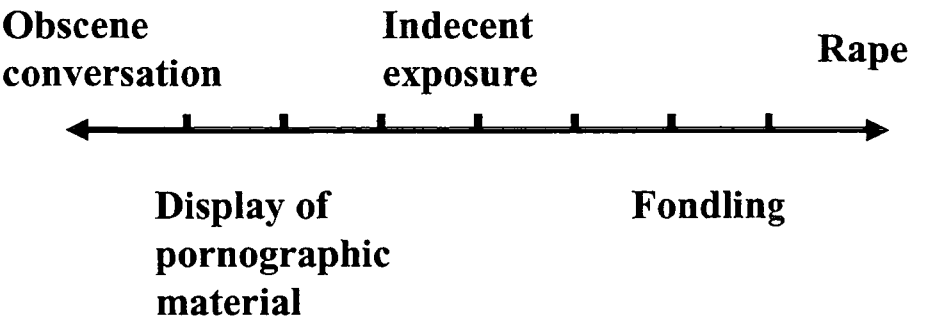
Dynamics of Sexual Abuse

- Relationship of child and offender
- Degree of sexual abuse
- Degree of force involved
- Effect on child

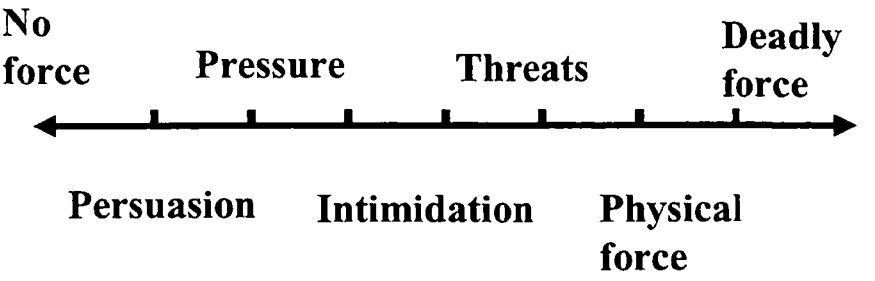
Relationship of Child and Offender



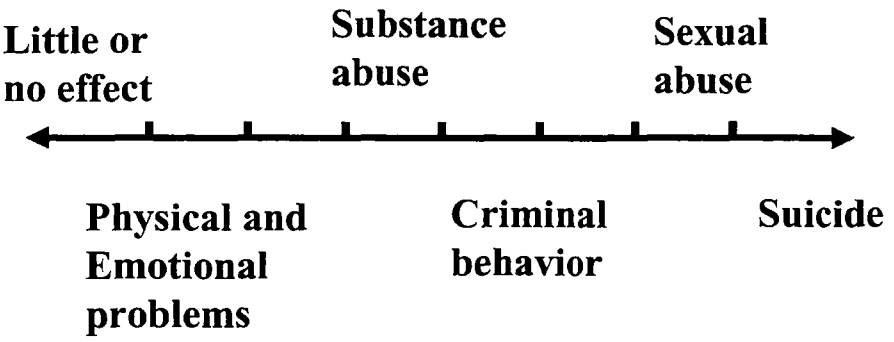
Degree of Sexual Abuse



Degree of Force Involved



Effect on Child Victim



PCO-CCAC-Walsh-31

Disclosure Process

- Some children tell promptly
- Some children delay disclosing
- Some children give partial and/or progressive disclosures
- Some children never tell
- Some disclosures occur accidentally
- Some disclosures are initiated by others

PCO-CCAC-Walsh-32

Reasons for Delayed Disclosures

- May be too embarrassed to tell
- Offender may be related or live with child
- Offender may have legal access to the child
- Child may be financially dependent on the offender

Reasons for Delayed Disclosures

- Child may not want offender exposed or punished, as they fear end to contact
- Child may believe offender's threats, promises
- May may fear punishment for their own *"prohibited conduct"* or participation in sexual behavior
- Child fears being *"grounded"* from using the computer

Forensic Interviews

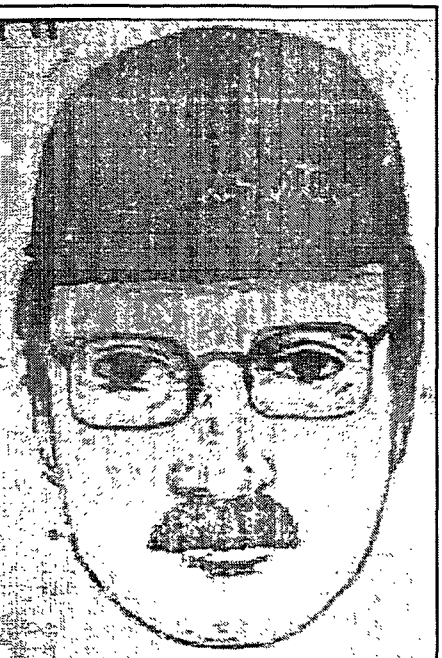
- Quality investigative interviews are critical to the investigation
- Require special training
- Must be legally defensible
- Must be developmentally appropriate

Problem Interview Cases

- McMartin Pre-school - California
- Little Rascals Case- North Carolina
- Fells Acres Case- Massachusetts
- Kelly Michaels Case - New Jersey

Girl, 8, is abducted, assaulted

Continued from Page 1A



PCO-CCAC-Walsh-37

Roger Dale Godbehere . . . could be eligible for parole in 12 years.

trial. Had Mr. Godbehere been con-

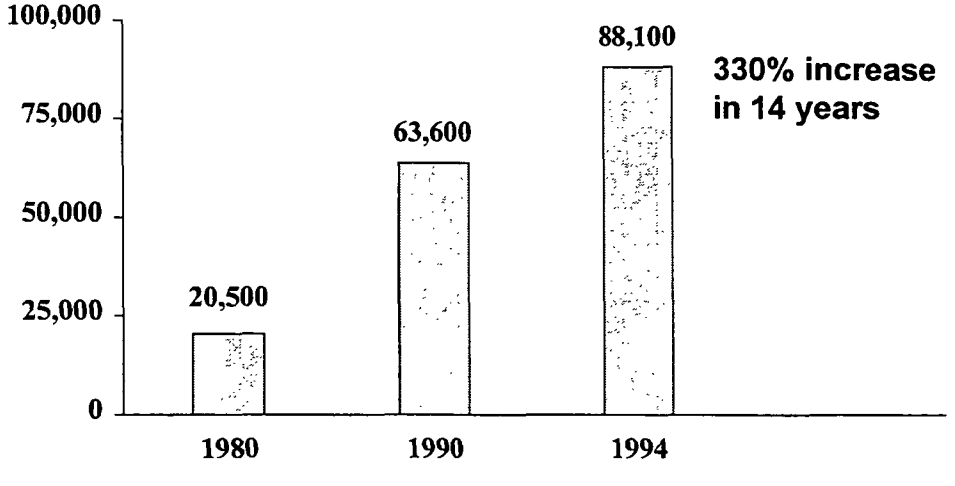
PCO-CCAC-Walsh-38

Dallas police prepared this sketch of the kidnapper

Child Molesters

- In the majority of cases, the victim either knows, or is related to the offender.
  - Intra-familial (Incest, family member)
  - Non-familial (acquaintances)
- Stranger-Danger cases
  - less common, but more dangerous

Sex Offenders in State Prison



DMN 8-17-98

Figures show record number on probation or parole in '97

From Wire Reports

WASHINGTON — A record 3.9 million men and women were on probation or parole in the United States at the end of 1997, the Justice Department said Sunday.

The department's Bureau of Justice Statistics said that 110,000 people were added to the total last year, a 2.9 percent increase. The average annual increase has been 3.0 percent since 1990.

A record has been set each year because of the increasing number of people moving through the criminal justice system since the 1980s.

By the end of 1997, nearly one out of every 35 adults in the United States was in prison, in jail or on probation or parole — a total of 5.7 million adults, or nearly 2.9 percent of the population, the department said.

Felony convictions accounted for 54 percent of the 3,261,838 adults on probation at the end of the year. Another 28 percent had been convicted of misdemeanors.

Convictions for driving while intoxicated or under the influence of alcohol accounted for 14 percent of the probationers.

There were 685,033 adults on parole. Virtually all of them, 96 percent, had been imprisoned on felony convictions.

More than 1.6 million probationers and 400,000 parolees were released from supervision in 1997, the department said. During that year, 18 percent of the probationers and 41 percent of the parolees who were released from supervision wound up incarcerated again because of a rule violation or a new offense.

Texas leads the nation with 328,500 persons under supervision; California had the second-highest number, with 408,900. About one-quarter of the entire supervised population is in these two states.

Texas also has the third-highest rate of supervision, with about three adults out of every 100 on probation or parole.

Experts say that policy changes of some states have contributed to the nationwide increase in the supervised population.

"Neither the arrest rate nor the crime rate has raised in a similar way [as the probation and parole population]," said Kevin Wright, a criminal justice professor at Binghamton University in New York who has conducted research in probation departments.

Mr. Wright said that states seem to be punishing more of the criminals that are caught. "If you look at most state budgets, they have been willing to spend more money on punishment," he said.

The Associated Press and Scripps Howard News Service contributed to this report

PCO-CCAC-Walsh-41

DMN 8-17-98

Figures show record number on probation or parole in '97

From Wire Reports

WASHINGTON — A record 3.9 million men and women were on probation or parole in the United States at the end of 1997, the Justice Department said Sunday.

The department's Bureau of Justice Statistics said that 110,000 people were added to the total last year, a 2.9 percent increase. The average annual increase has been 3.0 percent since 1990.

A record has been set each year because of the increasing number of people moving through the criminal justice system since the 1980s.

By the end of 1997, nearly one out of every 35 adults in the United States was in prison, in jail or on probation or parole — a total of 5.7 million adults, or nearly 2.9 percent of the population, the department said.

Felony convictions accounted for 54 percent of the 3,261,838 adults on probation at the end of the year. Another 28 percent had been convicted of misdemeanors.

Convictions for driving while intoxicated or under the influence of alcohol accounted for 14 percent of the probationers.

There were 685,033 adults on parole. Virtually all of them, 96 percent, had been imprisoned on felony convictions.

More than 1.6 million probationers and 400,000 parolees were released from supervision in 1997, the department said. During that year, 18 percent of the probationers and 41 percent of the parolees who were released from supervision wound up incarcerated again because of a rule violation or a new offense.

Texas leads the nation with 328,500 persons under supervision; California had the second-highest number, with 408,900. About one-quarter of the entire supervised population is in these two states.

Texas also has the third-highest rate of supervision, with about three adults out of every 100 on probation or parole.

Experts say that policy changes of some states have contributed to the nationwide increase in the supervised population.

"Neither the arrest rate nor the crime rate has raised in a similar way [as the probation and parole population]," said Kevin Wright, a criminal justice professor at Binghamton University in New York who has conducted research in probation departments.

Mr. Wright said that states seem to be punishing more of the criminals that are caught. "If you look at most state budgets, they have been willing to spend more money on punishment," he said.

The Associated Press and Scripps Howard News Service contributed to this report

250,000 sex offenders

PCO-CCAC-Walsh-42

Child Molester Types

- For classroom purposes, there are two types of Child Molesters:
  - Situational Sex Offender
  - Preferential Sex Offender

Preferential Sex Offenders

- True preference for child sex partners
- Usually will have multiple victims
- Will go to great lengths to seduce a child
- Circle of friends are younger
- Skillful at manipulating children

Preferential Sex Offenders

- Numerous victims in their lifetime
- High rate of recidivism
- Well proven techniques for obtaining child victims
- Highly motivated to commit sex crimes
- Sexual fantasies focusing on children

Preferential Sex Offenders

- Sexual fantasies focusing on children
  - youth oriented decorations, games, music in their house or apartment
  - may engage in photographing or videotaping children
  - may engage in collecting, producing or trading child pornography or child erotica
  - may use computers as a tool to facilitate their sexual interest in children

Child Pornography

- Legal definition varies by jurisdiction
- If "real" child is involved:
  - Permanent visual record of a child's sexual victimization
  - A picture of a crime in progress
- A tool that facilitates the sexual victimization of children

Types

- Commercial
  - primary purpose is for profit
- Homemade
  - made for the offender's own purposes
- Digitally produced

Why Offenders Collect Child Pornography/Erotica

- Satisfy their excessive compulsive sexual fantasies about children
- Validation of their behavior
- Souvenir/Trophy of their sexual activities

Offender's Uses

- Made for the offender's own purposes
  - »sexual gratification *
  - »lowering the child's inhibitions *
  - »as a medium of exchange *
  - »blackmailing the victim
  - »rarely used for profit
    - * may also apply to commercial

Formats

- Film images
  - photographs
    - » Polaroid pictures
    - » 35 mm prints
  - Movie film
    - » 8mm & 16m
      - home movies
      - loops

Formats

- Video tape
  - VHS
  - 8 mm
  - Compact VHS
  - Beta
  - PAL

Formats

- Published material
  - magazines
    - » Lolita, Lolitot, Piccolo, Child Love
  - Photo sets

Formats

- Computer images
  - scanned images
  - downloaded files
  - video conferencing
  - computer generated
    - » morphed
    - » digitally produced

Court upholds law on child-sex images

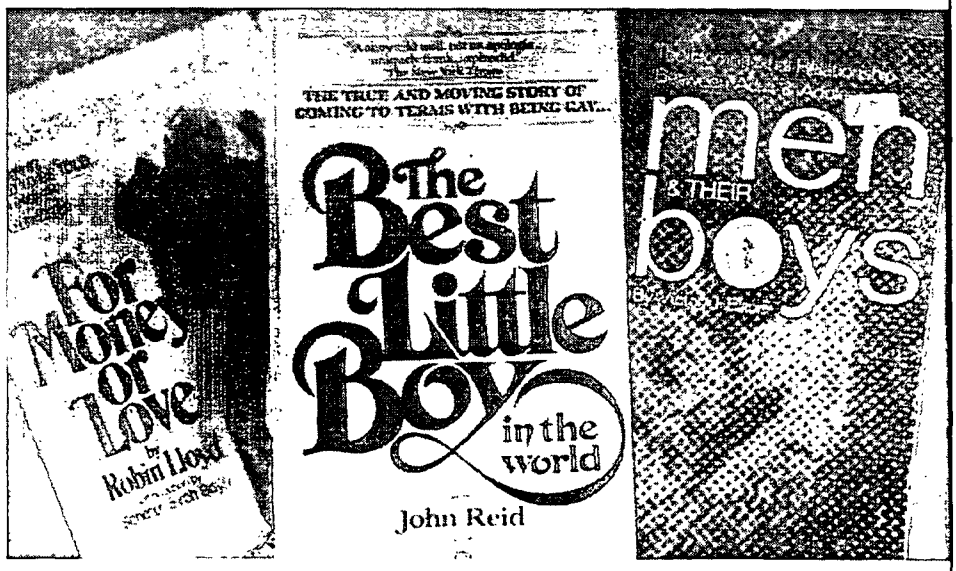
■ **PORTLAND, Maine** — A federal appeals court upheld a federal law that makes it illegal to possess computer images that look like children engaged in sex. The decision, made Wednesday in Boston, overturned the ruling of a lower court judge who declared the law unconstitutional. The law targets computer technology that can be used to alter an innocent image of a child into a picture of a child engaged in a sexually explicit act. It's the first time a federal appeals court has ruled on the Child Pornography Protection Act of 1996, U.S. Attorney Jay McCloskey said Friday.

Child Erotica

- **Any item that may cause sexual arousal in someone sexually interested in children**
  - **photos or videos of children**
  - **children's or teen's magazines**
  - **children's underwear or clothing**
  - **toys, sex devices, souvenirs of contact or sexual activity with children**

Child Erotica

- books, magazines and videos about children, child development, child sexual abuse, medical books & journals
- nudist magazines, pornographic teaser material, cut-and-paste child porn
- personal writings, newspaper & magazine clippings



Investigative Importance

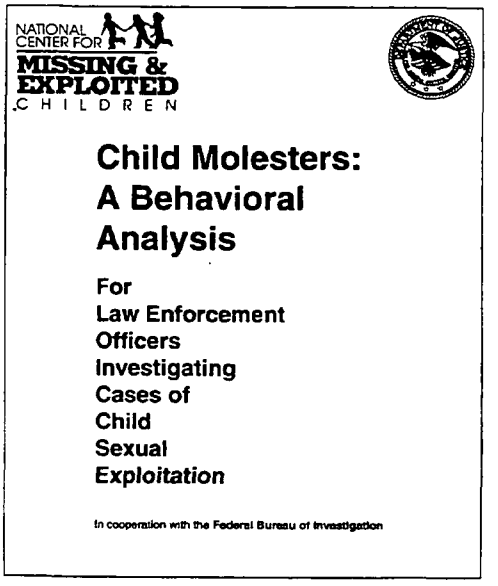
- *"The Collection"* is comprised of child pornography and child erotica
- It may provide clues to:
  - identity of child victims and offenders
  - items for purposes of corroboration
  - subject's preference in sexual activities
  - subject's specific victim preferences
    - » age, race, gender, physical attributes

Situational Sex Offender

- Sex offense may be part of another crime, residential burglary, carjacking, armed home invasion/robbery
- Victim is incidental, rather than targeted
- This offender may be a drifter and a loner
- This offender is more likely to harm or kill the victim

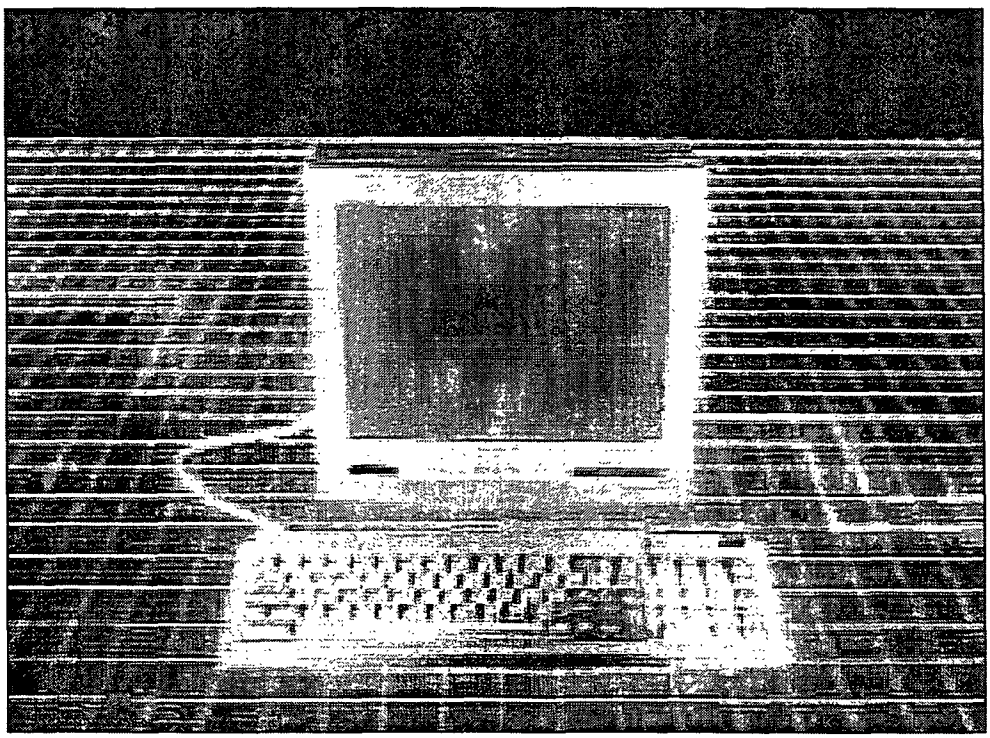
Situational Sex Offender

- Does not have a true preference for a child
- Will commit crimes against:
  - Senior Citizens
  - Prostitutes
  - Homeless and Street People
  - Mentally Incapacitated People
  - Any available victim



Child Molester Types

- Computer technology and the Internet may have identified and/or produced a new offender, i.e., the Preferential / Situational Sex Offender
  - Offender with no criminal record
  - Juvenile offender



The Keyboard Kids

Chatting on the Net is becoming the social activity of choice for techno-savvy early teens. BY BRAD STONE

AS SUMMER, THOSE LAZY AFTERnoons with the hot sun slowly giving way to the gentle winds, the homeward wing of birds and the sound of children playing . . . indoors on computers.

Yep, we've raised a generation of keyboard kids, and they're spending more, chatting more, making more long-distance friends and generally getting into more trouble online than ever before. As usual, it's up to their beleaguered parents to maintain a watchful eye—the same parents, of course, who in school he Dwyer are widely considered as clueless about their identities as they are about Portishead is lonely. Weird children, particularly in the formative years from about 10 to 14, are eager for their first taste of independence, intrigued by the promiscuity of naughty stuff and feeling in the online world a means to navigate the minefield of adolescent awkwardness. "You can open up more and say what you want," says one 12-year-old America Online user. "I feel more comfortable among them as [anyone] people."

According to a recent study by the research group Paul, SVP, more than 8.8 million children are using the Internet, a number few projected to triple in the next few years. Aggressive marketer AOL now gets 52 percent of the 12-to-17 audience, says Web research firm PC Meter. Some of these numbers are coming at the expense of television. In a recent poll by CNN and USA Today, 54 percent of teens said they could live without their TV, but only 23 percent said they could get by without a computer. Perhaps the most sobering statistic of all: at the peak of "Titanic" mania, AOL says, there was a message posted about Leonardo DiCaprio every 30 seconds.

Twelve-year-old Liz contributed to that collective total. The Westchester County, N.Y., seventh grader comes home every day from school, jumps on AOL and meets up with, of all people, her schoolmates. She chats with them in member-only private chat rooms and sends Instant Messages (in the 203 friends she keeps on her Buddy List, the AOL function that alerts her when they sign on. She's also a publisher, working with two friends to send an e-mail newsletter on teen topics to 1,000 subscribers. The first issues a day she spends on AOL explains how spent watching television and using the phone. Her mother doesn't use the parental controls that AOL provides to block all adult areas. It she wanted to, Liz says cheerfully, "I would let her, but she is not very computer-literate."

Liz's mother is not alone. AOL says 52 percent of parents don't use the controls, even though they have increased in the past year. Last December AOL revamped the younger teen area and has since spruced up its related interests options. But run away kids from the private chat rooms where strangers can't penetrate and even hide the last obvious material on AOL and the Web. Parents can also specify exactly what their children can get to mail from and block the

FOCUS ON TECHNOLOGY

The Keyboard Kids

Chatting on the Net is becoming the social activity of choice for techno-savvy early teens. BY BRAD STONE

AS SUMMER, THOSE LAZY AFTERnoons with the hot sun slowly giving way to the gentle winds, the homeward wing of birds and the sound of children playing . . . indoors on computers.

Yep, we've raised a generation of keyboard kids, and they're spending more, chatting more, making more long-distance friends and generally getting into more trouble online than ever before. As usual, it's up to their beleaguered parents to maintain a watchful eye—the same parents, of course, who in school he Dwyer are widely considered as clueless about their identities as they are about Portishead is lonely. Weird children, particularly in the formative years from about 10 to 14, are eager for their first taste of independence, intrigued by the promiscuity of naughty stuff and feeling in the online world a means to navigate the minefield of adolescent awkwardness. "You can open up more and say what you want," says one 12-year-old America Online user. "I feel more comfortable among them as [anyone] people."

According to a recent study by the research group Paul, SVP, more than 8.8 million children are using the Internet, a number few projected to triple in the next few years. Aggressive marketer AOL now gets 52 percent of the 12-to-17 audience, says Web research firm PC Meter. Some of these numbers are coming at the expense of television. In a recent poll by CNN and USA Today, 54 percent of teens said they could live without their TV, but only 23 percent said they could get by without a computer. Perhaps the most sobering statistic of all: at the peak of "Titanic" mania, AOL says, there was a message posted about Leonardo DiCaprio every 30 seconds.

Twelve-year-old Liz contributed to that collective total. The Westchester County, N.Y., seventh grader comes home every day from school, jumps on AOL and meets up with, of all people, her schoolmates. She chats with them in member-only private chat rooms and sends Instant Messages (in the 203 friends she keeps on her Buddy List, the AOL function that alerts her when they sign on. She's also a publisher, working with two friends to send an e-mail newsletter on teen topics to 1,000 subscribers. The first issues a day she spends on AOL explains how spent watching television and using the phone. Her mother doesn't use the parental controls that AOL provides to block all adult areas. It she wanted to, Liz says cheerfully, "I would let her, but she is not very computer-literate."

Liz's mother is not alone. AOL says 52 percent of parents don't use the controls, even though they have increased in the past year. Last December AOL revamped the younger teen area and has since spruced up its related interests options. But run away kids from the private chat rooms where strangers can't penetrate and even hide the last obvious material on AOL and the Web. Parents can also specify exactly what their children can get to mail from and block the

"According to a recent study by the research group Find/SVP, more than 9.8 million children are using the Internet, a number projected to triple in the next four years."

NEWSWEEK June 8, 1998

PCO-CCAC-Walsh-67

TIME/CNN TEEN POLL *

Telephone interview with 409 teenagers aged 13-17

- 82% use the Internet for e-mail, chat rooms or visiting websites
- 44% have visited websites with X-rated or sexual content

** April 27-29, 1999*

PCO-CCAC-Walsh-68

TIME/CNN TEEN POLL

Asked of the 341 teenagers that admitted to using the Internet:

- **What do your parents know about the websites you visit?**
  - **38 % A lot**
  - **45% A little**
  - **17% Nothing**

TIME/CNN TEEN POLL

- **Do your parents have rules about your Internet use, and do you follow them?**
  - **31% Yes, and always follow them**
  - **26% Yes, but don't always follow them**
  - **43% No, parents don't have rules**

TIME/CNN TEEN POLL

- **Have you ever encountered people online who you suspect are pretending to be someone that they're not?**

YES	
Girls	Boys
72%	57%

TIME/CNN TEEN POLL

- **Have you ever encountered people online who want personal information like your address or phone number?**

YES	
Girls	Boys
58%	39%

Impact of Computer Technology on the Sexual Abuse of Children

Advancements in computer technology

Offender's sexual interest in children

\+ Children's increased use of computers

= *Increased use of computers by sex offenders in the sexual abuse and exploitation of children*

Unique Problems Encountered with Sexual Abuse Investigations

- Child victims
- Dynamics of sexual abuse
- Disclosure process
- Forensic interviews of children
- Sex offenders
- Requires multi-disciplinary response

Unique Problems Encountered with Sexual Abuse Investigations

- Child victims
- Dynamics of sexual abuse
- Disclosure process
- Forensic interviews of children
- Sex offenders
- Requires multi-disciplinary response
- *Backlash*

Complex Jurisdictional Issues

- Who has jurisdiction?
  - Municipal
  - County
  - State
  - Federal
    - » FBI
    - » US Customs
    - » US Postal Service
    - » Secret Service

Complex Jurisdictional Issues

- Trafficking in child pornography
- Traveler cases
- What if investigation involves multiple jurisdictions?
  - Who's in charge?
  - Sharing of information, resources
  - Prosecution (State or Federal?)
  - Publicity (Who decides when?)
  - Civil forfeiture (Who gets what?)

Complex Technical Issues

- Seizure of computer equipment as evidence
- Transportation and storage of computer and related storage media as evidence
- Forensic evaluation of computer equipment and related storage media

Complex Legal Issues

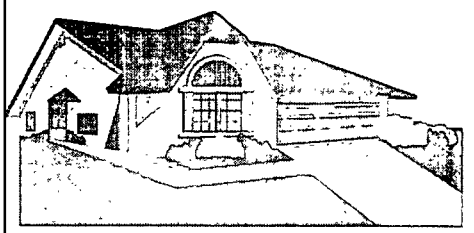
- Knowing and understanding relevant state and federal law
  - When to use search warrant
  - When to use court order
  - When to use subpoena
- Individual and agency exposure to civil liability

Complex Investigative Issues

- Identifying the victims
- Interviewing the child about computer related issues
- Identifying the suspect
- Interviewing and interrogating the suspect about computer related issues

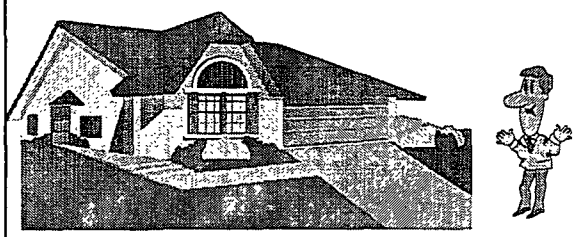
PCO-CCAC-Walsh-81

Relationship of Child and Offender



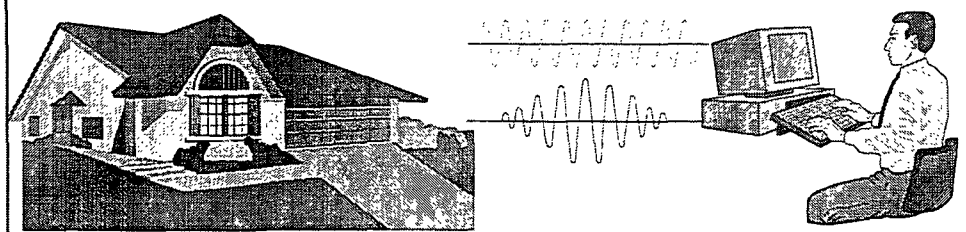
PCO-CCAC-Walsh-82

Relationship of Child and Offender



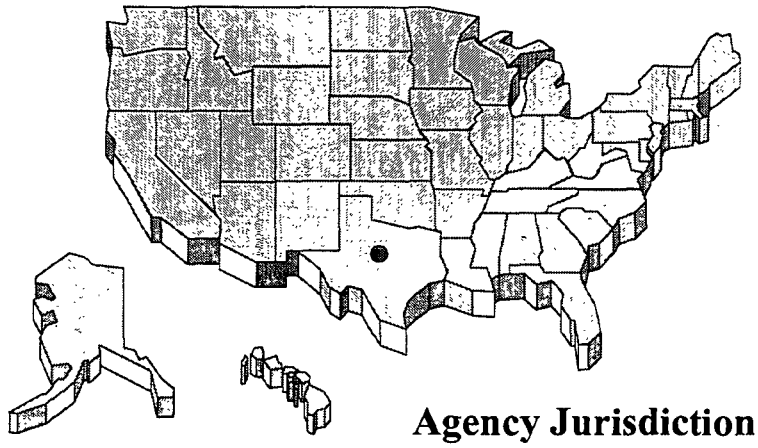
PCO-CCAC-Walsh-83

Relationship of Child and Offender



PCO-CCAC-Walsh-84

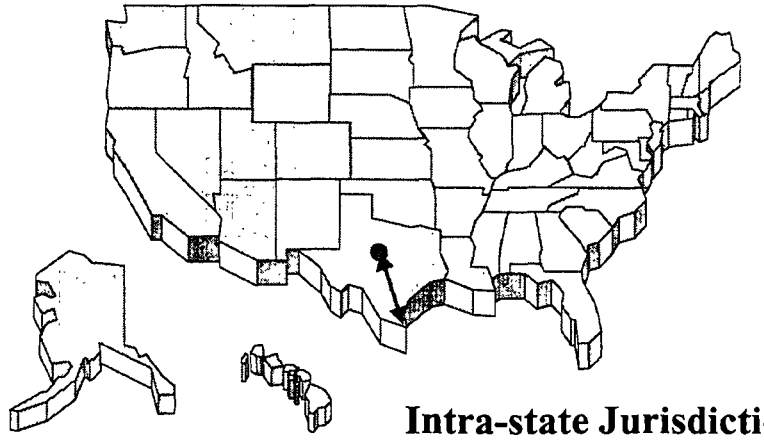
Relationship of Child and Offender



Agency Jurisdiction

PCO-CCAC-Walsh-85

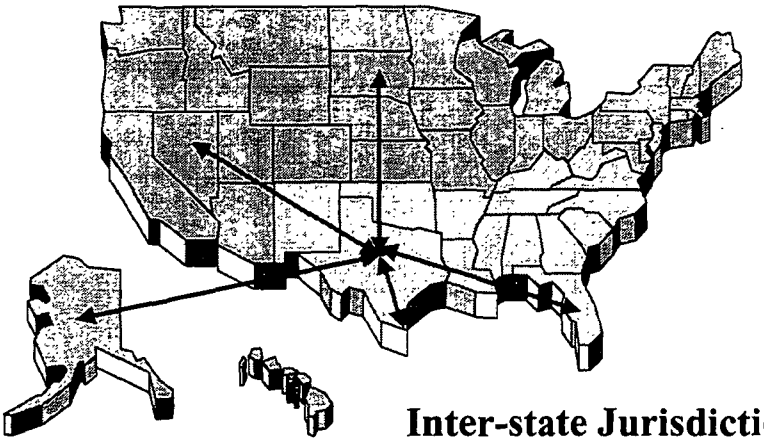
Relationship of Child and Offender



Intra-state Jurisdiction

PCO-CCAC-Walsh-86

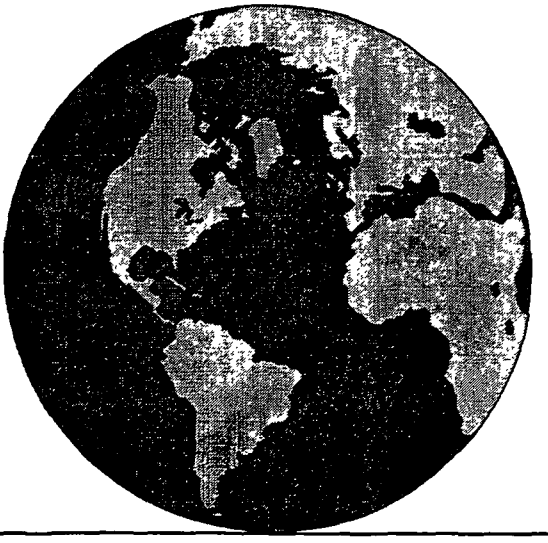
Relationship of Child and Offender



Inter-state Jurisdiction

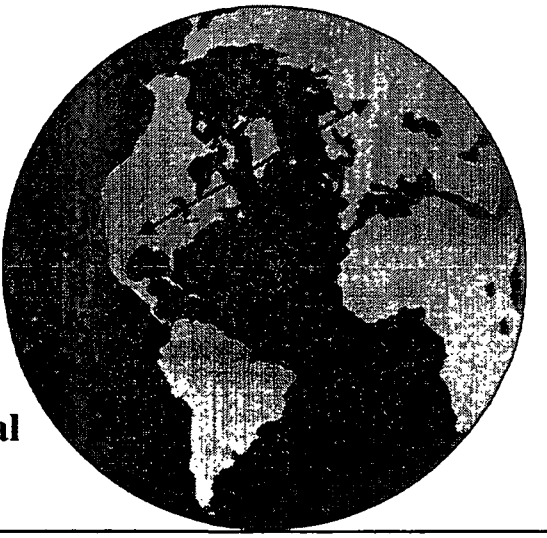
PCO-CCAC-Walsh-87

Relationship of Child and Offender



PCO-CCAC-Walsh-88

Relationship of Child and Offender



International Jurisdiction

PCO-CCAC-Walsh-89

Abilene man gets six years in computer child porn case

Associated Press

SAN ANGELO, Texas — After a yearlong investigation by U.S. Customs Service agents, an Abilene man has been sentenced to six years in prison for violating federal child pornography laws.

It took a federal jury 20 minutes Friday to find Terry Burton Kimbrough guilty of importing child pornography, possession of child pornography and interstate transportation of child pornography in Northern District Court in Lubbock. He will remain free on bond pending appeal.

Mr. Kimbrough, 30, was originally indicted by a federal jury in July 1992 as part of a customs investigation known as "Operation Longarm." He was arrested Aug. 10, 1993 by customs agents in San Angelo.

Operation Longarm resulted in 31 search warrants in 15 states and 30 cities across the country. Customs agents investigated the buying and distribution of child pornography from Denmark via computer bulletin boards.

Mr. Kimbrough's case set a precedent by becoming the first federal jury trial conviction involving the importation of child pornography by computer.

PCO-CCAC-Walsh-90

Degree of Sexual Abuse

All types of sexual abuse are facilitated by the offender's use of computers

Obscene conversation

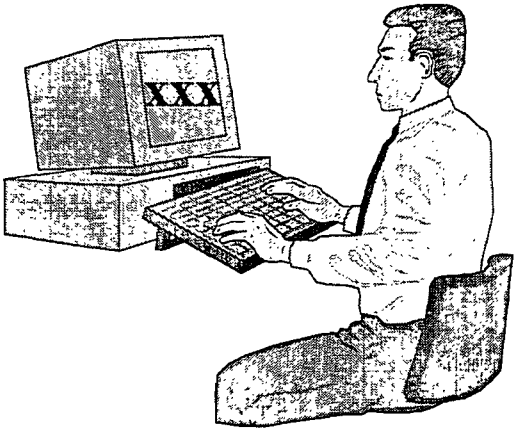
Indecent exposure

Rape

Display of pornographic material

Fondling

Computers as Tools used for the Sexual Abuse of Children

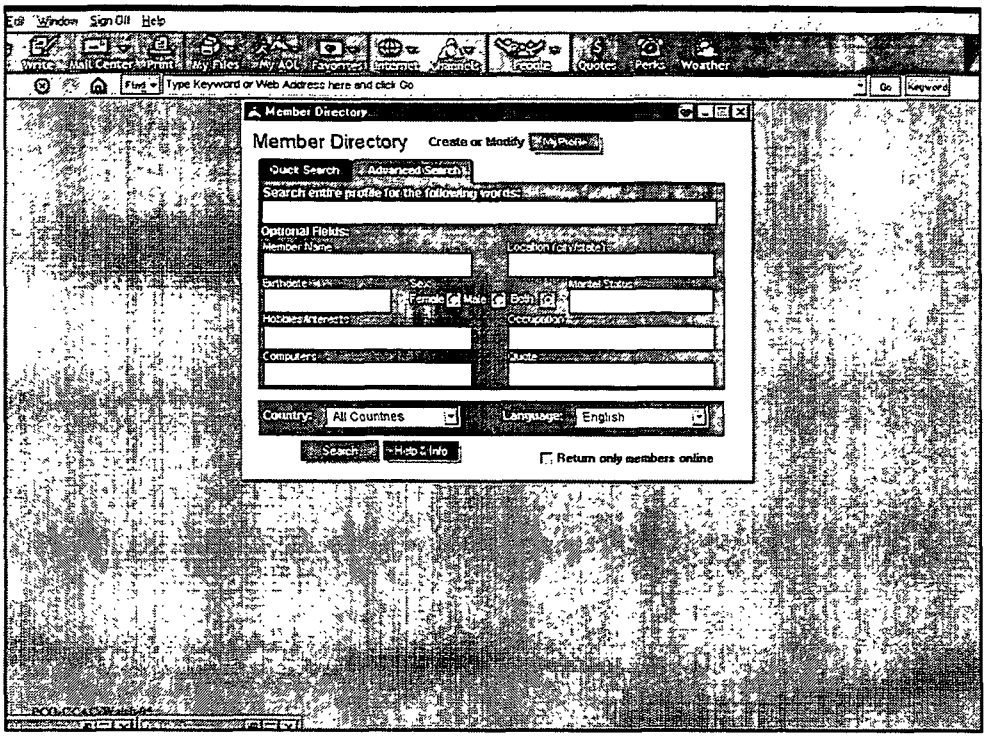


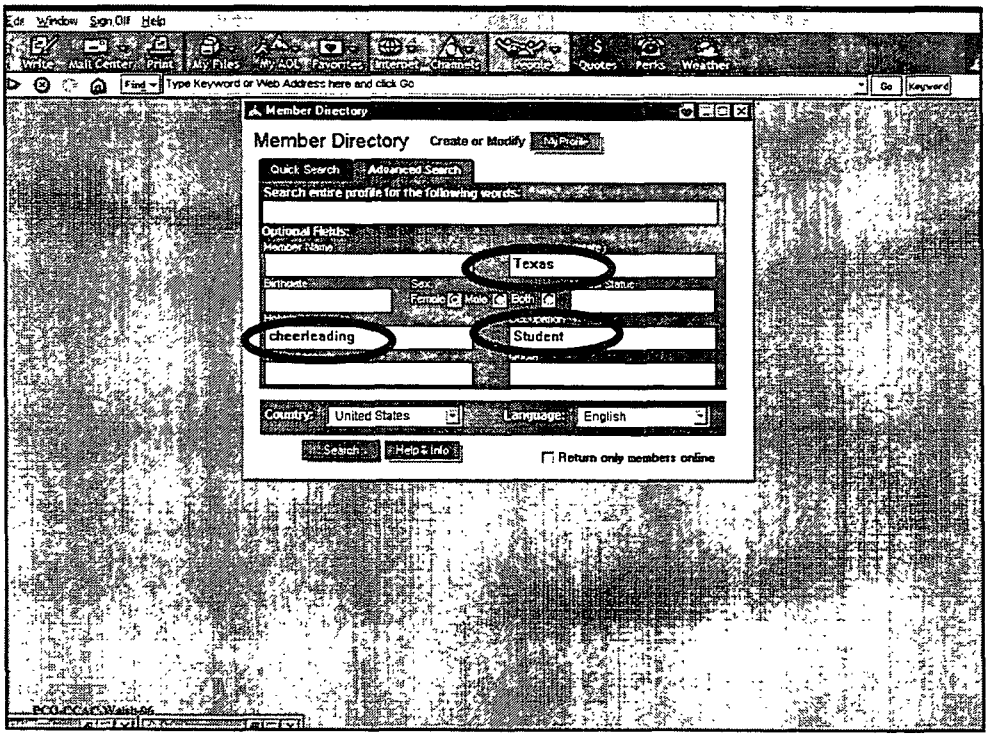
Computers Appeal to Offenders

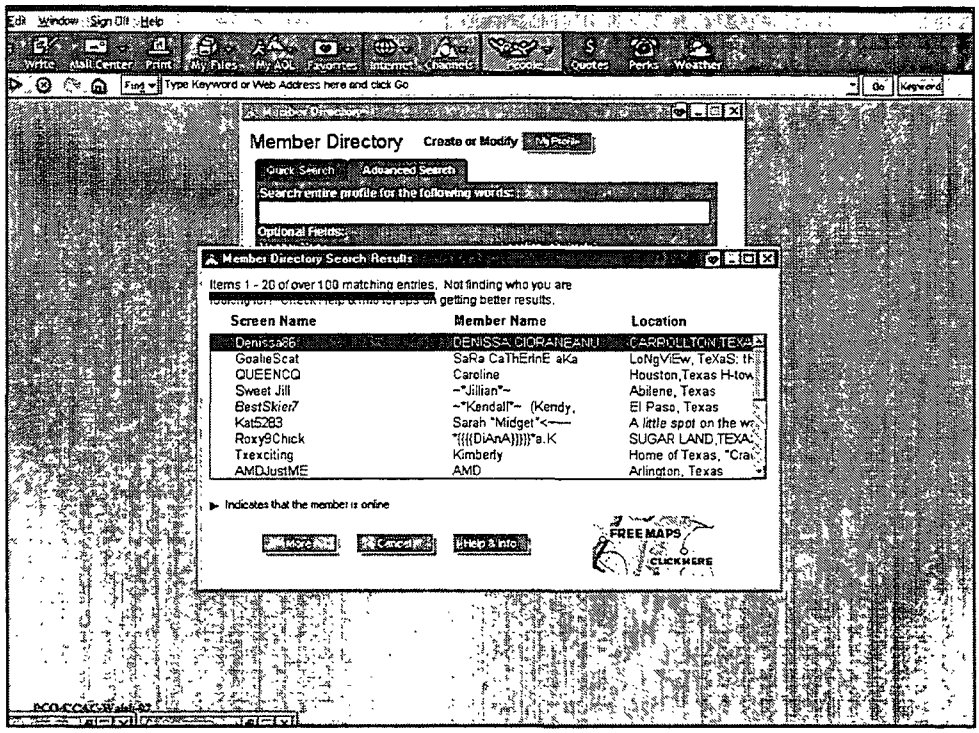
- Tool that facilitates their interest in children
- Provides the offender with:
  - Privacy
  - Anonymity
  - Instant gratification
  - Easy accessibility
  - Security

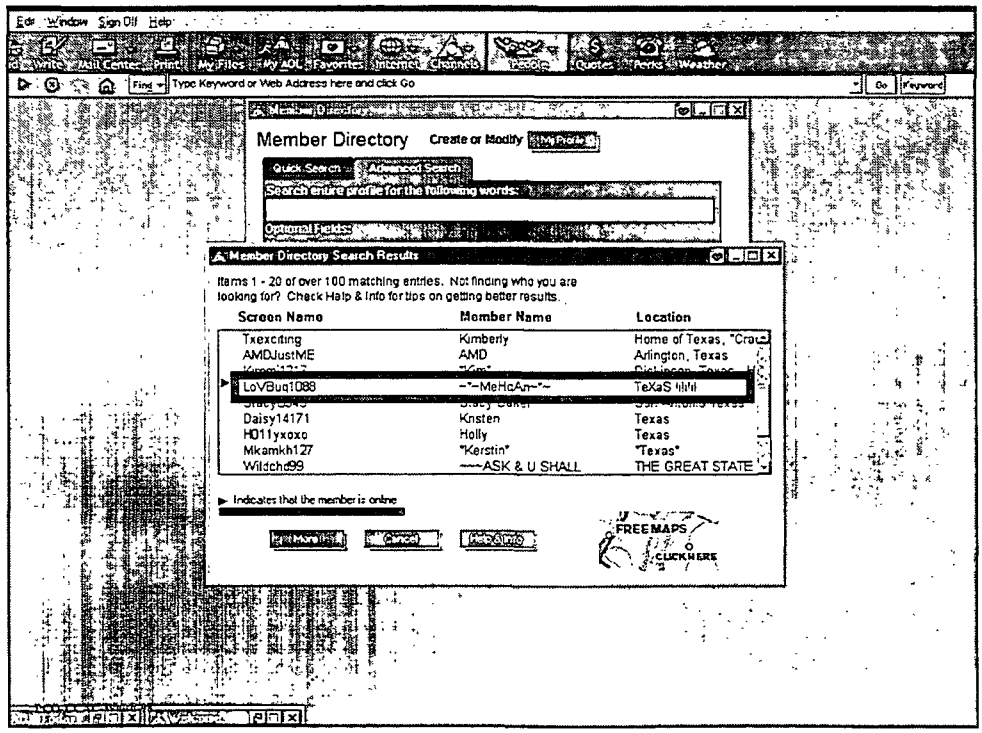
Computers Appeal to Offenders

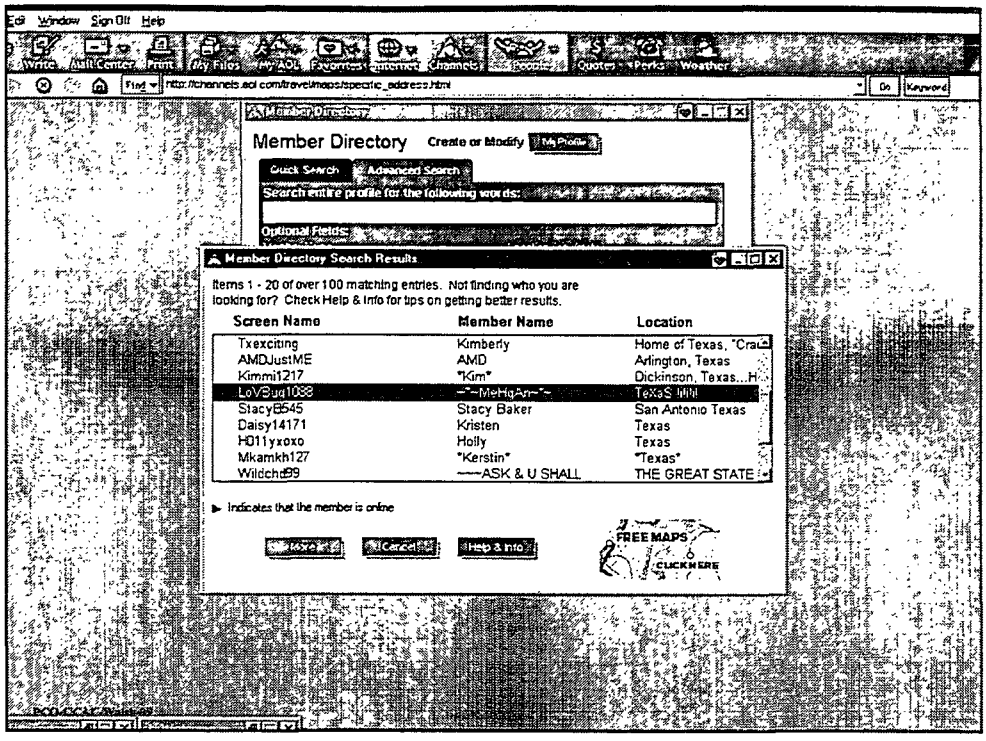
- Expanded opportunity for contact with children

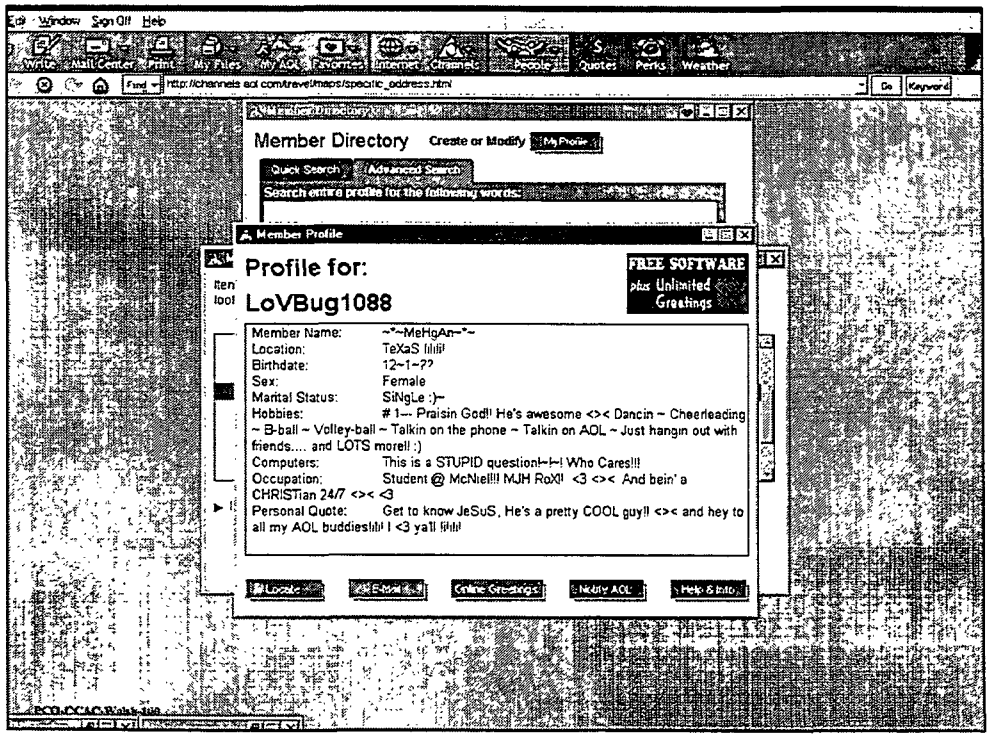

Edit Window Sign Off Help
Write Mail Center Print My Files My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go Keyword
Member Directory
Member Directory Create or Modify My Profile
Quick Search Advanced Search
Search entire profile for the following words:
Optional Fields:
Member Name
Location (City, State)
Birthdate
Sex: Female Male Both
Marital Status
Hobbies/Interests
Occupation
Computers
Quote
Country: All Countries
Language: English
Search Help & Info
Return only members online

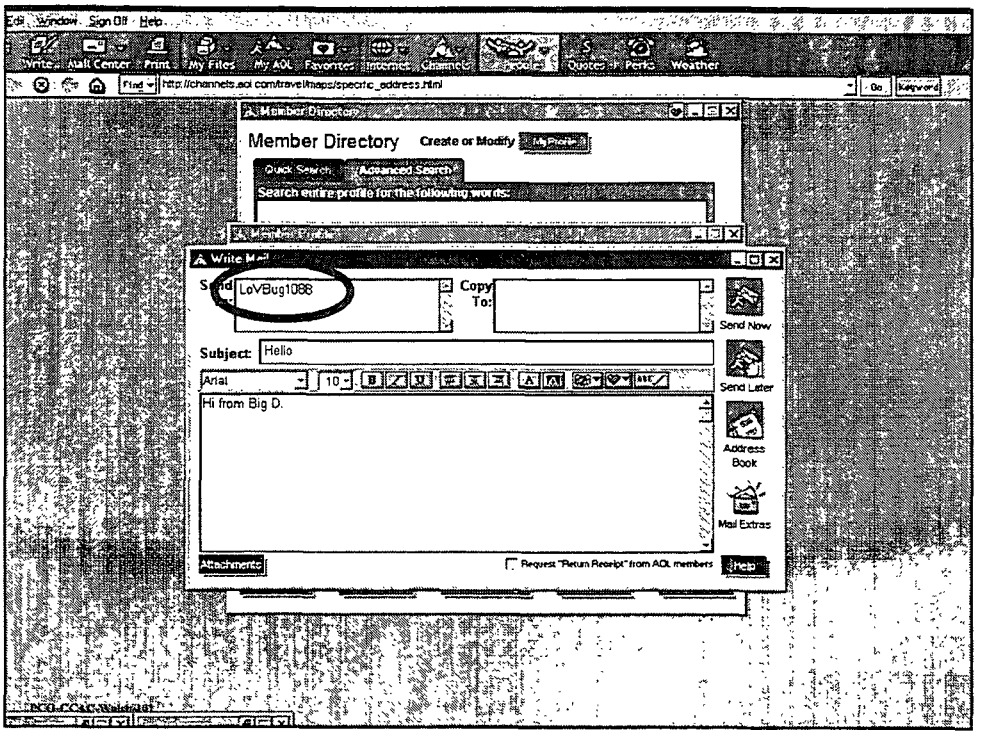

Edit Window Sign Off Help
Write Mail Center Print My Files My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go Keyword
Member Directory
Member Directory Create or Modify My Profile
Quick Search Advanced Search
Search entire profile for the following words:
Optional Fields:
Member Name
Texas
Birthdate
Sex: Female Male Both
Marital Status
cheerleading
Occupation
Student
Country: United States
Language: English
Search Help & Info
Return only members online


Edit Window Sign Off Help
Write Mail Center Print My Files My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go Keyword
Member Directory Create or Modify My Profile
Quick Search Advanced Search
Search entire profile for the following words:
Optional Fields:
Member Directory Search Results
Items 1 - 20 of over 100 matching entries. Not finding who you are looking for? Check Help & Info for tips on getting better results.
Screen Name Member Name Location
Denissa86 DENISSA CIORANEANU CARROLLTON,TEXAS
GoalieScat SaRa CaThErInE aKa LoNgViEw, TeXaS: th
QUEENCQ Caroline Houston,Texas H-tow
Sweet Jill ~*Jillian*~ Abilene, Texas
BestSkier7 ~*Kendall*~ (Kendy, El Paso, Texas
Kat5283 Sarah "Midget"<— A little spot on the wo
Roxy9Chick "{{{{DiAnA}}}}"a.K SUGAR LAND,TEXAS
Txexciting Kimberly Home of Texas, "Cra
AMDJustME AMD Arlington, Texas
Indicates that the member is online
More Info Cancel Help & Info
FREE MAPS CLICK HERE


Edit Window Sign Off Help
Write Mail Center Print My Files My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go Keyword
Member Directory Create or Modify My Profile
Quick Search Advanced Search
Search entire profile for the following words:
Optional Fields:
Member Directory Search Results
Items 1 - 20 of over 100 matching entries. Not finding who you are looking for? Check Help & Info for tips on getting better results.
Screen Name Member Name Location
Txexciting Kimberly Home of Texas, "Cra
AMDJustME AMD Arlington, Texas
LoVBug1088 ~*~MeHcAm~*~ TeXaS !!!!!
Daisy14171 Kristen Texas
H011yxoxo Holly Texas
Mkamkh127 "Kerstin" "Texas"
Wildchd99 ~~ASK & U SHALL THE GREAT STATE
Indicates that the member is online
More Info Cancel Help & Info
FREE MAPS CLICK HERE

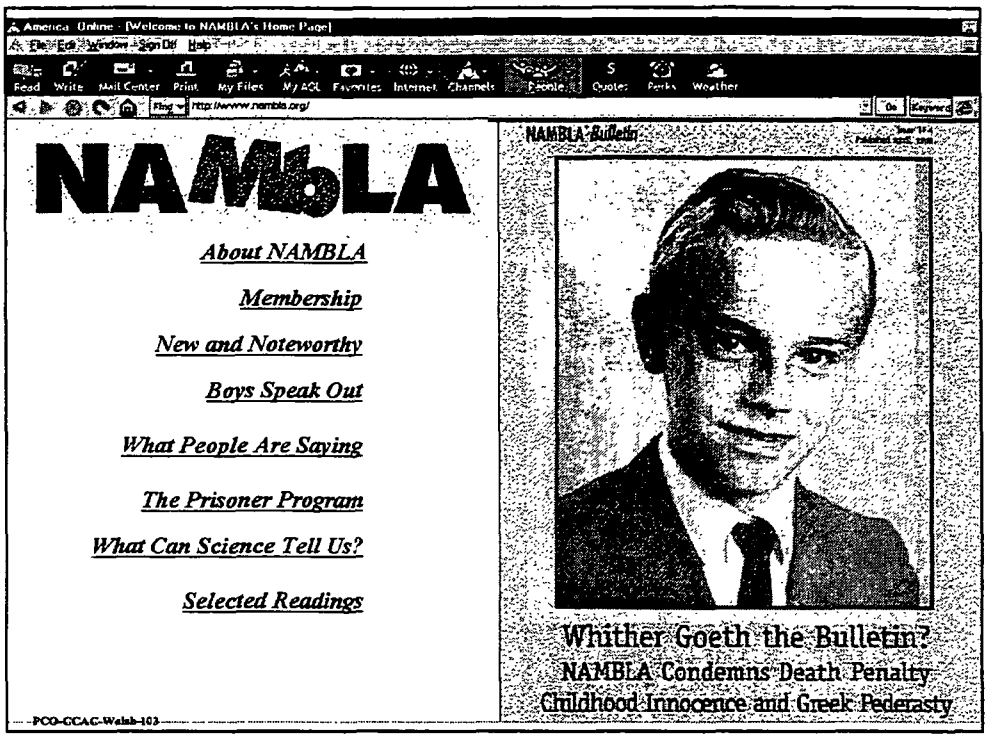

Member Directory
Create or Modify
Quick Search
Advanced Search
Search entire profile for the following words:
Optional Fields:
Member Directory Search Results
Items 1 - 20 of over 100 matching entries. Not finding who you are looking for? Check Help & Info for tips on getting better results.
Screen Name
Member Name
Location
Txexciting
Kimberly
Home of Texas, "Cra
AMDJustME
AMD
Arlington, Texas
Kimmi1217
"Kim"
Dickinson, Texas...H
LoVBug1088
~*~MeHgAn~*~
TeXaS !!!!!
StacyB545
Stacy Baker
San Antonio Texas
Daisy14171
Kristen
Texas
H011yxoxo
Holly
Texas
Mkamkh127
"Kerstin"
"Texas"
Wildchd99
~~ASK & U SHALL
THE GREAT STATE
Indicates that the member is online
Locate
Cancel
Help & Info
FREE MAPS
CLICK HERE

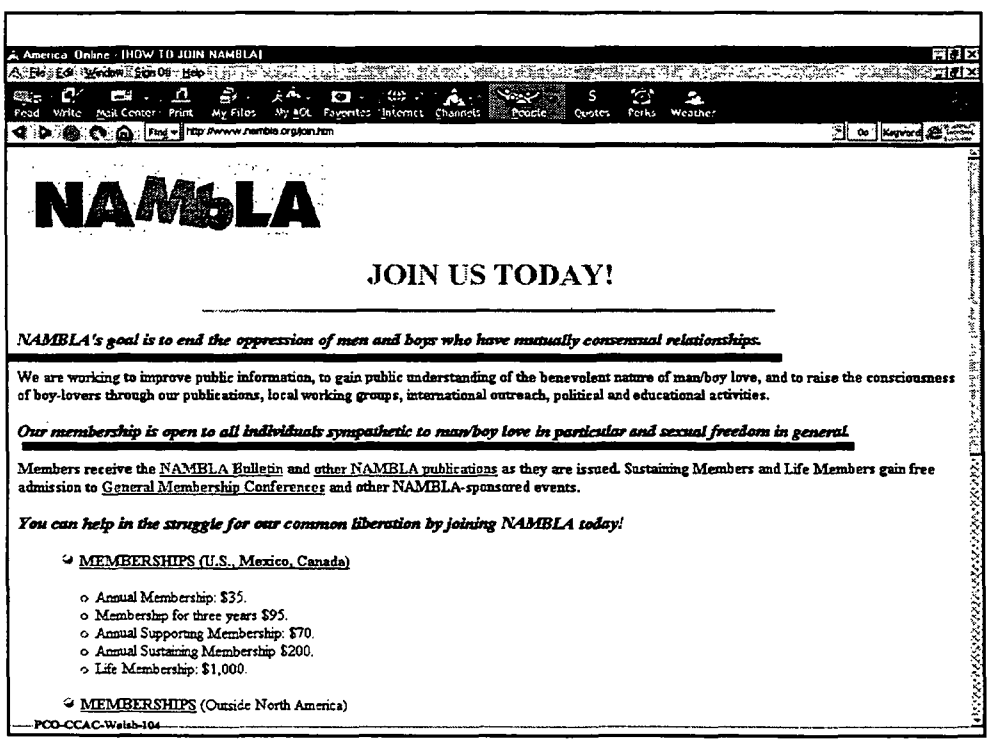

Member Directory
Create or Modify
Quick Search
Advanced Search
Search entire profile for the following words:
Member Profile
Profile for:
LoVBug1088
FREE SOFTWARE
plus Unlimited Greetings
Member Name: ~*~MeHgAn~*~
Location: TeXaS !!!!!
Birthdate: 12~1~??
Sex: Female
Marital Status: SiNgLe :)~
Hobbies: # 1~~ Praisin God!! He's awesome <>< Dancin ~ Cheerleading ~ B-ball ~ Volley-ball ~ Talkin on the phone ~ Talkin on AOL ~ Just hangin out with friends.... and LOTS more!! :)
Computers: This is a STUPID question!~!~! Who Cares!!!
Occupation: Student @ McNiel!!!! MJH RoX!! <3 <>< And bein' a CHRISTian 24/7 <>< <3
Personal Quote: Get to know JeSuS, He's a pretty COOL guy!! <>< and hey to all my AOL buddies!!!! I <3 ya!!! !!!!
Locate
Send Mail
Online Greetings
Notify AOL
Help & Info

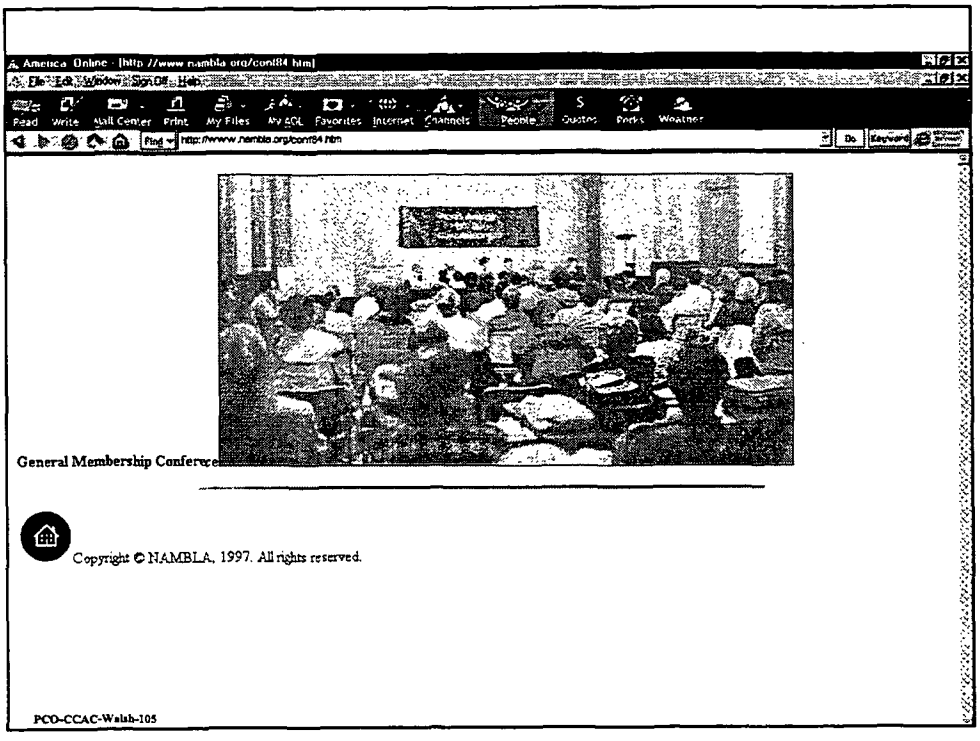


Computers Appeal to Offenders

- **Expanded opportunity for contact with children**
- **Provides them with a sense of *"legitimacy"* and *"acceptability"* for their *"interest in children"***


America Online - [Welcome to NAMBLA's Home Page]
NAMbLA
About NAMBLA
Membership
New and Noteworthy
Boys Speak Out
What People Are Saying
The Prisoner Program
What Can Science Tell Us?
Selected Readings
NAMBLA Bulletin
Whither Goeth the Bulletin?
NAMBLA Condemns Death Penalty
Childhood Innocence and Greek Pederasty
PCO-CCAC-Walsh-103

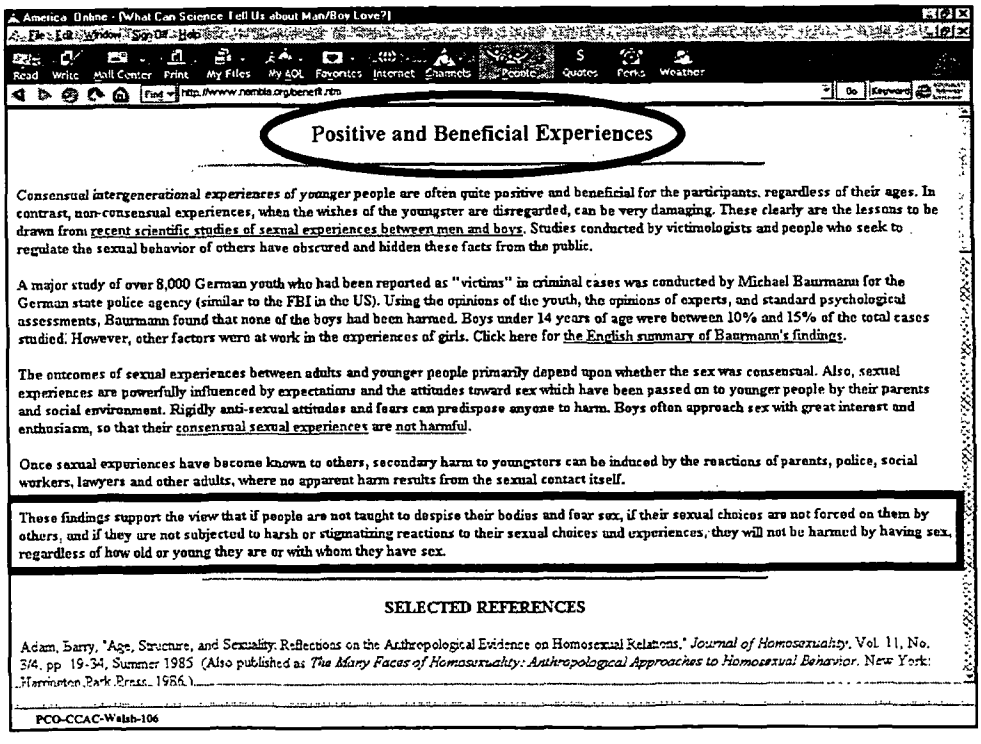

America Online - [HOW TO JOIN NAMBLA]
NAMbLA
JOIN US TODAY!
NAMBLA's goal is to end the oppression of men and boys who have mutually consensual relationships.
We are working to improve public information, to gain public understanding of the benevolent nature of man/boy love, and to raise the consciousness of boy-lovers through our publications, local working groups, international outreach, political and educational activities.
Our membership is open to all individuals sympathetic to man/boy love in particular and sexual freedom in general.
Members receive the NAMBLA Bulletin and other NAMBLA publications as they are issued. Sustaining Members and Life Members gain free admission to General Membership Conferences and other NAMBLA-sponsored events.
You can help in the struggle for our common liberation by joining NAMBLA today!
MEMBERSHIPS (U.S., Mexico, Canada)
Annual Membership: $35.
Membership for three years $95.
Annual Supporting Membership: $70.
Annual Sustaining Membership $200.
Life Membership: $1,000.
MEMBERSHIPS (Outside North America)
PCO-CCAC-Walsh-104



General Membership Conference

Copyright © NAMBLA, 1997. All rights reserved.

PCO-CCAC-Walsh-105



Positive and Beneficial Experiences

Consensual intergenerational experiences of younger people are often quite positive and beneficial for the participants, regardless of their ages. In contrast, non-consensual experiences, when the wishes of the youngster are disregarded, can be very damaging. These clearly are the lessons to be drawn from recent scientific studies of sexual experiences between men and boys. Studies conducted by victimologists and people who seek to regulate the sexual behavior of others have obscured and hidden these facts from the public.

A major study of over 8,000 German youth who had been reported as "victims" in criminal cases was conducted by Michael Baurmann for the German state police agency (similar to the FBI in the US). Using the opinions of the youth, the opinions of experts, and standard psychological assessments, Baurmann found that none of the boys had been harmed. Boys under 14 years of age were between 10% and 15% of the total cases studied. However, other factors were at work in the experiences of girls. Click here for the English summary of Baurmann's findings.

The outcomes of sexual experiences between adults and younger people primarily depend upon whether the sex was consensual. Also, sexual experiences are powerfully influenced by expectations and the attitudes toward sex which have been passed on to younger people by their parents and social environment. Rigidly anti-sexual attitudes and fears can predispose anyone to harm. Boys often approach sex with great interest and enthusiasm, so that their consensual sexual experiences are not harmful.

Once sexual experiences have become known to others, secondary harm to youngsters can be induced by the reactions of parents, police, social workers, lawyers and other adults, where no apparent harm results from the sexual contact itself.

These findings support the view that if people are not taught to despise their bodies and fear sex, if their sexual choices are not forced on them by others, and if they are not subjected to harsh or stigmatizing reactions to their sexual choices and experiences, they will not be harmed by having sex, regardless of how old or young they are or with whom they have sex.

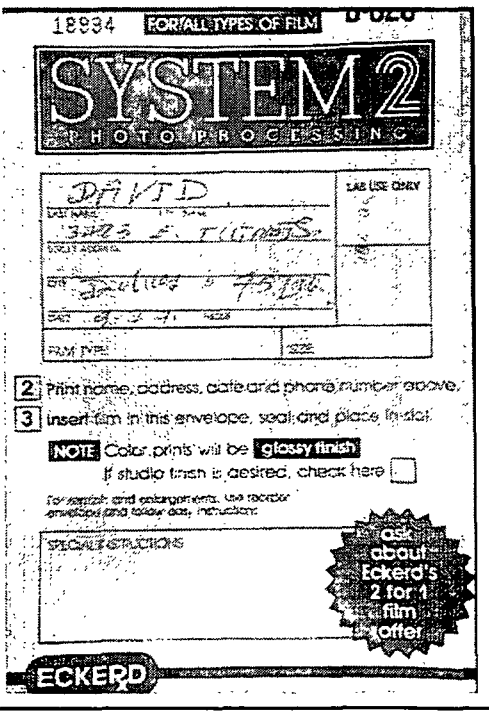
SELECTED REFERENCES

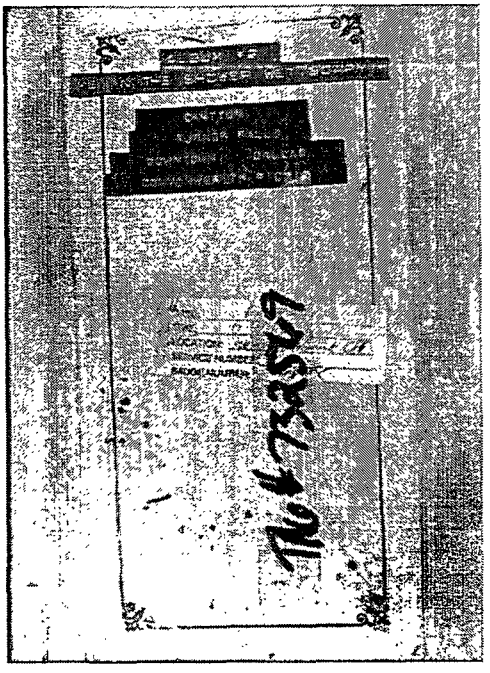
Adam, Barry, "Age, Structure, and Sexuality: Reflections on the Anthropological Evidence on Homosexual Relations," *Journal of Homosexuality*, Vol. 11, No. 3/4, pp. 19-34, Summer 1985 (Also published as *The Many Faces of Homosexuality: Anthropological Approaches to Homosexual Behavior*. New York: Harrington Park Press, 1986.)

PCO-CCAC-Walsh-106

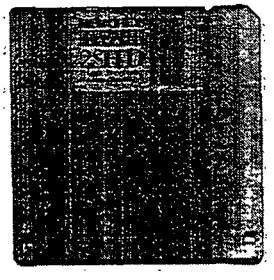
Uses of Computers in the Sexual Abuse and Exploitation of Children

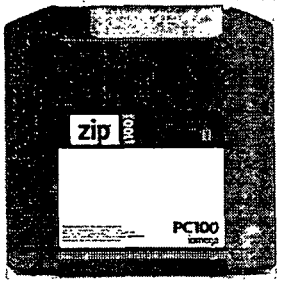
- Storage devices
  - child pornography
  - child erotica
  - diaries, letters
  - information on potential and actual victims

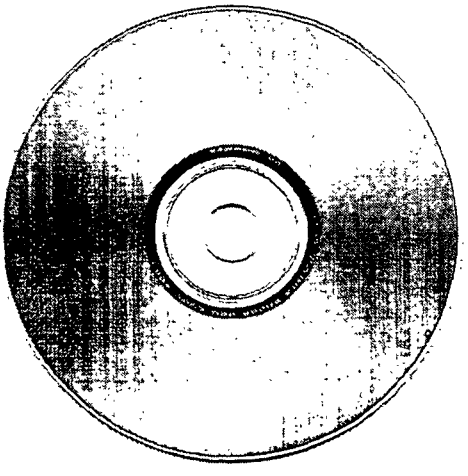




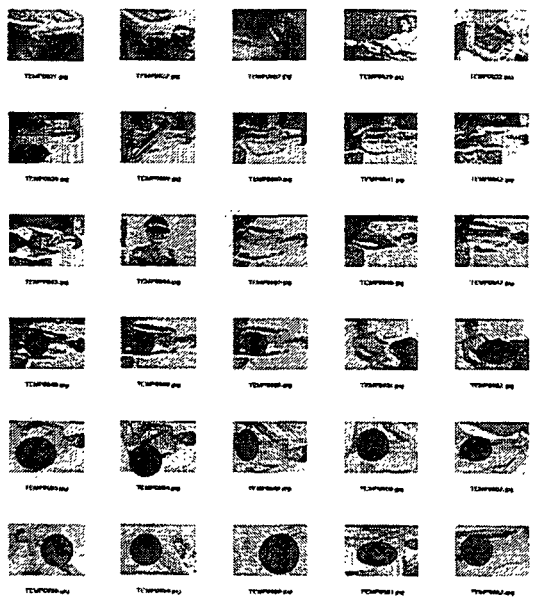
PCO-CCAC-Walsh-109







PCO-CCAC-Walsh-110

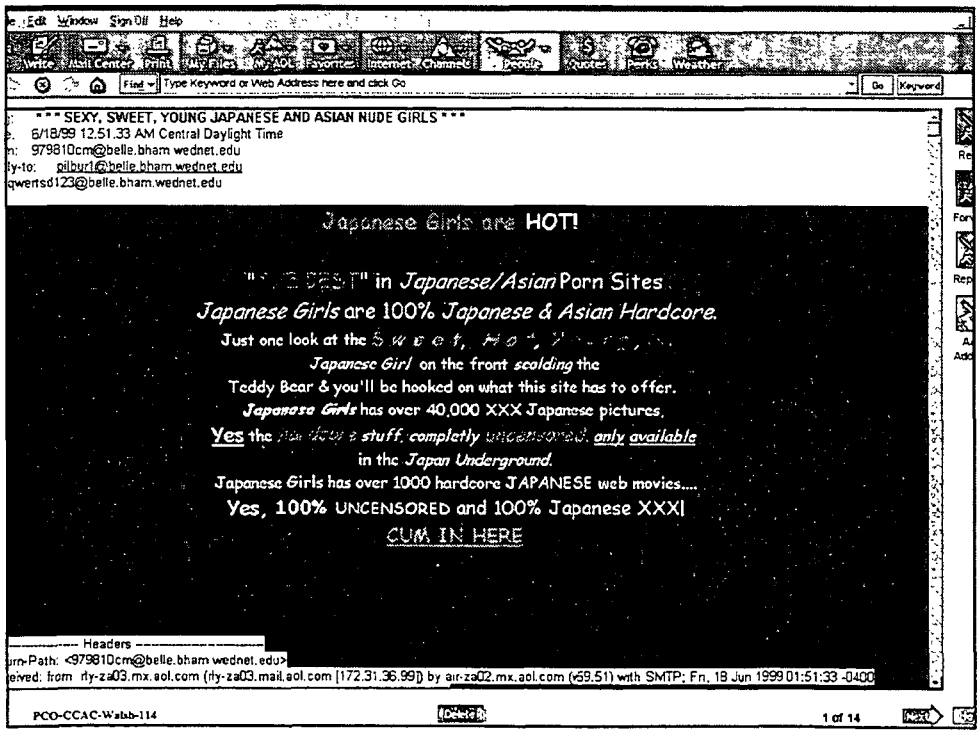


Computer Storage Capacity

- 1 kilobyte = 1 thousand characters
  - 1 page of double-spaced text
- 1 megabyte = 1 million characters
  - 1 average sized novel
- 1 gigabyte = 1 billion characters
  - 1,000 novels

Uses of Computers in the Sexual Abuse and Exploitation of Children

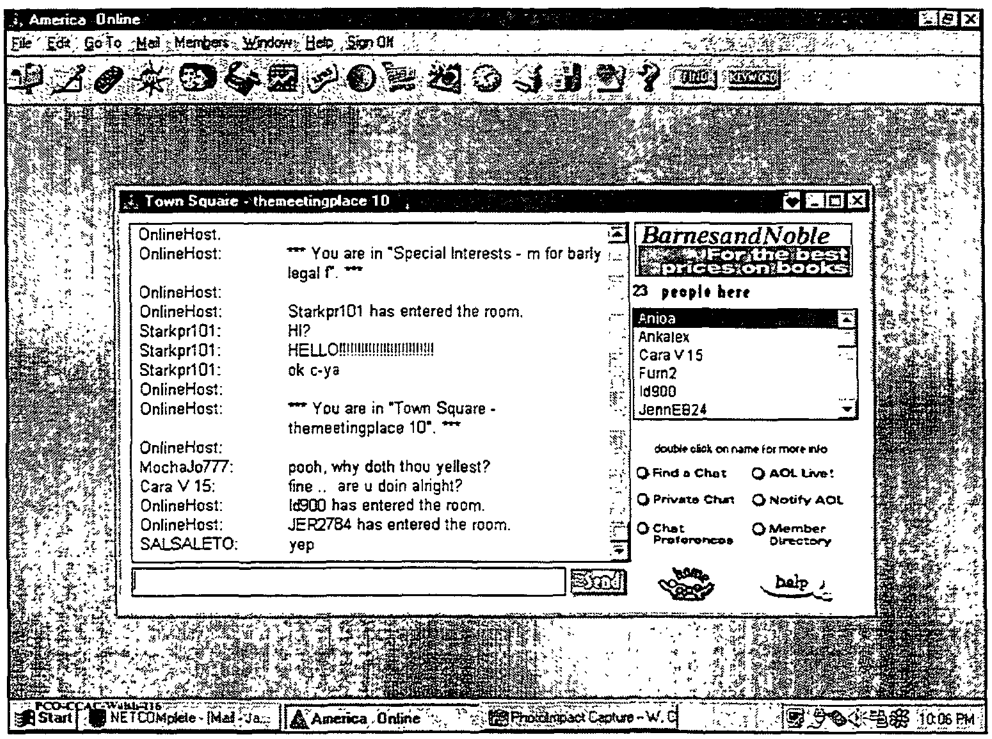
- **Medium for real time communication with children and other offenders using:**
  - **E-Mail**



Uses of Computers in the Sexual Abuse and Exploitation of Children

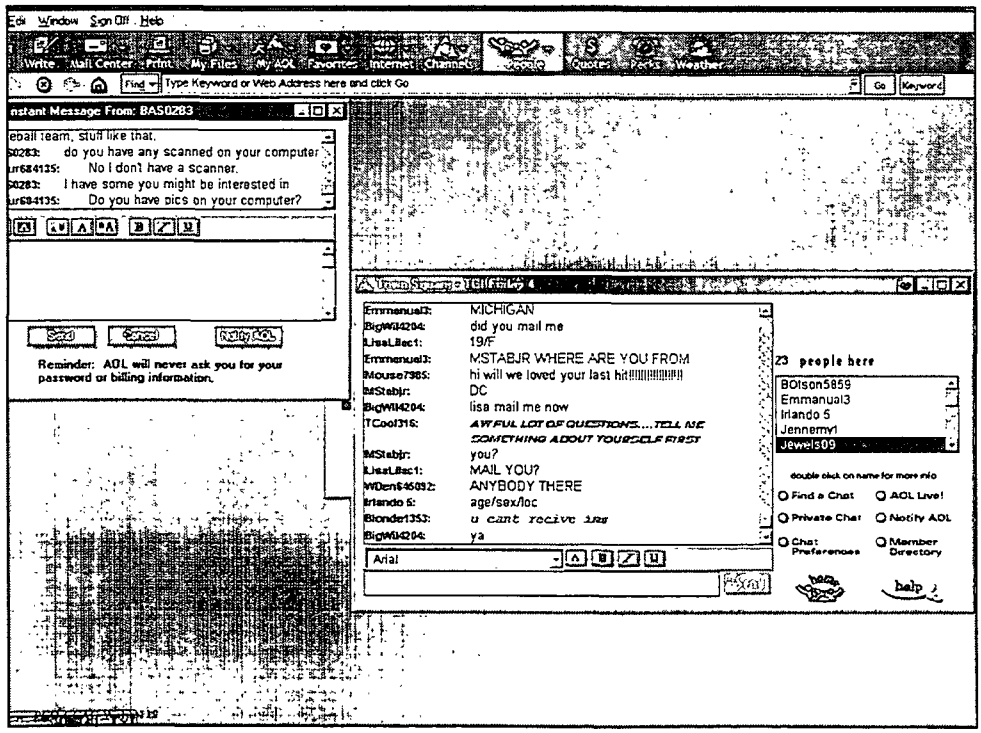
- Medium for real time communication with children and other offenders using:
  - E-Mail
  - Chat Rooms

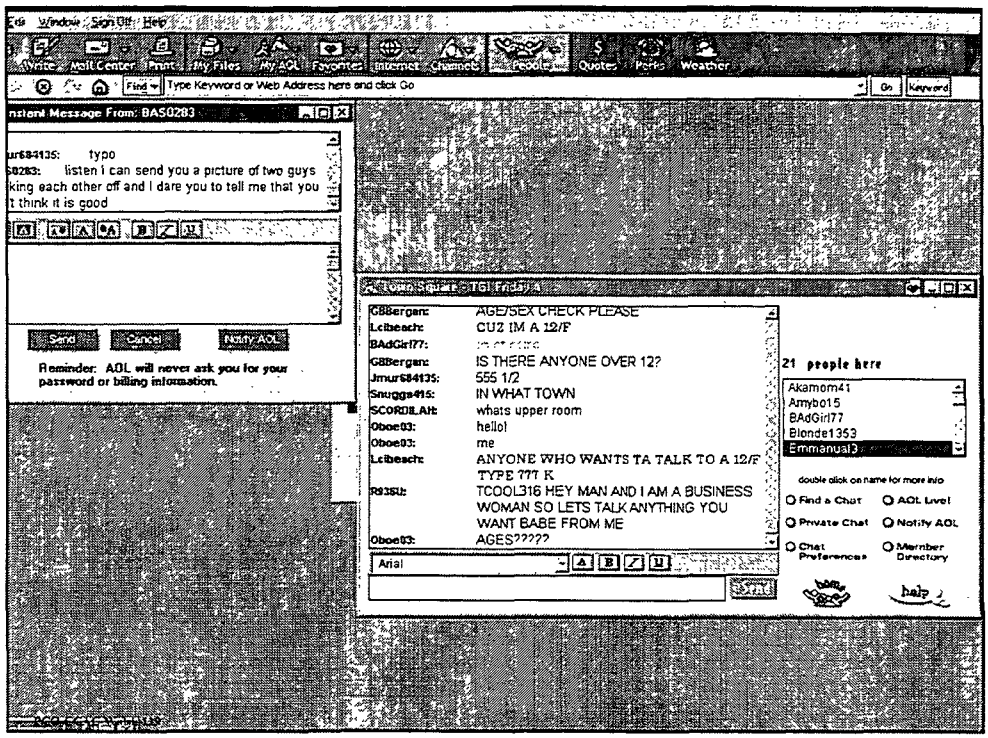
PCO-CCAC-Walsh-115

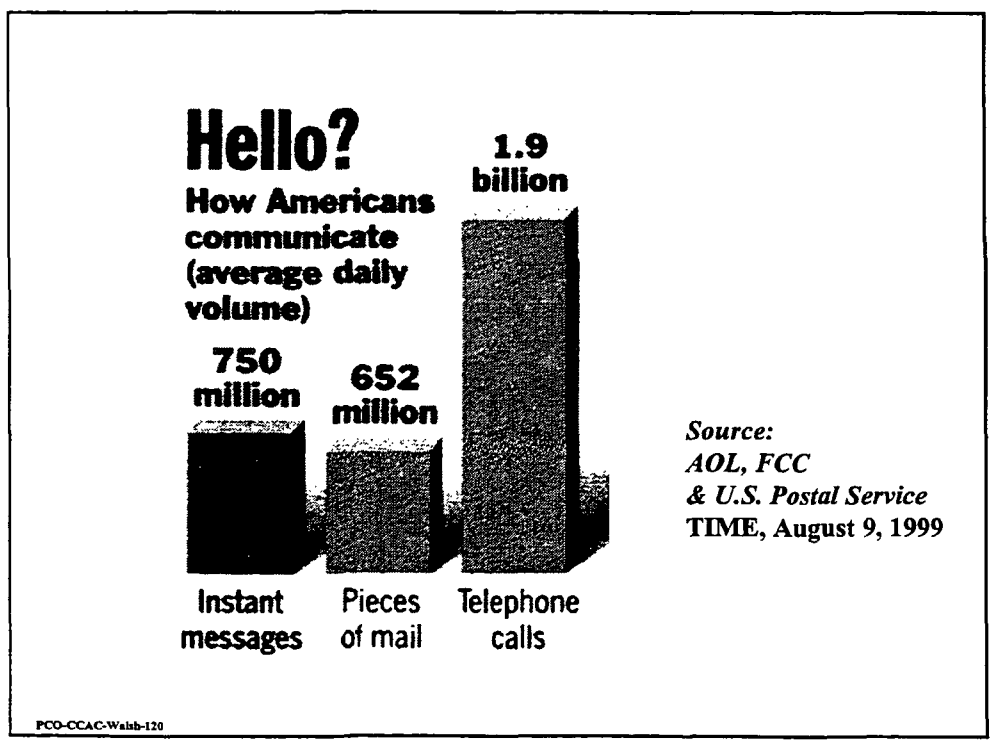


Uses of Computers in the Sexual Abuse and Exploitation of Children

- **Medium for real time communication with children and other offenders using:**
  - **E-Mail**
  - **Chat Rooms**
  - **Instant Messages (IM)**

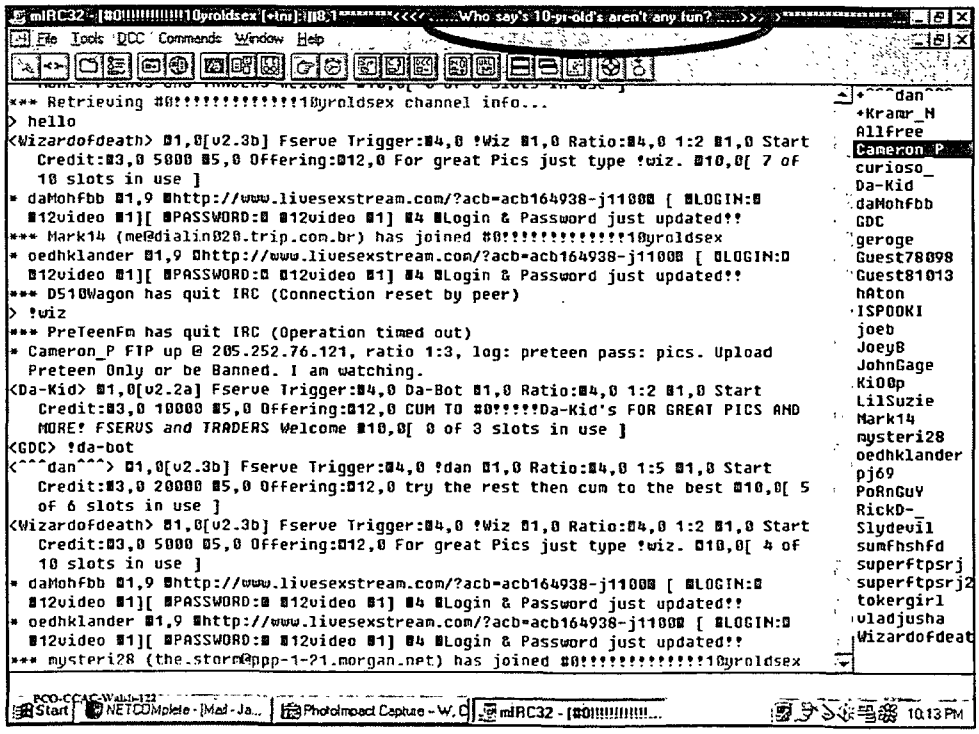



Write
Mail Center
Print
My Files
My AOL
Favorites
Internet
Channels
People
Quotes
Perks
Weather
Type Keyword or Web Address here and click Go
Go
Keyword
Send
Cancel
Notify AOL
Reminder: AOL will never ask you for your password or billing information.
GBbergan: AGE/SEX CHECK PLEASE
Lcibeach: CU2 IM A 12/F
GBbergan: IS THERE ANYONE OVER 12?
Jmur684135: 555 1/2
Snuggs415: IN WHAT TOWN
Oboe03: hello!
Oboe03: me
Lcibeach: ANYONE WHO WANTS TA TALK TO A 12/F TYPE ??? K
TCOOL316 HEY MAN AND I AM A BUSINESS WOMAN SO LETS TALK ANYTHING YOU WANT BABE FROM ME
Oboe03: AGES?????
21 people here
Akamom41
Amybo15
BAdGirl77
Blonde1353
Emmanual3
double click on name for more info
Find a Chat
AOL Live!
Private Chat
Notify AOL
Chat Preferences
Member Directory
Arial
help


Hello?
How Americans communicate (average daily volume)
750 million
652 million
1.9 billion
Instant messages
Pieces of mail
Telephone calls
Source:
AOL, FCC
& U.S. Postal Service
TIME, August 9, 1999
PCO-CCAC-Walsh-120

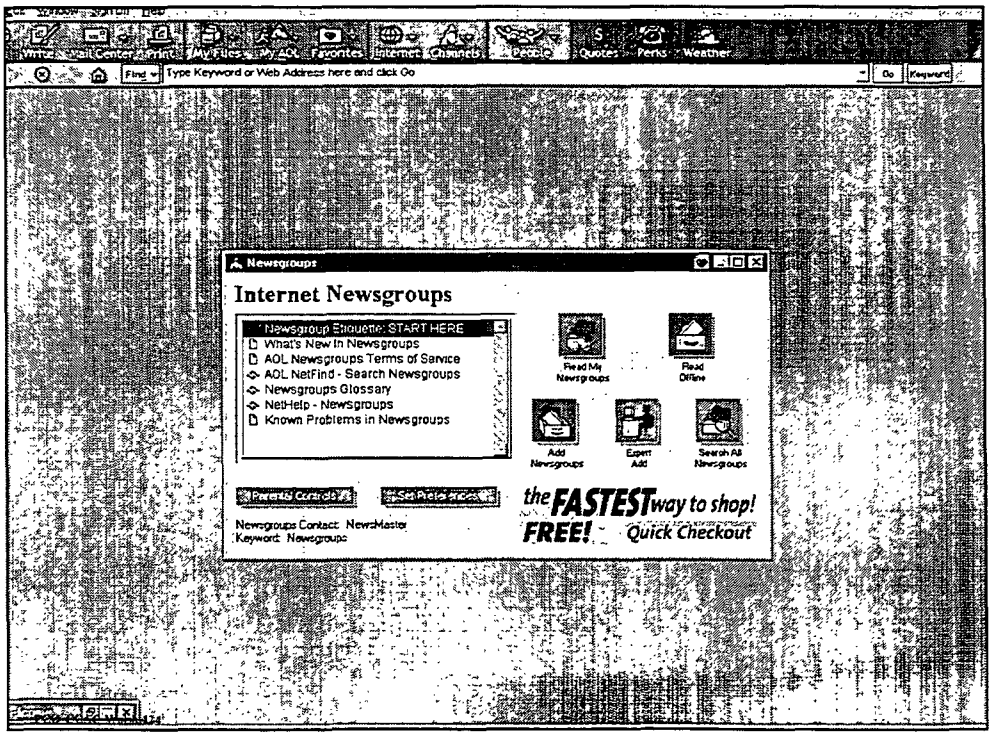
Uses of Computers in the Sexual Abuse and Exploitation of Children

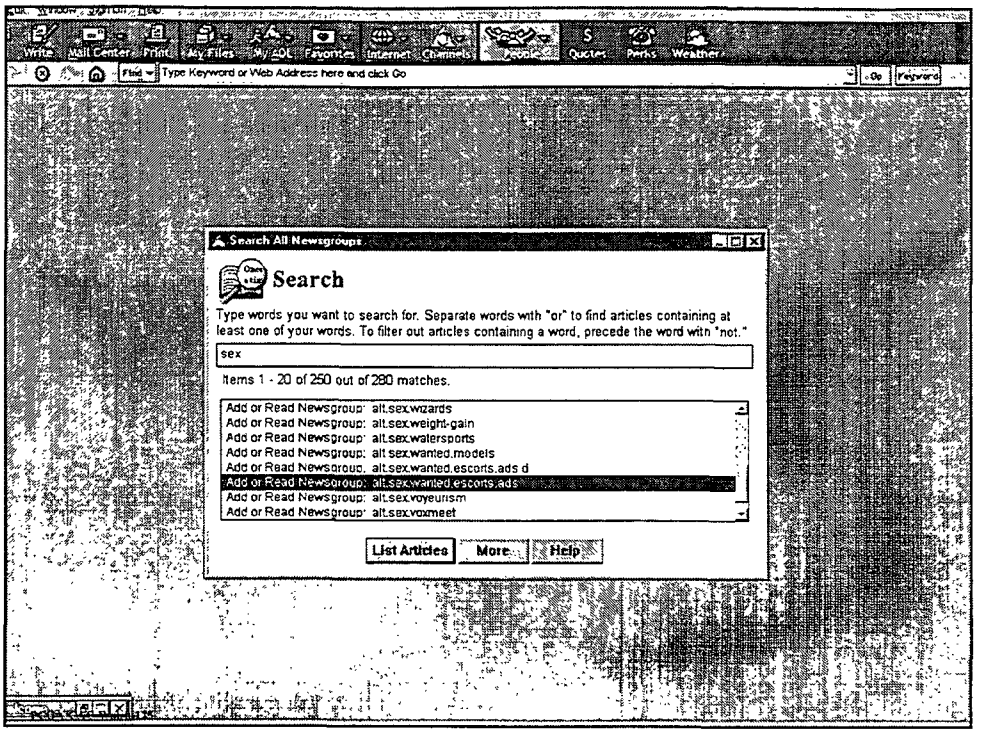
- **Medium for real time communication with children and other offenders using:**
  - **E-Mail**
  - **Chat Rooms**
  - **Instant Messages (IM)**
  - **Internet Relay Channel (IRC)**

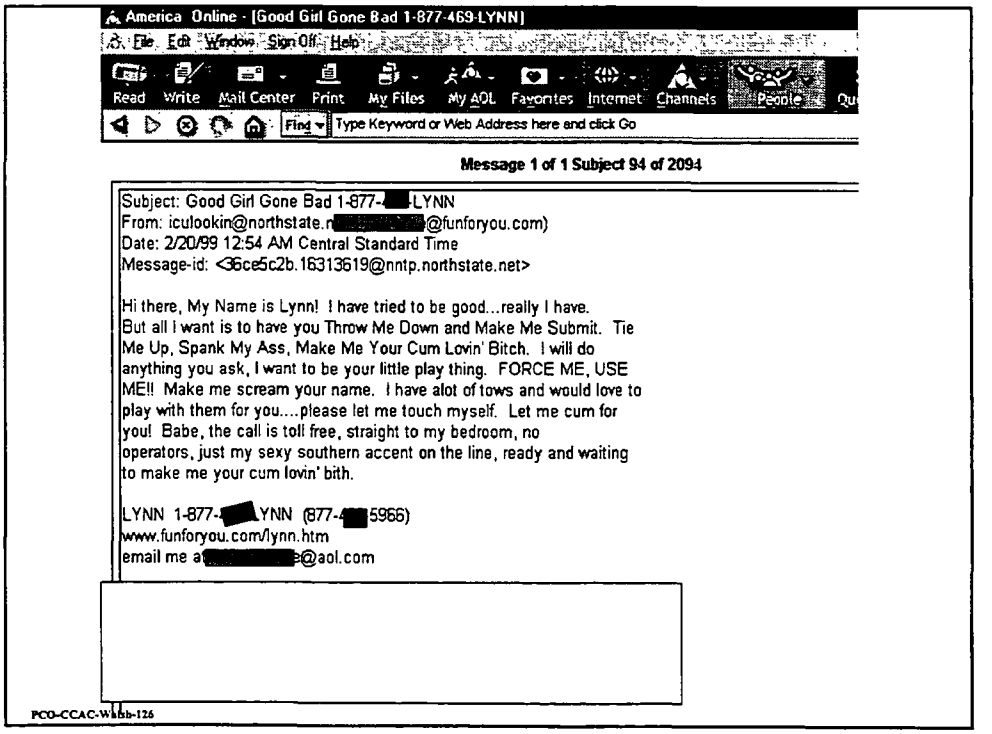


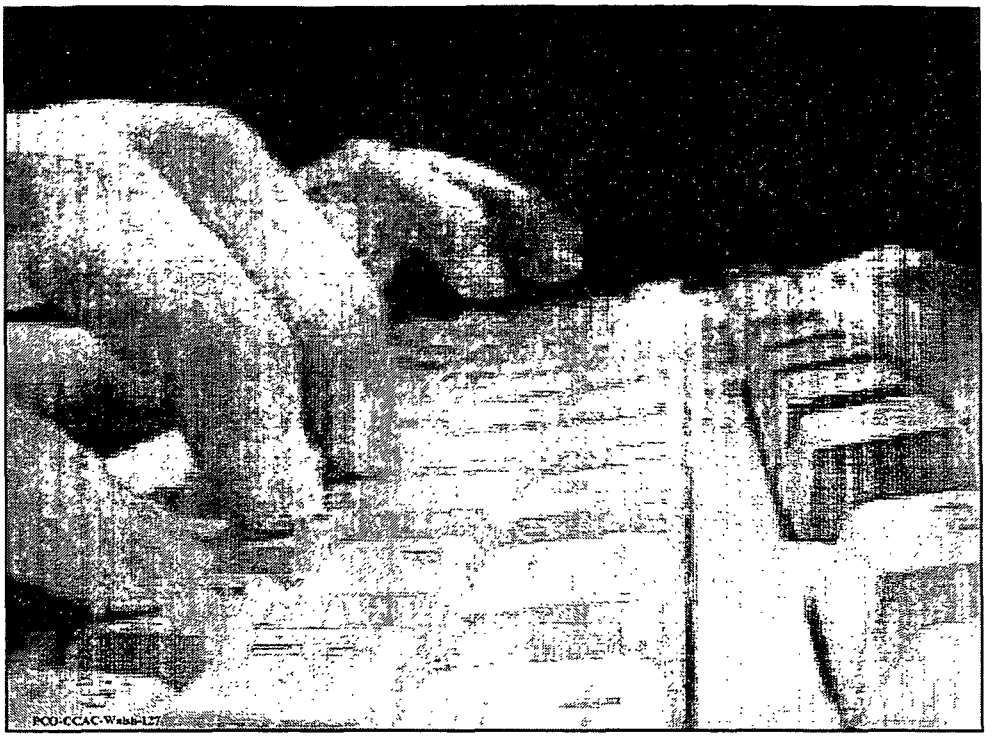
Uses of Computers in the Sexual Abuse and Exploitation of Children

- **Medium for real time communication with children and other offenders using:**
  - **E-Mail**
  - **Chat Rooms**
  - **Instant Messages (IM)**
  - **Internet Relay Channel (IRC)**
  - **Newsgroups**




Write
Mail Center
Print
My Files
My AOL
Favorites
Internet
Channels
People
Quotes
Perks
Weather
Find
Type Keyword or Web Address here and click Go
Go
Keyword
Search All Newsgroups
Search
Type words you want to search for. Separate words with "or" to find articles containing at least one of your words. To filter out articles containing a word, precede the word with "not."
sex
Items 1 - 20 of 250 out of 280 matches.
Add or Read Newsgroup: alt.sex.wizards
Add or Read Newsgroup: alt.sex.weight-gain
Add or Read Newsgroup: alt.sex.watersports
Add or Read Newsgroup: alt.sex.wanted.models
Add or Read Newsgroup: alt.sex.wanted.escorts.ads d
Add or Read Newsgroup: alt.sex.wanted.escorts.ads
Add or Read Newsgroup: alt.sex.voyeurism
Add or Read Newsgroup: alt.sex.voxmeet
List Articles
More...
Help


America Online - [Good Girl Gone Bad 1-877-469-LYNN]
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People
Find
Type Keyword or Web Address here and click Go
Message 1 of 1 Subject 94 of 2094
Subject: Good Girl Gone Bad 1-877-[redacted]-LYNN
From: iculookin@northstate.n[redacted]@funforyou.com)
Date: 2/20/99 12:54 AM Central Standard Time
Message-id: <36ce5c2b.16313619@nntp.northstate.net>
Hi there, My Name is Lynn! I have tried to be good...really I have. But all I want is to have you Throw Me Down and Make Me Submit. Tie Me Up, Spank My Ass, Make Me Your Cum Lovin' Bitch. I will do anything you ask, I want to be your little play thing. FORCE ME, USE ME!! Make me scream your name. I have alot of tows and would love to play with them for you....please let me touch myself. Let me cum for you! Babe, the call is toll free, straight to my bedroom, no operators, just my sexy southern accent on the line, ready and waiting to make me your cum lovin' bith.
LYNN 1-877-[redacted]YNN (877-[redacted]5966)
www.funforyou.com/lynn.htm
email me a[redacted]@aol.com



Uses of Computers in the Sexual Abuse and Exploitation of Children

- **On-line solicitation of children for meetings and subsequent sexual activity**
  - ***(Traveler Cases)***

PCO-CCAC-Webb-128

◆ *Suspect:*	*A nude dancer needed for discrete pleasure, I am generous and rich, you must be very attractive and young.*
◆ **UC:**	**Saw your ad, very interesting, how young are you looking for?**
◆ *Suspect:*	*Age doesn't matter.*
◆ **UC:**	**If you don't care about age, I am 13, looking for independence.**
◆ *Suspect:*	*I'm looking for a girl who dares to be nude and will watch me masturbate.*

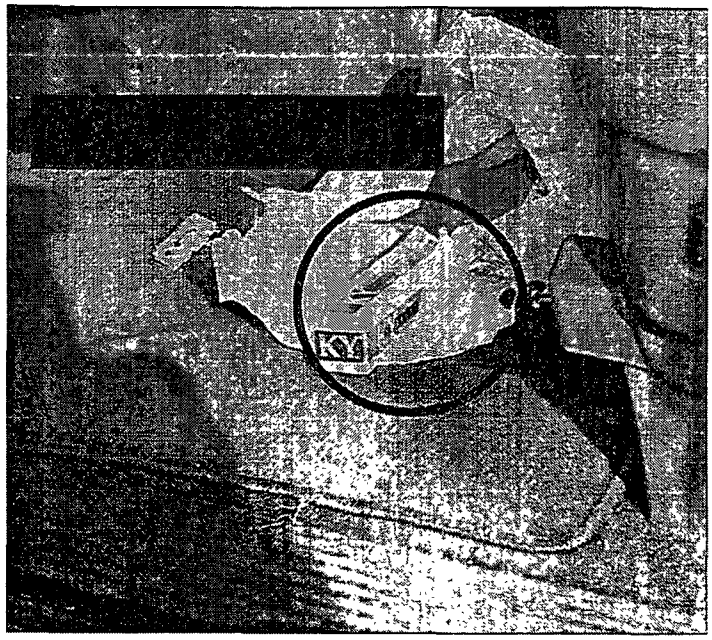
PCO-CCAC-Walsh-129

◆ **UC:**	**I've never watched a man masturbate, I have to be careful my parents don't find out. Were you wanting to do anything else?**
◆ *Suspect:*	*I just want to watch you undress and masturbate myself.....you will be surprised how big my dick is. Pick a place you want to meet.*
◆ **UC:**	**There's a park real close to my house called Cotillion Park, my girlfriend said it hurts when you have sex.**
◆ *Suspect:*	*I'll meet you at the park and I will bring some lubrication for sex.*

PCO-CCAC-Walsh-130

PCO-CCAC-Walsh-131

PCO-CCAC-Walsh-132

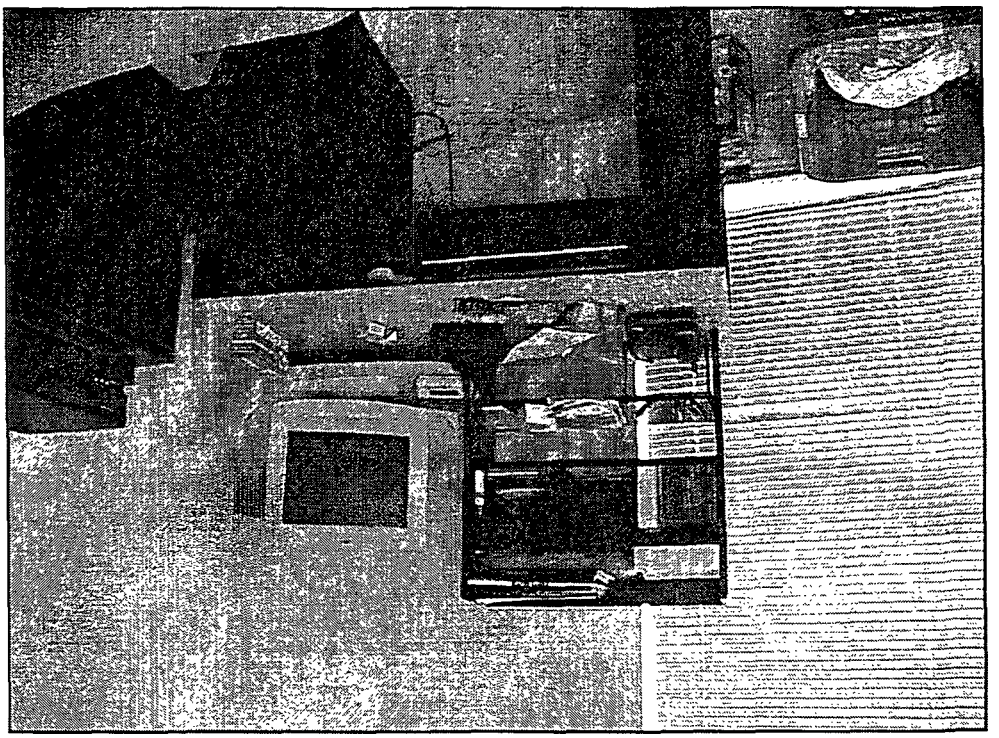


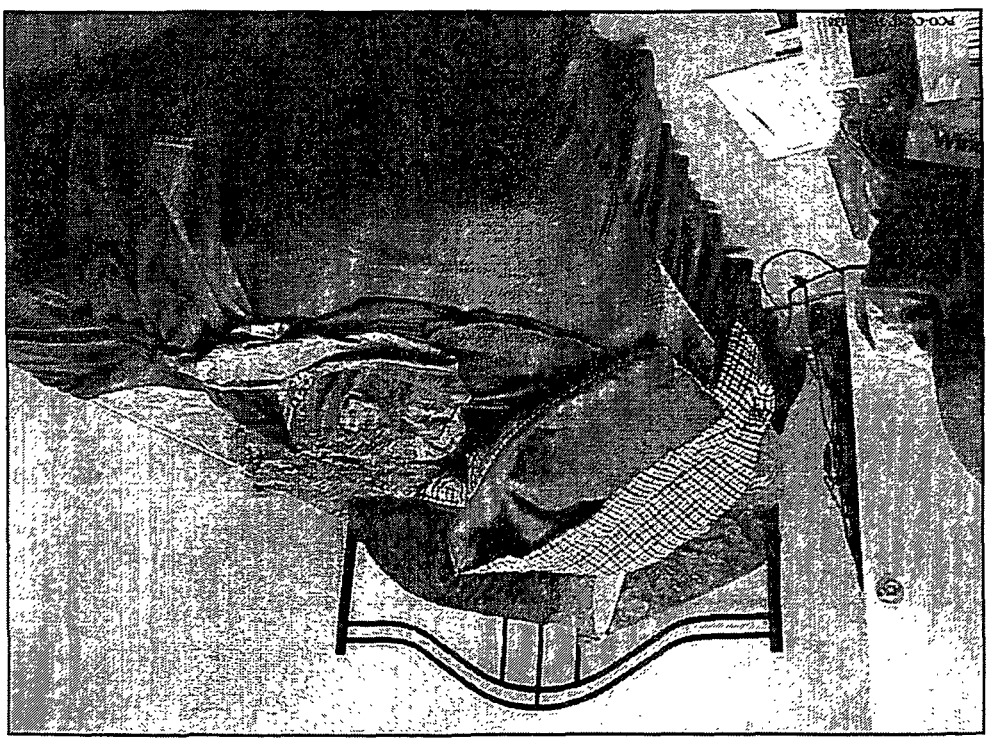
PCO-CCAC-Walsh-133

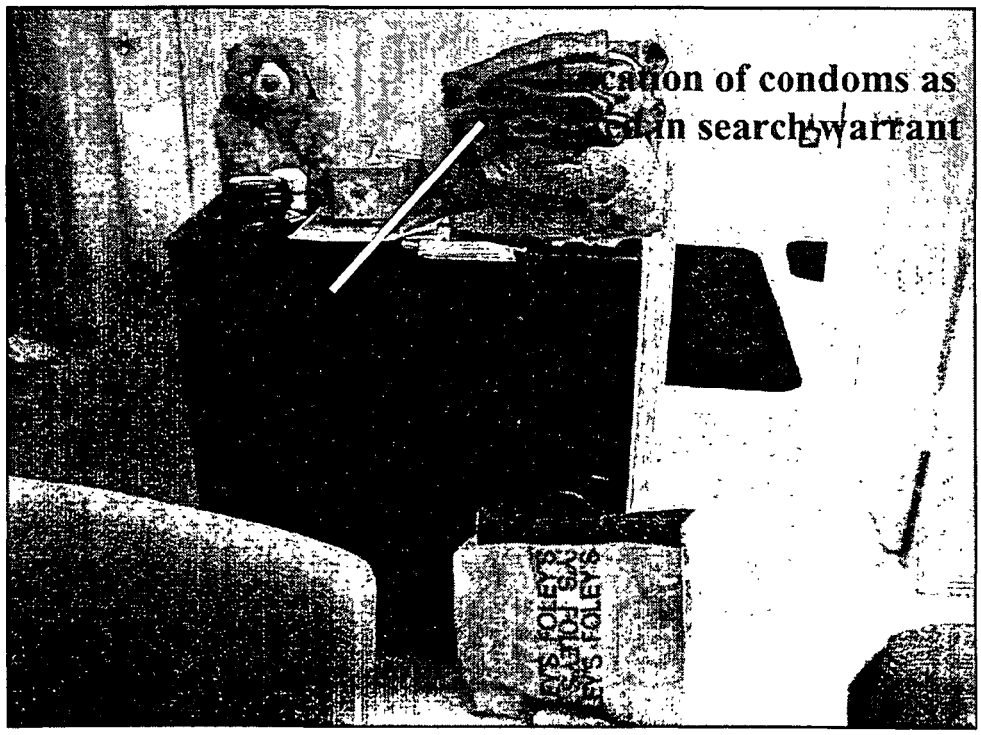
Man gets probation in Internet sex assault case

■ A 29-year-old man was sentenced Friday to seven years' deferred-adjudication probation after pleading no contest to sexually assaulting a 15-year-old girl he met through an America Online chat room. Jeffrey Glen Garner of Irving faces up to 20 years in prison if he violates terms of his probation. If he successfully completes it, his record would not reflect the conviction.

PCO-CCAC-Walsh-134

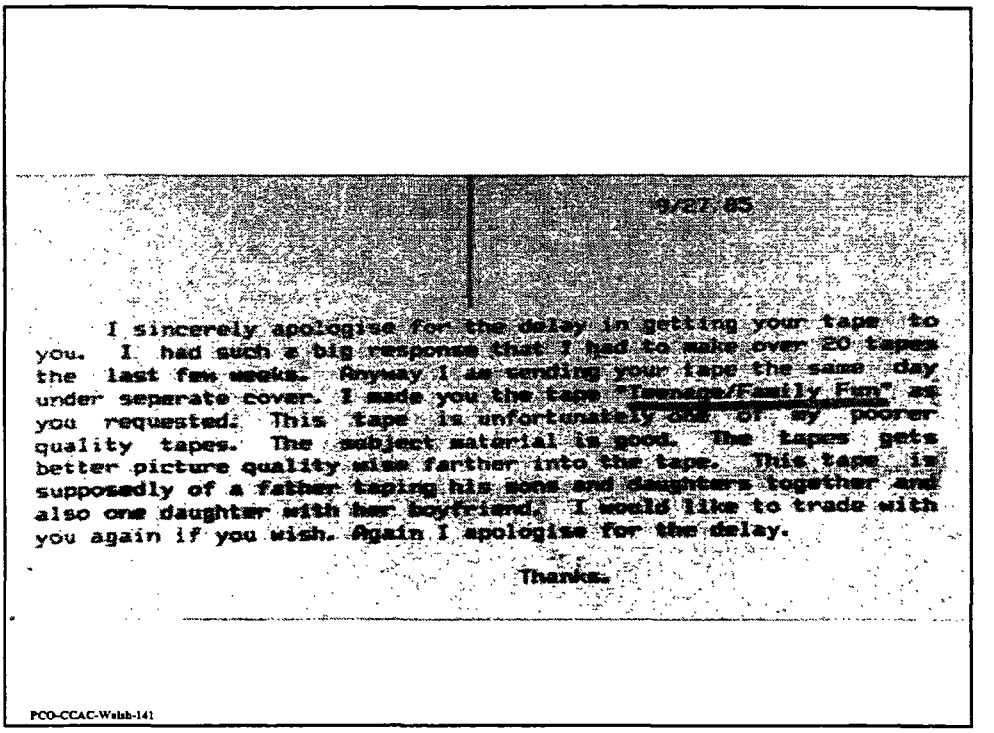





cation of condoms as
in search warrant

Uses of Computers in the Sexual Abuse and Exploitation of Children

- Opportunity to contact others with a sexual interest in children for discussion, trading of material or actual meetings

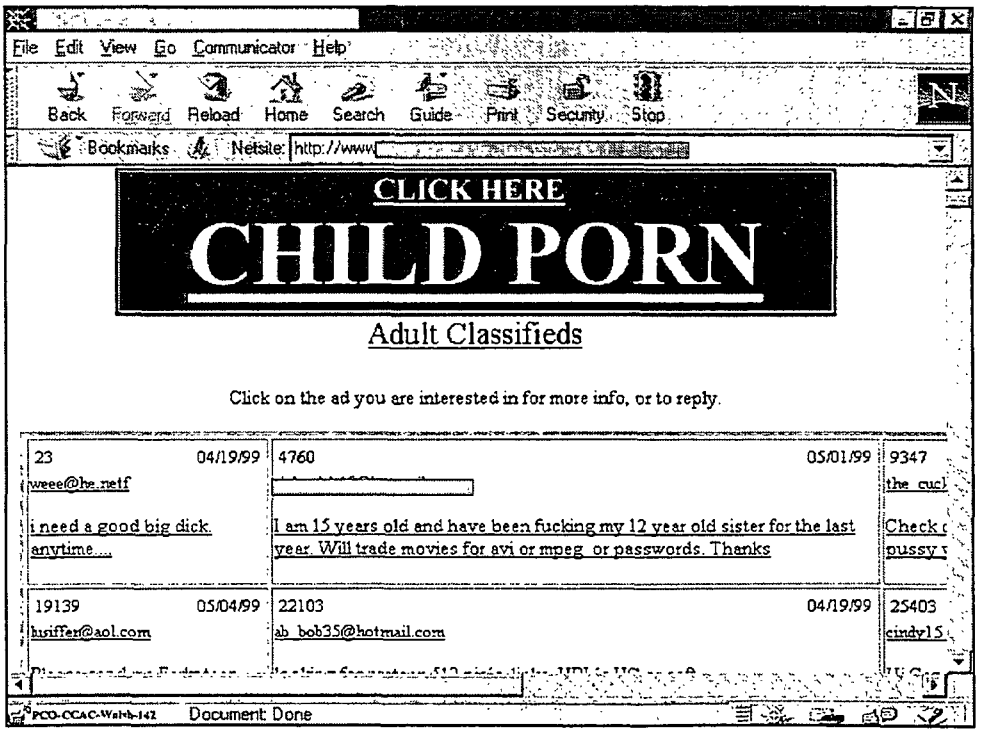


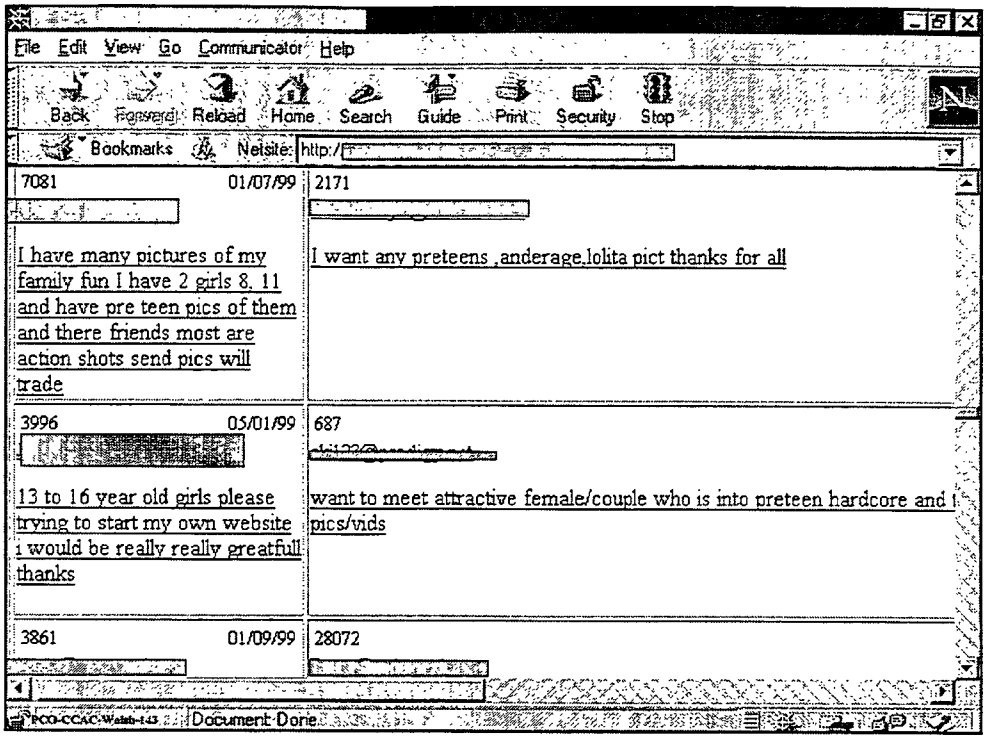
9/27/65

I sincerely apologise for the delay in getting your tape to you. I had such a big response that I had to make over 20 tapes the last few weeks. Anyway I am sending your tape the same day under seperate cover. I made you the tape "Teenage/Family Fun" as you requested. This tape is unfortunately one of my poorer quality tapes. The subject material is good. The tapes gets better picture quality mine farther into the tape. This tape is supposedly of a father taping his sons and daughters together and also one daughter with her boyfriend. I would like to trade with you again if you wish. Again I apologise for the delay.

Thanks.

PCO-CCAC-Walsh-141





7081 01/07/99

[redacted]

I have many pictures of my family fun I have 2 girls 8, 11 and have pre teen pics of them and there friends most are action shots send pics will trade

AOL CHAT ROOM

Suspect: *Are you offended by young?*

UC: Not at all, how young are you talking about

Suspect: *8, 9 through early teens? You?*

UC: I prefer 8 and 10.

Suspect: *What's the youngest you've had?*

UC: I have a 6 year old niece.

PCO-CCAC-Walsh-145

Flower Mound doctor arrested on child porn charge

■ **FLOWER MOUND** — An anesthesiologist at Denton Regional Medical Center has been arrested on charges of possession and promotion of child pornography, authorities said. The arrest late Tuesday of Dr. Booker T. Rogers, 42, of Flower Mound stemmed from an interstate investigation of Internet distribution of child pornography. Officials said the investigation centered on pictures distributed to Internet "chat rooms." Officers said they seized computers and files, drug paraphernalia and 33 vials of suspected illicit drugs at Dr. Rogers' home. Dr. Rogers, reached after being freed Wednesday on $20,000 bond, said he might comment on the charges later. Hospital officials said Dr. Rogers joined the staff in 1989 and resigned Wednesday, pending the outcome of the investigation.

PCO-CCAC-Walsh-146

Uses of Computers in the Sexual Abuse and Exploitation of Children

- **Opportunity to distribute pornographic material to children to lower their inhibitions**

NATIONAL

Man accused of using Internet in bid to arrange rape of woman

By Greg Miller
and Davan Maharaj
Los Angeles Times

LOS ANGELES — In the first prosecution under a new California cyberstalking statute, a man has been charged with using the Internet in an attempt to arrange the rape of a woman who had spurned his romantic advances.

The case centers on the chilling account of a North Hollywood woman. According to testimony, six different men showed up at her apartment over a five-month period last year, saying they were responding to online ads and steamy e-mails sent in her name that described fantasies of being raped.

Authorities said Thursday that these were not her ads, her e-mails or her fantasies, and that she was the victim of Gary S. Dellapenta, a 50-year-old security guard from North Hollywood who was ordered to stand trial on charges of stalking, computer fraud and solicitation of sexual assault.

Mr. Dellapenta has pleaded not guilty to the charges. His attorney, deputy public defender Irene Nunez, declined to comment Thursday.

Experts say the case is a sinister example of the ways that new technology can be put to criminal purposes.

"This technology has created a whole new class of criminals who would not otherwise have the forbearance to terrorize people face to face," said Assistant U.S. Attorney Michael J. Gennaco, who two years ago prosecuted the first federal hate crime in cyberspace. "It emboldens them to hide behind computer screens and interfere with other people's lives."

Law enforcement officials testified in Los Angeles Municipal Court last week that Mr. Dellapenta admitted to the crimes and said he was driven by an "inner rage" against the woman, whose identity is being protected by authorities.

Scott Gordon, the deputy district attorney prosecuting the case, said the woman was not physically harmed and that Mr. Dellapenta, who is being held in jail with bail set at $300,000, faces as much as seven years in prison.

Mr. Dellapenta, who worked as a security guard at the Los Angeles building that houses the West Coast offices of the Motion Picture Association of America, is accused of sending e-mail to men who responded to personal ads placed in the woman's name on America Online, the Microsoft-owned e-mail service Hotmail and other Internet sites.

The e-mails said the woman was "into rape fantasy and gang-bang fantasy," authorities said, and told numerous men everything from the address of her apartment to her physical description, her phone number and how to bypass her home security system.

Mr. Dellapenta's arrest in November culminated an investigation that included the cooperation of the FBI, the district attorney's office and even the victim's father, who responded to the ads himself in an attempt to learn the poster's identity.

Law enforcement officials have predicted an outbreak of stalking crimes aided by the Internet, mainly because of its anonymity as well as the proliferation of directories and services online that often enable users to get detailed information about where people live, their phone numbers, their credit histories and even the online message boards they frequent.

The possibility of such crimes prompted California to overhaul the state's stalking statute last year. State Sen. Tim Leslie of Tahoe City wrote a bill that expanded stalking and harassment laws to include threats sent via pagers, e-mail, faxes, voice mail and other electronic communications.

Most online companies set strict rules about what kind of information can be contained in an ad, and they post guidelines urging users to be cautious about revealing personal information. But even the most careful companies allow users to set up multiple online identities and are limited in their ability to safeguard users.

"There is a level of anonymity on the Net, and unless you know who you're dealing with it's risky," said John Ryan, assistant general counsel at AOL.

The victim in the North Hollywood case, authorities said, could not be accused of making any online blunders, however. She didn't even have a home computer.

Mr. Dellapenta had met the woman in church, according to the testimony of Brian Hale, an investigator with the district attorney's office.

Woman accused of trying to sell child via Internet

Couple in Burleson alerted Colorado sheriff after e-mails

By Mark Wrolstad
Staff Writer of The Dallas Morning News

Child-selling charges were filed Tuesday against a Colorado woman who investigators said offered her newly adopted 8-year-old daughter to a Burleson couple via the Internet.

Officials said it could be the first prosecution for such a crime committed by computer.

The Burleson couple, whose names haven't been released, called the Arapahoe County sheriff's office in Littleton, Colo., on Friday after exchanging e-mails with Denise K. Thomas about payment.

The girl, named Elena, was adopted four months ago from Russia and has an emotional-attachment disorder, according to her adoptive parents. The girl's 10-year-old sister also was adopt-

PCO-CCAC-Walsh-149

Child-selling charges filed against woman

Continued from Page 25A

ed and lives in Mississippi, authorities said.

Mrs. Thomas, 42, and her husband, Peter, 50, have said she wasn't trying to sell the child but was seeking reimbursement for some adoption expenses, which exceeded $13,000.

Investigators said the woman wanted $4,000 for the girl, plus air fare to get her to Texas, under the pretense of a private adoption.

"You can't sell a child, and that's exactly what she was trying to do," Undersheriff Grayson Robinson said. "She was trying to avoid the bureaucracy and the inconvenience of the adoption process."

During their electronic conversation, the Burleson couple told Mrs. Thomas that what she was doing was a felony in Texas, Undersheriff Robinson said. She allegedly responded, "This is the way to avoid the attorney's fees ... You must really be naive."

Undersheriff Robinson said he didn't know exactly how or when the couple found Mrs. Thomas on the Internet, or if they want a child.

Mrs. Thomas was arrested and booked Friday, then released. She was charged Tuesday with "criminal attempt trafficking in children," a Class 4 felony in Colorado carrying a prison term of up to eight years.

Investigators confiscated her home computer and are looking at other

Burleson police are contacting Colorado authorities about the case but may have nothing to pursue, Capt. Doug Sandifer said Tuesday.

"On the face of it, the offense looks like it occurred in Colorado," he said, adding that the vastness of the Internet has opened the way for criminal offenses.

Mrs. Thomas said Monday that she only wanted to find the right home for the troubled girl.

"I had no intention of selling a child or anything like that," she said. "We realized that it just wasn't going to work out here for her. It was a mistake, a tragic mistake."

Mr. Thomas, who hasn't been charged, defended his wife, saying the girl's emotional detachment nearly destroyed the family after their 18-month ordeal to gain a daughter. Their 14-year-old biological son remains in their home.

"We have tried and tried and tried to love this girl," Mr. Thomas said.

"If she mentioned money she was thinking about reimbursement of expenses."

It's illegal in most states, including Texas, for an adoptive parent to pay for anything more than medical, legal and some pregnancy-related expenses, said Heidi Cox, general counsel for Fort Worth's Gladney Center, one of the nation's oldest and largest adoption agencies.

Ms. Cox said this doesn't sound like a child-selling case, which typically involves "nothing less than $10,000."

"I think she was desperate. The whole thing is unfortunate," Ms. Cox said. "She made a very poor decision, no doubt."

Marshall Williams, Gladney's head of international adoptions, called baby-selling allegations "the worst thing that can happen." Word of the Colorado case is certain to reach Russia and could temporarily slow or halt adoptions there, he said.

Undersheriff Robinson said $4,000 might seem insignificant compared to the Thomases' overall expenses.

"But this isn't a business, it's a child," he said. "The bottom line is she was going to gain some benefit from removing the child and that's in the statute."

The Associated Press contributed to this report.

PCO-CCAC-Walsh-150

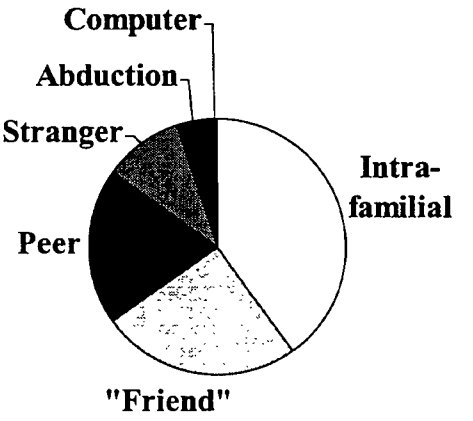
Burleson police are contacting Colorado authorities about the case but may have nothing to pursue, Capt. Doug Sandifer said Tuesday.

"On the face of it, the offense looks like it occurred in Colorado," he said, adding that the vastness of the Internet has opened the way for criminal offenses.

Effect on Society

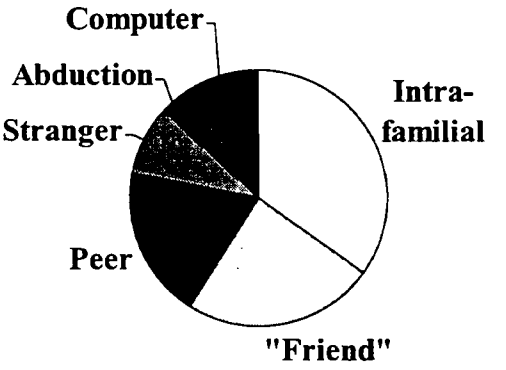
- Need for New Legislation
- Increase in Computer Related Litigation
- Increased Funding for Criminal Justice Agencies
  - Law Enforcement
  - Prosecution
  - Probation and Parole
- Need for On-Line and Internet Oversight by Law Enforcement

Crimes Against Children 1999



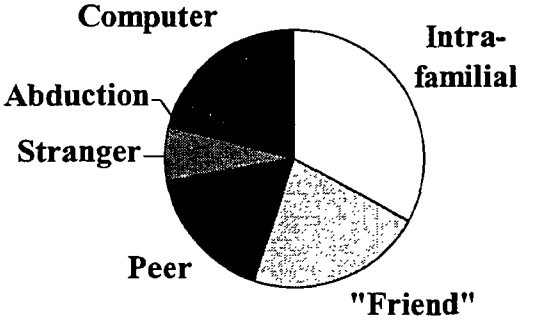
PCO-CCAC-Walsh-153

Crimes Against Children in 2000 ?



PCO-CCAC-Walsh-154

Crimes Against Children in 2005 ?



Challenges to Law Enforcement

- To learn and stay current with the latest developments in computer technology
- To learn and stay current with the latest developments with relevant state and federal laws
- To overcome the arguments against the need to investigate these cases

Challenges to Law Enforcement

- To obtain the necessary resources (equipment, personnel and training)
- To select the right investigative personnel for these cases
- To overcome agency pride and learn to work cooperatively

1998 Justice Appropriations Act

- $10 M to FBI to enhance "Innocent Images"
  - 40 new positions
  - Creation of a second "Innocent Images" Squad
- $2.4 M to Office of Justice Programs & NCMEC
  - 10 Internet Crimes against Children Task Forces

City to get U.S. aid to boost Internet child-porn battle

By Tomas J. Lewis DMN 9-16-98
Staff Writer of The Dallas Morning News

Dallas will receive a $300,000 grant from the U.S. Department of Justice to expand a program to combat sexual exploitation of children on the Internet, police officials announced Tuesday.

The one-year grant will pay for a full-time detective, a full-time prosecutor and a part-time Sheriff's Department investigator. The money also will be used to buy computer equipment and pay for prevention and training programs, police Lt. Bill Walsh said.

"We've already been working in this area, but this grant will give us a considerable shot in the arm to get the job done," he said. "This is going to help us investigate and prosecute people who use computers to sexually abuse children."

Lt. Walsh said the grant will help authorities apprehend sex offenders who use computers to traffic in child pornography and solicit children online for sexual encounters. He said solicitations are a growing problem worsened by the increasing number of children who use the Internet.

"We believe there are as many as 10 million children using the Internet right now," Lt. Walsh said, "and that figure is expected to triple in the next four years."

Lt. Walsh said the funds — from the Justice Department's Missing and Exploited Children's Program — will supplement the existing Dallas Police Department-FBI Crimes Against Children Task Force.

Cheryl Sutterfield, executive director of the Dallas Children's Advocacy Center, called the grant "great news."

She said the center, which helps local law enforcement agencies investigate child abuse and provides therapy for victims, has not dealt with any cases of children victimized through the Internet. Nonetheless, she said, the problem is real and must be addressed.

"It's alarming to me to see the number of children who come through our center who have been abused and then come across this huge monster of pornography on the Internet," she said.

Lt. Walsh said the task force will catch and prosecute anyone exploiting children via the Internet.

"We want the offenders to know that we're here," he said, "and they'd better watch out."

Staff writer Tony Hartzel contributed to this report.

PCO-CCAC-Walsh-159

Internet Crimes Against Children Task Forces

- Bedford County SO, Virginia
- Broward County SO, Florida
- Colorado Springs PD, Colorado
- Dallas PD, Texas
- Illinois State Police

PCO-CCAC-Walsh-160

Internet Crimes Against Children Task Forces

- New York State Division of Criminal Justice Services
- Portsmouth PD, New Hampshire
- Sacramento SO, California
- S. Carolina Office of the Attorney General
- Wisconsin Dept. of Justice

Challenges to Law Enforcement

- To conduct competent and thorough criminal investigations
- To conduct competent forensic examinations of computer equipment
- To deal with jurisdiction issues
- To obtain and share information with other agencies

Challenges to Law Enforcement

- To protect children from sexual abuse and exploitation by offenders that use computers

LT. BILL WALSH

Youth & Family Crimes Division
Dallas Police Department
106 S. Harwood St. Rm. 225
Dallas, Texas 75201
214-670-5936
214-670-3957 Fax
800-381-4779 Pager
waldo4122@aol.com

SGT. BYRON FASSETT

Youth & Family Crimes Division
Dallas Police Department
106 S. Harwood St. Rm. 225
Dallas, Texas 75201
214-670-4978
214-670-3957 Fax

Orientation to Computer Technology

Protecting Children On-line

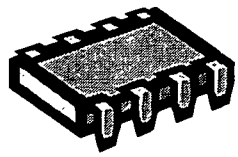
Orientation to Computer Technology
and Online Communications

Today's Topics

- Computers and crime
- How computers work
- Computer hardware and software
- Computer networks
- The Internet
- Hardware and software demonstrations

What is Driving the Rapid Pace of Change in Society?

Here is a Hint!



Hyperculture

America's Addiction to Speed

Information Technology is Driving Profound Change

- For society
- For corporations
- For law enforcement agencies
- For individuals

The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn

Alvin Toffler

Old Crimes

- New techniques and tools
- New types of evidence

Cybercops Face Net Crime Wave

Interactive Week Magazine, June 1996

In a bank robbery , we know to put up yellow tape around the scene, watch the video, and dust for prints. But on the Internet, you cannot seal off the area and get out of the way.

Scott Charney, U.S. Department of Justice

Futurists Predict

- Technology and policing tactics will eliminate much conventional crime
- Technology and computer crime will take the place of conventional criminal acts

---

"By the year 2000, there will be so much computer related crime, law enforcement will be reduced to taking reports because we will not know how to investigate it."

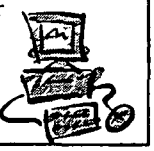
Dr. William Tafoya
1988 and 1997

Attorney General Janet Reno

- 10/26/96 IACP General Assembly
- Identified computer crime as one of her top three priorities
  - Computers used to commit crimes
  - Computers that were victims of crime
  - Computers used to store data of a criminal enterprise

Pornography

- Rule in cyberspace is anything goes
- Sex flourishes on the Internet
- Gigabytes of graphic material that is easily downloaded
- Virginia security firm says there is some form of pornography in one of four corporate computers



Sexual Predators

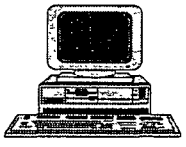
- Find victims on the Internet
- Pose as other children
- Find kids in chat rooms, newsgroups
- Transmit and exchange child pornography
- Send unsolicited pornography
- Market in kiddy porn
- Other techniques will be discussed

Our Aim

- To understand how computer technology is changing the nature of criminal investigations and evidence
- To understand computers and the on-line world and be conversant in technology matters
- To reinforce the importance of competent and thorough investigations

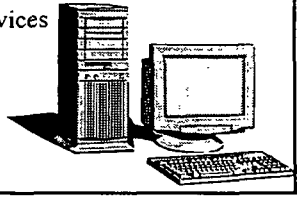
How Do Computer's Work?

- They manipulate and store bits and bytes of digital information
- 1's and 0's
- Requires a combination of hardware and software to work



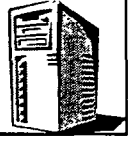
Hardware

- Processing devices
- Input / output devices
- Storage devices and media
- Communications devices



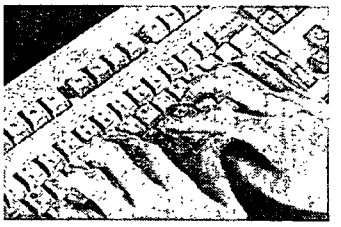
System or Base Unit

- Contains mother board, CPU, hard drive, power supply
- Floppy drive is generally installed
- Higher capacity storage devices may be installed, such as zip or tape drives



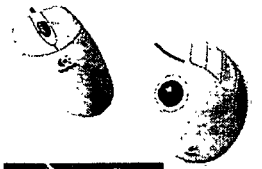
Monitor or CRT

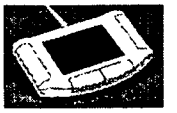
Keyboard



Pointing Devices

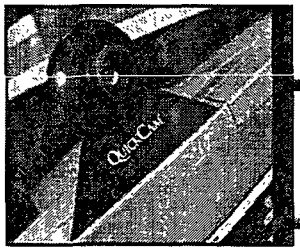
- Mouse
- Trackball
- Touch pads
- Touch screens





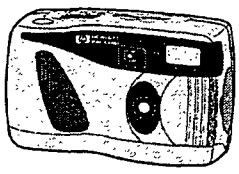
Video and Audio Devices

- Speakers, microphones and headsets for online voice communications
- Video cameras for online video applications



Peripherals Commonly Used

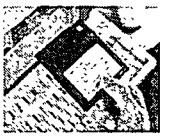
- Scanners
- Digital Cameras



Storage Devices and Magnetic Media

- Used to store digital information
- May be part of the computers system unit or a separate peripheral
- Consists of a devise to read and write the data and a magnetic media to store the data on.
- Capacity measured in the amount of bytes of information they will store

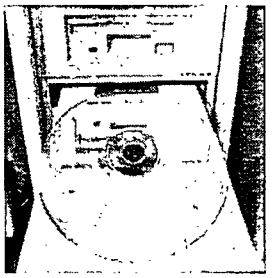
Some Examples

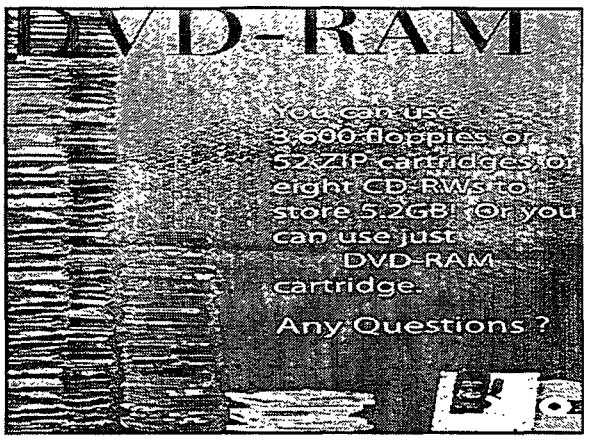


- Floppy disks 1.44 MB
- Zip Drives 100 or 250 MB

CD-Roms

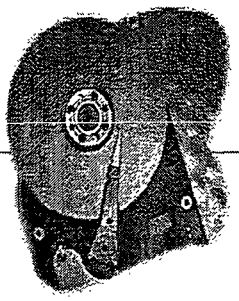
•650 MB Capacity





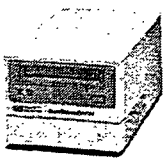
Hard Drive

- Generally installed in system unit
- Up to 20 GB capacity on consumer computers

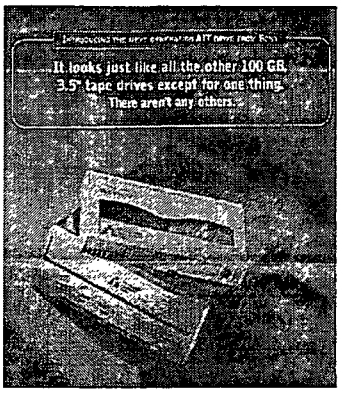


Tape Drives

- Back up tape drives store up to 10 GB
- 8 mm tapes (DAT) up to 20 GB

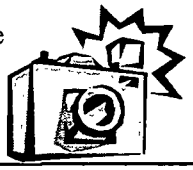


Advanced Intelligent Tape

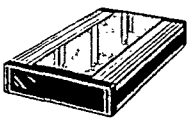


With an average picture size of 50,000 bytes

- You could store 2000 images on one zip drive
- You could store 400,000 on a DAT tape
- 2,000,000 on an AIT tape



Modem



- Modulator/demodulator
- Turns digital computer data--bits and bytes--into analog information
- Allows computer data to be transmitted over conventional phone lines
- Capabilities are rapidly changing

The Evolution of Computer Power

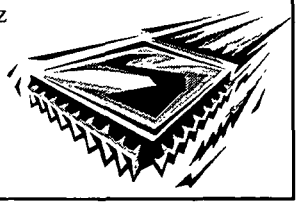
- The growth of computer capabilities in several areas has made today's applications and communications possible
  - Processing speed
  - Communications speed
  - RAM (random access memory)
  - Storage

If Aviation Had Progressed at the Same Rate As Computers...

- You could fly around the world for 2 cents
- The plane would fly at 2,000,000 mph
- The trip would take 50 seconds

Processor Speed

- Early computers had clock speed of less than 1 MHz
- Today you can affordably buy a computer that runs at 500 MHz



Communication Speed

- Earliest consumer modems communicated at 120 BPS
- Today you can purchase one that is capable of 56,000 BPS over conventional phone lines
- 1.5 million BPS in near future

Random Access Memory

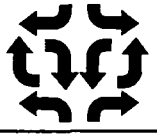
- Early consumer PC's had 1000 to 4000 bytes
- Today this laptop has 128 million bytes.

Storage

- Early floppy disks held 120,000 bytes of data
- Early hard drives held 10 million bytes
- Today you can store a gigabyte (billion)of data on a small cartridge
- Hard drives in consumer machines hold up to 20 gigabytes and more

This Power Enables

- Great strides in productivity in many areas
- Easier means to store, share and manipulate images, such as child pornography
- Real time audio and video communications via computer networks

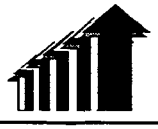


Computer Power is Rapidly Increasing

It is safe to predict that computers in the year 2047 will be at least one hundred thousand times more powerful than those of today

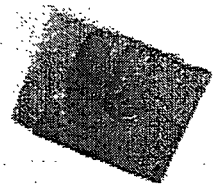
Gordon Bell and James Gray of Microsoft

Computing Power in the Future will Create More Benefit, but will also Create More Opportunity to Exploit the Technology for Criminal Purposes



Software

- Operating systems
- Application software
- Data files

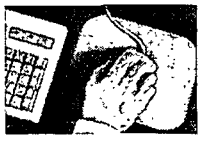


Operating Systems

- DOS
- Windows 98
- Windows NT
- Unix and its derivatives
- Many others

Applications Software

- Word and Word Perfect
- Excel
- Database packages
- Thousands of others, both commercial or developed for specific users

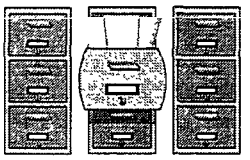


Applications Used in Child Pornography

- Photo editing software
- Graphics viewers and converters
- Scanning software

Data Files

- Data files from specific application
- Text
- Sound
- Graphics



Picture Formats

- Pictures on computers come in hundreds of formats
- The most common formats on the Internet are GIF (graphics information format) and JPEG (photographic experts group format)
- These two formats compress pictures into small file sizes
- Files will appear as **filename.gif** or **filename.jpg**

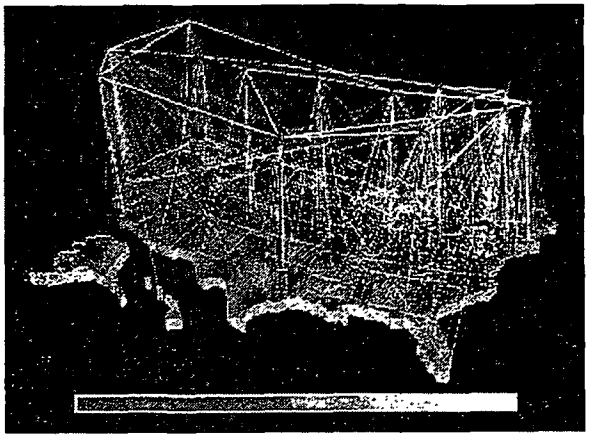
Connectivity and Computer Networks

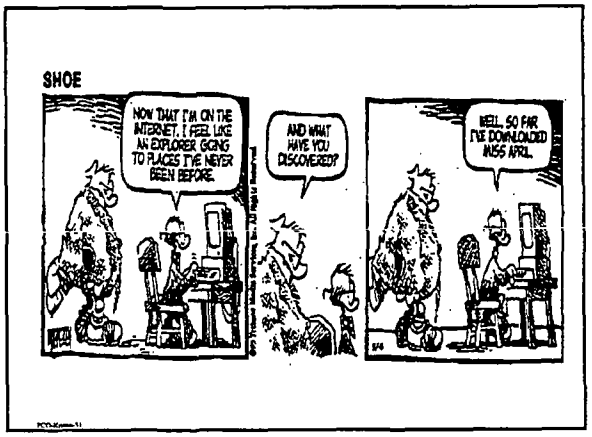
Networks

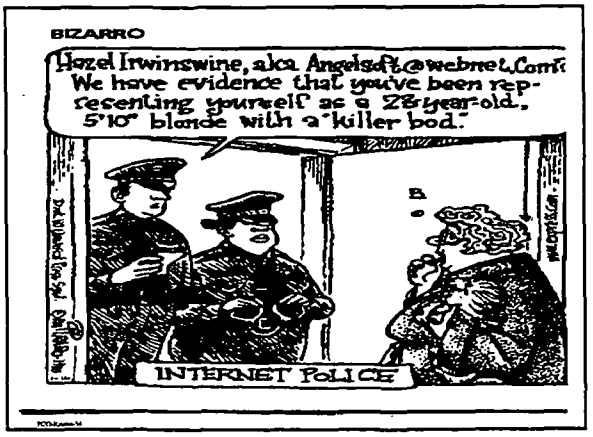
- Interconnected computers that can share data
- May be in one room or around the world
- Usually a client/server architecture
- May be as small as a two machine peer to peer network
- May be as big as Hewlett Packard's intranet consisting of 90,000 PC's, 23,000 workstations, 4000 servers, and 800 mini-computers

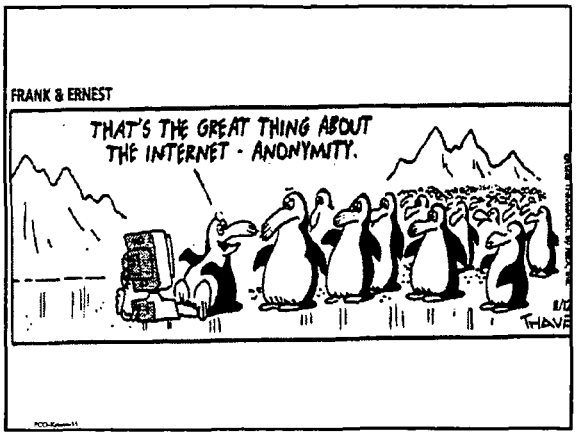
But the World's Biggest Network is the Internet

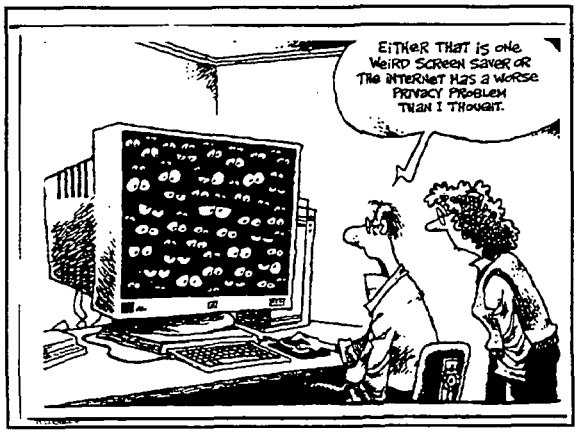
A Network of Networks




SHOE
NOW THAT I'M ON THE INTERNET, I FEEL LIKE AN EXPLORER GOING TO PLACES I'VE NEVER BEEN BEFORE.
AND WHAT HAVE YOU DISCOVERED?
WELL, SO FAR I'VE DOWNLOADED MISS APRIL.


BIZARRO
Hazel Irwinswine, aka Angelsoft@webnet.com:
We have evidence that you've been representing yourself as a 28-year-old, 5'10" blonde with a "killer bod."
INTERNET POLICE





"Everyone has a different Internet."

- Bruce Sterling, science fiction writer and Internet philosopher

Why was the Internet Created?

- Why was the Internet created?
  - Defense Dept.. Strategy
  - Share information
  - Communication

Internet Timeline

- **1957** -- the USSR launched Sputnik, the first artificial earth satellite. In response, the US Department of Defense formed the Advanced Research Projects Agency (ARPA) to establish the US as a leader in military technology and science.
- **1969** -- ARPANET commissioned by DoD for research into national networking in the event of a nuclear disaster. First nodes: UCLA, Stanford, UCSB, and U of Utah.
- **1979** -- USENET established between Duke and UNC.

- **1986** -- NSFNET created, linking the United States into one large network, hundreds of universities come online.
- **1988** -- First foreign countries connect into NSFNET and
  - IRC (Internet Relay Chat) developed.
- **1992** -- World-Wide Web is released.
- **1993** -- Business and media begin to take notice of the Internet. Mosaic takes the Internet by storm, WWW proliferates at a 341,634% annual growth rate,

- **1996** -- The Internet is the dominant theme throughout the the computer industry.
- **And Beyond**-- Personal and private use of the net grows exponentially, and will continue to do so

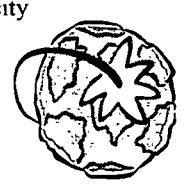
The Internet

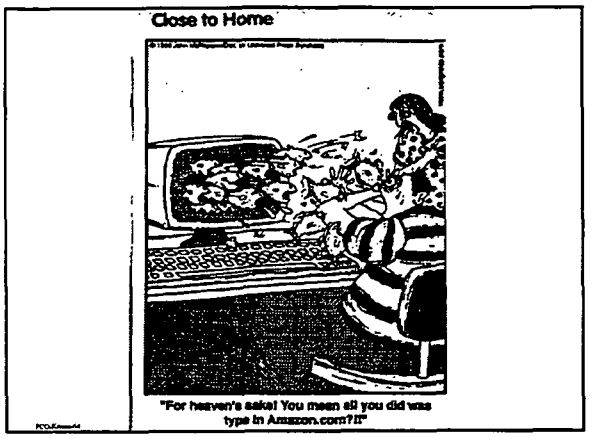
It is not far-fetched to expect that the net will gradually reorganize how, what, where and when we produce and consume

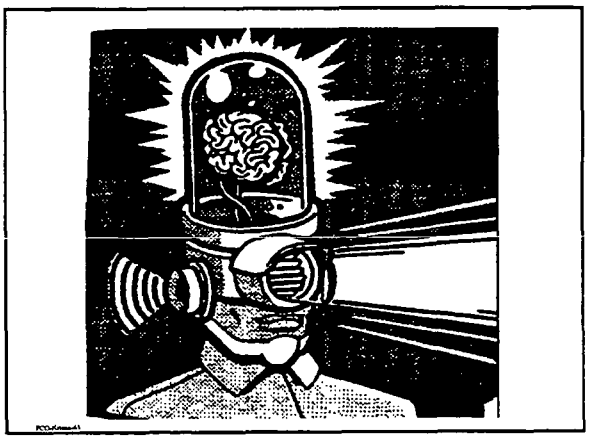
Riel Miller, The Internet in Twenty Years: Cyberspace, the Next Frontier?, 1997

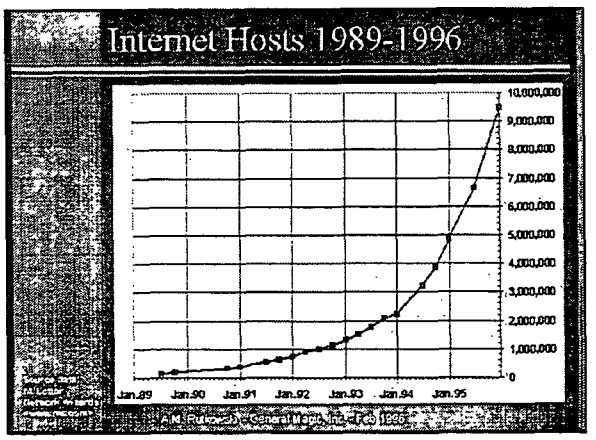
Internet Implications

- E-Commerce
- The Internet as catalyst...the Internet is transforming corporate America like no other invention since electricity
- Convergence
- Human evolution

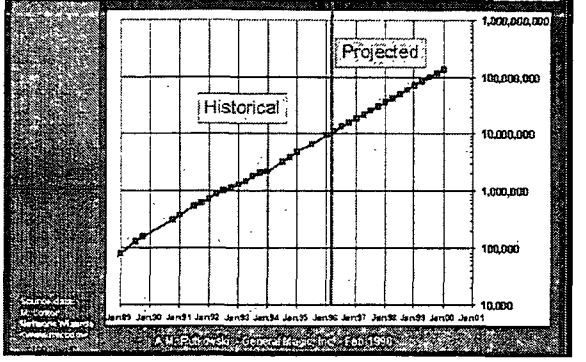



Close to Home
"For heaven's sake! You mean all you did was type in Amazon.com?!!"

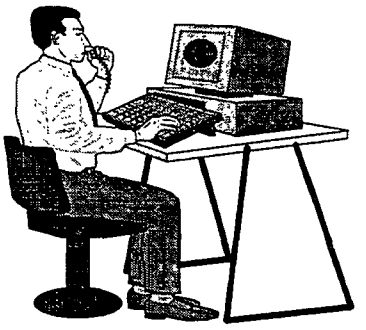



Internet Hosts 1989-1996
10,000,000
9,000,000
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
Jan.89
Jan.90
Jan.91
Jan.92
Jan.93
Jan.94
Jan.95

Internet Hosts - Overall Trend

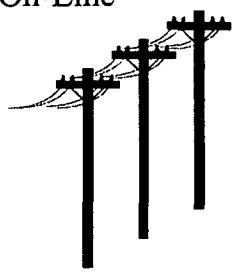


Connecting to the Internet

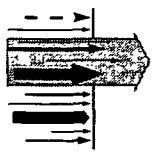


Getting On-Line

- Hardware
  - Modem
  - Computer
  - Telephone Line
- Software
  - Web browser
  - Other applications
- Internet Account



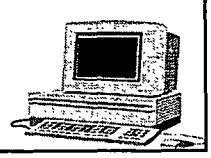
Four Basic Ways to Access the Internet



- Shell Account access
- PPP Dial-Up access
- Commercial Service access
- Leased-line access

Shell Account Access

- Low end connection
- Computer acts as dumb terminal
- No graphics
- BBS or FreeNet
- Unix Connection

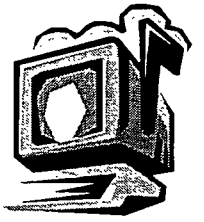


PPP Dial-Up Access

- PPP = Point to Point Protocol
- High end connection
- Local Service Provider
- Low cost
- Allows for greater flexibility - software stored on your computer

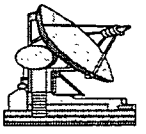
Commercial Service Access

- Prodigy
- CompuServe
- America Online
- Delphi
- MSN



Leased Line Access

- Most expensive access, $10K + per month
- High speed, digital transmission
- Direct Line available 24 hrs /day
- 5 to 10 times faster than regular modem
- Government agencies, corporations and research institutions

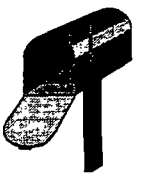


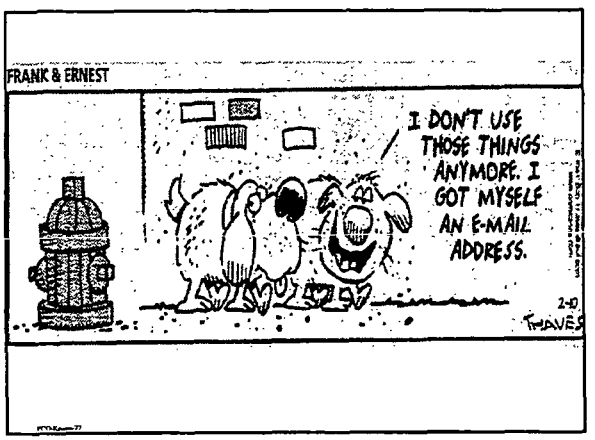
Some Internet Clients/Applications

- E-Mail
- Mailing Lists
- Newsgroups
- IRC
- FTP
- Telnet
- Gopher
- World Wide Web

E-Mail

- Most popular Internet application
- Easy way to send /receive messages and files
- No long distance charges, fast, cost-effective
- Global communication and data exchange
- Ability to send mail to a group
- Permanent log of correspondence

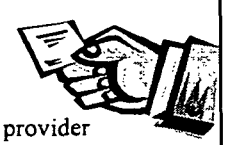




Names and Addresses

- E-mail users will have an e-mail address
- An e-mail address will resemble the following:

cja@coredcs.com



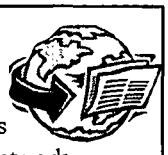
cja=	username
coredcs=	internet service provider
com=	domain

Common Address Domains

- **Domestic US Domains**
  - **.COM** -- Commercial Institutions
  - **.EDU** -- Academic Institutions
  - **.GOV** -- US Government
  - **.MIL** -- Military
  - **.NET** -- Network Institutions
  - **.ORG** -- Non-profit Organizations

- **International Domains**
  - **.AU** - Australia
  - **.CA** - Canada
  - **.CH** - Switzerland
  - **.NL** - Netherlands
  - **.UK** - United Kingdom

Newsgroups/Usenet



- Subject specific discussion forums
- Delivered via a universal feeder network called Usenet
- Messages kept on news servers, which carry various newsgroups
- Messages are not delivered to your mailbox, you must visit a Newsgroup
- 75,000+ Newsgroups exist

Newsgroup Basics

- All newsgroups are divided into categories or hierarchies, which try to define a broad commonality.
- Newsgroup names start with a very broad hierarchy area, followed by more specifics on the topic of discussion.

Newsgroup Hierarchies

Hierarchy:	Category:
bionet	Biology Research
bit.listserv	LISTSERVs
biz	Business
comp	Computers
misc.	Stuff that doesn't fit elsewhere
news	News about USENET
rec	Hobbies, games and recreation
sci	Science other than biology
soc	Social groups, ethnic groups
talk	Politics and related topics
alt	Controversial or unusual topics

Sample Newsgroups

- alt.abuse-recovery -- Helping victims of abuse recover
- alt.2600.warez
- alt.conspiracy.area51
- alt.barney.dinosaur.die.die.die
- comp.cog-eng -- Cognitive engineering
- sci.bio.ecology

Newsgroups Are Used Extensively by Sexual Predators

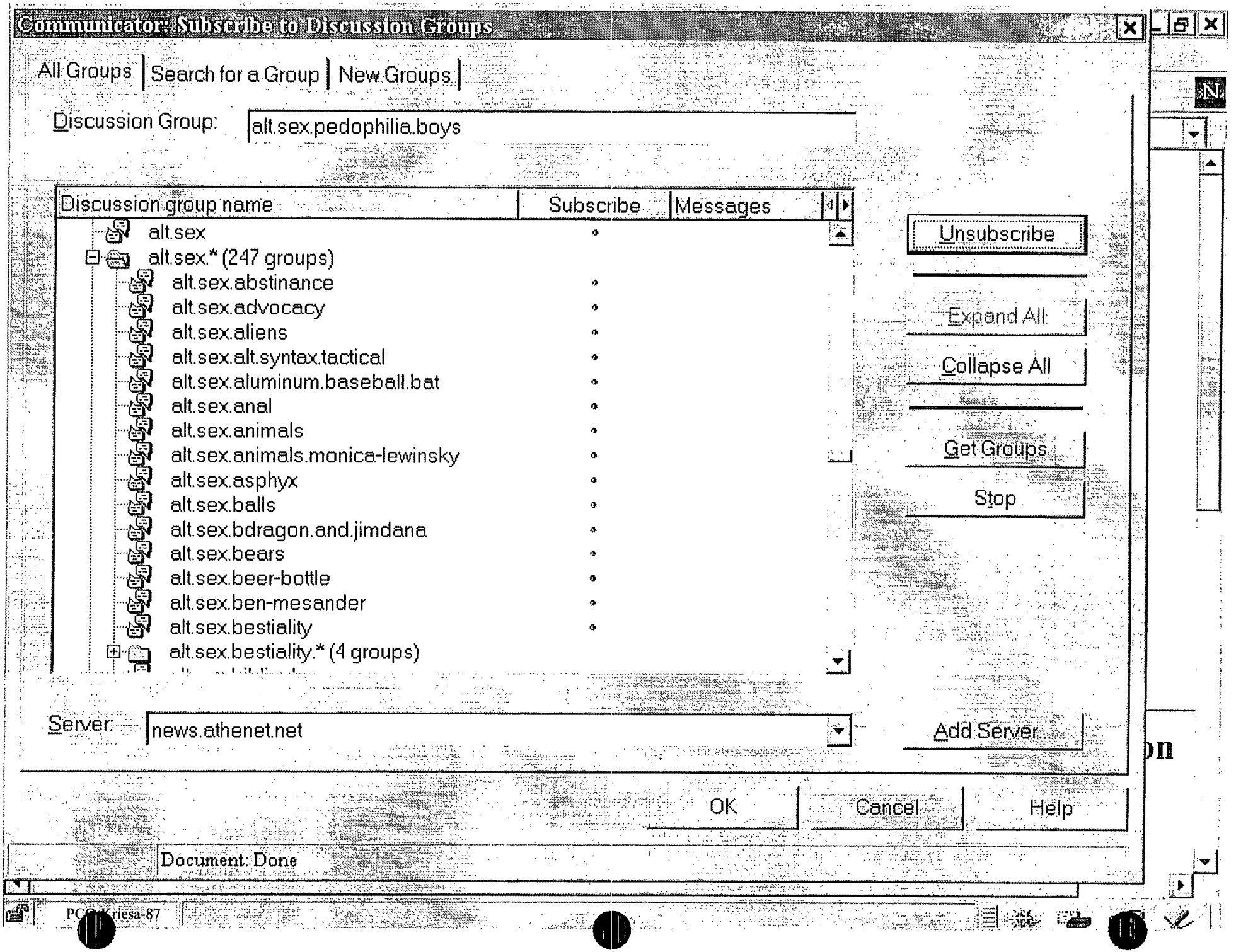
- Some believe they are the largest single area of pornography and child pornography on the Internet
- No controls over newsgroups except by ISP's who may decided not to carry some

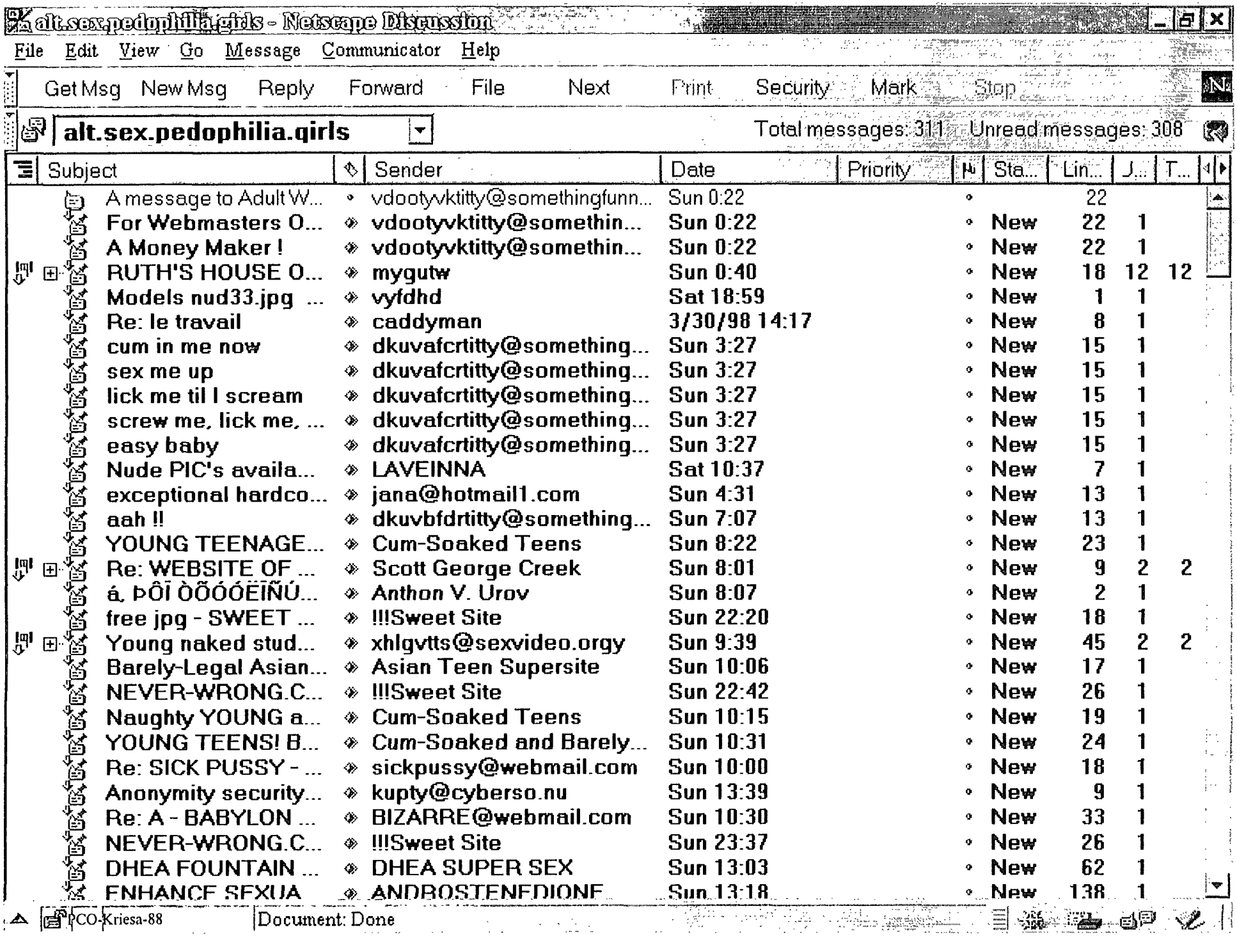
Some Examples

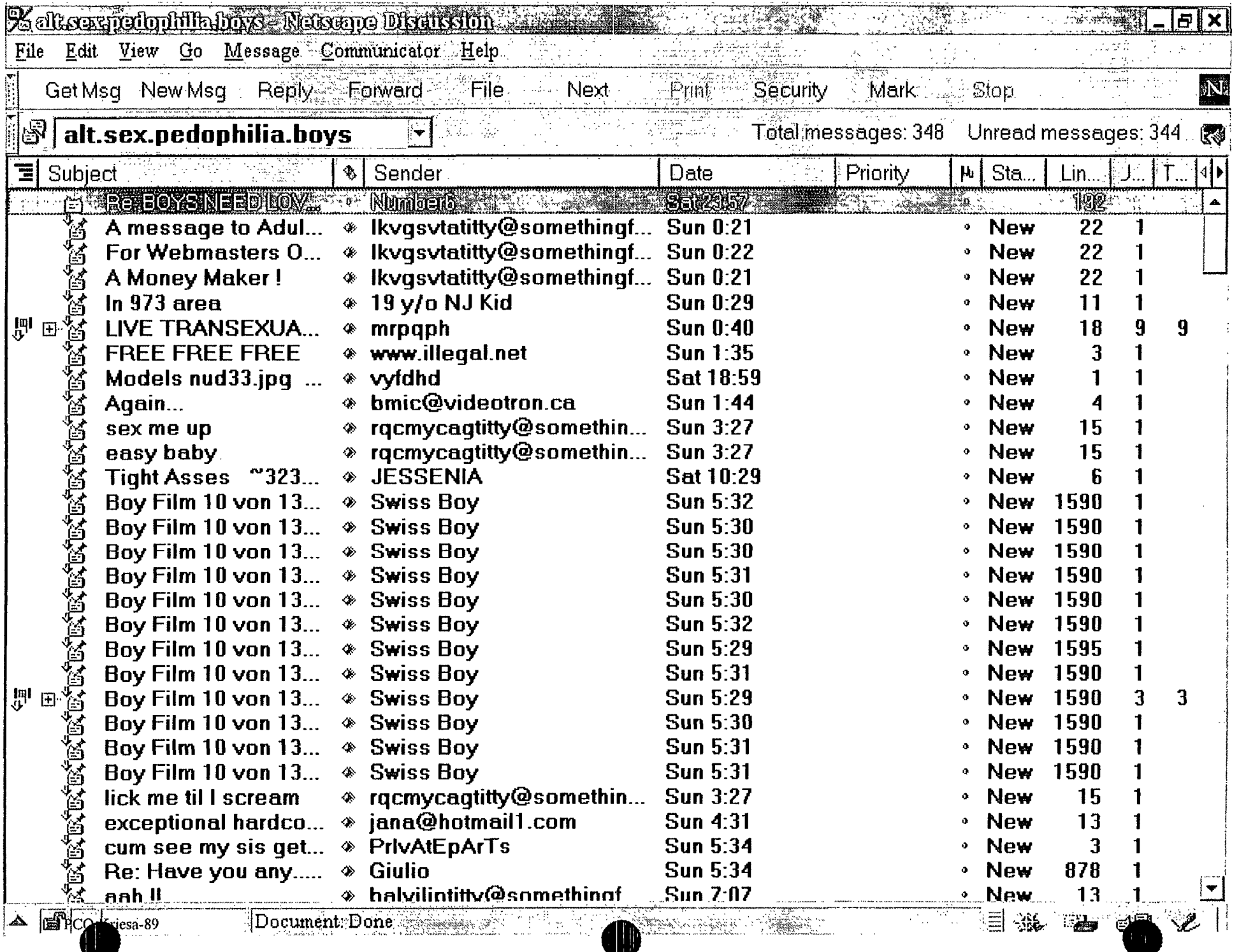
- alt.binaries.pictures.erotica.child.female
- alt.binaries.pictures.erotica.child.male
- alt.binaries.pictures.erotica.children
- alt.binaries.pictures.erotica.pre-teen
- alt.binaries.pictures.erotica.teen
- alt.binaries.pictures.erotica.teen.female
- alt.binaries.pictures.erotica.teen.male
- alt.binaries.pictures.erotica.female.teen

And More....

- alt.sex.boys
- alt.sex.children
- alt.sex.preteens
- alt.sex.pedophilia
- alt.sex.pedophilia.boys
- alt.sex.pedophilia.girls
- alt.sex.pedophilia.pictures
- alt.sex.pedophilia.swaps

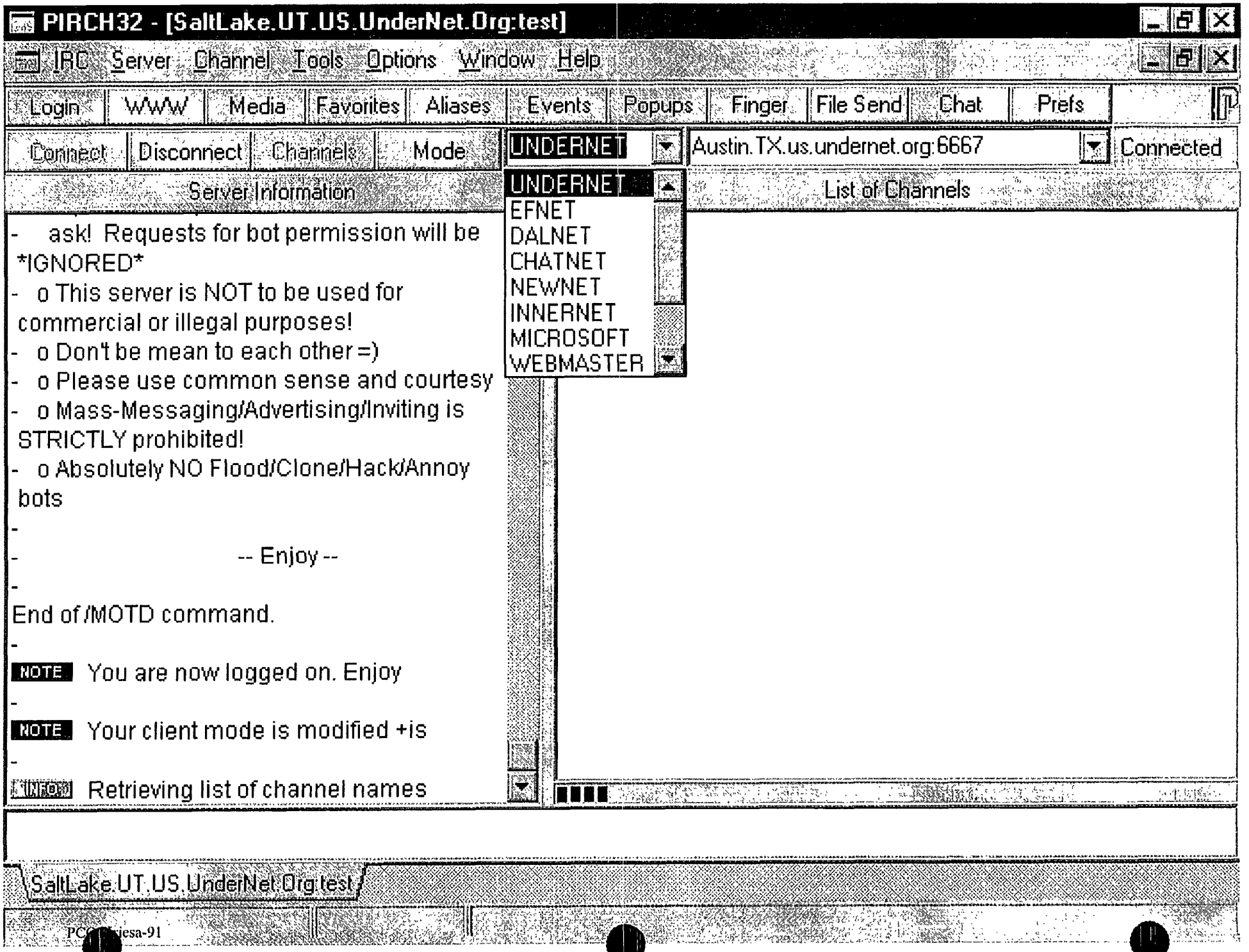

Communicator: Subscribe to Discussion Groups
All Groups
Search for a Group
New Groups
Discussion Group:
alt.sex.pedophilia.boys
Discussion group name
Subscribe
Messages
alt.sex
alt.sex.* (247 groups)
alt.sex.abstinance
alt.sex.advocacy
alt.sex.aliens
alt.sex.alt.syntax.tactical
alt.sex.aluminum.baseball.bat
alt.sex.anal
alt.sex.animals
alt.sex.animals.monica-lewinsky
alt.sex.asphyx
alt.sex.balls
alt.sex.bdragon.and.jimdana
alt.sex.bears
alt.sex.beer-bottle
alt.sex.ben-mesander
alt.sex.bestiality
alt.sex.bestiality.* (4 groups)
Unsubscribe
Expand All
Collapse All
Get Groups
Stop
Server:
news.athenet.net
Add Server...
OK
Cancel
Help
Document: Done

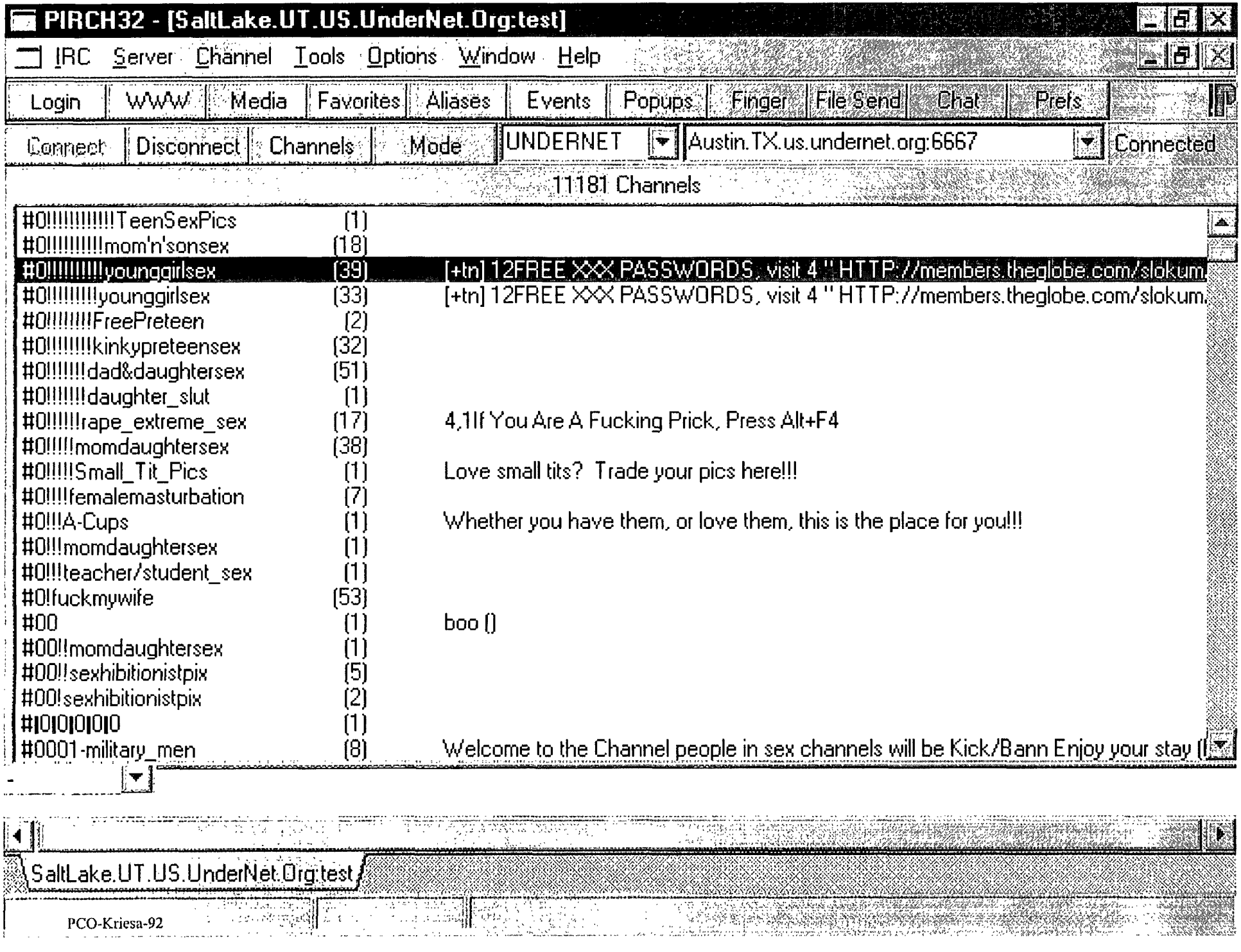

alt.sex.pedophilia.girls - Netscape Discussion
File Edit View Go Message Communicator Help
Get Msg New Msg Reply Forward File Next Print Security Mark Stop
alt.sex.pedophilia.girls
Total messages: 311 Unread messages: 308
Subject Sender Date Priority Sta... Lin... J... T...
A message to Adult W... vdootyvktitty@somethingfunn... Sun 0:22 22
For Webmasters O... vdootyvktitty@somethin... Sun 0:22 New 22 1
A Money Maker ! vdootyvktitty@somethin... Sun 0:22 New 22 1
RUTH'S HOUSE O... mygutw Sun 0:40 New 18 12 12
Models nud33.jpg ... vyfdhd Sat 18:59 New 1 1
Re: le travail caddyman 3/30/98 14:17 New 8 1
cum in me now dkuvafcrtitty@something... Sun 3:27 New 15 1
sex me up dkuvafcrtitty@something... Sun 3:27 New 15 1
lick me til I scream dkuvafcrtitty@something... Sun 3:27 New 15 1
screw me, lick me, ... dkuvafcrtitty@something... Sun 3:27 New 15 1
easy baby dkuvafcrtitty@something... Sun 3:27 New 15 1
Nude PIC's availa... LAVEINNA Sat 10:37 New 7 1
exceptional hardco... jana@hotmail1.com Sun 4:31 New 13 1
aah !! dkuvbfdrtitty@something... Sun 7:07 New 13 1
YOUNG TEENAGE... Cum-Soaked Teens Sun 8:22 New 23 1
Re: WEBSITE OF ... Scott George Creek Sun 8:01 New 9 2 2
á. ÞÔÎ ÒÕÓÓÉÏÑÚ... Anthon V. Urov Sun 8:07 New 2 1
free jpg - SWEET ... !!!Sweet Site Sun 22:20 New 18 1
Young naked stud... xhlgvtts@sexvideo.orgy Sun 9:39 New 45 2 2
Barely-Legal Asian... Asian Teen Supersite Sun 10:06 New 17 1
NEVER-WRONG.C... !!!Sweet Site Sun 22:42 New 26 1
Naughty YOUNG a... Cum-Soaked Teens Sun 10:15 New 19 1
YOUNG TEENS! B... Cum-Soaked and Barely... Sun 10:31 New 24 1
Re: SICK PUSSY - ... sickpussy@webmail.com Sun 10:00 New 18 1
Anonymity security... kupty@cyberso.nu Sun 13:39 New 9 1
Re: A - BABYLON ... BIZARRE@webmail.com Sun 10:30 New 33 1
NEVER-WRONG.C... !!!Sweet Site Sun 23:37 New 26 1
DHEA FOUNTAIN ... DHEA SUPER SEX Sun 13:03 New 62 1
ENHANCE SEXUA ANDROSTENEDIONE Sun 13:18 New 138 1
PCO-Kriesa-88
Document: Done

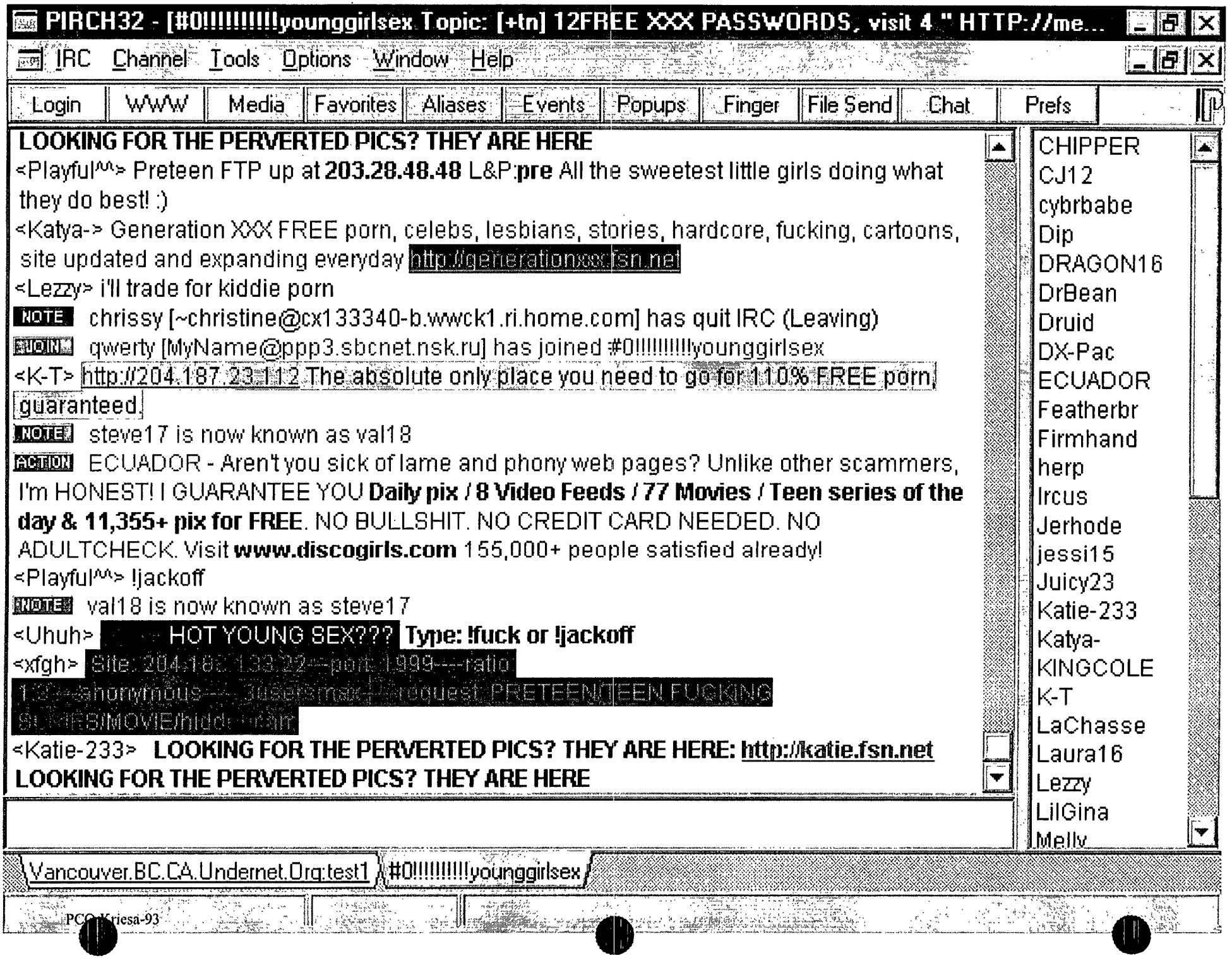

alt.sex.pedophilia.boys - Netscape Discussion
File Edit View Go Message Communicator Help
Get Msg New Msg Reply Forward File Next Print Security Mark Stop
alt.sex.pedophilia.boys
Total messages: 348 Unread messages: 344
Subject Sender Date Priority Sta... Lin... J... T...
Re: BOYS NEED LOV... Number6 Sat 23:57 192
A message to Adul... lkvgsvtatitty@somethingf... Sun 0:21 New 22 1
For Webmasters O... lkvgsvtatitty@somethingf... Sun 0:22 New 22 1
A Money Maker ! lkvgsvtatitty@somethingf... Sun 0:21 New 22 1
In 973 area 19 y/o NJ Kid Sun 0:29 New 11 1
LIVE TRANSEXUA... mrpqph Sun 0:40 New 18 9 9
FREE FREE FREE www.illegal.net Sun 1:35 New 3 1
Models nud33.jpg ... vyfdhd Sat 18:59 New 1 1
Again... bmic@videotron.ca Sun 1:44 New 4 1
sex me up rqcmycagtitty@somethin... Sun 3:27 New 15 1
easy baby rqcmycagtitty@somethin... Sun 3:27 New 15 1
Tight Asses ~323... JESSENIA Sat 10:29 New 6 1
Boy Film 10 von 13... Swiss Boy Sun 5:32 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:30 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:30 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:31 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:30 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:32 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:29 New 1595 1
Boy Film 10 von 13... Swiss Boy Sun 5:31 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:29 New 1590 3 3
Boy Film 10 von 13... Swiss Boy Sun 5:30 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:31 New 1590 1
Boy Film 10 von 13... Swiss Boy Sun 5:31 New 1590 1
lick me til I scream rqcmycagtitty@somethin... Sun 3:27 New 15 1
exceptional hardco... jana@hotmail1.com Sun 4:31 New 13 1
cum see my sis get... PrIvAtEpArTs Sun 5:34 New 3 1
Re: Have you any..... Giulio Sun 5:34 New 878 1
aah II halvilintitty@somethingf Sun 7:07 New 13 1
Document: Done

IRC

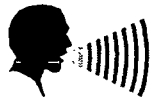
- Internet relay chat
- Huge multi-user chat facility
- Number of major IRC servers around the world that are linked to each other
- Anyone can create a "channel" and anything typed on that channel is seen by everyone else on the channel
- Private channels can be created


PIRCH32 - [SaltLake.UT.US.UnderNet.Org:test]
IRC Server Channel Tools Options Window Help
Login WWW Media Favorites Aliases Events Popups Finger File Send Chat Prefs
Connect Disconnect Channels Mode
UNDERNET
Austin.TX.us.undernet.org:6667
Connected
Server Information
List of Channels
UNDERNET
EFNET
DALNET
CHATNET
NEWNET
INNERNET
MICROSOFT
WEBMASTER
- ask! Requests for bot permission will be *IGNORED*
- o This server is NOT to be used for commercial or illegal purposes!
- o Don't be mean to each other =)
- o Please use common sense and courtesy
- o Mass-Messaging/Advertising/Inviting is STRICTLY prohibited!
- o Absolutely NO Flood/Clone/Hack/Annoy bots
-
- -- Enjoy --
-
End of /MOTD command.
-
NOTE You are now logged on. Enjoy
-
NOTE Your client mode is modified +is
-
INFO Retrieving list of channel names
SaltLake.UT.US.UnderNet.Org:test


PIRCH32 - [SaltLake.UT.US.UnderNet.Org:test]
IRC Server Channel Tools Options Window Help
Login WWW Media Favorites Aliases Events Popups Finger File Send Chat Prefs
Connect Disconnect Channels Mode
UNDERNET
Austin.TX.us.undernet.org:6667
Connected
11181 Channels
#0!!!!!!!!!!!!TeenSexPics (1)
#0!!!!!!!!!!!mom'n'sonsex (18)
#0!!!!!!!!!!younggirlsex (39) [+tn] 12FREE XXX PASSWORDS, visit 4 " HTTP://members.theglobe.com/slokum
#0!!!!!!!!!younggirlsex (33) [+tn] 12FREE XXX PASSWORDS, visit 4 " HTTP://members.theglobe.com/slokum.
#0!!!!!!!!FreePreteen (2)
#0!!!!!!!!kinkypreteensex (32)
#0!!!!!!!!dad&daughtersex (51)
#0!!!!!!!daughter_slut (1)
#0!!!!!!rape_extreme_sex (17) 4,1If You Are A Fucking Prick, Press Alt+F4
#0!!!!!momdaughtersex (38)
#0!!!!!Small_Tit_Pics (1) Love small tits? Trade your pics here!!!
#0!!!!femalemasturbation (7)
#0!!!A-Cups (1) Whether you have them, or love them, this is the place for you!!!
#0!!!momdaughtersex (1)
#0!!!teacher/student_sex (1)
#0!fuckmywife (53)
#00 (1) boo ()
#00!!momdaughtersex (1)
#00!!sexhibitionistpix (5)
#00!sexhibitionistpix (2)
#0!0!0!0!0!0 (1)
#0001-military_men (8) Welcome to the Channel people in sex channels will be Kick/Bann Enjoy your stay (
SaltLake.UT.US.UnderNet.Org:test
PCO-Kriesa-92

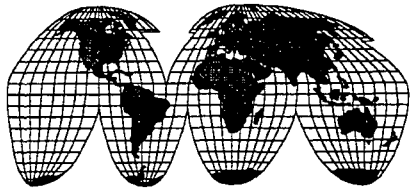

PIRCH32 - [#0!!!!!!!!!!younggirlsex Topic: [+tn] 12FREE XXX PASSWORDS, visit 4 " HTTP://me...
IRC Channel Tools Options Window Help
Login WWW Media Favorites Aliases Events Popups Finger File Send Chat Prefs
LOOKING FOR THE PERVERTED PICS? THEY ARE HERE
<Playful^^> Preteen FTP up at 203.28.48.48 L&P:pre All the sweetest little girls doing what they do best! :)
<Katya-> Generation XXX FREE porn, celebs, lesbians, stories, hardcore, fucking, cartoons, site updated and expanding everyday http://generationxxx.fsn.net
<Lezzy> i'll trade for kiddie porn
NOTE chrissy [~christine@cx133340-b.wwck1.ri.home.com] has quit IRC (Leaving)
JOIN qwerty [MyName@ppp3.sbcnet.nsk.ru] has joined #0!!!!!!!!!younggirlsex
<K-T> http://204.187.23.112 The absolute only place you need to go for 110% FREE porn, guaranteed.
NOTE steve17 is now known as val18
ACTION ECUADOR - Aren't you sick of lame and phony web pages? Unlike other scammers, I'm HONEST! I GUARANTEE YOU Daily pix / 8 Video Feeds / 77 Movies / Teen series of the day & 11,355+ pix for FREE. NO BULLSHIT. NO CREDIT CARD NEEDED. NO ADULTCHECK. Visit www.discogirls.com 155,000+ people satisfied already!
<Playful^^> !jackoff
NOTE val18 is now known as steve17
<Uhuh> HOT YOUNG SEX??? Type: !fuck or !jackoff
<xfgh> Site: 204.188.133.22---port: 1999---ratio 1:2---anonymous---3user@nsk---request: PRETEEN/TEEN FUCKING SCENES/MOVIE/hidden chair
<Katie-233> LOOKING FOR THE PERVERTED PICS? THEY ARE HERE: http://katie.fsn.net
LOOKING FOR THE PERVERTED PICS? THEY ARE HERE
CHIPPER
CJ12
cybrbabe
Dip
DRAGON16
DrBean
Druid
DX-Pac
ECUADOR
Featherbr
Firmhand
herp
Ircus
Jerhode
jessi15
Juicy23
Katie-233
Katya-
KINGCOLE
K-T
LaChasse
Laura16
Lezzy
LilGina
Melly
Vancouver.BC.CA.Undernet.Org:test1
#0!!!!!!!!!younggirlsex
PCO Kriesa-93

Chat Rooms



- Similar to IRC
- Provided by commercial services, such as AOL and CompuServe
- Chat feature is easily set up on any web page.

World Wide Web

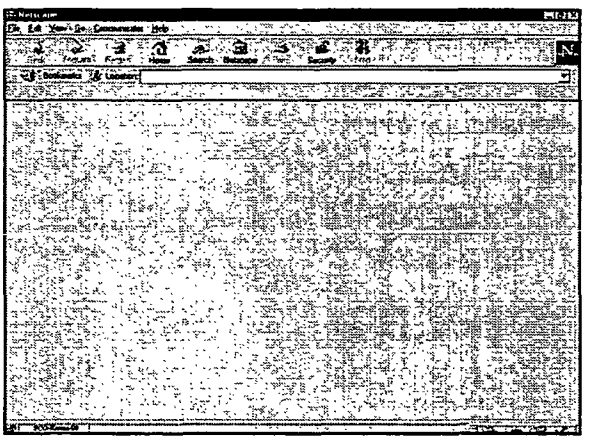


What is the World Wide Web?

The World Wide Web (WWW) is a global interactive, dynamic, cross platform, graphical hypertext information system that runs on the Internet.

What is a Web Browser?

- A Web Browser is special software such as Netscape Communicator or Internet Explorer which allows a user to view pages delivered from a Web Site situated at a particular URL on the World Wide Web.



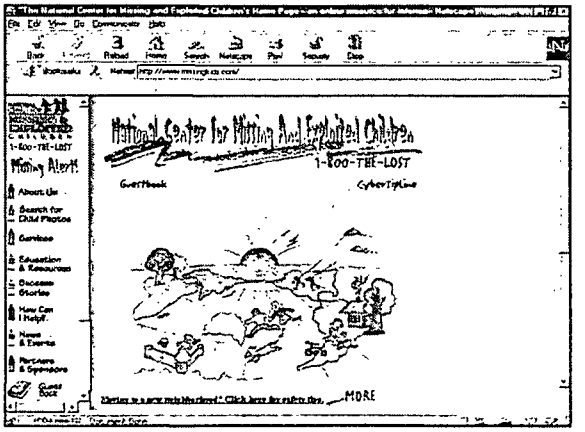
What is a URL?

A URL or Uniform Resource Locator is a unique address for the location of any type of Internet resource. A typical World Wide Web URL looks like this:

http://www.ibm.com

What is a Web Page?

A Web Page is a single document written in HTML (Hyper Text Mark-up Language) that includes the text of the document, its structure, any links to other documents and graphic images and other media.



What Is Available on the Web?

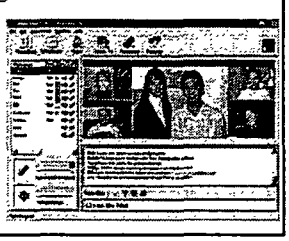
- Every type of organization, business, and enterprise has a web presence
- Many individuals have their own web sites
- Every digital resource imaginable is available
- There is too much information for anyone to comprehend

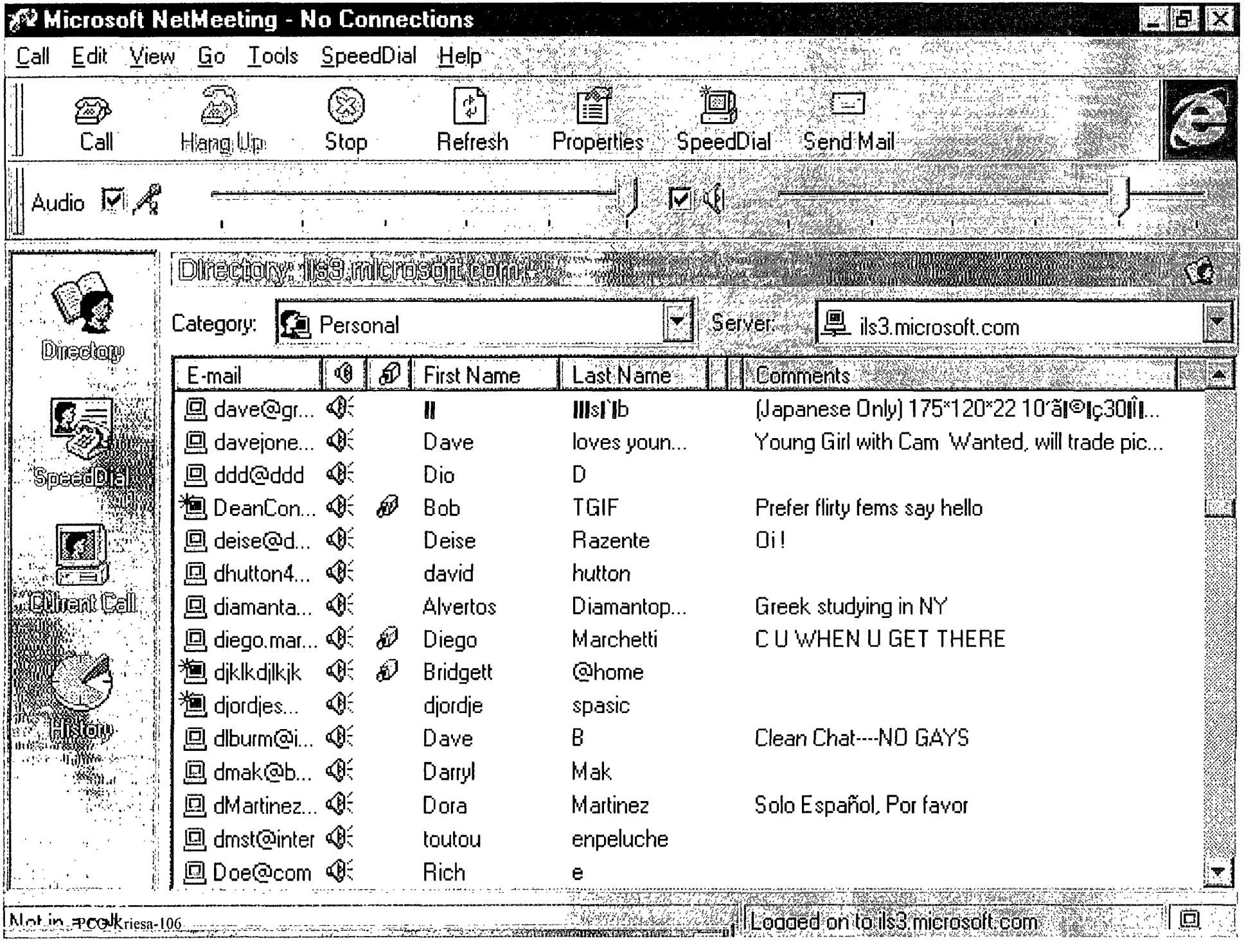
And on the Darkside

- Hundreds of thousands of sites dedicated to questionable or illegal activities
- Sex sites flourish
- It is simple and inexpensive for anyone to set up a web site in minutes and post child pornography
- WWW sites are advertised in Newgroups and IRC

Growing Use of Internet Telephony and Video

- Netscape Conference
- Microsoft NetMeeting
- CU-See Me




Microsoft NetMeeting - No Connections
Call Edit View Go Tools SpeedDial Help
Call
Hang Up
Stop
Refresh
Properties
SpeedDial
Send Mail
Audio
Directory: ils3.microsoft.com
Directory
SpeedDial
Current Call
History
Category: Personal
Server: ils3.microsoft.com
E-mail
First Name
Last Name
Comments
dave@gr... Ⅱ IIIsI`Ib (Japanese Only) 175*120*22 10´ãI©Iç30ÎÎ...
davejone... Dave loves youn... Young Girl with Cam Wanted, will trade pic...
ddd@ddd Dio D
DeanCon... Bob TGIF Prefer flirty fems say hello
deise@d... Deise Razente Oi!
dhutton4... david hutton
diamanta... Alvertos Diamantop... Greek studying in NY
diego.mar... Diego Marchetti C U WHEN U GET THERE
djklkdjlkjk Bridgett @home
djordjes... djordje spasic
dlburm@i... Dave B Clean Chat---NO GAYS
dmak@b... Darryl Mak
dMartinez... Dora Martinez Solo Español, Por favor
dmst@inter toutou enpeluche
Doe@com Rich e
Not in a call
Logged on to ils3.microsoft.com

Summary

- Computer crime is a growth industry
- Computer hardware allows computers to process, input, display, store, and communicate data
- Computer software consists of operating systems, applications, and data files
- Networks are interconnected computers
- The Internet is the world's largest computer network
- Different Internet applications are used to exploit children

Protecting Children On-line

Orientation to Computer Technology and Online Communications

ON-LINE CHILD PORNOGRAPHY/CHILD SEXUAL EXPLOITATION INVESTIGATIONS

RECOMMENDED HARDWARE AND SOFTWARE

SOFTWARE

Operating System: Windows 95 or 98. Windows NT Workstation is not recommended because it may not be compatible with the application software you will be using and is more complex to administer.

Application Software:

1. **Web Browser**: There are two major products in use, Microsoft Internet Explorer and Netscape Navigator. Both are functionally equivalent and you only need one of them to view web pages.

2. **Word Processor**: A major product such as WordPerfect or Microsoft Word is needed to read different types of text and word processed files.

3. **Internet Mail Client**: An application that will allow you to send and receive Internet E-Mail from multiple accounts. Some examples are Microsoft Outlook Express and Eudora Pro.

4. **NewsGroup Client**: An application that allows you to visit NewsGroups and download postings. Some examples are Outlook Express and Forte Agent.

5. **IRC Client**: An application that allows you to chat on the IRC system. Some examples are MIRC and PIRCH.

6. **Internet Tools**: An application that allows you to trace the origins of a particular Internet patron. You should choose a tool that has the capacity to conduct a TraceRoute, WHOIS, DNS, e-mail verification, PING and Port Scanner with FINGER. Some examples are Network Toolbox and NeoTrace.

7. **Graphic Viewing Software**: An application that allows you to view and analyze a multitude of graphic image types. Some examples are ThumbsPlus, Quickview Plus and ViewPrint.

8. **Commercial On-line Service**: If you are planning on working on America Online (AOL), Microsoft Network or any other self-contained on-line service, you will need that service's proprietary client software. If you choose to conduct investigations on AOL, an add on product that can be used is PowerTools by BPS Software. PowerTools augments the logging capabilities and Instant Messaging windows of the standard AOL Client.

HARDWARE - MINIMUM REQUIREMENTS:

Pentium 120 MHZ Processor
32MB RAM
2GB Hard Drive
Video Card with 2MB Video RAM
14" VGA Monitor
CD-ROM Drive
3.5" Floppy Disk Drive
28.8 Modem

HARDWARE - RECOMMENDED REQUIREMENTS:

Pentium II 266 MHZ Processor or better
64MB RAM
4GB Hard Drive
Video Card with 8MB Video RAM
17" SVGA Monitor
CD-ROM Drive
3.5" Floppy Disk Drive
56K V90 Modem
Iomega Zip Drive

The Investigation: Technical Aspects

Protecting Children Online

The Investigation: Technical Aspects

OJJDP

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Fox Valley Technical College
Knowledge That Works

FOR LAW ENFORCEMENT DISSEMINATION ONLY

PCO-Technical Aspects-1

Objectives

- Methods used to sexually exploit children on-line
- Organizational aspects to combating on-line crimes against children
- Overview of Structure and routing of Internet traffic
- Investigator's tool-kit
- Email Tracing and practical use of tools in an investigation.
- Search and Seizure
- Computer Forensics

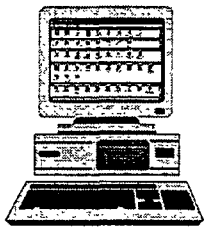
PCO-Technical Aspects-2

Not All Exits on The Highway Are Safe

PCO-Technical Aspects-3

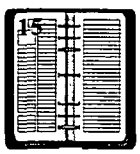
Child Molester and the PC

- Privacy
- Anonymity
- Invisibility
- Instant Gratification
- Lure



Privacy

Diaries and Journals



The computer provides the child molester a tool in which to organize and compose his inner thoughts, feelings and actions. This journal provides a means to share these thoughts without fear of exposure.

The ability to lock these entries with passwords and encryption schemes assures the privacy of such a journal. All text, pictures, sound, video and other computer data can be encrypted and secured with passwords

Anonymity

The ability to assume an identity while on-line provides the child molester with an air of confidence.

Invisibility

Invisibly lurking or skulking about on-line allows the child molester the ability to confidently and leisurely measure potential victims without fear of detection.

Instant Gratification

Instantaneously, a child molester can satisfy his cravings by going on-line and immediately downloading child pornography, fantasy stories, or even engaging in the process of courting a potential victim. Immediate feedback is obtained while interacting on-line

Hockey Chat

Tommy: "HI, any NJ Devils fans out there?"

Curt: "Devils suck, Rangers Rule?"

JB: "Devils - 1995 Stanley Cup Champions!"

TZinVa: "Go Devils - Brodeur for President."

JB: "Tommy, you go to the games?"

Tommy: "I wish; I live too far away."

JB: "Where?"

Tommy: "Toms River"

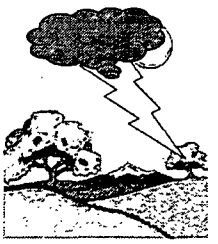
TZinVA: "That's only 1.5 hours, why don't you drive there?"

JB: "Cool, that's near Seaside"

Tommy: "I'm only 11, I don't drive and my Dad hates hockey."

The Dangers

- Web Sites
- Electronic Mail
- Newsgroups
- Interactive Chat
- FTP Sites
- New Technology



America Online

- Largest commercial on-line service provider
- Chats can occur in a 'chat room'
- Chat can occur via Instant Message (IM) session
- System based electronic mail
- Members only content
- Internet Gateway

Types of Cases

- *Distribution/Manufacturing of Child Pornography*
- Possession of Child Pornography
- Endangering the Welfare of a Child
- Obscenity Statutes
- Traveler Cases
- Harassment
- Terroristic Threats, Theft of Identity
- Organized Conspiracies
- Child Sex Tourism

How The Case Begins

- Visual Evidence: Photos,Pix,Movies
- E-Mail Messages
- Victim-Witness Disclosure
- Concerned Parent or Citizen
- Police Undercover Activity
- Inadvertent Discovery
- Law Enforcement Referral
- Media Referral

Responsibility

- Computer Crimes Unit
- Vice Unit
- Child Exploitation Unit
- All of the Above
- None of The Above
- Ginsu Approach

Policies & Procedures

- State/Federal Law Compliance
- Department SOP's and Operations Instructions
- Review Undercover Operations Guidelines
- ICAC standards
- Preservation of Electronic Evidence
- Prosecutorial Guidance

Recommended Equipment

- Dedicated Personal Computer
- Modem/Network Connection
- Printer/Video Output & Capture Device
- Magnetic/Optical Media
- Registered Software
- Hello Line
- Undercover Credentials
- Tape Recorder - Phone Tap
- Caller Id

Undercover Credentials

- Online Accounts
- Phone
- Address (PO Box, Mail Boxes etc.)
- DMV Identification
- Credit Cards
- Ability

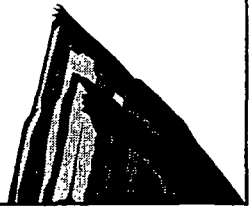
Dedicating Resources

- Pick your target, balanced decision
- Undercover Operations: manpower
- Pre-search warrant: resources within unit
- Complexity of gathering evidence
- Computer forensics: special skills, methodical, time and labor intensive, money, man hours
- Spider web growth of case

Challenges for Computer Investigations

Technical Challenges

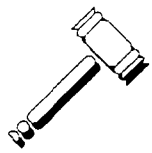
Legal Challenges



Technical Challenges

- Hardware, Software, Operating Systems
- Networks
- Passwords, Encryption, Stegonography
- Anonymous Remailers
- Spoofing
- Ever Changing Technology

Legal Challenges



- Jurisdictional Boundaries
- Insufficient Case Law
- Law Enforcement Competence
- ECPA
- Privacy Protection Act
- Cable Privacy Protection Act

Protecting Children Online

Understanding the Structure of the Internet

Internet Protocols

- Formal description of message formats and the rules computers must use to exchange those messages.
- Provide a set of rules that allow disparate computers and networks to communicate.
- Internet is based on the TCP/IP protocol suite.

Transmission Control Protocol over Internet Protocol (TCP/IP)

- Consists of a set of protocols that are used to link dissimilar computers across many different type of networks.
- TCP and IP are two of the protocols that make up this suite.
- Popular protocols include FTP, HTTP, SMTP, NNTP.

Internet Protocol Address

- Assigned number that uniquely identifies a host on the Internet.
- For routing purposes, no two computers can have the same IP Address
- Consists of a network part and a host part. The network part is assigned by IANA (Internet Assigned Numbers Authority) and the host part by the ISP.
- The network and host owners can be identified by examination of the address

IP Address 135.17.231.12

Internet protocol (IP) address is a unique 32 bit binary number usually represented as 4 fields each representing 8 bit numbers in the range 0 to 255 (called octets) separated by decimal points and identifies a connection to the network. The address consists of a network part and a host part. IP addresses are configured by software; they are not hardware specific. IP Addresses are often hidden from users who instead make use of the domain naming system. Software translates these domain names into IP addresses for routing.

IP Addressing

Dynamic Address: assigned by the ISP at time of connection from a pool of IP addresses. Upon disconnect, the address is returned to the ISP for reuse. It is important to maintain accurate recording of dates/times for later correlation.

Static Address: IP Address for the host does not change; can imply a persistent connection to the Internet. (i.e. cable modems)

Spider Servers or Proxy Servers.

IP Address Classes

There are 5 different address classes.

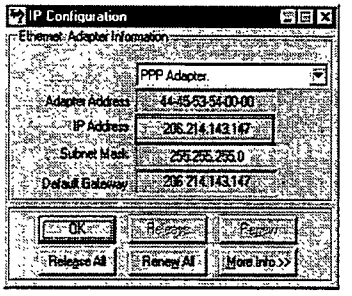
	1st Octet		Network IDs	Host Ids
Class A	1-126	1st Octet	126	16,777,214
Class B	128-191	1st 2 Octet	16,382	65,534
Class C	192-223	1st 3 Octets	>2,000,000	254
Class D	224-239	Used for multicasting		
Class E	240-255	Reserved for Future Use		

- In a Class A address the network is identified by the first octet and the host by the remaining 3 octets.
- In a Class B Address the network is identified by the first two octets and the host by the last two.
- In a Class C Address the network is identified by the first three Octets and the host by the 4th Octet.

What's my IP Address?

In Windows 95/98 you can determine your computer's IP Address by clicking on the Start, Run and then typing in winipcfg.

Or from a command prompt type ipconfig and then hit enter.



Domain Name System (DNS)

- **Distributed database that is used to map Internet names to their corresponding IP addresses, and vice versa.**
- **A method of identifying and locating a computer on the Internet**
- **Domain Name format:**
  security.lucent.com = 135.118.231.12

Domain Field

The domain for a name appears as its right-most label. If in the U.S., each host is assigned one of the following domains based on its usage:

gov	Non-military government affiliated
edu	Educational institution
com	Commercial or industrial organizations
org	Other organizations, such as non-profits
net	Network operations and service centers
mil	Military
arpa	ARPANET members

Domain Name Format

- Read from left to right
- Hierarchical Structure
- subdomain3.subdomain2.subdomain1.com

Examples:
orion.webspan.net
njw.injersey.com
bullwinkle.security.lucent.com
ftp.microsoft.com

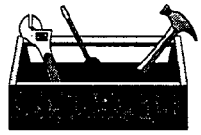
International Domain Labels

Countries have a domain name assigned to it that corresponds to its two-letter country code.

United states	us
Brazil	br
Ireland	ie
Paraguay	py
England	uk

Investigative Tools

- Whois
- Finger
- Ping
- Traceroute
- Audit Trails & Logs
- Search Engines
- Sniffers
- Protocol Analyzers



Investigative Tools

- Most tools are just commands and/or utilities that are part of your operating system and may be run from the command line.
- Graphical front ends at web sites and client side programs provide for ease of use.
- They exploit and interrogate computers, networks, databases, routers, etc. to provide the investigator with leads, corroborative information and evidence.
- Investigator should always double check the results of these queries.

Useful Software Tools

- Netscan Tools
- Netlab
- Sam Spade
- Visual Route
- Neotrace
- Ferretsoft Tools

Some Useful Web Based Tools

- ARIN: http://www.arin.net/whois/arinwhois.html
- Asia-Pacific Information: http://www.apnic.net
- European Information: http://www.ripe.net
- IP Tools: http://home.ag.org/iptools.htm
- ISP lookup: http://www.webisplist.com
- ISP lookup: http://www.isps.com
- Dragon Star: http://ipindex.dragonstar.net/index.html

Whois

- Registry of host and network administrators or other points of contact.
- Consists of a database of all registered domains.
- Domains do not exist unless they are registered with the Internic.
- Both a protocol and an application.
- Valid for for second level domain names.
- Whois databases include domain names, IP addresses, points of contact for a domain, postal mail addresses, telephone numbers, etc.

The WHOIS Database

injersey.com :

```
Registrant:
     New Jersey Press (INJERSEY-DOM)
     3601 Hwy 66
     Neptune, NJ 07754

     Domain Name: INJERSEY.COM

Administrative Contact:
     Byrum, Frank . (FB2441)  byrum@INFI.NET
     (757) 624-2695 (FAX) (757) 625-2473
     Technical Contact, Zone Contact:
     Borchers, Marr M  (MMB111)  mborchers@NETMORETWO.COM
     (877) 800-6574
Billing Contact:
     ADP Autonet  (ADP-BIL)  billcontact@autonet.net
     (800) 521-2732    fax (313) 995-6458

     Record last updated on 24-Feb-99.
     Record created on 29-Dec-94.
     Database last updated on 19-Aug-99 04:22:31 EDT.

     Domain servers in listed order:

     NS1.NW2.NET                    207.187.0.20
     NS2.NW2.NET                    207.187.8.20
```

Finger

- **Finger is a Unix command which is used to get information on a given user.**
- **If no user name specified, FINGER displays information on all users currently logged in on that host.**
- **Host must have a "FINGER" daemon running.**

```
finger phillips

Login name: phillips              In real life: Richard D. Phillips
Directory: /home/phillips         Shell: /bin/bash
On since July 12 12:43:02 on ttyb
No Plan
```


Finger

- Provides information about each user on a specified host
  - login name
  - full name
  - home directory
  - login shell
  - time of login (if user is currently logged in)
  - time of last login (if user is not currently logged in)
  - terminal or host from which the user logged in
  - last time received mail
  - last time read mail
  - idle time
  - plan in file ".plan" or project in ".project" in home directory

Ping

Ping is the networking equivalent of a sonar device and is used to verify that a given Internet address is actually reachable. Ping resolves the hostname to an IP address and sends an echo request to that host on a periodic basis. Each line beginning with "64 bytes..." is the echo reply received from the host. The time field tells you the round trip time for the packet.

```
# ping htc.net.org
PING htc.net.org (206.192.153.4) : 56 data bytes
64 bytes from 206.192.153.4:   icmp_seq=0    ttl=254  time=35.9 ms
64 bytes from 206.192.153.4:   icmp_seq=1    ttl=254  time=22.1 ms
64 bytes from 206.192.153.4:   icmp_seq=2    ttl=254  time=25.7 ms
```

Traceroute

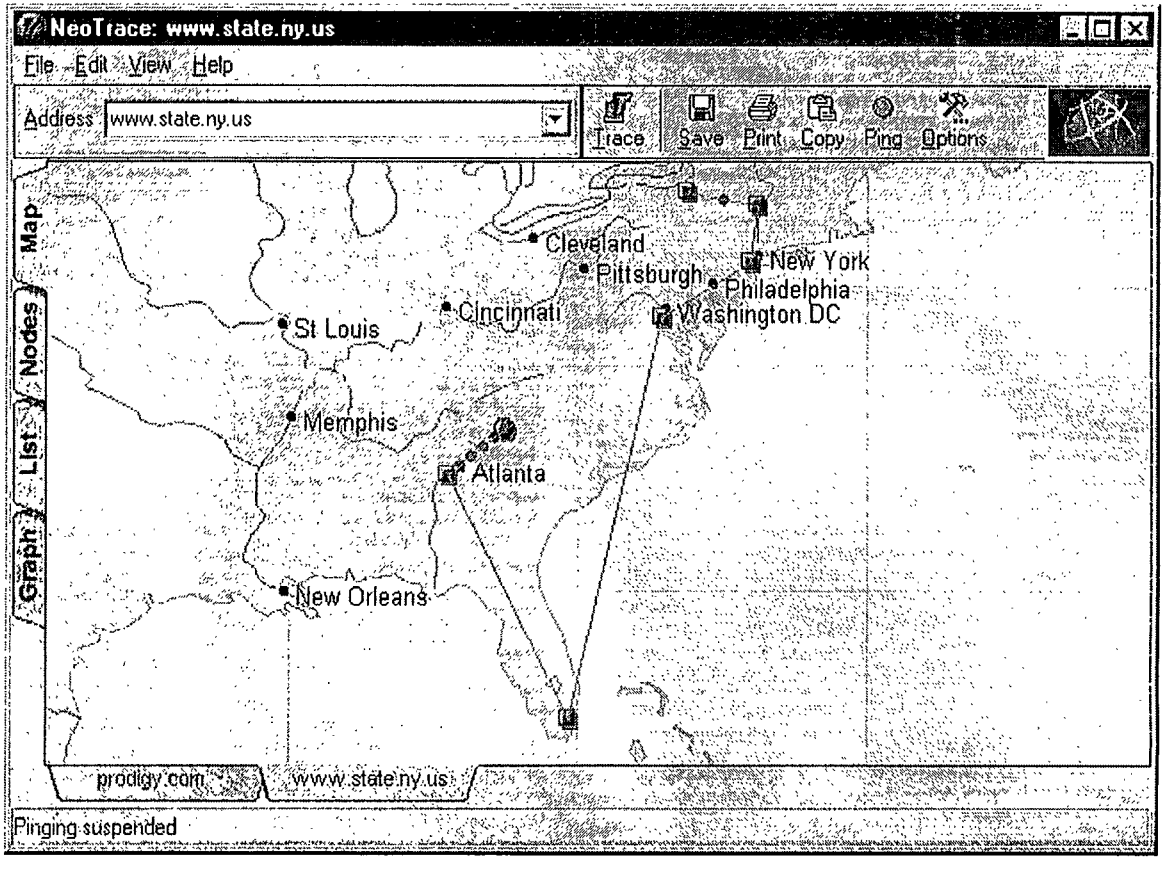
A utility that traces a packet from your computer to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. Using traceroute is useful in order to determine the delivery path of a packet.

In Windows 95/98/NT traceroute is named "tracert" and can be invoked at the DOS command line using the following syntax: *c:\tracert ip-address*

Traceroute can narrow down the geographic location of a particular host. Do not rely on whois information for this as it is non-authoritative.

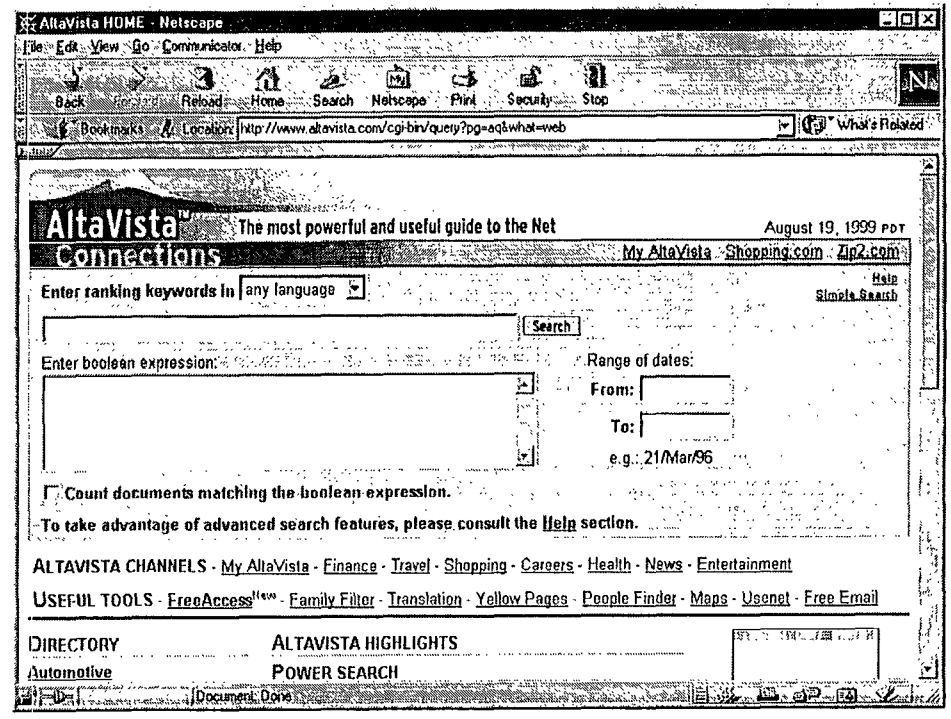
Third Party Traceroute Tools

- Netlab
- Netscan Tools
- Neotrace
- Visual Route
- Sam Spade



Search Engines

- Web based programs that will make a list of web sites matching user-chosen criteria.
- Some Useful sites include:
  - www.thebighub.com
  - www.dogpile.com
  - www.altavista.com
  - www.deja.com
  - www.switchboard.com



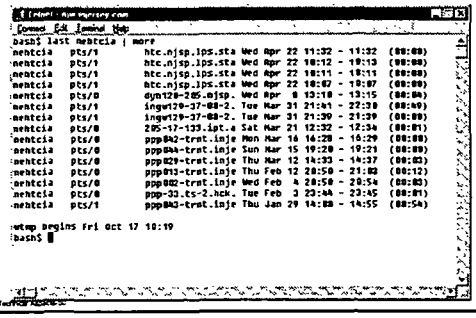
Unix and its variants

A basic understanding of the Unix operating system will go a long way towards making your computer related investigations much simpler. Recommended texts include Unix for Dummies and Unix for MS-DOS Users.

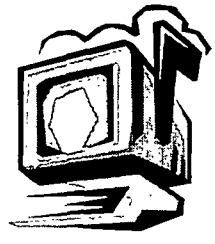
All the utilities you just saw are Unix commands.

Last

The last command will provide you with the logins for users on a particular system. The syntax is: last username.



Anatomy of an E-mail



- How it gets from here to there
- Where's it stored?
- What's a header?
- What's the sender's address?
- Tools to help decipher
- Spoofing

E-Mail Addresses

An Internet e-mail address consists of two parts:

Username @ domain.name

The username indicates the name of the particular user's mailbox. This "mailbox" is stored as a file on a mail server

The domain name indicates where the user's mailbox is located on the Internet. Or more specifically the domain name of the computer that it is stored on.

E-Mail Addresses

From: molester@trouble.com
To: victim@the-end.com
Subject: You're Dead

Most e-mail software by default displays limited information with respect to the message delivered and its route. It appears the message above came from the e-mail address "**molester@trouble.com**".

Understanding E-Mail Headers

Each mail server receiving an e-mail message adds a Received: header to the full message headers. It is possible for end users to add their own Received: headers to messages. But, end-users cannot modify the Received: headers added by the mail servers which deliver the message.

The exact format of Received: headers may vary from site to site, but in general, they follow the format below. There may be several entnes for "received from" lines. These "received from" entries are the keys to tracking back the email through the servers it traversed.

Received: from reported-sender (DNS-hostname [Connecting-IP-Address]) by mail-server-configured-name (mailer-version/mailer-config-version) with protocol id mail-server-job-identification; time-and-date-stamp.

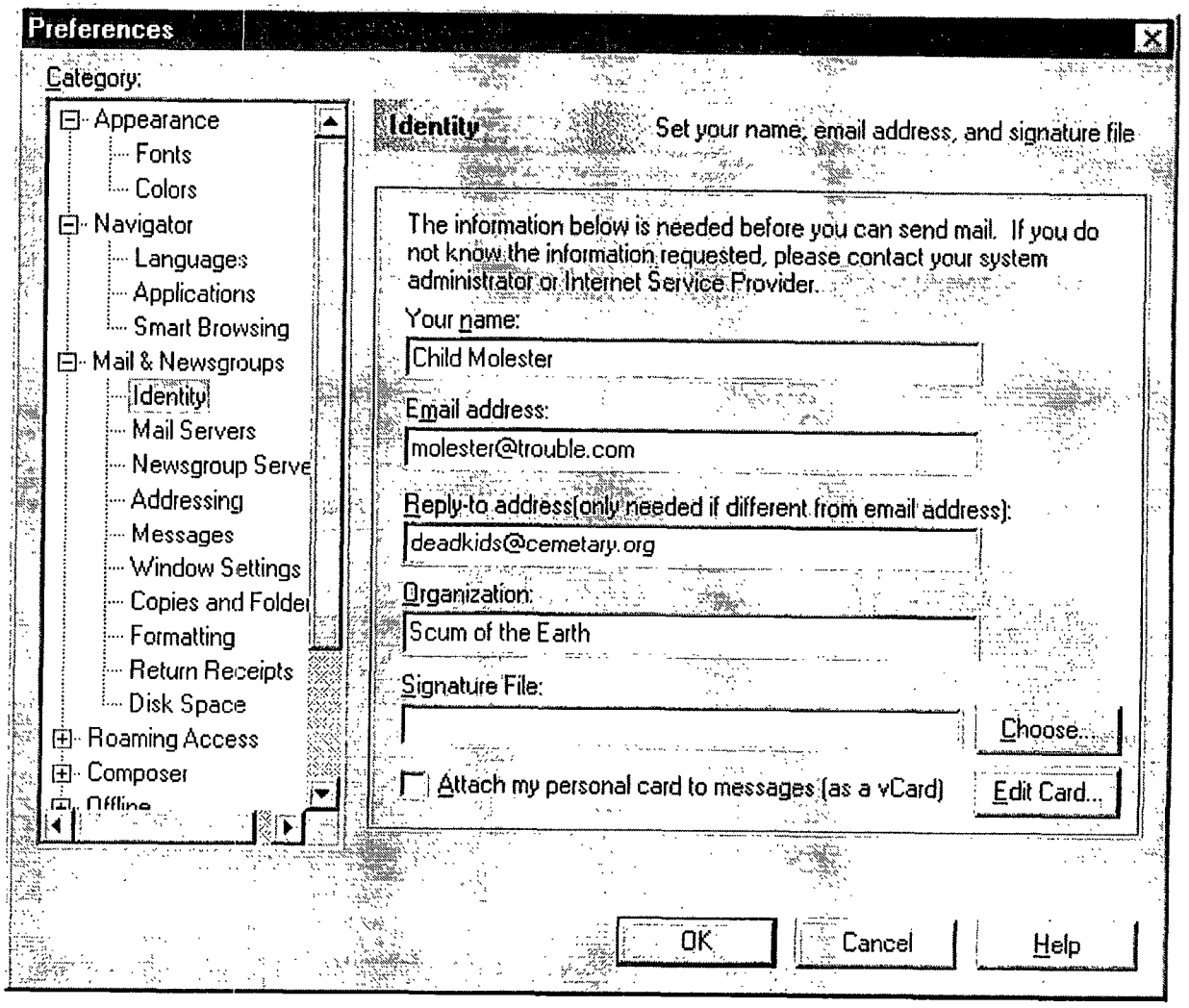
Suspect Header Entries

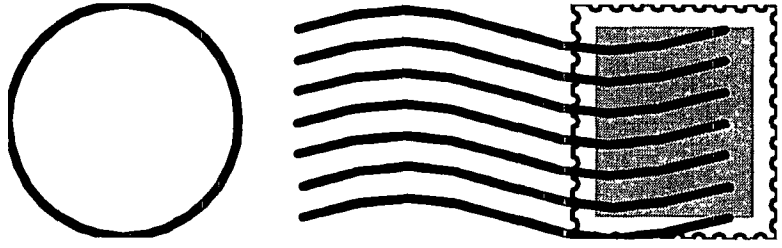
When analyzing an email header do not rely on the below listed fields. The only authontative information included in a header is that which is inserted by the mail servers the message traverses, and where no human interaction takes place.

- Subject
- Sender name/address
- Return Path
- Recipient name/address
- Date
- Time
- Organization
- Comments
- Message ID
- Signature

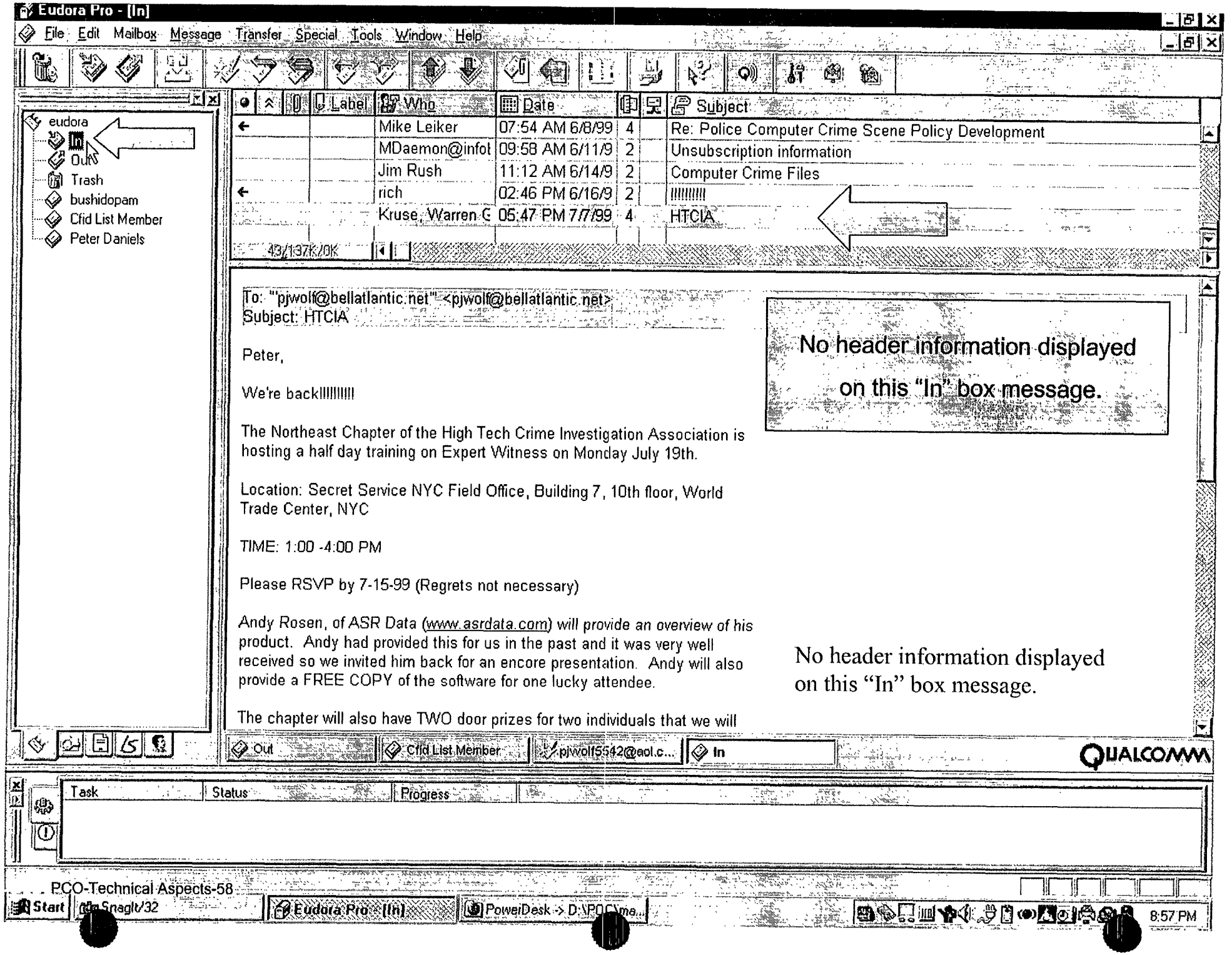
E-Mail Addresses:

Most of today's e-mail software allows the end user to configure their e-mail address placed in outgoing messages. Because of this, e-mail addresses are very easily forged or made to be fictitious and should never be considered the authoritative pointer to the true source of message origination.

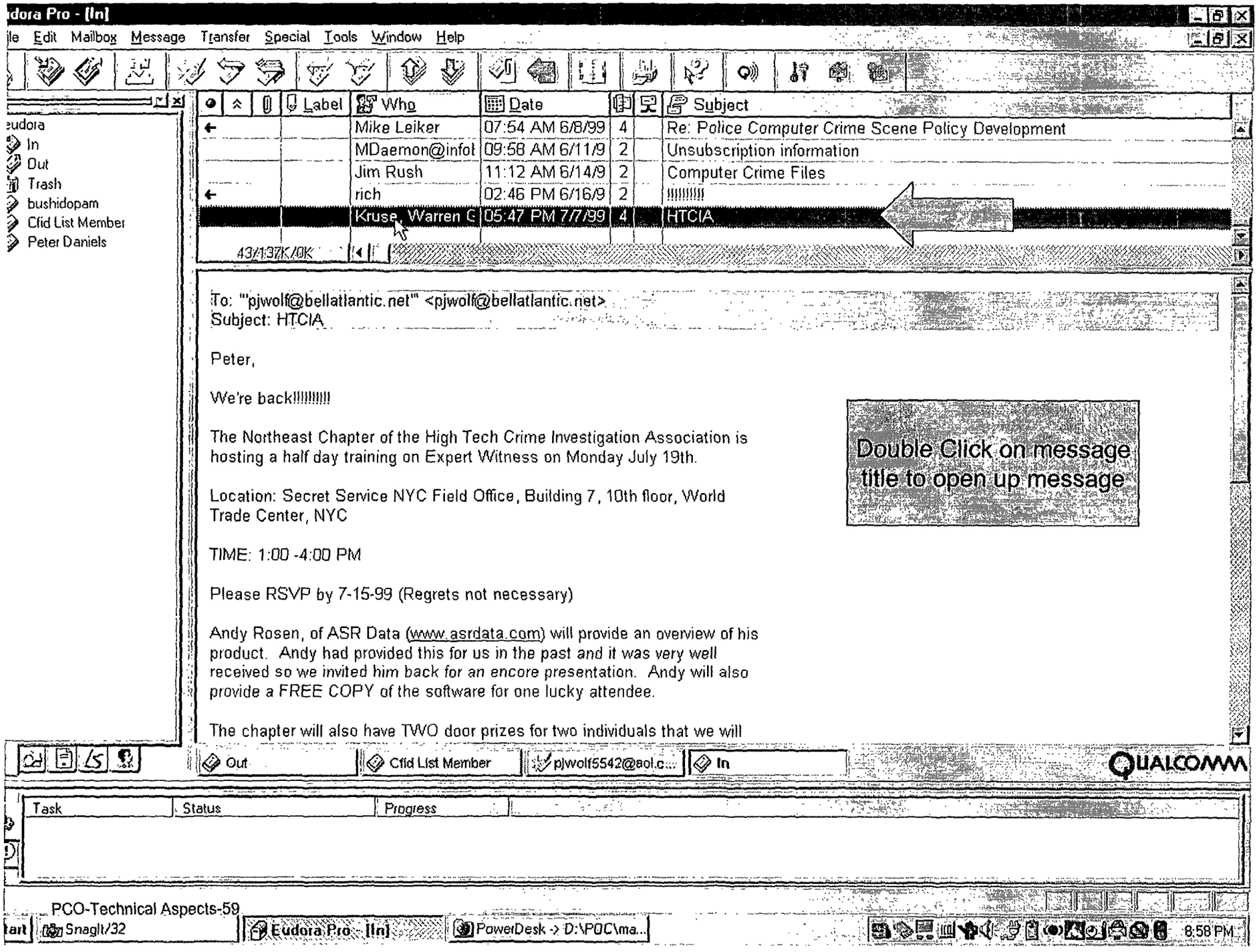


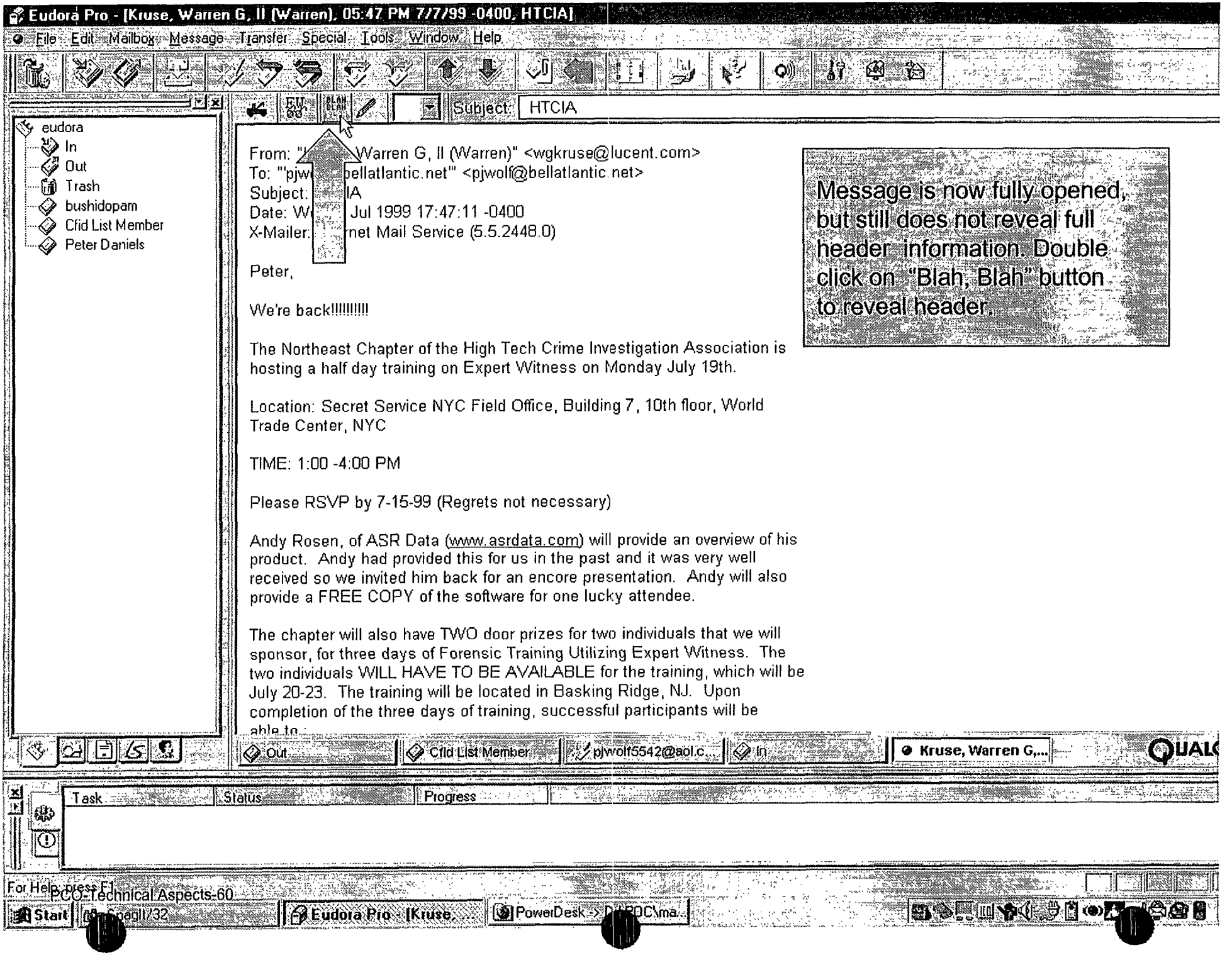


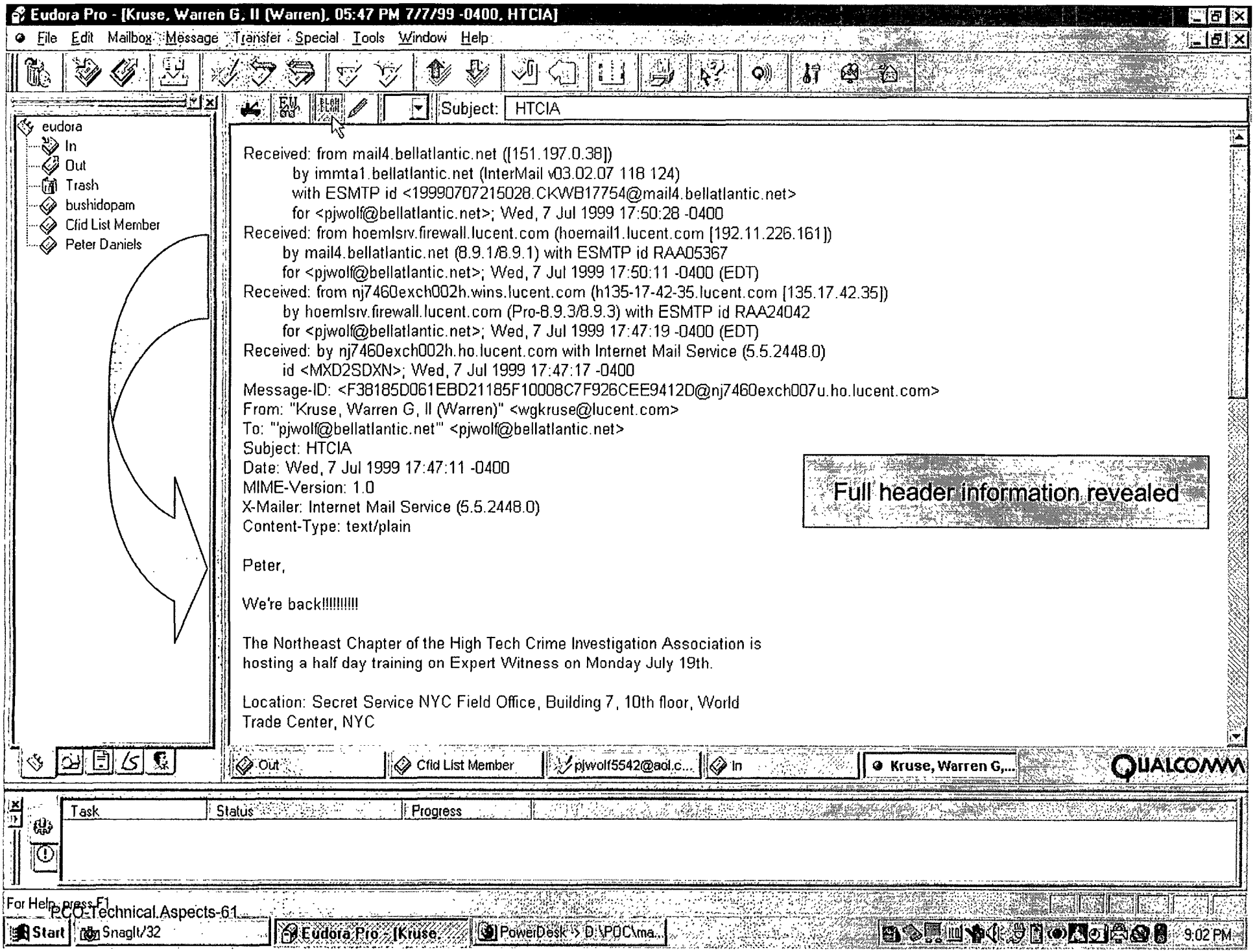
Displaying Headers in Popular Email Programs

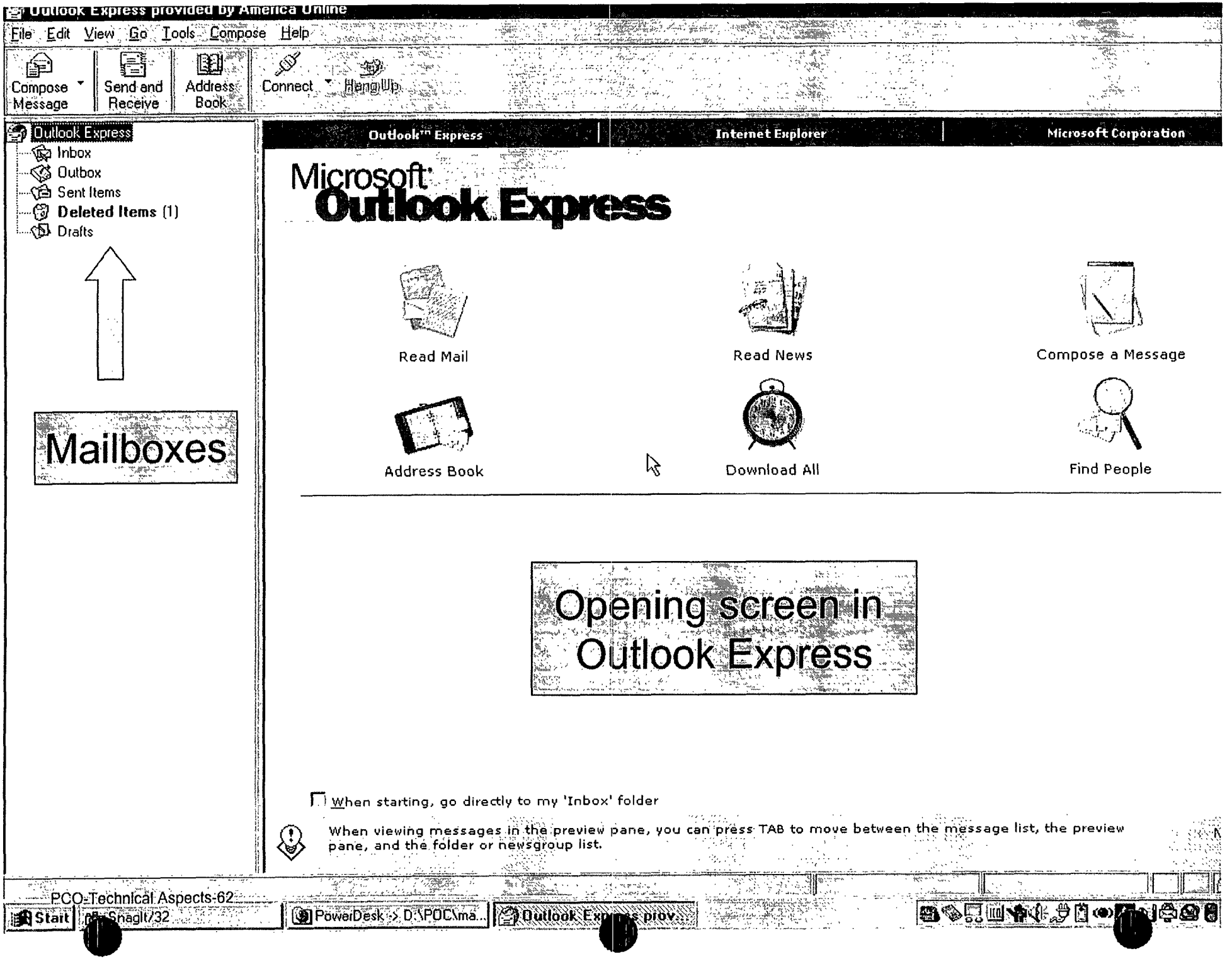


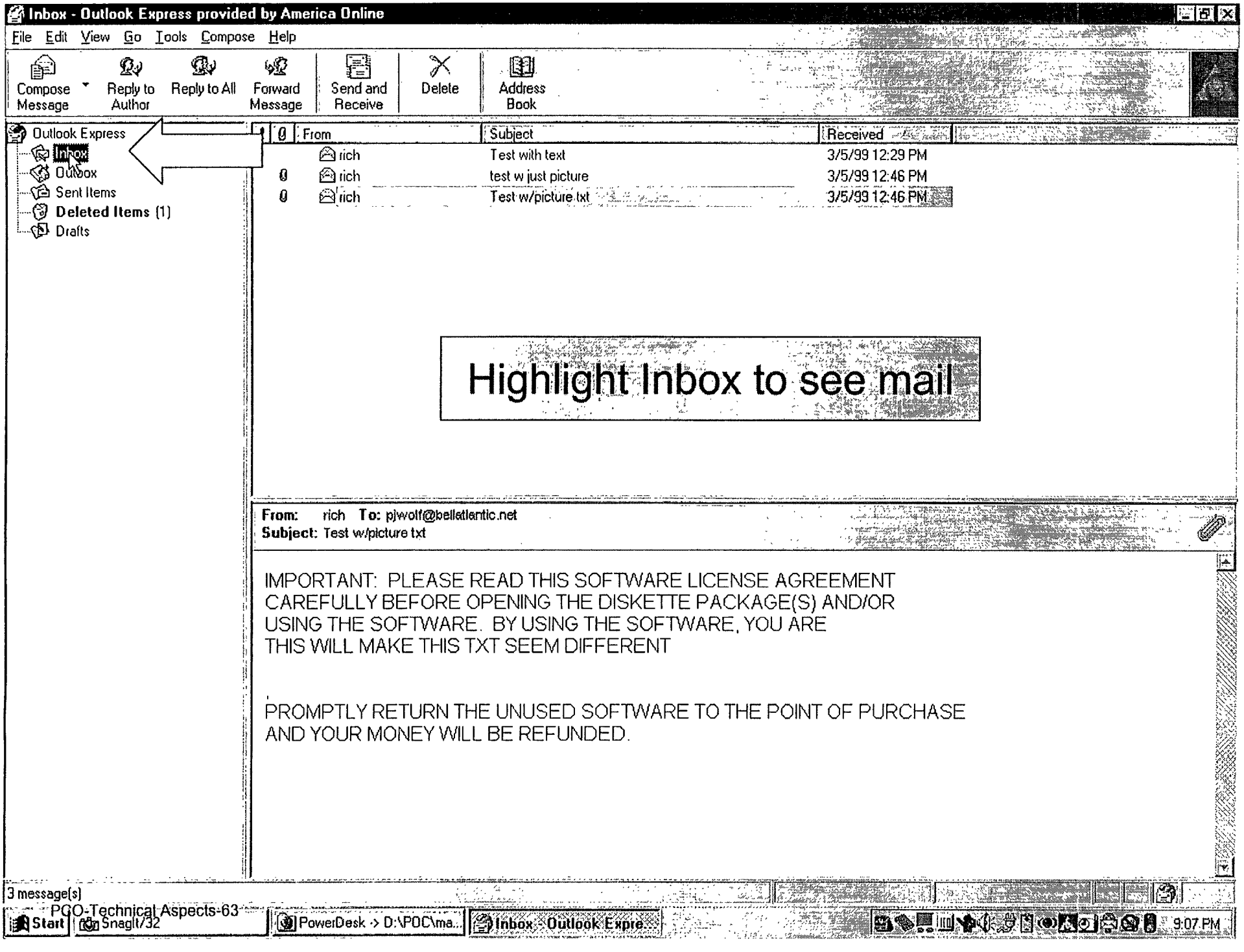
No header information displayed on this "In" box message.

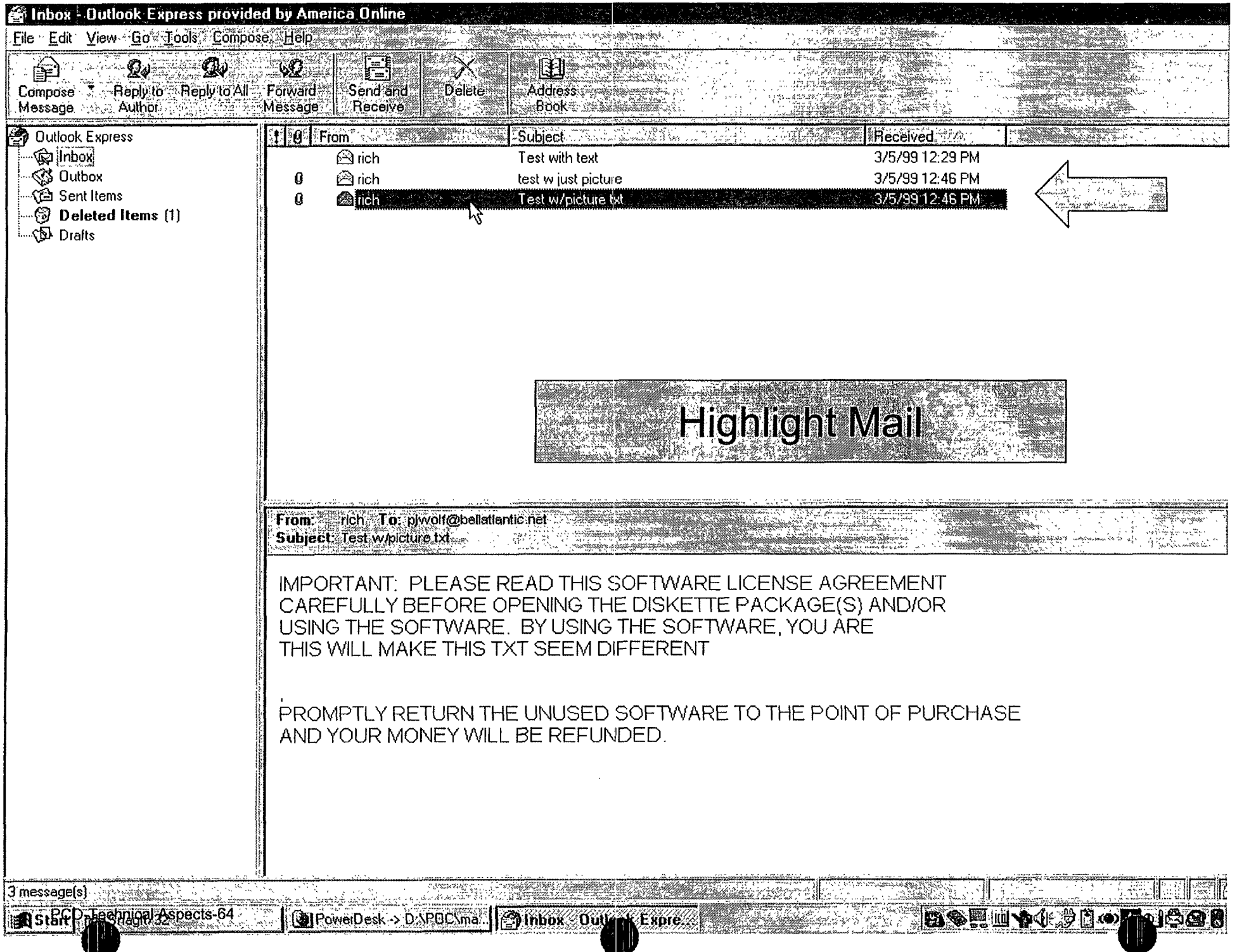

dora Pro - [In]
File Edit Mailbox Message Transfer Special Tools Window Help
Label
Who
Date
Subject
Mike Leiker 07:54 AM 6/8/99 4 Re: Police Computer Crime Scene Policy Development
MDaemon@infot 09:58 AM 6/11/9 2 Unsubscription information
Jim Rush 11:12 AM 6/14/9 2 Computer Crime Files
rich 02:46 PM 6/16/9 2 !!!!!!!!!
Kruse, Warren G 05:47 PM 7/7/99 4 HTCIA
43/1:37K/0K
To: "'pjwolf@bellatlantic.net'" <pjwolf@bellatlantic.net>
Subject: HTCIA
Peter,
We're back!!!!!!!!!
The Northeast Chapter of the High Tech Crime Investigation Association is hosting a half day training on Expert Witness on Monday July 19th.
Location: Secret Service NYC Field Office, Building 7, 10th floor, World Trade Center, NYC
TIME: 1:00 -4:00 PM
Please RSVP by 7-15-99 (Regrets not necessary)
Andy Rosen, of ASR Data (www.asrdata.com) will provide an overview of his product. Andy had provided this for us in the past and it was very well received so we invited him back for an encore presentation. Andy will also provide a FREE COPY of the software for one lucky attendee.
The chapter will also have TWO door prizes for two individuals that we will
Double Click on message title to open up message
Out
Cfid List Member
pjwolf5542@aol.c...
In
QUALCOMM
Task
Status
Progress
PCO-Technical Aspects-59
SnagIt/32
Eudora Pro - [In]
PowerDesk - D:\POC\ma...
8:58 PM

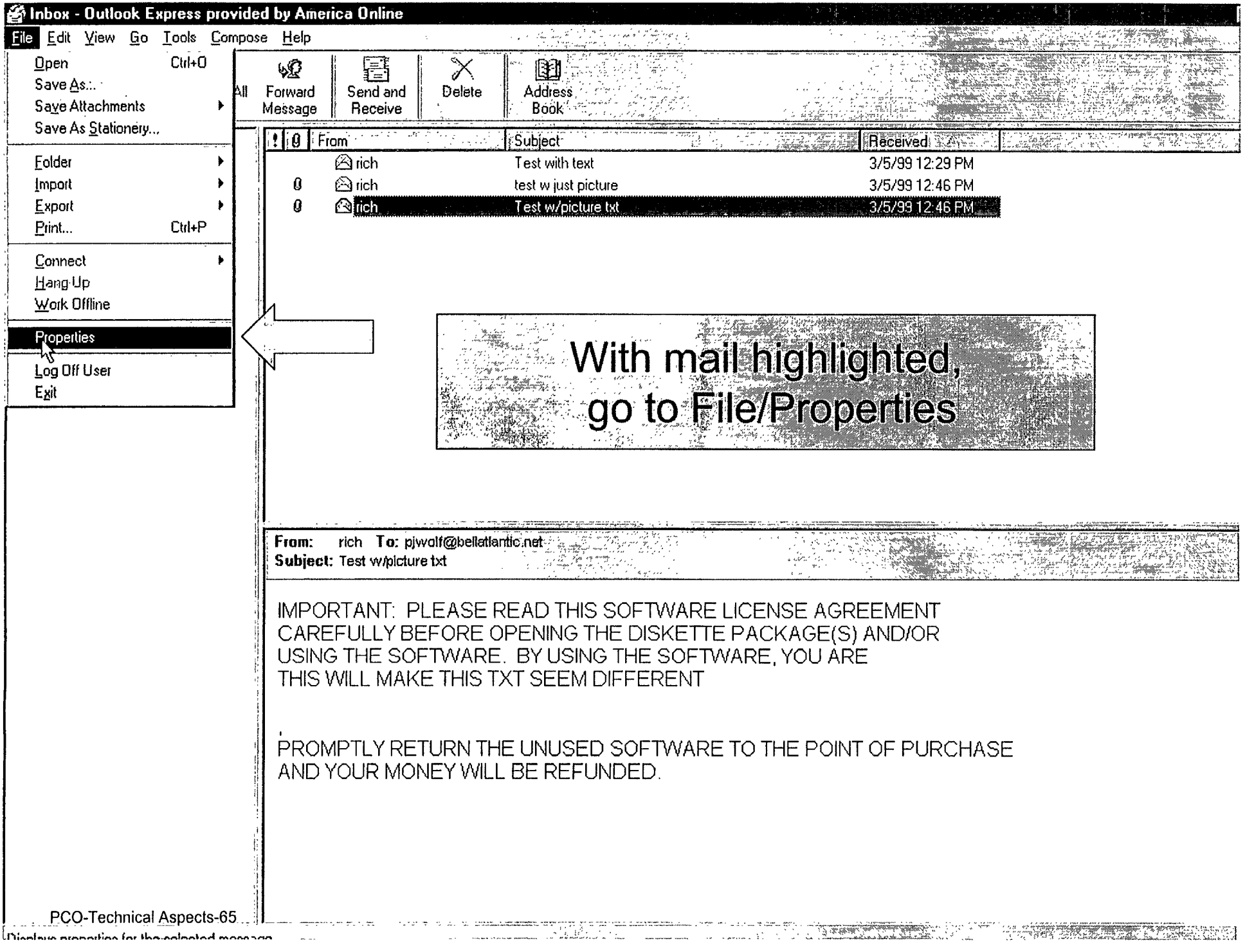

Eudora Pro - [Kruse, Warren G, II (Warren), 05:47 PM 7/7/99 -0400, HTCIA]
File Edit Mailbox Message Transfer Special Tools Window Help
Subject: HTCIA
eudora
In
Out
Trash
bushidopam
Cfid List Member
Peter Daniels
From: "Warren G, II (Warren)" <wgkruse@lucent.com>
To: "'pjw bellatlantic.net'" <pjwolf@bellatlantic.net>
Subject: IA
Date: W Jul 1999 17:47:11 -0400
X-Mailer: net Mail Service (5.5.2448.0)
Peter,
We're back!!!!!!!!!!
The Northeast Chapter of the High Tech Crime Investigation Association is hosting a half day training on Expert Witness on Monday July 19th.
Location: Secret Service NYC Field Office, Building 7, 10th floor, World Trade Center, NYC
TIME: 1:00 -4:00 PM
Please RSVP by 7-15-99 (Regrets not necessary)
Andy Rosen, of ASR Data (www.asrdata.com) will provide an overview of his product. Andy had provided this for us in the past and it was very well received so we invited him back for an encore presentation. Andy will also provide a FREE COPY of the software for one lucky attendee.
The chapter will also have TWO door prizes for two individuals that we will sponsor, for three days of Forensic Training Utilizing Expert Witness. The two individuals WILL HAVE TO BE AVAILABLE for the training, which will be July 20-23. The training will be located in Basking Ridge, NJ. Upon completion of the three days of training, successful participants will be
Message is now fully opened, but still does not reveal full header information. Double click on "Blah, Blah" button to reveal header.
Out
Cfid List Member
pjwolf5542@aol.c...
In
Kruse, Warren G,...
Task
Status
Progress
For Help, press F1
PCO-Technical Aspects-60
Start
Eudora Pro - [Kruse, ...
PowerDesk ->

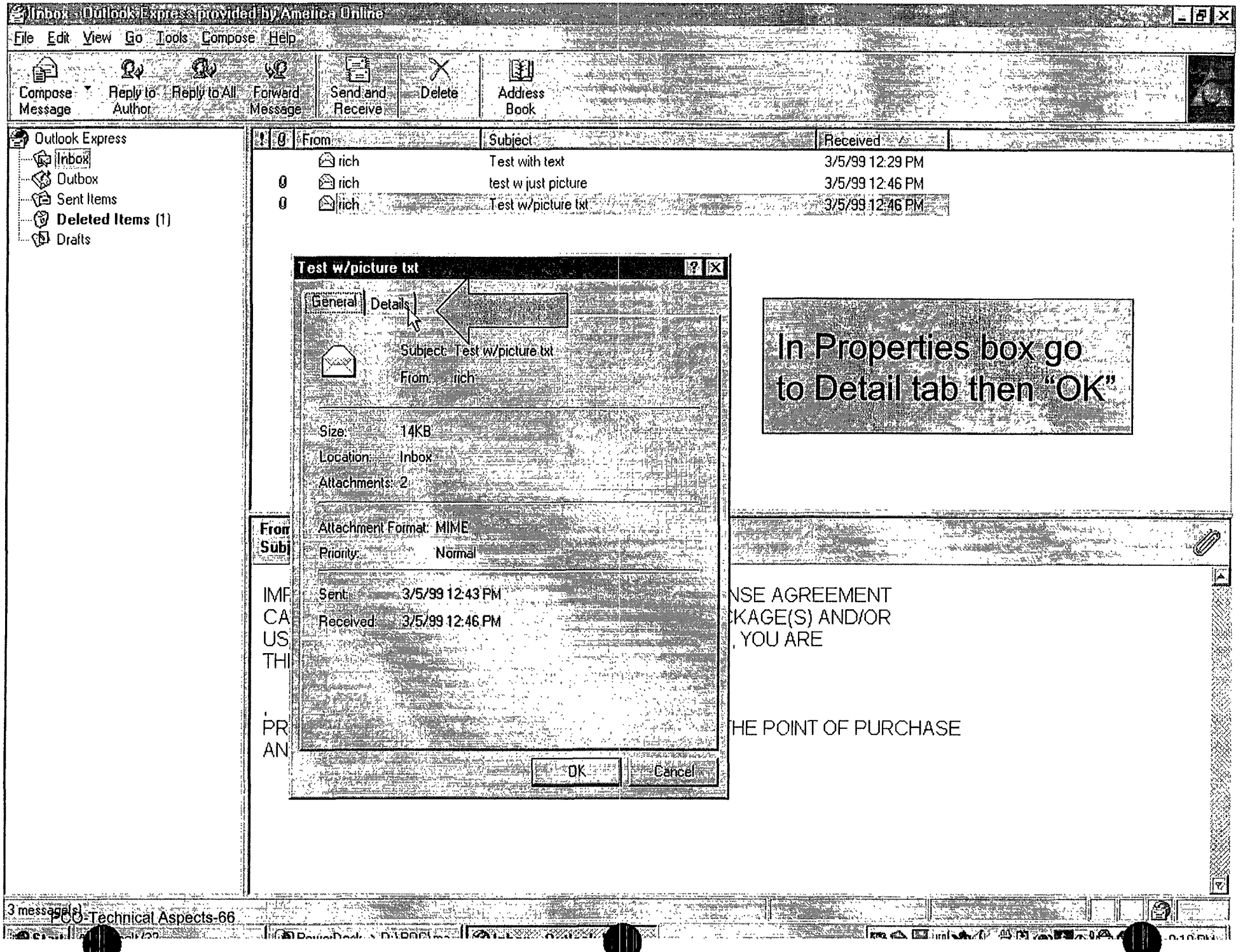

Eudora Pro - [Kruse, Warren G, II (Warren), 05:47 PM 7/7/99 -0400, HTCIA]
File Edit Mailbox Message Transfer Special Tools Window Help
eudora
In
Out
Trash
bushidopam
Cfid List Member
Peter Daniels
Subject: HTCIA
Received: from mail4.bellatlantic.net ([151.197.0.38])
by immta1.bellatlantic.net (InterMail v03.02.07 118 124)
with ESMTP id <19990707215028.CKWB17754@mail4.bellatlantic.net>
for <pjwolf@bellatlantic.net>; Wed, 7 Jul 1999 17:50:28 -0400
Received: from hoemlsrv.firewall.lucent.com (hoemail1.lucent.com [192.11.226.161])
by mail4.bellatlantic.net (8.9.1/8.9.1) with ESMTP id RAA05367
for <pjwolf@bellatlantic.net>; Wed, 7 Jul 1999 17:50:11 -0400 (EDT)
Received: from nj7460exch002h.wins.lucent.com (h135-17-42-35.lucent.com [135.17.42.35])
by hoemlsrv.firewall.lucent.com (Pro-8.9.3/8.9.3) with ESMTP id RAA24042
for <pjwolf@bellatlantic.net>; Wed, 7 Jul 1999 17:47:19 -0400 (EDT)
Received: by nj7460exch002h.ho.lucent.com with Internet Mail Service (5.5.2448.0)
id <MXD2SDXN>; Wed, 7 Jul 1999 17:47:17 -0400
Message-ID: <F38185D061EBD21185F10008C7F926CEE9412D@nj7460exch007u.ho.lucent.com>
From: "Kruse, Warren G, II (Warren)" <wgkruse@lucent.com>
To: "'pjwolf@bellatlantic.net'" <pjwolf@bellatlantic.net>
Subject: HTCIA
Date: Wed, 7 Jul 1999 17:47:11 -0400
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.2448.0)
Content-Type: text/plain
Peter,
We're back!!!!!!!!!
The Northeast Chapter of the High Tech Crime Investigation Association is hosting a half day training on Expert Witness on Monday July 19th.
Location: Secret Service NYC Field Office, Building 7, 10th floor, World Trade Center, NYC
Full header information revealed
Out
Cfid List Member
pjwolf5542@aol.c...
In
Kruse, Warren G,...
QUALCOMM
Task
Status
Progress
For Help, press F1
PCO-Technical.Aspects-61
Start
SnagIt/32
Eudora Pro - [Kruse
PowerDesk - D:\POC\ma...
9:02 PM

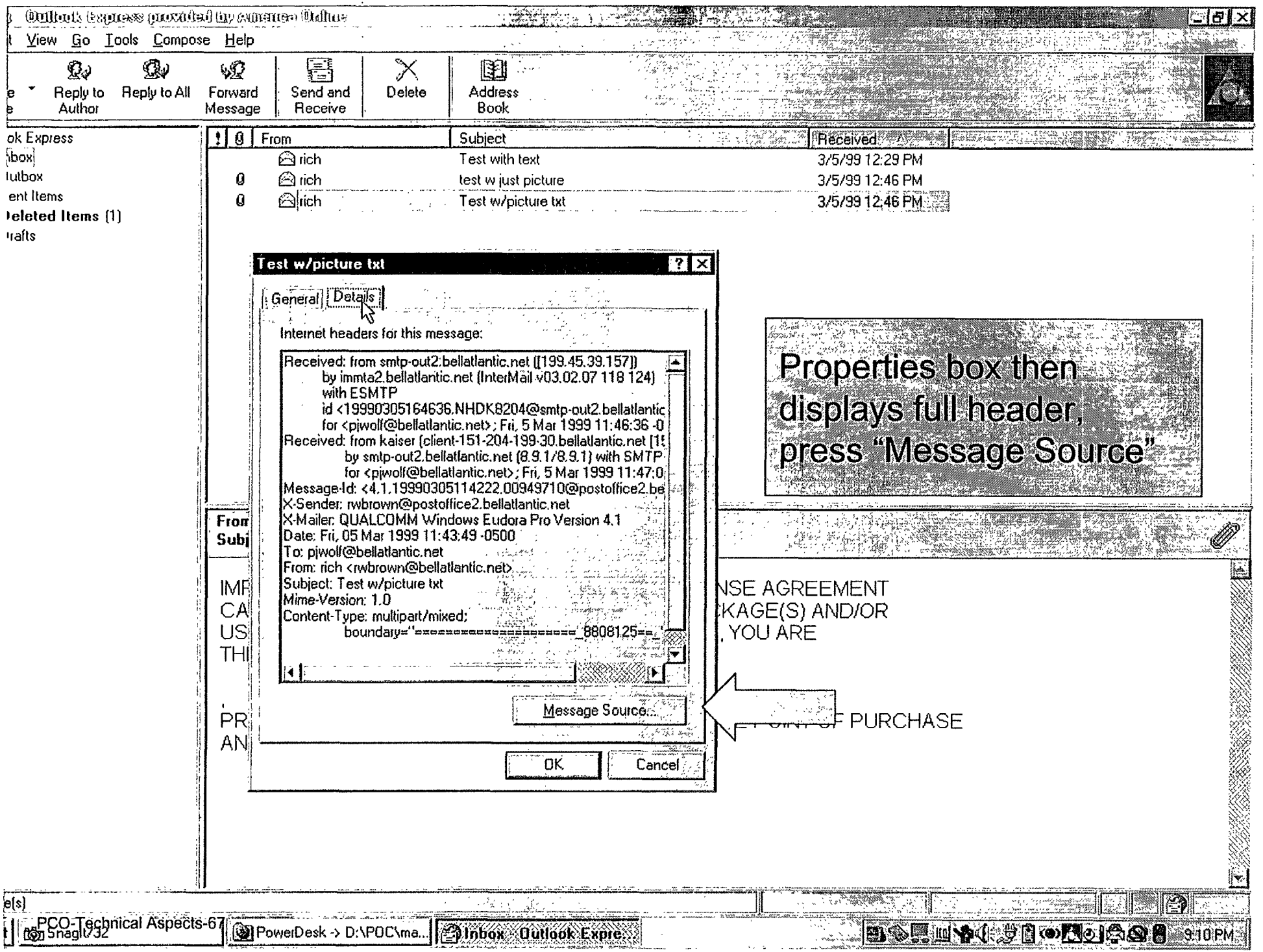

Outlook Express provided by America Online
File Edit View Go Tools Compose Help
Compose Message
Send and Receive
Address Book
Connect
Hang Up
Outlook Express
Inbox
Outbox
Sent Items
Deleted Items (1)
Drafts
Mailboxes
Outlook™ Express
Internet Explorer
Microsoft Corporation
Microsoft Outlook Express
Read Mail
Read News
Compose a Message
Address Book
Download All
Find People
Opening screen in Outlook Express
When starting, go directly to my 'Inbox' folder
When viewing messages in the preview pane, you can press TAB to move between the message list, the preview pane, and the folder or newsgroup list.
PCO-Technical Aspects-62
Start
SnagIt/32
PowerDesk -> D:\POC\ma...
Outlook Express prov...

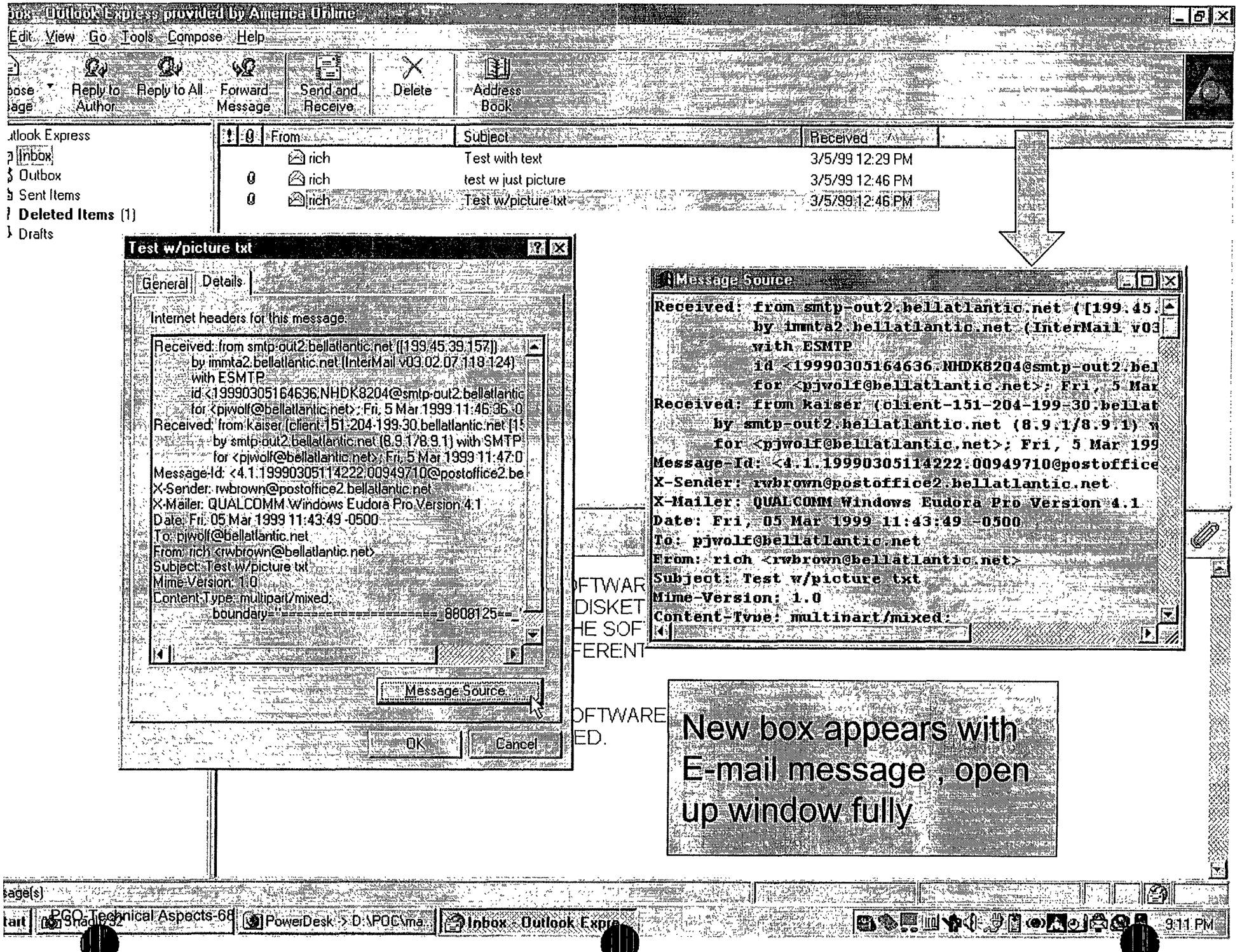

Inbox - Outlook Express provided by America Online
File Edit View Go Tools Compose Help
Compose Message
Reply to Author
Reply to All
Forward Message
Send and Receive
Delete
Address Book
Outlook Express
Inbox
Outbox
Sent Items
Deleted Items (1)
Drafts
From
Subject
Received
rich
Test with text
3/5/99 12:29 PM
rich
test w just picture
3/5/99 12:46 PM
rich
Test w/picture.txt
3/5/99 12:46 PM
Highlight Inbox to see mail
From: rich To: pjwolf@belletlantic.net
Subject: Test w/picture.txt
IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE AGREEMENT
CAREFULLY BEFORE OPENING THE DISKETTE PACKAGE(S) AND/OR
USING THE SOFTWARE. BY USING THE SOFTWARE, YOU ARE
THIS WILL MAKE THIS TXT SEEM DIFFERENT
PROMPTLY RETURN THE UNUSED SOFTWARE TO THE POINT OF PURCHASE
AND YOUR MONEY WILL BE REFUNDED.
3 message(s)
PGO-Technical Aspects-63
Start
SnagIt/32
PowerDesk -> D:\POC\ma...
Inbox - Outlook Expre...
9:07 PM


Inbox - Outlook Express provided by America Online
File Edit View Go Tools Compose Help
Compose Message
Reply to Author
Reply to All
Forward Message
Send and Receive
Delete
Address Book
Outlook Express
Inbox
Outbox
Sent Items
Deleted Items (1)
Drafts
From
Subject
Received
rich
Test with text
3/5/99 12:29 PM
rich
test w just picture
3/5/99 12:46 PM
rich
Test w/picture txt
3/5/99 12:46 PM
Highlight Mail
From: rich To: pjwolf@bellatlantic.net
Subject: Test w/picture txt
IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE AGREEMENT
CAREFULLY BEFORE OPENING THE DISKETTE PACKAGE(S) AND/OR
USING THE SOFTWARE. BY USING THE SOFTWARE, YOU ARE
THIS WILL MAKE THIS TXT SEEM DIFFERENT
PROMPTLY RETURN THE UNUSED SOFTWARE TO THE POINT OF PURCHASE
AND YOUR MONEY WILL BE REFUNDED.
3 message(s)
Start
PCD Technical Aspects-64
PowerDesk -> D:\POC\ma...
Inbox - Outlook Expre...


Inbox - Outlook Express provided by America Online
File Edit View Go Tools Compose Help
Open Ctrl+O
Save As...
Save Attachments
Save As Stationery...
Folder
Import
Export
Print... Ctrl+P
Connect
Hang Up
Work Offline
Properties
Log Off User
Exit
All
Forward Message
Send and Receive
Delete
Address Book
From
Subject
Received
rich
Test with text
3/5/99 12:29 PM
rich
test w just picture
3/5/99 12:46 PM
rich
Test w/picture txt
3/5/99 12:46 PM
With mail highlighted, go to File/Properties
From: rich To: pjwolf@bellatlantic.net
Subject: Test w/picture txt
IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE DISKETTE PACKAGE(S) AND/OR USING THE SOFTWARE. BY USING THE SOFTWARE, YOU ARE
THIS WILL MAKE THIS TXT SEEM DIFFERENT
PROMPTLY RETURN THE UNUSED SOFTWARE TO THE POINT OF PURCHASE AND YOUR MONEY WILL BE REFUNDED.


Inbox - Outlook Express provided by America Online
File Edit View Go Tools Compose Help
Compose Message
Reply to Author
Reply to All
Forward Message
Send and Receive
Delete
Address Book
Outlook Express
Inbox
Outbox
Sent Items
Deleted Items (1)
Drafts
From
Subject
Received
rich
Test with text
3/5/99 12:29 PM
rich
test w just picture
3/5/99 12:46 PM
rich
Test w/picture txt
3/5/99 12:46 PM
Test w/picture txt
General
Details
Subject: Test w/picture txt
From: rich
Size: 14KB
Location: Inbox
Attachments: 2
Attachment Format: MIME
Priority: Normal
Sent: 3/5/99 12:43 PM
Received: 3/5/99 12:46 PM
OK
Cancel
In Properties box go to Detail tab then "OK"
3 message(s)


View Go Tools Compose Help
Reply to Author
Reply to All
Forward Message
Send and Receive
Delete
Address Book
From
Subject
Received
rich Test with text 3/5/99 12:29 PM
rich test w just picture 3/5/99 12:46 PM
rich Test w/picture txt 3/5/99 12:46 PM
Test w/picture txt
General
Details
Internet headers for this message:
Received: from smtp-out2.bellatlantic.net ([199.45.39.157])
by immta2.bellatlantic.net (InterMail v03.02.07 118 124)
with ESMTP
id <19990305164636.NHDK8204@smtp-out2.bellatlantic
for <pjwolf@bellatlantic.net>; Fri, 5 Mar 1999 11:46:36 -0
Received: from kaiser (client-151-204-199-30.bellatlantic.net [1
by smtp-out2.bellatlantic.net (8.9.1/8.9.1) with SMTP
for <pjwolf@bellatlantic.net>; Fri, 5 Mar 1999 11:47:0
Message-Id: <4.1.19990305114222.00949710@postoffice2.be
X-Sender: rwbrown@postoffice2.bellatlantic.net
X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1
Date: Fri, 05 Mar 1999 11:43:49 -0500
To: pjwolf@bellatlantic.net
From: rich <rwbrown@bellatlantic.net>
Subject: Test w/picture txt
Mime-Version: 1.0
Content-Type: multipart/mixed;
boundary="_8808125=_
Message Source...
OK
Cancel
Properties box then displays full header, press "Message Source"
NSE AGREEMENT
KAGE(S) AND/OR
, YOU ARE
PURCHASE
PCO-Technical Aspects-67
PowerDesk -> D:\POC\ma...
Inbox - Outlook Expre...
9:10 PM

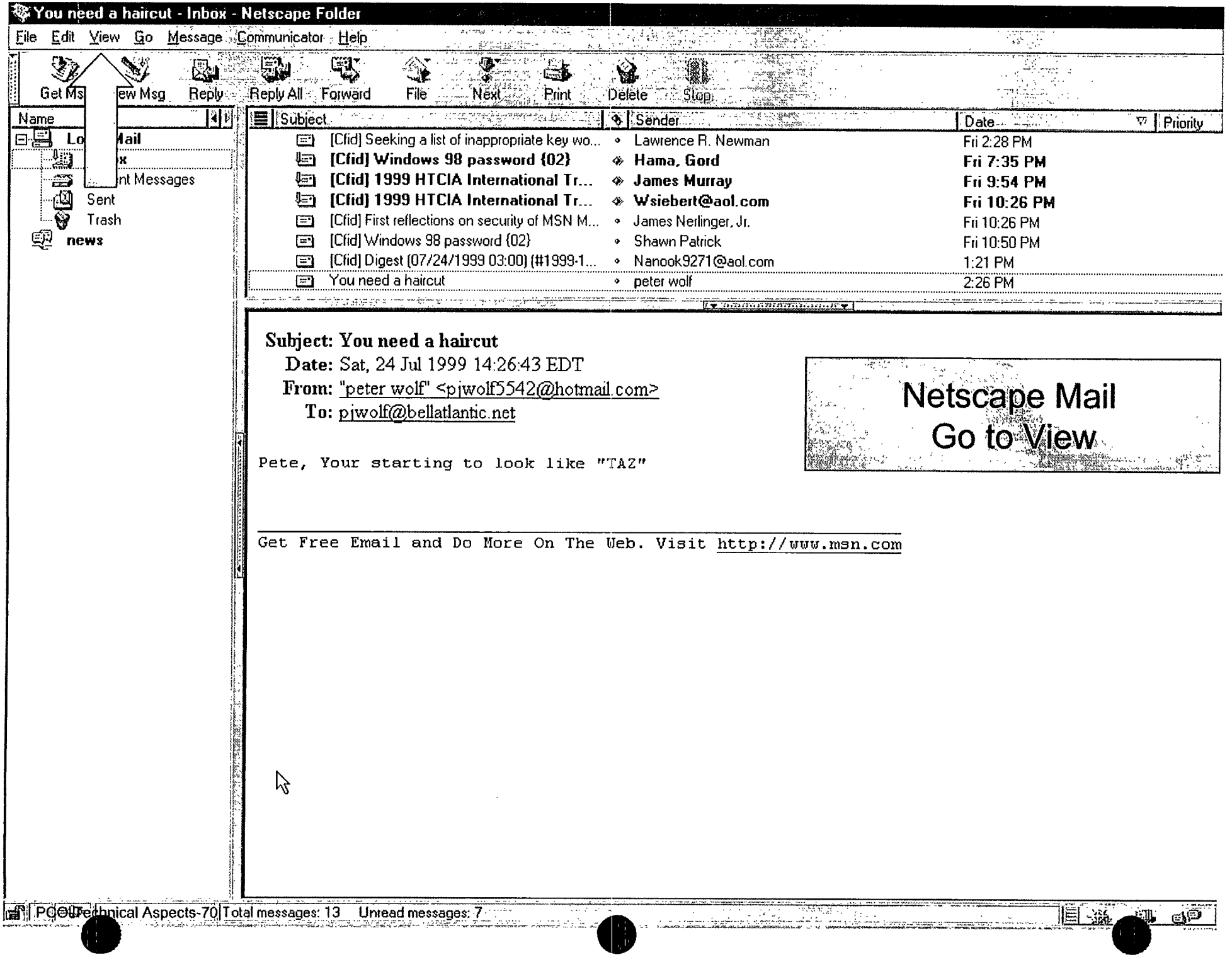

Edit View Go Tools Compose Help
Reply to Author
Reply to All
Forward Message
Send and Receive
Delete
Address Book
Outlook Express
Inbox
Outbox
Sent Items
Deleted Items (1)
Drafts
From
Subject
Received
rich
Test with text
3/5/99 12:29 PM
rich
test w just picture
3/5/99 12:46 PM
rich
Test w/picture txt
3/5/99 12:46 PM
Test w/picture txt
General
Details
Internet headers for this message:
Received: from smtp-out2.bellatlantic.net ([199.45.39.157])
by immta2.bellatlantic.net (InterMail v03.02.07.118-124)
with ESMTP
id <19990305164636.NHDK8204@smtp-out2.bellatlantic
for <pjwolf@bellatlantic.net>; Fri, 5 Mar 1999 11:46:36 -0
Received: from kaiser (client-151-204-199-30.bellatlantic.net [15
by smtp-out2.bellatlantic.net (8.9.1/8.9.1) with SMTP
for <pjwolf@bellatlantic.net>; Fri, 5 Mar 1999 11:47:0
Message-Id: <4.1.19990305114222.00949710@postoffice2.be
X-Sender: rwbrown@postoffice2.bellatlantic.net
X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1
Date: Fri, 05 Mar 1999 11:43:49 -0500
To: pjwolf@bellatlantic.net
From: rich <rwbrown@bellatlantic.net>
Subject: Test w/picture txt
Mime-Version: 1.0
Content-Type: multipart/mixed;
boundary="----------_8808125=_
Message Source...
OK
Cancel
Message Source
Received: from smtp-out2.bellatlantic.net ([199.45.
by immta2.bellatlantic.net (InterMail v03
with ESMTP
id <19990305164636.NHDK8204@smtp-out2.bel
for <pjwolf@bellatlantic.net>; Fri, 5 Mar
Received: from kaiser (client-151-204-199-30.bellat
by smtp-out2.bellatlantic.net (8.9.1/8.9.1)
for <pjwolf@bellatlantic.net>; Fri, 5 Mar 199
Message-Id: <4.1.19990305114222.00949710@postoffice
X-Sender: rwbrown@postoffice2.bellatlantic.net
X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1
Date: Fri, 05 Mar 1999 11:43:49 -0500
To: pjwolf@bellatlantic.net
From: rich <rwbrown@bellatlantic.net>
Subject: Test w/picture txt
Mime-Version: 1.0
Content-Type: multipart/mixed;
New box appears with E-mail message , open up window fully
PCO Technical Aspects-68
PowerDesk - D:\POC\ma...
Inbox - Outlook Expre...
9:11 PM

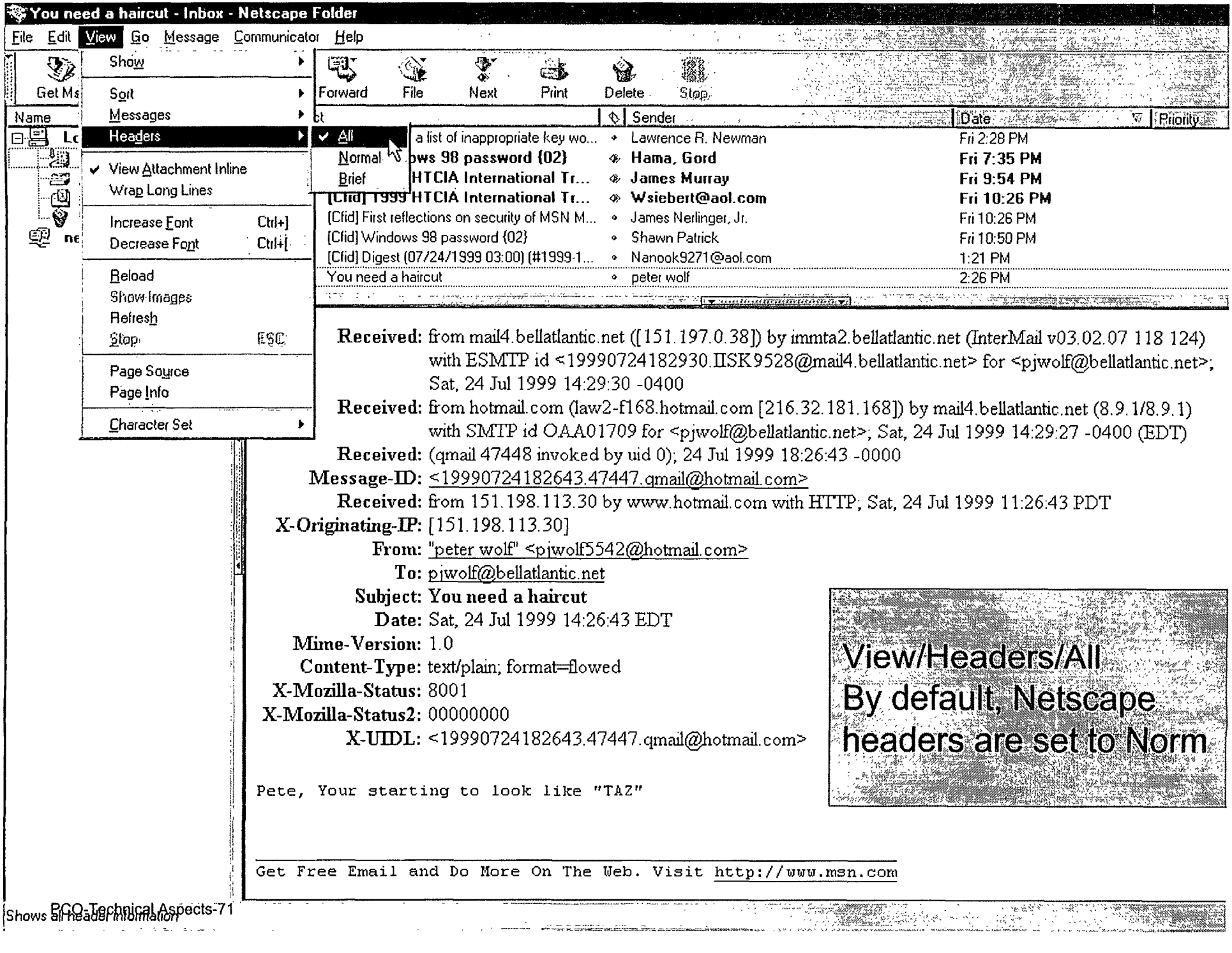
Message Source

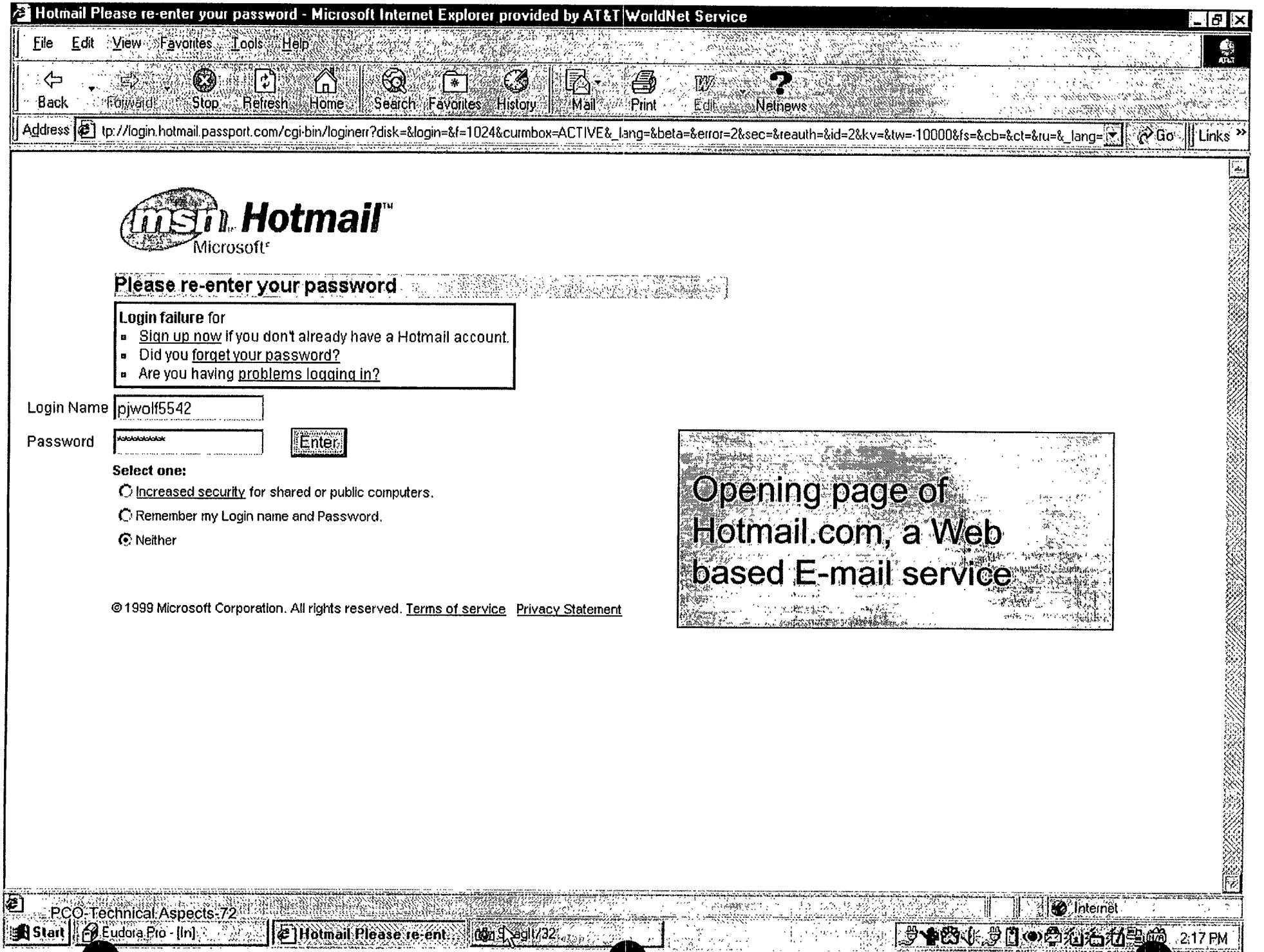
```
eived: from smtp-out2.bellatlantic.net ([199.45.39.157])
       by immta2.bellatlantic.net (InterMail v03.02.07 118 124)
       with ESMTP
       id <19990305164636.NHDK8204@smtp-out2.bellatlantic.net>
       for <pjwolf@bellatlantic.net>; Fri, 5 Mar 1999 11:46:36 -0500
eived: from kaiser (client-151-204-199-30.bellatlantic.net [151.204.199.30])
    by smtp-out2.bellatlantic.net (8.9.1/8.9.1) with SMTP id LAA23031
    for <pjwolf@bellatlantic.net>; Fri, 5 Mar 1999 11:47:02 -0500 (EST)
sage-Id: <4.1.19990305114222.00949710@postoffice2.bellatlantic.net>
ender: rwbrown@postoffice2.bellatlantic.net
ailer: QUALCOMM Windows Eudora Pro Version 4.1
e: Fri, 05 Mar 1999 11:43:49 -0500
 pjwolf@bellatlantic.net
m: rich <rwbrown@bellatlantic.net>
ject: Test w/picture txt
e-Version: 1.0
tent-Type: multipart/mixed;
    boundary="====================_8808125==_"

====================_8808125==_
tent-Type: text/plain; charset="us-ascii"

ORTANT:  PLEASE READ THIS SOFTWARE LICENSE AGREEMENT
EFULLY BEFORE OPENING THE DISKETTE PACKAGE(S) AND/OR
NG THE SOFTWARE.  BY USING THE SOFTWARE, YOU ARE
S WILL MAKE THIS TXT SEEM DIFFERENT


MPTLY RETURN THE UNUSED SOFTWARE TO THE POINT OF PURCHASE
 YOUR MONEY WILL BE REFUNDED.

====================_8808125==_
tent-Type: application/octet-stream; name="bitsy"
tent-Transfer-Encoding: base64
tent-Disposition: attachment; filename="bitsy"
```

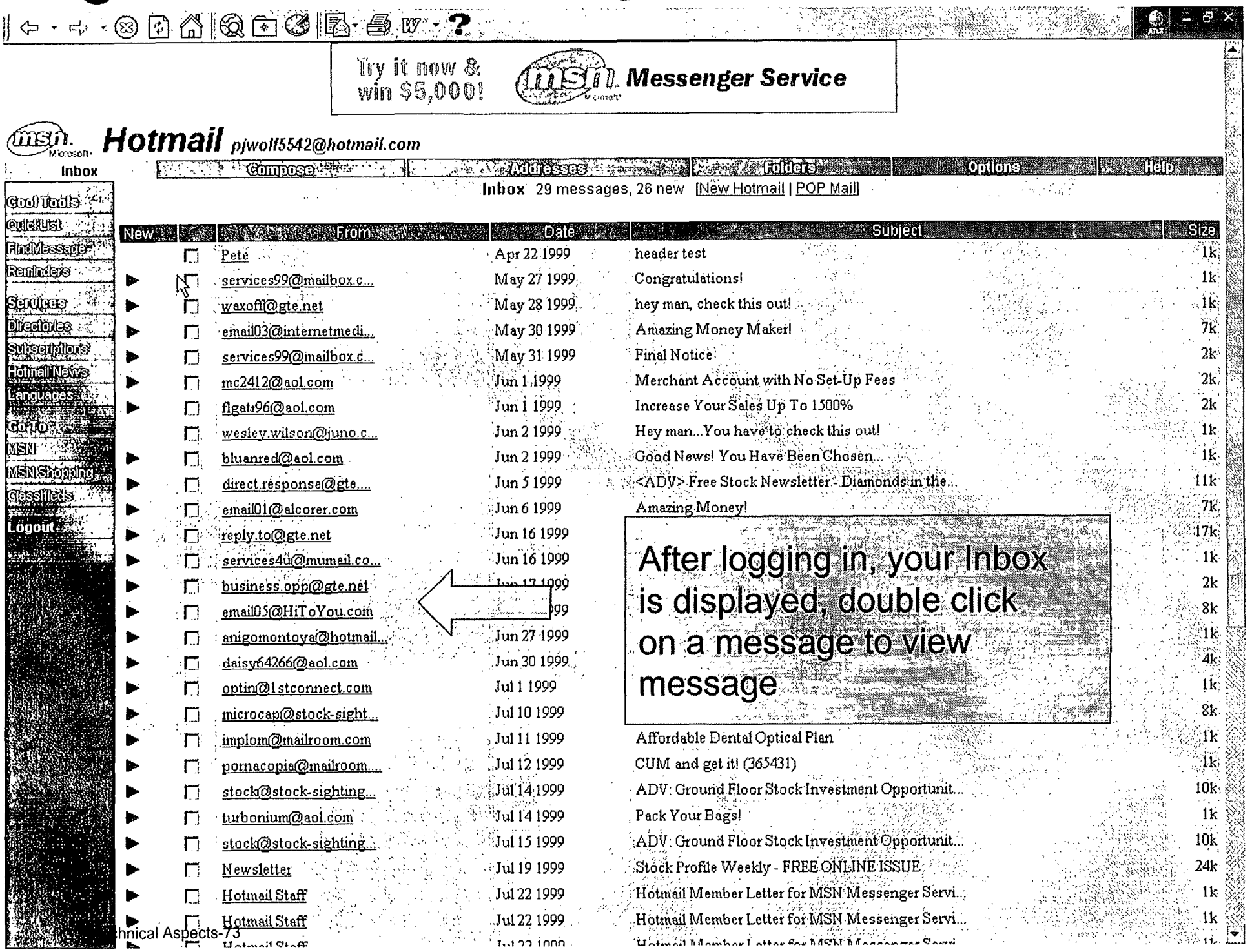

/4AAQSkZJRgABAQEASABIAAD/2wBDAAUDBAQEAwUEBAQFBQUGBwwIBwcHBw8LCwkMEQ8SEhEP
TFhwXExQaFRERGCEYGhOdHx8fExciJCIeJBweHx7/2wBDAQUFBQcGBw4ICA4eFBEUHh4eHh4e
eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh4eHh7/wAARCAEWASMDASIA
BAxEB/8QAHAAAAgIDAQEAAAAAAAAAAAAAABAUDBgABAgcI/8QAMBAAAQQCAQMDAwQCAgMBAAAA
CAxEEBSEGEjETIkFRYXEHFCMyFYEkkTNCUjT/xAAaAQACAwEBAAAAAAAAAAAAAACAwABBAUG
AJREAAgICAwEAAgMAAwAAAAAAAAAECEQMhBBIxQRMiFDJRBWFx/9oADAMBAAIRAxEAPwC2McAF
1jDaEyJ2xtJtINrt2sa73jhIkzqRNb/bxxE24Kj7fqaNpLQ4JN1hupHSuax6pmRPLM4kkobDL
StMn9k+weomFosryjEEgk81M45pY/BKFyV1O2eoxdQRh/9wmuNv4yy+8Lxd+dM13d3FD5PUk8
G81wuLb8K1UfT?zL6sxMVhe+WrH3VD6u/U?eSN8GJfh4rUiFdk78nqZeQWs+bKn?z9PRbOiVO

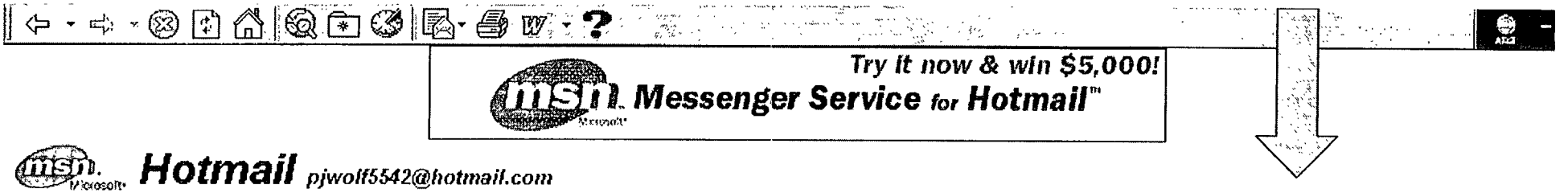
Start | Snagit/32 | RCO-Technical Aspects-69 | PowerDesk -> D:\POC\ma... | Inbox - Outlook Expre... | 9:11 PM


You need a haircut - Inbox - Netscape Folder
File Edit View Go Message Communicator Help
Get Ms
ew Msg
Reply
Reply All
Forward
File
Next
Print
Delete
Stop
Name
Lo
Mail
x
nt Messages
Sent
Trash
news
Subject
Sender
Date
Priority
[Cfid] Seeking a list of inappropriate key wo... Lawrence R. Newman Fri 2:28 PM
[Cfid] Windows 98 password {02} Hama, Gord Fri 7:35 PM
[Cfid] 1999 HTCIA International Tr... James Murray Fri 9:54 PM
[Cfid] 1999 HTCIA International Tr... Wsiebert@aol.com Fri 10:26 PM
[Cfid] First reflections on security of MSN M... James Nerlinger, Jr. Fri 10:26 PM
[Cfid] Windows 98 password {02} Shawn Patrick Fri 10:50 PM
[Cfid] Digest (07/24/1999 03:00) (#1999-1... Nanook9271@aol.com 1:21 PM
You need a haircut peter wolf 2:26 PM
Subject: You need a haircut
Date: Sat, 24 Jul 1999 14:26:43 EDT
From: "peter wolf" <pjwolf5542@hotmail.com>
To: pjwolf@bellatlantic.net
Pete, Your starting to look like "TAZ"
Get Free Email and Do More On The Web. Visit http://www.msn.com
Netscape Mail
Go to View
PCOU Technical Aspects-70 Total messages: 13 Unread messages: 7


You need a haircut - Inbox - Netscape Folder
File Edit View Go Message Communicator Help
Show
Sort
Messages
Headers
All
Normal
Brief
View Attachment Inline
Wrap Long Lines
Increase Font Ctrl+]
Decrease Font Ctrl+[
Reload
Show Images
Refresh
Stop ESC
Page Source
Page Info
Character Set
Get Ms
Forward
File
Next
Print
Delete
Stop
Name
Sender
Date
Priority
a list of inappropriate key wo... Lawrence R. Newman Fri 2:28 PM
ows 98 password {02} Hama, Gord Fri 7:35 PM
HTCIA International Tr... James Murray Fri 9:54 PM
[Cfid] 1999 HTCIA International Tr... Wsiebert@aol.com Fri 10:26 PM
[Cfid] First reflections on security of MSN M... James Nerlinger, Jr. Fri 10:26 PM
[Cfid] Windows 98 password {02} Shawn Patrick Fri 10:50 PM
[Cfid] Digest (07/24/1999 03:00) (#1999-1... Nanook9271@aol.com 1:21 PM
You need a haircut peter wolf 2:26 PM
Received: from mail4.bellatlantic.net ([151.197.0.38]) by immta2.bellatlantic.net (InterMail v03.02.07 118 124) with ESMTP id <19990724182930.IISK9528@mail4.bellatlantic.net> for <pjwolf@bellatlantic.net>; Sat, 24 Jul 1999 14:29:30 -0400
Received: from hotmail.com (law2-f168.hotmail.com [216.32.181.168]) by mail4.bellatlantic.net (8.9.1/8.9.1) with SMTP id OAA01709 for <pjwolf@bellatlantic.net>; Sat, 24 Jul 1999 14:29:27 -0400 (EDT)
Received: (qmail 47448 invoked by uid 0); 24 Jul 1999 18:26:43 -0000
Message-ID: <19990724182643.47447.qmail@hotmail.com>
Received: from 151.198.113.30 by www.hotmail.com with HTTP; Sat, 24 Jul 1999 11:26:43 PDT
X-Originating-IP: [151.198.113.30]
From: "peter wolf" <pjwolf5542@hotmail.com>
To: pjwolf@bellatlantic.net
Subject: You need a haircut
Date: Sat, 24 Jul 1999 14:26:43 EDT
Mime-Version: 1.0
Content-Type: text/plain; format=flowed
X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000
X-UIDL: <19990724182643.47447.qmail@hotmail.com>
Pete, Your starting to look like "TAZ"
Get Free Email and Do More On The Web. Visit http://www.msn.com
View/Headers/All
By default, Netscape
headers are set to Norm
Shows all header information


Hotmail Please re-enter your password - Microsoft Internet Explorer provided by AT&T WorldNet Service
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Netnews
Address tp://login.hotmail.passport.com/cgi-bin/loginerr?disk=&login=&f=1024&curmbox=ACTIVE&_lang=&beta=&error=2&sec=&reauth=&id=2&kv=&tw=-10000&fs=&cb=&ct=&ru=&_lang=
Go
Links
msn Hotmail™
Microsoft
Please re-enter your password
Login failure for
Sign up now if you don't already have a Hotmail account.
Did you forget your password?
Are you having problems logging in?
Login Name pjwolf5542
Password
Enter
Select one:
Increased security for shared or public computers.
Remember my Login name and Password.
Neither
©1999 Microsoft Corporation. All rights reserved. Terms of service Privacy Statement
Opening page of Hotmail.com, a Web based E-mail service
PCO-Technical Aspects-72
Internet
Start
Eudora Pro - [In]
Hotmail Please re-ent...
2:17 PM


Try it now & win $5,000!
msn Messenger Service
msn Hotmail pjwolf5542@hotmail.com
Inbox
Compose
Addresses
Folders
Options
Help
Cool Tools
QuickList
FindMessage
Reminders
Services
Directories
Subscriptions
Hotmail News
Languages
Go To
MSN
MSN Shopping
Classifieds
Logout
Inbox 29 messages, 26 new [New Hotmail | POP Mail]
New
From
Date
Subject
Size
Pete Apr 22 1999 header test 1k
services99@mailbox.c... May 27 1999 Congratulations! 1k
waxoff@gte.net May 28 1999 hey man, check this out! 1k
email03@internetmedi... May 30 1999 Amazing Money Maker! 7k
services99@mailbox.c... May 31 1999 Final Notice 2k
mc2412@aol.com Jun 1 1999 Merchant Account with No Set-Up Fees 2k
figats96@aol.com Jun 1 1999 Increase Your Sales Up To 1500% 2k
wesley.wilson@juno.c... Jun 2 1999 Hey man...You have to check this out! 1k
bluanred@aol.com Jun 2 1999 Good News! You Have Been Chosen... 1k
direct.response@gte.... Jun 5 1999 <ADV> Free Stock Newsletter - Diamonds in the... 11k
email01@alcorer.com Jun 6 1999 Amazing Money! 7k
reply.to@gte.net Jun 16 1999 17k
services4u@mumail.co... Jun 16 1999 1k
business.opp@gte.net 2k
email05@HiToYou.com 8k
anigomontoya@hotmail... Jun 27 1999 1k
daisy64266@aol.com Jun 30 1999 4k
optin@1stconnect.com Jul 1 1999 1k
microcap@stock-sight... Jul 10 1999 8k
implom@mailroom.com Jul 11 1999 Affordable Dental Optical Plan 1k
pornacopia@mailroom.... Jul 12 1999 CUM and get it! (365431) 1k
stock@stock-sighting... Jul 14 1999 ADV: Ground Floor Stock Investment Opportunit... 10k
turbonium@aol.com Jul 14 1999 Pack Your Bags! 1k
stock@stock-sighting... Jul 15 1999 ADV: Ground Floor Stock Investment Opportunit... 10k
Newsletter Jul 19 1999 Stock Profile Weekly - FREE ONLINE ISSUE 24k
Hotmail Staff Jul 22 1999 Hotmail Member Letter for MSN Messenger Servi... 1k
Hotmail Staff Jul 22 1999 Hotmail Member Letter for MSN Messenger Servi... 1k
After logging in, your Inbox is displayed, double click on a message to view message



Folder: **Inbox**

Reply | Reply All | Forward | Delete | Previous | Next | Close

Rich , check out these sites.....

Move To (Move to Selected Folder)

Inbox | Compose | Addresses | Folders | Options | Help

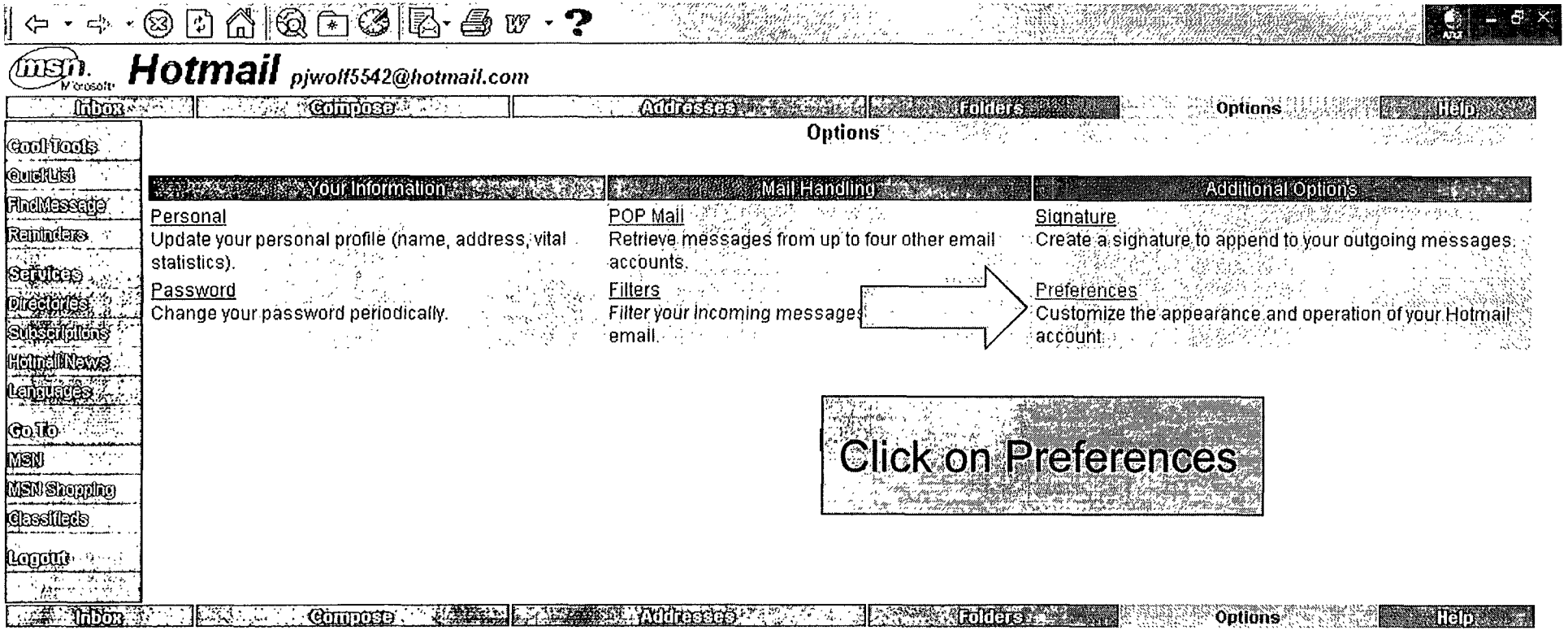
Get notified when you have new Hotmail or when your friends are on-line. Send instant messages. Click here to get your **FREE download of MSN Messenger Service!**

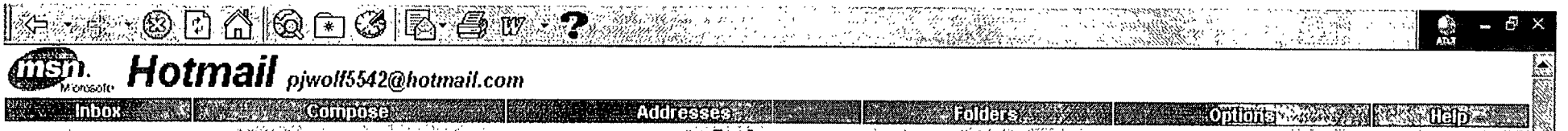
Air Tickets | Buy Music | Downloads | Entertainment | Free Games | Yellow Pages
Headlines | Sporting Goods | Buy Videos | Weather | Buy books | More cool stuff...

Search the web: Search

©1999 Microsoft Corporation. All rights reserved. Terms of service Privacy Statement

Message is displayed with no header info, click on "Options"


Hotmail pjwolf5542@hotmail.com
Inbox
Compose
Addresses
Folders
Options
Help
Cool Tools
QuickList
FindMessage
Reminders
Services
Directories
Subscriptions
Hotmail News
Languages
Go To
MSN
MSN Shopping
Classifieds
Logout
Options
Your Information
Mail Handling
Additional Options
Personal
Update your personal profile (name, address, vital statistics).
Password
Change your password periodically.
POP Mail
Retrieve messages from up to four other email accounts.
Filters
Filter your incoming messages email.
Signature
Create a signature to append to your outgoing messages.
Preferences
Customize the appearance and operation of your Hotmail account
Click on Preferences
Get notified when you have new Hotmail or when your friends are on-line. Send instant messages. Click here to get your FREE download of MSN Messenger Service!
Air Tickets | Buy Music | Downloads | Entertainment | Free Games | Yellow Pages
Headlines | Sporting Goods | Buy Videos | Weather | Buy books | More cool stuff...
Search the web:
Search
© 1999 Microsoft Corporation. All rights reserved. Terms of service Privacy Statement



Preferences

OK Cancel

Click on Message Headers/Advanced then click "OK"

Hotmail Display Options

You can customize the appearance and operation of Hotmail for your personal preferences.

Messages per Page

- ○ 10
- ○ 20
- ○ 50
- ◉ 100

Select the number of messages that are displayed on
Inbox and other folders. This affects the pages' loading times as well as the amount of memory that your browser requires to load a page.
Tip: For the fastest Inbox loading time, set this option to 10.

Line Width

- ○ 64
- ○ 72
- ◉ 80
- ○ 96
- ○ 132

Select the width (in characters) of each line of your messages. Smaller widths are better for smaller screens, including laptops

Other Hotmail Options

AutoJump (Folders)

- ◉ Off
- ○ On

AutoJump affects how the **Move To** menu operates.
If you select Off, you click the **Move To** button to confirm your folder selection.
If you select On, the move is automatically performed as soon as a folder name is selected from the **Move To** menu. This option only works if your browser supports JavaScript™.

Message Headers

- ○ None
- ○ Basic
- ○ Full
- ◉ Advanced

The None option does not display any header information.
Basic displays the sender's and recipients' names, the date, and the subject.
Full also displays routing information that is useful for tracing messages.
Advanced displays complete MIME headers for power users.

Replying To Messages

- ○ Separator
- ◉ ">"
- ○ None

If you choose to quote original text when replying to a message, you can select the type of indicator that you want to appear.
The Separator option marks the beginning of quoted text with a full line of bars ("====").
The ">" option adds the greater than (>) symbol to each line of quoted text.
The None o[illegible] does not mark the quoted text

Protect Your Privacy!
Look For The TRUSTe Seal
Click Here To Learn More

msn Hotmail pjwolf5542@hotmail.com

Inbox | Compose | Addresses | Folders

Folder: **Inbox**

Full header information is now displayed. Copy/Paste into a text document

From: PJ Wolf <pjwolf@bellatlantic.net> Save Address Block Sender

To: pjwolf5542@hotmail.com

Subject: porn sites

Date: Sat, 24 Jul 1999 14:07:34 -0400

MIME-Version: 1.0

From pjwolf@bellatlantic.net Sat Jul 24 11:07:40 1999

Received: from [199.45.39.157] by hotmail.com (2.1) with ESMTP id MHotMailB9634BEC009FD820F39DC72D279DBF550; Sat Jul 24 11:07:40 1999

Received: from bellatlantic.net (client-113-40.bellatlantic.net [151.198.113.40])by smtp-out2.bellatlantic.net (8.9.1/8.9.1) with ESMTP id OAA02746for <pjwolf5542@hotmail.com>; Sat, 24 Jul 1999 14:11:40 -0400 (EDT)

Message-ID: <379A00E6.76B40C77@bellatlantic.net>

X-Mailer: Mozilla 4.61 [en] (Win95; I)

X-Accept-Language: en

View Email Message Source

Reply | Reply All | Forward | Delete | Previous | Next | Close

```
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

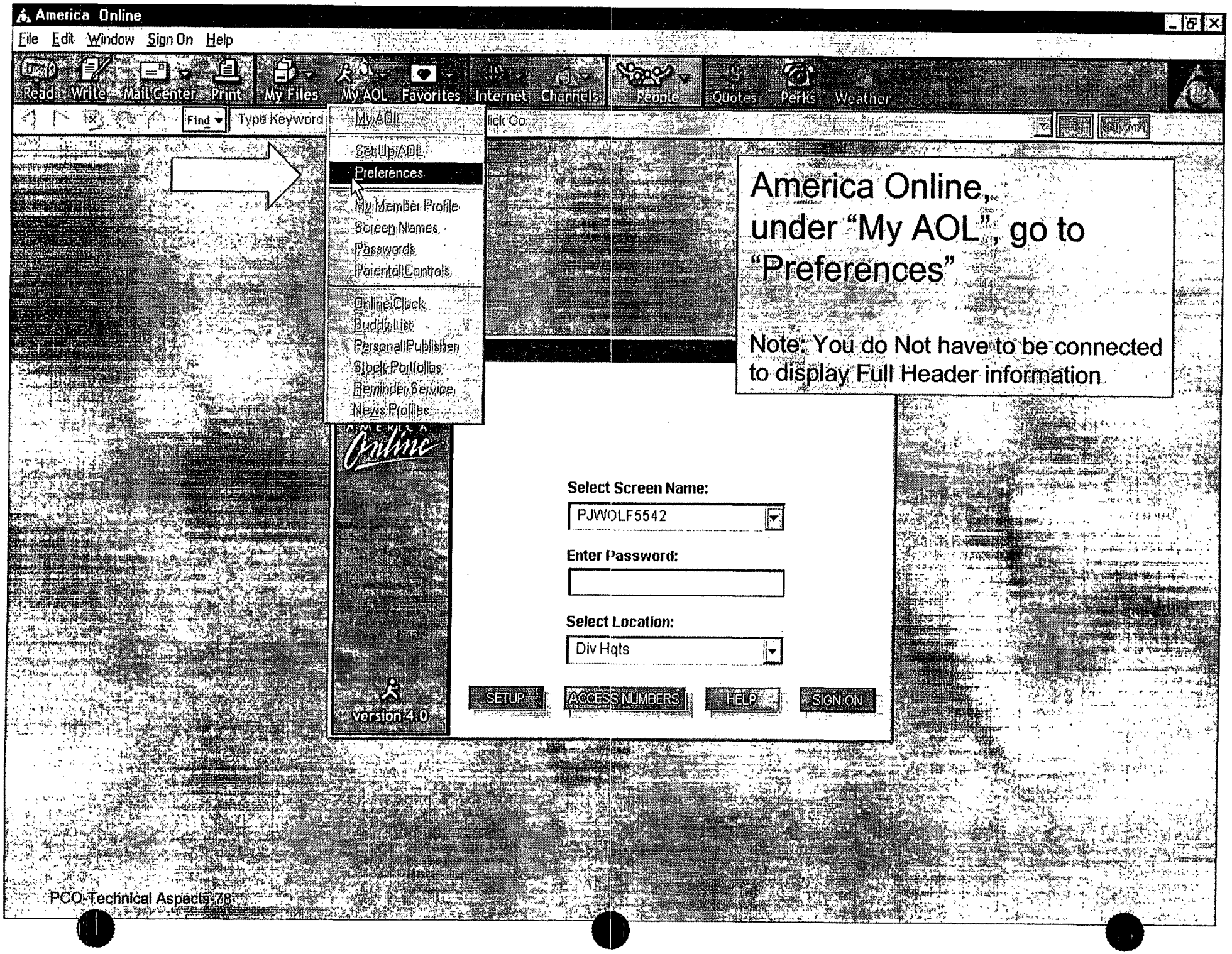
```
Rich , check out these sites.........
```

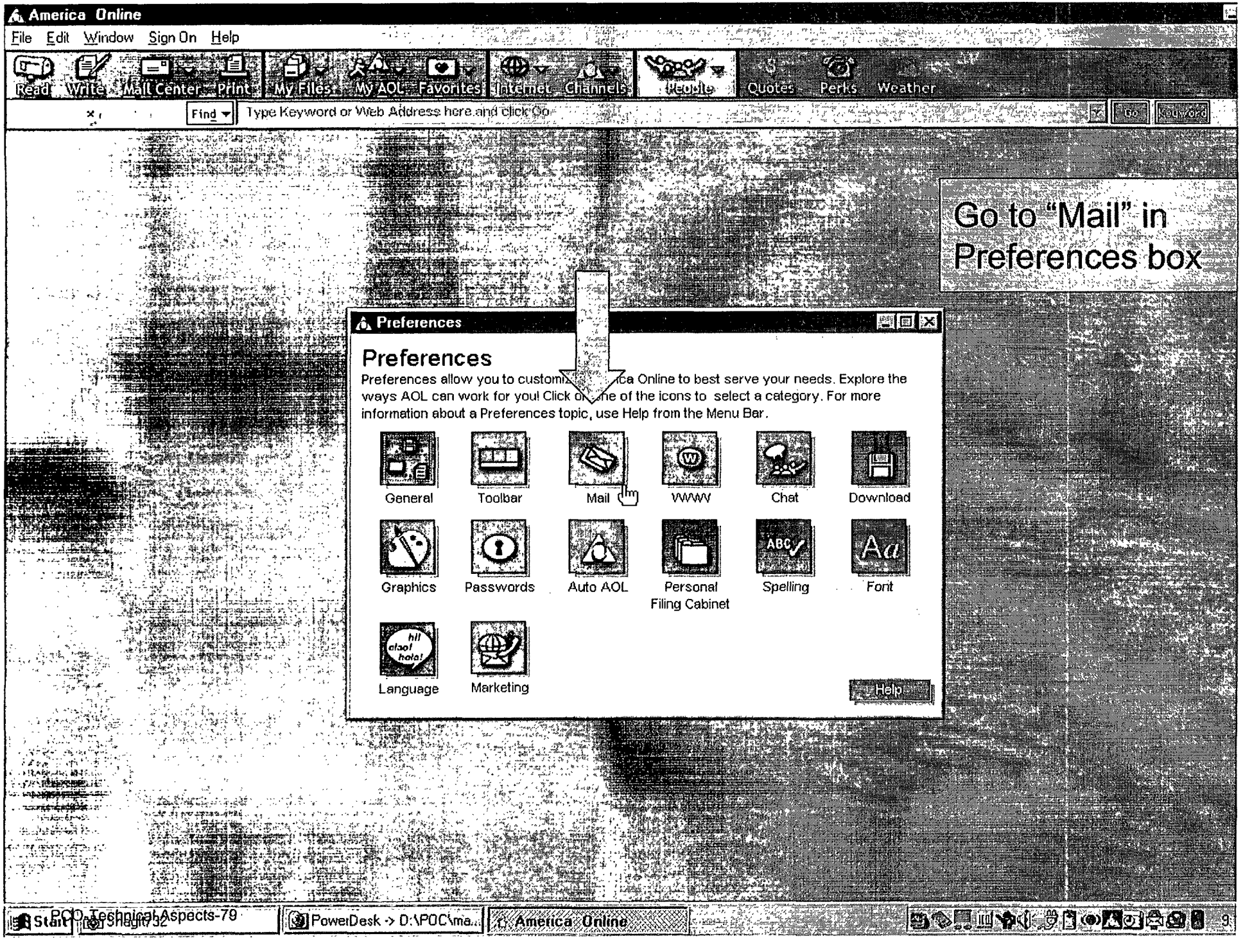
Reply | Reply All | Forward | Delete | Previous | Next | Close

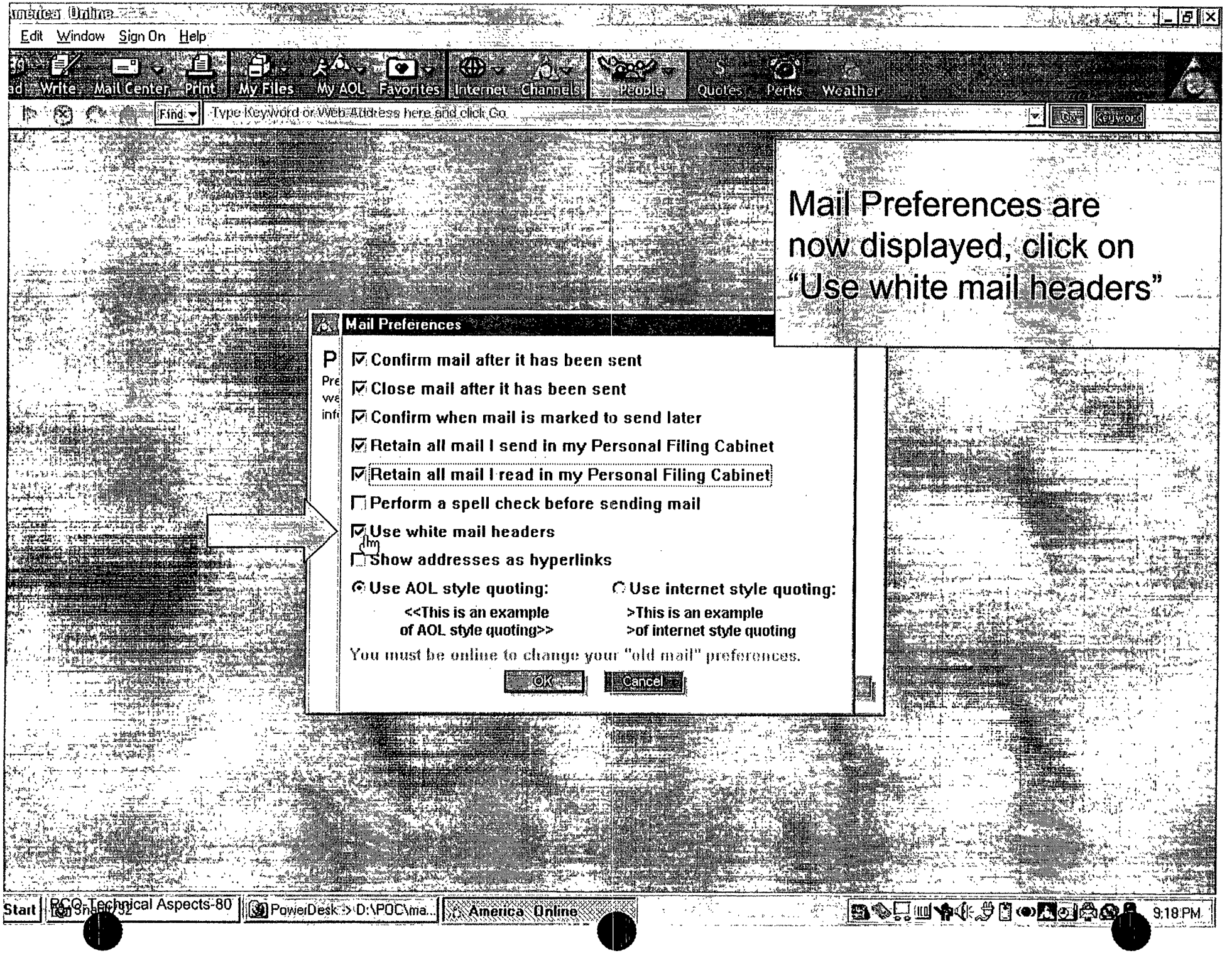
Move To (Move to Selected Folder)

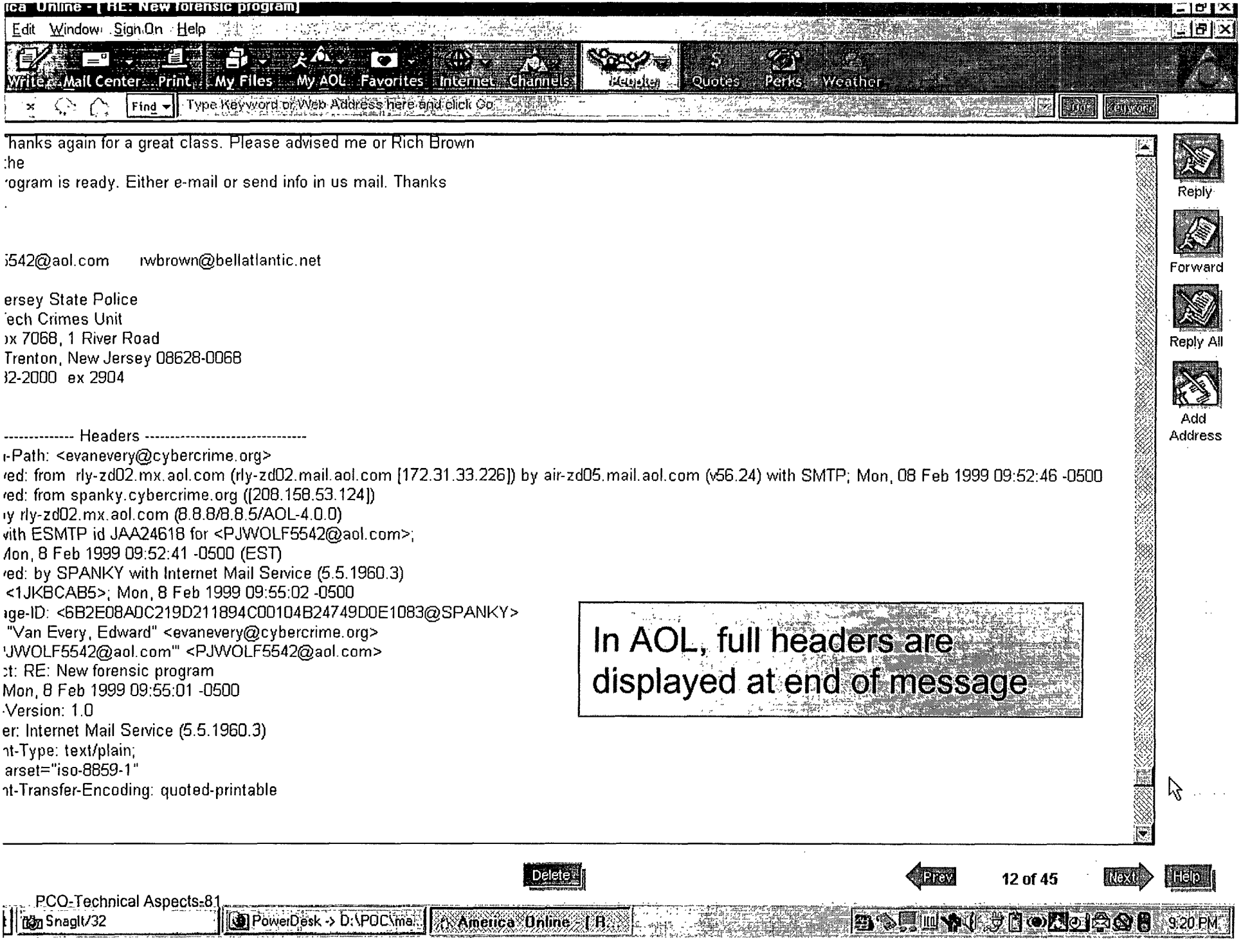
Inbox | Compose | Addresses | Folders | Options | Help

Protect Your Privacy!
Look For The TRUSTe Seal
Click Here To Learn More


America Online
File Edit Window Sign On Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword
lick Go
My AOL
Set Up AOL
Preferences
My Member Profile
Screen Names
Passwords
Parental Controls
Online Clock
Buddy List
Personal Publisher
Stock Portfolios
Reminder Service
News Profiles
America Online
version 4.0
America Online, under "My AOL", go to "Preferences"
Note: You do Not have to be connected to display Full Header information
Select Screen Name:
PJWOLF5542
Enter Password:
Select Location:
Div Hqts
SETUP
ACCESS NUMBERS
HELP
SIGN ON


America Online
File Edit Window Sign On Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels Reminder Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go to "Mail" in Preferences box
Preferences
Preferences
Preferences allow you to customi ca Online to best serve your needs. Explore the ways AOL can work for you! Click o e of the icons to select a category. For more information about a Preferences topic, use Help from the Menu Bar.
General
Toolbar
Mail
WWW
Chat
Download
Graphics
Passwords
Auto AOL
Personal Filing Cabinet
Spelling
Font
Language
Marketing
Help
Start
PowerDesk -> D:\POC\ma...
America Online


Edit Window Sign On Help
Write Mail Center Print My Files My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Keyword
Mail Preferences are now displayed, click on "Use white mail headers"
Mail Preferences
Confirm mail after it has been sent
Close mail after it has been sent
Confirm when mail is marked to send later
Retain all mail I send in my Personal Filing Cabinet
Retain all mail I read in my Personal Filing Cabinet
Perform a spell check before sending mail
Use white mail headers
Show addresses as hyperlinks
Use AOL style quoting:
<<This is an example
of AOL style quoting>>
Use internet style quoting:
>This is an example
>of internet style quoting
You must be online to change your "old mail" preferences.
OK
Cancel
Start
PCQ-Technical Aspects-80
PowerDesk - D:\POC\ma...
America Online
9:18 PM


ica Online - [RE: New forensic program]
Edit Window Sign On Help
Write Mail Center Print My Files My AOL Favorites Internet Channels Register Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
hanks again for a great class. Please advised me or Rich Brown
he
ogram is ready. Either e-mail or send info in us mail. Thanks
542@aol.com rwbrown@bellatlantic.net
ersey State Police
ech Crimes Unit
)x 7068, 1 River Road
Trenton, New Jersey 08628-0068
)2-2000 ex 2904
---------- Headers ----------
-Path: <evanevery@cybercrime.org>
ed: from rly-zd02.mx.aol.com (rly-zd02.mail.aol.com [172.31.33.226]) by air-zd05.mail.aol.com (v56.24) with SMTP; Mon, 08 Feb 1999 09:52:46 -0500
ed: from spanky.cybercrime.org ([208.158.53.124])
y rly-zd02.mx.aol.com (8.8.8/8.8.5/AOL-4.0.0)
vith ESMTP id JAA24618 for <PJWOLF5542@aol.com>;
Mon, 8 Feb 1999 09:52:41 -0500 (EST)
ed: by SPANKY with Internet Mail Service (5.5.1960.3)
<1JKBCAB5>; Mon, 8 Feb 1999 09:55:02 -0500
age-ID: <6B2E08A0C219D211894C00104B24749D0E1083@SPANKY>
"Van Every, Edward" <evanevery@cybercrime.org>
'JWOLF5542@aol.com'" <PJWOLF5542@aol.com>
t: RE: New forensic program
Mon, 8 Feb 1999 09:55:01 -0500
-Version: 1.0
er: Internet Mail Service (5.5.1960.3)
nt-Type: text/plain;
arset="iso-8859-1"
nt-Transfer-Encoding: quoted-printable
In AOL, full headers are displayed at end of message
Reply
Forward
Reply All
Add Address
Delete
Prev
12 of 45
Next
Help
PCO-Technical Aspects-81
SnagIt/32
PowerDesk -> D:\POC\ma...
America Online - [R...
9:20 PM

Obtaining More Information

What information can we expect from a site to have regarding an e-mail message?

Mail server logs - Each message passing though a mail server is generally automatically logged. Time of retention for logs varies from site to site, as they take up space on computers.

Access logs - Use of an IP address is generally logged by access providers. Again, the time of retention for logs varies from site to site, as they take up space on computers.

The key is to request the information as soon after the event as possible. Otherwise, the offline backup practices of the site will determine availability of the information.

Obtaining More Information

Example from a mail log:

An ISP's mail logs contain information on messages that successfully traversed the server as well as those that were rejected. The format of these logs varies.

Obtaining More Information

Given an IP address and a time stamp, most providers or sites can find the end user who was using the IP address at the specific time. Knowing who to ask can save valuable time and insure availability of accurate information.

Warrants, court orders or subpoenas are typically required to release exact end user information to law enforcement officials. These requests should contain the IP address and a time stamp including time zone. For e-mail investigations, providing the full e-mail headers is very helpful.

Dial in logs from commercial services or Local Internet Service Providers are used to corroborate undercover activity.

Based on level of cooperation, you may be able to have service provider do text string searches (grep) of their cache files for pertinent information.

PROTECTING CHILDREN ON-LINE

The Investigation

Investigative Concerns

- Have a plan
- Don't use department's computer system
- Strict undercover accounts w/ good backstop credentials
- When/Where is the investigation authorized to be conducted
- Document and record online sessions
- Stick with what you know
- Know when to say when

Background Information

- Personal data
- Place of employment
- Job description
- Vocational attributes
- Outside interests, hobbies

Electronic Records

- Account start and disconnect dates
- Billing/Credit card information
- Screen names or nicknames used
- Violations or complaints on record
- Terminated or active (current) account
- LOGS : connecting/disconnecting times
- IP info...Internet Protocol Addresses

Investigative Methods

- Physical Surveillance
- Victim-Witness Interview
- Pre-text phone Call
- Pen Register
- Electronic Surveillance
- Undercover Approach
- Informant Contact
- Sting Operation
- Advanced Techniques (sniffers, datascopes..)

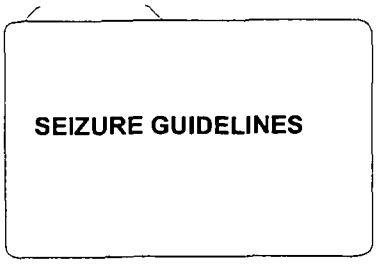
Keys to Success

- Preservation of Evidence
- Swift action to collect electronic audit trails ("electronic bloody foot prints")
- Focus on identifying the actual violator behind the internet address
- Exploiting corroborative computer evidence
- Support, resources and time...

Gee Whiz

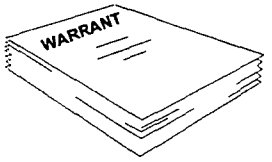
In addition to using the Internet and the computer to enhance your investigation don't get caught up in the technology. Traditional investigative methods such as surveillance, background checks, physical evidence, and interview & interrogation will always make your case.

Computers As Evidence

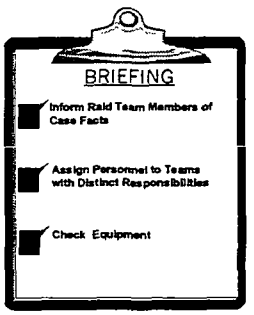


Authorization

- Warrant
- Consent
- Probable Cause



Pre-Raid Briefing



Raid Preparation: Tools

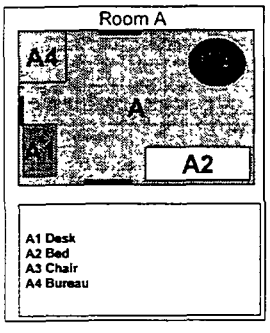
- Screw drivers, pliers, needle nose pliers, wire cutter, hammer
- Cable Ties, Tape, Boxes, Paper Bags
- Labels, marking pens, scribe
- Cameras
- Rubber Gloves
- Telephone Handset
- Laptop computer/printer
- Bootable floppy (multiple OS's and hardware drivers)
- SCSI Backup Device, Adaptor cables and media
- NIC, Hub, Patch Cord
- Magnetometer or compass

Executing the Search

- Secure the Premises
- Organize the Scene
- Photograph the Scene

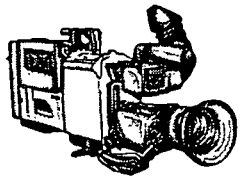
Organize the Scene

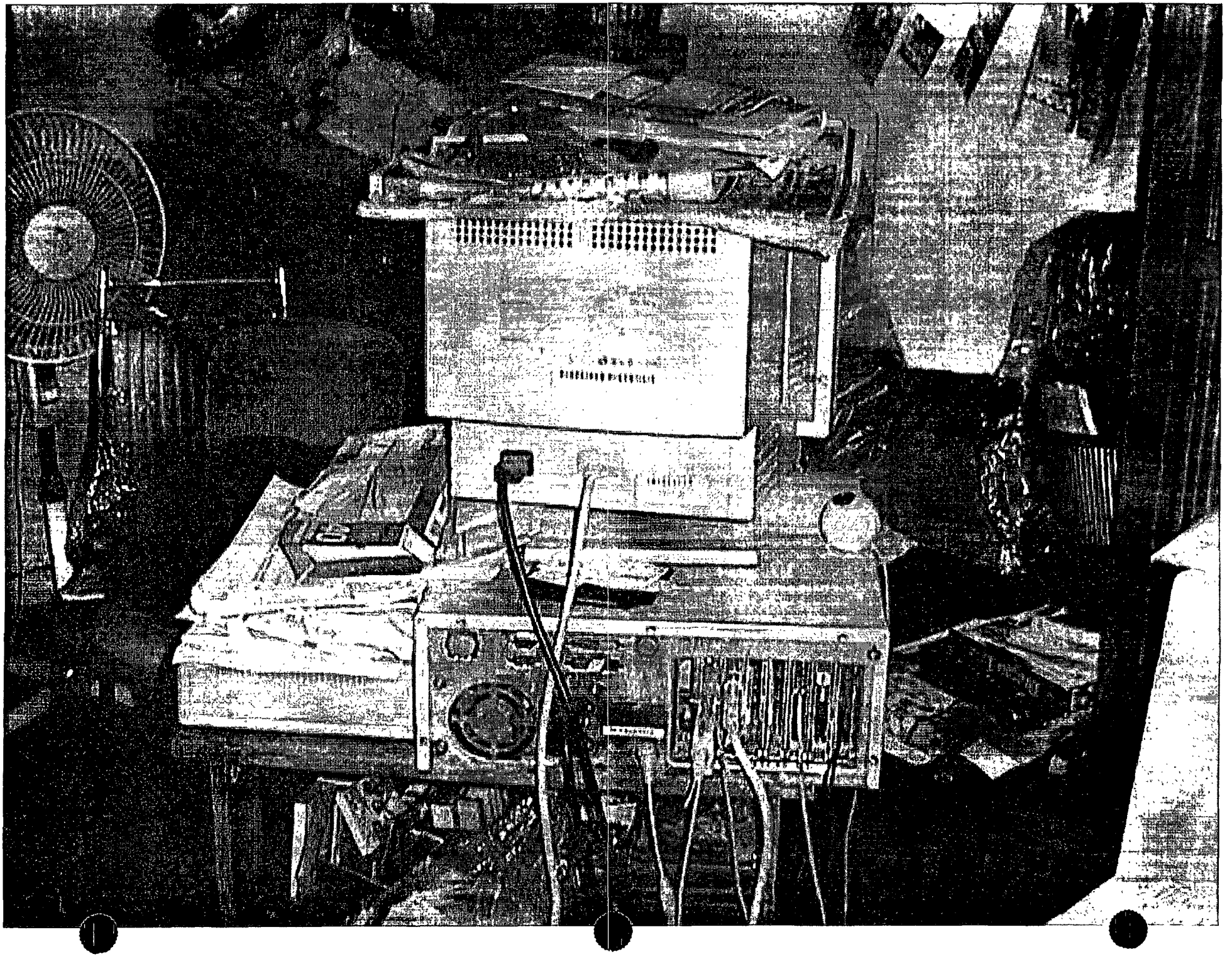
- Diagram the Site
- Label Rooms
- Sub-Label Components

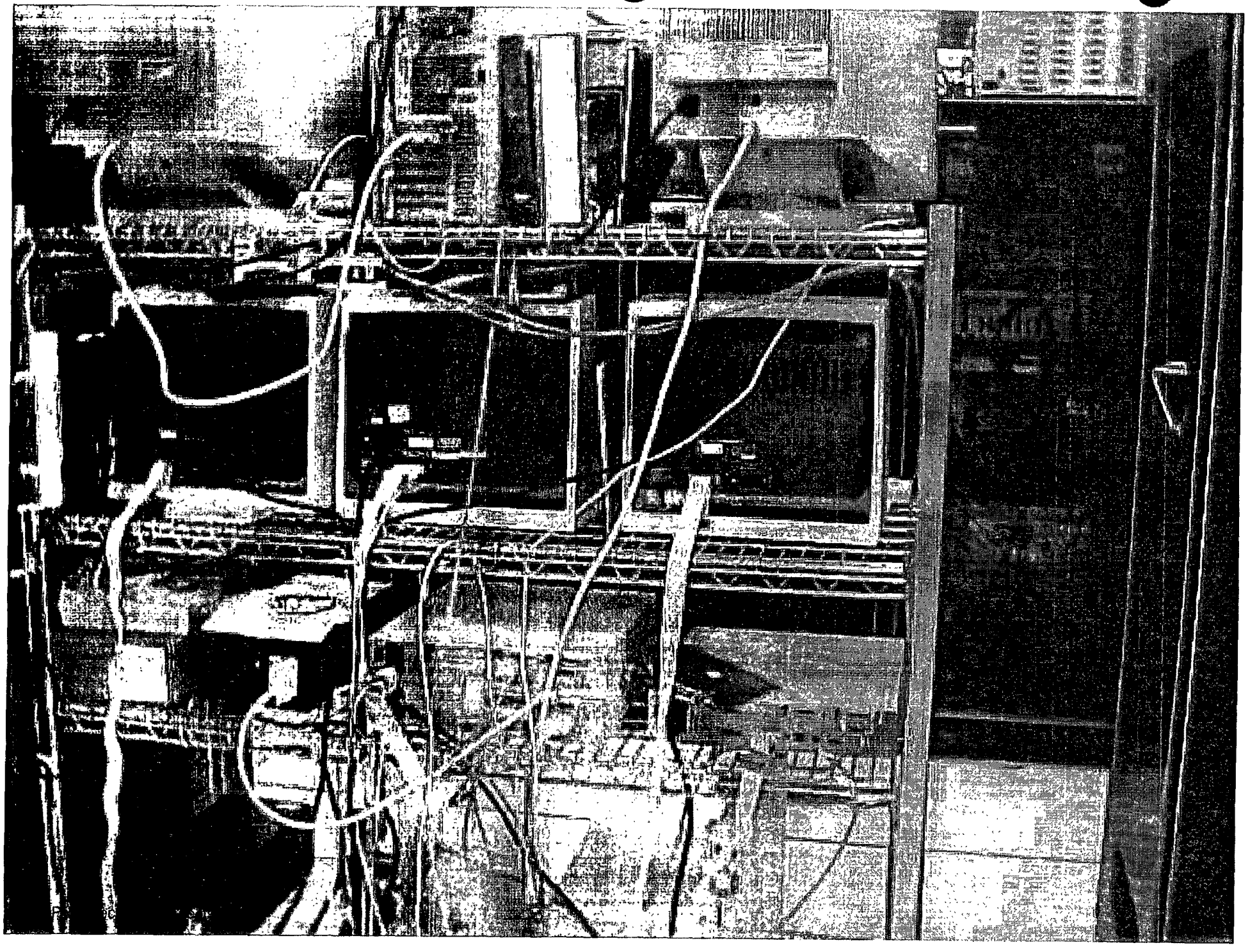


Photograph/Videotape Scene

- Entire Scene - Start from exterior
- Notes, Doodles, Papers near computer(s)
- Books, Bookshelves, Manuals
- Computers and all connections







A Little Knowledge Can Be Dangerous

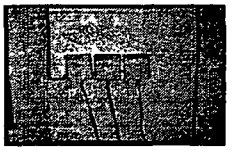
- Sophisticated computer users can easily bobby trap the computer with destructive programs.
- These programs are intended to destroy evidence.
- Safeguard the computer, prevent anyone from taking a quick "peek" that could engage these destructive devices.
- Evidence can be retrieved after destructive means have been used to attempt to destroy evidence.
- Retrieval hinges on the safe recovery methods that are performed in the lab.

What Items To Look For

- Video, photography equipment
- Magazines, letters, newsletters
- Sex Toys, games, video games
- Radio Scanners.
- Telephone access devices.
- Hacking Literature.
- Software to facilitate the crime.
- Credit Card receipts/list.
- Storage Devices: Zip, Jaz, Sysquest or Tape Drives
- Credit Card readers.
- MacKinnon Theory of Concentric Circles

Processing the Scene

- Disconnect modem lines from wall, note numbers on blocks.
- Retrieve phone numbers using handset (958).
- If Department has 800 number that captures ANI, call it.
- Survey for network connections, disconnect if applicable and feasible.



Processing the Scene

- Photograph monitor if on.
- Determine if dusting for fingerprints is necessary. (Do not dust at scene)
- Do not remove media from drives, seal with tape to *prevent removal.*
- Photograph and diagram wiring - if possible.
- Tag both ends of all wires.
- Mark and Log components and peripheral devices
- Voucher/Inventory Intelligently.

Processing The Scene

- Only disassemble to facilitate transport.
- Pack and pad components in boxes.
- Use paper bags or cardboard boxes to store computer media.
- Do not use plastic baggies.
- Look for indicia of ownership (receipts, invoices, etc).
- Leave copy of inventory and warrant with owner.

Transportation and Storage

- Keep media away from electromagnetic fields.
- Store in dry, clean location with moderate temperature.
- Store floppy disks in sleeves and other media in their respective storage containers.
- Rule of thumb: if you're comfortable so is the evidence.
- Clearly label evidence with a "DON'T TOUCH OR OPERATE" warning.

What Not To Do

- **Do Not Unplug Memory Phones,Fax machines, digital cameras or external Modems from Power Source!**
- **Never examine or turn on/off Computer.**
- **Note: If situation warrants turn off computer by pulling plug from rear of computer.**

Submitting Evidence For Forensic Analysis

- Identify by serial number and mark all equipment vouchered. Count the floppies and other media; number and categorize!
- Prepare Request for Laboratory Analysis and document chain of custody.
- Attach copy of affidavit, search warrant, subpoena, consent as well as, all investigation and arrest reports.

Submitting Evidence for Analysis

- **Fully describe incident and be specific about the information you need retrieved.**
- **Remember, The forensic analyst has no knowledge of your case.**
- **There is no "Evidence key" on the computer.**

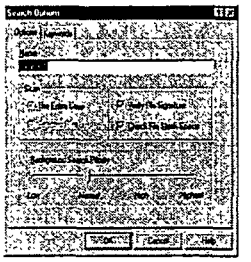
Forensic Data Analysis

- Process in which computer evidence is analyzed.
- Requires specialized training, tools and equipment.
- Advanced knowledge of computer hardware, networks and operating systems.
- Admissibility depends on qualifications and actions of the analyst.
- Chain of Custody and Integrity of evidence must be maintained.

The Forensic Process

- Image
- Authenticate
- Analyze

During each phase of your examination documentation of your actions is paramount to its admissibility and your credibility.



Concerns Within High Tech Units

- Cops into Techno-Geeks
- Techies into Cops
- How do you supervise
- Islands of Information
- Empire Builders
- Research and Development=Seats of your pants
- Internet Research="Playing on the computer again"

Training

- High Technology Crime Investigations Association (www.htcia.org)
- Search Incorporated (www.search.org)
- National White Collar Crime Center (www.nwccc.org)
- Federal Law Enforcement Training Center (www.cybercop.org)
- International Association of Computer Investigations Specialists (www.cops.org)
- Private Corporations (Lucent, IBM, ASR-Data, Encase, NTI)
- List Serves:
  - Computer Forensics: jnj@infobin.org

Courtroom Presentation

- You may have to educate a judge and jury
- Use standard terms, Microsoft Dictionary
- Expect the unexpected!
- Can you rebuild offenders' system, prove it worked?
- Video Capture devices to prepare videotapes
- Will the defense hire their own expert?
- What is level of expertise of your examiner?
- Will you be able to present policies?

Help on the Technical Front

- Northeast Chapter of the High Technology Crime Investigators Association (www.ne-htcia.org) or International (www.htcia.org)
- International Association of Computer Investigations Specialists (www.cops.org)
- ASR DATA- Expert Witness for macintosh and Windows 95 (www.asrdata.com)
- Tech Assist: (www.toolsthatwork.com)

Other Avenues

- Asset Forfeiture
- M.O.U. when performing analysis for outside your agency, overtime and equipment procurement
- Sentencing and Probation conditions- restrictions on use of Internet
- On Line orders or protection

Bibliography

- Netscape Communicator (www.netscape.com)
- Eudora Mail (www.eudora.com)
- Deja News Newsgroup Search Engine (www.deja.com)
- Webferret; Mailferret, NewsFerret, (www.ferretsoft.com)
- Netlab (www.eb.uah.edu/~adanil)
- Mirc (http://www.mirc.co.uk)
- Free Agent (www.forteinc.com)
- Quickview Plus (www.inso.com)
- Sam Sade (www.blighty.com)
- Netscan Tools (www.nwps.com)

Administrative

INTERIM ORDER

NUMBER 101-~

OKTE -96

TO ALL COMMANDS

Subject: INVESTIGATION OF CRIMES INVQLVING COMPUTERS OR COMPUTER TECHNOLOGY

1. The Computer Investigation and Technology Unit, a subunit of the Detective Bureau's Central Investigation and Resource Division, was established to provide the Department with the capability of responding to criminal complaints involving the use of computers (See Interim Order 111, series 1995).

2. Effective immediately, in order to protect computer evidence obtained by this Department during the course of investigations or arrests, and to enhance the prosecution of defendants, the following measures will be complied with:

a. Whenever a uniformed member seizes, or expects to seize, evidence consisting of a computer that has been used to commit a crime or is suspected of being a device that stores evidence, an immediate notification will be made to the Computer Investigation and Technology Unit.

b. Whenever a unit of this Department conducts a criminal investigation where computers or computer evidence may be involved, such unit will confer with the Computer Investigation and Technology Unit at the earliest possible stage of the investigation.

c. Whenever a warrant to seize computers or computer related evidence is being sought by a member of this Department, the Computer Investigation and Technology Unit will be conferred with Drior to the preparation of the warrant. Notification to the Computer Investigation and Technology Unit concerning search warrants will be of a limited nature pertaining only to computers and computer-related equipment to be seized.

d. Whenever an arrest involving a computer crime is made, the Computer Investigation and Technology Unit will be notified to determine if a response to debrief the prisoner(s) is necessary.

3. When requested, the Computer Investigation and Technology Unit will provide technical assistance in properly securing computer evidence, conducting computer forensic examinations and preparing warrants. The Computer Investigation and Technology Unit will make the determination whether a response to the scene is required, based on the totality of the circumstances presented in each r;~so

4. The Computer Investigation and Technology Unit is located at Police Headquarters, Room 1312U. The unit can be contacted between 0600 and 2000 hours, Monday through Friday, at (212) 374-4247. At all other times, the Computer Investigation and Technology Unit can be contacted through the Office of the Chief of Detectives at (212) 374-5430.

5. Any provisions of the Department Manual or other Department directives in conflict with this order are suspended.

BY DIRECTION OF THE POLICE COMMISSIONER

DISTRIBUTION
All Commands

Computer Investigations And Technology Unit

What Is CITU?

CITU is the New York City Police Departments Computer Investigations and Technology Unit, an investigative sub-unit of the Detective Bureau .

Mission of CITU

- Investigate Computer Related Crimes
- Maintain Computer Forensic Laboratory capabilities
- Serve as a high-tech resource for law enforcement and business.

Staff

- Lt. Christopher Malinowski
  Commanding Officer
- Sgt. James Doyle
  Supervisor
- Sgt. Brian McGuinness
  Supervisor
- Det. Theodore Capozziello
  Investigator / Technician
- Det. Gerard Schoenacher
  Investigator / Technician
- Det. Kevin Coco
  Investigator / Technician
- Det. Donald Callahan
  Investigator / Technician
- P.O. Mark Kirschner
  Forensic / Technician
- P.O. Luke Cats
  Forensic / Technician

How CITU Works

- **Did A Crime Occur?**

CITU is available to investigate and determine if a criminal offense has occurred such as:

- ♦ Any offense involving related to the use of a computer or where the computer is the object of the crime, which includes theft of intellectual property, e-mail abuse, internet related crimes, harassment, hacking, telecommunications fraud, software piracy, pornography, forgery, counterfeiting, cellular cloning.
- ♦ Any illegal activity such as drug trafficking, prostitution, bookmaking, credit card fraud, and even rape and homicide cases, where computers may have been used to record or store information.
- ♦ Any offense involving data destruction or required data recovery techniques.

- **What if it did?**

Utilizing a well-defined forensic protocol, CITU provides the law enforcement and business community with expertise and technical tools to gather and access critical electronic evidence. Procedures include; search warrant preparation addressing sensitive privacy issues and detailed description of electronic components, determination of what and how to seize evidence during the search, data recovery, detailed analysis of hard drives and other recordable media, and preservation of evidence

- **Prosecution**

CITU's goal in any investigation is the successful apprehension and prosecution of the offender.

We have access to legal counsel, local prosecutors, and a national network of computer crime investigators which affords complainants the latest information on case law, crime trends and technology issues.

- **Investigation**

Investigations are conducted with the utmost professionalism and discretion. CITU will address concerns of the victims

- **Is this for law enforcement use only?**
  NO. Anyone who believes they have been the victims of a high tech crime should call. If you are not sure, CITU will assist in making that determination.

- **When should I call?**
  AS SOON AS POSSIBLE! Electronically stored evidence is extremely volatile and can be lost or over written during the normal use of the computer.

- **How to reach us:**
  Phone: (212) 374-4247 / 4247
  Fax: (212) 374-4249

  We can be contacted 24 hours a day, 7 days a week through the Detective Bureau @ (212) 374-5430

DETECTIVE GUIDE AMENDMENT Procedure No. 203-02
DUTIES AND RESPONSIBILITIES

COMPUTER INVESTIGATION AND TECHNOLOGY UNIT

DEFINITION: *Computer Crime is defined as any violation of criminal law for which* knowledge of computer technology is used to commit an offense, whether or not the computer is used to commit an offense.

1. Investigate crimes committed involving the use of computers.

2. Assist all Department Units, during the course of investigations, Search Warrants and arrests by securing computers and associated evidence

3. Provide and maintain intelligence information about known computer hackers and organized computer crime groups, etc.

4. Assist Department Units in burglary investigations where large quantities of computer equipment involved

5. Conduct surveillance of on-line services including the Internet, Compuserve, Prodigy, etc. when investigations warrant.

6. Investigate pedophilia crimes committed via on line services.

7. Provide technical assistance to Major Case, Special Frauds, Sex Crimes, etc. on high profile cases.

8. Maintain response team capability in the event of such cases

9. Provide technology enhancements to the Detective Bureau to increase the effectiveness of information management.

10. Identify and conduct research in computer technology that will enhance this departments ability to investigate computer crimes

11. Maintain computer equipment, mobile units, to collect and develop evidence.

12. Maintain, distribute and account for all computers assigned to all Detective Bureau commands. Field all requests for computer equipment and peripherals.

13. Provide Technological assistance and support for all subordinate commands within the Detective Bureau upon request

POLICE DEPARTMENT
CITY OF NEW YORK

October 7, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to US Internet Corp. to release "subscriber and billing information" along with the corresponding "dial in number(s)" for the users assigned the following dynamic IP Addresses on these dates and times:

usimsptc2-34.usinternet.com	IP Address: 208.160.34.34	Mon Sep 28 13:34
usimsptc2-34.usinternet.com	IP Address: 208.160.34.34	Mon Sep 28 11:08
usimsptc6-101.usinternet.com	IP Address: 208.160.38.101	Fri Sep 25 11:43
usimsptc3-25.usinternet.com	IP Address: 208.160.35.25	Thu Sep 24 16:48
usimsptc2-26.usinternet.com	IP Address: 208.160.34.26	Tue Sep 22 21:48
usimsptc2-26.usinternet.com	IP Address: 208.160.34.26	Tue Sep 22 21:40
usimsptc7-194.usinternet.com	IP Address: 208.162.74.194	Tue Sep 22 16:12
usimsptc7-194.usinternet.com	IP Address: 208.162.74.194	Tue Sep 22 15:44
usimsptc7-194.usinternet.com	IP Address: 208.162.74.194	Tue Sep 22 13:18
usimsptc7-194.usinternet.com	IP Address: 208.162.74.194	Tue Sep 22 12:54
usimsptc2-136.usinternet.com	IP Address: 208.160.34.136	Tue Sep 22 00:35
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 22:14
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 17:29
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 17:24
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 15:16
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 13:01
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 12:57
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 12:56
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 12:52
usimsptc3-250.usinternet.com	IP Address: 208.160.35.250	Mon Sep 21 00:25
usimsptc2-184.usinternet.com	IP Address: 208.160.34.184	Sun Sep 20 17:37
usimsptc2-184.usinternet.com	IP Address: 208.160.34.184	Sun Sep 20 17:30
usimsptc2-184.usinternet.com	IP Address: 208.160.34.184	Sun Sep 20 15:03

2. The person(s) using these IP addresses on the above dates and times committed the crime of Computer Tampering utilizing a US Internet account.

3. The subpoena can be directed to the attention of:

Curt Lange
US Internet Corp
12450 Wayzata Blvd. Suite 224
Minnetonka, MN 55305
Tel# (612) 253-3211; FAX (612) 545-0302

4. This matter is assigned to:

P.O. Mark Kirshner

5. Thank you for your assistance.

Mark Kirshner
Police Officer

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to Deputy Commissioner, Legal Matters, October 7, 1999. I certify that the records requested are required for the above investigation.

Christopher Malinowski
Lieutenant

Laserjet 4 Toner		$ 92.99	2	$	185.98
Deskjet 660C Black Cartridge		$ 25.99	30	$	779.70
Deskjet 660C Color Cartridge		$ 26.99	30	$	809.70
Deskjet 855C Black Cartridge		$ 29.99	5	$	149.95
Deskjet 855C Color Cartridge		$ 27.99	5	$	139.95
Lexmark Optra		$ 300.00	12	$	3,600.00
Apple Laserwriter 600/4		$ 59.99	2	$	119.98
Calcomp Black		$ 10.00	30	$	300.00
Calcomp Color		$ 7.50	90	$	675.00
Brother PC Touch Cart		$ 29.99	2	$	59.98
Muratec F-60 Imaging Cart		$ 100.00	3	$	300.00
				$	-
Calcomp Paper Roll E		$ 24.35	24	$	584.40
Calcomp Paper Roll E		$ 24.35	24	$	584.40
Calcomp 5336 24" Adaptor		$ 200.00	1	$	200.00
HP Prem Glossy	C3836A	$ 55.95	5	$	279.75
HP Prem Paper	C1824A	$ 11.95	5	$	59.75
HP Prem Transparency	C3834A	$ 47.95	5	$	239.75
				$	-
Iomega Zip 10Pak		$ 149.99	10	$	1,499.90
Iomega Jazz 5 Pack		$ 499.99	8	$	3,999.92
Sysquest 230		$ 29.95	10	$	299.50
Sysquest 150		$ 19.95	10	$	199.50
TDK CDR74		$ 6.00	50	$	300.00
DC4 90 4mm Tape		$ 8.75	50	$	437.50
3M TR1		$ 30.00	10	$	300.00
3M TR4		$ 40.00	10	$	400.00
3.5 Floppies 100 pack		$ 15.00	100	$	1,500.00
				$	-
Compressed Air		$ 6.00	25	$	150.00
Inkjet Care Cleaner		$ 9.00	1	$	9.00
Markers		$ 0.59	100	$	59.00
Wire Ties (100) 4"		$ 0.99	3	$	2.97
Wire Ties (100) 6"		$ 2.18	3	$	6.54
Wire Ties (100) 11"		$ 5.45	3	$	16.35
				$	-
Polaview 90		$ 5,395.00	1	$	5,395.00
Network Cards		$ 100.00	6	$	600.00
Network Hub 8 Port		$ 200.00	2	$	400.00
ConnerTape Stor 800		$ 479.00	4	$	1,916.00
Recordable CD Writer 4X		$ 999.00	2	$	1,998.00
Tools		$ 1,000.00	1	$	1,000.00
Color Scanner w/ ADF		$ 1,200.00	1	$	1,200.00
56 KB Modems		$ 199.00	6	$	1,194.00
9 GB Drive		$ 2,399.00	2	$	4,798.00
Laser Printer		$ 7,000.00	1	$	7,000.00
Canon 620 Inkjet		$ 400.00	1	$	400.00
				$	-

Safeback		$	250.00	5	$ 1,250.00
Snapback		$	595.00	5	$ 2,975.00
TPU Tape Viewer		$	695.00	5	$ 3,475.00
Poly Tape		$	695.00	5	$ 3,475.00
Norton Utilities 95		$	79.95	5	$ 399.75
Norton Utilities 8.0		$	119.95	5	$ 599.75
Quickview Plus		$	119.95	5	$ 599.75
Conversions Plus		$	69.99	5	$ 349.95
Mac Opener		$	34.99	5	$ 174.95
Wordperfect		$	299.00	5	$ 1,495.00
MS Office Win 31		$	449.00	5	$ 2,245.00
MS Office 97		$	539.00	5	$ 2,695.00
Winzip		$	29.00	5	$ 145.00
Ontrak Disk Util		$	35.00	5	$ 175.00
Direct Access Password SW		$	622.50	1	$ 622.50
Ghost		$	125.00	5	$ 625.00
Disk Search		$	249.50	5	$ 1,247.50
Pagemaker		$	579.00	5	$ 2,895.00
Net tools 32		$	25.00	5	$ 125.00
Photoshop		$	589.00	5	$ 2,945.00
PKZIP		$	29.00	5	$ 145.00
Winzip		$	25.00	5	$ 125.00
WinImages		$	50.00	5	$ 250.00
Training		$	25,000.00	1	$ 25,000.00
Total					$ 98,183.62

Computer Investigation & Technology Unit

CITU MEMO

Date: October 7, 1999

Re: FORENSIC EXAMINATIONS

The following are general guidelines for completing a forensic examination on evidence submitted for analysis by C.I.T.U. The steps outlined here must be completed but the methods used to accomplish them are up to the examiner. Record the procedure and methods used on the Forensic Examination Worksheet. You may be required to defend your course of action in court. Only use software registered to the New York City Police Department or to C.I.T.U. for the examination. All notes will become part of case folder (Rosario).

Inventory Equipment

A. Identify all submitted equipment and cross reference against the property voucher. If there are items not listed or items are listed but not physically present, make note of the discrepancy on the Forensic Exam Worksheet. **Immediately notify a supervisor** if property is listed but not physically present. CITU supervisor will prepare letter to vouchering officer detailing discrepancy.

B. Itemize all of the equipment on a Computer Evidence Inventory Sheet. Each CPU gets listed on a separate sheet along with it's associated peripherals.

C. Remove the cover to the CPU and inventory the following:

- hard drives connected and disconnected
- installed cards
- number and type of RAM chips
- processor

D. Disconnect the power to the hard drive(s).

E. Using a write protected bootable floppy inserted in the A: drive, power on the computer and access C.M.O.S.. Ascertain the system date, time, boot sequence, installed RAM and the hard drive information. Enter information in the appropriate fields on the Inventory Sheet.

Examination

Remember, every case is different and the methods used to recover evidence will change from case to case and from examiner to examiner. Record **all of your actions** on the Forensic Worksheet. Be prepared to defend your methods.

A. Remove drive 0 from the CPU and attach to the Lab Forensic Computer as drive 1. The jumper on the evidence drive will most likely have to be changed as the drive will now be a slave. Jumper information can be found on the Internet if the drive is not properly marked.

B. Boot the lab computer and write protect drive 1. It is imperative that any examination of the evidence drive proceed only after the drive is properly protected from being modified by an inadvertent write. ***Never boot the lab computer into Win95 while an evidence drive is attached***. Win95 will make modifications to the drive before you will have a chance to write protect it. If you need to run Win95, you must use an image copy of the evidence drive.

C. Scan the evidence drive for virus infection. Record findings on the Forensic Examination Worksheet. **Do not disinfect or modify the evidence drive**.

D. Identify all partitions and examine the drive for evidence of indicated criminality.

E. Perform for each found drive.

Archiving Evidence

There are several methods available to us to archive and safeguard evidence. As the technology develops, higher capacity and faster methods will become available and these guidelines will also evolve.

A. There will be times when the entire evidence drive will need to be duplicated and stored as evidence. These duplicates or "Images" can later be restored to virgin media and examined. Absent the following indicators, the necessity of making image copies of drives is up to the investigator. In the following instances you must duplicate the drive:

- evidence is found in slack space
- the drive is encrypted
- extensive use of passwords
- erased files containing evidence found
- other subterfuge is found
- functionality of original setup must be examined

B. When deleted files are found to contain information evidentiary in nature, the drive *must* be duplicated prior to recovery. Unerasing files, even to another location, **will modify** the evidence drive.

C. Image files from Safeback will be archived to either CD-ROM or TR-4 tape. Snapback images will remain on the tape media used in the original duplication. In all cases, the software utilized to perform the back up will be indicated on the Forensic Worksheet. In cases when duplication or "Imaging" of the evidence drive is not required, files containing information evidentiary in content will be archived to CD-ROM or TR-4 tape collectively. All files from each examination will be copied and stored in their own subdirectory on the CD-ROM or tape.

D. When the functionality of the equipment must be established, a copy of the drive will be utilized for the examination.

Report

Following the examination a Forensic Report will be completed. This report should include all steps taken during the examination, software used and results of the search. Copies of printouts will be placed into the investigation folder along with the completed Computer Evidence Inventory Sheets and the Forensic Examination Worksheets. Copies of evidence derived from the submitted equipment will be given to the case investigator along with a copy of the report.

End procedure.

Informational

AVAILABLE TRAINING ON SEIZING AND EXAMINING COMPUTER EVIDENCE

1. Florida Department of Law Enforcement Center for Advanced Law Enforcement Studies
   PO Box 1489
   Tallahasse, Fl 32302
   (904) 488-1340

2. FBI Academy
   Economic and Financial Crime Training Unit
   SA Ervin Suggs
   Quantico, VA 22135
   (703) 640-1156

3. Federal Law Enforcement Training Center
   Carlton Fitzpatrick
   Building 210
   Glynco, GA 31524
   (912) 267-2724

4. SEARCH
   7311 Greenhaven Drive, Suite 145
   Sacramento, CA 95831
   (916) 392-2550

5. Royal Canadian Mounted Police
   Canadian Police College
   Ottawa, Ontario
   (613) 998-2541

6. IACIS
   PO Box 21688
   Keizer, Oregon 9730-1688
   (503) 557-1506

COMPUTER CRIME SCENE CHECKLIST

- ❑ **Label Each Room-**
- ❑ **Sub-Label the components in the room**
- ❑ **Diagram the Site**
- ❑ **Assign Areas of responsibility**
- ❑ **Photo or video the entire scene**
- ❑ **Photo or video any notes, doodles or papers near the computer**
- ❑ **Photo or video the computer, from all sides**
- ❑ **Set Up Laptop with Seized Items Database**
- ❑ **Check the scene with a compass or magnetometer**
- ❑ **When seizing evidence carefully note its location**
- ❑ **Test phone jacks for tone and retrieve number**
- ❑ **Seize software and manuals you will need to process evidence-especially proprietary or non-mainstream software**
- ❑ **Seize notes, scribbles, and notebooks, concentrate on area around computer work area**
- ❑ **Check for concealed compartments**
- ❑ **Tag both ends of cabling**
- ❑ **Record component identifiers, mark evidence with no serial numbers**
- ❑ **Transport**

This list in not all-inclusive.

Source: SEARCH, Inc. reprinted with permission

CRIME SCENE TOOL KIT

- **Screwdriver-** Phillips for cases
- **Screwdriver-** Small Slotted for peripherals
- **Small Diagonal cutters-**cutting nylon wire ties
- **Rubber bands-** to wrap cables to facilitate transport
- **Color Tape or Coded Buttons-** for tagging cabling and terminus
- **Small Scissors-** for cutting tape
- **Wire Ties-** to wrap cables to facilitate transport
- **Boxes-** for transporting
- **Digital or 35 mm Camera-** To record Crime Scene, screen capture
- **Indelible markers-** for marking
- **Evidence tags-** Adhesive, can be pre-made with software
- **Bootable Floppies-** Should only be used in presence of experts, at minimum should have disklok and autoexec.bat modified to load on boot.
- **Rubber Gloves-** to preserve latents and as a health precaution
- **Tape-** Masking, Plastic
- **Evidence tape-** To secure floppies and CD-ROMs in computers
- **Packing material**
- **Standard Telephone-** to check modem lines
- **Video camera**
- **Hammer or nail puller-** to remove cable fasteners
- **Laptop-** On large seizures a database can facilitate logging
- **Power Strip-** for investigator use if bringing laptop and printer
- **Batteries or power adapters for electronic equipment-** especially cell phones

This list in not all-inclusive.

Source: SEARCH, Inc. reprinted with permission

Internet Service Provider Contacts

Maintained by James Nerlinger, Jr. --> jnj@infobin.org for updates and corrections. If you have any additions, please put the information in the same format as below.

@HOME NETWORK	
Contact Name	Legal Department, Attention Karen McNally
Online Service	@Home Network
Online Service Address	425 Broadway, Redwood City, CA 94063
Voice Number	650-569-5335
Fax Number	650-482-4606

AMERICA ONLINE	
Contact Name	Justyna Kilbourne / Sophie Haynie
Online Service	America Online
Online Service Address	22000 AOL Way, Dulles, Virginia 20166
Voice Number	703-265-2745 / 3298
Fax Number	703-265-2305

ARCH PAGING	
Contact Name	Bonnie Miller
Online Service	Arch Paging
Online Service Address	11570 Mosteller Road, Cincinnati, OH 45241
Voice Number	513-771-4666
Fax Number	513-782-1960

AT&T WORLDNET	
Contact Name	Edward Stephenson
Online Service	AT&T Worldnet
Voice Number	919-319-8187
Fax Number	919-319-8154

(AT&T Worldnet is different from all other ISPs as they require you to use your registered agent. Speak to your Secretary of State to obtain this information. Unfortunately, this will significantly lengthen the process of obtaining the information. Edward Stephenson at least USED to accept a copy as well.)

CINCINNATI BELL FUSE.NET / ZOOMTOWN	
Contact Name	S. McCammon, Director Of Security
Online Service	Cincinnati Bell Telephone, Inc.
Online Service Address	201 East Fourth Street, Cincinnati, Hamilton County, Ohio 45202
Voice Number	513-397-6800
Fax Number	513-381-5352

COMPUSERVE	
Contact Name	Dan Piskur, Security Manager & Legal Liaison

Online Service	CompuServe
Online Service Address	Unknown
Voice Number	614-538-4257
Fax Number	Unknown

DLP TECHNOLOGIES INCORPORATED

Contact Name	Lee Penn
Online Service	DLP Technologies, Incorporated
Online Service Address	7444 Jager Court, Cincinnati, OH 45230
Voice Number	513-232-7791
Fax Number	513-232-7801

DONET

Contact Name	David Mezera (dmezera@donet.com)
Online Service	The Dayton Ohio Network
Online Service Address	1425 Arbor Avenue, Dayton, Ohio 45420
Voice Number:	937-256-7288
Fax Number:	937-258-5331

EARTHLINK

Contact Name	Harlen Bayha (also Chris Hanson & Rob Quinn)
Online Service	Earthlink
Online Service Address	3100 New York Drive, Pasadena, California 91107
Voice Number	626-296-5735
Fax Number	626-398-5477

EBAY

Contact Name	Kristen Crowley (Also, Jeff Dvorak)
Online Service	EBay
Online Service Address	2005 Hamilton Avenue, Suite 350, San Jose, California 95125
Voice Number	408-558-5905
Fax Number	408-558-6100

EPOCH NETWORKS

Contact Name	Heidi Griffin
Online Service	Epoch Networks (ENI.NET)
Online Service Address	18201 Von Karman Ave, 5th floor, Irvine, CA 92612
Voice Number	949-474-4950
Fax Number	

EROLS INTERNET / RCN

Contact Name	Peggy Chittal, Custodian of Records
Online Service	EROLS INTERNET / RCN
Online Service Address	7921 Woodruff Court, Springfield, VA 22151
Voice Number	703-321-2403
Fax Number	703-321-7432

(As of 12/29/98, Erols and it's sister ISPs were rolled into a single ISP

under RCN.COM. Existing customers will maintain their email addresses but
new customers will be user@rcn.com. For the time being, Peggy is still able
to access Erols subscriber information as well as RCN information.)

EXCITE, INC.	
Contact Name	Dan Brush, Corporate Counsel
Online Service	Excite (Excite.com among others)
Online Service Address	555 Broadway, Redwood City, CA 94063
Voice Number	650-569-2923
Fax Number	650-298-4430
FLASHNET COMMUNICATIONS	
Contact Name	Jason Wingard
Online Service	FlashNet Communications
Online Service Address	1812 North Forest Park Boulevard, Fort Worth, Texas 76102
Voice Number	817-877-1132
Fax Number	817-332-9594
HOTMAIL	
Contact Name	Randy Delucchi, Director of Customer Service
Online Service	MSN Hotmail
Online Service Address	1290 Oakmead Parkway, Suite 218, Sunnyvale, CA, 94086
Voice Number	408-222-7037
Fax Number	408-222-7020
HOPEWELL FAMILY COMMUNICATIONS	
Contact Name	Yolanda Miller
Online Service	Hopewell Family Communications
Online Service Address	5350 W. New Market Road, Hillsboro, OH 45133
Voice Number	937-378-4722
INAME CORPORATION	
Contact Name	Josh Barrack
Online Service	(iname.net, iname.com, mail.com, email.com, globecomm.com)
Online Service Address	11 Broadway, Suite 660, NY, NY 10004
Voice Number	212-425-3477, Ext. 218
Fax Number	212-525-3487
IOWA NETWORK SERVICES, INC.	
Contact Name	James Turner
Online Service	Iowa Network Services, Inc.
Online Service Address	321 Eighth Street, Des Moines, IA, 50309
Voice Number	800-205-1110
Fax Number	515-830-0552
JUNO ONLINE SERVICES	
Contact Name	Joel Pulliam

Online Service	Juno Online Services
Online Service Address	120 West 45th Street, NY, NY 10036
Voice Number	212-597-9211
Fax Number	212-597-9200

LYCOS

Contact Name	Anna Kumar, Custodian of Records
Online Service	Lycos
Online Service Address	1675 North Shore LineBlvd, Mountain View, CA 94043
Voice Number	650-938-4400 x215
Fax Number	650-938-4500
E-mail	anna@whowhere.com

MEDIAONE

Contact Name	Jane Sherwood, Legal Demands Office
On-line Service	Media One
On-line Service Address	9785 Maroon Circle, Suite 420, Englewood, CO 80112
Voice Number	800-871-6298
Fax Number	303-792-4774
E-mail	jsherwood@mediaone.com

MICROSOFT CORPORATION (MSN, HOTMAIL)
Tony Saputo
Sr. Security Manager,
Information Security Investigations
Microsoft, Corporation
1 Microsoft Way
Redmond, WA 98052
425-703-2000
425-936-7329 (FAX)
425-703-5555 (24 Hr Emergency Law Enforcement Hotline)
tsaputo@microsoft.com

or

Howard A. Schmidt
Director, Information Security
Microsoft, Corporation
1 Microsoft Way
Redmond, WA 98052
425-703-2000
425-936-7329 (FAX)
425-703-5555 (24 Hr Emergency Law Enforcement Hotline)
howards@microsoft.com

MSN

Contact Name	Pat Kirsch
Online Service	MSN, Microsoft Corporation
Online Service Address	1 Microsoft Way, Redmond, Washington, 98052-6399
Voice Number	425-936-2760
Fax Number	425-936-7409

Responses will be sent via email

NETCOM ONLINE COMMUNICATIONS

Contact Name	Spencer Doherty
Online Service	Netcom Online Communications
Online Service Address	Two North Second Street, San Jose, CA 95131
Voice Number	408-881-3026
Fax Number	408-881-3387

NETWORK SOLUTIONS, INC.

Contact Name	Richard Forno, Security
Online Service	Network Solutions, Inc.
Online Service Address	505 Huntmar Park Drive, Herndon, VA 20170
Voice Number	703-925-6848
Fax Number	703-834-7175

ONENET COMMUNICATIONS

Contact Name	Larry Moyer
Online Service	OneNet Communications
Online Service Address	9944 Reading Road, Cincinnati, Ohio 45241
Voice Number	513-618-2107
Fax Number	513-618-2001

PSI NET

Contact Name	John LoGalbo, Esq., General Counsel
Online Service	PSI Net
Online Service Address	510 Huntmar Park Drive, Herndon VA 20170-5100
Voice Number	703-904-4100
Fax Number	703-904-4200
E-mail	legal@psinet.com

USA.NET

Contact Name	Brenda Mientka
Online Service	USA.Net, Inc.
Online Service Address	1155 Kelly Johnson Blvd., Suite 400, Colorado Springs, CO 80920
Voice Number	719-265-2930
Fax Number	719-265-2922

UUNET

Contact Name	Martina Knee, General Counsel
Person to Call	Justin Marino
Online Service	UUNet
Online Service Address	3060 Williams Drive, Fairfax, Virginia 22031
Voice Number	703-289-8072
Fax Number	703-645-4424

WEBTV

Contact Name	Valerie "Bobbi" Hirota
Online Service	WebTV
Online Service Address	2593 Coast Avenue, Mountainview, CA, 94043

Voice Number	650-614-5593
Fax Number	650-614-2782
XMISSION LLC	
Contact Name	Peter Ashdown
Online Service	Xmission LLC
Online Service Address	51 East 400 South, Suite 200, Salt Lake City, Utah 84103
Voice Number (Direct to Ashdown)	801-539-0852 (General) 801-990-0816
Fax Number	801-539-0853
YAHOO	
Contact Name	Mike Haswell
Online Service	Yahoo
Online Service Address	3420 Central Expressway, 2nd Floor, Santa Clara, California 95051
Voice Number	408-616-3760
Fax Number	408-731-3400

COMPUTER INVESTIGATION AND TECHNOLOGY UNIT ARREST LOG FOR 1998

#	DATE ARRESTED	DETECTIVE	CRIME	CLASS	CASE #	ARR #	PERP NAME

POLICE DEPARTMENT
CITY OF NEW YORK

PERMISSION TO SEARCH

Complaint Number:	**Case Number:**
Assigned Detective:	**Command:**

I, _____, having been informed of my constitutional right not to have a search made of my premises, motor vehicle, or other personal property without a search warrant, and having been informed of my right to refuse to consent to such a search, and understanding that evidence and/or contraband found as a result of such may be seized and used against me in a court of law, hereby authorize: _____, a police officer of the New York City Police Department , or any police officer of the New York City Police Department, to conduct a complete search of:

( ) My premises, and all property found therein, located at:

_____, _____, _____, _____
Street Address Town County State

( ) I do voluntarily provide the keys to above location for access.

( ) My motor vehicle; a 19__, _____, VIN _____, bearing registration plates _____, issued by the state of _____, and all property found therein. This vehicle is currently located at :

_____, _____, _____, _____
Street Address Town County State

( ) My personal computer or electronic storage device: _____ to include an examination of any data stored.

This written permission is being given by me to the above named Police Officers voluntarily and with no promises made to me or threats against me.

FALSE STATEMENTS MADE HEREIN ARE PUNISHABLE AS A CLASS A MISDEMEANOR PURSUANT TO SECTION 210.45 OF THE PENAL LAW OF THE STATE OF NEW YORK

Signature: _____ Time: _____
Date: _____

_____
Witness

_____
Witness

NEW YORK CITY POLICE DEPARTMENT
COMPUTER INVESTIGATION AND TECHNOLOGY UNIT

DATE OUT	TIME OUT	INVESTIGATOR Name/Shield	CASE #	EQUIPMENT (one line for each item removed)	DATE RETD

INVESTIGATIVE ANALYSIS REPORT

To: Detective XXXXXX
Unit Name)
From: Forensic Analyst
Computer Investigation Unit
(Unit Phone Number)
Date: Date
Re: **EXAMINATION OF EVIDENCE UNDER INVOICE# xxxxx LAB# xx/97**

SUMMARY

I have examined and analyzed investigatory evidence submitted by Detective XXXXX of Vice Enforcement Squad and itemized on Property Clerk's Invoice number xxxxx. All items referenced were marked in the format CIU-xx .My findings are as follows:

- THIS SYSTEM DID CONTAIN ELECTRONIC IMAGES FILES OF CHILD PORNOGRAPHY

A complete detailed Forensic Processing Report follows.

GENERAL PROCEDURES

The following outlines standard processing procedures used in examining all fixed and removable media:

1. The examining computer system is a Police Department owned DOS based Pentium 100 MHz CSS Lab PC, running under MS-DOS 6.22 and Windows for Workgroups 3.11. The operating system software is licensed to run on this computer. The system is equipped with one 5.25" floppy drive and one 3.5" floppy drive, both capable of reading/writing to both high and low density floppy diskettes. 1 6X CD-ROM drive (SCSI read only), 1 Pinnacle Micro CD-ROM writer (SCSI), 1 Iomega Jaz drive (1gig), 1 Iomega Zip drive (100mb), 2- 2 gig Internal Western Digital Hard drives (scratch). 1-Seagate 8000 tape drive. The video system is VGA and is capable of displaying at least 256 simultaneous colors at 640 x 480 dpi.
2. Diskettes measuring 5.25" are write-protected by placing an adhesive write protect tab over the write protect notch. Diskettes measuring 3.5" have their write protect notch opened. Both of these actions prevent any accidental writing to the diskettes by the examining system. In the event copies are needed prior to analysis, an exact image is made using ***AnaDisk*** version 2.08 by Sydex Corporation.
3. Prior to hard drive analysis an exact duplicate of the hard drive is made using Image MAsster 500 IDE, Intelligent Computer Solutions. In addition, an image of the original hard drive is created utilizing ***Safeback*** version 1.1 Sydex Corporation. The image files are archived to CD-ROM or tape for future reference.

4. *Note: Due to the fact that DOS assigns drive letters automatically, the evidence hard drive when attached to it's Central Processing Unit is normally drive C:, when the hard drive is removed and installed as a slave in a lab computer and disklok.exe is executed the hard drive is then assigned the next drive letter which would be D:, so therefore during the examination of the evidence drive and any screen captures are performed the drive letter would be D:.*

SPECIFIC FINDINGS

Comments and findings which resulted from the examination and processing of all submitted hardware and software follows. Findings have only been provided regarding diskettes or files, which either contain relevant information or was specifically requested by the investigator.

Hardware

Invoice xxxxxx, Item #2, is a TriGem computer serial number QS133002539 containing a single IDE Conner CFS1621A 1548-MB hard drive and 16MB RAM. The embedded serial number for this drive is FJBBNA2. The computer was properly set up and no attempt was made by the owner/operator to conceal data through the use of passwords, data encryption or manipulation of the operating system. The system date and time were correct. Drive parameters in CMOS are 16 heads, 3146 cylinders and 63 sectors with a normal geometry.

Physical Analysis

1. The investigatory drive was installed on forensic lab computer #2 and set up to be the slave IDE drive.
   - A virus check was performed with negative results, report saved as "\reports\fp5797.txt..
   - The AUTOEXEC.BAT and CONFIG.SYS files were examined. The files were normal and there were no lines REMarked out as to indicate special settings for programs that no longer resided on the computer.
   - ***Fdisk*** was executed and reported one 100% DOS partition. The DIR command was executed and generated the directory listings then saved to file DIR5797.TXT and saved to a directory "\reports".
   - Norton's *Unerase* was used to Unerase any recoverable files. Erased files were recovered and saved to a folder "\erased". Files of evidentiary value consisting of electronic images were recovered and printed as CIU#1, a directory listing of files recovered was compiled as "\reports\direras.txt".
   - The following files specifically requested by the investigator were found to reside on the subject computer's hard drive:

FILE:	DIRECTORY	CIU#
◆ Rik1.jpg	C:\PONTIAC	CIU#2
◆ Rik2.jpg	C:\PONTIAC	CIU#3
◆ Rik3.jpg	C:\PONTIAC	CIU#4
◆ Rik4.jpg	C:\PONTIAC	CIU#5
◆ Cumshot.avi	C:\AUDI	CIU#6
◆ Stand. avi	C:\AUDI	CIU#7

- CIU#6 and CIU#7 are windows based video files (.avi) which are digitized movies
- CIU#6: 97 frames of a male masturbating
- CIU#7: 178 frames of a male masturbating.

A search was made for Joint Photographic Experts Format (JPG), Graphics Interchange Format (GIF), Tagged Image File Format (TIF), UNIX to UNIX Encoded (UUE) or Bit Mapped Images (BMP, RLE) for pornographic images with positive results.

The following subdirectories contained pornographic images or movie files, not all files were of a pornographic nature.

\AUDI	36 AVI files	CIU#8
\CORSICA	2 JPG files 1AVI files	CIU#9
\GALLON	18 MPG files	CIU#10
\PONTIAC	986 files, (GIF, JPG)	CIU#11
\USERS	270 files, (BMP, GIF, JPG, PCX)	CIU#12
\WORKDESK	5 files (JPG, GIF)	CIU#13
\X-CELEBS	23 files (JPG, GIF)	CIU#14

The directory listing of the above subdirectories were printed and labeled as shown. All of the images were printed as 1" X 1" thumbnail image files and attached to the directory listing. All of the above items have been archived to the CD-ROM accompanying this report.

The files in \Gallon were ".MPG" and in order to print a sample a screen capture program was utilized to capture the first frame of each movie file.

The hard drive was searched for text files or evidence of electronic communications detailing sexual relations between adults and children. It is noted that the subject computer had the following Internet related software installed:

- Netcom- software to connect to the Internet
- Mirc, New MIRC, software enabling one to electronically chat on the internet
- Quickcam, CuSeeME,- software when used with a computer attached camera can send realtime video over the Internet to another individual
- Microsoft NetMeeting- software utilized to set up an electronic conferencing between individuals computers

\PROGRAMS\NETMEETING\RECEIV~1\	3 JPG files
\PROGRAMS\NETMEETING\SPEEDD~1\	5 CNF files
\WINDOWS\DESKTOP\MYBRIE~1\	3 TXT files

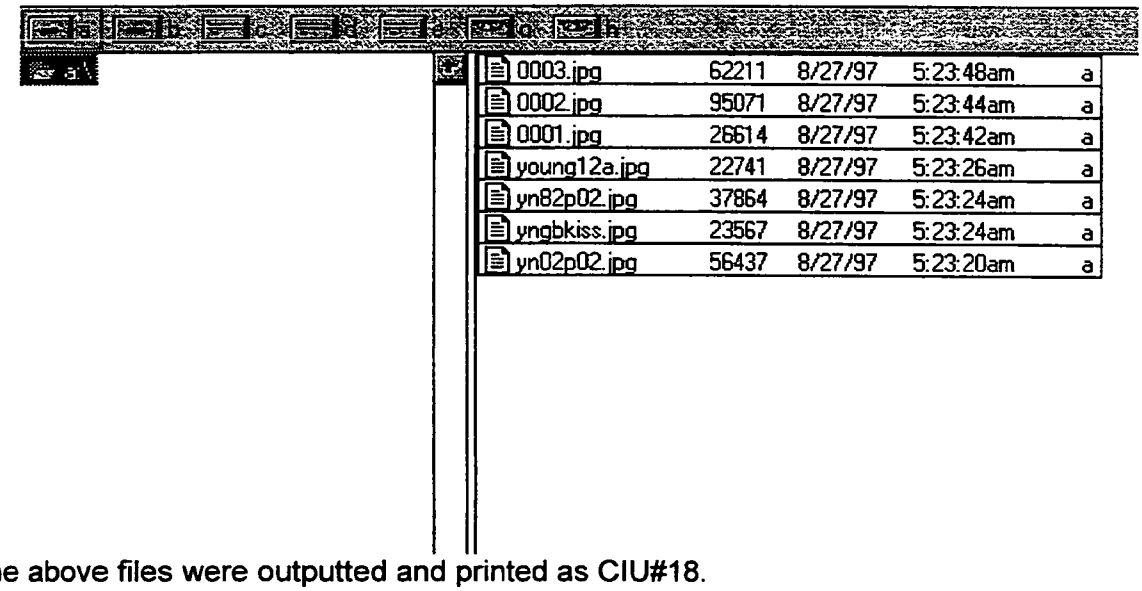
Above printed as CIU#15.

The following directories yielded logs of electronic chats between the operator of the subject 's computer and other individuals. A representative sample was reviewed which showed the conversations to be of a sexual nature directed towards minors. These logs are printed, with each file a separate record of the conversation, the files are separated by a separator page indicating the name of the file and the file creation date. A directory listing accompanies each directory output.

- LOGS IN DIRECTORY \newmirc\mirc CIU#16
- LOGS IN DIRECTORY \mirc CIU#17

2. Invoice H005108, Item #4, two beige 3.5 high density floppy diskettes, marked with shield #1234, identified as recovering officer, Detective HIS NAME#1234 of the adb Squad. These diskettes were marked CIU #57_97D1 and CIU #57_97D2. The disks were write protected and examined. Disk 57_97D1 was unreadable, DOS reporting an unrecoverable disk error. A copy of this disk was made with ***ANADISK*** and ***Norton Utilities 8.0*** was utilized to repair the disk. The following are screen captures of the directory entries for each disk: Each diskette contained images of child pornography.

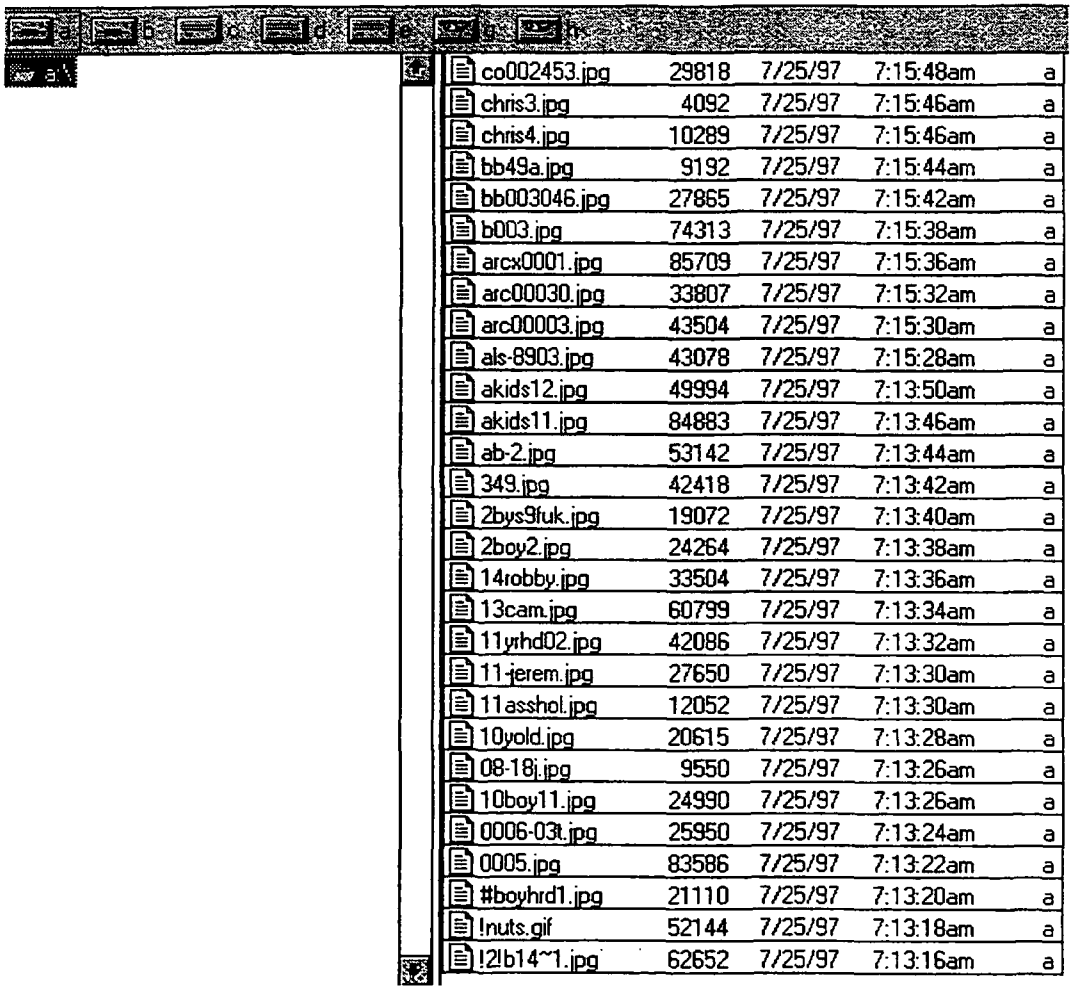
DISK S7_97D1 (Recovered Disk)



The above files were outputted and printed as CIU#18.

Initials

DISK S7_97D2



co002453.jpg	29818	7/25/97	7:15:48am	a
chris3.jpg	4092	7/25/97	7:15:46am	a
chris4.jpg	10289	7/25/97	7:15:46am	a
bb49a.jpg	9192	7/25/97	7:15:44am	a
bb003046.jpg	27865	7/25/97	7:15:42am	a
b003.jpg	74313	7/25/97	7:15:38am	a
arcx0001.jpg	85709	7/25/97	7:15:36am	a
arc00030.jpg	33807	7/25/97	7:15:32am	a
arc00003.jpg	43504	7/25/97	7:15:30am	a
als-8903.jpg	43078	7/25/97	7:15:28am	a
akids12.jpg	49994	7/25/97	7:13:50am	a
akids11.jpg	84883	7/25/97	7:13:46am	a
ab-2.jpg	53142	7/25/97	7:13:44am	a
349.jpg	42418	7/25/97	7:13:42am	a
2bys9fuk.jpg	19072	7/25/97	7:13:40am	a
2boy2.jpg	24264	7/25/97	7:13:38am	a
14robby.jpg	33504	7/25/97	7:13:36am	a
13cam.jpg	60799	7/25/97	7:13:34am	a
11yrhd02.jpg	42086	7/25/97	7:13:32am	a
11-jerem.jpg	27650	7/25/97	7:13:30am	a
11asshol.jpg	12052	7/25/97	7:13:30am	a
10yold.jpg	20615	7/25/97	7:13:28am	a
08-18j.jpg	9550	7/25/97	7:13:26am	a
10boy11.jpg	24990	7/25/97	7:13:26am	a
0006-03t.jpg	25950	7/25/97	7:13:24am	a
0005.jpg	83586	7/25/97	7:13:22am	a
#boyhrd1.jpg	21110	7/25/97	7:13:20am	a
!nuts.gif	52144	7/25/97	7:13:18am	a
!2lb14~1.jpg	62652	7/25/97	7:13:16am	a

The above files were outputted and printed as CIU#19.

THE ABOVE IS A COMPLETE DESCRIPTION OF MY EXAMINATION OF THE SUBMITTED EVIDENCE.

END ANALYSIS

(Forensic Examiner) (Supervisory Review)

Initials

Computer Investigation & Technology Unit

S A R

SAR Number	Date Received	Code	Type of Request	Unit Requesting	Detective Assigned	Date Closed	Supv Init

Code:

SW	Search Warrant Execution	
494	Assistance with 494 Program	
OA	Outside Agency Request	
SP	Subpoena / Warrant Preparation	
DB	Debrief Suspect/Prisoner	
TA	Technical Assistance	
GP	Graphics / Presentation	
PI	Preliminary Investigation	
TL	Training / Lecture	

Technical

Here are some known Award BIOS default passwords to try (all are case sensitive):

1EAAL
589589
589721
595595
1322222
01322222
ALFAROME
ally
aLLy
aPAf
AWARD_PS
AWARD_SP
AWARD_SW
AWARD_WG
awkward
BIOSTAR
CONCAT
CONDO
condo,
dirrid
efmukl
g6PJ
h6BB
h996
H996
HCT
HLT
j00j
j09F
j252
j256
j262
J262SER
j322
J64
KDD
LKWPETER
lkwpeter
oder
SER
SKY_FOX
switches_sw
Syxz
SZYX
TTPTHA
TzqF
Wodj
ZAADA
ZBAAACA
ZJAAADC

File Extension Parent Programs

.pfb=Adobe Type 1 Font
.htm=HTML file (Hyper Text Metafile)
.fif=Iterated Systems Fractal Image
.stx=SBIG Astronomical Image
.dxf=Autocad Exchange
.wmf2=Embedded Bitmap Metafile (Windows Meta File)
.uue=UUencoded file (Unix to Unix Encoded)
.wri=Windows Write
.mpg=MPEG video (Moving Pictures Expert Group)
.dwg=AutoCAD
.png=PiNG
.cel=Autodesk Animator CEL
.ppt=PowerPoint
.mov=Apple QuickTime
.avi=Video for Windows
.psd=Adobe Photoshop
.bmf=Corel Gallery clipart
.ico=Windows ICON file
.ras=Sun
.iff=Amiga IFF/LBM
.img=GEM Image
.tdb=ThumbsPlus database
.eps=Encapsulated Postscript
.raw=Raw grayscale file
.wpg=DrawPerfect
.gem=GEM Metafile
.pcd=Kodak PhotoCD
.mid=MIDI Recording
.doc=Word for Windows Document
.cgm=Computer Graphic Metafile
.wav=Sound
.txt=Text
.exe=Executable
.tif=Tagged Image Format
.tga=Targa Truevision
.cdr=CorelDRAW Picture
.mnd=Mandelbrot Image
.jpg=JPEG Compressed (Joint Photographics Expert Group)
.ttf=TrueType Font
.gif=CompuServe GIF (Graphics Interchange Format)
.pcx=Zsoft PC Paintbrush
.wmf=Placeable Metafile (Windows Meta File)
.cur=Windows Cursor
.mf=Windows Metafile
.bmp=Windows Bitmap
.mac=MacPaint
.pct=Macintosh PICT
.cam=Casio Camera
.kdc=Kodak DC40/DC50
.kqp=Konica Camera
.sgi=Silicon Graphics Image
.sfw=Seattle Filmworks Mangled JFIF
.dcs=Kodak Profession Digital Camera
.dcx=Multi-page PCX
.mic=Microsoft Image Composer

File Extension Equivalents

.pss=>.pfb
.ani=>.cur
.st4=>.raw
.st9=>.stx
.st8=>.stx
.st7=>.stx
.st6=>.stx
.st5=>.stx
.html=>.htm
.001=>.uue
.pal=>.pcx
.tnb=>.bmp
.scr=>.exe
.cch=>.tif
.cpt=>.tif
.pat=>.cdr
.mni=>.mnd
.jfi=>.jpg
.jif=>.jpg
.ttr=>.ttf
.ini=>.txt
.tt_=>.ttf
.pcc=>.pcx
.rle=>.bmp
.dib=>.bmp
.dll=>.exe
.lbm=>.iff
.cmx=>.cdr
.kiz=>.uue
.jpeg=>.jpg
.tiff=>.tif
.pict=>.pct
.vue=>.jpg
.rgb=>.sgi
.jpe=>.jpg
.j6i=>.jpg
.pdd=>.psd
.pmp=>.jpg
.dat= Unknown

COMPUTER INVESTIGATION AND TECHNOLOGY UNIT (212) 374-4247

Probable cause to seize computer has been established?

NO → Confer with CITU immediately. Confer with District Attorney.

Yes

Secure scene and move people away from computer and power supply

Yes

Is the computer switched on?

NO → Under no circumstances turn on the computer

Yes

Is CITU Available?

No → Do Not Touch the Keyboard

→ Do Not take advice from the owner/ user

→ Photograph or make note of what is on the screen

→ Allow printer to complete run

→ Switch off all equipment and remove power cords from rear of unit

→ If modem connected, trace wire to phone block, ascertain phone number with handset

Yes

FOLLOW ADVICE

Under no circumstances turn on the computer → Photograph or video and label the components as they are

Photograph or video and label the components as they are

→ Remove all other connected cabels leading to wall sockets or devices after tagging

→ Ensure all components are labelled or properly marked and carefully remove

→ Search area for notes, notebooks or paper which may have passwords or other evidence

→ Ask the user for passwords, usernames, logon name and record

→ Submit evidence in accordance with Interim Order 74, 74-1, s1995

TRANSPORT

Handle all equipment with care
Keep all equipment away from magnetic sources
Place hard disks and circuit boards in anti-static bags
Do not bend floppy disks or place labels directly on them

WHAT SHOULD BE SEIZED

For reconstruction of the system:

-Main Unit-the box the keyboard and monitor are attached to Monitor
-Keyboard and Mouse
-Cables
-Power Supplies
-Dongles: connectors plugged into ports on back of computer labelled PRINTER or LPT1
-Modems

FOR EVIDENCE RETRIEVAL:

-Floppy disks, DAT Tapes, Jazz, Zip or Syquest cartridges
-CD-ROMS
-Hard disks not connected to the computer

Source: ACPO Crime Committee 3/25/99

Edited for what is of interest for us in an investigation, I.e. tracking back documents to a computer that created the document

Warren

MICROSOFT'S HEAVY HAND IN THE COOKIE JAR
A special report from YEOW - Barry Simon.
Due to wonderful sleuthing by Richard Smith of PharLap (who earlier located the April Fool's Bug discussed in WWW issue 2.2), the world has discovered a number of places that Microsoft has been using these MACs - in Windows 98 IDs, in Office 97 documents and in the microsoft.com cookies. And privacy concerns result from all these uses.

To understand the issues, try a few experiments. First, you'll need your MAC assuming you have an Ethernet adapter. With Windows 9x, run the program winipcfg from the Run box. It should load with a dropdown that says 'PPP Adapter'. Change the dropdown to the name of your hardware adapter. The Adapter Address field will say something like 00-70-06-9A-8E-43. That's your MAC. Each byte is presented as two hex digits (0 through 9 or A-F) for a 12 character ASCII string which is what Microsoft uses. With Windows NT, run instead winmsd, go to the Network tab and pick Transports and you'll get the MAC.

For the next experiment, you'll need to look at a Word 97 document in text mode. You can't do this with Word. If you have **Quick View Plus** (plain Quick View won't do), open a Word doc in QVP, go to the View menu and pick View as Text. Or make a small Word doc, save it and rename it to a .txt extension and open it in Notepad. Now search for the string PID. You should find _PID_ GUID and shortly afterwards, a long hex string inside braces such as {F96EB3B9-C9F1-11D2-95EB-0060089BB2DA}. Those 12 hex digits at the end will be your MAC. Yup, **every Word doc, every Excel spreadsheet and every Power Point presentation is branded with an identifier showing the PC it came from. If your boss has a Word memo you sent her and a copy of the anonymous whistle blowing attachment you sent to the Feds, she could determine they were made on the same machine**. (Of course, if you aren't careful, the document includes an author name and if any corrections were made, it may say who made the corrections. Within the next few days, Microsoft expects to post a white paper on all the 'metadata'; embedded in Office documents).

To run the next experiments, you'll need Windows 98, so I'll tell you what happens so you can follow along in any event. In your Windows directory, you'll find a file called reginfo.txt. Open it in Notepad and look for a line called HWID; it ends with your MAC. This file is created when you install Windows and is transmitted to Microsoft when you register. And here's the clincher: even if you check the box not to send hardware information, this data is sent. And it's even worse - the data collection code is in an ActiveX control that can be used by any Internet site out there. Pharlap has a demo to illustrate this: go there and it displays your MAC on screen. Any site knowing of this control could track MACs of all Windows 98 visitors to their sites. There is also a demo and discussion at Windows Magazine. By

the way, this ActiveX control is also in the Windows 2000 beta so if Microsoft hadn't been found out, NT users would have been hit next.

Next, go to your cookies directory and open the text file whose name ends with microsoft.txt (it probably has a username@ in front where username is your login name). In it you'll find a string called GUID that includes your MAC (GUID, by the way, is short for Global Unique Identifier). This cookie is sent to www.microsoft.com every time you visit that site. You may have realized they were making a cookie when you registered at their site but I bet you didn't realize they were adding hardware information without your permission. (Actually the Win98 Registration Wizard made the cookie before you went to the Microsoft site.)

You might want to search your Registry for your MAC as a string. I found mine numerous times - two in suspicious places viz a viz Microsoft. It's part of a key for Media Player called Client ID (is this passed on to the Media Player servers?) and as part of a key HKCU\Identities that seems to be connected with Outlook Express 5.0.

Policies

COMPUTER INVESTIGATION AND TECHNOLOGY UNIT SUBPOENA LOG

CASE# SAR#	DATE RECEIVED	DETECTIVE	SCREEN NAME	DATE to DCLM	DATE RET	FAXED to PROVIDER	FAXED BY	DATE RESULTS

U/C Caller:_____ Time Started:_____
Date: _____ Time Ended:_____

Recorded: yes/no

Ficticious company name

e.g: Uplink Network Corporation, PO Box 4000, Bridgeton, MO. 63044-9718

Survey Questionaire

Hello my name is Cathy Upjohn of the Uplink Corporaton. We are offering 50 free hours of On-line service on any commercial service of your choice (Prodigy, Delphi, Compuserve or Americal On Line) for answering our questions. It will take only two minutes of your time and we send you via mail our software with the ten free hours of usage for your input.

1. What type of computer do you own?

2. Do you own a modem, if so what speed?
   a. Internal or external
   b. What brand

3. Do you own any other type of computer such as a laptop?
   a. Does it have a modem, what speed?

4. Who in your household uses the computer most frequently?

5. Which computer do you use most frequently?

6. Do any of your computers have multimedia capability?

7. Is it utilized for business, childrens homework, entertainment?

8. Are you a member of any online service? If so, which one?

9. What do you like most about your online service?

10. What do you like least about our online service?

11. Do you own or are a Systems operator of a Bulletin Borard or Webmaster?

12. What time of dya do use the computer most frequently?

13. Do you use it most frequently at home or work?

14. What is your occupation?

15. And which online service do want We have Delphi, America On line, Compuserve, Prodigy and Imagination network.

16. Where can I mail the software to? **(Be sure to get his/her name with the address)**

Thank you for assisting us in our survey and your software should arrive within 12 to 14 working days.

Provided by New York State Attorneys Office

Computer Investigation & Technology Unit

CITU

To: Sgt. James Doyle, Computer Investigation & Technology Unit

From: Detective Donald Callahan

Date: October 7, 1999

Re: REORGANIZATION OF CITU PHYSICAL PLANT AND PROCEDURES

The following steps are suggested for the reorganization of CITU in an effort to better secure evidence, provide for an audit trail for stored evidence, track and control the use and distribution of CITU equipment and to provide for a procedure for the examination of evidence.

Evidence

A. ALL evidence will be accepted into the lab by the Lab Master. In the event that the Lab Master is not present, evidence will be locked in an off hours property locker along with all the paperwork required by IO 74/96. Property will be removed and processed by the Lab Master at the beginning of his/her next tour.

B. Lab Master will be responsible for inventorying vouchered evidence, determining operational status, noting deficiencies and properly storing the evidence and paperwork in the lab.

C. Property and equipment in the lab is under the **exclusive** control of the assigned Lab Master. An audit trail of equipment will be maintained by the Lab Master.

D. All information will be recorded on forms (to be developed) until such time as the CITU Master Control Program is written in Microsoft's Access to track all aspects of case progress. This program will be accessible from the CITU LAN.

E. The Lab Master will be responsible for preparing a copy of the evidence drive onto a scratch drive for the investigator to examine. This request will be made on the appropriate form. GHOST will be used to create the copy in the cases where hard drives are involved. Files from all media other than floppies (see I. below) will be recovered by the Lab Master and restored to scratch drive. Lab Master will generate CRC checks on the original and copy to assure duplicity. Scratch drive will be mounted on CITU LAN as a read-only drive.

F. Investigator maps drive letter on his workstation to mounted volume. Investigator uses CITU standardized utilities (Norton, Quick View, Vueprint etc.) provided on LAN to examine files,

erased files and slack on duplicate drive. Searching on unallocated space will be done upon request by the Lab Master on the original media.

G. Drive can have read-only status removed upon request. Lab Master will make note on audit sheet. Drive can then be mapped as C: and evidence programs be executed from the workstation.

H. Drive will remain mounted until investigator notifies Lab Master of completion. Lab Master confirms CRC check. Investigator informs Lab Master of files needed as evidence. Lab Master will archive needed files to appropriate media for storage. Lab Master determines necessity of Mirror Image File (i.e. evidence found in erased file, slack or unallocated space).

I. Floppy disks are to be examined by the investigator. Lab Master will write protect all floppies prior to their release for examination. Investigator needs to fill out request to maintain chain of custody and audit trail. Problem disks can be examined by the Lab Master upon request. Disks determined to be evidentiary in nature will be imaged by the Lab Master. Image files will be archived along with other recovered files.

J. Upon completion of Forensic Report, property and voucher will be released by the Lab Master to the assigned investigator for return to the property clerk. Property will be returned to the property clerk no later than 2 tours following the completion of the report.

The above procedure will allow for the maintaining of a proper chain of evidence, a proper audit trail and the security of vouchered property under the control of CITU. **The Lab Master and supervisors are the only persons permitted in the lab**. Only the Lab Master upon properly documenting it, handles original evidence.

Computer Investigation & Technology Unit

CITU

To: Sgt. James Doyle, Computer Investigation & Technology Unit

From: Detective Donald Callahan

Date: October 7, 1999

Re: REORGANIZATION OF CITU PHYSICAL PLANT AND PROCEDURES

The following steps are suggested for the reorganization of CITU in an effort to better secure evidence, provide for an audit trail for stored evidence, track and control the use and distribution of CITU equipment and to provide for a procedure for the examination of evidence.

Software

A. ALL original software disks will have compressed image files made of the by the Lab Master. Image files will be archived onto CD-R and stored in the lab. Original media will be secured by the Lab Master in the lab in a media safe.

B. GHOST will be used to make these compressed images where applicable. Special software is available to the Lab Master to circumvent copy protection when necessary.

C. Until such time as the CITU LAN is operational, copies of these disks can be obtained upon request from the Lab Master. Original media will not be released except upon direct order from CITU supervisor.

D. Upon operational status of CITU LAN, image files will be available to all members from a read-only directory on the LAN.

E. Information on each image file will be entered into the CITU Master Control Program Software Inventory by the Lab Master. This application will be written in Microsoft's Access and will be describe in a later section.

F. Lab Master will be responsible for the maintaining of proper upgrades to software from Internet, BBS and WWW access. Lab Master will be responsible for registering software properly. All software documentation will be maintained in CITU library. This library will also be catalogued on the CITU MCP.

Computer Investigation & Technology Unit

CITU MEMO

Date: October 7, 1999

Re: FORENSIC EXAMINATIONS

The following are general guidelines for completing a forensic examination on evidence submitted for analysis by C.I.T.U. The steps outlined here must be completed but the methods used to accomplish them are up to the examiner. Record the procedure and methods used on the Forensic Examination Worksheet. You may be required to defend your course of action in court. Only use software registered to the New York City Police Department or to C.I.T.U. for the examination. All notes will become part of case folder (Rosario).

Inventory Equipment

A. Identify all submitted equipment and cross reference against the property voucher. If there are items not listed or items are listed but not physically present, make note of the discrepancy on the Forensic Exam Worksheet. **Immediately notify a supervisor** if property is listed but not physically present. CITU supervisor will prepare letter to vouchering officer detailing discrepancy.

B. Itemize all of the equipment on a Computer Evidence Inventory Sheet. Each CPU gets listed on a separate sheet along with it's associated peripherals.

C. Remove the cover to the CPU and inventory the following:

- hard drives connected and disconnected
- installed cards
- number and type of RAM chips
- processor

D. Disconnect the power to the hard drive(s).

E. Using a write protected bootable floppy inserted in the A: drive, power on the computer and access C.M.O.S.. Ascertain the system date, time, boot sequence, installed RAM and the hard drive information. Enter information in the appropriate fields on the Inventory Sheet.

Examination

Remember, every case is different and the methods used to recover evidence will change from case to case and from examiner to examiner. Record **all of your actions** on the Forensic Worksheet. Be prepared to defend your methods.

A. Remove drive 0 from the CPU and attach to the Lab Forensic Computer as drive 1. The jumper on the evidence drive will most likely have to be changed as the drive will now be a slave. Jumper information can be found on the Internet if the drive is not properly marked.

B. Boot the lab computer and write protect drive 1. It is imperative that any examination of the evidence drive proceed only after the drive is properly protected from being modified by an inadvertent write. ***Never boot the lab computer into Win95 while an evidence drive is attached***. Win95 will make modifications to the drive before you will have a chance to write protect it. If you need to run Win95, you must use an image copy of the evidence drive.

C. Scan the evidence drive for virus infection. Record findings on the Forensic Examination Worksheet. **Do not disinfect or modify the evidence drive**.

D. Identify all partitions and examine the drive for evidence of indicated criminality.

E. Perform for each found drive.

Archiving Evidence

There are several methods available to us to archive and safeguard evidence. As the technology develops, higher capacity and faster methods will become available and these guidelines will also evolve.

A. There will be times when the entire evidence drive will need to be duplicated and stored as evidence. These duplicates or "Images" can later be restored to virgin media and examined. Absent the following indicators, the necessity of making image copies of drives is up to the investigator. In the following instances you must duplicate the drive:

- evidence is found in slack space
- the drive is encrypted
- extensive use of passwords
- erased files containing evidence found
- other subterfuge is found
- functionality of original setup must be examined

B. When deleted files are found to contain information evidentiary in nature, the drive *must* be duplicated prior to recovery. Unerasing files, even to another location, **will modify** the evidence drive.

C. Image files from Safeback will be archived to either CD-ROM or TR-4 tape. Snapback images will remain on the tape media used in the original duplication. In all cases, the software utilized to perform the back up will be indicated on the Forensic Worksheet. In cases when duplication or "Imaging" of the evidence drive is not required, files containing information evidentiary in content will be archived to CD-ROM or TR-4 tape collectively. All files from each examination will be copied and stored in their own subdirectory on the CD-ROM or tape.

D. When the functionality of the equipment must be established, a copy of the drive will be utilized for the examination.

Report

Following the examination a Forensic Report will be completed. This report should include all steps taken during the examination, software used and results of the search. Copies of printouts will be placed into the investigation folder along with the completed Computer Evidence Inventory Sheets and the Forensic Examination Worksheets. Copies of evidence derived from the submitted equipment will be given to the case investigator along with a copy of the report.

End procedure.

Computer Investigation & Technology Unit

CITU

To: Sgt. James Doyle, Computer Investigation & Technology Unit

From: Detective Donald Callahan

Date: October 7, 1999

Re: REQUIRED EQUIPMENT FOR DOS FORENSICS

Forensics on DOS Based Systems

Hardware:

Tower Case	6 External, 3 Internal bays	100.00
PCI Motherboard	512K Cache, 5 ISA, 3 PCI Slots, EIDE, EPP	150.00
Processor	Pentium P120	150.00
2.0 GB Hard Drive	Medalist ST32140A IDE	250.00
RAM	32MB EDO RAM	270.00
Graphics	ATI Graphics Expression 2 MB RAM	200.00
Monitor	17" MAG Innovision (Req. Contract)	500.00
SCSI Card	Adaptec AHA-3940U	300.00
CDR-CD ROM	Pinnacle Micro RCD 4X4 (Internal)	1500.00
CD-ROM	NEC 8XI SCSI (Internal)	300.00
Removable Drive Bay	SCSI 5.25"	40.00
Removable Drive Bay	IDE 5.25"	40.00
9 GB Hard Drive	Seagate Barracuda ST-19171N SCSI	2200.00
3 GB Hard Drive	Medalist ST34250A IDE	400.00
Jaz Drive	Jaz SCSI (Internal)	400.00
ZIP Drive	ZIP SCSI (Internal)	200.00
Modem	Hayes Accura 288 V.34 w/Fax (External)	140.00
Mini Tower	4 Bay SCSI, 150 Watt	150.00
Network Card	3Com 900 Ethernet XL PCI Combo 10/100	140.00
Tape Drive DAT	HP SureStor 6000I (Internal)	1100.00
Tape Drive Travan	TapeStor 8000 (Internal)	325.00
Connector	2.5" Hard Drive IDE Adapter	20.00
Adapter	Internal SCSI to External SCSI	40.00
Floppy Drives	3.5" & 5.25" internal floppy drives	70.00

FORENSIC EXAMINATION WORKSHEET

General Information

Date:	Time:	
CITU Investigator:	Shield:	Tax:
CITU Case #:	CITU Log#:	SAR #:
Time Examination Began:		
Time Examination Concluded:		
Storage Location (Locker):		

Notes

Additional Notes on Rear

Additional Notes

CITU#

POLICE DEPARTMENT
CITY OF NEW YORK

June 26, 1998

From: Chief of Detectives

To: Deputy Commissioner, Policy and Planning

Subject : **GRANT PROPOSAL FOR INTERNET CRIMES AGAINST CHILDREN PROGRAM**

1. The Computer Investigation and Technology Unit (CITU) is proposing to submit the following application in response to a FY 1998 Discretionary Program Announcement from the United States Department of Justice Office of Juvenile Justice and Delinquency Prevention entitled "Internet Crimes Against Children Grant".

2. Forwarded for action deemed necessary.

William H. Allee
Chief of Detectives

GRANT PROPOSAL FOR INTERNET CRIMES AGAINST CHILDREN PROGRAM

To: Office of Juvenile Justive and Delinquency Prevention

c/o Juvenile Justice Resource Center

2277 Research Boulevard, Mail Stop 2K

Rockville, MD 20850

1. This grant would be utilized to enhance our existing investigative response to computer facilitated sexual exploitation of children by offenders using the Internet, online communication systems, or other technology and the transmission of child pornography.

2. The CITU was formed within the Detective Bureau in July 1995. Its mission is to investigate computer-related crime, perform investigative analysis of seized computers and provide technical assistance to units within the department and outside law enforcement agencies.

3. The area of investigating computer related crime and the analysis of seized computer systems is an emerging area confronting law enforcement as we enter the next millenium. CITU is considered to be on the cutting edge of this technology, developing procedures and investigative techniques to combat the computer literate criminals. CITU is constantly educating prosecutors and other units in the proper preparation of high tech search warrants, preparing our own warrants when situations arise. CITU introduced the use of electronic mail covers when investigating Internet crime. In addition, CITU is constantly adapting old detective methods to a new area of crime: utilization of electronic undercover identities, electronic stings and the interrogation of the computer literate criminal.

4. The CITU has developed a computer laboratory to analyze seized systems, constantly researching and developing new tools to aid investigators. The forensic lab is a testament to the

inventiveness and dedication to the members of CITU. CITU is constantly adapting programs to use in the analysis of seized systems. In addition, CITU is collaborating with the computer industry in the development of a forensic hard drive duplicator, which will benefit all of law enforcement. CITU has developed protocols and procedures in the seizure of computers and proper execution of computer search warrants.

5. The Computer Investigation and Technology Unit is an outstanding example of inventiveness in addressing an arena totally new to law enforcement. The CITU is one of the few high tech crime units in a major metropolitan area dedicated solely to the investigation of computer related crime. The CITU has been operational since July of 1995 and it totally funded by the Department. Based on the accomplishments, policies and procedures developed, it is clear that the CITU has significantly contributed towards the education and training of not only the NYPD, but all of law enforcement, the business community, educational institutions and the general community.

OBJECTIVE 1

This grant would enhance the abilities of the CITU to conduct pro-active undercover operations, sting web sites. The Internet is a vast resource of vital information, but as with all technology those who prey on children have subverted it for criminal use. The CITU has been involved in the investigation of crimes against children and would further refine existing protocols between existing units within the New York City Police Department to address the victimization of children. The CITU currently interfaces with the following squads during the course of investigations relating to the victimization of children:

Pedophile Squad

Special Victims Squads in each borough

Missing Persons Squad

District Attorneys Squads and Prosecutors

Electronic Crimes Task Force

Federal Bureau of Investigation, New York Field Office

Westchester County DA High Technology Crimes Bureau

The Special Victims Liaison Unit

Advocacy Center in Kings County

Protective Services for Children

The New York City Police Department has long made a commitment to combat child victimization and has taken steps to ensure that the victimization of children in the electronic community neighborhood is addressed as well. As noted above, a multi-agency, multi disciplinary approach has long been the policy of this department.

OBJECTIVE 2

With regards to the Attorneys General's Guidelines for conducting undercover investigations, the policies of NYPD are consistent with those of the Attorney General's and in some cases more restrictive. These policies are enumerated within the Patrol Guide and Detective Guide of the NYPD. In addition the Computer Investigation Unit has been involved in the formulation of policies and procedures with the National Cybercrime Training Partnership and the Office of Juvenile Justice and Delinquency Prevention to formulate policies in these areas. CITU constantly liaisons with other law enforcement agencies to further refine our own practices and procedures.

OBJECTIVE 3

The members of this unit have received extensive training in the investigation of computer-related crime; Internet Investigations and the analysis of seized systems. In recognition of their talent and expertise, members of this unit are constantly requested to speak

and lecture on these topics to law enforcement all over the country. Members of CITU have attended the following courses:

IACIS- International Association of Computer Investigative Specialist- Investigation of Computer Crime.

FLETC- Federal Law Enforcement Training Center- Computer Investigations in an Automated Environment (CIAETP)

NWCCC- National White Collar Crime Center- Cybercop 101

Search-Investigation of Computer Crime

FBI-Advanced Forensics

Protecting Children Online- Investigators Course

Protecting Children Online- Unit Commanders Course

FBI- Advanced Internet Investigations

The NYPD CITU has an established computer forensic lab in operation; YTD has examined over 100 personal computers. It has been the practice to analyze not only evidence seized by members of this department, but to serve as a resource for all law enforcement, assisting law enforcement on the Federal, Local and State Level including the following agencies

United States Customs Service

New York Attorney General

New York City Department of Investigation

Westchester, Nassau, Suffolk County Police Departments

OBJECTIVE 4

The CITU has in operation a case management system for investigative and lab cases. The offenses and investigative results are maintained in the crime reporting system of the department.

OBJECTIVE 5

As a pioneer investigating crimes through the use of computer technology, this unit has developed case protocol based on collaboration, information sharing and the delivery of services, the ultimate aim of any investigation is the identification, apprehension and prosecution of the offender. We have been involved in this area in its nascent stages, and have developed a comprehensive protocol that exemplifies cooperation.

PROTOCOLS ONE: A case is received by CITU directly, either from

a. individual complainant

b. referral by NYPD Detective Squad

c. referral by outside agency

In this scenario, the CITU detective will be the lead investigator, developing information and utilizing technical expertise. In cases where a sexual assault has occurred, the Special Victims squad will be conferred with and lend assistance with their areas of expertise, support services or the victim, interview of the child victim, interrogation of the child predator. It has been our experience that the computer literate child predator interrogation be conducted jointly with a computer literate detective and the expert in dealing with child victimization. In those cases where the child victim is sexually assaulted the Special Victims Squad coordinates counseling and support through the Special Services for Children and the District Attorneys Office.

In cases where no sexual assault has occurred, the Pedophile Squad of the NYPD provides assistance in their expert subject area, interview of the predator.

PROTOCOL TWO-

CITU is requested to assist Special Victims Squad, in these cases the Special Victims is the lead detective and CITU will provide investigative expertise in the areas of evidence retrieval, interrogation assists, locating the offender on the internet.

The Pedophile Squad initiates the case regarding transmission of child pornography or stalking, CITU will assist with technical assistance, seizure and analysis of evidence, and assist in the interview of the offender regarding computer use.

In addition CITU coordinates investigations with the following units:

Missing Children, CITU will scan photos, perform analysis of computers.

Outside Jurisdiction, will coordinate with FBI or ECTF.

Customs and NYAG assist by doing forensic exams.

In addition, CITU has done reverse stings with Postal and Customs regarding child pornography. The Unites States Customs Service's New York Office has referred cases within New York City to CITU for investigation.

These policies and procedures of the NYPD CITU have been the basis for many new computer crime units, and is one of the few units with an actual policy regarding the investigation of these crimes, seizing and preserving evidence from crime scenes and the analysis of seized systems

Problems to be addressed

The purpose of this project is to enhance the investigative capabilities of the New York City Police Department in order to ensure a safer medium for all netizens, especially as they relate to the victimization of children for sexual exploitation.

The proliferation of computers in our society has increased productivity, however on the dark side has presented law enforcement with a totally new set of problems. The explosive growth of computerization has left many in the law enforcement community at a distinct disadvantage as they attempt to investigate the computer-related crime. The continuing drop in the price of the personal computers is making the acquisition of one for the home as common as the VCR.

It is anticipated that this grant will enable this unit to refine and develop techniques to address this new arena of criminal activity, and serve as a blueprint for all law enforcement. Business and educational institutions utilize the computer to automate and increase the flow of information, but the criminal element has discovered this new technology and has subverted it for illegal use. As the popularity of the Internet grows, and our children become computer literate in grade school, the dangers lurking about become more ominous. These new dangers include the sexual predator targeting the young, using the anonymity and structure of the Internet to hide, waiting to victimize. These predators have embraced this new technology, achieving instant gratification, and an efficient means of cataloging and storing their trophies, no longer do they have to travel outside, and they are coming right into the homes of their victims. The activities of the sexual predator do not affect only the victim; it reaches the family and possibly the community. The computer of the sexual offender is a repository of evidence of additional victims and the scope of the predators' actions; evidence that is not discovered until the analysis of the system is completed.

Goals and Objectives

The need to address what is a rapidly growing problem that targets children is the impetus for the NYPD to apply for this grant. The implementation of this program will enhance the productivity of the CITU and enable it to be more proactive. The ultimate goal of this program

will be to enhance the operations of NYPD CITU, increase our ability to investigate computer related crime, specifically those that solicit children for sexual exploitation, distribution of child pornography and those cases where the offender exhibits an aggressiveness to travel. The program would identify actual and/or potential victims of computer related sexual predator crimes and develop a protocol by which counseling and support will be delivered to victims and other affected members. The policies and procedures developed over the last three years by this unit have become a blue print for other units, and this grant will create a unit that could serve as the model for the nation, establishing a paradigm which will reduce the risks for our children and increase the investigative abilities in identifying and incarcerating sexual predator offenders.

The New York City Police Department Police will continue to establish initiatives that will accomplish these objectives, and the following are the objectives defined, which are measurable and attainable.

1. Investigate computer related crimes where a sexual predator locates, identifies, and solicits children over the Internet, the trolling traveler. Computer technology continues to change at an exponential rate, and this program would provide investigators the tools necessary to keep pace with the criminal element.

2. Utilize current forensic computer analysis to identify additional victims of computer related crimes and provide those victims and their families with the necessary support and counseling. These crimes go beyond the violation of penal law statutes, these acts are so abhorrent that the victimization does not end with prosecution and incarceration of the offender, the scars will be carried forever.

3. Utilize current procedures for undercover online accounts that comply with the Attorney General's Guidelines for Undercover Operations and the policies of the NYPD.

4. Continue to deliver lectures and presentations to law enforcement agencies, civic, business and educational groups regarding computer crime, On line safety, Protecting Children Online, and proper handling of computer evidence. Past presentations to the community will provide guidelines for parents, Internet awareness and the victimization that can occur. The handouts and brochures provided by the National Center for Missing and Exploited Children have been an integral part of our On Line Safety presentations.

5. In conjunction with the Deputy Commissioner of Community Affairs, an outreach program will be developed to publicize the new endeavor with professionally produced brochures for distribution in the schools and community.

6. Develop and implement an AEducational Outreach Program" in the Community Affairs Division where an awareness program would be delivered to the educational community. The program will be designed to help educators instruct students on both the benefits and dangers of the Internet, and to stress responsible surfing of the net.

7. Continue to develop relationships with various federal, state, county, and local law enforcement agencies to efficiently and effectively conduct criminal investigations and share information relevant to these investigations.

8. Establish lines of communication with Child Abuse Units, Special Victims Squads, Missing Persons Squads, and Advocacy centers to enhance the existing NYPD website and any other private site that deals with the victimization of Children. Information on counseling and support services, including the Cyber Tipline, would be provided to the victims of Internet predators.

9. Establishment a database, modeled after the Florida Department of Law Enforcement, utilizing legally releasable information from the Sexual Offender Monitoring Unit, that will serve a repository for information on both sexual predators and individuals utilizing the

Internet to victimize children. The NYPD would make the information available to law enforcement within existing guidelines and policies of the Department.

Project Design

The New York City Police Department recognized that criminal activity and the use of high technology and computers was a looming threat, and to address it the CITU was created in May of 1995. The CITU is one of the pioneers in the investigation of computer related crime, and one of the first units dedicated solely to the investigation of computer crime and the analysis of seized computers. The CITU has witnessed the increasing growth of computer related crime and the increase in the victimization of children, the sexual exploitation and solicitation of children and the continued problems with the distribution and possession of child pornography. Currently, the NYPD has a Special Victims Squad in each borough, a pedophile squad, and a Missing Persons Squad who interact to combat the victimization of children.

The personnel assigned to CITU have generated and earned the respect of their peers and gained a national and international reputation for being one of the leaders in the investigation of computer related crime. As such, the NYPD has provided investigative and technical assistance to a plethora of federal, state, county and municipal law enforcement agencies regarding their criminal investigations involving the sexual exploitation of children and child pornography.

CITU continue to generate and investigate criminal activity involving the sexual exploitation of children and child pornography. Numerous cases have been resolved where suspects have been arrested and convicted for the aforementioned crimes.

CITU has established an undercover Internet account with the profile of a juvenile to locate and identify sexual predators who would solicit children. Utilizing chats and other investigative techniques, electronic conversations were held with these suspects and arrests made after child pornography was transmitted, a meet was arranged or a sting conducted with the

controlled delivery of Child Pornography. The CITU plans to establish and implement additional undercover accounts with Internet Service Providers, utilizing the excellent rapport developed through past investigations.

The investigative analysis performed by CITU of computer equipment seized during an investigation is another aspect of the operation of this unit. These examinations are performed by personnel trained by recognized training entities, and members have achieved expert status in court based on their expertise and training. Investigative analysis has yielded evidence to enhance investigations, support prosecution and identify additional victims. The CITU is a recognized expert in this area, having received requests from police agencies all over the world for assistance in setting up their own units, Massachusetts Attorney General, Philadelphia, Los Angeles, Knoxville, and the Isle of Malta) Unit personnel have conducted forensic examinations for a wide variety of law enforcement agencies. These forensic examinations require the duplication of evidence and analysis of the duplicated work copies. Unit personnel will continue to perform these examinations but plan to purchase additional duplication equipment to shorten or even eliminate the elapsed time from the request of the examination to the actual completion, thereby shortening the elapsed time from delivery of evidence to the completion of the analysis.

CITU personnel will continue to provide training to law enforcement personnel regarding the investigation of computer related crimes. A major portion of this training pertains to the sexual exploitation of children and child pornography. Investigators are taught about the behavior of the sexual predators, their victims, and equipment utilized to commit these offenses. Investigators are also taught how to properly recover and preserve the confiscated evidence.

Training initiatives are also implemented by lectures and presentations to the community. Unit personnel have spoken to parents, teachers, business leaders, and administrators about the Internet and how to protect the children while online. Numerous letters of appreciation have been received that request future presentations.

The technical and investigative expertise of members of CITU has lead to many requests for these members to participate on local, county, state and federal committees responsible to develop and implement a curriculum for other training programs directed at law enforcement investigators and supervisors.

The implementation of this program will not alter the responsibilities of CITU, new initiatives will be implemented that would generate liaison between other law enforcement agencies and the people of New York City.

Unit personnel will assist Special Victims Squads, Missing Persons Squad, and the Pedophile Unit refine their Web sites on the Internet, which will provide support, service and counseling to victims of Internet crimes, in addition to continuing to educate these groups about Internet Safety.

Finally, the unit will continue to develop liaison with other law enforcement units within and outside the department that would be comprised of law enforcement agencies from various levels of government, prosecutorial agencies, and governmental agencies that provide assistance and counseling service to the child victims and their families. CITU has an excellent working relationship with these units and the investigations conducted by the unit have been multi agency/multi jurisdictional levels and have been brought to successful conclusion which has brought credit to the New York City Police Department.

This work plan does not diverge from the unit's current mission and the outline of this program is linked to the achievement of the project objectives. These new initiatives will be embraced by the CITU, and we will continue to be at the forefront of developing techniques and practices which have made this unit so respected among its peers.

The Office of Public Information and The Community Affairs Division will be requested to announce these new initiatives and enlist existing contacts to further enhance implementation

of this program. It is anticipated that this phase of the workplan could be developed and implemented within 6 months upon receipt of the project award.

We will assist the units within the Department in enhancing their Web Pages within a 3-month period of the grant approval. This relationship will generate public awareness of the sexual solicitation and exploitation of children on the Internet and provide support services and counseling to the identified victims.

The CITU will construct a database program to catalog sexual predators with the assistance of the NYPD Missing Persons Squad, Special Victims Squad, Sex Offender Monitoring Unit, Pedophile Squad and will be designed to be shared among law enforcement agencies within existing law and guidelines of the Department. This database could be implemented within 7 months of the project award.

Management and Organizational Capability

The CITU is an investigative unit of the Detective Bureau under the Special Investigations Division. The current staffing is

One Lieutenant, Commanding Officer, responsible for overall operation of the unit

Two Sergeants, one handling Investigation, the other the Computer Lab

Six Detectives and Two Police Officers who conduct investigations and analysis of seized systems

There is a current proposal to assign more investigators and computer literate memebers of the Department to this unit.

It should be noted that all members of CITU have Federal Marshall status.

The Lieutenant is the Commanding Officer and is responsible for the overall operation of the unit. The sergeants coordinate investigative overview and direction, administrative functions and lab operations.

The Sergeants and Investigative personnel, four Detectives and two Police Officers conduct computer related criminal investigations and these cases are recorded according to current NYPD Detective Bureau procedures. These members conduct analysis of seized computer evidence and generate a concise report, which has been reviewed and approved by the Departments Legal Bureau. Training programs and lectures that are provided to various law enforcement agencies, civic, business and educational groups are developed and implemented by the personnel assigned to CITU. Unit personnel coordinate information relevant to prosecutions and assist efforts by the Special Victims Squads to provide services and counseling to the various victims of computer crimes.

CITU has earned an international reputation for the investigation of computer-related crime and the analysis of seized systems. The awarding of this grant will increase our productivity and provide additional training and equipment, which will enable CITU to continue to address this new investigative arena. This program will allow the new implementation of the initiatives outlined in the AProject Design" , providing the means to assist children who have been victimized by the sexual predators on the Internet.

CITU has developed an extensive network among other law enforcement members involved in the investigation of computer related crime, having created a database of over 800 individuals all over the world. CITU share their information through networks developed at training sessions and membership in high technology oriented associations. Members of this unit are members of the High Technology Crime Investigators Association, International Association of Computer Investigation Specialists, National White Collar Crime Center Association, American Society of Industrial Security, National Cyber Crime Training Partnership, High Technology Crime Network Association, and Protecting Children On-Line Group, in conjunction with the National Center for Missing and Exploited Children, the Department of Justice, and Fox

Valley Technical College, to develop a national curriculum for law enforcement officers training program and were participating members in the On Line Family Summit.

The investigation of Internet crimes against children has been part of the mission of CITU since its inception and will always be a priority issue for this unit.

The District Attorney's offices of Manhattan, Kings, Queens, the Bronx andd Richmond County will continue to support the investigative efforts of this unit.

Budget

1. Equipment: $215,000 Total

The current computers utilized to conduct forensic ananlysis should be replaced by current state of the art computers on a yearly basis. The current computers have been adapted for use as investigative workstation with the installation of peripheral cards, tapes drives, removable drive bays, large capacity drives and CR-Rom writers. Emerging technologies demand more robust computer processors, larger memory and storage capacity and new software that will require CITU to upgrade their systems.

Inherent with the operation of CITU is the challenge of dealing with a rapidly changing environment with technological advancements occurring on an exponential basis. The very nature of the computer industry and the design of new products does not lend itself to budget forecasting or the ordering of products which may not yet exist. The criminal element utilizing computers will have the latest systems, a distinct disadvantage for law enforcement. CITU, in order to properly investigate computer related crime and conduct investigative analysis of seized systems need to be able to avail themselves of the latest technology. Software is another highly volatile field with rapidly changing dynamics. The ability to procure new products and properly licensed software is critical to present evidence in court, address liability

issues and potential embarrassment to the department. This grant will provide funding to keep pace with current trends in the computer industry and the computer literate criminal.

These expenditures will be for infrastructure, recurring expendable supplies, investigative software, investigative equipment, computer peripherals for evidence analysis, archiving and storage.

a. Expendable Supplies- $35,000

The expendable supplies are critical to the operation of CITU to maintain a high level of delivery of services and must be purchased on a recurring basis. The computer media identified is used to store evidence for later courtroom presentation.

Toner cartridges for laser printers, ink for printers and plotters, paper supplies, media of different types and capacities, supplies necessary for the execution of search warrants and seizures. Film for cameras, tape for video recorders and audio recorders.

b. Investigative Software- $35,000

To maintain compliance with software copyright laws and provide investigators with latest tools. Software development evolves rapidly, a current concern will be the introduction of 32 bit based software programs which may necessitate expenditures on this software.

Software necessary to examine hard drives, floppy drives, tape media, password breaking software, network software, graphics packages, presentation software, software necessary to produce reports, spreadsheets, communication software, internet investigative software, data recovery, technical information software, forensic software packages

c. Investigative Equipment- $75,000

Digital Cameras, Covert recorders, Covert communication devices, VCR, Video Recorders, caller id boxes, undercover internet accounts, fictitious post office boxes, Cellular phones, cellular modems, radio modems for connection to NYPD mainframe, skypagers for undercover invests, binoculars, carrying cases for investigative equipment

d. Infrastructure-$70,000

Workbenches and laboratory equipment(Chairs, monitor arms, lights), media safes, replacement forensic workstations, laptops, tape drives, optical drives, T-1 line with hardware for high speed access, high speed modems, tools, high quality printers, plotters, scanners, network cards, cabling, hubs, large monitors, Uninterrupted power supplies with filtering, hard drive duplicators, media capture devices, microscope, oscilloscope, chip tester, diagnostic equipment.

2. Training $65,000

In order to maintain our ability to investigate high technology crimes, it is crucial that members of CITU attend specialized training that often entails travel out of state and overnight lodging. The training required is not available within the department.

Protecting Children On-Line- Offered by OJJDP/NCMEC no cost

Unit Commander Training-Offered by OJJDP/NCMEC no cost

Child Sexual Exploitation-Offered by OJJDP/NCMEC no cost

Responding to Missing and Abducted Children-Offered by OJJDP/NCMEC no cost

CRIMINAL INVESTIGATIONS IN AN AUTOMATED ENVIRONMENT TRAINING PROGRAM (CIAETP)

Program Title: SEIZED COMPUTER AND EVIDENCE RECOVERY SPECIALIST TRAINING PROGRAM (SCERS)

Program Title: FRAUD AND FINANCIAL INVESTIGATIONS TRAINING PROGRAM (FFITP)

Program Title: INTERNATIONAL BANKING AND MONEY LAUNDERING TRAINING PROGRAM (IBLMTP)

Program Title: TELECOMMUNICATIONS FRAUD TRAINING PROGRAM (TCFTP)

Program Title: ELECTRONIC SOURCES OF INFORMATION TRAINING PROGRAM
(ESOI)

Program Title: Computer Intrusion Investigations- Offered by CSTAC ($945.00) per attendee. In NYC

Program Title: Law Enforcement Forensic Computer Training- Offered by IACIS ($895.00) per attendee. Plus travel, lodging and meals.

A subsection of the training budget will encompass the production of pamphlets, roll call videos, professional quality brochures, equipment for presentations for the educational, business and civic populations.

3. Undercover Funding- $20,000

These investigations will require expenditure of funds to initiate buys of pornography, pay for undercover accounts, post office boxes, setting up fictitious companies, and other investigative expenses

Computer Investigation & Technology Unit

CITU MEMO

Date: October 7, 1999

Subject: ACCEPTING EVIDENCE FOR ANALYSIS

The following procedure will be followed when accepting computer evidence for examination by C.I.T.U.

Receiving Computer Equipment as Evidence

A. When accepting evidence from a member of the service, ensure that the following forms are delivered with the property as per **Interim Order 74** dated 11/14/96:

- Original voucher with 1st white and yellow copy;
- Completed Request for Laboratory Exam
- Completed Letter of Transmittal-Evidence
- Copy of the Search Warrant

B. Make an entry in the Computer Forensics Log completing all captions. Utilizing the next available log number, transfer this number to the upper right corner of the Request for Laboratory Exam and the Letter of Transmittal-Evidence.

C. Sign both forms and return to the delivering M.O.S. the last copies of each.

D. Affix a label to each item received indicating the date, C.I.T.U. log number and the voucher number.

E. Start an examination folder for the case:

- Left side - Vouchers, Request for Laboratory Exam, Search Warrant, Letter of Transmittal-Evidence and DD5s
- Right side - Forensic Report, Inventory and Forensic Examination Worksheet

F. Secure all property in a locker with the case folder affixed to the outside.

End of procedure.

Policies and Procedures
Computer Investigation and Technology Unit

Submission of Evidence:

1. The following MUST be submitted with evidence to be analyzed:
   a. Original voucher, second white copy and yellow copy of Property Clerks invoice when property has been delivered directly from precinct.
      - If property has been removed from property clerk, the property clerk storage number must be on the copy of the voucher.
      - In Federal Cases, the property Transfer receipt will be accepted in lieu of voucher.
   b. Request for lab analysis
   c. Letter of Transmittal
   d. Copy of Search Warrant, Subpoena or Consent.

IF ANY OF THE ABOVE PAPERWORK IS NOT PRESENT, SUBMITTING OFFICER WILL BE DIRECTED TO RETURN TO COMMAND WITH PROPERTY. UNDER NO CIRCUMSTANCES WILL PROPERTY BE ACCEPTED AT CITU WITHOUT THE ABOVE FORMS.
(Ref. IO 74, 74-1, s. 1996)

2. Review paperwork for completeness and accuracy.
   a. Check voucher against property submitted, special attention to description on voucher and property submitted. In some cases CITU member will have to prepare a DD5 for clarification of evidence submitted. In all cases where there is a discrepancy between the voucher and property submitted a CITU supervisor will be notified.
   b. The request for lab analysis will be prepared for all evidence submitted, including outside agencies. The submitting officer must include a concise summary of information requested, do not accept forms with nebulous requests such as "data, evidence, or everything."
   c. The letter of transmittal is the submitting officer's receipt and indicates chain of custody; it must mirror the voucher.
   d. The search warrant, subpoena or consent is the authorization for CITU to examine the contents of evidence submitted it must be proper according to rules of evidence and training received by CITU.

3. Once the paperwork and property has been verified, the CITU member will begin the logging in process.
   a. Obtain a case folder, obtain the next log # from the evidence log, affix the log number to the folder in the "CASE NO._____" caption. The log number will be suffixed by the year, e.g. 61/97. Complete captions on folder.
   b. Make entries in Log, completing all captions including phone number of assigned investigator.

c. Affix Log Number to original voucher in the top right corner of voucher, above the perforation. Enter Log # and CITU member on Request for Lab Analysis and also on Letter of Transmittal in the Laboratory Serial Number Column. The Letter of Transmittal should have been signed by D.O. at Precinct of record, the messenger signature is the delivering officer, and the Police Laboratory Evidence Clerk is the receiving member of CITU. The CITU member will also indicate his shield number on the line. Time Stamp the Letter of Transmittal and Request for Lab Analysis prior to separating copies.
d. Make two copies of voucher.
e. Distribute each form as follows:
   Voucher- Original will have affixed to it the pink copy of the letter of transmittal, and the pink copy of the Request for lab analysis. This package will be forwarded to CITU supervisor.
   Letter of Transmittal- Original will be placed in Analysis folder, blue is returned to submitting officer, pink is forwarded to CITU supervisor with original voucher.
   Request for Lab Analysis -Original will be placed in Analysis folder, blue is returned to submitting officer; pink is forwarded to CITU supervisor with original voucher.
f. Prepare Analysis folder as follows:
   On left hand side the following:
   Copy of Voucher(s) or Submitting Agency Property Form
   Original Request for Lab Analysis
   Original Letter of Transmittal
   Search Warrant, Subpoena or Consent
   Any other paperwork prepared in connection with investigation, which may be considered Rosario material.
g. Store property in cabinets, placing second photocopy of voucher on outside of cabinet in plastic sleeve to indicate location, attach card stock evidence tracking sheet.
h. Forward folder to CITU supervisor, analysis will be assigned to CITU member by supervisor. Supervisor will make entries into database, indicating number of CPU's, hard drives or floppies on each voucher in the voucher table.
i. CITU supervisor will forward folder to investigator for analysis. Original Voucher will be placed in file cabinet pending completion of analysis and subsequent forwarding of property to property Clerk.

END PROCEDURE: SUBMISSION OF EVIDENCE.

Policies and Procedures
Computer Investigation and Technology Unit

Analysis of Evidence:

1. Remove evidence from locker, make notation of time and items removed on attached tracking sheet. Record all steps on the Investigative Analysis Worksheet. *(DON UPDATE FORM TO CHECKOFF BOXES)*
2. Remove cover from CPU and inventory the following:
   - Hard drives connected and disconnected
   - Installed cards
   - Number and type of ram chips
   - Processor

   Itemize all of the equipment on a Computer Evidence Sheet. Each CPU gets listed on a separate sheet along with its associated peripherals.
3. Disconnect the power to the hard drives.
4. Using a write protected floppy inserted in the A: drive, power on the computer and access CM.O.S. Ascertain the system date, time, boot sequence, installed ram and the hard drive parameters. Enter the information in the appropriate fields on the Inventory Sheet.

EXAMINATION OF EVIDENCE

The investigative analysis of all evidence is defined by the request of the submitting investigator and the scope of the search warrant. Analyzing the hard drive is for evidence of both and incriminating and exculpatory nature. The analysis should be unbiased in its approach. Each analysis is different and the methods used to recover evidence will change from case to case. All actions must be recorded on the Investigative Analysis Worksheet *(DON RENAME THIS FORM).* **ONLY REGISTERED LICENSED COPIES OF SOFTWARE WILL BE USED. (APPENDIX A lists all software registered to NYPD/CITU) DON.**

1. The first step in the analysis procedure will be to make an exact copy of the subject's hard drive. No analysis will be performed on original hard drives. At present time, the IMAGEMASSTER will be utilized to make the copy.

   NEED: Certification from IMAGEMATSR that copies are exact.
   Will need training, certificate and maybe independent testing of the LE version. DON ANY IDEAS to verify this.. CRC HASH?
2. Upon completion of the copy procedure, an image of the hard drive can be undertaken on a separate workstation. *NAMING STANDARD OF IMAGE FILES*
3. Attach the copy of Drive 0 from the subjects CPU and insert it into the CITU Workstation as Drive 1. This will necessitate setting the jumpers of the copy as drive 1. Jumper settings can be obtained form the Internet. Note that when examining the subject drive as a slave in the CITU workstation it will be Drive D, note in the Investigative report this is due to DOS standards in the naming of drives.
4. Power up the lab computer and access the CMOS, you must dial in the original drive parameters from the subjects drive when utilizing copies made by ImageMasster.
5. Prepare a scratch drive on the workstation to act as a repository for evidence recovered, directory outputs, reports generated by RED X, MH-IDE, erased files recovered. *DON NEED REDX FOR WIN 95* Reports generated should be named in the following fashion: *LETS GET A STANDARD*

6. RUN MH-IDE, output report to scratch drive
7. RUN CHKDSK on Target Drive, output report to scratch drive
8. Perform a virus scan on the target drive, output report to scratch drive. Do not disinfect or modify the drive.
9. Perform a REDX on Target report, output report to scratch drive. If 32 bit fat, output directory listing to scratch drive. *NEED TO DISCUSS THIS*
10. Run Norton Utilities 8.0, Unerase, sort the files by prognosis and recover in order to the scratch drive. DO NOT RECOVER TO ORIGINAL DRIVE, YOU MAY OVERWRITE OTHER ERASED FILES. REVIEW DOCUMENTION OF UNERASE. RECOVER FILES TO A SEPARATE UNERASED DIRECTORY ON SCRATC DRIVE.
11. View recovered files through File Manager and Quickview Plus
12. WINDOWS 95: Or those cases where we have to boot the target drive as drive 0 in CITU Workstation.
13. OTHER THINGS TO REVIEW:
    INI Files
    Registry
    The actual files on hardrive
    END PROCEDURE

SAR PREPARATION

FILL OUT LOG, TAKE NEXT NUMBER
LOG INTO NETWORK
ENTER DETAILS
PREPARE SAR
PRINT SAR
SUBMIT

CASE MANAGEMENT

Cases b

Phone

Written
Make Folder
Folder Storage

Initial receipt
Catch order
Bring to attention of boss

Initial 5

Sub 5's

Entry into computer

Monitor

TO: **All Members CITU**

FROM: **Sgt. James Doyle**

DATE: **June 30, 1998**

RE: **Undercover Protocol – On line activities**

These record keeping procedures and protocols are being published to reinforce the New York City Police Department's commitment to professionalism and to standardized the approach to the investigation and prosecution of cases developed through Online activities. The Internet and particularly this area of law enforcement is an extremely new area of law and is subject to challenges both by the defense bar and the Courts. As we pursue our investigative objectives, we must continue to show a Agood faith effort≅ in investigating these cases in the absence of any established case law in the area. We have been extremely successful in our efforts. This protocol is meant as a guide and should be followed as closely as possible to further our operational objectives. Deviations from the protocols can be made on a case by case basis as investigative situations arise.

RECORD KEEPING PROTOCOL
REVISED

Undercover Participation Record Keeping:

All undercover investigators MUST document the date of each and every undercover activity, the name of the officer, and the undercover identity used for each instance, and the time on and off for all undercover activity. One such notebook is used for each area of undercover activity, and is located next to the internet machine. (i.e. a notebook is maintained for activity on America Online, one for activity on Internet Relay Chat, etc.) **If it is not logged-in, it did not happen.**[1]

---

[1]As a general rule, all on-line activity for Operation Rip Cord should only take place on equipment owned and/or licensed by the New York State Attorney General=s Office.

Online Activity Record Keeping

Officers MUST maintain complete records of all online activity. Officers will utilize the software present in both the America Online program and the Internet Relay Chat program to do so. These programs are referred to as Alogging≅ programs. There are two kinds of logs that are created; they are called Achat logs≅ and Asession logs≅. Both types of logs document all user interface with the activity occurring in the computer program and all other Aonline≅ activity. All logs are started after the initialization of the INTERNET programs, but before any online activity occurs. **If it is not logged-in, it did not happen.**

File Naming Convention (Logs)

All on line activity, for each session MUST be logged to a clean 3.5 A diskette. The diskette will be inserted into the A:\ drive prior to sign on. Once the logging option is enabled the log files will be named accordingly:

1) Chat log will be opened and named (A:\(Date of activity)≅chat.log≅ - i.e. **1223chat.log**);
2) Session log will be opened and named (A:\(Date of activity) Asess.log≅ - i.e. **1223sess.log**)
3) Log Instant Messages box will also be checked to log instant message chat between undercover officers and targets.
   There should be a check mark in the box to indicate enabled.

After the undercover activity is completed and prior to signing off AOL, the undercover officer MUST CLOSE ALL LOGS BEFORE EXITING THE PROGRAM. This will enable the log file to be written to the floppy diskette. The disk is then write protected by opening the write protect notch on the floppy diskette located on left side of diskette. The disk is then re-inserted into the a:\drive and copies of the logs are made to the C:\OLI\OLLOGS ("On Line Investigations, On line Logs")directory on the hard drive for later use in investigative activity. The floppy disks are once again removed and are then filed in a locked filing cabinet. The placement of these floppy disks into storage is noted by the creating officer in a hard copy notebook documenting the floppy disk label, date and the accessing officer. These floppy disks are never accessed again, but are maintained as original recordings. **If there is no diskette, it did not happen.**

Instant Messages

It is common for undercover officers and targets to converse on line using the Instant Message (AIM≅) function of AOL. When ever IM=s are used to

converse electronically with a target, a record of such conversation should be made for ease of accessing this information for later investigation needs. It is not mandatory because the information is also recorded through the overall logging function previously described in this memo. The process of recording and saving the IM=s is as follows:

1) While an IM box is open and the undercover officer is conversing with a target, it is important that the IM box remain open throughout the entire conversation.

2) The IM box can be minimized but should never be closed or portions of the entire conversation will not be saved.

3) Once the conversation has concluded, the text of the box should be highlighted and the file - save as - function invoked. The file should be named as follows:

(AIM(target name).log≅) - i.e. IMRUDO99.log.

The file will default to the a:\ drive because all other chat and session logs are all ready being saved to that drive. Upon completion of the undercover activity, these files should be printed out and put in the appropriate case files for reference by the assigned investigator preparing the search warrant.

Directory Tree Structure

The following directory tree format on the investigative computer hard drive will be implements to aid the investigators in evidence collection and retrieval. The directories and sub-directories are logically established on the hard drive. The Directory Tree structure is as follows:

C:\..

\OLI

\OLILOGS - were copies of all logs are kept.

\OLTARGETS

\AOLREFER

\UNWORKED (root entries are targets for which no further activity contemplate

\ACTIVE

\SCREEN NAME of TARGET (Those targets being investigated)

\IMAGES – images received are stored

\LOGS-

\TO - All E-mail sent to Target by U/C
\FROM - All E-mail received from Target
\TXT - Text E-mail messages provided by AOL

E-Mail Download Record Keeping

When e-mail is generated by on-line activity, the downloading of the resulting messages is specifically recorded. E-mail generally arrives in two forms-text messages, and text messages accompanied by computer generated graphics. In either case, the text messages are recorded in the same way. Prior to any email downloading, the downloading officer MUST first establish target directories and sub directories in the appropriate manner as described above. The actual downloading and record keeping for graphics is described in the following section.

A hard copy notebook in which the downloading officer MUST record his/her name, the date and time of the downloading, and the undercover name of the account that is downloaded. The downloading of text messages and text messages that also include an attached computer generated graphic image is done using the logging option of the program from which the mail was generated. Before beginning the downloading activity. **This E-Mail log is created by opening the ASession Log≅ option on AOL.** In addition, the downloading officer should check the Log Instant Messages box in the event other targets IM the downloading officer during the download process. The log file is saved to the computers hard drive and the following name is given to the file:

C:\OLI\OLLOGS\ (date of download) Aemai.log≅ - i.e 1223emai.log.

The downloading of computer graphic image files are directed to the target AIMAGES≅ sub directory responsible for its transmission. Often times, a target will send the same computer graphic image on more than one occasion. Each transmission of the computer graphic by the target is potentially a felony violation. Accordingly, each picture needs to be saved regardless of how many times it is sent. If the computer prompts the download officer that a AFile Already Exist≅ in a targets subdirectory, the downloading officer will create a new sub directory under the APICS≅ sub directory named ADUPES.≅ Each time the computer prompts the downloading officer that a AFile Already Exist≅ a new sub directory will be created (DUPES2; DUPES3; etc).

In addition each E-mail message which accompanies the graphic image MUST be saved in the target AFrom≅ sub directory. All E-mail associated with a particular target can later be printed by the investigator assigned to the search warrant application or can be printed and forwarded to the appropriate law enforcement agency upon a referral.

Contact with Targets through E-mail

At times it is necessary to further contact targets and engage them (him/her) in further E-mail conversation. When ever an undercover officer sends an E-mail to a target, that activity MUST be recorded and saved. In addition, any E-mail response from the target MUST also be recorded and saved. Accordingly, when ever an E-mail message is sent to a target, the message will be saved in the following manner using the **File - Save As** function:

E-MAIL SENT TO:

C:\OLI\OLTARGETS\UNWORKED\ **Target screen name \LOGS\TO.**
The name of the file will be in the following format: (first 2 letters of name, date, ATO.wpd≅) - i.e. TA1223TO.wpd.)

E-MAIL RECEIVED FROM:
C:\OLI\OLTARGETS\UNWORKED\ **Target screen name \LOGS\FROM.**
The name of the file will be in the following format: (first 2 letters of name, date, AFR.wpd≅) - i.e. TA1223FR.wpd)

NOTE: In many instances, numerous E-Mails are received from the target by the U/C on the same date. The file will be named with alphabetical letters a,b,c,d, etc. to denote multiple E-Mail message occurring on one date, i.e. TA1223Fa.wpd.

All E-mail contact between the undercover and the target should be printed out and put the case folder for reference by the assigned investigator preparing the search warrant.

Seizure/Analysis of Evidence

It is the standard operating procedure of the undercover operation that no violative files of any kind are ever transmitted, only received. Based on the reception of these files, search warrants are sought to search for the computer or related computer storage device that holds the file that was originally used in the transmission to the undercover. These computers or computer storage devices are then forensically searched by a computer forensic investigative specialist for evidence or presence of these files.

Additional equipment is used for the analysis of seized computers. The originals must be secured as evidence and a Aclone≅ hard-drive created to function as a working copy. At least one hard drive with memory capabilities similar to that set forth earlier in this memo must be obtained for this purpose.

TO: **All Members CITU**

FROM: **Sgt. James Doyle**

DATE: **June 30, 1998**

RE: **Undercover Protocol – On line activities**

These record keeping procedures and protocols are being published to reinforce the New York City Police Department's commitment to professionalism and to standardized the approach to the investigation and prosecution of cases developed through Online activities. The Internet and particularly this area of law enforcement is an extremely new area of law and is subject to challenges both by the defense bar and the Courts. As we pursue our investigative objectives, we must continue to show a Agood faith effort≅ in investigating these cases in the absence of any established case law in the area. We have been extremely successful in our efforts. This protocol is meant as a guide and should be followed as closely as possible to further our operational objectives. Deviations from the protocols can be made on a case by case basis as investigative situations arise.

RECORD KEEPING PROTOCOL
REVISED

Undercover Participation Record Keeping:

All undercover investigators MUST document the date of each and every undercover activity, the name of the officer, and the undercover identity used for each instance, and the time on and off for all undercover activity. One such notebook is used for each area of undercover activity, and is located next to the internet machine. (i.e. a notebook is maintained for activity on America Online, one for activity on Internet Relay Chat, etc.) **If it is not logged-in, it did not happen.**[1]

---

[1]As a general rule, all on-line activity for Operation Rip Cord should only take place on equipment owned and/or licensed by the New York State Attorney General=s Office.

Online Activity Record Keeping

Officers MUST maintain complete records of all online activity. Officers will utilize the software present in both the America Online program and the Internet Relay Chat program to do so. These programs are referred to as Alogging≅ programs. There are two kinds of logs that are created; they are called Achat logs≅ and Asession logs≅. Both types of logs document all user interface with the activity occurring in the computer program and all other Aonline≅ activity. All logs are started after the initialization of the INTERNET programs, but before any online activity occurs. **If it is not logged-in, it did not happen.**

File Naming Convention (Logs)

All on line activity, for each session MUST be logged to a clean 3.5 A diskette. The diskette will be inserted into the A:\ drive prior to sign on. Once the logging option is enabled the log files will be named accordingly:

1) Chat log will be opened and named (A:\(Date of activity)≅chat.log≅ - i.e. **1223chat.log**);
2) Session log will be opened and named (A:\(Date of activity) Asess.log≅ - i.e. **1223sess.log**)
3) Log Instant Messages box will also be checked to log instant message chat between undercover officers and targets.
   There should be a check mark in the box to indicate enabled.

After the undercover activity is completed and prior to signing off AOL, the undercover officer MUST CLOSE ALL LOGS BEFORE EXITING THE PROGRAM. This will enable the log file to be written to the floppy diskette. The disk is then write protected by opening the write protect notch on the floppy diskette located on left side of diskette. The disk is then re-inserted into the a:\drive and copies of the logs are made to the C:\OLI\OLLOGS ("On Line Investigations, On line Logs")directory on the hard drive for later use in investigative activity. The floppy disks are once again removed and are then filed in a locked filing cabinet. The placement of these floppy disks into storage is noted by the creating officer in a hard copy notebook documenting the floppy disk label, date and the accessing officer. These floppy disks are never accessed again, but are maintained as original recordings. **If there is no diskette, it did not happen.**

Instant Messages

It is common for undercover officers and targets to converse on line using the Instant Message (AIM≅) function of AOL. When ever IM=s are used to

converse electronically with a target, a record of such conversation should be made for ease of accessing this information for later investigation needs. It is not mandatory because the information is also recorded through the overall logging function previously described in this memo. The process of recording and saving the IM=s is as follows:

1) While an IM box is open and the undercover officer is conversing with a target, it is important that the IM box remain open throughout the entire conversation.

2) The IM box can be minimized but should never be closed or portions of the entire conversation will not be saved.

3) Once the conversation has concluded, the text of the box should be highlighted and the file - save as - function invoked. The file should be named as follows:

(AIM(target name).log≅) - i.e. IMRUDO99.log.

The file will default to the a:\ drive because all other chat and session logs are all ready being saved to that drive. Upon completion of the undercover activity, these files should be printed out and put in the appropriate case files for reference by the assigned investigator preparing the search warrant.

Directory Tree Structure

The following directory tree format on the investigative computer hard drive will be implements to aid the investigators in evidence collection and retrieval. The directories and sub-directories are logically established on the hard drive. The Directory Tree structure is as follows:

C:\..

\OLI

\OLILOGS - were copies of all logs are kept.

\OLTARGETS

\AOLREFER

\UNWORKED (root entries are targets for which no further activity contemplate

\ACTIVE

\SCREEN NAME of TARGET (Those targets being investigated)

\IMAGES – images received are stored

\LOGS-

\TO - All E-mail sent to Target by U/C
\FROM - All E-mail received from Target
\TXT - Text E-mail messages provided by AOL

E-Mail Download Record Keeping

When e-mail is generated by on-line activity, the downloading of the resulting messages is specifically recorded. E-mail generally arrives in two forms-text messages, and text messages accompanied by computer generated graphics. In either case, the text messages are recorded in the same way. Prior to any email downloading, the downloading officer MUST first establish target directories and sub directories in the appropriate manner as described above. The actual downloading and record keeping for graphics is described in the following section.

A hard copy notebook in which the downloading officer MUST record his/her name, the date and time of the downloading, and the undercover name of the account that is downloaded. The downloading of text messages and text messages that also include an attached computer generated graphic image is done using the logging option of the program from which the mail was generated. Before beginning the downloading activity. **This E-Mail log is created by opening the ASession Log≅ option on AOL.** In addition, the downloading officer should check the Log Instant Messages box in the event other targets IM the downloading officer during the download process. The log file is saved to the computers hard drive and the following name is given to the file:

C:\OLI\OLLOGS\ (date of download) Aemai.log≅ - i.e 1223emai.log.

The downloading of computer graphic image files are directed to the target AIMAGES≅ sub directory responsible for its transmission. Often times, a target will send the same computer graphic image on more than one occasion. Each transmission of the computer graphic by the target is potentially a felony violation. Accordingly, each picture needs to be saved regardless of how many times it is sent. If the computer prompts the download officer that a AFile Already Exist≅ in a targets subdirectory, the downloading officer will create a new sub directory under the APICS≅ sub directory named ADUPES.≅ Each time the computer prompts the downloading officer that a AFile Already Exist≅ a new sub directory will be created (DUPES2; DUPES3; etc).

In addition each E-mail message which accompanies the graphic image MUST be saved in the target AFrom≅ sub directory. All E-mail associated with a particular target can later be printed by the investigator assigned to the search warrant application or can be printed and forwarded to the appropriate law enforcement agency upon a referral.

Contact with Targets through E-mail

At times it is necessary to further contact targets and engage them (him/her) in further E-mail conversation. When ever an undercover officer sends an E-mail to a target, that activity MUST be recorded and saved. In addition, any E-mail response from the target MUST also be recorded and saved. Accordingly, when ever an E-mail message is sent to a target, the message will be saved in the following manner using the **File - Save As** function:

E-MAIL SENT TO:

C:\OLI\OLTARGETS\UNWORKED\ **Target screen name \LOGS\TO.**
The name of the file will be in the following format: (first 2 letters of name, date, ATO.wpd≅) - i.e. TA1223TO.wpd.)

E-MAIL RECEIVED FROM:
C:\OLI\OLTARGETS\UNWORKED\ **Target screen name \LOGS\FROM.**
The name of the file will be in the following format: (first 2 letters of name, date, AFR.wpd≅) - i.e. TA1223FR.wpd)

NOTE: In many instances, numerous E-Mails are received from the target by the U/C on the same date. The file will be named with alphabetical letters a,b,c,d, etc. to denote multiple E-Mail message occurring on one date, i.e. TA1223Fa.wpd.

All E-mail contact between the undercover and the target should be printed out and put the case folder for reference by the assigned investigator preparing the search warrant.

Seizure/Analysis of Evidence

It is the standard operating procedure of the undercover operation that no violative files of any kind are ever transmitted, only received. Based on the reception of these files, search warrants are sought to search for the computer or related computer storage device that holds the file that was originally used in the transmission to the undercover. These computers or computer storage devices are then forensically searched by a computer forensic investigative specialist for evidence or presence of these files.

Additional equipment is used for the analysis of seized computers. The originals must be secured as evidence and a Aclonedâ hard-drive created to function as a working copy. At least one hard drive with memory capabilities similar to that set forth earlier in this memo must be obtained for this purpose.

Investigatory Forms

USE ONLY AFTER PERP IS APPREHENDED, AOL WILL FREEZE E-MAIL AND TERMINATE ACCOUNT

Your Unit
Address
Date

America On Line Incorporated
22000 AOL Way
Dulles, Virginia 21066
Att: John Ryan Legal Compliance

Re: Preservation Request

Dear Mr. Ryan:

It is requested that a block be placed on the America On Line account subscribed to by the following:

Name:
Address:
Telephone:

Screen Name:
Possible AOL Account
Credit Card:

Through an official criminal investigation, the (Your Department) has determined that the above individual has an active account with America On-Line Incorporated, and it is known that this account has been used to participate in the trading of sexually explicit pornographic images via the personal computer (May modify: to engage minors in conversation for the purposes of sexual exploitation, etc)

You are being advised that a search warrant was executed at the (residence, address) on DATE. It is anticipated that a search warrant will be executed at your office in the near future.

Sincerely Yours,

New Jersey State Police
High Technology Crimes Unit

Disk Evidence Worksheet

Division Case #:	HTCU Case #:	Submitting Agency Case #:	Rank/Name:	Badge #:
Computer Description	Evidence Tag #:	Date:	Signature:	

Note: This worksheet can be used to assist the HTCU in the analysis process examining the computer for evidence. It will be used when working on either the original media or a restored image of the original media. All steps may not be required, depending on the analysis required. Some steps may have been performed during other analysis processes. Some steps may have been performed previously.

☐ Establish the scope of examination relevant to warrant or consent to search

☐ Original Media ☐ Image

☐ Writeblock

Examination Boot Disk OS Version used ☐ 620 ☐ 95A ☐ 98 ☐ 95B ☐ Other:

Note: All 95 OS will change Last Accessed File Date if file viewed
95B partitions are not accessible without 95B boot disk or LINUX OS

☐ TREE (TREE C: >> X:\TREE_EXP.C) if needed - can keep track of examination in tree structure using edit file

☐ Fixed Disk Search Routine (look for keywords save as file - X:\FDSR.C) ☐ Writeblock on reminder

☐ Erased files: ☐ Writeblock on reminder

☐ a. Deleted Directories first (document by print screens or using Norton Unerase (prn2file undir.c)

☐ b. Deleted Files (document) (option - DOS UNDELETE (sweep undelete /list >> X:\undel.c)
Number of deleted files: _____

☐ c. Undelete the Files
Norton Unerase for directories
Option - DOS Undelete for files (sweep undelete *.* /all)
Option - Number of auto recovered files: _____
Option - Number of auto non-recoverable: _____

☐ d. Recover partial .WK1, .DBF, and .TXT files
Norton Unerase (Search /Data Type and Lost Names)
Observations:

Notes:

☐ File Attributes

☐ DIR C:*.* /S/AH >> X:\DIR.HID

☐ DIR C:*.* /S/AS >> X:\DIR.SYS

Disk Evidence Worksheet - Continued

- [ ] DIR C:*.* /S/AR>> X:\DIR.RO
- [ ] Other drives

- [ ] Passwords (look in communication programs menu items, script files) Also in DOC files, office papers, etc.. ASK for passwords.

a. Menu Passwords

- [ ] Users of system:

- [ ] Corporate / other possible business / name referenced:

- [ ] Run all programs (use tree printouts and note below any observations)

a. Communications programs (Call Log Info?, Password Info?)

b. Spreadsheets

c. Wordprocessing

d. Draw programs

e. Accounting programs

f. Utility programs

g. Database programs

h. Backup programs

l. Graphics files (View graphic files for contents)
Note: View graphic files using viewers or the native program. It is best to have the case agent view the files.

j. Other programs

ternet Files

Disk Evidence Worksheet - Continued

Internet cache

Internet Mail

Internet Newsgroup

Swap File review (copy to another media – filter, search)

Additional Comments

New Jersey State Police
High Technology Crimes Unit

Disk Integrity Worksheet

Division Case #:	HTCU Case #:	Submitting Agency Case #:	Rank/Name:	Badge #:
Computer ID:	Evidence Tag #:	Date:	Signature:	

Note: This worksheet is intended to assist the HTCU in an in-depth analysis of disk structure. All steps may not be required depending on the analysis required. Some steps may have been performed during other analysis processes.

☐ Establish the scope of examination

☐ Control Disk used - ID:

☐ Working on Original Media ☐ Working from Restored Image - ID:

Examination DISK OS Version used ☐ 622 ☐ 95 - v7.0 ☐ 95B v 7.1 ☐ Other:
☐ 95 - GUI ☐ 95B – GUI

Note: All 95 OS will change Last Accessed File Date if file viewed
95B partitions are not accessible without 95B boot disk or LINUX OS

☐ Writeblock installed (if needed for documentation)

SYSTEM AREAS via Diskedit

To Save system areas as workpapers:
PRN2FILE DISKSTRU.C to redirect printer writes to file or use Diskedit print functions under tools and print each disk area separately to file.
CTRL + P to saved as system workpapers

C		Area		Activity (hex and area view)
☐	☐	PARTITION RECORD	ALT + A	Cylinder gaps
☐	☐	BOOT RECORD	ALT + B	Unusual names / entries (& in HEX for IO & OS files before 55 AA)
☐	☐	FAT1	ALT + F1	Bad Clusters (F7 FF), gaps, fat slack
☐	☐	FAT2	ALT + F2	same
☐	☐	ROOT	ALT + R	inspect unused directory area, directory slack, hidden , split, ALT255, attributes
☐	☐	SUB-DIR	ALT + R	systematically go through each sub-dir for above

Observation of Partition and Boot Areas

Observation of FATS (gaps, bad clusters, slack etc) (Hex and as FAT)

Observation of Root and Sub-Directory areas: (gaps, split, or locked directories, ALT 255 (HEX FF), unusual entries, review past "unused directory areas" in HEX):

Observation of Track 0

Boot Process: (to verify that boot files do not appear to have been tampered with)

No	
☐	1st file in root directory is an IO system file
☐	2nd file in root directory is an OS system file
☐	The IO system file calls config.sys (at approx 95%)
☐	The IO system file calls command.com
☐	Review config.sys (print out and note observations)
☐	Review Autoexec.bat (print out and note observations)
☐	Locate command.com's call to autoexec.bat (at approx 15%)
☐	Review command.com's internal commands - "dir,type,copy, rename,date,time" (at approx. 70%)
☐	Locate command.com's ".com.exe.bat" order (at approx 90%)
☐	Check for multiple command.com's - review each one (use Norton commander to find them and use CRC's to eliminate dups)

☐ Virus detection
Program Used _____ Version _____ Results filename (X:\<filename.c, etc)
☐ Clean ☐ Infected

☐ CRC verification - Verify restored files (Word - Options/compare version) (CRC_DS.exe)
☐ Compares or explanation:

☐ Fixed Disk Search Routine/Disksearch (Save as file - X:\DS.C)

☐ CHKDSK (Save as file X:\CHKDSK.C)

☐ 10. TREE (TREE C: >> X:\TREE.C)

Disk Integrity Worksheet continued

☐ 11. File Attributes

- ☐ DIR C:*.* /S/AH >> X:\DIR.HID
- ☐ DIR C:*.* /S/AS >> X:\DIR.SYS
- ☐ DIR C:*.* /S/AR>> X:\DIR.RO
- ☐ Don't forget other drives

☐ Batch file comments Number of batch files (use CRC_C.DBF to find):_____

☐ Erased files: ☐ Write Protect On reminder

- ☐ a. Deleted Directories first (document by print screens or using Norton Unerase (prn2file undir.c)
- ☐ b. Deleted Files (document) (option - DOS UNDELETE (sweep undelete /list >> X:\undel.c)
  Number of deleted files: _____
- ☐ c. Undelete the Files
  Norton Unerase for directories
  Option - DOS Undelete for files (sweep undelete *.* /all)
  Option - Number of auto recovered files: _____
  Option - Number of auto non-recoverable: _____
- ☐ d. Recover partial .WK1, .DBF, and .TXT files
  Norton Unerase (Search /Data Type and Lost Names)
  Observations:

Disk Integrity Worksheet continued

Notes: (Names of deleted directories, etc.)

High Technology Crimes Unit
Disk Size Verification Checksheet

Division Case #:	HTCU Lab #:		

The steps outlined below will assist in checking that the disk size and values as reflected in CMOS and the Partition Tables compare to other disk testing reports. This process can help discover hidden or unpartitioned areas of a fixed disk drive. All information does not have to be recorded. You may need t explore and resolve indicated conflicts using additional tools.

I. Drive information per Physical Inspection (see CIS Computer Evidence Inventory - SCER use only)

You may have to research drive manufacturer and serial # to obtain these values.

HD Type	HD Size	# Heads	# Tracks	Sect/Trk

II. Information from SYSINFO (SI) SUMMARY

	SYSTEM	CMOS		
	HD Size	HD Type	Floppy	Memory
Primary				Base:
Secondary				Extended:

Disk Summary (drive C: & >)

Drive:	Type	Size
C:		

III. Disk Editor Partition Table Summary

			starting location			ending location			relative	no. of
	system	boot	side	cyl	sector	side	cyl	sector	sectors	sector

* each partition table sector ends with a HEX 55 AA.
* partition tables are in sector 1 side 0 of the first track of a cylinder
* first partition info starts at offset 446 for 16 bytes, 2nd at offset 462

IV. FDISK Summary

Fixed Disk #	Partition	Status	Type	MBytes			Usage %	
				MBytes	Computed Cumulative	Total Per Fdisk	Usage	Comput Cumulati

Notes & Observations: (Additional Comments on Back or Continuation Sheets

New Jersey State Police
Internal Parts Inventory Sheet
(HTCU Use Only - Detail of Inside Components)

Division Case #	HTCU Case #:	Submitting Agency Case #:	Rank/Name:	Badge #:

Computer Description:	Evidence Tag #:	Date:	Signature:

Item	Qty	Computer	MB		Manufacturer	Model #	Serial #
		Fixed Drive					
		Fixed Drive					
		Fixed Drive					
			Occupied				
			YES	NO			
		Slot 1	☐	☐			
		Slot 2	☐	☐			
		Slot 3	☐	☐			
		Slot 4	☐	☐			
		Slot 5	☐	☐			
		Slot 6	☐	☐			
		Slot 7	☐	☐			
		Slot 8	☐	☐			
			☐	☐			

Additional Comments: (switch settings, markings, listing of bad tracks, monitor switches, etc.) (Continued comments on back or continuation sheets)

NEW JERSEY STATE POLICE
ORIGINAL MEDIA ACCESS WORKSHEET

TO DOCUMENT EACH ACCESS TO ORIGINAL MEDIA

COMPUTER ID:

LOG OF EVERY ACCESS TO ORIGINAL MEDIA

(Complete the following every time you access the Original Media)

1.	Access Date:			System Date: (Optional)
	Access Time:			System Time:
	☐	**Boot** with Control Government Disks Virus Free	3.5 or 5.25	Control Disk operating system: DOS WIN95 95FAT32
	☐	**WriteBlock Installed**		
	☐	**System info - saved as SIREPORT.**	3.5 or 5.25	
	☐	**Evidence Lock (if applicable)**	3.5 or 5.25	
2.	Access Date:			System Date: (Optional)
	Access Time:			System Time:
	☐	**Boot** with Control Government Disks Virus Free	3.5 or 5.25	Control Disk operating system: DOS WIN95 95FAT32
	☐	**WriteBlock Installed**		
	☐	**System info - saved as SIREPORT.**	3.5 or 5.25	
	☐	**Evidence Lock (if applicable)**	3.5 or 5.25	
3.	Access Date:			System Date: (Optional)
	Access Time:			System Time:
	☐	**Boot** with Control Government Disks Virus Free	3.5 or 5.25	Control Disk operating system: DOS WIN95 95FAT32
	☐	**WriteBlock Installed**		
	☐	**System info - saved as SIREPORT.**	3.5 or 5.25	
	☐	**Evidence Lock (if applicable)**	3.5 or 5.25	:
4.	Access Date:			System Date: (Optional)
	Access Time:			System Time:
	☐	**Boot** with Control Government Disks Virus Free	3.5 or 5.25	Control Disk operating system: DOS WIN95 95FAT32
	☐	**WriteBlock Installed**		
	☐	**System info - saved as SIREPORT.**	3.5 or 5.25	
	☐	**Evidence Lock (if applicable)**	3.5 or 5.25	:

Comments or Observations

NEW JERSEY STATE POLICE
ORIGINAL MEDIA ACCESS WORKSHEET

Note: This worksheet may assist the CIS in tracking access to original media (seized computer). All steps may not need to be completed.

TO DOCUMENT EACH ACCESS TO ORIGINAL MEDIA	DATE:	INITIALS:
	COMPUTER ID:	

PROCEDURAL OPTIONS AND NOTES

☐ **Initial view of Computer's Drives** | Norton Commander, Sysinfo, DiskEdit

Drives	C:	D:	E:
Size			
1st two unsorted (system) files i.e. iosys and msdos.sys			

Comments on review of config.sys and autoexec.bat and other comments

Yes or No	Is this a compressed (Doublespace, Stacker, SuperStor, Drvspace, other) Disk?
Yes or No	Optional Reboot with proper drivers loaded (know purpose of drivers or seek assistance)

Comments

☐ **OPERATING SYSTEM:** Determine the Computer's Operating System – need to know as other control disks may need to be used. Couple of methods of locating

Operating System : _____

- ☐ - Dates and times on unsorted IO.sys and OS.sys files
- ☐ - Examine using DiskEdit – Boot record = _____
- ☐ - Examine unsorted first file (io.sys) – search for version

☐ **Rescue Disk required ?** | 3.5 or 5.25 | Rescue

- ☐ Copy system files to a blank diskette - Copy IO, OS, and command.com to disk in that order
- ☐ Run RESCUE to save CMOS, BOOT, & PART info to disk

Comments

☐ **CHKDSK (Copy to disk CHKDSK C: >> A:)** | 3.5 or 5.25 | Disk No.:

	Total Size	Bytes Free	Hidden Files	Errors	Bad Bytes
Drive C:					
Drive D:					
Drive E:					

Comments

☐ **SYSINFO (SI) SUMMARY** | 3.5 or 5.25 | Disk No.:

	SYSTEM		CMOS		
	HD Size	HD Type	Floppy Size	RAM MEMORY	
Primary				Base:	
Secondary				Extended:	

SYSINFO cont'd

NEW JERSEY STATE POLICE
ORIGINAL MEDIA ACCESS WORKSHEET

Hard Disk #		Size	Type	Heads/Sides	Cylinders/Tracks	Sectors
	C:					
	D:					
	E:					

Partition Table Info:

Hard Disk #	Start side	End Side	Start Track	End Track	# of sectors		Total Size
						x512	
						x512	
						x512	
						x512	
						x512	
						x512	

Comments – If a conflict exist, you may want to use the DISK SIZE VERIFICATION CHECKSHEET to assist in locating the problem.

☐ **Copy Autoexec.* and Config.* , and hidden files for all drives to disk** | 3.5 or 5.25 | Disk No.:
Comments

☐ **TREE >> A:TREE.C (etc.)** | 3.5 or 5.25 | Disk No.:
Comments

☐ **VIRUS CHECK** | 3.5 or 5.25 | Disk No.:
Virus Found: Y or N
Comments

☐ **DISKEDIT /M to create SAFETY NET diskette)** | 3.5 or 5.25 | Disk No.:

- ☐ Test Cylinder Info: Last # of CYLINDERS (Physical Drive Mode) ALT+P
- ☐ Switch to Logical Drive Last # of CYLINDERS (Logical Drive) ALT+P
- ☐ Capture System Area - boot, fat & dir areas to disk (filename- A:sysarea.c (etc.))
- ☐ Review &/or capture Track 0 to disk A:DRV0_TRK.0

Note # of Cylinders (Logical Drive) Alt+P
Note DOS Version ALT+B

- ☐ Review & capture TEST Cylinders to disk A:DRV0_TST.CYL Disk No.:

NOTE: If disk discrepancies observed above, use DISK SIZE VERIFICATION WORKSHEET
Comments

☐ **CRC** | 3.5 or 5.25 | Disk No.:
CRC /s /h C:*.* >> A:CRC.C1 **or** RUNCRC <drive> <Job#_org> <A:job#_org.crc>
Comments

☐ **SAFEBACK** | 3.5 or 5.25 | Disk No.:

	DRIVE	CAPACITY	CYLINDERS	HEADS	SECTORS	SECTOR SIZE
DIRECT	0					
DIRECT	1					
	0					
	C					

NEW JERSEY STATE POLICE
ORIGINAL MEDIA ACCESS WORKSHEET

		D					
		E					

Backup File Name:

Output to:

Comments

☐ **Examined for ERASED files** | 3.5 or 5.25 | Disk No.:

erased files	lost names	data type

Comments

☐ **DiskSearch performed** | 3.5 or 5.25 | Disk No.:

output file saved as (ex. A:dsout.c) Disk No.

Comments

☐ **LAPLINK PRO** | 3.5 or 5.25 | Disk No.:

Comments

☐ **HEADS PARKED & SHUTOFF** | 3.5 or 5.25 | Disk No.:

Comments

ADDITIONAL COMMENTS & OBSERVATIONS

POLICE DEPARTMENT
CITY OF NEW YORK

PERMISSION TO SEARCH

Complaint Number:	Case Number:
Assigned Detective:	Command:

I, _____, having been informed of my constitutional right not to have a search made of my premises, motor vehicle, or other personal property without a search warrant, and having been informed of my right to refuse to consent to such a search, and understanding that evidence and/or contraband found as a result of such may be seized and used against me in a court of law, hereby authorize: _____, a police officer of the New York City Police Department , or any police officer of the New York City Police Department, to conduct a complete search of:

( ) My premises, and all property found therein, located at:

_____, _____, _____, _____
Street Address Town County State

( ) I do voluntarily provide the keys to above location for access.

( ) My motor vehicle; a 19__, _____, VIN _____, bearing registration plates _____, issued by the state of _____, and all property found therein. This vehicle is currently located at :

_____, _____, _____, _____
Street Address Town County State

( ) My personal computer or electronic storage device: _____ to include an examination of any data stored.

This written permission is being given by me to the above named Police Officers voluntarily and with no promises made to me or threats against me.

FALSE STATEMENTS MADE HEREIN ARE PUNISHABLE AS A CLASS A MISDEMEANOR PURSUANT TO SECTION 210.45 OF THE PENAL LAW OF THE STATE OF NEW YORK

Signature: _____ Time: _____
Date: _____

_____
Witness

_____
Witness

POLICE DEPARTMENT
CITY OF NEW YORK

Date: _____

CONSENT FOR REMOVAL OF COMPUTER AND OTHER RELATED MATERIAL

I _____, do give permission and consent to Det. _____, shield # _____ of the Computer Investigation and Technology Unit of the New York Police Dept. to remove my computer, floppy disks, manuals, books and any other related material. No promises or threats have been made by anyone, the property will be vouchered and I will receive a receipt for all property.

Signature: _____
Witness: _____
Witness : _____

POLICE DEPARTMENT
CITY OF NEW YORK

_____

From: Commanding Officer, Computer Investigation and Technology Unit

To: Commanding Officer, Headquarters Security

Subject: REMOVAL OF EQUIPMENT FROM 1 POLICE PLAZA

1. The undersigned authorizes _____ to remove _____ from 1 Police Plaza.

2. For your information.

Christopher Malinowski
Lieutenant

Computer Investigation & Technology Unit

S A R

SAR Number	Date Received	Code	Type of Request	Unit Requesting	Detective Assigned	Date Closed	Supv Init

Code:

SW	Search Warrant Execution	**TA**	Technical Assistance
494	Assistance with 494 Program	**GP**	Graphics / Presentation
OA	Outside Agency Request	**PI**	Preliminary Investigation
SP	Subpoena / Warrant Preparation	**TL**	Training / Lecture
DB	Debrief Suspect/Prisoner		

POLICE DEPARTMENT
CITY OF NEW YORK

July 27, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to the New York State Department of Motor Vehicles to produce color copies of the following photo images as defined in V.T.L. 490 and V.T.L. 504 for the following New York State Drivers License and Non-Driver Identification holders:

Name	D.O.B.	Client	SAR#
Catalano, Larry	6/26/46	93882991	263

2. These photos are reuested for an investigation of endangering welfare of a minor investigated under SAR 263 of 1999.

3. The subpoena can be directed to the attention of:

Donna Kahnle
New York State Department of Motor Vehicles
Hearings & Support Services
Swan Street Building- ESP Rm 529
Albany, NY 1228-0700
FAX (518) 474-8537

4. This matter is assigned to Sgt. James Doyle this unit under SAR #263, telephone 212-374-4247.

Sgt. James Doyle
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 28, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

July 27, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to America Online to release subscriber information and all other screen names for the following screen names:

rwhite431

2. These screen names were used on America Online and are needed for the identification of persons committing Grand Larceny investigated under SAR 262 of 1999.

3. The subpoena can be directed to the attention of:

Justyna Kilbourne
America Online Legal Division
22000 AOL Way
Dulles, VA 20166
tel# (703) 265-2745; FAX (703) 265-2305

4. This matter is assigned to Sgt. James Doyle this unit under SAR #262, telephone 212-374-4247. Thank you for your assistance.

Sgt. James Doyle
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 28, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

February 18, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to AT&T Worldnet for any subscriber and detailed billing information and other related information for the following AT&T Worldnet customer telephone numbers listed below:

212 534 9139
212 534-8425

To the attention of:

Edward Stephenson Tel (919) 319-8187, Fax (919) 319-8154
AT&T Subpoena Management Center
1200 Peachtree Street
NE Promenade II, Room 05E52
Atlanta, GA 30309
Tel (800) 732-5689, Fax (404) 810-6250

2. This information is needed to identify the subject of an investigation of a Homicide Investigation being conducted by Det. Robert Mooney of the 23rd Precinct Detective Squad. This request is forwarded by Police Officer Mark Kirshner of the Computer Investigation and Technology Unit under SAR#90/98, telephone 212-374-4247.

Police Officer Mark Kirshner
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, February 18, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski

POLICE DEPARTMENT
CITY OF NEW YORK

September 22, 1998

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to AT&T Wireless Services Investigative Group located at 801 Northpoint Parkway, West Palm Beach, Florida, 33407 to the attention of the Subpoena Group, telephone number (800) 635-6840 for calls to destination, any subscriber and billing information and other related information for the following telephone numbers listed below:

(732) 370-3801
(800) 245-5160
(212) 397-1411

2. This information is needed to identify the subject of an investigation of Grand Larceny. This matter is assigned to Police Officer Luke Cats under Case #119, telephone 212-374-4247. Thank you for your assistance.

Police Officer Lucas Cats
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, September 22, 1998. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

June 23, 1997

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Chase Manhattan Bank to release bank records for the following account:

Gina Donato

2. This information is needed for further investigation of the crime of Grand Larceny.

3. The subpoena can be directed to the attention of:
Cindy Honma
Sprynet
3535 128th Ave SE
Bellview, Washington 98006

4. This matter is assigned to Det. Capozziello.Case # M96-1388. Telephone 212-374-4247. Thank you for your assistance.

Det. Ted Capozziello
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, November 14, 1996. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

February 5, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Bell Atlantic Subpoena Group, 1095 Avenue of the Americas, Room 2900, New York, N.Y., 10036 to the attention of Mary Ann Gainer (212 395-0523) for subscriber and billing information, published or non-published, and related information for the telephone number listed below:

(212) 879-3730
(718) 439-4749

2. This information is needed to identify the subject in an investigation of Sexual Abuse, assigned to Detective Kevin Coco under SAR#69/99, telephone 212-374-4247.

Detective Kevin Coco
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 27, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

January 27, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Mr. Roman Kazanof Escape.com, 16 East 55th Street, New York, NY 10022, telephone #(212) 888-8780. This subpoena is request to find subscriber information, billing information and dial in logs for an individual assigned the following ip address and username for the time period November 1, 1998 to the present:

globe@escape.com
205.160.44.30

2. This information is needed to identify the subject of unlawful software duplication. Also request that non-disclosure statement be written into the subpoena.

3. This matter is assigned to Det. Coco under case #18102/98, telephone 374-4247. Thank you for your assistance.

Det. Kevin Coco
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 27, 19998. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski

POLICE DEPARTMENT
CITY OF NEW YORK

October 8, 1996

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Frontier Telephone Co. located at 145 North Main St., Monroe, NY, 10950 to the attention of Mr. Brynne Donovan, Senior Service and Sales Associate, telephone number (914) 782-1020 for subscriber and billing information for the following number:

(914) 569-0264

2. This information is required to identify the subject of an ongoing investigation concerning Endangering the Welfare of a Child. This matter is assigned to Det. Ted Capozziello under Case #019, telephone 212-374-4247. Thank you for your assistance.

Detective Ted Capozziello
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, October 3, 1996. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

October 3, 1997

From: Commanding Officer, Computer Investigation and Technology Unit
To: Deputy Commissioner, Legal Matters
Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Good.Net to release subscriber and billing information and all other screen names for the following:

Sauron@.GoodNet.Com

2. This information is needed to identify the subject of a Computer Trespass.

3. The subpoena can be directed to the attention of:

David Jemmett
GoodNet
3443 North Central, 17th Floor
Phoenix, AZ 85012
(602) 303-9500x3224

4. This matter is assigned to Det. Schoenacher Case #47, telephone number 212-374-4247. Thank you for your assistance.

Det. Gerard Schoenacher
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, October 3, 1997. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

January 27, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to the Legal Division of Hotmail Communications of at 2 North Second St., Plaza A, San Jose, CA 95113, tel #(888) 316-1122. Contact at Hotmail is Tricia Martin Del Campo at (408) 222-7310. This subpoena is request to find subscriber information and billing information for an individual using the following user name:

poopzy@hotmail.com

2. This information is needed to identify the subject of unlawful software duplication. Also request that non-disclosure statement be written into the subpoena.

3. This matter is assigned to Det. Coco under case #18102/98, telephone 374-4247. Thank you for your assistance.

Det. Kevin Coco
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 27, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

January 14, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Hotmail Corporation for all subscriber information including all access dates and times, and the registration IP address. For the e-mail address listed below;

JerryWillis@hotmail.com

2. The subpoena can be directed to the attention of:

Randy DeLucchi
Hotmail Corporation
1290 Oakmead Parkway
Sunnyvale, CA 94086

3. This investigation is assigned to Detective Donald Callahan under CITU#450/98 Telephone 212-374-4247. Thank you for your assistance.

Donald Callahan
Detective , CITU

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 14, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

February 4, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to the Manager of Network Security, Mr. Robert Frederick, for IBM Corporation at Route 100, Building 2, Maildrop 2239, Somers, New York 10589, telephone number (914) 766-2008. This subpoena is request to find subscriber information, billing information and dial-in logs for the following user names:

Dddd99@ibm.net
Faxcom@ibm.net

2. This information is needed to identify the subject of a grand larceny. Also request that non-disclosure statement be written into the subpoena.

3. This matter is assigned to Det. Schoenacher #18/99, telephone 374-4247. Thank you for your assistance.

Det. Gerard Schoenacher
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 27, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

December 23, 1997

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Bell Atlantic Subpoena Group at 1095 Avenue of the Americas, Room 2900, New York, NY 10036 to the attention of Mary Ann Gainer, telephone (212) 395-0523 for records of outgoing telephone calls (LUDS and tolls) for the number listed below for the time period between 1:00 AM on November 14, 1997 to 11:00 PM on November 14, 1997 for the below listed number:

(212) 539-1363

2. This information is required to identify the subject of an ongoing investigation concerning Computer Tampering 2. This matter is assigned to Det. Gerard Schoenacher under Case #065, telephone 212-374-4247. Thank you for your assistance.

Det. Gerard Schoenacher
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, December 23, 1997. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

December 4, 1997

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Bell Atlantic Subpoena Group at 1095 Avenue of the Americas, Room 2900, New York, NY 10036 to the attention of Mary Ann Gainer, (212) 395-0523 for records of incoming telephone calls to the number listed below for the 24 hour period from 12:01 AM on November 14, 1997 to 11:59 PM on November 14, 1997:

(212) 529-8440

2. This request for the processing of an "N-File" search requires the following instructions to be included in the subpoena:

"All calls and listings derived from a special computer run regarding calls to Classic Sports Network located at 300 Park Ave. South, New York City, for the telephone number (212) 529-8440 for the time period beginning at 12:01 AM on November 14, 1997 and ending 11:59 PM on November 14, 1997. This special computer run is a billing tape search. Stephen Greenberg, President of Classic Sports Network located at 300 Park Ave. South, New York City, telephone number (212) 529-8000 has given consent for this file search and that the company has agreed to pay for the cost of this search".

3. This information is required to identify the subject of an ongoing investigation concerning Computer Tampering 1. This matter is assigned to Detective Gerard Schoenacher under Case #065, telephone 212-374-4247. Thank you for your assistance.

Detective Gerard Schoenacher
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, C.I.T.U. to the Deputy Commissioner, Legal Matters, December 4, 1997. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski

POLICE DEPARTMENT
CITY OF NEW YORK

February 16, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to America Online to release subscriber information consisting of **all other screen names, billing records showing login dates and times, and assigned IP addresses and/or POP servers phone numbers accessed.** This information must cover the period from January 1, 1999 to February 16, 1999 for the following screen names:

LAWMAN44

2. This information is needed in connection with an official misconduct case currently being investigated by the Computer Investigation and Technology Unit, SAR#93/99.

3. The subpoena can be directed to the attention of:

Justyna Kilbourne
America Online Legal Division
22000 AOL Way
Dulles, VA 20166
Voice (703) 265-2745
FAX (703) 265-2305

4. This investigation is assigned to Det. Donald Callahan, Telephone 212-374-4247, FAX 212-374-4249.

5. Thank you for your assistance.

Det. Donald Callahan
Computer Investigation &
Technology Unit

FIRST ENDORSEMENT

POLICE DEPARTMENT
CITY OF NEW YORK

January 28, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to IBM Corp. to release any and all records relating to IP 129.37.112.18 on 1/28/99 at 08:36:37 EST, including subscriber information and detailed account and billing records.

2. This information is needed in connection with a grand larceny being investigated by the Computer Investigation and Technology Unit.

3. The subpoena can be directed to the attention of:

   Robert Frederick
   IBM Corporation
   Route 100, Building 2
   Maildrop 2239
   Somers, New York 10589
   1-914-766-2008
   FAX 914 766-7264

4. This investigation is assigned to Det. Gerard Schoenacher under CASE 18/99. Telephone 212-374-4247, FAX 212-374-4249.

5. Thank you for your assistance.

Det. Gerard Schoenacher
Computer Investigation &
Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 28, 1999. I certify that the records requested are

POLICE DEPARTMENT
CITY OF NEW YORK

January 26, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to San Diego Union Tribune at P.O. Box 191, North San Diego, CA, 92112 to the attention of Mr. Marilyn Creason, Business Department, telephone number (619) 299-3131 for billing information in regards to a classified ad placed in the San Diego Union Tribune on December 1, 1998 in the Air Travel Section (1701) relating to the sale of airline tickets by one "jerrywillis@hotmail.com" :

2. This information is required to identify the subject of an ongoing investigation concerning Grand Larceny and Criminal Impersonation. This matter assigned to Det. Donald Callahan under SAR# 44/99, telephone 212-374-4247.

3. Thank you for your assistance.

Detective Donald Callahan
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, January 27, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

December 11,1996

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to U.S. Sprint, known as Sprint Communications: located at 9221 Ward Parkway Suite 400, Kansas City, MO 64114 Att: subpoena compliance group Tel# 913-624-4734 Fax# 913- 624-4706 for all subscriber and billing information for the following number:

(800) 786-8241
Pin# 129357

2. This information is required to identify the subject of an ongoing investigation concerning a scam that was reported from America-On-Line.This matter is assigned to Det. Ted Capozziello under SAR# 487, telephone 212-374-4247. Thank you for your assistance.

Detective Ted Capozziello
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, December 11, 1996. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski

POLICE DEPARTMENT
CITY OF NEW YORK

November 14,1996

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Spry Net to release subscriber information and all other screen names for the following screen name:

TROYK9 @sprynet.com

2. This information is needed to identify the subject of an on going investigation involving the Inspection Unit. A member of the service receiving threatening e-mail .

3. The subpoena can be directed to the attention of:
Cindy Honma
Sprynet
3535 128th Ave SE
Bellview, Washington 98006

4. This matter is assigned to Det. Capozziello.Case # M96-1388. Telephone 212-374-4247. Thank you for your assistance.

Det. Ted Capozziello
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, November 14, 1996. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

POLICE DEPARTMENT
CITY OF NEW YORK

April 12, 1999

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject : **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Mr. Ronald Maas, TheGlobe.com, 31 West 21st Street, New York, NY 10010, telephone #(212) 886-0766, Fax (212) 367-8588. This subpoena is request to find subscriber information, billing information and dial in logs for an individual assigned the following ip address and username for the time period November 1, 1998 to the present:

sonic461@theglobe.com

2. This information is needed to identify the subject of dissemination of child pornography and bestiality over the internet. Further request that non-disclosure statement be written into the subpoena.

3. This matter is assigned to Det. Coco under SAR#142/99, telephone 374-4247. Thank you for your assistance.

Det. Kevin Coco
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, April 12, 1999. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski

POLICE DEPARTMENT
CITY OF NEW YORK

October 3, 1997

From: Commanding Officer, Computer Investigation and Technology Unit

To: Deputy Commissioner, Legal Matters

Subject: **REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to US West Communications, Custodial Records, located at 1801 California St. Room #3250, Denver, Colorado, 80202 for subscriber information and records of outgoing telephone calls (LUDS and tolls) for the numbers listed below for the time period between 12:01 AM on August 28 and 3:00 AM on August 29, 1997:

(602) 487-1047
(602) 935-0244

2. This information is required to identify the subject of an ongoing investigation concerning Computer Tampering 1. This matter is assigned to Det. Gerard Schoenacher under Case #047, telephone 212-374-4247. Thank you for your assistance.

Det. Gerard Schoenacher
Computer Investigation and Technology Unit

FIRST ENDORSEMENT

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, October 3, 1997. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski
Commanding Officer, C.I.T.U.

COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

IN THE MATTER OF AN APPLICATION FOR A
WARRANT TO SEARCH THE PREMISED LOCATED AT
_____ EAST ____ STREET, Apt. #__
NEW YORK, NEW YORK.

AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT

Det. _____, being duly sworn, deposes and says:

1. I am a Detective, Shield #_____, assigned to the _____ Squad/ Unit of the New York City Police Dept., and as such I am a public servant of the kind specified in C.P.L. Section 690.05 (1).

2. I have been a Police Officer for ___ years and a Detective for ___ years and have been assigned the _____ Squad/Unit for ____ years and have [list expertise in crime being investigated, such as training or specific knowledge in the area of this type of crime investigation where possible].

3. I am currently assigned to an ongoing investigation of [describe the investigation].

4. This affidavit is submitted in support of an application for a warrant to search the designated premises to wit: ___ _____ Street, Apt. #__ New York, New York, where there is reasonable cause to believe that the following property may be found: [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property...],
computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure. Moreover, as set forth below, there is reasonable cause to believe that this property constitutes evidence or tends to demonstrate that an offense was committed or that a particular person participated in the commission of said offense.

5. My basis for believing that the property is in the above stated location(s) is as follows: [describe personal observations, past investigations, registered informants, etc.).

WHEREFORE, deponent respectfully requests that the Court issue a warrant and order seizure in the form annexed authorizing a search of premises to wit: ___ _____ Apt. #__, New York, New York and search occupants if present therein for [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property...], computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure and all items used to facilitate or evidencing violations of Penal Law Article ___ and directing that if such evidence be found, it be brought before the Court without unnecessary delay. No previous application has been made in this matter to any other Judge, Justice or Magistrate.

_____

Detective _____

Shield #_____, NYPD, ____ Squad/Unit

Sworn to before me this

_____ day of November, 1997

_____

Judge of the Criminal Court

CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

IN THE MATTER OF THE APPLICATION
OF DET. _____
OF THE NEW YORK CITY POLICE DEPARTMENT
FOR A SEARCH WARRANT

THE NAME OF THE PEOPLE OF THE STAE OF NEW YORK
TO ANY PPOLICE OFFICER IN THE CITY OF NE YORK

Proof by affidavit having been made this day before me that there is reasonable cause to believe that certain property, to wit, [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property…], computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure is located at the premises, to wit: ___ _____ Street Apt. #__, New York, New York and is [stolen, unlawfully possessed, has been used or is possessed for the purpose of being used, to commit or conceal the commission of an offense or constitutes evidence or tends to demonstrate that a n offense was committed to wit: [crime].

YOU ARE THEREFORE COMMANDED [,at any time of the day or night,] to make an immediate search at the above-described premises, to wit: ___ _____ Street, Apt. #__, New York, New York and search of occupants therein, for [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property…], computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure and if you find such property or any part thereof to bring it before the Court without unnecessary delay. This warrant must be executed within 10 days of the date of issuance.

_____
Judge of the Criminal Court

Dated:

COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

In the matter of the application of Detective _____,
shield #_____ of the New York City Police Department,
Computer Investigation and Technology Unit,
for a Search Warrant authorizing the search of computer equipment,
to wit: [number] computer[s] vouchered under NYPD invoice #G_____,
recovered from 111 _____ St., New York, New York.

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

Detective _____, New York City Police Department, shield #_____, being duly sworn, deposes and says:

1. I am the applicant herein and am a public servant of the kind specified in C.P.L. Section 690.05 (1), my title being Detective, _____ Computer Investigation and Technology Unit of the New York City Police Department.

2. I have been a Police Officer for eighteen years and have been a Detective for eight years and during the course of that time a have been assigned to the Computer Investigation and Technology Unit. I have attended seminars and conferences concerning the forensic examination of computers given by SEARCH, HTCIA, National White Collar Crime Association FinCEN among others, am a current member of HTCIA and have assisted in presentations to various NYPD units in the area of computer crime investigation.

3. This affidavit is submitted in support of an application for a warrant to search files stored inside computer equipment, to wit: [number] computer[s] recovered from 111 ____ St., New York, New York ("the target computer[s]"), where there is reasonable cause to believe that the following property may be found: (a) [databases containing gambling records, electronic images depicting child pornography, etc.]; (b) electronic communications detailing the [sale, purchase, transfer, etc.] of the [files, images, etc.] described above. Moreover, as set forth below, there is reasonable cause to believe that this property constitutes evidence or tends to demonstrate that an offense was committed or that a particular person participated in the commission of said offense.

4. My basis for believing that the property is in the above-stated location is as
follows: I was informed by [investigator's name] of [Squad, Unit or Agency name] that [tell their story].

5. The foregoing constitutes grounds for my belief.

WHEREFORE, deponent respectfully requests that the Court issue a search warrant and order seizure in the form attached (i) authorizing a search of files stored inside computer equipment vouchered under NYPD invoice #_____, recovered from ____ _____ Street, New York, New York for (a) [databases containing gambling records, electronic images depicting child pornography, etc.]; (b) electronic communications detailing the [sale, purchase, transfer, etc.] of the [files, images, etc.] described above, and (ii) directing that if such evidence is found, it be brought before the Court. The deponent also requests permission to decode protective passwords, download data from the computer, convert or transfer such data to storage in another device. No previous application in this matter has been made to this Court or to any other Judge, Justice or Magistrate.

_____
Detective _____
Shield #2416, NYPD, CITU

_____
[assigned ADA]
APPROVED: Assistant District Attorney

Sworn to before me this
_____ day of November, 1997

_____
Judge of the Criminal Court

CRIMINAL COURT OF THE CITY OF NEW YORK
PART AR-1, COUNTY OF NEW YORK

IN THE MATTER OF THE APPLICATION OF
Det. _____ of the
_____ Squad/Unit of the
New York City Police Department for a
Search Warrant to search ___ _____ Street,
Apt. #__, New York, New York

TO ANY POLICE OFFICER OF THE CITY OF NEW YORK

Proof by affidavit having been made this day before me by Det. _____, shield #_____ of the _____ Computer Investigation and Technology Unit, that there is reasonable cause to believe that certain property [belonging to (subject of investigation/defendant) and] constituting evidence to wit: [computer databases containing gambling records, electronic images depicting child pornography, etc.]; electronic communications detailing the sale, purchase and/or transfer of the [files/images] described above, may be found in files inside computer vouchered under NYPD invoice #_____, which was recovered from ____ _____ Street, New York, New York.

YOU ARE THEREFORE COMMANDED, at any time of the day or night, to search the computer vouchered under NYPD invoice #_____ which was recovered from ___ _____ Street, New York, New York, for (a) [databases containing gambling records, electronic images depicting child pornography, etc.]; (b) electronic communications detailing the [sale, purchase, transfer, etc.] of the [files, images, etc.] described above, and if you find such property or any part thereof to bring it before the Court without unnecessary delay. You are also authorized to decode protective passwords, download data from the computer, convert or transfer such data to storage in another device.

This warrant must be executed within ten days of the date of issuance.

_____
Judge of the Criminal Court

Dated: New York, New York

_____

Search Warrants

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS TO AND FROM SIX SPECIFIED AMERICA ONLINE ACCOUNT NUMBERS: 000-0000-001; 000-0000-002;000-0000-003; 000-0000-004;000-0000-005; and 000-0000-006.	**UNDER SEAL** John Doe No. A00-000

APPLICATION FOR INTERCEPTION OF ELECTRONIC COMMUNICATIONS

COMES NOW _____, United States Attorney for the Eastern District of Virginia and _____, Assistant United States Attorney, and, being duly sworn, states:

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of United States federal felony offenses. I am also an attorney for the Government as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 2516(3) of Title 18, United States Code, I am authorized to make an application to a Federal judge of competent jurisdiction for an order authorizing approving the interception of electronic communications.

2. This application is for an order pursuant to Section

2518 of Title 18, United States Code, authorizing the interception of electronic communications for a thirty (30) day period of ABE ABESON, aka A.A., America Online (AOL) acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006 concerning federal felony offenses, that is, offenses involving violations of Section 2252 of Title 18, United States Code (U.S.C.) (Certain activities relating to material involving the sexual exploitation of minors) as well as Title 18, U.S.C., Section 371 (Conspiracy).

3. I have discussed all of the circumstances of the above offenses with Special Agent Doris Hepler of the Federal Bureau of Investigation, who has directed and conducted this investigation, and have examined the Affidavit of Special Agent Hepler of this date (attached to this application as Exhibit 1, and which is incorporated by reference). Whereof your applicant states upon information and belief that:

a. there is probable cause to believe that ABE ABESON, aka A.A., America Online (AOL) acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006; GREG GREGSON, (account not targeted); HENRY HENRYSON (account not targeted); IGOR IGORSON (account

not targeted); JERRY JERRYSON
(account not targeted); and KIRBY KIRBYSON (account not targeted) have committed, are committing and will continue to commit violations of Section 2252 of Title 18, United States Code (U.S.C.) (Certain activities relating to material involving the sexual exploitation of minors) as well as Title 18, U.S.C., Section 371 (Conspiracy).

b. there is probable cause to believe that particular electronic communications of ABE ABESON, aka A.A., acc. no. 000-0000-001; BEN BENSON, aka B.B., acc. no. 000-0000-002; CARL CARLSON, acc. no. 000-0000-003; DIRK DIRKSEN, acc. no. 000-0000-004; EDGAR EDGARSON, acc. no. 000-0000-005; and FRED FREDSON, acc. no. 000-0000-006 concerning the above-described offenses will be obtained through the interception for which authorization is herein applied. In particular, there is probable cause to believe that the communications to be intercepted will concern the identities and account numbers of associates of ABE ABESON, aka A.A., AOL acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006; GREG GREGSON, (account not targeted); HENRY HENRYSON (account not targeted);

IGOR IGORSON (account not targeted); JERRY JERRYSON (account not targeted); and KIRBY KIRBYSON (account not targeted) and the dates, times and places for commission of the aforementioned federal felony offenses when ABE ABESON, aka A.A., America Online (AOL) acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006 communicate with their co-conspirators, aiders and abettors, and other participants in the conspiracy, thereby identifying the co-conspirators and aiders and abettors of the aforementioned targets and others as yet unknown, their places of operation. In addition, these communications are expected to constitute admissible evidence of the above-described offenses;

c. normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as are described in further detail in the attached affidavit of Special Agent Hepler; and

d. there is probable cause to believe that the facilities of America Online (AOL), 8619 Westwood Center Drive, Vienna, Virginia, within the Eastern District of Virginia, a commercial computer service,

are being, and will continue to be used in connection with the commission of the above-described offenses.

The attached affidavit contains a full and complete statement of facts concerning all previous applications that have been made to any judge of competent jurisdiction for authorization to intercept, or for approval of interception of wire, oral or electronic communications involving any of the same individuals, facilities, or places specified in this application.

On the basis of the allegations contained in this application and on the basis of the attached affidavit of Special Agent Hepler,

IT IS HEREBY REQUESTED that this Court issue an order, pursuant to the power conferred on it by Section 2518 of Title 18, United States Code, authorizing the Federal Bureau of Investigation to intercept electronic communications to the above-described accounts, and providing that such interceptions not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but continue until all communications are intercepted which reveal fully the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first

begin to conduct an interception under this Court's order or ten (10) days after this order is entered, whichever is earlier.

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518(4) of Title 18, United States Code, directing that America Online, a communication service provider as defined in Section 2510(15) of Title 18, United States Code, shall furnish, and continue to furnish, the applicant and investigative agency with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such providers are according the persons whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of electronic communications over the above-described accounts, with the service provider to be compensated by the applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS REQUESTED FURTHER that, to avoid prejudice to this criminal investigation, the Court order the said provider of electronic communication service and its agents and employees not to disclose or cause a disclosure of this Court's order or the request for information, facilities and assistance by the Federal Bureau of Investigation or the existence of the investigation to any person other than those of their agents and employees who require said information to accomplish the services hereby requested. In particular, said provider and its agents and

employees should be ordered not to make such disclosure to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

IT IS REQUESTED FURTHER that this Court direct that this order be executed as soon as practicable after it is signed and that all monitoring of communications shall be recorded and examined by monitoring agents or attorneys to determine the relevance of the intercepted electronic communications to the pending investigation and that the disclosure of the contents or nature of the electronic communications intercepted be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of communications authorized by this Court's order must terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's order or ten (10) days after the order is entered, whichever is earlier.

IT IS REQUESTED FURTHER that the Court order that either _____, or any Assistant United States Attorney familiar with the facts of this case, provide to the Court a report on or about the tenth, twentieth and thirtieth days following the date of this order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the aforementioned reports should become

due on a weekend or holiday, IT IS REQUESTED FURTHER that such report become due on the next business day thereafter.

IT IS REQUESTED FURTHER that the Court order that its orders, this application and the accompanying affidavit and proposed order, and all interim reports filed with the Court with regard to this matter be sealed until further order of this Court, except that copies of the order, in full or redacted form, may be served on the Federal Bureau of Investigation and the service provider as necessary to effectuate the Court's order as set forth in the proposed order accompanying this application.

Respectfully submitted,

_____
United States Attorney

BY: _____
Assistant U.S. Attorney

SUBSCRIBED and SWORN to before me
this _____ day of ___, 19__.

_____
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS TO AND FROM SIX SPECIFIED AMERICA ONLINE ACCOUNT NUMBERS: 000-0000-001; 000-0000-002;000-0000-003; 000-0000-004;000-0000-005; and 000-0000-006.	**UNDER SEAL** John Doe No. A00-000

ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS

Application under oath having been made before me by _____, United States Attorney for the Eastern District of Virginia, and _____, Assistant United States Attorney, those persons being "investigative or law enforcement officers" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and an attorneys for the Government as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, for an Order authorizing the interception of electronic communications pursuant to Section 2518 of Title 18, United States Code, and full consideration having been given to the matter set forth therein, the Court finds that:

a. there is probable cause to believe that ABE ABESON, aka A.A., AOL acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no.

000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006; GREG GREGSON, (account not targeted); HENRY HENRYSON (account not targeted); IGOR IGORSON (account not targeted); JERRY JERRYSON (account not targeted); and KIRBY KIRBYSON (account not targeted) have committed, are committing, and will continue to commit violations of Section 2252 of Title 18, United States Code (U.S.C.) (Certain activities relating to material involving the sexual exploitation of minors) as well as Title 18, U.S.C., Section 371 (Conspiracy);

b. there is probable cause to believe that particular electronic communications of ABE ABESON, aka A.A., AOL acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006 concerning the above-described offenses will be obtained through the interception for which authorization is herein applied. In particular, there is probable cause to believe that the communications to be intercepted will concern the identity and account numbers of associates of ABE ABESON, aka A.A., AOL acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006; GREG GREGSON, (account not targeted); HENRY HENRYSON (account not targeted); IGOR IGORSON (account not targeted); JERRY JERRYSON (account not targeted); and KIRBY KIRBYSON (account not targeted)

and the dates, times, and places for commission of the aforementioned federal felony offenses when ABE ABESON, aka A.A., AOL acc. no. 000-0000-001; BEN BENSON, aka B.B., AOL acc. no. 000-0000-002; CARL CARLSON, AOL acc. no. 000-0000-003; DIRK DIRKSEN, AOL acc. no. 000-0000-004; EDGAR EDGARSON, AOL acc. no. 000-0000-005; and FRED FREDSON, AOL acc. no. 000-0000-006 communicate with their co-conspirators, aiders and abettors and other participants in the conspiracy, thereby identifying the co-conspirators and others as yet unknown, and their places of operation. In addition, these communications are expected to constitute admissible evidence of the above-described offenses;

c. It has been established adequately that normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ;

d. there is probable cause to believe that the facilities of America Online (AOL), 8619 Westwood Center Drive, Vienna, Virginia, within the Eastern District of Virginia, a commercial computer service, have been, are being and will continue to be used in connection with the commission of the above-described offenses.

WHEREFORE, IT IS HEREBY ORDERED that Special Agents of the Federal Bureau of Investigation are authorized to intercept electronic communications over the above-described facilities.

PROVIDED that such interception shall not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown

conduct their illegal activities, but may continue until all communications are intercepted which fully reveal the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this Order or ten (10) days after this Order is entered, whichever is earlier.

IT IS ORDERED FURTHER that, based upon the request of the Applicant pursuant to Section 2518(4) of Title 18, United States Code, America Online, a communication service provider as defined in Section 2510(15) of Title 18, United States Code, shall furnish, and continue to furnish, the Applicant and investigative agency with all information, facilities, and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such provider is according the persons whose communications are to be intercepted, with the service provider to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS ORDERED FURTHER that, to avoid prejudice to the Government's criminal investigation, the above provider of electronic communication service and its agents and employees are ordered not to disclose or cause a disclosure of this Order or the

request for information, facilities, and assistance by the Federal Bureau of Investigation or the existence of the investigation to any person other than those of its agents and employees who require said information to accomplish the services hereby ordered. In particular, said provider and its agents and employees shall not make such disclosure to a lessee, telephone or paging device subscriber or any interceptee or participant in the intercepted communications.

IT IS ORDERED FURTHER that this Order shall be executed as soon as practicable and that all monitoring of the communications relevant to the pending electronic communications shall be recorded and examined by the monitoring agents or attorneys to determine the relevance of the intercepted electronic communications to the pending investigation and that the disclosure of the contents or nature of the electronic communications intercepted be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of communications must terminate upon the attainment of the authorized objectives, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Order or ten (10) days after the Order is entered.

IT IS ORDERED FURTHER that _____, or any Assistant United States Attorney familiar with the facts of this case shall provide this Court with a report on or about the tenth, twentieth and

thirtieth days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the above-ordered reports should become due on a weekend or holiday, such report shall become due on the next business day thereafter.

IT IS ORDERED FURTHER that this Order, the application, affidavit, and proposed Order, and all interim reports filed with this Court with regard to this matter shall be sealed until further order of this Court, except that copies of the Order, in full or redacted form, may be served on the Federal Bureau of Investigation and the service provider as necessary to effectuate this Order.

_____
UNITED STATES DISTRICT JUDGE

Done at Alexandria, Virginia
On this ____ day of _____, 19__.

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS TO AND FROM SIX SPECIFIED AMERICA ONLINE ACCOUNT NUMBERS: 000-0000-001; 000-0000-002;000-0000-003; 000-0000-004;000-0000-005; and 000-0000-006.	**UNDER SEAL** John Doe No. A00-000

AFFIDAVIT IN SUPPORT OF APPLICATION

INTRODUCTION

Doris Hepler, being duly sworn, deposes and states as follows:

I am a Special Agent (SA) with the Federal Bureau of Investigation and have been so employed for the past ten years. I am stationed in the Metropolitan Resident Agency for the Southern Maryland Field Office and have received special training and courses on the subject of child abuse, sex abuse, child sexual assault and sexual exploitation of children. My areas of expertise as an FBI agent include investigation of those cases involving child sexual assault and sexual exploitation, including the possession and trafficking of visual depictions of minors engaged in sexually explicit conduct.

I have read and studied over 300 books and articles on the subject of child sexual assault, sexual exploitation of children, child prostitution, and child pornography. I have viewed thousands of sexually explicit pictures of children that depict them in the nude, in sexually provocative poses, lewd poses, and engaged in

virtually every sex act conceivable.

I have also received instruction from a pediatric endocrinologist on child development and have read several articles on the developmental stages of children which have assisted me in recognizing and identifying the ages of children. I have read thousands of electronic mail messages, written by pedophiles, which described the acts they desire to commit upon children. I have also read similar electronic mail messages, by the same individuals, which seek to encourage children to have sexual relations with them. These mail messages show the manner in which pedophiles seduce their victims, and the way they seek out, find and successfully molest children.

I am presently assigned to a squad dedicated to the investigation of violent crime and drug matters. Specifically, I am currently investigating violations of Title 18, United States Code, Sections 2251 (Sexual exploitation of children) and 2252 (Activities relating to material involving the sexual exploitation of children).

I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

This affidavit is submitted in support of an application for an order authorizing the interception of electronic communications to and from certain accounts, specified below, operated by America

Online (AOL), 8619 Westwood Center Drive, Vienna, Virginia, within the Eastern District of Virginia, a commercial computer service that offers electronic message bulletin boards enabling its subscribers to post messages that can be read by other subscribers.

This application for authorization to intercept electronic communications and the affidavit in support thereof are being filed in the Eastern District of Virginia because that is where the interception will actually occur. As noted above, AOL is located in Vienna, Virginia which is in the Eastern District of Virginia. Pursuant to this Court's order, AOL will set up a "mirror" or clone mailbox for the FBI for each of the six targeted accounts. This will be done at AOL's headquarters at the above described address. Whenever an electronic mail message (and any attached file) is sent from or delivered to any of the targeted accounts, the FBI will be simultaneously notified that the electronic mail message (and any attached file) has been delivered to the FBI clone mailbox. Agents will then open the electronic mail message (and any attached file(s)) at the receiving site in Pocatello, Idaho.

I have participated in the investigation of the above offenses. As a result of my personal participation in this investigation, through interviews with and analysis of reports submitted by other Special Agents of the FBI and other state and local law enforcement personnel, I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information which I have reviewed and determined to be reliable, I allege the facts to show the following:

There is probable cause to believe that the following individuals (hereinafter "the named interceptees") and others as yet unknown, using the targeted America Online accounts specified below, are committing, and will continue to commit violations of Section 2252 of Title 18, United States Code (U.S.C.) (Certain activities relating to material involving the sexual exploitation of minors) as well as Title 18, U.S.C., Section 371 (Conspiracy):

INTERCEPTEE	TARGETED AOL ACCOUNT #
1) ABE ABESON, aka A.A.	000-0000-001
2) BEN BENSON, aka B.B.	000-0000-002
3) CARL CARLSON	000-0000-003
4) DIRK DIRKSEN	000-0000-004
5) EDGAR EDGARSON	000-0000-005
6) FRED FREDSON	000-0000-006
7) GREG GREGSON	Account not targeted
8) HENRY HENRYSON	Account not targeted
9) IGOR IGORSON	Account not targeted
10) JERRY JERRYSON	Account not targeted
11) KIRBY KIRBYSON	Account not targeted

(Due to limitations on technical equipment, only six accounts are targeted for interception of electronic communications. However, there are eleven named interceptees because investigation has shown, as detailed below, that they are in regular contact with each other by means of their AOL accounts.)

There is probable cause to believe that particular electronic communications of the named interceptees and others yet

unknown concerning the above offenses will be obtained through the interception of such electronic communications to and from certain accounts, specified above, on AOL computers located in the Eastern District of Virginia and used by the named interceptees and others yet unknown. In particular, these communications are expected to concern the specifics of the above offenses, including (i) the nature, extent and methods of the child pornography distribution network operated by ABE ABESON and others; (ii) the identities and roles of accomplices, aiders and abettors, co-conspirators, and sources of child pornography who are involved in ABE ABESON's child pornography distribution operation; (iii) the existence and location of records pertaining to ABE ABESON's child pornography distribution operation; and (iv) the locations and items used in furtherance of ABE ABESON's child pornography distribution network. In addition, these electronic communications are expected to constitute admissible evidence of the commission of the above-described offenses.

The statements contained in this Affidavit are based in part on information provided by Special Agents of the FBI, on conversations held with detectives and officers from other state and local law enforcement agencies, on information provided by confidential sources, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing authorization for the interception of electronic communications, I have not included each and every fact known to me concerning this investigation. I have

set forth only the facts that I believe are necessary to establish the necessary foundation for an order authorizing the interception of electronic communications.

PERSONS EXPECTED TO BE INTERCEPTED

Pursuant to Federal Grand Jury subpoenas that have been served on America Online, the following information was obtained about the above named interceptees:

Subscriber Name	Address	Screen Names Used[1]	AOL Account #
ABE ABESON	123 Abe Lane Abe, AB 00000	Abe123 SonofAbe7 BabyAby	000-0000-0001
BEN BENSON	123 Ben Lane Ben, BN 00000	Ben456 SonofBen2 BigBen903	000-0000-0002
CARL CARLSON	87 Carl Ave. Carl, CL 00000	Carl9789 YoCarlson2 CarlCarl	000-0000-0003
DIRK DIRKSEN	8 Dirk St. Dirk, DK 00000	Dirk9283 SonDirkSon2 DirkedAgin	000-0000-0004
EDGAR EDGARSON	1 Edgar Circle Edgar, ED 00000	EDGARhere Eeisme	000-0000-0005
FRED FREDSON	98 Fred St. Fred, FD 00000	Yzaguirre	000-0000-0006

[1] A "screen name" is simply a name a subscriber chooses to send and receive communications through the America OnLine computer service. These names need not provide any information about the subscriber or have any relation to the subscriber's true name or identity.

GREG GREGSON	96 Greg Rd. Greg, GR 00000	Greg69 Sonof8787	000-0000-0007 (Account not targeted)
HENRY HENRYSON	876 Henry St. Henry, HY	henry39746	000-0000-0008 (Account not targeted)
IGOR IGORSON	7 Igor Rd. Igor, IG 00000	Igor124	000-0000-0009 (not targeted)
JERRY JERRYSON	789 Jerry Ave. Jerry, JY 00000	JerrySon JJ987978 jERRY9879 SoNOF234	000-0000-0010 (not targeted)
KIRBY KIRBYSON	2 Kirby Cir. Kirby, KI	Kirby	000-0000-0011 (not targeted)

FACTS AND CIRCUMSTANCES

COLLECTION OF CHILD PORNOGRAPHY

I have consulted with SA KEN LANNING of the FBI and he has relayed the following information to your affiant. SA LANNING is an author and a nationally recognized expert in the field of child pornography investigations and investigations of preferential child molesters. According to SA LANNING, the term preferential child molester has been used interchangeably with the more familiar term "pedophile." SA LANNING informed me of the following:

Preferential child molesters and child pornographers receive sexual gratification, stimulation and satisfaction from actual physical contact with children and from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs or other visual media) or from literature describing such activity.

They collect sexually explicit or suggestive materials (hard-core and soft-core pornography, whether of adults and/or children, and child erotica) consisting of photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. Further, they commonly use this type of sexually explicit material to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, and to demonstrate the desired sexual acts.

Child pornographers and preferential child molesters almost always maintain and possess their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, child erotica[2] etc.) in the privacy

---

[2] According to Dr. Ann Burgess, the author of Child Pornography and Sex Rings, (Lexington Books 1984), a book which deals with the subject of child pornography and pedophiles who collect and produce child pornography, "child erotica" are materials or items which are sexually arousing to pedophiles but which are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions. She defines it in her book as:

and security of their homes or some other secure location. According to SA LANNING, preferential child molesters and child pornographers typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica and video tapes for many years.

In addition, they often correspond and/or meet others to share information and materials; rarely destroy correspondence from other preferential child molesters and child pornographers; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

Preferential child molesters and child pornographers who collect sexually oriented pictures of minors are not without their child pornography and/or child erotica for any prolonged time period. This behavior, according to SA LANNING, has been documented by law enforcement officers involved in the

---

> any material, relating to children, that is sexually arousing to a given individual... [S]ome of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

id. at 83

investigation of child pornography throughout the United States.

COMPUTERS AND CHILD PORNOGRAPHY

MARK POLLITT is a SA with the FBI and has held that position for approximately twelve years. For the last four years he has been assigned principally to the investigation of computer related crimes and the forensic examination of electronic evidence. He has attended numerous computer related schools and is an instructor of the investigation of computer crimes, computer security, and computer forensic subjects for the FBI, the International Association of Computer Investigative Specialists, and the National Security Agency. SA POLLITT is designated as a Field Examiner for the FBI Laboratory's Computer Analysis and Response Team. In connection with these duties, he has been involved with the execution of over 30 search warrants involving computer evidence. He has conducted forensic examinations of over a hundred computers and thousands of diskettes and other removable media. SA POLLITT has participated in the investigation of child pornography violations and has executed search warrants on computers during the course of those investigations. He has conducted laboratory examinations of computers and storage media used by pedophiles. SA POLLITT has provided your affiant with the following information which is based on his knowledge, experience and training:

Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which pedophiles interact with each other. Child pornography formerly was produced using

cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings and telephone calls. Any reimbursement would follow these same paths.

The development of computers has changed all of this. Computers serve four functions in connection with child pornography. These are: production, communication, distribution, and storage.

Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed out directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically

easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as have methods that have been used in the past.

Previously, pedophiles had to rely on personal contact, U.S. Mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone lines. By connection to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial concerns, such as Compuserve and America-Online which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks. Some of these systems, including America Online, offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms." Contact with others in this online format can be either very open and anonymous, in front of everyone else who happens to be in the same room at the same time, or very private and personal in the form of person to person instant messages. This communication structure is ideal for the pedophile. The open and anonymous communication allows the user to

locate others of similar inclination and still maintain their anonymity. Once contact is established, it is then possible to send text messages and graphic images to a trusted conspirator. In addition to the use of large service providers, pedophiles and pornographers can use standard internet connections, such as those provided by business, universities, and government agencies to communicate with each other and to distribute pornography. These communications links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure and as anonymous as desired. These advantages are well known and are the foundation of commerce between pedophiles.

The computer's ability to store images in digital form makes them an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Hard drives with a capacity of one gigabyte are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is almost as easy to store an electronic image on a computer located half a world away as it is to store one locally. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and to save that image to storage in another country. Once this is done, there is no readily apparent evidence

at the scene of the crime. It is only with careful laboratory examination of electronic storage devices that it is possible to recreate the evidence trail.

The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. This pornography can be electronically mailed to anyone with access to a computer and modem. With the proliferation of commercial services that provide both electronic mail services and chat services, it is no wonder that the computer is the preferred method of distribution of pornographic materials. SA POLLITT advised that all of the above described information is known to him as the result of his education and experience in the investigation of computer related crime.

America Online

America Online (AOL) is a commercial computer service, also known as a commercial bulletin board, that offers electronic message bulletin boards to its subscribers enabling them to post messages that can be read by other AOL subscribers. It also provides an electronic mail service, enabling its subscribers to communicate individually by computer. Each AOL subscriber has access to a computer which communicates through a modem connected to a telephone line with the central computer system operated by AOL in Vienna, Virginia, within the Eastern District of Virginia. The subscriber can communicate with other subscribers, either in real time if the other subscribers are simultaneously on line, or

via electronic mail. With this system, subscribers can send messages to each other and attach files to those messages. These files (in computer format) may be items such as written documents, or graphic image files which are photographs that have been scanned into the computer system. Both types of files can be printed out by anyone who has them on their system and has a printer.

The equipment possessed by the FBI and the computer programs to be run by AOL pursuant to the proposed order will allow the simultaneous interception only of the targets' AOL electronic mail and attached files. Put another way, when an electronic mail message is delivered to or sent from a targeted account, the FBI will receive a duplicate of the message (and attachments, if any) in a separate mailbox accessible only to the agents. Therefore, the only communications via AOL that your affiant herewith seeks authorization to intercept are the electronic mail messages and attached computer files sent to and from the named interceptees.

Subscribers to the service provided by AOL are able to use screen names during communications which in most cases do not provide the subscriber's true name or identifying data. In addition, the subscriber can fill out a subscriber profile which corresponds to the subscriber's screen name. However, the subscriber can put any identifying data into this profile. There is no check by AOL as to the accuracy of subscriber information entered in this profile. Subscribers can easily access the

identifying data entered in any other subscriber's profile.

Information from SA D. Douglas Rehman

The information provided in this section of the affidavit was provided to me by Special Agent (SA) D. DOUGLAS REHMAN of the Florida Department of Law Enforcement. SA REHMAN has approximately nine and one half years experience in criminal investigation, including, but not limited to, narcotics, gambling, robbery, homicide, kidnapping, money laundering, arson, theft, sexual battery, and burglary. This investigative experience is from two and one half years as an inspector with the Illinois State Police and seven years as a SA with the Florida Department of Law Enforcement. REHMAN has one and one half years experience as a uniformed police officer for the cities of Jones, Florida, and Pitstown, Florida. He has a bachelor's degree in Criminal Justice from the University of Southern Coast and has attended the criminal investigative academies of both the Delaware State Police and the Florida Department of Law Enforcement.

Between September of 19xx and March of 19xx SA REHMAN provided the FBI with 111 image files and accompanying mail messages described in a list attached to this affidavit (Attachment "A"). An image file is so named because it contains images or photographs which have been converted into computer format by use of a scanner. An image file itself can be either a single image file (one picture only, also known as a computer file), or a multiple image file (two or more pictures). Multiple image files can be distinguished from single image files by the designation

"ZIP" at the conclusion of the file title. SA REHMAN obtained these image files in one of two ways. Some of the image files he obtained from a confidential informant (CI) who is a subscriber to AOL and who obtained them while signed on to AOL. The CI has provided information regarding the distribution of child pornography and other illegal activities on AOL to SA REHMAN from March of 19xx to the present. According to SA REHMAN, this CI has always proven to be reliable and has never provided false or misleading information. Three people have been arrested and a number of search warrants executed on the basis of information provided by the CI. SA REHMAN advised your affiant that the CI is simply a concerned citizen and not a criminal suspect who is trying to forge a better deal for himself.

The remainder of the 111 images files were obtained by SA REHMAN personally while signed on to AOL in an undercover capacity. The list that appears at Attachment "A" details the date on which the file was received by SA REHMAN or the CI from one or more of the interceptees listed below, and the title of the image file transmitted. The 111 image files listed in Attachment "A" constitute the entire universe of image files that are analyzed in this Affidavit. Those 111 image files, which were received by SA REHMAN or the CI in 111 separate transactions, consist of 290 separate computer files (individual pictures). The common thread running throughout these 111 computer transactions is that an individual using the screen name "BabyAby" was involved in each and every one of them, either as a recipient or as both a recipient

and a forwarder. The remaining 10 named interceptees were involved in a large number, but not all, of the 111 transactions, either as a recipient or as both a recipient and forwarder.

According to the electronic mail message accompanying each one of these 111 image files, they were each either forwarded by, received by, or received and then forwarded by an individual using the screen name "BabyAby." Pursuant to Federal Grand Jury subpoena issued by a grand jury sitting in this District, AOL identified "BabyAby" as ABE ABESON,123 Abe Lane, Abe, Abestate 00000, with AOL account number 000-0000-0001. Your affiant and other agents of the FBI have reviewed the 111 image files and accompanying mail messages provided by SA REHMAN. That review indicates that the overwhelming majority of these image files contain images depicting "minor" males engaged in "sexually explicit conduct" within the meaning of Title 18, United States Code, Section 2252, as defined in Title 18, United States Code, Section 2256. Specifically, these images depict unclothed "minor" males in various states of sexual arousal and many of the young males are engaged in sexual acts, as defined by Title 18, United States Code, Section 2256. Your affiant and other trained SA's of the FBI have examined these images and concluded that they depict individuals under the age of 18 years old engaging in actual or simulated sexual acts or lewd and lascivious exhibition of the genitals. (Copies of these image files, accompanied by their mail messages, are made Attachment "B" to this affidavit.)

Your affiant and other SAs of the FBI have reviewed the mail

messages which accompanied the 111 image files described above. Each mail message indicates the screen name of the AOL subscriber who first uploaded the image file onto the computer system, the screen name of the subscriber(s) to whom it was forwarded, the date and time of each transmission, and the title of the image file. Additionally, the mail message indicates the screen name of the AOL subscriber to whom the first recipient subsequently forwarded the image file, the date and time of that transmission, and the title of the file transmitted. In this manner, the screen name of each recipient and forwarder of a particular image, as well as the date and time of each transmission, is documented continuously until the document came into the possession of SA REHMAN. Some mail messages can be a number of pages long, thus documenting a large number of recipients and forwarders of a particular image file.

Detailed analysis of the mail messages that accompanied the 111 image files described above indicates that "BabyAby" regularly transmitted child pornography to, and received such transmissions from, a certain group of people whose screen names repeatedly appear on the mail messages attached to the image files. Of the most active screen names involved with the "BabyAby" child distribution network, investigation indicates that 11 are still subscribers to AOL. Below is a description of the involvement of each of the 11 named interceptees with the distribution of the 111 image files (290 computer files or pictures) listed in Attachment "A."

ABE ABESON

Between 9/6/xx and 12/18/xx, AOL account # 000-0000-0001, subscribed to by ABE ABESON was involved in all of the 111 computer transactions listed in attachment "A." (Two of the 111 transactions listed in Attachment "A" were transmissions of the same image file which contained a photograph of what "BabyAby" stated was himself. The person depicted is a fully clothed adult male. Therefore, the analysis as it pertains to ABE ABESON includes only 109 of the 111 total computer transactions reviewed.) During the course of those 109 transactions, 288 computer files (scanned images or photographs) were received, and of those, 238 were subsequently forwarded by an individual using that account under the screen name "BabyAby," either to one or more of the 11 other named interceptees or to other AOL subscribers. Your affiant has reviewed those image files and that review indicates that the majority of those files depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252. Your affiant notes that the individual using the screen name "BabyAby" routinely forwarded the above described computer files to many recipients in a single transaction. For example, on 11/25/XX, at 8:58 AM EST, "BabyAby" forwarded an image file to 22 recipients. That single image file contained 40 computer files (scanned images or photographs), all of which depict young boys engaged in "sexually explicit conduct." "BabyAby's" knowledge of the contents of what he was forwarding is clear from the text of his mail message in which he said, "Dudes!! This one is HOT!!!! A big one to download

but worth it!! 46 jpg files!!! I couldn't view them till I converted them to gifs. Enjoy!!!! Abe" (Your affiant cannot explain why there is a discrepancy between the number of computer files actually in the image file (40) and the number mentioned in "BabyAby's" text message (46).) Among the 22 screen names to whom "BabyAby" forwarded this file were "Ben123" "Carl235234," "Fred2435," "Yzaguirre" and "Kirby234" which are the screen names of 5 of the other 10 named interceptees. Additionally, "Dirk245" and "Edgar1," appear on the same mail message as having received the same image file from another sender, and "Greg7865" appears on that mail message as having both received and forwarded that same image file. Thus, including "BabyAby," a total of 9 of the 11 named interceptees either received or both received and forwarded the above described image file.

BEN BENSON

Between 10/30/XX and 12/4/XX, AOL account # 000-0000-0002, subscribed to by BEN B.B. BENSON was involved in 22 of the 111 computer transactions listed on Attachment "A." During the course of those transactions 111 of the 290 computer files (pictures) which are contained in the image files listed on Attachment "A," were received, and of those, nine were forwarded by a person using that account under the screen name "Ben1234" Having reviewed all of the 111 computer files (pictures) that were received by "Ben1234" it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in

violation of Title 18, United States Code, Section 2252.

CARL CARLSON

Between 9/6/xx and 12/18/xx, AOL account # 000-0000-003, subscribed to by CARL CARLSON, was involved in 29 of the 111 computer transactions listed on Attachment "A." During the course of those transactions, 138 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, 54 were subsequently forwarded by a person using that account number under the screen name "Carl1234" Having reviewed all of the 138 computer files (pictures) that were received by "Carl1234," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

On 5/17/XX, SA REHMAN, acting in an undercover capacity while signed on to AOL, received two computer transmissions from a person using the screen name "Carl1234." One computer file (scanned photograph) accompanied each of the two mail messages. Each computer file depicts what your affiant believes are unclothed minor males. These computer files (scanned photographs), accompanied by their mail messages, are contained in Attachment "C."

On 6/24/XX, SA REHMAN, again acting in an undercover capacity while signed on to AOL, received three computer transmissions from a person using the screen name "Carl1234." The computer files

(scanned photographs) that accompanied two of the three mail messages depict what your affiant believes are minor males in states of complete undress. These computer files (scanned photographs), accompanied by their mail messages, are contained in Attachment "C."

DIRK DIRKSEN

Between 8/31/xx and 12/18/xx, AOL account #s 000-0000-0004 (targeted account) and 004-0000-0000 (not a targeted account), subscribed to by DIRK DIRKSEN, were involved in 147 computer transactions. Because some of the 111 image files listed on Attachment "A" were sent or received by both accounts subscribed to by DIRK DIRKSEN, the total number of transactions associated with that subscriber is 147, more than the 111 listed on Attachment "A." During the course of those transactions 333 computer files (pictures) were received, and of those, 108 were subsequently forwarded by a person using those accounts under the screen names "DIrk1234" and "SonofDirk." Having reviewed all of the 333 computer files (pictures) that were received by "DIrk1234" and "SonofDirk," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

EDGAR EDGARSON

Between 9/3/xx and 12/3/xx AOL account # 000-0000-005, subscribed to by EDGAR EDGARSON, was involved in 95 of the 111 computer transactions listed on Attachment "A." During the course

of those transactions 184 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, 35 were subsequently forwarded by a person using that account under the screen name "Edgar1234" Having reviewed all of the 184 computer files (pictures) that were received by "Edgar1234," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

FRED FREDSON

Between 11/17/xx and 11/30/xx, AOL account # 000-0000-006, subscribed to by FRED FREDSON, was involved in 10 of the 111 computer transactions listed on Attachment "A." During the course of those transactions 85 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, 71 were subsequently forwarded by a person using that account under the screen name "Yzaguirre" Having reviewed all of the 85 computer files (pictures) that were received by "Yzaguirre," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

GREG GREGSON

Between 8/31/xx and 12/3/xx, AOL account # 000-0000-0007, subscribed to by GREG GREGSON, was involved in 61 of the 111

computer transactions listed on Attachment "A." During the course of those transactions, 177 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, 12 were subsequently forwarded by a person using that account under the screen name "Greg1234." Having reviewed all of the 177 computer files (pictures) that were received by "Greg1234," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

HENRY HENRYSON

Between 9/6/xx and 10/31/xx, AOL account # 000-0000-008, subscribed to by HENRY HENRYSON, was involved in 77 of the 111 computer transactions listed on Attachment "A." During the course of those transactions, 137 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, none were forwarded by a person using that account under the screen name "Henry69." Having reviewed all of the 137 computer files (pictures) that were received by "Henry69," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

IGOR IGORSON

Between 9/26/xx and 12/4/xx, AOL account # 000-0000-009,

subscribed to by IGOR IGORSON, was involved in 57 of the 111 computer transactions listed on Attachment "A." During the course of those transactions 180 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, none were forwarded by a person using that account under the screen name "Igor3425" Having reviewed all of the 180 computer files (pictures) that were received by "Igor3425," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

JERRY JERRYSON

Between 9/6/xx and 9/26/xx, AOL account # 000-0000-010, subscribed to by JERRY JERRYSON, was involved in 45 of the 111 computer transactions listed on Attachment "A." During the course of those transactions, 49 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, none were forwarded by a person using that account under the screen name "Jerry45." Having reviewed all of the 49 computer files (pictures) that were received by "Jerry45," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

KIRBY KIRBYSON

Between 9/6/xx and 12/4/xx AOL account # 000-0000-011,

subscribed to by KIRBY KIRBYSON, was involved in 98 of the 111 computer transactions listed on Attachment "A." During the course of those transactions, 231 of the 290 computer files (pictures), which are contained in the image files listed on Attachment "A," were received, and of those, none were forwarded by a person using that account under the screen name "Kirby." Having reviewed all of the 231 computer files (pictures) that were received by "Kirby," it is your affiant's opinion that a substantial majority of them depict "minor" males engaged in "sexually explicit conduct" as defined by Title 18, United States Code, Section 2256, in violation of Title 18, United States Code, Section 2252.

INFORMATION DERIVED FROM AOL'S DETAILED BILLING RECORDS

Pursuant to a search warrant issued by Magistrate Judge Law V. Equity of the Eastern District of Virginia and executed on America Online, 8619 Westwood Center Drive, Vienna, Virginia, on 6/19/XX, your affiant and other SAs of the FBI obtained subscriber information and detailed billing records pertaining to the named interceptees, listed above, and their AOL account numbers. Analysis of those records indicates the following regarding the named interceptees:

ABE ABESON

AOL account number 000-0000-001, subscribed to by ABE ABESON, was activated 200 times between 1/1/xx and 6/19/xx, most recently on 6/19/xx.

BEN BENSON

AOL account number 000-0000-002, subscribed to by BEN BENSON,

was activated 713 times between 1/1/xx and 6/18/xx, most recently on 6/18/xx.

CARL CARLSON

AOL account number 000-0000-003, subscribed to by CARL CARLSON, was activated 339 times between 1/1/xx and 6/18/xx, most recently on 6/18/xx.

DIRK DIRKSEN

DIRK DIRKSEN subscribes to two AOL accounts. Between 1/1/xx and 6/19/xx, AOL account number 000-0000-004, subscribed to by DIRKSEN, was activated 701 times, most recently on 6/19/xx. Between 1/1/xx and 3/12/xx, AOL account number 004-0000-000, also subscribed to by DIRKSEN, was activated 62 times, most recently on 3/12/xx. This latter account is not a target of the electronic surveillance that is applied for herewith.

EDGAR EDGARSON

AOL account number 000-0000-005, subscribed to by EDGAR EDGARSON, was activated 439 times between 1/2/xx and 6/18/xx, most recently on 6/18/xx.

FRED FREDSON

AOL account number 000-0000-006, subscribed to by FRED FREDSON, was activated 726 times between 1/1/xx and 6/19/xx, most recently on 6/19/xx.

GREG GREGSON

AOL account number 000-0000-007, subscribed to by GREG GREGSON, was activated 146 times between 1/1/xx and 6/16/xx, most recently on 6/16/xx.

HENRY HENRYSON

AOL account number 000-0000-008, subscribed to by HENRY HENRYSON, was activated 222 times between 1/1/xx and 6/18/xx, most recently on 6/18/xx.

IGOR IGORSON

AOL account number 000-0000-009, subscribed to by IGOR IGORSON, was activated 364 times between 1/1/xx and 6/18/xx, most recently on 6/18/xx.

JERRY JERRYSON

AOL account number 000-0000-010, subscribed to by JERRY JERRYSON, was activated 203 times between 1/2/xx and 6/19/xx, most recently on 6/19/xx.

KIRBY KIRBYSON

AOL account number 000-0000-011, subscribed to by KIRBY KIRBYSON, was activated 456 times between 1/1/xx and 6/18/xx, most recently on 6/18/xx.

On the basis of the above described computer transmissions, your affiant respectfully submits that there is probable cause to believe that the eleven above described AOL subscribers are collectors of child pornography. I base this opinion on the quantity and frequency of their transmission and/or receipt of child pornography which is consistent with the characteristics of a child pornographer. I further base this opinion upon examination of the computer files which these individuals actually traded and exchanged on AOL (Attachment "B" to this Affidavit), on the highly suggestive user names chosen by many of these individuals, and on

the explicit electronic mail messages which accompanied many of the computer files traded by these individuals.

NEED FOR INTERCEPTION

Need for Interception of Electronic Communications

Based upon your affiant's training and experience, as well as the experience of the other Special Agents of the FBI, and based upon all of the facts set forth herein, it is your affiant's belief that the interception of electronic communications is the only available technique that has a reasonable likelihood of securing the evidence necessary to achieve the goals of this investigation. As discussed above, those goals include the determination of the extent of ABE ABESON's child pornography distribution network, to include the identities of individuals who supply child pornography to ABE ABESON, the identities of those to whom ABESON and the other named interceptees forward such pornography, and to determine the methods of operation used by the participants in that network.

Your affiant states that the following investigative procedures, which are usually employed in this type of criminal investigation, have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ.

ALTERNATIVE INVESTIGATIVE TECHNIQUES

Physical Surveillance

Although physical surveillance is a technique that is very useful in many types of investigations, its usefulness is very limited in this type of investigation. Because child pornography can be easily transmitted from one computer terminal to another located in a distant part of the country with a few keystrokes, and because

this activity occurs behind closed doors in the privacy of homes and offices, physical surveillance of the subjects would reveal very little. Although it would prove that a particular individual was at a certain location at a certain time, it would not prove that that person was seated at a computer, nor would it provide the content of a particular computer transmission, which is the criminal conduct under investigation. Although physical surveillance has proven valuable in identifying some activities of the targets of this investigation, its use is of limited value unless used in conjunction with other investigative techniques, including electronic surveillance. Physical surveillance, even if highly successful, has not succeeded in gathering sufficient evidence of the criminal activity under investigation. Physical surveillance of the alleged conspirators has not and will not establish conclusively the elements of the violations and has not and most likely will not establish conclusively the identities of various conspirators. In addition, surveillance is not expected to enlarge upon information now available; rather, such prolonged or regular surveillance of the movements of the suspects would most likely be noticed, causing them to become more cautious in their illegal activities, to flee to avoid further investigation and prosecutÃâåÉ'`",åßÑ

SUPERIOR COURT OF NEW JERSEY
COUNTY OF MONMOUTH

STATE OF NEW JERSEY)
SS. AFFIDAVIT
COUNTY OF MONMOUTH)

I, Detective Sergeant Michael T. Geraghty #4385, of full age, having been duly sworn to law upon my oath depose and say: I am a member of the New Jersey State Police and have probable cause to believe that on the premises known as 322 First Street, Apartment 2, Northfield Twp., Monmouth County, New Jersey and more particularly described as:

A brown, two story, multi-family residence which is set back approximately 75 feet from the roadway. Access to the residence is made via a driveway entrance off of First Street. The numerals "322" are affixed to the front fence post of a cyclone fence that delineates the adjacent property, Holy Trinity Elementary School. A row of small trees and bushes provide privacy from traffic on First Street. 322 First Street is located on the West side of the street at the intersection of Trinity and First Street. A yellow fire hydrant is located in front of this residence. Apartment 2 is located on the second floor of the residence.

there has been and now is located certain property which has been used in connection with the violation of the penal laws of the State of New Jersey, or which constitute evidence of, or tends to show the violation of Endangering the Welfare of a Child (N.J.S.A. 2C:4-4a) and Conspiracy (N.J.S.A. 2C:5-2) to commit this offense.

The said property consisting of any and all computers, including all related computer hardware, software, documentation, passwords and data security devices, magnetic media and peripheral computer equipment; telephones, phone books, phone bills, address books, correspondence, diaries, or any other material which would indicate additional victims or suspects involved in endangering the welfare of children; bank statements, and other indicators of occupancy; keys, statements and billings which show the location and the identity of safe deposit boxes and/or storage facilities; any and all records, business and otherwise, pertaining to the above mentioned crimes, including but not limited to, correspondence, notes, papers, ledgers, telephone message slips, memoranda, telexes, facsimiles; Any bank records, canceled checks, receipts and documents.

The facts tending to establish the grounds for this application and the probable cause of my belief that such grounds exist are as follows:

1. I am a member of the New Jersey State Police. In such capacity, I am empowered to conduct investigations of, and to make arrests for, the crimes of Endangering the Welfare of a Child, 2C:24-4a. I am currently responsible for the investigation detailed hereinafter involving the foregoing offense in aid of which investigation this Application is made.

2. I have been a member of the New Jersey State Police for over eleven (11) years. I am currently assigned to the High Technology Crimes and Investigations Support Unit of the Investigations Section. As such I am responsible for investigating criminal activity and supervising the investigations of criminal activity, including computer-related crimes.

In addition to graduating from the New Jersey State Police Academy, I have attended the following advanced courses given at the New Jersey State Police Academy:

Criminal Investigations School
Interview and Interrogation School

In addition, I have attended the following courses given by outside agencies:

SEARCH Computer Crimes Investigations School
NY/NJ CCIA Computer Forensics Seminar
HTCIA Telecommunications Crimes Seminar
HTCIA Cellular Fraud Seminar
Advanced Personal Computer Maintenance and Repair

3. I have been certified by the Police Training Commission as an Instructor. I have provided instruction and given lectures on numerous occasions on the topic of investigating computer crimes. These lectures have been given to Federal, State, County and local law enforcement agencies. I have acted as a consultant for numerous Federal, State, County and local law enforcement agencies throughout the Country, as well as various international law enforcement agencies. I am the past-president of the Northeast Chapter of the High Technology Crimes Investigators Association. I am a member of the High Tech Crimes Computer Network where I am the moderator of the Computer Forensics forum. I am a member of the National Computer Security Association. I am a member of the NY/NJ Computer Crimes Investigators Association and I am the New Jersey State Police Superintendent's designee on the National Association of Attorneys General Internet Work Group.

I have read numerous publications and documents regarding the methodologies of high technology crimes.

4. I have been involved in numerous criminal investigations which have resulted in the arrest and conviction of more than one hundred persons. These investigations and subsequent arrests involved the crimes of Murder, Kidnapping, Aggravated Sexual Assault, Sexual Assault, Endangering the Welfare of Children (Including the Production, Reproduction, Distribution and Possession of Child Pornography), Unauthorized Access to a Computer System, various weapons and narcotics offenses, as well as other violations of the New Jersey Statutes.

In addition, I have been involved in the preparation and execution of numerous search warrants. As a result of my previous aforementioned investigations I have received several commendations.

5. I have testified before the United States Congress on the subject of computer crimes investigations and child pornography. I have been qualified as an expert in United States Federal Court, Springfield, Illinois in computer crimes investigations and computer forensics. I am currently charged by the National Center for Missing and Exploited Children with developing the nation-wide course curriculum for training state and local law enforcement officers in the investigation of on-line crimes against children. As a result of my training and experience I am familiar with the methods employed by individuals to store, maintain, manufacture, transmit, distribute and reproduce child pornography using computers and online services, including Internet Service Providers.

6. For purposes of this affidavit, unless otherwise specifically indicated, the term "computer" refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communications devices (such as internal modems or fax cards) along with any other hardware stored / housed internally. Thus computer refers to hardware, software and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package the term computer system is used. Information refers to all the information on a computer system including both software applications and data.

Hardware

Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

Software

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric, or other special, characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

The facts tending to establish the grounds for this application and the probable cause for my belief that such grounds exist are as follows:

7. On Thursday, February 5, 1998, this Affiant received an electronic mail message from Jim Hart, the Network Administrator of SpiderWeb Communications, Incorporated, 4596 Route 9 North, Monmouth Valley Corporate Center, Howell Township, New Jersey. Mr. Hart asked me to look at the World Wide Web site. He further advised that the contents of the site appeared to be illegal.

8. On February 11, 1998 I accessed the Internet World Wide Web site http://www.SpiderWeb.net/~Caveman. Upon accessing this site I noted that the site is titled "An Unofficial Laika Home Page". As outlined by the site's author, Caveman, Laika is a young Finnish female whose approximate age is 12 years old. This web site is host to several pages that provide biographical information about Laika, several depictions of erotic images of her, and links to two other World Wide Web sites. These linked sites are: http://www.members.tripod.com/~logroll and http://www.geocities.com/RainForest/Brush/2x0. The images of Laika linked to at these sites contain graphic depictions of child erotica and child pornography. Upon viewing these images I downloaded same. In addition, Caveman offers for sale a CD-ROM disk containing images that are described as "nude-glamour or nude-portrait"

images. The World Wide Web page http://www.SpiderWeb.net/~Caveman/goods-cd.htm includes a series of thumbnail sample images that are included on the CD-ROM. These thumbnails contain images of child pornography and child erotica.

9. A Deja News search of the Internet Usenet Newsgroups for articles posted by Caveman revealed that Caveman has posted numerous articles to the following newsgroups: alt.sex.incest, alt.fan.teen.starlets, alt.binaries.pictures.erotica.teen.female, alt.binaries.erotica.teen, alt.binaries.pictures.erotica.pre-teen, alt.binaries.pictures.erotica.schoolgirls, alt.sex.pedophilia and alt.binaries.pictures.child.erotica.female. In addition, Caveman has numerous articles posted to newsgroups pertaining to bicycling, and the sale of bicycle parts. These postings have links back to http://www.SpiderWeb.net/Caveman where he maintains advertisements for the sale of various bicycle parts.

10. Based upon the forgoing facts, on February 19, 1998 I appeared before the Honorable Judge Ricciardi of the Monmouth County Superior Court and made application for Communication Data Warrants ordering the Internet Service Providers that host Caveman's web pages and files to turn over subscriber information and computer logs for Caveman. Judge Ricciardi found sufficient probable cause for such an order and authorized said Warrants.

11. On February 19, 1998 I served the above mentioned warrants on the three Internet Service Providers. Records received from SpiderWeb Communications, Inc. identified Caveman as Patrick O'Connor of 322 First Street, Northfield, NJ, telephone number (908)233-1143. Records also received from Tripod, Inc., revealed the subscriber of the World Wide Web site http://www.members.tripod.com/~logroll is Ange O'Connor, 322 1st Street, Northfield, NJ. His listed date of birth is 5/20/1976. The password for both the SpiderWeb account and the Tripod account is futura.

12. On February 20, 1998 I proceeded to 322 First Street Northfield, NJ to obtain a description of the premises and to determine its occupants. This residence is a brown, two story, multi-family residence which is set back approximately 75 feet from the roadway. Access to the residence is made via a driveway entrance off of First Street. The numerals "322" are affixed to the front fence post of a cyclone fence that delineates the adjacent property, Holy Trinity Elementary School. A row of small trees and bushes provide privacy from traffic on First Street. 322 First Street is located on the West side of the street at the intersection of Trinity and First Street. A yellow fire hydrant is located in front of this residence. According to Lt. Kelleher of the Northfield Police Department, apartment 2 is located on the second floor of the residence.

During my observation of the residence I noted two vehicles parked in the driveway at the end closest to the house. One vehicle, a green Oldsmobile sport utility vehicle bearing New Jersey registration UM127T is registered to Hilda Smith of 322 First Street, Northfield, NJ. The second vehicle, a blue Toyota four-wheel drive wagon with bicycle racks affixed to it roof displayed New Jersey registration KV655K. According to New Jersey Division of Motor Vehicles records this vehicle is registered to Patrick A. O'Connor, 322 First Street, Apartment 2, Northfield, New Jersey. A driver's license lookup for Patrick A. O'Connor listed his date of birth as 12/25/74.

He is described as a male, 5' 8" tall, with brown eyes and weight code 1. While making my observations of the residence a male matching the description of Patrick exited the residence and proceeded to drive away in the blue Toyota wagon. I followed this vehicle to a residence in Northfield where the driver proceeded to perform yard work and other landscaping tasks.

13. A search of the New Jersey Motor Vehicle database revealed no driver's license nor driver's registration were issued to an Patrick O'Connor. No other person with the last name O'Connor, other than Patrick is listed in the New Jersey Division of Motor Vehicle database at the 322 First Street, Northfield, New Jersey address.

14. On February 21, 1998 I again accessed the web site http://www.SpiderWeb.net/~Caveman maintained by Patrick O'Connor of 322 First Street, Northfield, New Jersey. I noted that this web site is still operational and provides links to images of child pornography and child erotica.

15. On February 24, 1998 I proceeded to the Northfield Post Office where I spoke with the Postmaster. He confirmed that Patrick O'Connor receives mail at 322 First Street, Northfield, New Jersey.

16. Based upon my training and experience this Affiant knows that searching and seizing information from computers often requires law enforcement personnel to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a controlled environment. Computer storage devices (like hard disks, diskettes, tapes, laser disks, and other data cartridges) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site. In addition, searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

This Affiant also knows that searching computerized information for evidence or instrumentalities of crime commonly requires law enforcement personnel to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a controlled environment. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the

system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

17. There is further probable cause to believe that records pertaining to the distribution of child pornography are maintained in Patrick O'Connor's (Caveman's) private electronic mail, computer files, computer storage facilities or other data storage facilities, and that within these files are contained certain records, namely correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles and documents that identify those to whom Patrick O'Connor has transferred child pornography.

18. Based on the contents of this affidavit, my training and experience and my investigation to date I have probable cause to believe and do believe that there has been and now is located on the mentioned premises, certain property, which has been used in connection with the violation of the penal laws of the State of New Jersey, or which constitute evidence of, or tends to show the violation of Endangering the Welfare of a Child (N.J.S.A. 2C:24-4a). All of the materials requested for seizure are components necessary to obtain evidence that will tend show that the person under investigation has committed the above listed crime.

WHEREFORE, I respectfully request that a search warrant be issued for the property described above, including basements, attics, storage spaces, appurtenant buildings, surrounding grounds and all containers therein or thereon which could contain any of the items sought; and that it be executed as prescribed by law.

It is also requested that this Affidavit and Order be sealed until further notice to this Court.

_____

Detective Sergeant Michael T. Geraghty #4385
High Technology Crimes & Investigations Support Unit
New Jersey State Police

SWORN AND SUBSCRIBED TO
BEFORE ME THIS DAY OF FEBRUARY, 1998

_____

Judge of the Superior Court

SUPERIOR COURT OF NEW JERSEY
COUNTY OF MONMOUTH

IN THE MATTER OF THE APPLICATION OF)
THE STATE OF NEW JERSEY FOR AN ORDER)
AUTHORIZING THE OBTAINING OF)
SUBSCRIBER INFORMATION FOR INTERNET)
ACCOUNTS: **javamon@webspan.net;**) **AFFIDAVIT**
http://www.members.tripod.com/~rolijun;)
AND **http://www.geocities.com/RainForest/Canopy/1301**)
AND FOR ALL SYSTEM AND SITE ACCESS LOGS)
FOR SAID INTERNET ACCOUNTSFOR THE PERIOD)
JANUARY 1, 1998 TO THE PRESENT.)

STATE OF NEW JERSEY)
SS.
COUNTY OF MONMOUTH)

I, Detective Sergeant Michael T. Geraghty #4385, of full age, having been duly sworn to law upon my oath depose and say: I am a member of the New Jersey State Police

I am applying to the court for the purpose of securing subscriber information for Internet accounts:

(1) javamon@webspan.net and corresponding World Wide Web site http://www.webspan.net/~javamon which is maintained and hosted by Internet Service Provider, Webspan Communications, Incorporated, Union Valley Corporate Center, 4596 Route 9 North, Howell Township, Monmouth County, New Jersey

(2) http://www.members.tripod.com/~rolijun maintained and hosted by Internet Service Provider Tripod, Incorporated, 160 Water Street, Williamstown, Massachusetts.

(3) http://www.geocities.com/RainForest/Canopy/1301 maintained and hosted by Internet Service Provider, GeoCities, 1918 Main Street, Third Floor, Santa Monica, California.

I am also seeking all system access logs, file transfer logs and mail logs for said Internet accounts which will detail all authorized accesses to said accounts by their subscriber. I am further seeking and all site access logs for said Internet accounts' corresponding World Wide Web pages for the period January 1, 1998 to the present. This information is sought as evidence of the crime Endangering the Welfare of a Child (N.J.S.A. 2C:24-4a(5)(a)) in the Township of Howell, Monmouth County, New Jersey.

The facts tending to establish the grounds for this application and the probable cause of my belief that such grounds exist are as follows:

1. I am a member of the New Jersey State Police. In such capacity, I am empowered to conduct investigations of, and to make arrests for, the crimes of Endangering the Welfare of a Child, 2C:24-4a. I am currently responsible for the investigation detailed hereinafter involving the foregoing offense in aid of which investigation this Application is made.

2. I have been a member of the New Jersey State Police for over eleven (11) years. I am currently assigned to the High Technology Crimes and Investigations Support Unit of the Investigations Section. As such I am responsible for investigating criminal activity and supervising the investigations of criminal activity, including computer-related crimes.

In addition to graduating from the New Jersey State Police Academy, I have attended the following advanced courses given at the New Jersey State Police Academy:

Criminal Investigations School
Interview and Interrogation School

In addition, I have attended the following courses given by outside agencies:

SEARCH Computer Crimes Investigations School
NY/NJ CCIA Computer Forensics Seminar
HTCIA Telecommunications Crimes Seminar
HTCIA Cellular Fraud Seminar
Advanced Personal Computer Maintenance and Repair

3. I have been certified by the Police Training Commission as an Instructor. I have provided instruction and given lectures on numerous occasions on the topic of investigating computer crimes. These lectures have been given to Federal, State, County and local law enforcement agencies. I have acted as a consultant for numerous Federal, State, County and local law enforcement agencies throughout the Country, as well as various international law enforcement agencies. I am the vice-president of the Northeast Chapter of the High Technology Crimes Investigators Association. I am a member of the High Tech Crimes Computer Network where I am the moderator of the Computer Forensics forum. I am a member of the National Computer Security Association. I am a member of the NY/NJ Computer Crimes Investigators Association and I am the New Jersey State Police Superintendent's designee on the National Association of Attorneys General Internet Work Group.

I have read numerous publications and documents regarding the methodologies of high technology crimes.

4. I have been involved in numerous criminal investigations which have resulted in the arrest and conviction of more than one hundred persons. These investigations and subsequent arrests involved the crimes of Murder, Kidnapping, Aggravated Sexual Assault, Sexual Assault, Endangering the Welfare of Children (Including the Production, Reproduction, Distribution and Possession of Child Pornography), Unauthorized Access to a Computer System, various weapons and narcotics offenses, as well as other violations of the New Jersey Statutes. In addition, I have been involved in the preparation and execution of numerous search warrants. As a result of my previous aforementioned investigations I have received several commendations.

I have testified before the United States Congress on the subject of computer crimes investigations and child pornography. As a result of my training and experience I am familiar with the methods employed by individuals to store, maintain, manufacture, transmit, distribute and reproduce child pornography using computers and online services, including Internet Service Providers.

The facts tending to establish the grounds for this application and the probable cause for my belief that such grounds exist are as follows:

5. On Thursday, February 5, 1998, this Affiant received an electronic mail message from Jim Hart, the Network Administrator of Webspan Communications, Incorporated, 4596 Route 9 North, Union Valley Corporate Center, Howell Township, New Jersey. Mr. Hart asked me to look at the World Wide Web site. He further advised that the contents of the site appeared to be illegal.

6. On February 11, 1998 I accessed the Internet World Wide Web site http://www.webspan.net/~javamon. Upon accessing this site I noted that the site is titled "An Unofficial Laika Home Page" (See Attachment A). As outlined by the site's author, javamon, Laika is a young Finnish female whose approximate age is 12 years old. This web site is host to several pages that provide biographical information about Laika, several depictions of erotic images of her, and links to at least two other World Wide Web sites (See Attachment B). These linked sites are: http://www.members.tripod.com/~rolijun and http://www.geocities.com/RainForest/Canopy/1301. The images of Laika linked to at these sites contain graphic depictions of child erotica and child pornography (See Attachment C). In addition, javamon offers for sale a CD-ROM disk containing images that are described as "nude-glamour or nude-portrait" images. The World Wide Web page http://www.webspan.net/~javamon/goods-cd.htm includes a series of thumbnail sample images that are included on the CD-ROM. These thumbnails contain several images of young nude females (See Attachment D).

7. A Deja News search of the Internet Usenet Newsgroups for articles posted by javamon revealed that javamon has posted numerous articles to the following newsgroups: alt.sex.incest, alt.fan.teen.starlets, alt.binaries.pictures.erotica.teen.female, alt.binaries.erotica.teen, alt.binaries.pictures.erotica.pre-teen, alt.binaries.pictures.erotica.schoolgirls, alt.sex.pedophilia, alt.binaries.pictures.child.erotica.female as well as other newsgroups.

8. Based upon the forgoing facts as well as my training and experience and the investigation to date, I have probable cause to believe and do believe that the subscriber information records and logs maintained by the aforementioned Internet Service Providers will provide evidence as to the identity of those responsible for perpetrating the crime of Endangering the Welfare of a Child, N.J.S.A. 2C:24-4a(5)(a).

WHEREFORE, I respectfully request an Order be issued directing

1. Webspan Communications, Incorporated, Union Valley Corporate Center, 4596 Route 9 North, Howell Township, Monmouth County, New Jersey

2. Tripod, Incorporated, 160 Water Street, Williamstown, Massachusetts.

3. GeoCities, 1918 Main Street, Third Floor, Santa Monica, California.

or any other applicable telecommunications carrier to provide to me copies of subscriber information records for the Internet accounts javamon@webspan.net; http://www.webspan.net/~javamon; http://www.members.tripod.com/~rolijun; and http://www.geocities.com/RainForest/Canopy/1301 for the time period January 1, 1998 to the present.

It is also requested that this Affidavit and Order be sealed until further notice to this Court.

_____

Detective Sergeant Michael T. Geraghty #4385
High Technology Crimes & Investigations Support Unit
New Jersey State Police

SWORN AND SUBSCRIBED TO
BEFORE ME THIS DAY OF FEBRUARY, 1998

_____

Judge of the Superior Court

SUPERIOR COURT OF NEW JERSEY
COUNTY OF MONMOUTH

IN THE MATTER OF THE APPLICATION OF)
THE STATE OF NEW JERSEY FOR AN ORDER)
AUTHORIZING THE OBTAINING OF SUBSCRIBER)
INFORMATION FOR INTERNET ACCOUNT:)
http://www.geocities.com/RainForest/Brush/2x0) **WARRANT**
AND FOR ALL SYSTEM AND SITE ACCESS LOGS)
FOR SAID INTERNET ACCOUNTS FOR THE PERIOD)
JANUARY 1, 1998 TO THE PRESENT.)

STATE OF NEW JERSEY)
SS.
COUNTY OF MONMOUTH)

TO: ANY LAW ENFORCEMENT OFFICER

This matter having been opened to the Court by the *ex parte* Application of the State of New Jersey, and the Court having had the opportunity to examine the supporting Affidavit of Michael T. Geraghty, a Trooper with the New Jersey State Police; and

Good cause being shown, therefore, in that the facts presented in the said Application show probable cause for believing that the OBTAINING OF SUBSCRIBER INFORMATION FOR INTERNET ACCOUNT http://www.geocities.com/RainForest/Brush/2x0 AND TO OBTAIN SYSTEM ACCESS LOGS, FILE TRANSFER LOGS, MAIL LOGS, AND WEB PAGE ACCESS LOGS FOR WORLD WIDE WEB SITE http://www.geocities.com/RainForest/Brush/2x0 constitute evidence of, tend to show violations of, tend to identify victims of, and/or tend to identify individuals engaged in activities in violation of Endangering the Welfare of a Child (N.J.S.A. 2C:24-4a(5)(a))

It is on this ___ day of _____, 1998, ***ORDERED*** that authority be and the same is granted to Detective Sergeant Michael T. Geraghty, a member of the New Jersey State Police, to obtain SUBSCRIBER INFORMATION FOR INTERNET ACCOUNT http://www.geocities.com/RainForest/Brush/2x0 AND TO OBTAIN SYSTEM ACCESS LOGS, FILE TRANSFER LOGS, MAIL LOGS, AND WEB PAGE ACCESS LOGS FOR WORLD WIDE WEB SITE http://www.geocities.com/RainForest/Brush/2x0 from January 1, 1998 to the present from Geocities.

It is further ***ORDERED*** that a copy of this Order be delivered to Geocities and the said information be released to Detective Sergeant Michael T. Geraghty, or any other member of the New Jersey State Police;

It is ***FURTHER ORDERED*** that this ***ORDER*** and Affidavit as well as all exhibits attached to the Affidavit are hereby sealed and are not to be released except upon motion to the Court and further order of the Court upon such conditions as the Court may permit.

_____
Judge of the Superior Court

SUPERIOR COURT OF NEW JERSEY
COUNTY OF MONMOUTH

IN THE MATTER OF THE APPLICATION OF)
THE STATE OF NEW JERSEY FOR AN ORDER)
AUTHORIZING THE OBTAINING OF)
SUBSCRIBER INFORMATION FOR INTERNET)
ACCOUNT: http://www.members.tripod.com/~logroll) **WARRANT**
AND FOR ALL SYSTEM AND SITE ACCESS LOGS)
FOR SAID INTERNET ACCOUNTS FOR THE PERIOD)
JANUARY 1, 1998 TO THE PRESENT.)

STATE OF NEW JERSEY)
SS.
COUNTY OF MONMOUTH)

TO: ANY LAW ENFORCEMENT OFFICER

This matter having been opened to the Court by the *ex parte* Application of the State of New Jersey, and the Court having had the opportunity to examine the supporting Affidavit of Michael T. Geraghty, a Trooper with the New Jersey State Police; and

Good cause being shown, therefore, in that the facts presented in the said Application show probable cause for believing that the OBTAINING OF SUBSCRIBER INFORMATION FOR INTERNET ACCOUNT http://www.members.tripod.com/~logroll AND TO OBTAIN SYSTEM ACCESS LOGS, FILE TRANSFER LOGS, MAIL LOGS, AND WEB PAGE ACCESS LOGS FOR WORLD WIDE WEB SITE http://www.members.tripod.com/~logroll constitute evidence of, tend to show violations of, tend to identify victims of, and/or tend to identify individuals engaged in activities in violation of Endangering the Welfare of a Child (N.J.S.A. 2C:24-4a(5)(a))

It is on this ___ day of _____, 1998, ***ORDERED*** that authority be and the same is granted to Detective Sergeant Michael T. Geraghty, a member of the New Jersey State Police, to obtain SUBSCRIBER INFORMATION FOR INTERNET ACCOUNT http://www.members.tripod.com/~logroll AND TO OBTAIN SYSTEM ACCESS LOGS, FILE TRANSFER LOGS, MAIL LOGS, AND WEB PAGE ACCESS LOGS FOR WORLD WIDE WEB SITE http://www.members.tripod.com/~logroll from January 1, 1998 to the present from Webspan Communications, Incorporated.

It is further ***ORDERED*** that a copy of this Order be delivered to Tripod, Incorporated and the said information be released to Detective Sergeant Michael T. Geraghty, or any other member of the New Jersey State Police;

It is ***FURTHER ORDERED*** that this ***ORDER*** and Affidavit as well as all exhibits attached to the Affidavit are hereby sealed and are not to be released except upon motion to the Court and further order of the Court upon such conditions as the Court may permit.

_____
Judge of the Superior Court

SUPERIOR COURT OF NEW JERSEY
COUNTY OF MONMOUTH

IN THE MATTER OF THE APPLICATION OF)
THE STATE OF NEW JERSEY FOR AN ORDER)
AUTHORIZING THE OBTAINING OF)
SUBSCRIBER INFORMATION FOR INTERNET)
ACCOUNT: **Caveman@SpiderWeb.net**) **WARRANT**
AND FOR ALL SYSTEM AND SITE ACCESS LOGS)
FOR SAID INTERNET ACCOUNTS FOR THE PERIOD)
JANUARY 1, 1998 TO THE PRESENT.)

STATE OF NEW JERSEY)
SS.
COUNTY OF MONMOUTH)

TO: ANY LAW ENFORCEMENT OFFICER

This matter having been opened to the Court by the *ex parte* Application of the State of New Jersey, and the Court having had the opportunity to examine the supporting Affidavit of Michael T. Geraghty, a Trooper with the New Jersey State Police; and

Good cause being shown, therefore, in that the facts presented in the said Application show probable cause for believing that the OBTAINING OF SUBSCRIBER INFORMATION FOR INTERNET ACCOUNT Caveman@SpiderWeb.net AND TO OBTAIN SYSTEM ACCESS LOGS, FILE TRANSFER LOGS, MAIL LOGS, AND WEB PAGE ACCESS LOGS FOR WORLD WIDE WEB SITE http://www.SpiderWeb.net/~Caveman constitute evidence of, tend to show violations of, tend to identify victims of, and/or tend to identify individuals engaged in activities in violation of Endangering the Welfare of a Child (N.J.S.A. 2C:24-4a(5)(a))

It is on this ___ day of _____, 1998, ***ORDERED*** that authority be and the same is granted to Detective Sergeant Michael T. Geraghty, a member of the New Jersey State Police, to obtain SUBSCRIBER INFORMATION FOR INTERNET ACCOUNT Caveman@SpiderWeb.net AND TO OBTAIN SYSTEM ACCESS LOGS, FILE TRANSFER LOGS, MAIL LOGS, AND WEB PAGE ACCESS LOGS FOR WORLD WIDE WEB SITE http://www.SpiderWeb.net/~Caveman from January 1, 1998 to the present from SpiderWeb Communications, Incorporated.

It is further ***ORDERED*** that a copy of this Order be delivered to SpiderWeb Communications, Incorporated and the said information be released to Detective Sergeant Michael T. Geraghty, or any other member of the New Jersey State Police;

It is ***FURTHER ORDERED*** that this ***ORDER*** and Affidavit as well as all exhibits attached to the Affidavit are hereby sealed and are not to be released except upon motion to the Court and further order of the Court upon such conditions as the Court may permit.

_____
Judge of the Superior Court

STATE OF NEW JERSEY :
SS ***SEARCH WARRANT***
COUNTY OF MONMOUTH :

TO: ***ANY LAW ENFORCEMENT OFFICER***

Detective Sergeant Michael Geraghty #4385, having personally appeared on this date, before me, a Judge of the Superior Court, State of New Jersey, upon an application for the issuance of a Search Warrant on the grounds that he has probable cause to believe that in and upon a certain premises within as 322 First Street, Apartment 2, Northfield Township, Monmouth County, New Jersey and more particularly described as:

A brown, two story, multi-family residence which is set back approximately 75 feet from the roadway. Access to the residence is made via a driveway entrance off of First Street. The numerals "322" are affixed to the front fence post of a cyclone fence that delineates the adjacent property, Holy Trinity Elementary School. A row of small trees and bushes provide privacy from traffic on First Street. 322 First Street is located on the West side of the street at the intersection of Trinity and First Street. A yellow fire hydrant is located in front of this residence. Apartment 2 is located on the second floor of the residence.

there has been and now is located certain property which has been used in connection with the violation of the penal laws of the State of New Jersey, or which constitute evidence of, or tends to show the violation of Endangering the Welfare of a Child (N.J.S.A 2C:24-4a) and Conspiracy (N.J.S.A. 2C:5-2) to commit that offense.

The said property consisting of any and all computers, including all related computer hardware, software, documentation, passwords and data security devices, magnetic media and peripheral computer equipment; telephones, phone books, phone bills, address books, correspondence, diaries, or any other material which would indicate additional victims or suspects involved in the unauthorized access to computer systems and the unlawful access to stored communications; bank statements, and other indicators of occupancy; keys, statements and billings which show the location and the identity of safe deposit boxes and/or storage facilities; any and all records, business and otherwise, pertaining to the above mentioned crimes, including but not limited to, correspondence, notes, papers, ledgers, telephone message slips, memoranda, telexes, facsimiles; Any bank records, canceled checks, receipts and documents.

And the Court being satisfied from the foregoing that grounds for granting the application exist,

NOW, THEREFORE, YOU ARE HEREBY AUTHORIZED to enter, by breaking if necessary, between the hours of _____ and _____ and search, with the necessary and proper assistance, the premises hereinabove named, including basements, attics, storage spaces, surrounding grounds and all containers therein or thereon which could contain any of the items sought, for the property specified and to take into possession all such specified property which may be found on the said premises, to the end that the same may be dealt with according to law.

YOU ARE COMMANDED in the event that you seize any of the above described articles to give a copy of this Warrant, together with a receipt for the property seized, to the person from whom it is taken or in whose possession it is found, or in the absence of such person to leave a copy of this Warrant together with such receipt in or upon the premises from which the said property is taken.

YOU ARE FURTHER AUTHORIZED to execute this Warrant within ten (10) days from the issuance hereof.

YOU ARE FURTHER COMMANDED to forthwith make return thereof to me, with your report of the execution of this Warrant and the written inventory of the property seized hereunder by you.

GIVEN AND ISSUED under my hand at ____ a.m./p.m. this ___ Day of February, 19__.

_____

_____
Judge of the Superior Court

Legal Issues: Winning in Court

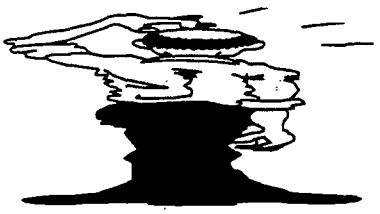
PROTECTING CHILDREN ONLINE REGIONAL TRAINING

DANIEL ARMAGH
DIRECTOR OF LEGAL EDUCATION
National Center for Missing and Exploited Children

NATIONAL CENTER FOR PROSECUTION OF INTERNET CRIMES AGAINST CHILDREN

(703) 837- 6337
TECHNICAL ASSISTANCE
RESEARCH
PUBLICATIONS
TRAINING
darmagh@ncmec.org

WHY HAVE A POLICY FOR DEALING WITH COMPUTER ASSISTED EXPLOITATION?



THE PRESS

CHIEF, COULD YOU EXPLAIN TO THE PEOPLE OF THIS JURISDICTION WHY YOUR DEPARTMENT VIOLATED THE CIVIL RIGHTS OF OUR CITIZENS?

THE POLITICIAN

"I VOTED AGAINST HIM BEING NAMED DIRECTOR - IT IS A SAD DAY FOR OUR COMMUNITY AND I AM PERSONALLY GOING TO ASSURE QUALITY CONTROL ON OUR FORCE"

DISCIPLINARY BOARD

WHY DID YOU APPROVE THIS OPERATION?

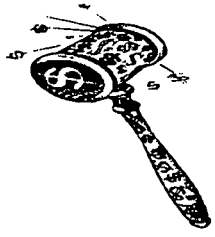
HOW COULD YOU NOT PROPERLY TRAIN YOUR OFFICERS?

CAREER PATH TITANIC

PLAINTIFF'S LAWYER

ARE YOU AWARE THAT YOUR OFFICERS ARE WOEFULLY UNTRAINED?

DO YOU NOW REALIZE HOW YOUR DECISION COST MY CLIENT THOUSANDS OF DOLLARS?



PROTECTION OF OUR CHILDREN

ANSWERING THE TOUGH QUESTIONS FROM PARENTS OF DEAD OR MISSING CHILDREN

POLICY FUNDAMENTALS

ANY PROTOCOL MUST BE BUILT UNDERSTANDING THAT:

- ***these are sexual abuse cases, not computer crime cases***
- ***computers are not the victims in these cases, they are the tools***
- ***do not abandon your investigative training when you see a computer***

WHY LEGAL ISSUES DRIVE POLICY CONSIDERATIONS

- Failure To Incorporate The Law In Your Management Decisions Is Asking For Disaster
- You Will Not Make Cases That Will Hold Up In Court
- You Will Alienate The Prosecutor
- Your Civil Exposure Is Increased

PRIVACY ISSUES

- Federal Constitutional Protections
- State Constitutional Protections
- Statutory Protections
- Privileges / Confidential Communications - Court Decisions

FEDERAL PRIVACY STATUTES

- **Privacy Protection Act**
- **Stored Wire and Electronic Communication and Transaction Records Access Act (ECPA)**
- **Video Privacy Protection Act**
- **Protection of Children From Sexual Predators Act (enacted October 30, 1998)**
- **Children's Online Privacy Protection Act to be codified as 47 U.S.C. 231et. seq..**

Monica and Wolfman

PRIVACY PROTECTION ACT

42 U.S.C. 2000aa

Provides protection against searches beyond what the fourth amendment affords for activities related to publishing. This law applies not only to traditional publishers, but also to anyone who may reasonably claim to be a publisher, including publishers of pornographic material.

PPA

YOU MUST BE EXTREMELY CAREFUL BEFORE USING A SEARCH WARRANT TO OBTAIN EVIDENCE FROM PERSONS WHO ARE ABLE TO CLAIM THAT THEY PUBLISH INFORMATION TO THE PUBLIC (e.g., bulletin board sysops).

PPA

- **ZURCHER v. STANFORD DAILY PRESS,** 436 U.S. 547 (1978).
- PPA applies only to law enforcement
- PPA provides for damages even where officers acted in good faith (no less than $1000, plus attorneys fees and costs

PPA

- Regulates searches or seizures of work product materials or documentary materials which are intended to be published to the public.
- Law enforcement may not search or seize wpm or dm (almost everything) from any person who intends to publish information to the public.

PPA

- Under PPA almost anyone is allowed to claim they are a publisher
- Law enforcement must serve the target with a court order or subpoena which the target may seek to have quashed by a court
- Practical effect is to prohibit law enforcement from obtaining records from anyone that claims publisher status

WORK PRODUCT MATERIALS

- MENTAL IMPRESSIONS, THEORIES, OR CONCLUSIONS
- WHICH A PERSON CREATED WITH THE INTENT TO PUBLISH
- TO THE PUBLIC
- e.g., reporter's field notes, summary notes or interviews for a story.

DOCUMENTARY MATERIALS

DOCUMENTARY MATERIALS INCLUDE ANY RECORDED INFORMATION WHETHER BY VIDEO, PHOTOGRAPH OR OTHER SIMILAR DEVICE.

THE LANGUAGE OF THE PPA IS SUFFICIENTLY BROAD THAT VIRTUALLY ANY EVIDENCE WOULD BE INCLUDED IF PUBLISHER STATUS IS PROVEN

ESMAY v. UNITED STATES, 1993 U.S. Dist. Lexis 20362

" Thus, for a valid claim to be stated under the PPA;

(1) there must have been a search and seizure; and

(2) there must be a showing of intent to publicly disseminate the information

EXCEPTIONS TO PPA

Congress excluded from definitions of wpm or dm "any contraband or the fruits of any crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as the means of committing a crime."

EXCEPTIONS WITHIN THE PPA

- YOU MAY USE A **SEARCH WARRANT** WHERE;
- Materials relate to a criminal offense(other than mere possession themselves);
- Immediate seizure of materials is necessary to save lives;

EXCEPTIONS WITHIN THE PPA

- **IN THE CASE OF DOCUMENTARY MATERIALS ONLY**, service of a subpoena would result in destruction, alteration, or concealment of evidence, **or;**
- A court order was not complied with, and either appellate remedies are exhausted or delay would threaten the ends of justice.

ANALYSIS UNDER PPA

- Reasonable that target intends to publish?
- If **after** you seize materials you discover intent to publish?
- If you determine ppa applies, cease reading materials until target has chance to challenge seizure in court

ANALYSIS UNDER PPA

- Mixed materials: consider seizure but not examining until target contests in court
- If target runs a bulletin board service the answer is almost always he is a publisher under ppa

ANALYSIS UNDER PPA

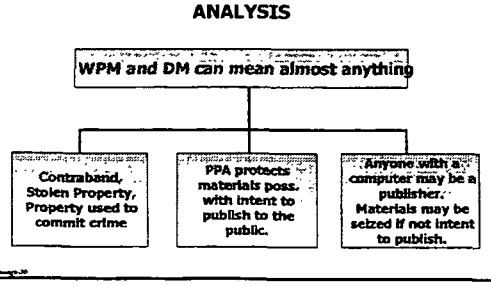
- THE MATERIALS ARE ALMOST ALWAYS EITHER WPM OR DM IF YOU HAVE REASON TO BELIEVE THAT TARGET IS KEEPING MATERIALS THAT RELATE TO HIS PUBLISHING ACTIVITY ON THE COMPUTER YOU INTEND TO SEIZE OR SEARCH

EXCEPTIONS

3. Reasonable that immediate seizure of materials prevents sbi or death

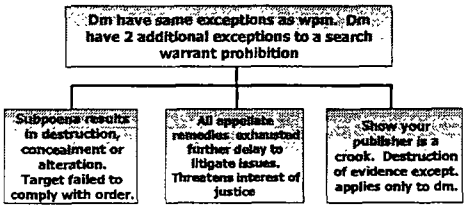
   If you are seizing **dm** which do not fall into the above cited exceptions, you may use a search warrant if your affidavit establishes that serving a subpoena would result in *destruction, alteration, or concealment* of dm.

PARADIGM SUMMARY- wpm



PARADIGM SUMMARY- dm

ANALYSIS



ANALYSIS SUMMARY

- PPA prohibits search or seizure of protected materials; this means that law enforcement can not use a search warrant to obtain the materials. Law enforcement must use a subpoena for such materials on the person who possesses the materials, allowing for the target to challenge the subpoena before complying with it.

REASONABLE BELIEF STANDARD

For the ppa to apply to either wpm or dm, the person possessing such materials must be a person **REASONABLY BELIEVED** to have a purpose to disseminate such information to the public

SPECIAL PROBLEMS - PPA

- Poorly drafted language
- Commingled materials - some of the material is protected and some is not: how do you proceed?
- What if you are unaware there is also protected material on computer until seized?
- Conflicts with the Omnibus Act

SPECIAL PROBLEMS - PPA

- Copy the disk or the criminal portion of the disk?
- Insuring accurate copies
- Is law enforcement required to examine every file on system before removal?
- Letter to the editor in every file of the target's computer

ANSWERS

- Courts are deciding these issues every month, with varying degrees of consistency
- So far, it appears if you don't know there is protected material at seizure, you may not be in violation unless, once you realize the material is protected, and it is requested, you are in violation if you fail to return materials

ANSWERS

- Use a subpoena when possible
- Get court approval on subpoena obtained records based on probable cause (may equal a warrant standard for purposes of the Omnibus Act)
- **Your job is to draft your affidavit to fit one of those exceptions to the search warrant prohibitions**

PPA CASE HOLDINGS THROUGH APRIL, 1998

- **CITICASTERS v. McCaskill,** 89 F.3d 1350 (1996) PPA does not require application for search warrant to describe exceptions to the PPA.
- **UNITED STATES v. MITTLEMAN**, 999 F.2d 440 (1993) PPA does not apply to criminal suspects and no greater showing of prob. cause for search warrant involving confidential relationships.

CASES - PPA

- **LAMBERT v. POLK COUNTY**, 723 F. Supp. 690 (1989) what constitutes "reasonably believed" to have a purpose to disseminate to the public a broadcast...
- **MINNEAPOLIS STAR & TRIBUNE CO. v. UNITED STATES,** 713 F.Supp.1308 (1989) attorney fees and costs under PPA

CASES - PPA

- **POWELL v. DEPUGH**, 911 F.Supp. 1184 (1995) statute of limitations for action under PPA is same as state's for tort or personal injury, not property or contract.
- **BENSON v. U.S.**, 1995 Lexis 31837, PPA did not apply because plaintiffs were suspects in criminal investigation and information seized not w/in PPA.

CASES - PPA

- **DEPUGH v. SUTTON**, 917 F. Supp. 690 (1996) plaintiff was within class of exceptions of criminal possessing materials relating to his criminal offense, namely poss. of child porn.
- **DAVIS v.GRACEY et.al.**, 111 F.3d 1472, (1997) sued police officers and department for violations of PPA - lacked subject matter juris. Case has very pro-police analysis under ECPA.

CASES - PPA

- **STATE OF OKLAHOMA ex. rel.Robert Macy et.al. v. PIONEER CD-ROM**..., 891 P.2d 600 (1994) civil forfeiture of items seized under PPA- seizure upheld because the criminal verdict upheld- court gave no opinion on whether defendant had a viable civil suit under PPA.

CASES - PPA

- **STEVEN JACKSON GAMES v. U.S.**, 816 F. Supp. 432, affirmed 36 F.3d 457 (5th Cir. 1994) - court decided that immediate seizure did not violate PPA under reasonable belief standard, however once agent discovered materials were protected and failed to immediately return to plaintiff, PPA violated.

CASES - PPA

COMMINGLING PROTECTED AND NON-PROTECTED MATERIALS: in construing the fourth amendment protections, the court has held "that sometimes there is no viable alternative to seizing non-evidentiary items and sorting them out later." **Nat'l City Trading Corp. v. U.S.**, 635 F.2d 1020

CASES - PPA

- " If commingling prevents on site inspection, and no practical alternative exists, the entire property may be seizable, at least temporarily." **United States v. Tropp**, 725 F.Supp. 482 (1989). Obviously, these cases interpret the fourth amendment and not the PPA, but could be helpful as precedent on commingling issues.

Electronic Communications Privacy Act (ECPA)

- **Katz v. United States, 389 U.S. 347 (1967)** supreme court ruled that the fourth amendment does apply to wiretapping because people talking on the phone have an "expectation of privacy...Any attempt to capture that conversation is a search." Since Katz, a multitude of communication devices not in existence at the time fall under this rule.

ECPA - HISTORY

- In response to Katz Congress passed Title lll of the Omnibus Crime Control and Safe Streets Act of 1968 which regulated interception of oral and wire communications. Congress eventually decided to regulate newer forms of communication- amending Title lll in 1986 by enacting ECPA. Congress has amended some of ECPA last year.

ECPA - A Collection of Statutes

- Title 18 U.S.C. 2510 - 2521 deal with regulation of interception of electronic communications
- Sections 2701 - 2711 regulate government access to stored electronic communications
- Sections 3121 - 3127 regulate trap and trace devices and pen registers.

ECPA - PPA

- The PPA protects a select group of communicators - media / publishers
- The ECPA protects communications based on their form - electric, wire, magnetic media...
- The ECPA applies not only to law enforcement as does the PPA; ECPA also applies to private parties

Cautions and Caveats

- These statutes do not replace the fourth amendment requirements, they supplement them
- State laws may have granted even greater protections than ECPA / PPA
- Laws are complex and many issues have not been resolved by the courts: Always consult a qualified attorney when faced with these statutes

ECPA - INTERCEPTION

- Protects electronic communication from interception while being transmitted.
- IN TRANSMISSION communication is speech, electrical impulses,radio waves...that constitute communication while moving from one party to another.
- Communication is not in transmission once it is 1. received 2. Stored

Communications in Transmission

- Fax transmissions in progress
- Digital pager communications not received
- Any data or commands traveling from one computer to another

Law enforcement rarely need to intercept communications in transmission

ECPA - Interception

- Exceptions: a party to a communication may "keystroke" monitor a communication in transmission and intercept same. 2511(2) (d)
- U.S. v. Seidlitz, 589 F.2d 152 (1978) owner of computer is party to comms.
- U.S. v. Merriweather, 917 F.2d 955 (1990) owner of pager or computer, or possessor of pager or computer is a party to communication.

ECPA - Interception

- Equipment furnished by the telephone company to any subscriber or user of such service may be used in the ordinary course of business to intercept communications. 2510 (4) (5)
- Providers of wire or electronic communication services may intercept where necessary to provide communication services or protect provider's rights or property. 2511 (2) (a)

ECPA - Interception

- Provider of electronic communication services may provide to law enforcement any communication inadvertently obtained by provider which appears to be criminal activity. 2511 (3) (b) (iv)
- It is not an interception to examine a communications source or destination, as opposed to contents. 2510 (4)

ECPA- Interception - Law Enforcement

- ECPA mandates use of search warrant for law enforcement for interception
- ECPA distinguishes between federal and state court orders for interception
- State investigators are at a decidedly disadvantage in applying for intercept orders

State Law Enforcement - Intercept

- If communications covered by the ECPA, help from feds is encouraged
- 3 conditions for state investigators;
  1. authorized applicant under statute
  2. application meets state standards
  3. application demonstrates communication reveal enumerated crimes under state statute, >1yr.

Application for Court Order

- Prob. cause specific offense will happen
- Identity of suspect
- Identity of sender of communication
- Location of target equip. & facilities used
- Period of time intercept. is maintained
- Earlier applications? Course of invest.?
- Less intrusive means inadequate?

Application for Court Order- Intercept -2518 (1)

- Must meet a higher standard than ordinary search warrant
- Probable cause plus showing all less intrusive avenues have been used or considered and were not feasible - state reasons not possible.
- Be aware of stricter state requirements than that of ECPA

Congressional Notes - Judiciary Committee on Intercept Laws

- In monitoring wire transmissions, investigators must stop listening to innocent conversations. This concept is also desired in monitoring electronic communications as the committee "suggested" that all non-relevant material be deleted by initial law enforcement before being disseminated to others who would continue the investigation. Senate Rept. No. 99-541

ECPA - Intercept- Suppression

- Intercepting an **electronic communication** in violation of the ECPA can result in stiff penalties and possible criminal sanctions. It does not result in the suppression of the communication in a subsequent trial if no constitutional or state statutes were violated. (You loose your job, but the evidence is admissible!!)

ECPA - Suppression- Intercept

- Section 2515 omits electronic communication and only "wire or oral communication" remains as suppressible for violation of the ECPA.
- Section 2518 (10) © provides the exclusive remedies for violation of ECPA for non-constitutional grounds regarding electronic communications.

Governmental Access to Stored Electronic Communications

- ECPA sections 2701 - 2711
- Electronic service providers send and receive electronic messages and store them in "mailboxes". A message is not stored until it is received by the service provider / recipient.
- Generally there is a backup copy made for each message sent in case of system failure. Copy is with provider.

Storage in Different Locations

- ECPA protects only those communications in electronic storage in the possession of the provider. ECPA does not protect communications downloaded by the addressee to another computer not maintained by a provider.
- Provider = protected : Home computer downloaded message = not protected

ECPA Protects Electronic Communications Maintained by:

- Electronic communication services (e-mail)
- Remote computing services (data banks stored off - site)
- ECPA prohibits providers from disclosing the contents of communications to anyone, with certain exceptions

Law Enforcement Exceptions

- Law enforcement can compel disclosure from both types of providers by warrant or subpoena. The type of legal process required depends on the age of the communication and the pre-disposition of the government to inform the customer of the service about their request for contents.

Law Enforcement Exceptions

- ECPA also prohibits disclosure of information about their customers without legal process - identity of sender, location of origin of communication, identity of recipient.
- A communication obtained in violation of the Act does not result in suppression of the evidence (absent other constitutional violations)

Electronic Communication Service

- Usually an MCI mail service or Compuserve mail service
- ECPA defines the electronic communication service as " any service which provides to users thereof the ability to send or receive wire or electronic communications." 2510 (15)

Remote Computing Service

- Includes anyone who provides " to the public...computer storage or processing services by means of an electronic communication system."
- This means that a bulletin board may serve as a remote computing service covered under ECPA.

18 U.S.C. 2702 (1997) Disclosure of Contents

- Prohibits disclosure to anyone except:
- Addressee, recipient of communication or agent thereof
- As authorized under 2703
- Consent of originator, addressee or recipient (public bulletin boards can be accessed by law enforcement)
- Provider inadvertently obtains comm. which appears to be criminal - can disclose to law enforcement

2703 - Requirements for Governmental Access

- < 180 days requires a warrant
- 181 days or more gov. may use a warrant (no notice), administrative subpoena (notice), court order (delayed notice)
- (c) **records** - subscriber or customer (not contents of comm.) by warrant, court order or consent

2703 (c)

- **Records** - include name, address, long distance telephone toll billing records,telephone numbers or other information about length and type of services utilized
- Notice to customer not required under this section for administrative subpoena (2)

2703 (d) Requirements for Court Order

- Any court of competent jurisdiction 3127 (2) (a)
- Must offer specific and articuable facts that contents are relevant and material to an ongoing criminal investigation
- No state court may issue if prohibited under state law
- Service provider may move to quash if request voluminous or undue burden

2703 (e) Immunity for Provider

- No cause of action against provider disclosing information under this chapter, nor employees, officers, agents or other specified persons if acting in accordance with the terms of court order, warrant, subpoena...

2703 (f) Requirement to Preserve Evidence

- Provider, upon request of gov. entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of court order or other process
- Period of retention is for 90 days with option, on request of gov. for 90 day extension

2704 Backup Preservation

- May include in subpoena or order requirement to create backup of contents of communication
- Without notice to customer
- Asap w/in regular business (no later than 2 days after receipt of order)
- Confirm to gov. backup created

2704 (a) (2)-(5)

- Notice to customer by gov. in 3 days unless delayed under 2705
- Provider shall not destroy backup until later of delivery or resolution of legal challenges
- Provider releases no sooner than 14 days after no notice that customer has not challenged or challenge by customer not filed

2704 (a)(5)

- Gov. entity may seek to create a backup copy in its sole discretion without notice to customer if there is reason to believe that notification may result in the destruction or tampering with evidence. This determination is not subject to challenge by provider or customer under 2703 (a).(search warrant)

2704 (b) Customer Challenges

- File within 14 days quash,vacate with written notice to gov. and provider.
- Affidavit by customer shall state: they are a customer, contents have been requested, they are not relevant to investigation or no substantial compliance with the law.
- Service
- Sworn response (in camera) by gov.

2705 Delayed Notification

- Up to 90 days if court determines adverse result may be possible
- Adverse results
- Extension for 90 days
- Notice to customer after delay informing the date, agency, provision, and official in charge of action
- May extend time of notification indefinitely if certain circumstances exist

2706 Cost Reimbursement

- Fee for costs reasonably necessary and directly incurred, including disruptions in normal operations
- Amount is mutually agreed upon or the court will decide
- Records of common carrier are excluded, but court may consider case if unusually voluminous

2707 Civil Action

- Except as provided in 2703 (e) a cause of action may be commenced against any entity that has violated ECPA
- Damages - minimum $1000, plus costs, punitive damages and attorney fees.
- Disciplinary actions
- Good faith defense is complete
- Statute of limitations - 2 years from first discovery or reasonable opportunity

2708 Remedies

- Remedies described in this chapter are the exclusive remedies and sanctions for nonconstitutional violations of this chapter
- Muskovich v. Crowell (1995, Iowa) 12 BNA IER Cas 647

2710 Wrongful Disclosure of Video Tape Rental or Sale Records

- Not to disclose to law enforcement unless search warrant, state warrant, or court order used (supeona with court blessing)
- Court orders authorizing disclosure issue only with prior notice to customer and only if probable cause is shown that records are relevant to legitimate investigation.
- Civil action-see liability

Liability - PPA

- Steven Jackson Games v. U.S., 816 F.Supp. 432 (1993) Secret Service ordered to pay $50,000 in damages, $195,000 in attorney fees, and $57,000 in costs for violation of PPA
- Minneapolis Star & Tribune Co. v. U.S., 713 F. Supp. 1308 (1989) violation of PPA, damages of $750 per plaintiff, $48,246.93 to one law firm, $31,996.44 to a second firm, costs in excess of $15,000

Liability - ECPA

- Violations of ECPA may result in damages not less than $1000. If damages are intentional or willful, punitive damages are authorized and costs, plus a reasonable attorney fee.
- Disciplinary action - if willful or intentional the court will order agency or department to investigate and a hearing to determine whether action is warranted against employee.

Liability - ECPA

- Good faith defense exists for law enforcement
- 2 year statute of limitation
- Incidental seizure of e-mail on bulletin board by police officers did not violate ECPA because of good faith reliance on search warrant. Davis v. Gracey, 111 F.3d 1472 (1997)

Liability - ECPA

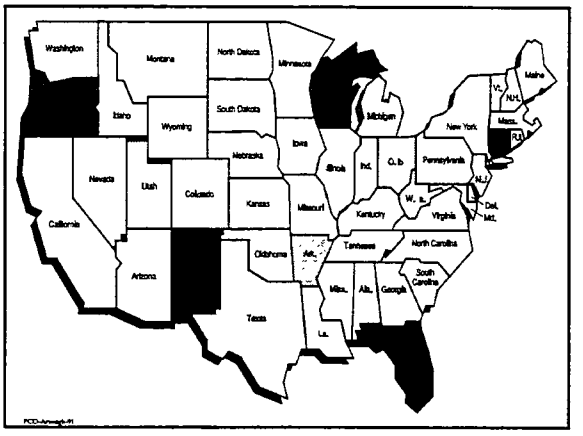
- Breaking or destroying equipment through negligence is actionable by victims
- Loss of business opportunity is actionable by victims, even if criminal activity is part of a wide sweep by law enforcement
- Failure to return equipment and comply with ECPA forms basis for liability

Liability - Searching and Seizing Computers

- Police officers must execute search warrants to avoid unnecessary destruction of property. Departments risk liability for failing to properly train officers proper procedures for searching and seizing computer evidence. **Ginter v. Stallcup,** 869 F. 2d 384 (1989)
- **Tarpley v. Green**, 684 F.2d 1 (1982)

Liability - Searching & Seizing

- Even perfectly reasonable search which destroys property may be a compensable taking... McGovern v. City of Minneapolis, 480 N.W.2d 121; Steele v. City of Houston,603 S.W. 2d 786 (1986); but see Customer Co. v. City of Sacramento, 10 Cal 4th 369 (1995) holding that only innocent third parties would be eligible for compensation

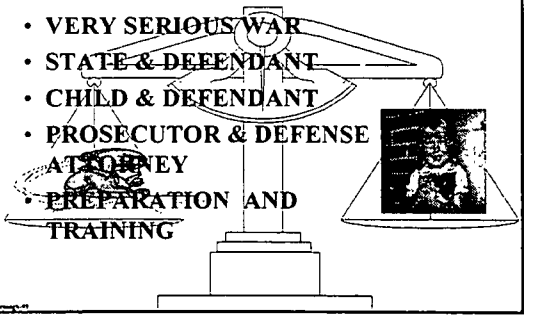


HOT TOPICS

- Interviewing
- Video-taping
- Munchhausen syndrome by proxy (factitious disorder)
- Plethysmograph
- Recantation
- Media backlash
- Computer assisted exploitation

BALANCING THE SCALES FOR CHILDREN

- VERY SERIOUS WAR
- STATE & DEFENDANT
- CHILD & DEFENDANT
- PROSECUTOR & DEFENSE ATTORNEY
- PREPARATION AND TRAINING



IMPRESSION MANAGEMENT

- **Sound bite society**
- **Attention span of jurors**
- **Educational level of jurors**
- **3 sources of expertise**
- **Jurors' " not enough evidence"**
- **Unprofessional mistakes**

PSYCHOLOGY OF THE INVESTIGATOR

- **Best of the best**
- **Think like a defense lawyer**
- **Think like a predator**
- **Take the testimonial view of everything you do**
- **Know your case**
- **Be organized and concise**

VERTICAL PROSECUTION

- Number of interviews
- Target for reasonable doubt
- Coordinated approach
- Prevents meeting new professional every time
- Multi-disciplinary teams

IMMUNITY

- **TRAINING - CITY OF CANTON v. HARRIS 109 S. Ct. 1179 (1989)**
- **INVESTIGATION - BUCKLEY v. FITZSIMMONS 113 S. Ct. 2606 (1993)**

INVESTIGATION

- **Interview or interrogation is critical to case**
- **Safe environment / be his pal**
- **Lock him in to the first five stories**
- **Miranda**
- **Consent and warrant**

CORROBORATION

- Sting
- Non - confession
- Confession
- Corpus delecti
- Call his mom
- Interview others
- Anticipate the defense

SUBSTANCE OF TESTIMONY

- Competency
- Remember
- Relate
- Communicate
- Truth and lie
- Punishment
- Kentucky v. Stincer 482 u.S. 730

DEFENSE EXPERTS

- **Ralph Underwager**
- **Richard Gardner**
- **What is their previous testimony?**
- **What is their expert background ?**
- **Educational relevance?**

OFFENSIVE DISCOVERY

- Blood typing
- DNA
- HLA
- HIV Testing
- STD
- Photo Corroboration
- Forensic Computer Analysis

ENTRAPMENT

- JACOBSON v. UNITED STATES
- 112 S. Ct. 1535
- Child Pornography
- Reverse Sting
- Several Agencies over many years
- Political Speech issue-1st amend

ENTRAPMENT

The government cannot "originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act and then induce the commission of the crime so that the government may then prosecute."

ENTRAPMENT

- <u>UNITED STATES v. GENDRON,</u> 18 F3d 955 (1994) - distinguished from Jacobson on predisposition issue. Grendon's correspondence sole desire was to view child pornography, not "launch a counter-attack against those who would curtail our freedoms."

ENTRAPMENT

- CHIN v. UNITED STATES, 833 F. SUPP. 154 (1993) - court distinguishes from Jacobson in that there is additional evidence of predisposition and that Chin demonstrated a predisposition to trade, loan, and order such material.

UNITED STATES v. GAMACHE

- 1998 wl 432080 (1st cir. N.H.)
- Can apply to chatroom and undercover sting protocols
- Non-computer case (mail)
- Travel interstate to engage in an illegal "sexual act" with minors 2423(b)
- Engage in sex to produce visual depiction 2251(a)

GAMACHE

- Case reversed-jury should be instructed on the defense of entrapment and failure to substantially affected his rights to a fair trial
- Def. can claim both innocence and entrapment concurrently
- Opportunity / plus

GAMACHE

- Def. must show inducement and lack of predisposition, then gov. must prove def. predisposition to engage in criminal conduct beyond a reasonable doubt.
- Improper inducement, time and motive of def., predisposition

Factors Considered in Assessment of Predisposition

- Character or reputation of defendant
- Initial suggestion of criminal activity by Gov. or defendant?
- Def. engaged in activity for profit?
- Def. reluctant to engage in conduct but persuaded by Gov. agent?
- Nature of inducement or persuasion by Gov.
- Focus must be def. before contact with Gov. began

GAMACHE

Court held that the evidence raises a reasonable doubt that the government *improperly induced* a citizen to commit a crime that he was *not predisposed* to commit, thereby requiring a new trial.

Other Defense Tactics and Themes

"Don't you people have anything better to do than violate the first amendment rights of decent Americans."

Fantasy Talk

- Never any intent to act on the communications
- Didn't really think my e-mail partner was a minor
- I thought this was still America
- I was just going along with the tone set by the other party and laughing about it

Countering Fantasy Defense

- Document actions Def. took in support of his conversation
- Corroborate by overt acts
- Always communicate the "age of the child" in the sting operation, several times if possible.

Evidence of Intent

- Pornography, erotica, cameras, equipment
- Intelligence that corroborates conversation
- Address books and journals
- E-mail printouts / photos / diaries
- Enticement objects
- Hotel room reservations, contents in the def. vehicles upon arrival relating to sexual content of discussions

Evidence of Intent

- Messages describe sexual fantasies of target
- Target sends porn to child
- Sends graphic sexual cartoons to child
- Sends morphed sexual pictures to child
- Asks child to send naked pictures
- Sets up face to face meeting
- Travels from another state to act on messages about sexual fantasies

No Real Victim in Being

- Luring sting wherein no child in fact was involved
- Factual impossibility is not a defense
- Attempts
- Can't prove age of persons in pictures
- Morphed images - Child Pornography Act of 1996 (Maine & California)
- Age of consent under state law is 16
- Case compilation available at NCPCA

Research for an Article...

No intent for sexual gratification, merely academic, investigative reporter, just curiosity, preparing the case for law enforcement.

Possession is a crime unless you are statutorily exempt. The federal law has not granted any exemptions for child pornography.

CHILD PORNOGRAPHY

- Unsolicited
- Did not know age of actor
- Was not my computer
- Was not the primary or secondary producer
- Records were stolen or burned
- Home movies - artistic

COMPUTER PORNOGRAPHY

- Determine ownership
- Determine who used computer
- Fingerprints
- Passwords, canceled checks
- Writing exemplars
- Access to common area

SODDI

- My wife
- My roommate
- Someone else loaded it on my computer via the internet
- Police uploaded porn and put it in my computer
- Did not know child porn on my computer

UNITED STATES v. KNOX

- 32 f. 3d 733 (1994)
- Knox knew the contents
- Knew traveled interstate
- No nudity was involved
- Lascivious conduct was not focal point - was there an exhibition, not character of exhibition (dost)

Other Concerns

- Value added techniques altering electronic evidence
- Mirror images was not done properly thereby altering the best evidence
- Custodian of record-input person not present and therefor suppression is urged
- Police uploaded porn-what belongs to who
- Poor forensic examination

Policies and Protocols

- On-line protocols which are written guidelines are important
- Document your chat logs
- Log all undercover activity
- Session logs, message logs
- Accurate documentation of all undercover activities protects against entrapment defenses and provides a stellar record of the best evidence for the prosecutor

Policies on Sting Conversation Protocols

- Documentation
- Avoid suggestive screen name
- Use open ended questions
- Avoid being to graphic or vulgar
- You want the target to come off like the pervert, not the undercover officer
- Encourage them to be graphic, just don't join them

Other Policy Considerations

- Probably a very bad idea to upload Porn
- Do not run an investigation from your home
- Early and close contact with prosecutor and investigator is essential
- Use experts - if civilian always have law enforcement present

Warrantless Searches

- Beware of these
- Withdraw consent
- Never gave consent
- Consent under duress
- Consent plus search warrant-document target's response

Repairman Case

- Get the call from the repair shop
- Do not instruct repairman to go back and look for more evidence or ever save or download what he saw
- Establish probable cause from description of what he saw before he called law enforcement

SEARCH WARRANT

Demonstrate specific and articuable *facts* showing reasonable grounds to believe that contents of electronic communications or the records or other information sought are *relevant* and *material* to an ongoing *criminal* investigation.

SEARCH WARRANTS

- Strong preference for search warrants and courts will scrutinize a warrantless search
- Most computer searches will be pursuant to a warrant

SEARCHING COMPUTERS

- Exceptions apply
- Plain view: lawful position to observe the evidence and its incriminating character is immediately apparent.

SEARCHING COMPUTERS

- Determine the computer's role in the offense
- Tool used in sending out pornography
- Repository for storing computer pornography

EXIGENT CIRCUMSTANCES

- Degree of urgency
- Time for warrant
- Evidence destroyed
- Danger
- Target knows your coming
- Destructibility of evidence
- Multi - network involved

BORDER SEARCHES

- Sovereign's power to exclude
- No warrant required
- No probable cause required
- Once evidence is in country and citizen downloads from bbs - do you need a search warrant to obtain child porn?

CONSENT SEARCHES

- Spouses: def. must show spouse actually denied access
- Parents: minor children
- Parents: adult children
- Employees: public / private
- Expectation of privacy

CONSENT SEARCHES

- Objectively reasonable expectation of privacy
- Network system administrators
- Informants and undercover agents must go no further than permitted by def.

CONSENT SEARCHES

- Scope exceeds consent
- Proper party consents but data is encrypted
- Limitations on consent either implied or expressed must be honored
- Third party consent to common area

SEIZING HARDWARE

- Contraband
- Instrumentality
- Evidence: physical components- central process. unit, keyboard, monitor, modem and printer
- Peripherals
- Documents / data only

INDEPENDENT COMPONENT DOCTRINE

- Each component is analyzed independently
- Seize only components that are evidence of a crime
- Officers must articulate a reason for seizing the item
- Not just anything connected

TRANSPORTING HARDWARE

- Handling information storage devices
- Careful packing
- Traditional evidence
- Integrity of evidence
- Videotape / photograph scheme
- Draw scheme

WHERE EVIDENCE MIGHT BE

- Identity investigation
- Fingerprints
- Handwritten notes
- Labels
- Password
- Telephone records
- Hard copy print out

SEIZING INFORMATION

- Information at the scene
- Information stored off - site
- Contraband - software, access codes, and manuals
- Instrumentality - digital software used in forming collages of children for child pornography

SEIZING INFORMATION

- Information as evidence
- Documents connecting evidence to crime
- Pattern of mailings
- Porn exchange
- History of operating chatroom or bbs - paper or electronic in form

PROBABLE CAUSE TO SEIZE

- Hardware
- Software
- Data
- Location of search: site, field office, or laboratory
- Ultimate goal
- Use a search warrant

DESCRIBING ITEMS TO BE SEIZED

- What are your objectives for search and seizure?
- Documentation, instrument or both
- Breadth of warrant depends on scope of criminality
- Focus on contents of relevant documents, not devices

DRAFTING THE AFFIDAVIT AND WARRANT

- Indicate whether there is electronic mail on target computer
- Identify mail to be read
- Establish rule of law that allows search
- If hardware - focus on detailed description of component

WARRANT FOR INFORMATION SEIZURE

- Data exists in essence, not in form or fact
- Physical location of data unknown
- Location of storage: on / off site
- Unknown location

WARRANT - INFORMATION

- Tell magistrate issuing warrant no way to identify site
- Indicate why there is no way to identify site and describe all attempts to locate
- Discuss the nature of storage in multi - network

FOURTH AMENDMENT

- Requires specificity
- Particularity
- Breadth/scope
- Assume that detailed and clearly described records are in electronic form and so provide in your warrant
- Generic "electronic" records are overbroad

NO - KNOCK WARRANT

- Injury to police officer
- Individual
- Suspect to flee
- Destruction of evidence
- Computer cases
- Preservation of evidence
- Hot keys, time delay, these premises or these people

SEARCHING TECHNIQUES

- Utilities software
- Key word searches
- Modem and software expands search and new warrants
- Rely on experts
- Discovering the unexpected not in the warrant - 4th amendment

DRAFTING THE WARRANT

- COMPUTER CRIME UNIT, DEPT. OF JUSTICE 202 - 514-1026
- ATF 301-217-5717
- FBI 202-324-9164
- SEC.SERV. 202-435-7700
- DEA 703-557-8250
- IRS 202-535-9130

NETWORKS AND BULLETIN BOARDS

- Electronic bulletin boards - messages are left
- Chatrooms are sub - boards
- Pirate bulletin boards = pornography
- Not protected by the first amendment - not a license to commit crimes against children

ENCRYPTION

- Encrypted computer = locked file cabinet
- Warrant to search and seize encrypted information
- Does that warrant authorize breaking the encryption?
- Looking over shoulder?
- Case specific

MISSING OR EXPLOITED CHILD?

NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

PROTECTION OF CHILDREN FROM SEXUAL PREDATORS ACT OF 1998

Establishes new criminal offenses
Amends existing statutes
Provides for enhanced penalties

New Criminal Offenses

Transfer of Obscene Materials to Minors

- < 16 years of age
- any facility or means of interstate or foreign commerce
- attempts
- 10 years/fine

New Criminal Offenses

Use of Interstate Facilities to Transmit Information About a Minor

- < 16
- entice, solicit, encourage any person
- to engage in any sexual activity
- that can be charged criminally, or attempts
- 5 years/fine

New Criminal Offenses

The term *sexual activity* for which any person can be charged now includes the production of child pornography - 18 U.S.C. 2427 as amended.

Amends Existing Statutes

- 18 U.S.C. 3486 A : **Authorizes use of admin. supoena to gain access to computer records from ISP for non-content information pursuant to Attorney General directives.**
- 18 U.S.C. 2252 a and 2252 A - **One matter or image of child pornography sufficient to prosecute (prior - 3 images)**

Amends Existing Statutes

- 18 U.S.C. 2251 (a) (b): **extends *jurisdictional reach to prosecute* production of child pornography to include any pornography made with materials that were made or transported via interstate or foreign commerce.**

Amends Existing Statutes

42 U.S.C. 227 : (amends Victims of Child Abuse Act of 1990)

Reporting of Child Pornography By Electronic Communication Service Providers - electronic or remote computing service to the public via interstate or foreign commerce shall report child pornography to law enforcement: failure to report $50k, 2nd failure = 100k

Amends Existing Statute

Investigation of Serial Killings: **Attorney General and Director of the FBI may investigate serial killings in violation of state laws of a State or political subdivision, if such investigation is requested by the head of a law enforcement agency with investigative or prosecutorial jurisdiction over the offense.**

Enhancement of Penalties

18 U.S.C. 2244 (c): **offenses involving children less than 12 years of age, maximum penalty imposed shall be twice that otherwise is provided in this section**

Prior Sex Offender: twice the term otherwise provided

Enhancement of Penalties

18 U.S.C. 3559 (d) : **Death or Imprisonment for Crimes against children -**

sexual exploitation against children gets you either life imprisonment or death penalty if:

- < 14
- victim dies as a result of offense and
- def. engages in conduct described in 3591(a) (2) "snuff films"

Affirmative Defenses

Affirmative defense if:

- < than three matters of visual depiction
- promptly & in good faith allow only law enforcement to access visual depiction
- took reasonable steps to destroy depictions or
- reported the matter to law enforcement and allowed access

The Children's Online Privacy Protection Act

ACLU v. Reno II

preliminary injunction issued on February 1, 1999

Child Online Protection Act

- ***Prohibited conduct: knowingly, for commercial purposes, makes a communication that is harmful to minors by means of the World Wide Web shall be fined 50k, 6 months or both.***
- ***Intentional violations: 50k for each violation and each day is a separate violation***

Children's Online Protection Act

- Civil penalty: 50k for each violation in addition to the criminal fines.
- must be in the business of making or offering to make a communication via the WWW with the objective of earning a profit
- Harmful materials to minors
- minor is under 17 under COPA
- Affirmative defenses: good faith restrict access, digital verification of age, other reasonable means

Children's Online Protection Act

- ***Standard of Scrutiny***
- ***Burden on Speech Imposed by COPA***
- ***Compelling Government Interest***
- ***Narrow Tailoring & Least Restrictive Means***
- ***Irreparable Harm***
- ***Balance of Interests***

Jurisdictional Issues

- Multiple sites in same district - (several targets in the same building)
- Multiple sites in same district - different buildings
- There is some precedent for allowing connected computers within the same district to be covered under one warrant, provided no violations of 4th amendment

JURISDICTIONAL ISSUES

- Searching a single personal computer is certainly different that searching a network of computers that reach around the world. Investigators must have intelligence that forms the basis of charging crimes and where those crimes occurred. Intelligence is crucial. Vendor/providers loyalty to the customer usually far outweighs any sense of obligation to police.

Jurisdictional Issues

- Multiple sites in different districts
- Did law enforcement know evidence was in a different district before executing a search warrant?
- United States v. Rodriguez, 968 F.2d 130 (1992)

Jurisdictional Issues

- Information at an Unknown Site
- Evidence at an off-site storage that law enforcement knew prior to execution of warrant, but does not know where the off-site storage is located
- Show a clear relationship between the target computer and connected computers
- Information/Devices which have been moved

Jurisdictional Issues

- Forum and jurisdiction is driven factually first and most importantly. In multiple jurisdictional crimes, prosecutors have options under most facts as to where to bring criminal charges.
- Resources
- Judges
- Prosecutor
- Double jeopardy

Jurisdictional Issues

- If you are going to search off-site computers located in the same jurisdiction, include that authorization in your application for search warrant.
- If you are going to search or access a computer off-site in another jurisdiction, it is unclear whether you need a judge in that other jurisdiction to authorize that search.

Partnering for investigating and prosecuting computer crimes

- Sexual exploitation of children by using computers involve many jurisdictions, agencies and laws.
- How do we involve the prosecutors, law enforcement agencies and other professionals in coordinating resources, talents and time to investigate and prosecute these cases.

Partnering

- Identify resources in your jurisdiction
- Identify federal and state resources which are available
- Developing a relationship with the prosecutors in your jurisdiction
- Developing and maintaining a multi-agency team and protocol

Partnering

- Civil forfeiture - what is in it for me
- Community prosecution
- Innocent Images and the FBI policy regarding co-investigations with local, state and other federal agencies: why you need a separate protocol for dealing with the FBI policy
- Developing your own investigation resources and abilities

THEME DEVELOPMENT

- Early in the case
- 80% of jurors make up their mind after opening statement
- A theme is the filter
- Out think the opponent before the testimony is given

TESTIFYING

IMPRESSION MANAGEMENT

FACT BEYOND CHANGE

- To get a witness to testify against a fact that is true beyond change is the ultimate in cross-examination
- Keep the theory of the state's case in mind as well as what the theory of the defendant will be

THREE THINGS

- Defendant can take the 5th
- He can tell the truth about everything
- He can lie
- How can we expose the lie and where is it coming from
- This is always a paradigm for policemen from defense attys.

TESTIFYING: TRAPDOORS AND PITFALLS

- Training at the academy: how many hours on:
  - 1. Police reports
  - 2. Child exploitation
- Personal opinion v. Professional opinion
- Answer the question officer, yes or no?

TESTIFYING

- You did not see Sarah raped by anyone did you?
- You have no personal knowledge that anything she told you is true, do you officer?
- How long have you been a police officer?

TESTIFYING

- How long have you investigated child abuse cases?
- Shouldn't you have taken her to the doctor immediately?
- Officer, you did not tape record or videotape the interview did you?

TESTIFYING

- Verbatim quotes and report impeachment
- Why didn't you put this information in your report?
- What other suspects did you investigate?
- There is no physical evidence in this case is there officer?

TESTIFYING

- You suggested the answers by the type of questions you asked didn't you? Well we don't know that do we?
- The truth is you got all your information from the cps, mother...

TESTIFYING

- Isn't it true that children lie about things?
- Isn't it true that children dream and fantasize about these things?
- You're aware of Sarah's reputation for lying, promiscuity, discipline problems...

TESTIFYING

- If you could do it all over...
- You would agree this was not a perfect investigation?
- What were you trying to hide by not including it in your report? In your testimony?

SCIENCE OF PERSUASION

- Societal values
- Dominant emotional theme
- Primacy and recency
- Emotional chronology
- 65% of all communication is body language
- B.F. Skinner

ART OF PERSUASION

- Trust and credibility
- Demeanor
- Relational communications
- How does your testimony fit in the overall impression management of the trial?

PRESENTING YOUR CASE

- Remember - impression management
- Average educational level of jurors
- There is no substitute for preparation
- Review questions with your prosecutor

PRESENTING YOUR CASE

- Review questions / traps from defense attorney
- Find out what part you play in creating the dominant emotional theme for the case
- Anticipate what emotional theme the defendant will take

PRESENTING YOUR CASE

- Appearance is professional
- Table manners are important
- Relational combinations
- Jurors are always watching
- Lunch with defense attorneys
- Be on time
- Professionally package exhibits

TESTIFYING

- Take the question from the attorney and give the answer to the jury
- Posture is communication
- Avoid copspeak
- Do not ramble, answer only the question asked

MODIFICATION OF THE COURTROOM

- Comfort level of the victim
- Clear the courtroom during her/his testimony
- U.S. V. Dixon 113 s. Ct. 2849
- Comfort friends
- Pro se defendants
- Defense attorneys

TESTIFYING

- Use words that convey the facts in emotionally compelling ways
- Speak loudly and clearly
- Do not look to the prosecutor or judge for the answer
- Do not argue or lose temper
- Do not lie

CROSS - EXAMINATION

- Defense attorneys are trying to score emotional points - at the initial question and the last question - primacy and recency
- If they start out easy they are trying to get you to agree with as much as possible

CROSS - EXAMINATION

- The whole point is for them to make you look stupid
- To get words from you that they can drive home in closing argument
- The most difficult witness to cross is the one who is telling the truth and is prepared

EVIDENCE

- Investigation judged in its entirety, not just the interview
- Commissions
- Case load
- Cases not arrested or founded

SEXUAL EXPLOITATION OF CHILDREN

- 18 u.S.C. 2251
- Intent to engage in sexually explicit conduct
- Visual depiction of conduct
- If defendant knows depiction will be transported interstate, foreign commerce or mailed-or has been so transported

SEXUAL EXPLOITATION OF CHILDREN

- Any parent, legal guardian or person having custody or control and knowingly permits or assists or has reason to know that a child is being exploited sexually and said depiction is transported or:

SEXUAL EXPLOITATION OF CHILDREN

- Advertises such depiction or
- Participates in such conduct with minor (adult "actor" in movie)
- 10 years/fine
- Death penalty if child dies

18 U.S.C. 2252

- Certain activities
- Transports or ships
- By computer or mail
- Visual depiction of minor engaging in sexually explicit conduct
- Sends, receives, sells, or possess

Transportation of Minors

- 18 u.S.C. 2423
- Transportation with intent to engage in criminal sexual activity
- Knowingly transport individual under 18 with intent to engage in prostitution or any criminal sexual activity, or conspires to do same

TRANSPORTATION OF MINORS

- 18 u.S.C. 2423
- Act of furnishing money for travel sufficient
- Knowledge of age by def. not an issue

18 U.S.C. 2422

- Coercing or enticing a minor to travel interstate / internationally for purpose of prostitution or unlawful sexual act
- Up to five years in prison/fine

18 U.S.C. 2422 (b)

- Using the mail or other forms of interstate commerce to coerce or entice a minor to engage in prostitution or unlawful act
- Up to ten years / fine

18 U.S.C. 2251 (a)

- Photographing/filming/videotaping minor's sexual acts (and coercing, enticing or transporting interstate/international for such purposes)
- Up to ten years/fine

CHILD PROTECTION, RESTORATION AND PENALTY ENHANCEMENT ACT

- American Library Association v. Reno
- Primary producers
- Secondary producers
- Show records to law enforcement without a warrant on request

COMMUNICATIONS DECENCY ACT OF 1996

- Two granted in Feb. of this year
- Injuction granted June 1996
- Define indecency
- Those who unknowingly send pornography should not be liable
- Unconstitutional-July, 1997 U.S. Supremes

UNITED STATES v. DOST

- Lascivious
- Focal point on genitalia
- Pose sexually suggestive
- Inappropriate attire
- Fully or partially nude
- Appear willing to engage in sex
- Elicit a sexual response in viewer

NEW YORK v. P.J. VIDEO

- Does material protected by the first ammd. require higher probable cause stand?
- No- fair probability that contraband evidence will be found

UNITED STATES v. LAYNE

- Search warrant suppression on grounds that prior restraint on ideas and lacked particularity
- Search was to corroborate child's statement, not for obscene material

UNITED STATES v. HARVEY

- Was search warrant stale because of a two year investigation?
- No- nature of crime, type of evidence, expert testimony of habits of pedeophiles in collecting child porn. All important factors

UNITED STATES v. WEBER

- Are boilerplate expert affidavits sufficient?
- No, experts opinion must be sufficiently grounded in the facts concerning this specific defendant and his behavior that concludes he is a pedeophile. Reversed.

UNITED STATES v. SIMPSON

- Federal Express searched package to find address
- Called F.B.I.
- F.B.I. posed as Federal Express
- Suppression denied. Original search did not aid F.B.I. and Federal Express did not intend to aid F.B.I.

UNITED STATES v. CAMPBELL

- Violation of Mann Act
- Prostitution must be a dominant purpose for transportation but need not be the sole dominant purpose for interstate transportation
- Campbell was "dating" Wilkins in many different states

UNITED STATES v. CLAYMORE

- Abuse of position of trust
- Police officer sexually abused a minor
- Court added 2 pts to sentencing guidelines
- Def. argued community hated police
- Position not attitude of comm.

UNITED STATES v. X-CITEMENT VIDEO

- 115 S. Ct. 464 (1994)
- Knowledge of a child's age
- Affirmative defense
- Lord's case on under age pornography

UNITED STATES v. LANGLEY

- 62 F.3d 602 (1995) holds that X-CITEMENT VIDEO does not apply to this case because it involves a felon-in-possession statute where the reasoning in X-CITEMENT was to avoid placing ordinary citizens at risk of criminal prosecution for "otherwise innocent conduct"

BENNIS v. MICHIGAN

- U.S. Supreme Court upholds the forfeiture of automobile owned by the wife even though the husband was engaging in criminal conduct with a prostitute
- Due process clause - 14th
- Takings clause - 5th not offended

INNOCENT OWNER DEFENSE

- OHIO v. HOCHHAUSLER, 668 N.E. 2d 457 (1996) - distinguished from Bennis in that statute in OHIO provided for an innocent owner defense.

TOME v. UNITED STATES

- 115 s. Ct. 696
- Prior consistent statement is admissible hearsay to rebut allegation of fabrication or memory
- Limitation: must be made before a reason to be improperly influenced arises

UNITED STATES v. IGNACIO

- Child unavailable to testify
- 10 f. 3d 608
- Pediatrician allowed to testify as to what the child told him under the medical treatment exception
- Patient is expected to tell treating physician the truth

UNITED STATES v. BROWN

- 862 f.2d 1033
- Def. ordered child pornography video
- Did not receive what he ordered
- Held: knowingly received child porn. is sufficient
- No requirement to prove order by def.

THANK YOU FOR YOUR ATTENTION

HAVE A GREAT WEEK!

QUICK REFERENCE GUIDE: STORED WIRE AND ELECTRONIC COMMUNICATIONS

	Voluntary Disclosure Allowed? (§ 2702)		Mechanisms to Require Disclosure (§ 2703)	
	Public	Non-public	Public	Non-public
Unopened Email 180 days or <	no	yes (not covered)	search warrant [2703(a)]	search warrant [2703(a)]
Unopened Email > 180 days	no	yes (not covered)	S.W., subpoena w/ notice or 2703(d) order w/ notice [2703(b)]	S.W., subpoena w/notice, or 2703(d) order w/ notice [2703(b)]
Opened Email	no	yes (not covered)	S.W. or subpoena w/ notice or 2703(d) order w/ notice [2703(b)]	Outside stat. - 4th Amendment analysis only [2711(2)]
Material in a Remote Computing Svc. (stored files)	no	yes (not covered)	S.W. or subpoena w/ notice or 2703(d) order w/ notice [2703(b)]	Outside stat. - 4th Amendment analysis only [2711(2)]
Basic subscriber/transactional info. [2703(c)(1)(C)]	no - for "customer" or "subscriber" records	no - for "customer" or "subscriber" records	subpoena, 2703(d) order, or search warrant [2703(c)(1)(C)]	subpoena, 2703(order, or searc.. warrant [2703(c)(1)(C)]
Other Subscriber/ Transactional Information	no - for "customer" or "subscriber" records	no - for "customer" or "subscriber" records	search warrant or 2703(d) order [2703(c)(1)(B)]	search warrant or 2703(d) order [2703(c)(1)(B)]

Consent

§2702: A public service provider may disclose the content of protected materials "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." [2702(b)(3)]

§2703(c): A service provider may disclose subscriber or transactional information with the "consent of the subscriber or customer to such disclosure." [2703(c)(1)(B)(iii)]

Information Useful in Locating Defendant

INFORMATION LAW ENFORCEMENT FIND HELPFUL IN LOCATING SUBJECT

PERSONAL INFORMATION

- **Name**
- **Address**
- **Date of Birth**
- **Social Security Number**
- **Drivers License Number**
- **Telephone Number (day/evening)**
- **Place of Employment**
- **Position**
- **Address**

ACCOUNT INFORMATION

- **Date account opened**
- **Credit Card Information**
- **Referrals-other customers user brought to ISP**
- **Account status-terminated/canceled**
- **Account History/any contacts with user, any violations, change of address**
- **Screen Names Used**

USAGE HISTORY

- **All records of**
  - **Log on times**
  - **Log off times**
  - **Corresponding IP address for as long as possible.**

Sample Grand Jury Subpoena for ISP to Identify User

AO 110 (Rev. 12/89) Subpoena to Testify Before Grand Jury

United States District Court

EASTERN DISTRICT OF VIRGINIA

TO: Custodian of Records
Erol's Internet, Incorporated
7921 Woodruff Court
Springfield, VA 22151
Attn: Keith Poulsen

SUBPOENA TO TESTIFY BEFORE GRAND JURY

SUBPOENA FOR:

☐ PERSON ☐ DOCUMENT(S) OR OBJECT(S)

YOU ARE COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

PLACE	COURTROOM
UNITED STATES DISTRICT COURT 401 Courthouse Square Alexandria, Virginia 22314	GRAND JURY ROOM DATE AND TIME August 19, 1997 9:30 a.m.

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):*

PLEASE PROVIDE ANY AND ALL INFORMATION, INCLUDING SUBSCRIBER NAME AND ADDRESS, ADDITIONAL SCREEN NAMES (IF ANY), ALL TERMS OF SERVICE STAFF COMPLAINTS AGAINST THE IDENTIFIED SCREEN NAMES OR INDIVIDUAL, ANY BILLING INFORMATION (INCLUDING METHODS OF PAYMENT), AND ANY ADDITIONAL INFORMATION FOR THE FOLLOWING SCREEN NAME/ADDRESS:

Eg 1 [redacted]@erols.com — e-mail address

Eg 2 NUDEGOLFER — screenname

Eg 3 CEOSDC @AOL.COM — e-mail address

Eg 4 CEOSDC — screen name

SAMPLES

* If not applicable, enter "none"

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court.

CLERK	DATE
NORMAN H. MEYER, JR., CLERK OF THE COURT	July 28, 1997
(By) Deputy Clerk	

This subpoena is issued on application of the United States of America

HELEN F. FAHEY
UNITED STATES ATTORNEY

NAME, ADDRESS and PHONE NUMBER OF ASSISTANT U.S. ATTORNEY
Gerald J. Smagala, AUSA
U.S. Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314 (703) 299-3700

TOTAL P.02

Items to Seize in Search of Defendant's Home

LIST OF COMPUTER ITEMS TO BE SEIZED

Any and all:

- **Tapes**
- **Cassettes**
- **Cartridges**
- **Streaming Tape**
- **Commercial Software and Hardware**
- **Computer disks**
- **Disk drives**
- **Monitors, computer printers**
- **Modems**
- **Tape drives**
- **Disk application programs**
- **Data disks**
- **System disk operating systems**
- **Magnetic media**
- **Floppy disks**
- **Tape systems and Hard drive and other computer related operations equipment**

In addition to:

- **Computer photographs**
- **Graphic interchange formats and/or photographs slides or other visual depictions of such Graphic Interchange format equipment which may be, or are used to visually depict child pornography, child erotica, information pertaining to the sexual interest in child pornography, sexual activity with children or the distribution, possession or receipt of child pornography, child erotica or information pertaining to the sexual interest in child pornography,**

sexual activity with children or the distribution, possession or receipt of child pornography, child erotica or information pertaining to an interest in child pornography or child erotica.

Items to Seize in Search of ISP

ATTACHMENT A

You are to provide the following information:

A. User Connection Logs for all connections from [all target usernames and/or screen names] to the ISP for the time period beginning [date] through and including [date] to include, for each connection:

1. Connection time and date to ISP;

2. Disconnect time and date from ISP;

3. Method of connection (e.g., telnet, ftp, http) and numbers of any and all telephone lines associated with such connection;

4. Data transfer volume (e.g., bytes);

5. The subscriber account associated with the connection;

6. Any information related to any and all sessions during which the connection from [all target usernames or screen names] to ISP was open, including:

   a. Connection time and date;

   b. Disconnect time and date;

   c. Method of connection;

   d. Ancillary and source information relating to such connection;

   e. Any other record or information pertaining to such connection.

B. Subscriber information for each subscriber account identified in Part A, above. For each such subscriber, the information shall include:

1. The subscriber's name, and any and all usernames, screen names and passwords;

2. The subscriber's address;

3. The subscriber's telephone number or other subscriber number or identity;

4. The subscriber's e-mail address;

5. Any other information pertaining to the identity of the subscriber, including, but not limited to, date of birth, social security number, driver's license, billing information (including type and number of credit cards or bank accounts).

6. Any other record or information pertaining to the subscriber account, including length of account activation, type of service, special requested services, records of contacts between the subscriber and ISP, or other service notes.

C. All subscriber information for each subscriber who, for any session that began or ended on [Dates] was assigned the [target usernames and screen names]. For each such subscriber, the information shall include:

1. The subscriber's name, and any and all usernames, screen names and passwords;

2. The subscriber's address;

3. The subscriber's telephone number or other subscriber number or identity;

4. The subscriber's e-mail address;

5. Any other information pertaining to the identity of the subscriber, including, but not limited to, date of birth, social security number, driver's license, billing information (including type and number of credit cards or bank accounts).

6. Any other record or information pertaining to the subscriber account, including length of account activation, type of service, special requested services, records of contacts between the subscriber and ISP, or other service notes.

D. User connection logs for all users identified in Part C, above, for the time period beginning [date] through and including [date] to include, for each connection to ISP:

1. Connection time and date;

2. Disconnect time and date;

3. Method of connection;

4. Data transfer volume (e.g., bytes);

5. Ancillary information relating to such connection;

6. Any other record or information pertaining to such connection.

E. Contents of any and all electronic communications held in electronic storage for more than 180 days, as such terms are defined in 18 USC § 2510.

Excerpts from Computer Search Warrants and Sample Affidavit Language for Particular Problems

Prepared by Gail Thackeray and Dean Chatfield
Maricopa County Attorney's Office, Arizona

EXCERPTS FROM COMPUTER SEARCH WARRANTS

I. ITEMS TO BE SEARCHED FOR AND SEIZED:

1. Electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as modems; together with system documentation, operating logs and documentation, software and instruction manuals.

[*Note:* this type of language applies to the situation in which the presence of a personal or small business computer is suspected (a large drug operation), or probable (a computer hacker), but where it has been impossible to determine in advance what kind of system it is. Ideally, investigation prior to execution of the warrant has produced specific information about the system, and those specifics should then be included in the description of items to be seized.]

2. [Follows the description of specific records to be seized]

All of the above records, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic address books", calculators, or any other storage media, together with indicia of use, ownership, possession, or control of such records.

[*Note:* if the search warrant is properly specific as to the nature and content of records to be seized, the form in which the record is found should be irrelevant. However, to avoid challenges to the seizure of computer diskettes, etc. not mentioned in a traditional "books and records" warrant, some language such as this should be included in situations in which it is not absolutely known that all the records sought are on paper. Of course, the search team can always obtain a supplemental warrant if there is any doubt that records found in unexpected "hardware" form, such as a programmable electronic telephone directory, are authorized to be seized.]

II. SAMPLE AFFIDAVIT LANGUAGE FOR PARTICULAR PROBLEMS:

A. Justification for seizing hardware, etc. (where appropriate):

1. Affiant interviewed *[expert]*, employed as a *Police Officer* in the *Chandler Police Dept.* (S)he informed affiant "that in connection with his/her employment, (s)he uses computer systems as well as conducting computer-related investigations. In the past *[...]* years, *[expert]* has supervised or participated in executions of search warrants for computer-stored records and evidence. *[expert]* informed affiant that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place which could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without expert technical assistance. Since computer evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the entire period of the search.

2. *[expert]* also stated that whether records are stored on floppy disks or on a hard drive, even when they purportedly have been erased or deleted, they may still be retrievable. *[expert]* is familiar with the methods of restoring "lost" data commonly employed by computer users, and has used those methods him/herself. *[expert]* has also obtained the assistance of a computer expert in several cases, in order to obtain the contents of computer-stored evidence, where normal methods were unsuccessful. (S)he stated that should such data retrieval be necessary, it is time-consuming, and would add to the difficulty of securing the system on the premises during the search.

3. *[expert]* stated that the accompanying software must also be seized, since it would be impossible without examination to determine that it is standard, commercially available software: it is necessary to have the software used to create data files and records in order to read the files and records. In addition, without examination, it is impossible to determine that the diskette purporting to contain a standard commercially available software program has not been used to store records instead. *[expert]* informed affiant that the system documentation, instruction manuals, and software manuals are also necessary to properly operate that specific system in order to accurately obtain and copy the records authorized to be seized.

B. Records-only Seizure (Hardware not to be seized, if search can be performed on scene)

1. Affiant interviewed *[expert]*, employed as a *Police Officer* with the *Police Department*. *[expert]* informed affiant that in connection with his/her employment, (s)he uses computer systems and conducts computer-related investigations. In the past *8* years, has supervised or participated in more than *30* executions of search warrants for computer or magnetically-stored records and evidence. *[expert]* has conducted training for law enforcement agencies on computer-related search warrants, and has instructed numerous classes on this topic.

2. *[expert]* informed affiant that conducting a search of even a personal or desktop computer system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is first necessary to determine that no security devices are in place which could cause the destruction of evidence during the search; in many cases it is impossible even to conduct the search without special tools, utility software, or expert technical assistance.

3. *[expert]* advised affiant that on *MM/DD/YR*, (s)he entered the premises to be searched and observed what appeared to be terminals on a network system (these might be connected to microcomputers, a minicomputer, a mainframe, a network server, or some combination of these and other computer processing units), rather than stand-alone personal computers. The brand of terminal that *[expert]* observed appeared to be *[name]* which could indicate that the operating system may be either IBM (MS-DOS), or a form of Unix/Zenix operating system. If the system is Unix/Zenix, the assistance of an expert in that type of system would be necessary in order to conduct the search; it might also be necessary for such an expert to bring or obtain the appropriate Unix/Zenix utility programs to aid in conducting the search and preserving and documenting the evidence.

4. The search team will first attempt to make a backup copy of the records and associated software (see below). If, upon preliminary examination of the system, that procedure is not practicable or appears to pose a risk to the integrity of the magnetically-stored originals, then *it* may be necessary to remove all or a portion of the system from the premises, in order to secure its contents while expert assistance is obtained to complete the analysis.

5. Since computer evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the entire period of the search. On a system with a large volume of records, even with expert assistance, this process might easily take days or weeks, during which time the owners of the premises would be denied access to the areas in which the computer system components are located.

6. *[expert]* also stated that whether records are stored on floppy disks, tape or on a hard drive, even when they purportedly have been erased or deleted, they may still be

retrievable. *[expert]* is familiar with the methods of restoring "lost" data commonly employed by computer users, and has used those methods him/herself. *[expert]* has also obtained the assistance of a computer expert when necessary, in order to obtain the contents of computer-stored evidence, where normal methods were unsuccessful. (S)he stated that should such data retrieval be necessary, it is time-consuming, and would add to the difficulty securing the system on the premises during the search.

7. *[expert]* stated that the accompanying software often must also be seized; it is frequently necessary to have the software used to create data files and records in order to read the files and records. It would be impossible without examination to determine that it is standard, commercially available software. In addition, without examination, it is impossible to determine that a diskette purporting to contain a standard commercially available software program has not been used to store records instead.

8. *[expert]* informed affiant that the system documentation, instruction manuals, and software manuals may also be necessary to properly operate that specific system in order to accurately obtain and copy the records authorized to be seized.

9. *[expert]* also stated that because of the ways in which various types of computer technologies operate in storing or processing records, in his/her experience, it is common to find that specific records authorized to be seized are inextricably mixed or without difficult or extremely time-consuming procedures are inseparable from other records, programs, or files (similar to a bound-volume book containing financial records, addresses, a diary, and notes, for example). In that event, the storage medium containing items to be seized will be backed up (at the search scene, if reasonably feasible as stated above, or after removal from the premises) and in later analysis, the items authorized to be seized will be printed out or otherwise copied for evidence purposes. Upon completion of the analysis, the backup, tape, diskette, hard drive, etc. from which those evidence copies were made will be sealed and secured for future comparison with the evidence copies.

10. If it should prove necessary to remove all or a portion of the system from the premises, as soon as reasonably can be done, those items of hardware no longer required for the purpose of analysis or copying of items authorized to be seized, or for preservation of magnetic evidence, will be returned to the party from whom they were seized, in order to minimize interference with the operation of the business.

COMMENTS:

The language above was designed for a situation in which we were sure for various reasons that we did not want to seize the system itself, if we could help it. (Factors which might lead to this conclusion could include: advance knowledge that records of businesses other than the target's are stored on the same system, that the system is simply too big or too fragile to be moved, situations where the computer is not an instrument of the crime as in a hacker case but is merely a neutral repository of records, etc. Each case must be considered on its own combination of technical, practical and strategic factors in determining whether it is necessary or advisable to remove the system itself.)

The warrant and affidavit lists of items to be seized should include all items which it is foreseeable might have to be seized for technical reasons, even though at the time of search, the decision may be made to leave a listed item behind (i.e., "If you don't leave me one computer, we can't make payroll by Friday") This is much easier than having to obtain a supplemental warrant during the search because the list failed to include an item which turns out to pose technical problems.

Paragraph 9 is an attempt to educate the judge in the practical realities of magnetically-stored evidence, and to obtain advance judicial blessing for post-search analysis techniques. In appropriate cases, this may help to avoid suppression or liability problems. It may also help to overcome an overbreadth challenge (i.e., "You took records which were not in the warrant!") By handling such media (diskette, hard drive, etc.) in a way analogous to original audio/wiretap tapes, working from a copy and sealing the original, you are protecting the integrity of the original and will be able to meet foundation and authentication challenges. By warning the court that for technical or legal reasons it may be necessary to seize or make a backup of all records on a disk, tape or drive rather than taking only the specific records itemized in the warrant, but also making it clear that other records will not be printed out or copied, you are demonstrating a good-faith attempt to minimize the potential harm to the owner of the other records. This is the computer equivalent of after-the-fact minimization in an interception.

If records not authorized to be seized, or which relate to crimes not under investigation, are discovered in the course of analysis, consider the advisability of obtaining a supplemental warrant. While there is a valid argument that such records were lawfully discovered in "plain view," this issue has not been resolved, like most other electronic-media search issues.

✪ Gail Thackeray, Maricopa County Attorney's Office, (602) 506-3411

SAMPLE LANGUAGE FOR COMPUTER SEARCH AFFIDAVIT

[Add to: "ITEMS TO BE SEARCHED FOR AND SEIZED"]

Electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as modems; together with backup media, system documentation, software and instruction manuals.

All of the above records, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic calendar\address books", calculators, wristwatches, personal communication service (PCS) devices, or any other storage media, together with indicia of use, ownership, possession, or control of such records.

(Note: Put this paragraph in ***all*** records search warrants! -- at least, when you encounter a "gadget" instead of a paper record, you'll have something in the warrant to justify your seizure. You may need consider getting a supplemental warrant, though, to authorize you to go in and search a computer seized under this language alone...)

SAMPLE EXPERT INTERVIEW LANGUAGE:

[Add to: end of Affidavit narrative]

Affiant interviewed *Dean Chatfield, a Criminal Investigator with the Maricopa County Attorney's Office, who has both received and given training through the International Association of Computer Investigative Specialists, in computer forensics and evidence processing. He has received IACIS' certification in computer evidence processing, and has performed and assisted at numerous computer-related search warrant executions for his own and many other law enforcement agencies. He currently serves on the IACIS Executive Board and Board of Directors, and is the chairman of its training and certification committees. In that capacity, he has trained law enforcement officers from numerous local, state and federal agencies, as well as from several foreign nations. Recently, he was selected to serve on the IACIS team which provided computer forensics training to the Royal Hong Kong Police. Chatfield is a computer user with ten years of experience in using, building, and repairing computer systems, and in data recovery.*

Chatfield informed affiant that conducting a search of a computer system, locating particular records, documenting the search, and making evidentiary and discovery copies is a lengthy process. Nowadays, it is not unusual for even a home computer system to contain 1 gigabyte or more of data storage capacity on its hard drive, with additional records stored in the form of tape or floppy disks. (A "byte" is equal to one character of the alphabet: the letter "A"

takes up one byte of space on computer storage media, such as a floppy diskette or a hard drive. A "megabyte" is equal to 1,400,000 bytes, which is also the capacity of a standard 3.5" high 1.44 meg high density diskette. A "gigabyte" is equal to 1,000 megabytes or 1,400,000,000 bytes. A standard 3.5" high density diskette might contain the equivalent of .5 -- 2.5 paperback books.)

In a forensic examination of a computer system, it is first necessary to determine that no security devices are in place which could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without specialized technical assistance. Since computer evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will permit retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It is also common to store records in compressed or archival formats, which require that appropriate software be employed to "unarchive" or "uncompress" each record before it can be viewed. It would be extremely difficult to secure the system on the premises during the entire period of the search, which can take days, or even weeks, depending upon the technical problems encountered.

Chatfield also stated that whether records are stored on floppy disks or on a hard drive, even when they purportedly have been erased or deleted, their content may still be retrievable. *Chatfield* is familiar with the methods of restoring "lost" data commonly employed by computer users, and has often used those methods himself. *Chatfield* has also obtained the assistance of a computer specialist with relevant expertise in several cases, in order to obtain the contents of computer-stored evidence, where normal methods were unsuccessful. He stated that should such methods be necessary, they are time-consuming, and would add to the difficulty of securing the system on the premises during the search.

Chatfield stated that the accompanying software must also be seized, since it would be impossible without examination to determine that it is standard, commercially available software: it can be necessary to have the software which was used to create data files and records, in order to gain access to their contents. In addition, without examination, it is impossible to determine that a diskette purporting to contain a standard commercially available software program has not been used to conceal evidence instead. *Chatfield* informed affiant that the system documentation, instruction manuals, and software manuals are also necessary to properly operate that specific system in order to accurately obtain and copy the records authorized to be seized.

Chatfield stated that because computer users often do not upgrade obsolete systems, or keep their hard drives in repair, situations can arise in which it is impossible to read a floppy diskette except upon the system which created it. (The same result can be achieved by a user intentionally altering his system in order to prevent the records on the diskettes from being read by others.)

Chatfield advised that because of the ways in which various types of computer technologies operate in storing or processing records, in his experience, it is common to find that

specific records authorized to be seized are inextricably mixed or without difficult or extremely time-consuming procedures are inseparable from other records, programs, or files (similar to a bound-volume book containing financial records, addresses, a diary, and notes, for example). In that event, the storage medium containing items to be seized will be backed up and in later analysis, only the items authorized to be seized will be disclosed, printed out or otherwise copied for evidentiary purposes. In order to determine which records those are, it is necessary to use the appropriate software to "open" and view the contents of each file; the file name in the directory is not a reliable indicator of the nature of its contents, especially where there may be a desire on the user's part to conceal certain records. Upon completion of the forensic analysis, the backup tape, diskette, hard drive, etc. from which those evidence copies were made will be sealed and secured for future comparison with the evidence copies.

Chatfield also stated that in his experience both as an investigator and as a computer user, it is common for individuals who have personal computers or "electronic calendar\address books" to store in the memories of those devices their records of financial transactions and expenses; notes, correspondence and memoranda; telephone and address databases; calendars and appointments; and business and personal records of all types. *Chatfield* stated that it is quite common for people with a home computer to advertise merchandise for sale, order goods and services, exchange correspondence and files, and pay their bills electronically. He also stated that because of the convenience of storing a large volume of records electronically, in his experience people store computer records for much longer periods than they would if they had to maintain the same volume of records in paper form. He has examined computer search scenes which proved to contain computer evidence five years old, and even older.

SAMPLE AFFIDAVIT LANGUAGE: MINIMIZATION PROBLEMS

Computer Searches:

[Where it is intended that the system will be searched on the premises, rather than seized and removed for later laboratory analysis]

The search team will first attempt to make a backup copy of the records and associated software (see below). If, upon preliminary examination of the system, that procedure is not practicable or appears to pose a risk to the integrity of the magnetically-stored originals, then it may be necessary to remove all or a portion of the system from the premises, in order to secure its contents while expert assistance is obtained to complete the analysis.

[expert] also stated that because of the ways in which various types of computer technologies operate in storing and processing records, in his experience, it is common to find that specific records authorized to be seized are inextricably mixed or without difficult or extremely time-consuming procedures are inseparable from other records, programs, or files (similar to a bound-volume book containing financial records, addresses, a diary, and notes, for example). In that event, the storage medium containing items to be seized will be backed up (at the search scene, if reasonably feasible as stated above, or after removal from the premises) and in later analysis, only those items authorized to be seized by the warrant will be printed out, and/or stored on an evidence disk, or otherwise copied for evidence purposes. Upon completion of the analysis, the complete backup, tape, diskette, hard drive, etc. from which those evidence copies were made will be sealed and secured for future discovery and for comparison with the evidence copies.

Digital pager interception:

The pager interception device [or duplicate pager] performs a function similar to a dialed number recorder (pen register) or trap and trace device, in that the only communications content intercepted will be the numbers dialed or punched from calling telephones and transmitted through the pager company's equipment to the digital pager assigned the number *(602)* _____. As a result, call-by-call monitoring and minimization of the type normally performed in connection with interception of wire communications is neither necessary nor feasible. The minimization is inherent in the technology, and in the very limited nature (telephone-punched digits) of the interception. ***

The relevance of each pager transmission cannot be determined during the extremely short signal-time, nor until the subscribers and users of telephones whose numbers are transmitted to the pager can be identified by the appropriate communications carriers.

****(Some paging systems can transmit brief text messages, but the minimization problems are the same – until the carrier identifies the calling party, the significance of a particular message may not be apparent.)*

Computer Bulletin Board (or other shared system):

[Warrant for files relating to offense, and e-mail of certain parties]

...Because of the volume of stored material and the fact that the files authorized to be seized may not be readily identifiable from their filenames, and are unlikely to be stored together but instead dispersed throughout the entire hard drive(s), searching for and extracting specific files would be extremely time-consuming and may not even be technically possible without the special tools and resources of a forensic environment. If possible, the hard drive(s) will be backed up; a "mirror image" (or duplicate original) of the drive(s) will be created at the scene, and the system itself will not be seized.

However, it is possible that the search team will encounter technical problems such as those described above *[earlier portion of affidavit]* which will preclude the copying of a mirror image backup at the scene. In that event, the system will be seized, along with any peripherals, software and technical manuals necessary for forensic data recovery procedures. In later analysis of the drive and/or mirror image backup, only the items authorized to be seized will be printed out or otherwise copied (i.e., to an evidence disk) for evidence purposes. Upon completion of the analysis, the media *[backup tape, Bernoulli cartridge, evidence hard drive, etc.]* from which those evidence items were produced will be sealed and secured for future discovery procedures and comparison with the evidence copies.

At present, affiant has no intention of reading any electronic mail other than that authorized to be searched *[named users, SYSOPS, etc.]* for evidence of their involvement in the crimes of *[offenses]*. In the course of the continuing investigation, if it appears that there is probable cause to believe that the electronic mail of other persons may contain evidence of these offenses, further application will be made to this court.

"Mirror image" backup of system:

Therefore, it is requested that the forensic specialists from the _____ Department or the _____ Attorney's Office be given access to the evidence including the computer system, diskettes, and the cards and correspondence seized from _____'s [house]. The forensic specialist will then make "mirror images" (in reality, duplicate originals, down to the sector and byte level) of the computer hard drive and diskettes, for forensic analysis.

After recovery of any hidden, deleted or erased data, the analyst will determine which files, communications, or documents found in the system constitute evidence of the offenses enumerated above; only those items will be copied. Evidence copies of the items relating to these offenses will be created, retained for further proceedings, [and made available to the _____ _____ authorities.] The duplicate original, or "mirror image" will be sealed and retained in evidence for later discovery and trial purposes. None of the contents of the "mirror image" or duplicate original, other than those which may be required for prosecution, will be displayed to any person other than the analyst, prosecutor(s) and case agents, or disclosed, used or copied.

Automated Text Search of Network, Bulletin Board, or other Shared System:

Affiant is aware of the requirement to protect the privacy of users of the *[network, shared system, bulletin board, etc.]* who may not be involved in the conspiracy to *[distribute child pornography, drugs, whatever]*. Because at this time it is not known who are the other coconspirators with *[Mr. X]* and who may be innocent users of the *[BBS, network, etc.]*, affiant will employ a computer program which searches the data storage areas of the system for "keywords" or "text strings" in order to identify those areas where records relating to the crimes of *[offenses]* may be found. Only after a match between a particular *[record, stored communication, etc.]* is discovered, will affiant open that file and read its entire contents to confirm that it is among those records authorized to be seized.

Affiant will document and save for future evidence review purposes: 1) a record of the content of the searches performed, and 2) a record of the matches found. Only those *[records, communications, etc.]* identified through this procedure and which, upon review, prove to be among those authorized to be seized, will be copied, displayed, printed out, or disclosed. Upon completion of the system analysis, the *[system, hard drive, backup copy, mirror image, etc.]* will be impounded and sealed for future evidentiary and discovery purposes, and *[the system, hard drive, a copy, a mirror image, etc.]* will be returned to *[Mr. X]*. *[Optional:]* A supplemental inventory list of those items which were copied and retained for evidence purposes will be returned to the court upon completion of the system analysis.

Fax Interception:

Because facsimile documents are transmitted over telephone lines in digital form by means of fax modems at very high speed, their content cannot be understood by the monitors during transmission. Therefore, it would be impossible for the monitors to determine the relevance of any particular fax communication to the crimes under investigation during transmission, for minimization purposes. Once the transmission is complete, the fax image is stored in the fax interception equipment which, in effect, "translates" the digital communication or code into human-readable form. Since the content of a fax communication (unlike wire or oral communications) cannot be evaluated during transmission, affiant requests authorization to perform after-the-fact minimization pursuant to *[A.R.S. §13-3010(M)]* as follows:

> The fax interception equipment will store the content of incoming or outgoing faxes on a computer hard drive for review. The equipment is located in a secure area *[describe]* and has a lock on it. Only affiant *[case agent, supervisor, etc.]* will have access to the equipment and the stored fax communications. Affiant will review all stored faxes and will make evidence diskette or printout copies only of those faxes relevant to the criminal offenses enumerated in the interception order(s), and will not copy, display or discuss the content of non-pertinent fax communications. The assigned prosecutor may be consulted where necessary in determining the relevance of particular communications.

At the conclusion of authorization for interception, a complete copy of all intercepted faxes will be transferred to an evidence diskette [tape, cartridge, etc. depending upon volume & available media], write-protected, and delivered to the court for sealing and preservation. A duplicate original will be sealed and maintained in evidence for future foundational/discovery purposes, and only the evidence copies relating to the criminal offenses will be made available to the investigating team for followup.

Choosing the Right Computer Expert

by
David Goldstone
USDOJ
Criminal Division
CCIP Section

Qualifications of Computer Experts

General Issues:

1. Do you in fact need to qualify your witness as an expert? Are they testifying as to something they did (e.g., "I copied a file off the defendant's hard drive"), in which case they are merely a witness, or do you want them to render an expert opinion on an issue in your case (e.g., "The defendant's specialized program was designed to hide pertinent files in hidden directories")?

2. What "expertise" is needed? Are you concerned with hardware (e.g., mainframe, personal computer, modem), specialized software applications (e.g., a spreadsheet, word processing application), an operating system (e.g., DOS, UNIX), or network architectures (e.g., Novell Netware)? Do you need an expert who understands a particular application as run on a particular operating system? Remember, a computer expert who builds mainframe computers may not know how a specific operating system or programming language works. THEREFORE, when preparing your qualifying questions, focus on your expert's training, certification, and experience on the specific areas important to your case: (1) hardware, (2) operating systems, (3) network architectures, (4) applications, (5) programming languages; and/or (6) data storage, retrieval and analysis.

3. Who is your target audience? If you are attempting to teach a jury the intricacies of computer technology, an academician who teaches for a living may be a good choice. If, on the other hand, you are conducting a suppression hearing before a computer literate judge, a more technical expert may be appropriate.

Specific Questions (not all questions will be appropriate for all witnesses):

1. Name
2. Current Employment
   - A. How long?
   - B. Current Assignment
3. Computer Education
   - A. Formal Education
     - (1) Schools
     - (2) Degrees
   - B. Technical Courses (outside formal schools)
     - (1) Vendors
     - (2) Professional Associations
     - (3) Law Enforcement Groups (such as the High-Tech Investigators Association, SEARCH, etc).
   - C. Certifications
     - (1) See Attached Article (Certified Computer Professionals--What Do All Those Letters Mean?
     - (2) Vendor Certifications (e.g., Novell certifies

system administrators on Novell products)

(3) Law Enforcement Certifications (some agencies, such as FBI, IRS, USSS run specialized training programs for field examiners and grant certifications upon completion).

4. Prior Experience
   A. Jobs
   B. Investigations/Cases
   C. Prior Testimony
      (1) Ever qualified as expert before?
      (2) Ever denied expert status?
5. Publications (if, in fact, the witness has been published)
   A. Topics Covered
   B. Place of publication
6. Teaching Experience
   A. Some experts teach courses to others and this should be brought out.
7. Membership in Professional Organizations (may overlap, in some cases, with certifications).
8. Although a judge may allow you to offer a witness as an expert in "computers," you may need to be more specific: "I offer him/her an expert in:" (1) electronic data storage, retrieval and analysis; (2) the programming or operation of application xxx (e.g., WordPerfect); (3) engineering, architecture, and operation of telecommunications computers; etc, etc.

Certified Computer Professionals--What Do All Those Letters Mean?

In complicated computer crime cases, it will often be necessary to use a computer expert. If you really want to impress the jury, you can call to the stand someone like Mr. Smith, CPP, CDP, CSP, CSSP, CISA. But what do all those letters mean? The answer can be found in Hal Tipton's informative article in the Winter 1993 issue of Information Systems Security.

CPP: ASIS (The American Society for Industrial Security) offers an examination which, if passed, earns the title Certified Protection Professional. The focus of this program is physical security (e.g., securing systems from fire, flood, etc.).

CCP, CDP, CSP: Individuals can be certified by the Institute of Computer Professionals by taking a core examination, an information security examination, and one of three specialized examinations. They are Certified Computer Programmer (CCP); Certified Data Processor (CDP), and Certified Systems Professional (CSP).

CSSP: The International Association for Computer System Security certifies its candidates with a lengthy examination and educational or work experience. Mr. Tipton writes: "This examination is not highly regarded, and it was not developed according to commonly accepted practices in information security."

CISA: This award, issued by the EDP (Electronic Data Processing) Auditors Association, focuses on the needs of system auditors and does not address other important security areas such as access controls and encryption.

Mr. Tipton's conclusion is that none of these certification procedures takes into account the full body of knowledge with which system administrators should be familiar. Therefore, the International Information Systems Security Certification Consortium (ISC-squared) is implementing a new certification process, leading to a new acronym: CISSP (Certified Information Systems Security Practitioner). Applicants will be required to pass an examination and have at least three years' experience in information security. They will be required to be conversant in a "common body of knowledge" which includes seventeen computer security topics including access controls, cryptography, telecommunications security, and legal and regulatory issues.

Conducting the Child Exploitation Investigation

CONDUCTING THE CHILD EXPLOITATION INVESTIGATION

By
Robert Hugh Farley

Child Exploitation Unit
708-865-4875

A "PRACTICAL" RESPONSE TO THE CRIME - MODULE OVERVIEW

- *What is really "practical" for your agency?*
- *The "online" problem*
- *Victim issues / the interview*
- *Offender issues*
- *Investigative techniques reactive vs. proactive*
- *Interrogation techniques*

ONLINE CHILD EXPLOITATION

- *Is it a crime?*
- *Who is the actual offender?*
- *Evidence?*

DOES YOUR COMMUNITY HAVE AN ONLINE PROBLEM ?

TYPICAL TYPES OF ONLINE INVESTIGATIONS

- *"Dirty conversations"*
- *Distribution of pornography*
- *Distribution of child pornography*
- *Luring the child for a meeting*
- *Luring the child for sex*
- *Traveling for sex*

HOW WILL YOUR COMMUNITY RESPOND TO YOU CONDUCTING "OUTSIDE" ONLINE INVESTIGATIONS ?

COORDINATION

- *Child Exploitation Unit*
- *Internet Task Force*
- *Local FBI Office*
- *Innocent Images*
- *U.S. Postal Inspectors*

PROSECUTION

- *Options...*
- *Cook County*
- *Other Countries or States*
- *U.S. Attorney's Office*
- *Local and Federal*

HOW DOES YOUR AGENCY RESPOND TO ONLINE COMPLAINTS ?

ONLINE INVESTIGATIONS

- *Do you have a designated law enforcement online officer?*
- *Do you have a computer unit?*
- *Are you capable to be reactive?*
- *Are you capable to be proactive?*
- *General orders and protocol?*

CONDUCTING THE CHILD EXPLOITATION VICTIM INTERVIEW

INTERVIEWING THE VICTIM

- *No parents present !*
- *Interview by a Juvenile Officer*
- *Interview by a Team Member at a Child Advocacy Center*
- *The victim may be in "love" with the offender*
- *Therapy*
- *May warn the offender*

INFORMATION TO BE OBTAINED

- *About the Victim or Offender :*
- *Nicknames or screen names*
- *Conversation times, length*
- *Conversation content*
- *Specific sexual conversations*
- *Specific personal information*
- *Telephone calls, pagers*
- *Gifts, cards, letters, etc.*

SPECIFIC QUESTIONS

- *Who is your best friend online?*
- *Who is your best friend off the computer?*
- *Where else do you, have you or can you go online?*
- *Have you ever gone and met with anyone as a result of the computer? Have any of your friends?*

FREEHAND DRAWING INTERVIEW

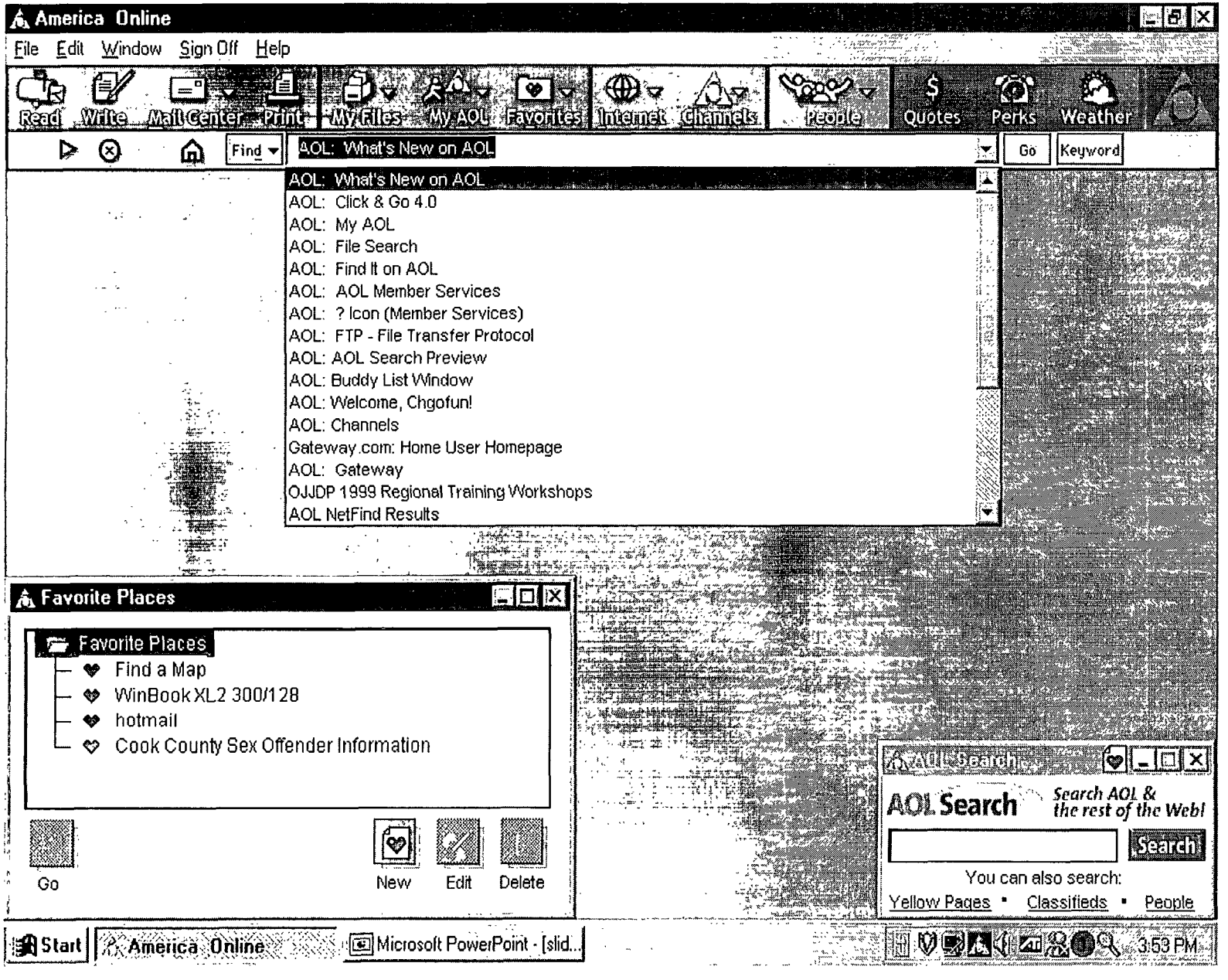
- *Write your name?*
- *Draw yourself?*
- *Draw your family?*
- *Draw what happened?*
- *See the Appendix for Selected Readings*

INSPECT THE VICTIM'S COMPUTER AREA

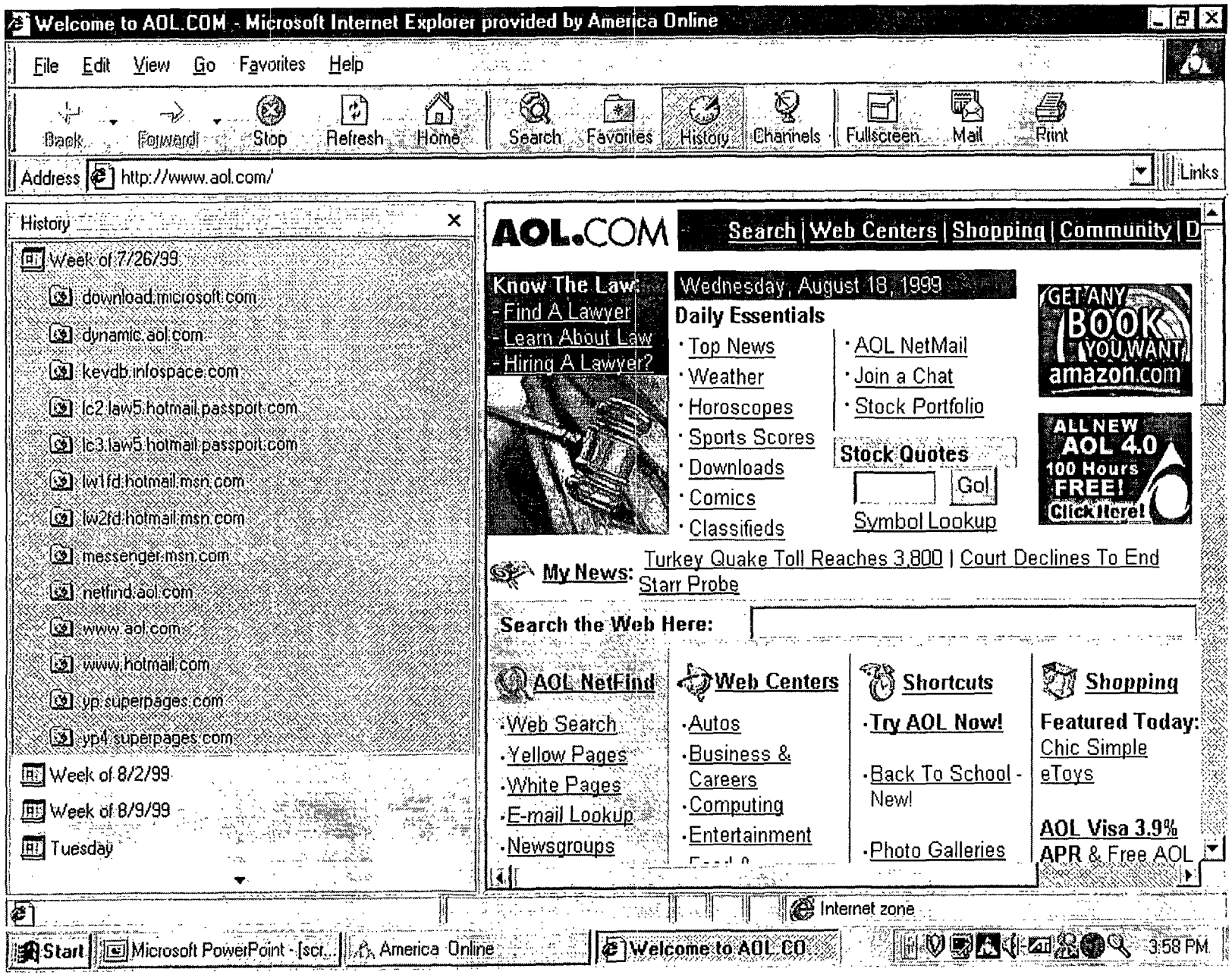
- *Consent to search*
- *Who uses the computer?*
- *Post-it notes*
- *Hard copies*
- *Discs*
- *Garbage can*

EXAMINE THE VICTIM'S COMPUTER

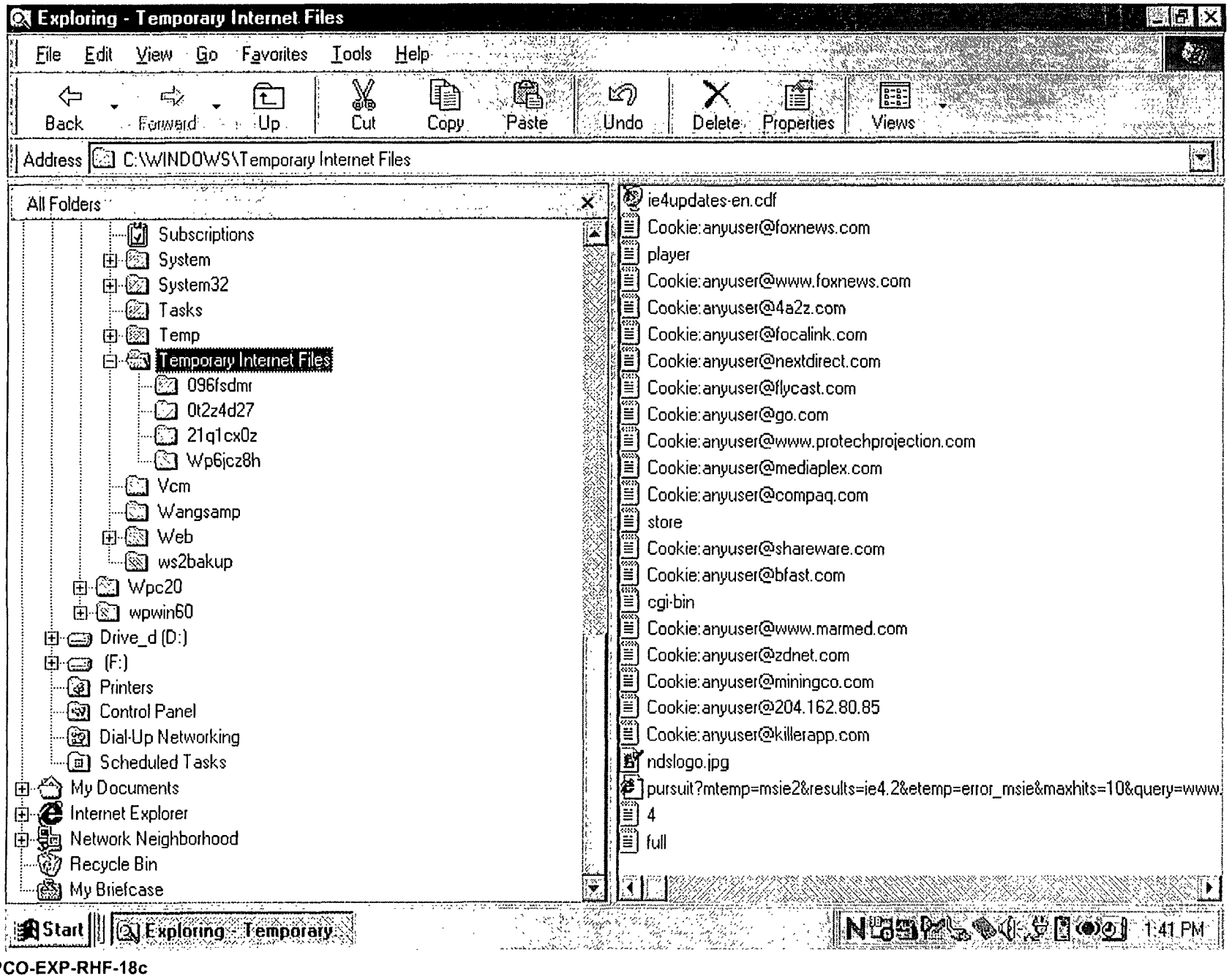
- *Buddy list*
- *Private files*
- *Download files*
- *Recycle bin*
- *History*
- *Temporary files*
- *Cookies*



PCO-EXP-RHF-18a



PCO-EXP-RHF-18b

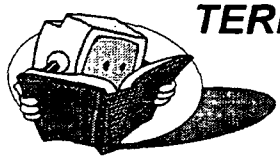


PCO-EXP-RHF-18c

COMPUTER AND ONLINE EDUCATION

AWARENESS versus EXPERT WITNESS

IDENTIFICATION OF COMPUTER TERMS



COMPUTER

- *Hard drive - memory storage*
- *Speed - how fast information is processed*
- *Windows environment - point and click*
- *Modem - telephone line*

OPENING A FILE

- *Display*
- *Text or document*
- *Photo*
- *Video or movie*

DOWNLOAD A FILE

- *Virus*
- *Received from an external source*
- *Storage - disc, hard drive*

DANGEROUS FILES

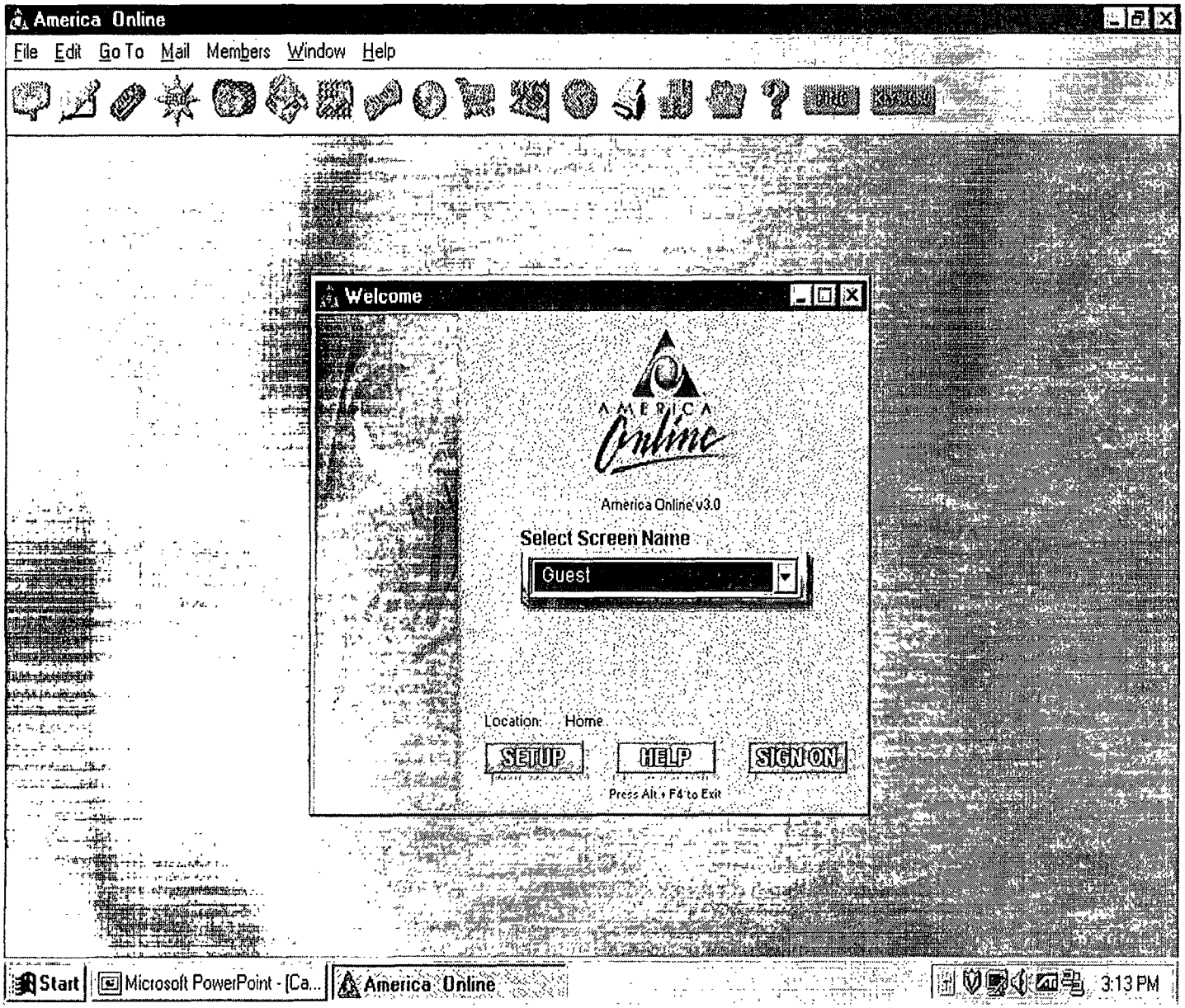
- *Virus*
- *.exe, .com, .bat, .doc*
- *Java*
- *Software - viewer*
- *Photos - .jpg, .gif*
- *Movies - .avi, .mpg*

UPLOAD A FILE

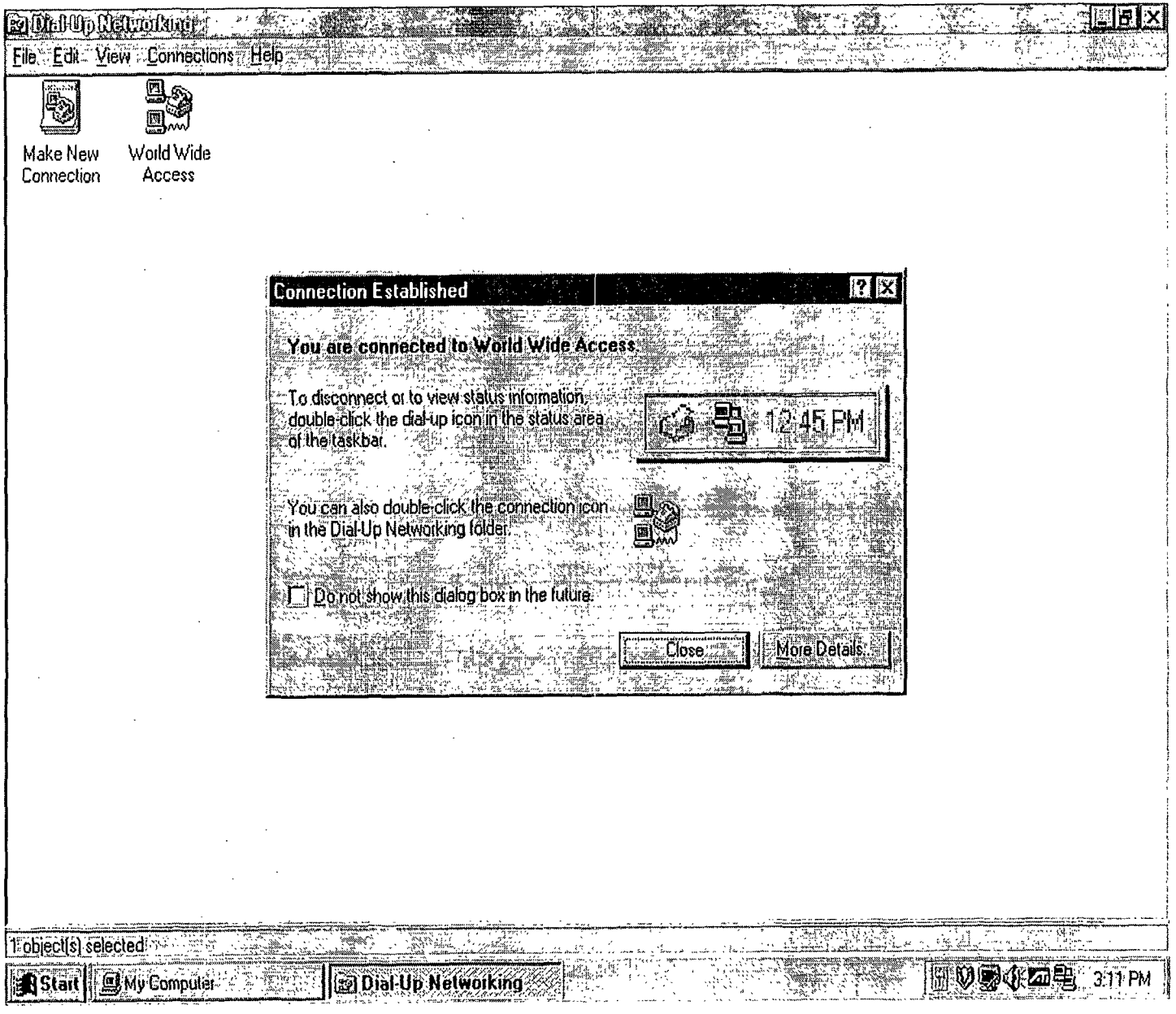
- *Send file from your computer to another site*

SURFING THE NET

- *Modem*
- *Commercial gateway*
- *Service Provider*



PCO-EXP-RHF-27a



PCO-EXP-RHF-27b

OBTAINING YOUR EQUIPMENT

- *Purchased*
- *Donated*
- *Seized - see form*

CCSPD / UNIT COMPUTER

- *Dedicated computer*
- *Windows 95 or 98*
- *Speed 300 MHZ or faster*
- *Pentium II processor*
- *Hard drive - 1.2 GB*
- *Modem -56 k baud*
- *Printer - 8mb upgrade*
- *Scanner*
- *Registered software*

INTERNET RELAY CHAT CHANNELS

- *mIRC shareware software*
- *Dalnet*
- *Undernet*
- *Chicago area server*

CHILD MOLESTER

- *Pedophile*
- *DSM IV*

CHILD MOLESTER

- *Situational Molester*
  Not a true sexual preference for a child
- *Preferential Molester*
  True sexual preference for a child
- *ONLINE CHILD MOLESTER*

MOLESTER SEDUCTION TECHNIQUES

- *Assumes a child or teen identity*
- *Bogus profile*
- *Language*
- *Asks for personal information*
- *Requests photos*
- *Talks about family/friends*
- *Telephone contact*
- *Wants to meet*

REACTIVE UNDERCOVER INVESTIGATIONS

- *REAL VICTIM*
- *Luring the child for a meeting*
- *Luring the child for sex*
- *Traveling for sex*
- *Can your agency assume the victim's identity?*
- *Can you identify the suspect?*

ONLINE "REAL VICTIM" CASE ILLUSTRATION

IDENTIFICATION OF MOLESTER

- *Server*
- *IP address*
- *Identify exact contact*
- *Computer*
- *Telephone records*
- *"Body"*

DEFENSES

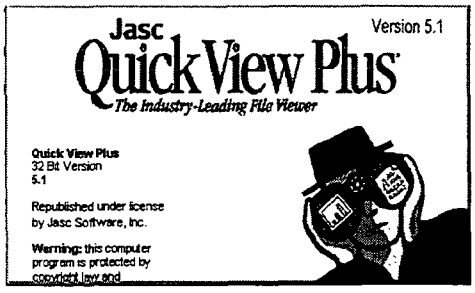
- *Wasn't me*
- *Stolen password*
- *Unknown age*
- *Wasn't a kid*

SCENE

- *IBM vs. Mac*
- *Photograph everything!*
- *Back and front*
- *Hard copies*
- *Passwords*
- *Discs*
- *Post-it notes*

FORENSIC REVIEW

- *Identification of your resources*
- *EVIDENCE !!!*
- *Local police agencies*
- *Computer stores*
- *Universities*
- *State agencies*
- *Federal agencies*



PROACTIVE UNDERCOVER INVESTIGATION TECHNIQUES

UNDERCOVER OFFICE

- *Secure area*
- *Dedicated computer(s)*
- *U/C Line - computer*
- *U/C Line - voice*
- *U/C Postal mailbox*
- *Shredder*

UNDERCOVER OFFICER

- *Full time versus part time*
- *Non-emotional*
- *Flexing shifts*
- *Training*
- *Expert witness*

UNDERCOVER OPERATIONS

- *U/C Identity*
- *U/C History*
- *U/C Credit Card*
- *U/C Checking Account*
- *U/C Address*

UNDERCOVER ACCOUNTS

- *U/C account with a commercial gateway or service provider*
- *U/C E-mail or Hotmail accounts*

CASE MANAGEMENT

UNDERCOVER OPERATIONS

- *NEVER CONDUCTED FROM HOME*
- *Never ask for photos*
- *Never upload anything*
- *Assume a child's screen name, profile and identity*
- *Let the suspect lead the conversation(s)*
- *"You" always pick the meeting place*

ENTRAPMENT ??

THE ENTRAPMENT DEFENSE

- *The government cannot "originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act and then induce the commission of the crime so that the government may then prosecute"*
- *Jacobson vs. United States*

COMBATTING ENTRAPMENT

- *PREDISPOSITION*
- *What chatroom was the suspect in?*
- *Did the suspect approach you?*
- *Who started talking about sex?*
- *Whose idea was it to send you the photos or pornography?*
- *Whose idea was it to meet?*
- *Did the suspect know what he was doing was wrong?*

UNDERCOVER CONVERSATIONS

- *Ask the suspect :*
- *What do you mean by that ?*
- *Will it hurt me ?*
- *What is that ?*
- *I'm only twelve ?*
- *Is that ok to do ?*
- *Do other kids do that ?*
- *NO PHONE SEX*
- *Lying ????????*

UNDERCOVER DOCUMENTATION

- *Identify start and conclusion of all the conversations*
- *Log all conversations*
- *Screen capture all downloads*
- *Log all downloaded materials*
- *Downloaded photos of the offender*
- *Neo Trace the IP*
- *Identify the offender's telephone number or address*

CONDUCTING OPERATIONS

- *Assume U/C role*
- *Control tactics*
- *Activity documentation*
- *Suspect identification*
- *Surveillance*
- *Crime?*
- *Arrest*
- *Suspect interrogation*

INTERROGATING THE ONLINE SUSPECT

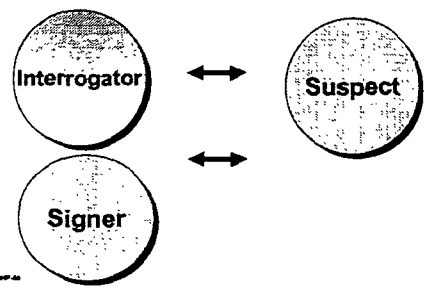
MIRANDA

- *Custody vs. non-custody*
- *Does the offender understand the Miranda warnings?*
- *Rights card vs. rights waiver form*
- *Given: field vs. station?*

What did I do wrong ?

Defense Motions

USING A SIGNER



CUSTODIAL INTERROGATION (MIRANDA) WARNING

After each part of the following warning, the officer must determine whether the suspect understands what he is being told.

1. You have a right to remain silent. You do not have to talk to me unless you want to do so.

2. If you do want to talk to me, I must advise you that whatever you say can and will be used as evidence against you in court.

3. You have a right to consult with a lawyer and to have a lawyer present with you while you are being questioned.

4. If you want a lawyer but are unable to pay for one, a lawyer will be appointed to represent you free of any cost to you.

5. Knowing these rights, do you want to talk to me without having a lawyer present? You may stop talking to me at any time and you may also demand a lawyer at any time.

PCO-EDP-RMF-47

TALKING TO THE SUSPECT

- *Will they talk?*
- *Good guy vs. bad guy?*
- *Police station*
- *Offender's home*

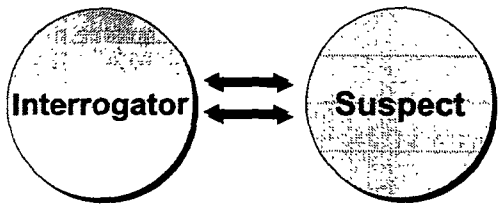
PCO-EDP-RMF-48

INTERVIEW SETTING POLICE STATION

- *Neutral setting and privacy*
- *No interruptions or distractions*
- *Two seats - one on one*
- *Offender's seat placed against the wall*
- *No smoking*

PCO-EDP-RMF-49

ONE ON ONE



INTERVIEW SETTING OFFENDER'S HOME

- *Check for weapons*
- *Consent to search*
- *Search warrant - victim or expert*
- *Privacy*
- *Identify offender's favorite seat*
- *Ask the offender for help to locate evidence*

CONSENT -TO - SEARCH FORMS FOR ONLINE INVESTIGATION see the Appendix

CONSENT TO SEARCH

I, ______________ have been informed of my constitutional right not to have a search made of the premises and/or automobile owned by me and/or under my care identified below without a search warrant. However, knowing my rights to refuse consent to such a search, I hereby authorize ______________ and ______________ of the Cook County Sheriff's Police Dept. Child Exploitation Unit to conduct a complete search of the premises, garage, storage shed or any structure at the property commonly known as ______________

and/or ______________ automobile, license ______

These officers are authorized by me to take from any premises and/or property and view any videos, photos, magazines, computer, computer data or any materials which are evidence in the nature of child abuse or child erotica. This written permission is given by me to the above named persons voluntarily and without any threats or promises of any kind, at ______ M on this ______ day of ______________, 19 ____. I fully understand that I will be given a receipt for property taken.

Signed ______________

Name ______________

WITNESSES

Signed ______________ ______________

Name ______________ ______________

PCO-EXP-RHP-42

COOK COUNTY SHERIFF'S POLICE DEPARTMENT

Authorization for Release of Medical or Confidential Information

[illegible]

PCO-EXP-RHP-43

TYPE OF CONFRONTATIONS

- *Questioning*
- *Interviewing*
- *Interrogating*

PCO-EXP-RHP-44

INTERVIEWING

- *Obtaining information from a reluctant or hostile suspect*
- *Last 5 - 10 minutes*
- *Notes may be taken*
- *Suspect may provide an explanation*
- *Can be conducted before the interrogation*
- *Will lock in the offender's statement*

INTERROGATING

- *Systematic questioning of a person in custody who can request an attorney at any time*
- *Accusatory by nature*
- *Not limited by time*
- *Ideally is a one time situation*
- *No notes are taken*
- *You must minimize moral support*

INTERROGATOR CHARACTERISTICS

- *Sympathetic*
- *Patient*
- *Good bluffer*
- *Understanding*
- *Non-judgmental*
- *Professional*

INTERROGATION GOALS

- *Manipulate the suspect to cooperate with the interrogator*
- *Force them to tell the truth*
- *Which is against their own self interest*
- *Meeting all legal requirements*

POLICE INTERROGATION CONSIDERATIONS

- *No badge, gun, handcuffs or pager*
- *Sit upright - no standing*
- *Open appearance*
- *Confident attitude and voice*
- *Dominate the majority of conversation*
- *"Father Farley"*

BACKGROUND CHECK ON THE OFFENDER

- *Criminal*
- *Juvenile court*
- *Civil court*
- *Child protection agency records*
- *Out of area or state*
- *Are there children in the home?*

THE PRE-INTERROGATION INTERVIEW

- *Introductions*
- *Establish who is in charge*
- *Evaluate offender's medical, physical and emotional condition*
- *Rapport building*

BEGINNING THE INTERVIEW

- *Constitutional rights*
- *Determine offender's intelligence*
- *Start with non-accusatory questioning*
- *State the allegation of crime*
- *Determine the level of offender's understanding*
- *Let the offender sit for a while*

INTERROGATION STRATEGY

- *Convince the offender that their guilt is known*
- *Guilt can be established*
- *Point out symptoms of guilt, futility to resist*
- *Not a bad person?*
- *Conduct not really planned*
- *Victim not really hurt*

TALKING ABOUT THE CRIME

- *Curious*
- *Accident*
- *Attempted to delete*

OFFENDER'S REACTION

- *If not you, then who?*
- *Fears about admission*
- *No secrets or promises*
- *Corroboration of physical evidence*

SAMPLE PHYSICAL EVIDENCE FOUND AT THE TIME OF THE ARREST

ONLINE "STING" CASE ILLUSTRATION

IP IDENTIFICATION OF SUSPECT AND NEO TRACE OF IP BY U/C OFFICER

ADMISSION

- *Allow offender to tell their story*
- *Identify any victim(s) and the age(s)*
- *Identify special names for the abuse*
- *Identify physical evidence and sources*
- *Statement*

TYPES OF STATEMENTS

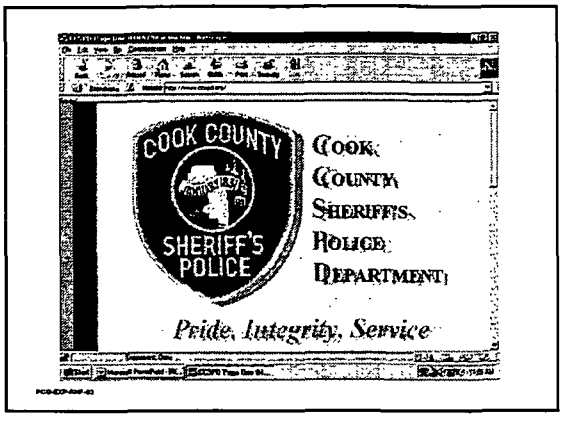
- *Recall vs. question and answer*
- *Handwritten*
- *Handwritten CCSPD form*
- *Typed or transcribed by court reporter*
- *Audio tape or video tape*
- *Freehand drawings*

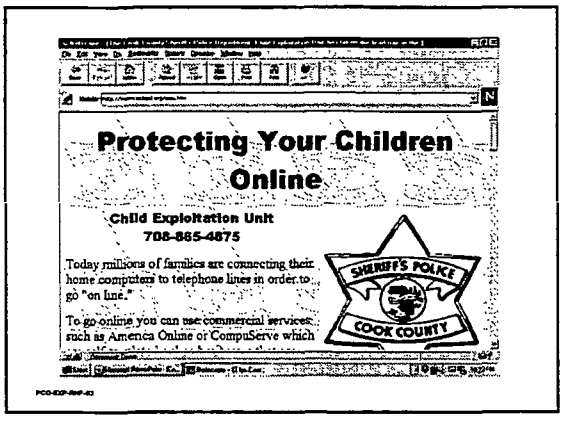
STATEMENT CONSIDERATIONS

- *Miranda warning was waived?*
- *Identify start and conclusion of interview*
- *Offender knew the age of the child?*
- *Offender knew that a crime had been committed?*
- *Specific circumstances of the conversations*
- *Offender had something to eat and drink?*
- *No promises or threats*
- *Offender given an opportunity to "say something"*

CLOSING THE INTERROGATION

- *Review the statement with the offender*
- *Are there other victims?*
- *Don't condemn the offender*
- *Don't make any promises*
- *Shake hands*
- *Take a "relaxed" photo of the offender*





www.ccspd.org

Thank you !

Detective Robert Hugh Farley
Commanding Officer
Child Exploitation Unit
Cook County Sheriff's P.D.
1401 South Maybrook Drive
Maywood, Illinois 60153
708-865-4875
FAX 708-865-4818
rhfarley@hotmail.com

Appendix

Consent Forms

Appendix III

CONSENT TO SEARCH

I, _____ have been informed of my constitutional right not to have a search made of the premises and/or automobile owned by me and/or under my care identified below without a search warrant. However, knowing my rights to refuse consent to such a search, I hereby authorize _____ and _____ of the Cook County Sheriff's Police Dept. Child Exploitation Unit or their agents to conduct a complete search of the premises, garage, storage shed or any structure at the property commonly known as_____

_____

and/or _____ automobile, license _____.
Year and Type of automobile

These officers are authorized by me to take from my premises and/or property and view any videos, photos, magazines, computer, computer discs or any materials which are evidence in the nature of child abuse or child erotica. This written permission is given by me to the above named persons voluntarily and without any threats or promises of any kind, at _____ _____ M on this _____ day of _____, 19 _____. I fully understand that I will be given a receipt for property taken. Signed _____

Name _____

WITNESSES:

Signed _____ _____

Name _____ _____
Printed Printed

Appendix IV

CONSENT TO SEARCH

I, _____ have been informed of my constitutional right not to have a search made of the computer system (s) owned by me and / or under my care identified below without a search warrant. However, knowing my rights to refuse consent to such a search, I hereby authorize _____ and _____ of the Cook County Sheriff's Police Dept. Child Exploitation Unit or their agents to conduct a complete search of my computer system

_____ _____
Brand of Computer Model

_____ _____
Serial Number

These officers are also authorized by me to take from my premises and/or property and review my computer, computer discs, hardware or software for any evidence in the nature of child abuse, child exploitation or child erotica. This written permission is given by me to the above named persons voluntarily and without any threats or promises of any kind, at _____ _____ M on this _____ day of _____, 19 _____. I fully understand that I will be given a receipt for property taken.

Signed _____

Name _____

WITNESSES:

Signed _____ _____

Name _____ _____
Printed Printed

Appendix V

CONSENT TO SEARCH

I, _____ have been informed of my constitutional right not to have a search made of online accounts owned by me and/or under my care identified below without a search warrant. However, knowing my rights to refuse consent to such a search, I hereby authorize _____ and _____ of the Cook County Sheriff's Police Dept. Child Exploitation Unit or their agents to conduct a complete search and review of the following online accounts: _____

_____

_____

These officers are authorized by me to review my accounts online looking for any evidence in the nature of child abuse, child exploitation or child erotica. This written permission is given by me to the above named persons voluntarily and without any threats or promises of any kind, at _____ _____ M on this _____ day of _____, 19 _____. I fully understand that I will be given a receipt for property taken.

Signed _____

Name _____
Printed

WITNESSES:

Signed _____ _____

Name _____ _____
Printed Printed

Authorization for Release of Medical or Confidential Information

I, _____ do hereby authorize

_____
Facility, Agency, Therapist, Etc.

_____ _____
Address City

to release _____
Specific Nature of Information to be Disclosed

for the investigation of _____ _____
Type of Police Investigation Police Report Number

about _____ _____
Name of Patient Date of Birth

to Detective _____ of the Cook County Sheriff's Police Department , **Child Exploitation Unit**, 708-865-4875 or FAX 708-865-4818.

I understand fully the nature of this authorization and further that the above named Detective has the right to view, inspect, copy or xerox any information to be disclosed.

_____ _____
Signature of Patient or Guardian Signature of Witness

_____ _____
Name Printed Name Printed

_____ _____
Date Date

Seizure Forms

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

The People of the State of Illinois)
Plaintiff)
)
v.)
)
_____)
Defendant

ORDER TO CONFISCATE AND DESTROY

This cause coming before the Court for a hearing on a Motion by the People of the State of Illinois, by and through it's attorneys, Richard A. Devine and the _____ District States Attorney's Office in the above-entitled action, supported by the testimonial evidence of the Complainants, for leave to file a Petition to Confiscate and Destroy, and this Court having heard arguments of counsel and being now in all respects, fully advised in the premises, and it appearing in this court that the use of the seized property was for an illegal purpose, in violation of Illinois Compiled Statutes, Section _____ to wit: _____

It is hereby Ordered and Decreed that the said property identified under Cook County Sheriff's Police Case Report # _____, to wit:

Inventory #	Description
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

shall be forfeited to the Cook County Sheriff's Police Department, Child Exploitation Unit and shall, thereupon, become the property of the Cook County Sheriff's Police Department to be destroyed or otherwise used in the exercise of its official discretion.

Richard A. Devine, States Attorney for Cook County by

ASA _____ District _____

ENTER:

_____ _____
Judge Judge's Number Date

Statement Forms

Appendix X

Cook County Sheriff's Police Department

Case Report # _____

CEU # _____

Voluntary Written Statement

Page One of _____ Pages

Location of Statement _____

Date _____

Time of Statement _____

Officer Taking Statement _____

Witness _____

Person Making the Statement _____

I have been advised that I have the following rights under the United States Constitution that the Officers will respect:

1 I may remain silent and not make any statement or answer any questions that are directed to me._____

2 If I do make a statement or answer any questions, I realize that the statement, questions and my answers may be used against me in a criminal trial._____

3 I have the right to the presence of an attorney of my choice and further have the right to talk with my attorney prior to any questioning, during any questioning or while making this statement._____

4 If I cannot afford an attorney one will be provided for me at public expense. If I request an attorney the police will not question me or take a statement until my attorney talks with me._____

5. I may refuse to answer any questions, make a statement or may request an attorney at any time. After having waived my rights and commenced making this statement I can stop at any time and talk with my attorney or may request an attorney be provided for me at public expense._____

After having been advised of these rights, I hereby waive all these rights and make the following voluntary statement:

_____

Signature of Person Making this Statement

_____ _____

Signature of Officer Reading Rights Signature of Officer Witnessing Rights

Appendix XI

Cook County Sheriff's Police Department

Case Report # _____
CEU # _____

Voluntary Written Statement

Page _____ of _____ Pages

Voluntary Statement of _____Continued

_____
Signature of Person Making this Statement

Appendix XII

Cook County Sheriff's Police Department

Case Report # _____
CEU # _____

Voluntary Written Statement

Page _____ of _____ Pages

Voluntary Statement of _____Continued

_____
Signature of Person Making this Statement.

Appendix XIII

Cook County Sheriff's Police Department

Case Report # _____
CEU # _____

Voluntary Written Statement

This _____ page statement has been read to me by _____ _____ as I have read along. I totally understand the contents of this statement. I am signing this statement voluntarily of my own free will and have received no threats, rewards nor have any promises been made to me.

_____
Signature of Person Making this Statement

_____
Name Printed

_____
Signature of Officer Taking this Statement

_____
Name Printed

_____
Signature of Officer Witnessing this Statement

_____
Name Printed

Selected Readings

Appendix C: "Drawing Interviews": An Alternative Technique

"Drawing Interviews": An Alternative Technique

By Robert Hugh Farley

In our first child abuse case, over 11 years ago, my partner and I were assigned to investigate the apparent physical abuse of a 5-year-old boy. During our short interview with the victim, we learned that he had been caught playing with matches and was subsequently punished by his mother's boyfriend, who placed the boy's hand on the open flame from a gas stove.

At the conclusion of the interview the boy was transported to the hospital, where he was treated for the burn before being turned over to a protective service worker from the Illinois Department of Children and Family Services.

On the way from the hospital to the Protective Service Office, the worker and the boy stopped at a restaurant for a hamburger. While he was eating, the 5-year-old boy told the worker the hamburger smelled funny—"like my mom's [vagina]." The worker rushed the boy back to the police station, where we finally conducted a lengthy interview. From this interview, it was learned that the victim had been subjected to extensive sexual abuse not only from his mother, but also from the mother's boyfriend. If not for his spontaneous announcement, however, the sexual abuse would have gone undetected, and the court would have returned the boy to the mother.

This incident demonstrated plainly that "simple" cases of physical child abuse are rare. We had thought that, once established from the victim, the interview could be concluded. But experience shows that in all child abuse investigations, a detailed, lengthy, and very sensitive interview of the victim is critical.

In recent years, extensive publicity has been given to the use of anatomically correct dolls for the interviewing of sexually abused children. While it is true that many clinical professionals have had very good results with these dolls, unfortunately, it is also true that a significant number of youth officers across the country have been expected to use the dolls in child abuse interviews despite a lack of training in their proper use.

Drawing Pictures

An excellent alternative for a police officer to use—either in conjunction with or instead of the dolls—is to have the child draw his own pictures. In many cases, using the child's own "drawings," rather than anatomically correct dolls, will provide a more productive interview with the child abuse victim.

Prior to starting the child abuse "drawing interview," the police officer should learn as much as he can about the case. It should be determined when the child last ate or if he is hungry. The interview should never be conducted during the child's regular nap time or when he normally goes to bed for the night.

When starting a child abuse interview, the police officer must first address the victim's fear of retaliation for revealing the circumstances of the abuse or identifying the abuser. This initial action is very difficult for both the victim and the interviewer, since a police officer represents a threat in the sense that he can arrest the abuser.

The interviewing officer should furnish the child abuse victim with a box of crayons, pencils, and several sheets of paper at the start of the interview. If he presents himself to the child as a warm and caring person, the child may think that the drawings are a game, not even realizing that he is being interviewed.

The "drawing interview" should begin with the interviewer asking the victim to write or print his name on a sheet of paper that, depending on the victim's age, is either lined or unlined and colored. This step of the interview will provide the police officer with some idea of the educational and developmental stage of the victim.

The second step is to ask the child to draw a "picture of himself." The child may object at this point, telling the interviewer that he can't draw very well, but he should simply be encouraged to do the best he can.

When the child has finished the drawing, the interviewer can use it to go over the child's name and the locations for the different body parts. The interviewer should begin this portion of the interview by asking the child the color of the hair on the drawing and locations of the eyes, the mouth, belly button, etc. The last questions asked should be the locations and names of the sexual body parts. In some cases, the interviewer may wish to have the child label the body part locations on the drawing.

If the drawing the child has done of himself portrays an unhappy face or scene, the interviewer should then ask, "She doesn't look happy; why is that?"

In the third step, the child is provided with another sheet of paper and asked to "draw a picture of his family." This step is very important as it may provide the interviewer with important information concerning an outsider such as a boyfriend, grandfather, etc., who is living in the family residence or has daily access to the family.

When the family drawing is completed, the child is asked to label all the people in the drawing, including the family pet. The interviewer can then ask such questions as where the various people sleep in the house, which person the child likes the least or the best, etc.

For the final step of the drawing interview, the child is provided with another sheet of paper and asked to "draw what happened." When the drawing is completed, the child is asked to explain the circumstances of the abuse portrayed in the picture. He is asked to label the name of the abuser and the victim and, in cases of physical abuse, asked to identify the instrument of abuse and where it is stored.

As the child completes each drawing, the interviewer must take the time to go over it in detail with the child. If the interviewer observes some portion of the drawing that is unusual, exaggerated or overemphasized, such as the mouth in figure 1, he should ask the child for an explanation rather than making assumptions of any kind.

Of course, the police officer/interviewer, who is typically untrained in art therapy, must remember not to fall into the trap of playing amateur psychologist and attempt to analyze the drawings himself. This job must be left to the professional art therapist.

Conclusions

"Drawing interviews" offer some advantages that the anatomical dolls do not:

- They allow an abused child to express graphically what he may be afraid or unable to express verbally.
- They decrease the child's anxieties during the interview by providing him with a motor activity.
- Drawings of "what happened" will provide written evidence of what actually happened to the child. The drawings may also allow the resurfacing of repressed feelings or facts that normally would not be uncovered in another type of interview.
- Drawings will provide "hard physical evidence" of what the child has related to the police investigator during the interview, making it easier for a police officer on the witness stand to explain the child's version of what happened.
- The paper, pencils, and crayons used in the drawings, if not readily available, can be carried easily by a police officer.

In conclusion, the police officer must remember that the child who has been sexually or physically abused has also been emotionally abused. The "drawing interview" can be conducted in such a manner that it is nonthreatening, nonaccusatory, and, hopefully, nonharmful to an already scarred child.

Figure 1: "Draw Yourself"

This drawing was done by a 14-year-old boy who had been anally and orally sodomized by his stepfather for over 6 years. When the picture was first drawn, there were no arms. When the boy was later questioned by the interviewer about the missing arms, he advised that he had forgotten to put them in, and the arms were then added to the drawing. When questioned about the object depicted in his mouth, the boy said it was a "wanger." Further questioning established that a "wanger" was the stepfather's penis.

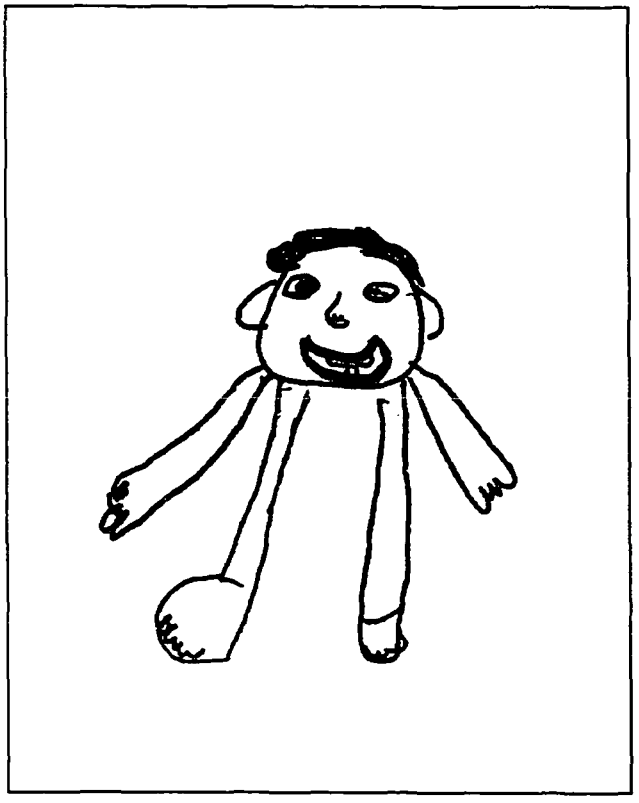


Figure 2: "Draw Your Family"

The purpose of this drawing, done by a 10-year-old-girl, was to identify the other members of the family unit. The girl depicted two "friends" between Mom and Step Dad. When later questioned by the interviewer, the girl advised that "those are Mom's two boyfriends, who visit the house when Step Dad is out driving his truck on the road."

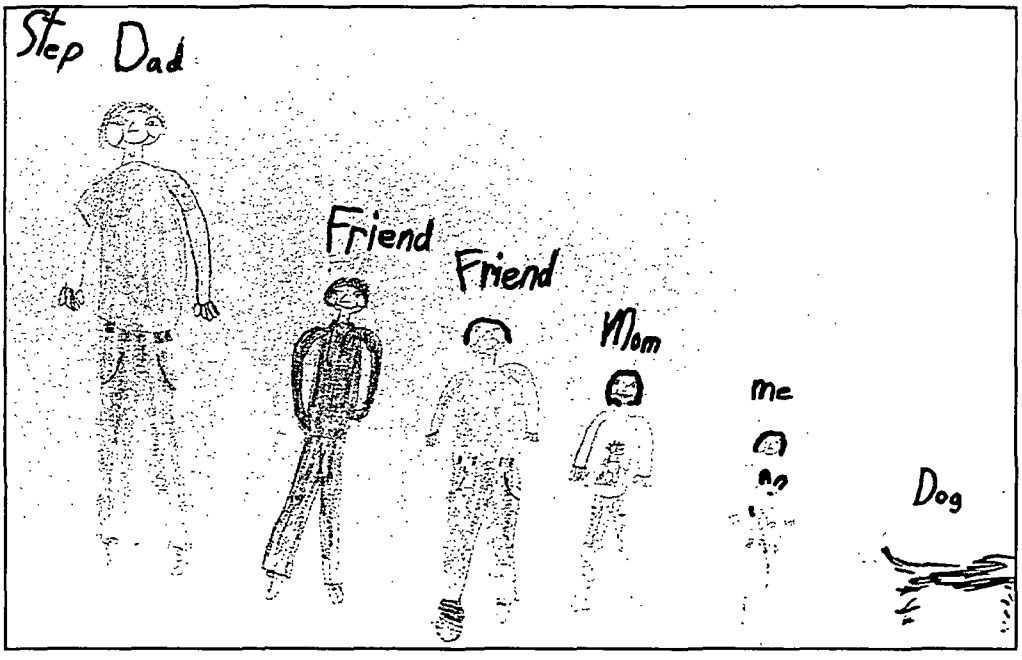
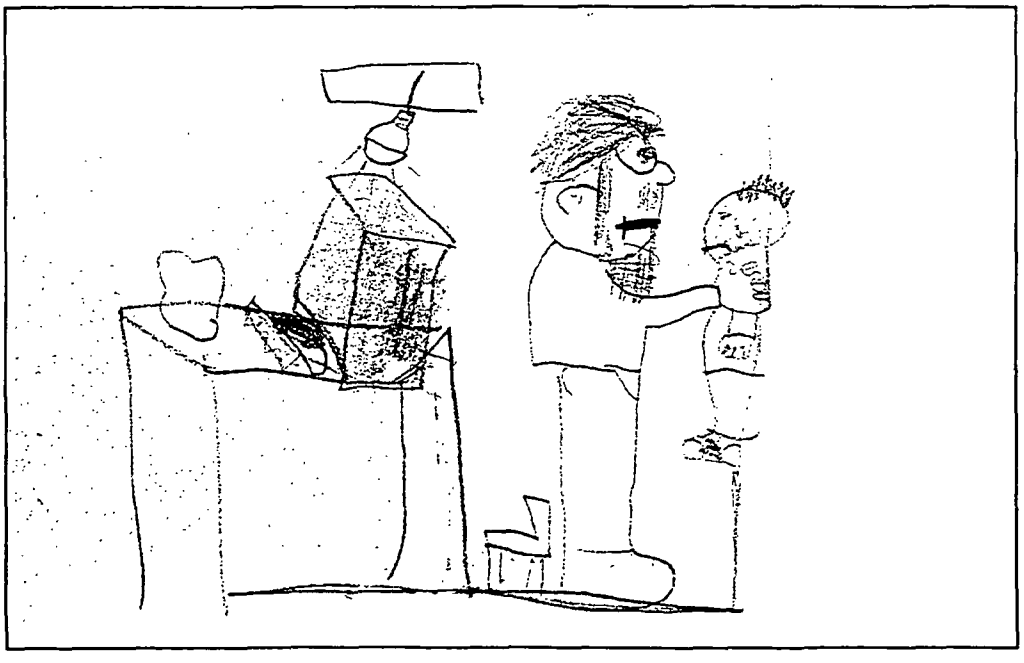


Figure 3: "Draw What Happened"

This drawing was done by an 8-year-old boy who has suffered a history of physical abuse from his stepfather. In this drawing, the boy had knocked over a bag of feed in the basement of the family home. The boy's 6'5" stepfather grabbed him by the neck and, while holding him in the air, choked the breath out of him. Going over the drawing with the interviewer, the boy explained that the shading on his face was when he had turned red and the tear was when he was crying. Note the heavy black line depicting the anger on the stepfather's face. Although the incident had been witnessed by the boy's uncle, the boy later recanted his testimony under pressure from his mother.



U.S. Department of Justice
Office of Justice Programs
Office of Juvenile Justice and Delinquency Prevention

Understanding and Investigating Child Sexual Exploitation

Portable Guides to Investigating Child Abuse

Overview

The sexual victimization of children ranges from one-on-one intrafamilial (within the family) abuse to multioffender/multivictim extrafamilial (outside the family) sex rings and from stranger abduction of toddlers to prostitution of teenagers. As used in this guide, the sexual exploitation of children refers to forms of victimization involving pornography, sex rings, or prostitution.

Although a variety of individuals sexually victimize children, preferential sex offenders are the primary sexual exploiters of children. They are serial offenders who prey on children through the operation of child sex rings and/or the collection, creation, or distribution of child pornography. The term "preferential sex offender" is a descriptive label used only to identify, for investigative purposes, a certain type of offender. The potential significance of this identification will be discussed. The commonly used term "pedophile" has not been used here to refer to these offenders, in order to avoid confusion over whether investigators are qualified to apply what is also a mental health or diagnostic term.

Apart from legally defined child prostitution (a significant form of child exploitation that will not be discussed here), the sexual exploitation of children does not necessarily involve commercial or monetary gain. In fact, in the United States, child pornography and child sex rings most often result in a net financial loss for the offender. Cases of sexual exploitation of children may involve intrafamilial offenders and victims, although this is not typical.

Child Sex Rings

The term "child sex ring" has no legal definition. For many it conjures up images of the buying and selling of children as sexual slaves. However, this term is used simply to describe the dynamics of one or more adult offenders who are sexually involved with two or more child victims during the same general time frame. The behavior pattern of such offenders is predatory, prolific, and serial: They usually recruit, seduce, molest, and "dump" numerous child victims repeatedly over many years.

In general, a child is defined as someone who has not yet reached his or her 18th birthday. However, legal definitions of who is considered a child and to what extent consent is an issue vary from case to case, from statute to statute, and from State to State and must be considered in any criminal investigation. Unlike one-on-one intrafamilial sexual abuse, in which the victim is most often a young female, in child sex rings the victim is frequently a boy between the ages of 10 and 16.[1]

A child sex ring need not and usually does not involve any moneymaking element. When something of monetary value is exchanged, it is usually given by the offender to the victim as part of the seduction or "grooming" process. A child sex ring can involve a daycare center, a school, a scout troop, a Little League team, and neighborhood or runaway children. It can also involve intrafamilial molestation of children, including the use of marriage or a live-in relationship as a method of access to children and the use of family children to attract other victims.

[1]It is possible for girls to be victims in child pornography and sex rings and for women to be sex offenders. In this guide, for simplicity's sake, the male pronoun has been used to refer to both victims and offenders.

However, the dynamics of child sex ring cases are different from those of the more commonly investigated cases of one-on-one intrafamilial sexual abuse. Child sex rings are more likely to involve interaction among the multiple victims. These interactions—both before and after discovery—must be examined and evaluated. Possible child victims in sex ring cases are more often interviewed as a result of discovery (e.g., identification in recovered pornography) or suspicion (e.g., a known offender had access to them) than as a result of voluntary disclosure by the victim.

Although parents are usually not the abusers in sex ring cases, they cannot be ignored in the investigation. Their interaction with their victimized children can be crucial to the case. If the parents interrogate their children or conduct their own investigation, the results can be damaging to the case. Investigators must maintain ongoing communication with the parents of victims and attempt to channel their energy and concern in positive ways.

Child Pornography

The legal definition of the term "child pornography" varies from State to State and under Federal law. Under most legal definitions, child pornography involves a visual depiction of a child that is sexually explicit. The Federal child pornography law defines a child (minor) as someone who has not yet reached his or her 18th birthday. Under the Child Pornography Prevention Act of 1996, the Federal definition of "child pornography" has been expanded to include not only a sexually explicit visual depiction using a minor, but also any visual depiction that "has been created, adapted, or modified to *appear* [emphasis added] that an identifiable minor is engaging in sexually explicit conduct." Although this new law makes the prosecution of cases involving manipulated computer images easier, it also means that it is no longer possible in every case to argue that child pornography is the permanent record of the abuse or exploitation of an actual child.

According to Federal law, sexually explicit conduct means actual or simulated sexual intercourse (including vaginal, oral, and anal), bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area. In some cases, the child may not need to be naked in order for the depiction to be covered by this definition. It is important to understand that the lasciviousness often mentioned in child pornography cases is *not* in the child's mind or even necessarily the photographer's, but in the mind of each producer, distributor, and collector of the material.

Some grossly explicit visual depictions of children clearly and obviously are always child pornography, and some visual depictions of children, no matter the context or use, do not meet the minimum legal threshold and are never child pornography. Often investigators and prosecutors want to make a decision about the nature of a visual depiction of a child based only on looking at it. The difference between simple nudity (e.g., innocent family photographs, works of art, or medical illustrations) and the lascivious exhibition of the genitals is often not in the visual depiction itself, but in the context. Many visual depictions of children may or may not be considered child pornography, depending on how they were produced (abuse, deception, trickery), saved (location, labels, packaging, modifications, computer file name), or used (to lower inhibitions of or arouse victims, to pander, to trade, to sell). Assuming it meets the minimum legal criteria, potential child pornography must always be evaluated in the total context in which it is discovered, and it must be objectively investigated.

Not all collectors of child pornography physically molest children, and not all molesters of children collect child pornography. Not all children depicted in child pornography have been sexually abused. For example, some have been photographed without their knowledge while undressing, others manipulated into posing nude. Depending on the use of the material, however, all can be considered exploited. For this reason, even those who "only" receive or collect child pornography produced by others play a role in the sexual exploitation of children, even if they have not physically molested a child.

Offenders

Preferential sex offenders tend to be predatory serial offenders.[2] Because operating a child sex ring or trafficking in child pornography usually requires above-average interpersonal skills and economic means, these offenders will generally be from a higher socioeconomic background. Preferential sex offenders may be "pillars of the community" and are often described as "nice guys." They almost always have a means of access to children (for example, through marriage, neighborhood, or occupation). Determining their means of access helps to identify potential victims. Investigators should always verify the credentials of those who attempt to justify their acts as part of some "professional" activity. Just because an individual is a doctor, priest, minister, or therapist, for example, does not mean that he cannot also be a child molester.

Characteristics of Preferential Sex Offenders

A preferential sex offender can usually be identified by the following interrelated behaviors:

- **Long-term and persistent patterns of behavior.**
  - Begins pattern in early adolescence.
  - Is willing to commit time, money, and energy.
  - Commits multiple offenses.
  - Makes ritual or need-driven mistakes.
- **Specific sexual interests.**
  - Manifests paraphiliac preferences (see next section), possibly more than one type.
  - Focuses on defined sexual interests and victim characteristics.
  - Centers life around preferences.
  - Rationalizes sexual interests.

---

[2]**Note:** The category of predatory serial sex offenders includes other types of offenders, such as those who use intimidation and force to engage in sexually motivated child abduction. A discussion of these other types of offenders is beyond the scope of this guide.

- **Well-developed techniques.**
  - Evaluates experiences.
  - Lies and manipulates, often skillfully.
  - Has method of access to victims.
  - Is quick to use modern technology (e.g., computer, VCR) for sexual needs and purposes.
- **Fantasy-driven behavior.**
  - Collects pornography.
  - Collects paraphernalia, souvenirs, videotapes.
  - Records fantasies.
  - Acts to turn fantasy into reality.

Because these sexual behavior patterns are highly predictable, it is important for investigators to recognize and utilize them, if present. If the investigation identifies enough of these characteristics, many of the remaining ones can be assumed. Most of these indicators mean little by themselves, but as they are identified and accumulated through the investigation, they can constitute reason to believe a suspect is a preferential sex offender.

Paraphilias and Sexual Ritual Behavior

Paraphilias are psychosexual disorders defined by the *Diagnostic and Statistical Manual of Mental Disorders, 4th edition* (DSM–IV, Washington, DC: American Psychiatric Association, 1994) as recurrent, intense sexually arousing fantasies, sexual urges, or behaviors that generally involve (1) nonhuman objects, (2) the suffering or humiliation of oneself or one's partner, or (3) children or other nonconsenting persons, and that occur over a period of at least 6 months. Pedophilia, sadism, voyeurism, and fetishism are examples of paraphilias.

On an investigative level, the presence of paraphilias often means highly repetitive and predictable behavior focused on specific sexual interests that goes well beyond a "method of operation" (MO). The concept of an MO—something done by an offender because it works and will help him get away with the crime—is well known to most investigators. An MO is fueled by thought and deliberation. Most offenders change and improve their MO over time and with experience.

The repetitive behavior patterns of preferential sex offenders involve some MO, but are more likely also to involve the less-known concept of sexual ritual. Sexual ritual is the repeated engaging in an act or series of acts in a certain manner because of a sexual need; that is, in order to become aroused and/or gratified, a person must engage in the act in a certain way. Other types of ritual behavior can be motivated by psychological, cultural, or spiritual needs. Unlike an MO, ritual is necessary to the offender but not to the successful commission of the crime. In fact, instead of facilitating the crime, ritual often increases the odds of identification, apprehension, and conviction because it causes the offender to make need-driven mistakes.

Ritual and its resultant behavior are fueled by erotic imagery and fantasy and can be bizarre in nature. Most important to investigators, offenders find it difficult to change and modify ritual, even when their experience tells them they should or when they suspect law enforcement scrutiny. Understanding sexual ritual is the key to investigating preferential sex offenders.

Victims

In child pornography and sex ring cases, offenders typically control their victims by seducing them with attention, affection, kindness, and gifts until they have lowered the victims' inhibitions and gained their cooperation and "consent." Because victims of child pornography and sex rings usually have been carefully seduced and often do not realize they are victims, they repeatedly and voluntarily return to the offender. Society and the criminal justice system find this difficult to understand. If victims are molested by a neighbor, teacher, or priest, why do they "allow" it to continue?

The offender may be treating these children better than anyone has ever treated them, and they may not realize they are victims until the offender pushes them out of the ring. Then they see that all the attention, affection, and gifts were just part of a master plan to use and exploit them. This may be psychologically harmful for a troubled child who has had a traumatic life.

Officers investigating child sex rings and child pornography cases must remember that children are human beings with human needs, not "innocent angels sent from heaven." Many children, especially those victimized through the seduction process, often:

- Trade sex for attention, affection, or gifts.
- Are confused about their sexuality and feelings.
- Are embarrassed and guilt ridden about their activity.
- Describe victimization in socially acceptable ways.
- Minimize their responsibility and maximize the offender's.
- Deny or exaggerate their victimization.

These things do not mean that the child is not a victim. The activity is not the fault of the child, even if he:

- Did not say no.
- Did not fight.
- Actively cooperated.
- Initiated the contact.
- Did not tell.
- Enjoyed the sexual activity.
- Accepted gifts or money.

Dynamics of Child Sex Rings

The operation of a child sex ring is like a pipeline. At any given moment, there are victims being recruited, victims being seduced, victims being molested, and victims being let go, or "dumped." For most preferential sex offenders, it is easy to recruit, seduce, and molest the victims. Offenders have the most difficulty in ending the relationship without causing their victims to turn against them and disclose the abuse.

Controlling the Victims

Once victims are in the pipeline, offenders control them through a combination of bonding, competition, and peer pressure. Most children, especially adolescents, want to be a part of some peer group. Any offender operating a sex ring has to find a way to bind the victims together. Some offenders use an existing

structure such as a scout troop, a sports team, or a school club. Others create their own group, such as a magic club, computer club, or religious cult. Some offenders just make up a name—for example, the "88 Club" or the "Winged Serpents"—and establish their own rules and regulations.

Offenders are most likely to use violence, threats of violence, and blackmail when pushing a victim out of the group or when attempting to hold on to a still-desirable victim who wants to leave. Sexually explicit notes, audiotapes, videotapes, and photographs effectively ensure a victim's silence. Victims worried about disclosure of illegal acts such as substance abuse, joyriding, petty theft, and vandalism are also subject to blackmail.

Many victims, however, are most concerned over (and therefore more likely to deny) disclosure of engaging in:

- Sex for money.
- Bizarre sex acts.
- Homosexual acts in which they were the active participant.
- Sex with other victims.

In child sex rings, not only does the offender have sex with the children but, in some cases, the children have sex with each other. While children may admit that they were forced by the offender to perform certain acts with him, they find it hard to explain sexual experiences with other children and frequently deny such activity. One offender stated that if you select and seduce your victims properly, getting them to keep the secret takes care of itself.

The Offender-Victim Bond

Because of their bond with the offender, victims frequently resent law enforcement intervention and may even warn the offender. Even the occasional victim who comes forward and discloses the abuse may feel guilty and then warn the offender. The offender may also continue to manipulate the victims after the investigation has begun—for example, by appealing to their sympathy or by making a feeble attempt at suicide to make them feel guilty or disloyal. Some offenders may threaten victims with physical harm or with disclosure of the blackmail material; some may bribe the victims and their families.

A particular aspect of the offender-victim bond is especially troubling for the criminal justice system. Some victims, when being pushed out or while still in the pipeline, may assist the offender in obtaining new victims. They become the bait to lure other victims. Such recruiters or "graduate" victims can and should be considered subjects of investigation. Their offenses, however, should be viewed in the context of their victimization and the dynamics of child sex rings.

Coordinating the Investigation

The investigation of sexual exploitation cases involving multiple victims molested by preferential offenders is usually complex and difficult, not only because of the amount of work involved, but also because of intense pressure from the media and the community to resolve the investigation quickly. To bring the investigation to a successful conclusion, law enforcement should work with the prosecutor, child protective services, and medical and mental health personnel in a **multidisciplinary team (MDT)**. If a protocol for MDT investigations has not been previously developed, the first step is for the team members to meet together to decide the following:

- Which agency will take the lead in the investigation, and who will be in charge?
- What office space will be utilized in order for the team to work together?
- Which agency will provide the clerical help for the team?
- Which agency will author all of the investigation reports that the team develops?
- Which agency will handle the telephone calls from the victims' parents, and who will serve as liaison with them?
- Where and when will the interviews of the victims take place, and who will conduct the interviews?
- Who will do the medical examinations of the victims and where will they be conducted?
- Will the victims be taken into protective custody and, if so, where will they be placed?
- Which agency will handle the press and the media?
- Which agency will handle the telephone calls from the community?

The agencies involved in the investigation should coordinate their needs and paperwork so that only one MDT report will be generated under the byline of one of the participating agencies—for example, the police department. If possible, all the victims should be interviewed at one centrally located, "safe" place such as a children's advocacy center. Every attempt should be made to have the same physician—ideally, a member of the MDT with experience in this type of case—conduct the medical examinations of all of the victims.

Interviewing the Victim

The interview of the "outcry" victim (the first victim to disclose abuse) or, if there is no outcry victim, of the first victim to be discovered, should be completed first. After this child has been interviewed, determine whether any children are living at the offender's residence or are in immediate danger. If a child is at risk, the MDT may need to take the child into protective custody immediately.

When attempting to identify additional victims of a child sex ring, begin with those who are about to leave or have just left the offender's pipeline. The victim most likely to disclose the abuse is one who has just left the ring and who has a sibling or close friend about to enter the ring. The desire to protect younger victims from what he has endured is a victim's strongest motivation for overcoming shame and embarrassment. Some victims are motivated by jealousy to disclose the abuse when they are pushed out of the ring after being replaced by younger victims. The next best candidates for interviewing are victims who have just entered the pipeline.

The victim may have many positive feelings for the offender and may resent law enforcement intervention. Before beginning the interview, take the time to attempt to develop a working relationship with the victim. Investigators should:

- Be able to discuss a wide variety of sexual activity without being judgmental.
- Understand the victim's terminology. Investigators must be familiar with the graphic street jargon used by victims.
- Carefully communicate to the victim that he is not at fault even though he did not say no, did not fight, did not tell, or even enjoyed it.

Investigators who have a stereotyped concept of child sexual abuse victims or who are accustomed to interviewing younger children molested within their family may have a difficult time interviewing adolescents molested in a sex ring, many of whom will be troubled, even delinquent children from broken homes. It may be more difficult to avoid being judgmental with a delinquent adolescent seduced by a "pillar of the community" than with an innocent 8-year-old girl abused by her father. A judgmental attitude can be easily and unknowingly communicated through gestures, facial expressions, and body language and can hinder the investigation. When the victim believes that the investigator understands what he experienced, he is more likely to talk.

Allow the victim to use scenarios to save face when disclosing the victimization. Adolescent boy victims are highly likely to deny certain types of sexual activity. Even if a victim discloses the abuse, the information is likely to be incomplete and may minimize his involvement and acts. Subsequent investigation may uncover evidence that contradicts the victim's sworn statement or additional victims whose stories directly conflict with the first victim's story. The most common example of this is that the victim admits that the offender performed oral-genital sex on him, but denies that he did the same to the offender. The execution of a search warrant then leads to the seizure of photographs of the victim performing oral-genital sex on the offender. Additional victims may also confirm this but vehemently deny that they did the same thing.

Investigators and prosecutors must understand and learn to deal with the incomplete and contradictory statements of victims of child sex rings. The dynamics of their victimization must be considered. They are embarrassed and ashamed of their behavior and rightfully believe that society will not understand their victimization. Many adolescent victims are most concerned about the response of their peers.

If all else fails, the investigator can try the no-nonsense approach. No matter what the investigator does, most adolescent boys will deny they were victims. Therefore, it is important to interview as

many potential victims as legally and ethically possible. It is also possible that some troubled teenagers may exaggerate their victimization or even falsely accuse individuals. Allegations must be objectively investigated and all possibilities considered.

After the interview, the child may feel the need to warn the offender that a child abuse investigation has commenced. Once warned by the victim, the preferential sex offender may attempt to hide or to destroy any evidence of the abuse. For this reason, investigators must be careful about what they disclose to the victims and must be prepared to move quickly with the search and other phases of the investigation.

Investigating the Offender

Preferential sex offenders are like human evidence machines. During their lifetime, they leave behind a string of victims and a collection of child pornography and erotica. This long-term, persistent pattern of behavior makes preferential sex offenders easy to convict if investigators understand how to recognize them and how they operate.

The investigation of the offender should establish:

- Where the offender lives and who lives with the offender.
- When the offender is usually at home.
- Where the offender works.
- Whether the offender does any volunteer work with children.
- Whether the offender has any hobbies or interests that appeal to children.
- The type of vehicle(s) the offender owns or drives and where they are located.
- Whether the offender has access to a computer and, if so, where it is located and whether the offender uses one of the online computer services.
- Whether there are any weapons in the offender's residence.
- Whether the offender has any storage places or safety deposit boxes.

Investigator's Checklist for Interviewing Victims of Preferential Sex Offenders

In interviewing victims, investigators should attempt to obtain information that would provide answers to the following questions:

The Abuse

- ❑ What are the specific circumstances of the abuse?
- ❑ Where did the abuse take place? (Obtain as specific a description as possible, including details about decorations and type of furniture.)
- ❑ When did the last incident of abuse take place?
- ❑ What were the specific dates, time of day, and frequency of the abuse?
- ❑ What was the duration of the abuse (i.e., days, weeks, months, years)?
- ❑ Did the offender use a specific name for the abuse?
- ❑ What specific items (e.g., toys, gifts, clothing) did the offender use to seduce or lure the victim, and where are these items now?
- ❑ Did the offender provide the victim with any drugs or alcohol in order to help him "relax"?

The Offender and the Victim

- ❑ Who is the offender? Were other offenders present at the time of the abuse?
- ❑ Does the offender know the exact age of the victim? If so, how?
- ❑ How can the victim identify the offender?
- ❑ Did the offender make any threats?
- ❑ When did the victim last speak with the offender?
- ❑ When did the victim last see or visit with the offender?

Other Victims

- ❑ Can the victim identify any other victims or possible victims?
- ❑ What witnesses were present at the time of the abuse? Is there anyone else who may have any knowledge of the abuse?

Pornography

- ❑ Did the offender display for the victim any pornographic images (e.g., photographs, magazines, videotapes, computer images)?

Investigator's Checklist for Interviewing Victims of Preferential Sex Offenders *(continued)*

- ❑ Did the victim independently observe any pornographic images of other children (e.g., photographs, videotapes, or computer files) in the residence of the offender? If so, does the victim know the identity of these children?

Photographing or Videotaping of the Victim

- ❑ Did the offender take any photographs or videotapes of the victim?
- ❑ Did the offender make sexually graphic photographs or videotapes of the victim?
- ❑ When were these photographs or videotapes made?
- ❑ When was the last date and time the victim saw these photographs or videotapes?
- ❑ What was the exact location where the victim last saw these photographs or videotapes?
- ❑ If photographs of the victim were taken, which processing laboratory developed them?
- ❑ How were the videotapes marked? How were the photographs packaged?

Other Forms of Physical Evidence

- ❑ Did the offender use items such as condoms, sexual devices, lingerie, lubricants, or oils with the victim?
- ❑ Did the offender keep any personal effects of the victim, such as hair, pubic hair, fingernail clippings, or soiled underwear?
- ❑ When and where were these items last seen?
- ❑ What is the specific location of any other physical evidence that may be involved in the abuse?
- ❑ Where and when did the victim last see this physical evidence?
- ❑ Does the offender hide anything anywhere and, if so, where is it hidden?

Other Instances of Abuse and Results for the Victim

- ❑ Has the victim ever been sexually abused in the past by any other offender?
- ❑ What were the circumstances of that abuse?
- ❑ Has the victim been in therapy as a result of the abuse?

Background Check

Identifying the type of offender with whom you are dealing requires the most complete, detailed, and accurate information possible. As part of the evaluation process and, if possible, before interviewing or interrogating a suspected preferential sex offender, investigate his background thoroughly. The following kinds of records should be considered as sources of information:

- Criminal records.
- Sex offender and child abuse registry records.
- Child protection records.
- Juvenile court records, unsealed or sealed.
- Civil court records, unsealed or sealed.
- Driving or automobile records.
- Military records.
- Bank records.
- School records.
- Medical records.
- Employment records.

Knowing the kind of offender with whom you are dealing can go a long way in determining investigative strategy. This knowledge can influence interview or interrogation approaches and help identify both the kind of corroborative evidence that might be found and where it might be found. It can also help determine the existence and location of other potential or past victims and of child pornography or erotica.

Interviewing the Offender

Unfortunately, many investigators put minimal effort into interviews of offenders who abuse children sexually. However, many of these offenders really want to discuss either their behavior or at least their rationalization for it. If treated with professionalism, empathy, and understanding, they will make significant admissions.

Before interviewing the alleged offender, evaluate his background information and develop an interview strategy. Simply asking an alleged perpetrator if he molested a child does not constitute a proper interview. If the offender is allowed to rationalize or project some of the blame for his

behavior onto someone or something else, he is more likely to confess. Most sex offenders will admit only what has been discovered and what they can rationalize. If you do not confront the subject with all your evidence, he might be more likely to minimize his acts rather than totally deny them. Many child molesters admit their acts but deny the intent. A tougher approach can always be tried if the soft approach does not work.

Consider noncustodial (i.e., no arrest), nonconfrontational interviews of the subject at home or work as well as interviews during the execution of a search warrant. Do not overlook admissions made by the offender to wives, girlfriends, neighbors, friends, and even the media.

Polygraphs and other lie detection devices can be valuable strategic tools in the hands of skilled interviewers. If the suspect believes that a lie detection test is available and, if administered, will reveal the truth or falsehood of his statements, he is more likely to be honest without taking the test. However, investigators must remember that, once these tests are utilized, their value is limited, because the results usually are not admissible in court. The results of polygraphs and other lie detection tests should never be the sole criterion for discontinuing an investigation of child sexual abuse allegations.

Recovery of Child Exploitation Evidence

The recovery of evidence in a case of multiple victim molestation can be very significant, because the evidence can be used both to corroborate the victim's statement and to identify other victims. Those who deal in child pornography and child erotica treat these materials as valuable commodities—sometimes even regarding them as collections—and retain them in secure but available places for extended periods of time. To recover this evidence from the preferential sex offender's collection, the MDT should:

- Obtain the offender's consent to search his premises and belongings. (A sample consent-to-search form is shown in figure 1 on page 18.)
- Obtain a search warrant.

Figure 2 (page 20) presents a list of items to recover from the offender. After the search, make a detailed inventory of all materials seized. Any videotapes seized should be reviewed from beginning to end, as child pornography often is found hidden

Figure 1

Sample Consent-To-Search Form

I, _____, have been informed
(name of property owner)
of my constitutional right not to have a search made of the premises and/or automobile owned by me and/or under my care, identified below, without a search warrant. However, knowing my right to refuse consent to such a search, I hereby authorize _____ and
(name of officer or agent)
_____ of _____
(name of officer or agent) *(name of law enforcement agency)*
to conduct a complete search of the premises, garage or storage shed, and any other structure at the property commonly known as _____

_____
(address and property description)
and/or the following automobile: _____
(vehicle description)
license # _____.These officers or agents are authorized by me to take from my premises and property any videotapes, photographs, letters, computer disks, or any material that is evidence in the nature of child abuse. This written permission is given by me to the above-named persons voluntarily and without any threats or promises of any kind at _____ on this _____
(time, a.m./p.m.)
day of _____, 19____.
(month)

I further understand that I will be given a receipt for any property that is taken.

Signed _____

Name _____
(please print)

WITNESSES *(both law enforcement officers named above):*

Signed _____ _____

Name _____ _____

Agency _____ _____

within commercial pornography and nonpornography videotapes. Identify any children found in photographs or videotapes taken by the offender.

Expert Search Warrants

An expert search warrant[3] is one in which an expert's opinion is used to supplement the case-specific facts learned through the investigation. The opinion usually sets forth known and documented behaviors that preferential sex offenders repeatedly engage in and then applies them to the targeted individual. Determining the type of offender in question and understanding the concept of sexual ritual (see above) are crucial to the use of expert search warrants. Note that if the expert opinion is based on the subject being a certain type of offender, the affidavit for the search warrant must set forth the probable cause to believe the subject is that type.

Because of legal uncertainties, expert search warrants in child sexual exploitation cases should only be used when absolutely necessary. These warrants should be considered in cases where they are needed to:

- Provide additional probable cause.
- Justify expansion of the scope of the search.
- Address problems concerning the staleness of information.

Prosecution

Most preferential sex offenders spend their entire lives attempting to convince themselves and others that they are not perverts and that they love and nurture children. Because most of them have hidden their activities for so long, when they are identified and prosecuted, they try to convince themselves that they will somehow continue to escape responsibility. This is why they often proclaim their innocence right up to the time of their trial. If, however, the investigator and prosecutor have properly developed the case, preferential sex offenders almost always change their plea to guilty. The last thing they want is to have

[3]For additional information on expert search warrants for child exploitation cases, see appendix I of Lanning K.V., *Child Molesters: A Behavioral Analysis. For Law-Enforcement Officers Investigating Cases of Child Sexual Exploitation.* 3d ed. Washington, DC: National Center for Missing and Exploited Children, 1992.

Figure 2

Suggested Items To Recover From Suspected Preferential Sex Offenders

- Any videotapes, 8mm movies, photographs, negatives, magazines, pictures, books, computer files, or any materials depicting a person under the age of 18 years engaged in sexual intercourse, sexually explicit conduct, or lewd exhibition of the genitals.
- Any undeveloped rolls of film or commercial and noncommercial videocassettes.
- Any video equipment, television equipment, photography equipment, darkroom equipment, computer equipment (both hardware and software), or any equipment used in the production, reproduction, display, or distribution of images of a minor being sexually exploited. Before computer equipment is seized, all connections should be noted and marked. The suspect should be prevented from touching the computer. Technical resources for avoiding accidental erasures and retrieving all available information should be identified and used in the investigation.
- Any and all documents, correspondence, calendars, telephone or address books, diaries, computer disks, or any other written or tape-recorded materials that identify or will lead to identification of persons under the age of 18 years.
- Any nonsexual photographs of a minor with whom the suspect may have had any contact.
- Any and all documents, correspondence, financial records, and other materials on paper, computer disk, or computer hard drive relating to the purchase, sale, ordering, receipt, or payment for any materials involving the exploitation of children.
- Any photographs, albums, posters, paintings, books, manuals, nudist magazines, advertisements, or any type of clothing material that could be used for training or instructing a minor in posing, modeling, or performing either clothed or unclothed.
- Any keys to safe deposit or post office boxes, bank statements, invoices, or canceled checks that would indicate the use, rental, or ownership of any storage facility, post office box, or safety deposit box.
- Any and all documents, correspondence, financial records, and other materials on paper, computer disk, or computer hard drive relating to the purchase, sale, transfer, ordering, or receipt of any materials involving the sexual exploitation of children.

the public hear the details of their sexual activity with children. After pleading guilty, they attempt to convince the sentencing authority that their lives have been ruined and that they are "sick" and need treatment. (However, they will usually tell everyone else that, although they pled guilty, they really are not guilty.)

Cases Involving Computers

The investigation of child sexual exploitation cases involving computers requires knowledge of the technical, legal, and behavioral aspects of the use of computers. However, because each of these areas is so complex, investigators must also identify experts and resources available to assist in these cases. Exploitation cases involving computers present many investigative challenges, but they also present the opportunity to obtain a great deal of corroborative evidence and investigative intelligence.

The computer—whether a system at work or, more likely, a personal computer at home—provides the preferential sex offender with an ideal means of filling his needs for validation, organization, and pornography and for finding potential new victims. It is simply a matter of modern technology catching up with long-known personality traits.

Uses of the Computer

Many preferential sex offenders are drawn to online computer services to validate their interests and behavior. The computer may enable them to communicate and obtain active validation with less risk of identification or discovery. The great appeal of this type of communication is perceived anonymity and immediate feedback.

Many preferential sex offenders are compulsive recordkeepers, and the computer offers an ideal means for organizing their collections and correspondence. Innumerable characteristics of victims and sexual acts can easily be recorded and analyzed. An extensive pornography collection can be cataloged by subject matter. Even fantasy writings and other narrative descriptions can be stored and retrieved for future use.

An offender can now use a computer to transfer, manipulate, and even create child pornography. With the typical home computer and modem, still images can easily be digitally stored, transferred from print or videotape, and transmitted, and the quality of each copy will be as good as the original. Visual images can be stored on hard drives, floppy disks, or CD–ROM's.

The offender can also use the computer to troll for and communicate with potential victims with minimal risk of being identified. The use of a vast, loose-knit network like the Internet can make identifying the actual perpetrator difficult. On the computer, the offender can assume any identity or characteristics he wants or needs. The child can be indirectly victimized through conversation ("chat") and the transfer of sexually explicit information and material or can be evaluated for future face-to-face contact and direct victimization.

Types of Offenders

Offenders who traffick in child pornography using computers usually fall into two broad categories:

- **Dabbler**— Usually either a typical adolescent searching for pornography or a curious adult with a newly found access to pornography. Dabblers can be investigated and prosecuted, but their behavior tends not to be as long term, persistent, and predictable.
- **Preferential offender**— Usually either a sexually indiscriminate adult with a wide variety of deviant sexual interests or a pedophile with a definite preference for children. The main difference between them is that the collection of the sexually indiscriminate preferential offender will be more varied, usually with a focus on the offender's particular sexual preferences or paraphilias, whereas a pedophile's collection will focus primarily on children. Also, the sexually indiscriminate offender is less likely to molest children, especially prepubescent children.

Conclusion

Investigators must recognize how child sexual exploitation cases are like and unlike other types of child sexual victimization cases. Understanding victim and offender patterns of behavior, identifying types of offenders, and applying this knowledge to the investigative process can be of significant value in the resolution of these complex and difficult cases.

Contributing Authors

Kenneth Lanning, M.S.
Supervisory Special Agent
Federal Bureau of Investigation
Missing and Exploited Children's
Task Force
FBI Academy
Quantico, VA 22135
540–720–4732
540–720–4792 (fax)

Robert Hugh Farley, M.S.
Commanding Officer
Cook County Sheriff's Police Department
Child Exploitation Unit
1401 South Maybrook Drive
Maywood, IL 60153
708–865–4875
708–865–6576 (fax)

Supplemental Reading

Burgess AW, Grant CA. *Children Traumatized in Sex Rings.* Washington, DC: National Center for Missing and Exploited Children, 1988.

Child Safety on the Information Highway (pamphlet). Washington, DC: National Center for Missing and Exploited Children, 1994.

Lanning KV. *Child Molesters: A Behavioral Analysis. For Law-Enforcement Officers Investigating Cases of Child Sexual Exploitation.* 3d ed. Washington, DC: National Center for Missing and Exploited Children, 1992.

Lanning KV. *Child Sex Rings: A Behavioral Analysis. For Criminal Justice Professionals Handling Cases of Child Sexual Exploitation.* 2d ed. Washington, DC: National Center for Missing and Exploited Children, 1992.

Shepherd JR, Dworin B, Farley RH, Russ BJ, Tressler PW, National Center for Missing and Exploited Children. *Child Abuse and Exploitation: Investigative Techniques.* 2d ed. Washington, DC: Office of Juvenile Justice and Delinquency Prevention, 1995.

Whitcomb D. *When the Victim is a Child.* 2d ed. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 1992.

Organizations

National Center for Missing and Exploited Children (NCMEC)
2101 Wilson Boulevard, Suite 550
Arlington, VA 22201–3052
800–THE–LOST (800–843–5678)
(hotline and child pornography tipline)
703–235–3900 (business number)
703–235–4067 (fax)
http://www.missingkids.org

A clearinghouse of information on missing and exploited children, NCMEC operates a 24-hour hotline and child pornography tipline. NCMEC also provides a wide range of free services, just a few of which are technical case assistance, link and pattern analysis on cases, forensic assistance, training programs, and educational material and publications. Single copies of the NCMEC publications listed above can be obtained free of charge by contacting NCMEC.

Other Titles in This Series

Currently there are 10 other Portable Guides to Investigating Child Abuse. Additional guides in this series may be developed at a later date. To obtain a copy of any of the guides listed below, contact the Office of Juvenile Justice and Delinquency Prevention's Juvenile Justice Clearinghouse by telephone at 800–638–8736 or e-mail at askncjrs@ncjrs.org.

Recognizing When a Child's Injury or Illness Is Caused by Abuse, NCJ 160938

Sexually Transmitted Diseases and Child Sexual Abuse, NCJ 160940

Photodocumentation in the Investigation of Child Abuse, NCJ 160939

Diagnostic Imaging of Child Abuse, NCJ 161235

Battered Child Syndrome: Investigating Physical Abuse and Homicide, NCJ 161406

Interviewing Child Witnesses and Victims of Sexual Abuse, NCJ 161623

Child Neglect and Munchausen Syndrome by Proxy, NCJ 161841

Criminal Investigation of Child Sexual Abuse, NCJ 162426

Burn Injuries in Child Abuse, NCJ 162424

Law Enforcement Response to Child Abuse, NCJ 162425

Resources and Prevention

Online Investigation of Crimes Against Children

Presented by:
The Federal Bureau of Investigation -
Operation "Innocent Images"

SA Colleen M Moss
cmoss.iitf@fbi.gov
301-572-5400
After Hours - 301-586-4500

Today's Presentation

- Background
- Investigative Scope
- Partnerships
- Resources
- Case Management System
- Case Studies

BACKGROUND

- George Burdynski, Jr. kidnapping investigation, May 1993.
- Several suspects developed.
- Search warrant executed in Winchester, Virginia.
- Computer seized, but no direct evidence of kidnapping found.
- Computer exam revealed a private BBS with evidence of Child Pornography.
- Active online investigation began in October 1994, with one Special Agent.

A NATIONAL INITIATIVE

- In 1997, Congress authorized $10 million to the FBI to combat online CP/CSE
- Innocent Images became the Bureau's National Initiative aimed at combating all online CP/CSE
- Baltimore Division Personnel
  - Provide coordination and support to CP/CSE investigations throughout the US
  - Conduct online UC sessions to identify targets and collect evidence
  - Train local, state and federal investigators on investigative techniques and protocols

BA RESOURCES /CENTRAL CLEARINGHOUSE

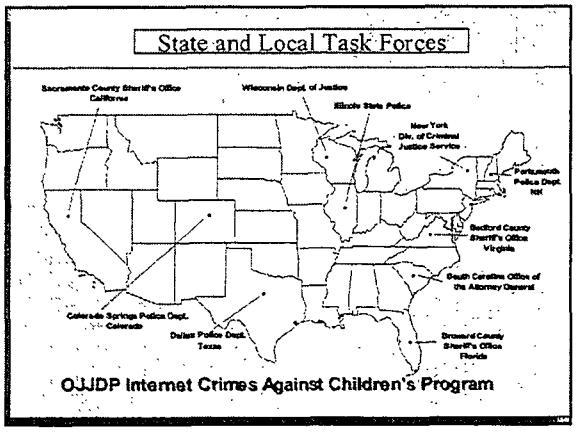
20	FBI Special Agents	(+2)
5	Detectives from local jurisdictions (Deputized)	
1	US Customs Special Agent	
1	US Postal Inspector	
1	NCIS Special Agent	
16	Intelligence Research Specialists	(+3)
4	Investigative Assistant	
8	Data Loaders	(+1)
1	Computer Specialist	(+1)
2	Squad Secretary	
2	Supervisory Special Agents	

INNOCENT IMAGES OPERATIONS

- Houston, Texas
- Newark, New Jersey
- Tampa, Florida
- Los Angeles, California "SAFE Team"
- Birmingham, Alabama
- Las Vegas and Dallas anticipated by September, 1999.

INNOCENT IMAGES PARTNERSHIPS

- 10 Office of Juvenile Justice and Delinquency Prevention (OJJDP) Internet Crimes Against Children (ICAC) Task Forces around the nation
- FBI, U.S. Customs Service, and U.S. Postal Inspection Service have assisted OJJDP in the development of this program



ICAC Task Forces

- Close working relationship
- FBI Baltimore "Innocent Images" maintains ICAC pointer system
- Planning toward 24 hour / 7 day per week operation to support these offices

Federal Adoption of Local Cases

- FBI can adopt local cases if they meet Federal prosecutive guidelines
- Bureau can open police cooperation case to enable local and state police agencies access to our resources
- Local case must comply with ICAC Task Force guidelines, at a minimum, to qualify for adoption

Federal Violations

- Interstate Travel with intent to have sex with a juvenile. "Traveler" cases.
- Enticement of a juvenile to engage in an illegal sex act, using an interstate facility.
- Child Pornography
  - Manufacture
  - Distribution
  - Possession

Innocent Images Resources

- CAC Coordinators
- Pocatello Information Center
  - Mass Disk Analysis
  - Public Source Information Searches
- C.A.R.T.
  - Requires Opening Police Cooperation Case
  - Lengthy Backlog - Can process urgent requests on case by case basis
  - 4 full-time examiners designated for Innocent Images cases

Innocent Images Resources

- Legal
  - Former Innocent Images Agent is Associate Chief Division Counsel (ACDC)
  - Office of General Counsel
  - DOJ Child Exploitation and Obscenity Section (CEOS)
  - Recent case decisions

Innocent Images Resources

- Training
  - Hardware and Software recommendations
  - Undercover backstopping issues
  - Policy development
  - Training at Calverton on special request
  - Law Enforcement presentations
    - Requires FBIHQ approval
    - Require as much notice as possible
    - Tailored to individual audience

Innocent Images Resources

- National Center for Analysis of Violent Crime (NCAVC) -
  - FBI Behavioral "Profilers"
  - Two Agents assigned to Innocent Images
  - Researching personality types of offenders
  - Can help regarding issues of staleness in warrants if suspect is preferential offender
  - Requires case by case analysis

Case Management
Inter-Division Coordination

- Information received by FBI or ICAC task forces is forwarded to Innocent Images, regardless of source.
- Innocent Images coordinates, analyzes and disseminates information.
- Prevents duplication of effort.
- Provides pool of expertise and information.

Case Management
Inter-Agency Coordination

- Provide a coordinated response by Law Enforcement
- Problems encountered in the past
  - One case, the target was in the Department where the lead went.
  - We have been pursued by another UCO.

Case Management
Inter-Agency Coordination

- Database information is available to all Law Enforcement Agencies, subject to Rule 6E.
- Administrative Subpoena has been approved by Congress, pending AG decision.
- The CMS allows for quick recovery of information & UC sessions between UCAs and targets.

Case Management
Inter-Agency Coordination

- AOL Terms Of Service (TOS) complaints available from our database.
- New Oracle based database under development.
- The CMS may hold the piece of evidence needed for probable cause in your case.

Case Management
Personnel

- Persons assigned this work should be volunteers.
  - Volunteers, not "chosen".
  - "Truth finding" vs. "Fact finding".
- Rotation policy.
- FBI Safeguard program.
- Child Abuse and Computer investigations are stressful. What about both?

Jurisdictional Considerations

Why work in Task Forces?

- Certain crimes lend themselves better to State and Local jurisdiction
  - Child Abuse (physical and sexual).
- Other crimes may share joint jurisdiction but one may have "more appropriate" sentencing
  - Child Pornography (Possession and Manufacturing)
- Federal Statutes cover some crimes most localities don't
  - Enticement of juvenile to commit illegal sex act

Jurisdictional Considerations

Why work in Task Forces?

- Many local and state statutes require an actual victim.
- Investigations can develop into multi-jurisdictional investigations.
  - Locally *and* Internationally
- Facts of the case should dictate involvement of different investigative/prosecutorial jurisdictions.

Case Studies

Joseph Klein

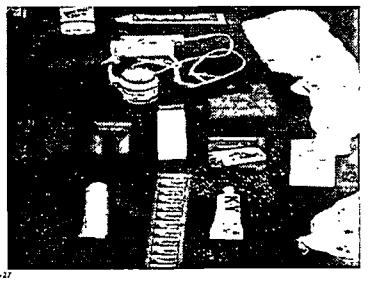
- Highly successful 62 year old Broadway music director
- Subject worked at a kids' summer arts camp and was suspected of illicit contact with a minor

Joseph Klein

- Local P.D. in New Hampshire contacted FBI
- P.D. supplied subject's AOL screen name
- Baltimore Undercover Agent posing as a 13 year old boy sent a message to subject

Joseph Klein

- Ensuing conversation resulted in subject's travel to a mall in Maryland to have sex with "boy"



Joseph Klein

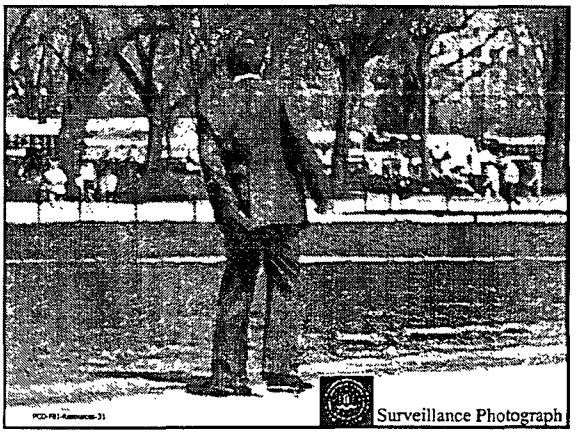
- Search executed at subjects home revealed victim "log" book
- Leading toward possibly dozens of victims
- Klein pled guilty, is incarcerated awaiting sentencing--and doesn't like the food

Bruce Gilson

- Romeoville Ill. PD was informed by source that Gilson had traveled to meet with known pedophile.
- UC contacted source who agreed to introduce Gilson and UC online in IRC channel.
- Posing as adult having access to minors UC establishes communication online.
- Communication included telephonic contacts and several face to face meetings in Washington DC.

Bruce Gilson

- During communications Gilson reveals he is in possession of pornographic images of known minor males he received over the Internet.
- Gilson is introduced to UC posing as 14 year old male both online and telephonically.
- Gilson travels from MD to VA to meet minor and was arrested, search warrant served, computer and approximately 10,000 pornographic images seized.
- Gilson currently incarcerated serving two years.



Surveillance Photograph

Resources Available

- National Center for Missing and Exploited Children
  - We work very closely with this agency
  - 24 Hour hotline 1-800-THE-LOST
  - CyberTipLine: www.missingkids.com
  - Legal and Technical assistance
  - Training and Education
  - Photo and imaging distribution system
    - "Aging" and "Reconstruction" processes

Resources Available

- Innocent Images, FBI Baltimore
  - Nationwide, coordinated coverage.
  - Extensive database of targets and sites.
  - FBI presence at the NCMEC.
  - Some information protected by RFCP, Rule 6e.
  - US Customs and US Postal Inspector presence.
  - 24 hour availability, 301-586-4500.

Innocent Images

National Initiative

On-Line Child Pornography -
Child Sexual Exploitation Investigations

Innocent Images

Innocent Images National Initiative	Section #1
Recommended Best Practices For On-line CP/CSE Investigations	Section #2
Recommended Hardware & Software For On-line Undercover Activity	Section #3
Use of Computers in the Sexual Exploitation of Children	Section #4
FBI Resources	Section #5
FBI Crimes Against Children Coordinators	Section #6

Section #1

Innocent Images National Initiative

INNOCENT IMAGES

Online Child Pornography/Child Sexual Exploitation Investigations

The FBI's Response to Online CP/CSE investigations

While investigating the disappearance of a juvenile in May 1993, FBI agents and Prince George's County, Maryland, Police detectives identified two suspects who had sexually exploited numerous juvenile males over a 25 year period. Investigation into the activities of the suspects determined that adults were routinely utilizing computers to transmit images of minors showing frontal nudity or sexually explicit conduct and to lure minors into engaging in illicit sexual activity. Further investigation and discussions with experts, both within the FBI and in the private sector, revealed that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which some sex offenders shared pornographic images of minors and identified and recruited children into sexually illicit relationships. Based on information developed during this investigation, the Innocent Images investigation was initiated, in 1995, to address the illicit activities conducted by users of commercial and private online services as well as the Internet.

The central operation and case management system for all FBI online CP/CSE investigations is located at the Maryland Metropolitan Office at Calverton, Baltimore Division. The Innocent Images field supervisor and investigative personnel work closely with the Innocent Images program manager at FBI Headquarters in investigative, administrative and policy matters involving the initiative. All FBI field offices forward copies of text and images obtained in all online CP/CSE investigations to the Baltimore Division for incorporation into the Innocent Images case management system. The Innocent Images initiative provides for a coordinated FBI response to a nationwide problem by collating and analyzing information and images obtained from numerous sources and avoids duplication of effort by all FBI field offices.

The FBI's national initiative focuses on individuals who indicate a willingness to travel for the purpose of engaging in sexual activity with a juvenile; producers of child pornography; and major distributors of child pornography (defined as one who appears to have transmitted a large volume of child pornography via computer on numerous occasions to numerous other subscribers), in violation of the following Sections of Title 18 of the United States Code:

- Section 2251- Sexual Exploitation of Children/Selling or Buying of Children
- Section 2252 - Sexual Exploitation of Minors
- Section 2253 - Criminal Forfeiture
- Section 2423(b) - Interstate Travel with Intent to Engage in a Sexual Act with a

Juvenile.

The FBI and the Department of Justice (DOJ) review all files and select the most egregious subjects for prosecution.

The FBI has taken the necessary steps to ensure that the Innocent Images national initiative remains viable and productive through the use of new technology and sophisticated investigative techniques, coordination of the national investigative strategy and a national liaison initiative with a significant number of commercial and independent online service providers. Innocent Images has been highly successful. It has proven to be a logical, efficient and effective method to identify and investigate individuals who are using the Internet for the sole purpose of sexually exploiting children.

The Beginning of Innocent Images

During the early stages of Innocent Images, a substantial amount of time was exhausted on commercial online service providers which provide numerous easily accessible "chat rooms" in which teenagers and pre-teens can meet and converse with each other. Through the use of chat rooms, children can chat for hours with unknown individuals, often without the knowledge or approval of their parents. Investigation revealed that computer-sex offenders utilized the chat rooms to contact children as a child does not know whether he/she is chatting with a 14 year old or a 40 year old. The chat rooms offer the advantage of immediate communication throughout the United States and provide the pedophile an anonymous means of identifying and recruiting children into sexually illicit relationships. The FBI has investigated more than 70 cases involving computer-sex offenders traveling interstate to meet juveniles.

The investigative operation involves undercover agents (UCAs) subscribing to various commercial online service providers, the Internet and various bulletin board systems (BBBs) utilizing fictitious screen names and engaging in real-time chat or E-mail conversations. UCAs do not "surf the net" and all areas of online service providers or the Internet are predicated prior to FBI entry. Predication can be by citizen complaint; complaint by an online service provider; or self-predication by virtue of title, i.e., alt.pedophilia.sex, alt.children.sex, alt.boys.sex., alt.girls.sex. Each undercover contact conducted over the computer is handled as a consensually monitored telephonic conversation. All contacts between UCAs and potential subjects are captured and archived on electronic media, to include, all conversations and images downloaded to the UCAs.

The Innocent Images investigation demonstrated the need for a mechanism to track subject transactions and to correlate the seemingly unrelated activities of thousands of subjects in a cyberspace environment so the Innocent Images case management system was developed which has proven to be an effective system to archive and retrieve the information necessary to identify and target priority subjects. All relevant data obtained during an undercover session is loaded into the Innocent

Images structured and full text retrieval case management system by Intelligence Research Specialists (IRSs). The IRSs update, review and analyze the information contained in the case management system on a daily basis to identify priority subjects. Once an individual has been targeted as a potential or priority subject, subpoenas are issued to the relevant online service providers to obtain all available identifying information. A subject is given a priority status based on any indication that he/she is a preferential child molester or is willing to travel for the purpose of engaging in sexual activity with a minor. Once a subject has been targeted for investigation, an IRS prepares a lead packet for the appropriate FBI field office. The packet contains copies of all evidence collected by the FBI, to include, UCA chat and session logs, relevant investigative reports, all electronic conversations between the UCA and the subject and all illicit images uploaded to the UCA. The lead packet is sent to the appropriate field office for further investigation and presentation to the U.S. Attorney's Office for prosecutive action.

The Progression of the Innocent Images Initiative

Innocent Images has expanded to include investigations involving newsgroups, Internet relay chat and fileservers.

Internet Newsgroups

A great deal of child pornography is regularly posted on Internet newsgroups which are electronic bulletin boards to which anyone with an Internet Service Provider (ISP) and news access can post messages, with or without attachments (sometimes taking the form of pornographic images). Anyone with an ISP can access newsgroups and download any posted messages and/or attachments. From an investigative standpoint, subjects who post to newsgroups are extremely difficult and labor intensive to investigate because it is hard to identify who they really are. Unlike online service providers, such as America Online, there are no unique screen names associated with each account. Each time a subscriber signs on with an ISP, he can assume any identity he wants but, through consultation with persons who are extremely proficient on the Internet, Innocent Images personnel have discovered a way to identify persons who post child pornography to newsgroups.

Internet Relay Chat (IRC) Channels

IRC channels are similar to chat rooms. They are places on the Internet where people can go to communicate with people who have similar interests. The communications are real time, just like telephone calls or face to face communications. The threat that they pose to children is similar to the threat posed by chat rooms. IRC channels can be dedicated to any topic including the trading of child pornographic images or the recruitment of children into illicit sexual relationships. The difference between IRC channels and chat rooms is that subscribers, to online service providers

providing chat rooms, have unique and traceable screen names assigned to them. IRC users can assume any screen name they want and change it at any time they want. They can assume one identity during one IRC session and another identity during another IRC session just minutes or hours later which makes identifying and tracking IRC users much more difficult.

File Servers ("FServes")

Fserves are a feature of IRC channels. An IRC user can set up an fserve that allows other users to access and download files from particular directories on his hard disk. It is a mechanism that child pornography collectors are using to build their collection. Fserves enable computer users to program their computers so that visitors can download a certain number of bytes in exchange for uploading a certain number of bytes. In other words, it is an automated, computer programmed, trading system. The person who sets up the fserve (the host) can establish the parameters of the trading. He can restrict the visitor to certain directories on his hard disk. He can give the visitor a credit of a certain number of bytes or no credit at all. Once the visitor uploads the minimum number of bytes, he can download a preset number of bytes, selecting from the file names listed on any of the directories made available by the host. Most often, a host programs his computer and leaves it on in his absence. The trading is then done automatically by his computer using the parameters the host previously established. Identifying people who establish fserves is done in the exact same way as identifying other users of IRC channels.

The Growth of Innocent Images

The Innocent Images initiative has been "franchised" to the FBI's Houston, Los Angeles, Newark and Tampa Divisions and it is anticipated that other FBI field offices, located at strategic locations around the country, will eventually operate Innocent Images franchise operations. The well-defined administrative and operational protocols established by the Baltimore Division will greatly assist in the expansion of the Innocent Images initiative by other FBI field offices. All of the franchised field offices will operate in close coordination with the FBI's Baltimore Division, FBIHQ and the Child Exploitation and Obscenity Section (CEOS), DOJ.

For further information concerning Innocent Images....

Contact:

Supervisory Special Agent (SSA) George L. Martinez
Innocent Images Squad 21 (south)
Maryland Metropolitan Office at Calverton
Baltimore Division
Telephone (301) 586-4521
Facsimile (301) 586-4547

Acting Supervisory Special Agent (SSA) Stacey M. Bradley
Innocent Images Squad 19 (north)
Maryland Metropolitan Office at Calverton
Baltimore Division
Telephone (301) 586-4519
Facsimile (301) 586-4499

SSA John (Jack) Boyle
Program Manager
Special Investigations and Initiatives Unit
Office of Crimes Against Children
FBIHQ
935 Pennsylvania Avenue, NW
Room 11163
Washington, D.C. 20535
Telephone (202) 324-6364
Facsimile (202) 324-2731

INNOCENT IMAGES OPERATIONS

LOCATION	SSA	TELEPHONE	FAX #	ADDRESS	CASE AGENT & DIRECT TELEPHONE
BALTIMORE	Jorge L. Martinez Stacey M. Bradley	301-586-4621 301-586-4619	301-586-4547 301-586-4499	11700 Beltsville Drive Suite 200 Calverton, MD 20705	
BIRMINGHAM	Robert M. Callhan	205-715-0330	205-715-0293	2121 8th Avenue, North Room 1400 Birmingham, AL 35201	Michelle R. Stafford 205-715-0370 George C. Moore, III 205-715-0339
LOS ANGELES	Randy J. Aden	310-996-4259	310-996-4083	1100 Wilshire Boulevard Suite 1700 Los Angeles, CA 90024	James Nice 310-996-4225
NEWARK	Rockie Fuller	732-469-7986 ext. 272 (voice mail number (732-805-0463)	732-469-7988	100 Davidson Avenue Suite 209 Somerset, NJ 08873	James Furry 732-469-7986 ext. 250 (voice mail number 732-805-0463)
TAMPA	Dave Thomas	813-272-8244	813-221-8100	500 Zack Street Room 610 Tampa, FL 33602	Diane Farrington 813-272-8240
HOUSTON	Tom McClenaghan	713-693-1830	713-868-9771	2500 East T.C. Jester Houston, TX 77008	Geoff Binney 713-693-1835 Kathy Crawford 713-693-1844

Section #2

Recommended Best Practices for On-line CP/CSE Investigations

On-line Child Pornography/Child Sexual Exploitation

Recommended Best Practices

* Personnel assigned to handle child pornography material should be psychologically tested periodically.

* All text and images from every on-line session should be saved. All undercover activity must be fully documented or "logged." Each session is considered consensual monitoring.

* Undercover law enforcement officers should limit their activities to areas of the Internet that are predicated as places where criminal activity occurs.

* Areas on the Internet can be predicated by name, by complaint, or by law enforcement or Internet Service Provider intelligence or referral.

* Undercover activities should only be conducted in approved office space. It is strongly recommended that undercover activities not be conducted at an undercover officer's home except under strictly defined circumstances and only with prior written authorization by a superior.

* Undercover officers should never upload pornographic images. On rare occasion, a need may arise to upload non-pornographic images. This should only be done with the prior approval of superiors and in consultation with the local/federal prosecutor..

* All computers used for undercover activity should be purchased covertly. Undercover activity should never be conducted on personally owned computers.

* Undercover law enforcement officers should use covertly registered software. Do not exceed trial periods on shareware.

* All Internet service accounts should be backstopped using undercover identities.

Recommended Best Practices (continued)

* Extreme caution must be utilized in dealing with informants. It is recommended that each agency develop a strict policy on how they will handle criminal informants/sources.

* Undercover law enforcement officers should allow the target of the investigation to lead the on-line conversation, particularly when sex topics are discussed. In each conversation with the subject, the undercover officer should never be the first to raise the subject of sex. Allow the target to choose the meeting location with subtle guidance from the undercover officer. The issue of entrapment must always be considered in these type of investigations.

Section #3

Recommended Hardware & Software for On-line Undercover Activity

ON-LINE CHILD PORNOGRAPHY/CHILD SEXUAL EXPLOITATION INVESTIGATIONS

RECOMMENDED HARDWARE AND SOFTWARE

SOFTWARE

Operating System: Windows 95 or 98. Windows NT Workstation is not recommended because it may not be compatible with the application software you will be using and is more complex to administer.

Application Software:

1. **Web Browser**: There are two major products in use, Microsoft Internet Explorer and Netscape Navigator. Both are functionally equivalent and you only need one of them to view web pages.

2. **Word Processor**: A major product such as WordPerfect or Microsoft Word is needed to read different types of text and word processed files.

3. **Internet Mail Client**: An application that will allow you to send and receive Internet E-Mail from multiple accounts. Some examples are Microsoft Outlook Express and Eudora Pro.

4. **NewsGroup Client**: An application that allows you to visit NewsGroups and download postings. Some examples are Outlook Express and Forte Agent.

5. **IRC Client**: An application that allows you to chat on the IRC system. Some examples are MIRC and PIRCH.

6. **Internet Tools**: An application that allows you to trace the origins of a particular Internet patron. You should choose a tool that has the capacity to conduct a TraceRoute, WHOIS, DNS, e-mail verification, PING and Port Scanner with FINGER. Some examples are Network Toolbox and NeoTrace.

7. **Graphic Viewing Software**: An application that allows you to view and analyze a multitude of graphic image types. Some examples are ThumbsPlus, Quickview Plus and ViewPrint.

8. **Commercial On-line Service**: If you are planning on working on America Online (AOL), Microsoft Network or any other self-contained on-line service, you will need that service's proprietary client software. If you choose to conduct investigations on AOL, an add on product that can be used is PowerTools by BPS Software. PowerTools augments the logging capabilities and Instant Messaging windows of the standard AOL Client.

HARDWARE - MINIMUM REQUIREMENTS:

Pentium 120 MHZ Processor
32MB RAM
2GB Hard Drive
Video Card with 2MB Video RAM
14" VGA Monitor
CD-ROM Drive
3.5" Floppy Disk Drive
28.8 Modem

HARDWARE - RECOMMENDED REQUIREMENTS:

Pentium II 266 MHZ Processor or better
64MB RAM
4GB Hard Drive
Video Card with 8MB Video RAM
17" SVGA Monitor
CD-ROM Drive
3.5" Floppy Disk Drive
56K V90 Modem
Iomega Zip Drive

Section #4

Use of Computers in the Sexual Exploitation of Children

USE OF COMPUTERS IN THE SEXUAL EXPLOITATION OF CHILDREN

By

SSA Kenneth V. Lanning

Understanding Behavior

The investigation of child sexual exploitation cases involving computers requires knowledge of the technical, legal, and behavioral aspects of the use of computers. However, because each of these areas is so complex, investigators must also identify experts and resources available to assist in these cases. Exploitation cases involving computers present many investigative challenges, but they also present the opportunity to obtain a great deal of corroborative evidence and investigative intelligence. This section of the guide will focus primarily on the dynamics of offender behavior in the use of computers.

Offenders

Although a variety of individuals sexually victimize children, preferential sex offenders are the primary sexual exploiters of children. Using a computer to validate behavior, facilitate interacting with child victims, or traffick in child pornography usually requires above average intelligence and economic means. Therefore, the offenders discussed here will generally be from a higher socioeconomic background. In addition, preferential sex offenders tend to be predatory, serial offenders. This document will not focus on other types of predatory, serial sex offenders such as those who use intimidation and force to engage in sexually motivated child abduction.

The term preferential sex offender, as used in this document, is only a descriptive label used to identify for investigative purposes a certain type of offender. An important step in investigating sexual exploitation of children is to recognize and utilize, if present, the highly predictable sexual behavior patterns of these preferential sex offenders.

You cannot hope to determine the type of offender with whom you are dealing unless you have the most complete, detailed, and accurate information possible. The investigator must understand that doing a background investigation on a suspect means more than obtaining the date and place of birth and credit and criminal checks. School, juvenile, military, medical, driving, employment, bank, and sex offender and child abuse registry records can be valuable sources of information about

an offender. Knowing the kind of offender with whom you are dealing can go a long way in determining investigative strategy. It can influence interview approaches and facilitate learning where and what kind of corroborative evidence might be found. It can be useful in determining the existence and location of other victims and child pornography or erotica.

Expert Search Warrants

An expert search warrant is one in which an expert's opinion is used to supplement the case-specific facts learned through the investigation. The opinion usually sets forth known and documented behaviors that preferential sex offenders repeatedly engage in and then applies them to the targeted individual. Determining the type of offender in question is crucial to the use of expert search warrants. If the expert opinion is based on the subject being a certain type of offender, the affidavit for the search warrant **must** set forth the probable cause to believe the subject is that type.

Because of legal uncertainties, expert search warrants in child sexual exploitation cases should only be used when absolutely necessary. These warrants should be considered in cases where they are **needed** to:

(1) provide additional probable cause;
(2) justify expanding the scope of the search;
(3) address problems concerning the staleness of information.

Recognizing Preferential Sex Offenders

A preferential sex offender can usually be identified by the following behaviors:

1. Long-Term and Persistent Pattern of Behavior
   A) Begins pattern in early adolescence
   B) Is willing to commit time, money, & energy
   C) Commits multiple offenses
   D) Makes ritual or need-driven mistakes

2. Specific Sexual Interests
   A) Manifests paraphiliac preferences (may be multiple)
   B) Focuses on defined sexual interests and victim characteristics
   C) Centers life around preferences
   D) Rationalizes sexual interests

3. Well-Developed Techniques
   A) Learns from experiences
   B) Lies and manipulates, often skillfully
   C) Has method of access to victims
   D) Is quick to use modern technology (e.g. computer, VCR) for sexual needs & purposes

4. Fantasy-Driven Behavior
   A) Collects pornography
   B) Collects paraphernalia, souvenirs, videotapes
   C) Records fantasies
   D) Acts to turn fantasy into reality

Because these sexual behavior patterns are highly predictable, it is important for investigators to recognize and utilize them, if present. If the investigation identifies enough of these characteristics, many of the remaining ones can be assumed. Most of these indicators mean little by themselves, but as they are identified and accumulated through investigation, however, they can constitute reason to believe a suspect is a preferential sex offender.

Use of Computers

The great appeal of a computer becomes obvious when you understand sex offenders, especially the preferential sex offender. The computer could be a stand alone system or one utilizing on-line service capability. The computer---whether a system at work or, more likely, a personal computer at home---provides the preferential sex offender with an ideal means of filling his needs for validation, organization, and pornography and for finding potential new victims. The sex offender using a computer is not a new type of criminal. It is simply a matter of modern technology catching up with long-known, well-documented personality traits. Such offenders are usually among the first to obtain and learn to use the latest computer technology. Because of these traits and needs, they are willing to spend whatever time and money it takes.

Validation

Many offenders are drawn to computers utilizing on-line service capability to communicate and validate their interests and behavior. This is actually the most important and compelling reason that preferential sex offenders are drawn to the on-line computer. Now, in addition to physical contact and putting a stamp on a letter or package, they can use their computer to exchange information and validation. Through the Internet, national and regional on-line services, or specialized electronic bulletin boards, offenders can use their computers to locate individuals with similar interests.

The computer may enable them to obtain active validation (i.e., from living humans) with less risk of identification or discovery. The great appeal of this type of

communication is perceived anonymity and immediate feedback. They feel protected as when using the mail, but get immediate response as when meeting face to face.

Like advertisements in "swinger magazines," computer on-line services are used to identify individuals of mutual interests concerning age, gender, and sexual preference. The offender may use an electronic bulletin board to which he has authorized access, or he may illegally enter a system. The offender can also set up his own or participate in other surreptitious or underground on-line bulletin boards.

In addition to adults with similar interests, offenders can sometimes get validation from the children they communicate with on-line. When it is provided to them, children needing attention and affection may respond to an offender in positive ways. They may tell the offender he is a "great guy" and that they are grateful for his interest in them. Validation is also obtained from the fact that they are utilizing the same cutting edge technology used by the most intelligent and creative people in society. In their minds, the time, technology, and talent it takes to engage in this activity is proof of its value and legitimacy.

Offenders' need for validation is the foundation on which proactive investigative techniques (e.g. stings, undercover operations, etc.) are built and the primary reason they work so often. Although their brain may tell them not to send child pornography or not to reveal details of past or planned criminal acts to a stranger they met on-line, their need for validation oftens compels them to do so.

Organization

Offenders use computers to organize their collections and correspondence. Many preferential sex offenders in particular seem to be compulsive record keepers. A computer makes it much easier to store and retrieve names and addresses of victims and individuals with similar interests. Innumerable characteristics of victims and sexual acts can be easily recorded and analyzed. An extensive pornography collection can be cataloged by subject matter. Even fantasy writings and other narrative descriptions can be stored and retrieved for future use.

One problem the computer creates for law enforcement is determining whether computer texts describing sexual assaults are fictional stories, sexual fantasies, diaries of past activity, plans for future activity, or current threats. This problem can be compounded by the fact that there are individuals who believe that cyberspace is a new frontier where the old rules of society do not apply. They do not want this "freedom" scrutinized and investigated. There is no easy solution to this problem. Meticulous analysis and investigation are the only answers.

Finding Victims

Offenders can use the computer to troll for and communicate with potential victims with minimal risk of being identified. The use of a vast, loose knit network like the Internet can make identifying the actual perpetrator difficult. On the computer, the offender can assume any identity or characteristics he wants or needs. Older children are obviously at greater risk than younger children of such victimization. Adolescent boys who spend many hours "hacking" on their computers are at particularly high risk of such contacts. The child can be indirectly "victimized" through conversation ("chat") and the transfer of sexually explicit information and material or can be evaluated for future face-to-face contact and direct victimization. The latest technology even allows for real-time group participation in child molestation by digital teleconferencing by computer.

Investigators must recognize that many of the children lured from their homes after on-line computer conversations are not innocents who were duped while doing their homework. Most are curious, rebellious, or troubled adolescents seeking sexual information or contact. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize what they were getting into.

Maintenance of Financial Records

Offenders who have turned their child pornography into a profit making business use computers the same way any business uses them. Lists of customers, dollar amounts of transactions, descriptions of inventory, and so on, can all be recorded on the computer. Because trafficking in child pornography by computer lowers the risks, there may be an increase in profit-motivated distribution.

Child Pornography

Because of computers utilizing on-line services, child pornography is now more readily available in the United States than it has been since the late 1970's. An offender can now use a computer to transfer, manipulate, and even create child pornography. With the typical home computer and modem, still images can easily be digitally stored, transferred from print or videotape, and transmitted, with each copy being as good as the original. Visual images can be stored on hard drives, floppy disks, or CD-ROM's. With newer technology, faster modems, digital cameras, and better computers, similar things can now be done with some moving images. For now, however, it is still difficult to transmit the most preferred child pornography format--high quality, lengthy moving images (e.g. videotape, films).

The other invaluable modern inventions for pornographers, the video camera and recorder, are now being integrated into and through the computer. Multimedia images with some motion and sound and virtual reality programs can

provide an added dimension to the pornography. The information and images stored and transmitted can be encrypted to deter detection.

Some of these uses are now small problems that can eventually become big problems. Computer software and hardware is being developed so rapidly that the potential of these problems is almost unlimited. In the near future, most communication systems in a home (e.g., telephone, television, fax, videotape, music, newspapers, financial records, etc.) may be funneled through a computer.

The ability to manipulate digital visual images may make it difficult to believe your own eyes. Television commercials now make it appear that Paula Abdul is dancing with Gene Kelly and John Wayne is talking to a drill sergeant, and movies show Forrest Gump meeting with Presidents. With computer graphics programs, images can be easily changed or "morphed." This is the same technology that is used to "age" the photographs of long-missing children.

Computer-manipulated and, soon, computer-generated visual images of "children" engaging in sexually explicit conduct may call into question the basis for highly restrictive (i.e., possession, advertising, etc.) child pornography laws. Under the recently passed Child Pornography Prevention Act of 1996, the federal definition of child pornography has now been expanded to include any visual depiction that "has been created, adapted, or modified to **appear** (emphasis added) that an identifiable minor is engaging in sexually explicit conduct." This new law makes prosecution of cases involving manipulated computer images easier, but it also dilutes the significance of child pornography. It would be hard to argue that child pornography is the permanent record of the abuse or exploitation of an actual child if no real child is involved. If the constitutionality of this new law is not upheld, only existing obscenity laws may apply to such simulated child pornography.

Computer Offenders

Offenders who traffick in child pornography using computers usually fall into two broad categories:

1. **Dabbler** - Usually either a typical adolescent searching for pornography or a curious adult with a newly found access to pornography. Dabblers can obviously be investigated and prosecuted, but their behavior is not as long-term, persistent, and predictable.

2. **Preferential Offender** - Usually either a sexually indiscriminate with a wide variety of deviant sexual interests or a pedophile with a definite preference for children. The main difference between them is that the collection of the sexually indiscriminate preferential offender will be more varied, usually with a focus on their particular sexual preferences or paraphilias, whereas a pedophile's collection will focus predominately on children. Also, the sexually indiscriminate offender is less likely to

molest children, especially prepubescent children. With either of the preferential types, the characteristics, dynamics, and techniques (i.e. expert search warrant) previously discussed concerning preferential sex offenders should be considered.

One sensitive area for investigators is the preferential offender who presents himself as a concerned citizen reporting what he inadvertently "discovered" in cyberspace or requesting to work with law enforcement to search for child pornography and to protect children. Other than the obvious benefit of legal justification for their past or future activity, most do this as part of their need to rationalize their behavior as worthwhile and to gain access to children. When these offenders are caught, instead of recognizing this activity as part of their preferential pattern of behavior, the courts sometimes give them leniency because of their "good deeds." Preferential offenders who are also law enforcement officers sometimes claim their activity was part of some well-intentioned, but unauthorized investigation.

Other miscellaneous "offenders" include: media reporters who erroneously believe they can traffick in child pornography as part of a news expose; pranksters who disseminate false or incriminating information to embarrass the targets of their "dirty tricks"; and concerned citizens who go overboard doing their own private investigations into this problem. Investigators must be cautious of all overzealous citizens offering their services in these cases. Only law enforcement officers as part of official, authorized investigations should be downloading child pornography on a computer.

When attempting to determine if an individual using a computer to traffick in child pornography is a dabbler or a preferential offender, evaluate all available background information. The following information from the on-line computer activity can be valuable in this assessment. This information can often be ascertained from the on-line service provider and through undercover communication, pretext contacts, informants, and other investigative techniques.

* Screen Name
* Screen Profile
* Accuracy of Profile
* Length of Time Active
* Amount of Time Spent On-line
* Number of files
* Number of Transmissions
* Originate, Forward, Receive
* Number of Recipients
* Theme of Messages & Chat
* Theme of Pornography

One big problem in these cases is that it is often more difficult to identify the specific person using the computer than it to identify the computer being used. It is harder to do a background investigation when multiple people have access to the computer. Pretext phone calls can be very useful in such situations.

Summary

Investigators must be alert to the fact that any offender with the intelligence, economic means, or employment access might be using a computer in any or all of the above ways, but preferential sex offenders are highly likely to do so.
As computers become less expensive, more sophisticated, and easier to operate the potential for abuse will grow rapidly.

Section #5

FBI Resources

U.S. Department of Justice

Federal Bureau of Investigation

Agency Description

The Federal Bureau of Investigation (FBI) exercises its jurisdiction and investigative responsibilities pursuant to Federal statutes addressing various crimes against children, including kidnaping and sexual exploitation. Federal law defines children as minors under the age of 18, often referred to as "children of tender years." FBI investigations involving crimes against children generally include violations of Federal statutes relating to child abuse, sexual exploitation of children, interstate transportation of obscene material, computer pornography, interstate transportation of children for sexual activity, parental kidnaping, and violations of the Child Support Recovery Act. In some instances, the RICO (Racketeer Influenced and Corrupt Organizations) statute also may apply. While some of those Federal violations may not necessarily involve the sexual abuse or sexual exploitation of children, such as violations of the International Parental Kidnaping Act, the FBI pursues any child victimization offense within its lawful jurisdiction, often coordinating those investigations with other Federal, State, and local agencies.

Cases related to the sexual abuse and exploitation of children and other crimes against children are given high priority within the FBI. All available and necessary FBI resources are used during these investigations, and each case is aggressively prosecuted. Nonfamily abductions, often referred to as stranger abductions, receive immediate attention. Particular attention is also given to investigations involving organized criminal activity, commercialized child prostitution, and the manufacture and distribution of child pornography. The transmission and exchange of child pornography through computer bulletin boards are aggressively investigated as an insidious form of child sexual exploitation.

The FBI also investigates allegations of sexual assault in Indian country, including the investigation of child abuse and the sexual exploitation of children. The FBI addresses these sensitive investigations by participating with other professionals in a multidisciplinary team approach that enlists the expertise of investigators, social workers, clinical psychologists, victim-witness coordinators, and Federal prosecutors.

Services

Investigative Services and Support

FBI Headquarters. On January 20, 1997, a new unit and two new offices were

established within the Violent Crime and Major Offenders Section, Criminal Investigative Division, at FBI Headquarters. These entities, the Office of Crimes Against Children (OCAC) and the Office of Indian Country Investigations (OICI), are managed within the Special Investigations and Initiatives Unit (SIIU), and became operational during March 1997. Staffed by Supervisory Special Agents and Support professionals, the entities were established to specifically focus on crimes against children and crimes in Indian country. The OCAC addresses all crimes under the FBI's jurisdiction that in any way involve the victimization of children, providing program management and field wide investigative oversight of those critical FBI operations. Likewise, the OICI addresses crimes in Indian country, providing program management and investigative oversight of those sensitive FBI operations. The SIIU, OCAC and OICI work closely with FBI field offices, other FBI components, and various other entities including the National Center for Missing and Exploited Children (NCMEC), to provide and coordinate operational support to more effectively address crimes against children.

FBI Field Offices. Individual FBI field offices throughout the country serve as the primary point of contact for persons requesting FBI assistance. Special agents assigned as Crimes Against Children Coordinators use all available resources--including investigative, forensic, tactical, informational, and behavioral science--in the investigation of crimes against children. The special agents coordinate their investigations with appropriate local law enforcement agencies, as well as with Federal or State prosecutors. Upon receiving notification that a child has been abducted, FBI Evidence Response Team personnel may be assigned immediately to conduct the forensic investigation of the abduction site and any other appropriate areas, while other special agents typically join law enforcement personnel in coordinating and conducting the comprehensive neighborhood investigation that is vital to the resolution of these cases. A Rapid Start Team may also be deployed immediately to begin the overwhelming task of coordinating and tracking the investigative leads, which often number in the thousands during protracted child abduction investigations. Special Agents will also coordinate child abduction investigations with NCMEC and other entities to make full use of all available resources.

National Center for the Analysis of Violent Crime. The National Center for the Analysis of Violent Crime (NCAVC) is a rapid response element of the FBI's Critical Incident Response Group (CIRG). The unit has primary responsibility for providing investigative support through profiling, violent crime analysis, technical forensic resource coordination, and application of the most current expertise available in matters involving the abduction or mysterious disappearance of children and serial murder. (Serial murder involves the killing of two or more victims in separate incidents.)

Child abductions are among the most difficult crimes to resolve and require immediate dedication of significant resources. A specialized NCAVC staff provides operational

assistance to Federal, State and local law enforcement agencies involved in these important investigations. The unit responds immediately to requests and provides onsite assistance as appropriate. NCAVC services include:

- Profiles of unknown offenders.
- Crime analysis.
- Investigative strategies.
- Interview and interrogation strategies
- Behavioral assessments.
- Trial preparation and prosecutive strategy.
- Expert testimony.
- Coordination of other resources, including FBI Evidence Response Teams and FBI Laboratory services.

Case consultations may include any or all of the services listed above. Services are provided by telephone, in writing, or in person. In some cases investigators may travel to Quantico for consultation sessions, or NCAVC members may be sent to the area of the crimes.

NCAVC can also assist in coordinating the deployment of Rapid Start, a computerized major case management support system. NCAVC maintains a close working relationship with NCMEC and can help to arrange the use of their resources, such as poster distribution and age enhancement of photographs.

Another CIRG component, the Violent Criminal Apprehension Program (VICAP), provides automated support. To assist investigators working on cases, VICAP analysts perform standard and ad hoc searches of their databases, as well as other law enforcement databases. The VICAP database contains reports submitted by participating law enforcement agencies concerning certain violent crimes, and can be used to analyze and link multiple cases.

In addition to case consultation services, NCAVC conducts research regarding child abduction and serial murder in an effort to develop further understanding of the crimes and criminals. Results of research are applied to cases and shared with the criminal justice community through publications and training.

FBI Forensic and Technical Support Services

NCAVC was created to centralize services in child abduction and serial homicide cases.

In addition to providing investigative consultation, NCAVC can coordinate the application of all FBI headquarters resources needed in particular cases.

The FBI Laboratory is the only full-service Federal forensic science laboratory serving the law enforcement community. The FBI is mandated by Title 28, CFR Section 0.85, to conduct scientific examinations of evidence, free of charge, for any duly constituted law enforcement agency in the United States. Assistance is provided through:

- Evidence response teams.
- Document services.
- Latent fingerprint services.
- Scientific analysis services (including chemistry-toxicology, DNA analysis/serology examination, explosives, firearms-toolmarks, hairs and fibers, and materials analysis.)
- Special projects (including graphic design, photographic processing, special photographic services, structural design, and visual production and video enhancement.)
- Forensic science research and training.

Detailed information about these services, including instructions for collecting, preserving and shipping evidence, can be found in the *Handbook of Forensic Science*, which is available from the Government Printing Office. The FBI's Rapid Start Team, developed since the *Handbook* was last revised, provides on-site information management services to support the handling of crisis situations. The team is capable of operating in a bivouac environment, bringing with them all equipment required.

The Special Techniques Program, established in 1993, is another part of the Information Resources Division/Engineering Section. This group uses geophysical methodology and other remote sensing equipment to search for clandestinely concealed evidence. These techniques are considered as an investigative tool only after more expedient measures have been exhausted.

Criminal Justice Information Services. Criminal justice information services provided by the FBI include a fingerprint repository and the National Crime Information Center (NCIC).

- **Fingerprint repository**. The FBI serves as the Nation's civil and criminal fingerprint repository and responds to the information needs of Federal, State,

local and international members of the criminal justice community. The FBI receives more than 34,000 fingerprint cards each day.

- **National Crime Information Center.** NCIC is a nationwide computer-based inquiry and response information system that was established in 1967 to serve the criminal justice community. NCIC's purpose is to maintain a computerized filing system of accurate, timely, documented criminal justice information that is readily available through a telecommunications network. An average of 1.3 million inquiry-response transactions per day are processed through more than 100,000 NCIC terminals.

The *Handbook of Forensic Science* describes technical Services of the Criminal Justice Information Services Division and the Information Resources Division of the FBI.

Training

The FBI offers an extensive training program for the law enforcement community. Training in a broad spectrum of topics is offered to bonafide law enforcement personnel in settings throughout the United States, around the world, and at the FBI Academy. Each FBI field office has a training coordinator. International requests for training can be made through the FBI Legal Attaches at American Embassies.

Victim-Witness Assistance

Each FBI field office has a victim-witness coordinator. The FBI's Victim-Witness Assistance Program operates on a referral basis for victims of Federal violations.

Availability of Services

Recipients of FBI services include law enforcement agencies and the U.S. Government (hence the citizens of the United States). Services can be accessed by a request from a law enforcement agency, either through the Child Abduction and Serial Killer Unit or through the local FBI field office or Legal Attache.

Legislative Citations

FBI investigations involving child victimization are based upon violations of Federal statutes, including the crime of Kidnaping (Title 18, U.S. Code, Sections 1201 and 1202); International Parental Kidnaping Act (Title 18, U.S. Code, Section 1204); Unlawful Flight to Avoid Prosecution (UFAP) - Parental Kidnaping (Title 18, U.S. Code, Section 1073); crimes committed in Indian country (Title 18 U. S. Code, Section 1153); child sexual abuse (Title 18, U.S. Code, Sections 2241, 2242, 2243, and 2244); sexual

exploitation of children (Sections 2251, 2251A, 2252, and 2258); interstate transportation of obscene material (Sections 1462, 1465, and 1466); interstate transportation of children for sexual activity (Sections 2421, 2422, 2423, and 2424); Child Support Recovery Act (Title 18, U. S. Code, Section 228), and in some instances the RICO statute (Title 18, U.S. Code, Section 1961).

Agency Contact

For further information about services or to request immediate FBI assistance, contact one of the local FBI Crimes Against Children Coordinators or contact one of the units listed below:

FBI Headquarters
Special Investigations and Initiatives Unit
Office of Crimes Against Children
Office of Indian Country Investigations
935 Pennsylvania Avenue, NW, Room 11163
Washington, D.C. 20535-0001
Telephone: (202) 324-3666
Fax: (202) 324-2731

National Center for the Analysis of Violent Crime
Federal Bureau of Investigation
Quantico, VA 22135
Telephone: (540) 720-4700
Fax: (540) 720-4790

Section #6

FBI Crimes Against Children Coordinators

Crimes Against Children Coordinators

FO	Name	Squad or RA	Telephone	Fax
AL	E. K. Wilson	HQ/Squad 5	(518) 465-7551	(518) 431-7463
AL	Lionel Shapiro	Rutland RA	(802) 773-6455	(802) 773-2733
AQ	John Schum	HQ/VC	(505) 224-2349	(505) 224-2276
AQ	Molly A. Amman	Farmington RA	(505) 564-7520	(505) 564-7754
AN	Bruce Milne	Fairbanks RA	(907) 452-3250	(907) 456-2282
AT	Alan Sosebee	HQ/Squad 7	(404) 679-6392	(404) 679-9081
AT	Kelly Wade	HQ/Squad 11	(404) 679-6106	(404) 679-9081
BA	Barry Maddox	HQ/Squad 2	(410) 281-0225	(410) 281-0339
BA	Allison M. Mourad	MMOC	(301) 586-4519	(301) 586-4499
BH	George C. Moore, III	HQ/Squad 3	(205) 715-0300	(205) 715-0232
BH	Michelle R. Stafford	HQ/Squad 3	(205) 715-0300	(205) 715-0232
BS	James Grant	HQ/Squad C-6	(617) 742-5533	(617) 223-6327
BS	Neil Cronin	HQ/Squad C-7	(617) 742-5533	(617) 223-6327
BF	Thomas Doktor	HQ/Squad 6	(716) 843-5254	(716) 843-5288
BF	Frank Runles	Niagara Falls RA	(716) 285-9215	(716) 286-3773
CE	Mark Rozzi			
CE	Mark Aysta	Ashville RA	(704) 253-1643	(704) 252-9447
CG	Linda Krieg	HQ/VCTF	(312) 786-2758	(312) 786-2525
CG	Patrick Crouch	HQ/VCTF	(312) 786-2943	(312) 786-2525
CI	Harry Trombitas	Columbus RA	(614) 224-1183	(614) 433-6235
CI	Karen Fannin	Dayton RA	(937) 222-7485	(937) 234-1008
CV	Richard Wrenn	HQ/Squad 3	(216) 622-6731	(216) 622-6717
CV	Robin Rhoads	HQ/Squad 6	(216) 622-6764	(216) 622-6717
CV	Jane Pearson	Elyria RA	(440) 240-1452	(440) 240-1462
CO	Cynthia J. McCants	Charleston RA	(843) 722-9164	(843) 577-2286
CO	Wesley Holbrook	Aiken RA	(803) 648-0728	(803) 649-1486

(Rev.6/24/1999)

FO	Name	Squad or RA	Telephone	Fax
DL	Joe Ullmann	HQ/VC	(214) 922-7324	(214) 922-7608
DL	Mike Flinchbaugh	HQ/VC	(214) 922-7281	(214) 922-7608
DN	Joseph Schwecke	HQ/Squad 3	(303) 628-3223	(303) 629-7171
DN	Michael Howell	HQ/Squad 3	(303) 628-3270	(303)-629-7171
DE	Roy Johnson	St. Joseph RA	(616) 982-0390	(616) 982-1758
DE	William Townley	HQ/Squad C-4	(313) 237-4226	(313) 237-4009
DE	Maria Llompart	HQ/Squad C-4	(313) 237-4148	(313) 237-4009
EP	Kent Switzer	HQ/Squad 9	(915) 832-5000	(915) 521-4287
EP	Andrea Simmons	HQ/Squad 9	(915) 832-5000	(915) 521-4287
EP	Hans Martin	Midland RA	(915) 570-0255	(915) 683-4855
HN	Anthony Cardon	HQ/Squad 6	(808) 566-4467	(808) 566-4470
HN	Garold W. Hewitt	Saipan RA	(670) 234-6934	(670) 234-6783
HO	Mark Young	HQ/VC-1	(713) 693-1840	(713) 693-3879
HO	David Resch	Texas City RA	(409)935-7327	(409)935-7972
IP	William Wagoner	HQ/Squad 4	(317) 639-3301	(317) 321-6193 X-276
IP	Ruth Hovey	South Bend RA	(219) 233-4488	(219) 233-4574
JN	Jeffery Artis	HQ/Squad 3	(601) 360-7713	(601) 360-7550
JN	Dale Killinger	Oxford RA	(601) 234-1713	(601) 234-1714
JK	Tracy Cunningham	HQ/Squad 2	(904) 721-1211	(904) 727-6242
JK	John Patarini	Ft. Walton Beach	(850) 862-1722	(850) 862-1926
KC	Robert Novotny	HQ/Squad 5	(816) 691-8200	(816) 691-8312
KC	Dirk Tarpley	HQ/Squad 3	(816) 691-8200	(816) 691-8312
KX	Steven Chopin	Oak Ridge RA	(423) 482-7122	(423) 482-6192
KX	Roderick Walls	HQ/VC	(423) 544-3620	(423) 544-3624
LV	Kip Steele	Carson City RA	(775) 882-1248	(775) 883-8194
LV	Roger Young	HQ/Squad 5	(702) 385-1281	(702) 383-3519
LA	April Brooks	HQ/Squad C-4	(310) 996-4235	(310) 996-4083
LA	Jim Nice	HQ/Squad C-4	(310) 996-4235	(310) 996-4083

FO	Name	Squad or RA	Telephone	Fax
LS	Brian Blanchard	HQ/Squad 3	(502) 569-3804	(502) 569-3869
LS	Gail Thomas	London RA	(606) 877-6009	(606) 878-2557
LR	Jimmie Caudle	Fort Smith RA	(501) 478-7154	(501) 783-9528
LR	Jill Hill	HQ/Squad 2	(501) 228-8469	(501) 228-8545
ME	Joseph N. Rinehart	HQ/VC	(901) 747-9546	(901) 747-9621
ME	Lisa Lancaster	Nashville RA	(615) 292-5159	(615) 460-7159
MM	Sandra Farrow	HQ/Squad C-3	(305) 787-6681	(305) 787-6160
MM	Deborah Cool	HQ/Squad C-3	(305) 957-7410	(305) 787-6160
MW	Dale G. Mueller	HQ/Squad 6	(414) 291-4282	(414) 276-6560
MW	Gerald Mullen	Green Bay RA	(920) 432-3868	(920) 432-7505
MP	Richard Waldie	St. Paul RA	(651) 291-7100	(612) 291-0912
MP	Richard Fuhrman	Bismarck RA	(701) 223-4875	(701) 223-0002
MP	Kevin McGrane	Pierre RA	(605) 224-1331	(605) 224-2909
MO	Charles Spaht	HQ/VC	(334) 415-3205	(334) 415-3235
MO	Margaret Faulkner	Montgomery RA	(334) 263-1691	(334) 241-9823
NK	James Furry	FTRA	(732) 805-0463	(732) 469-7988
NK	Daniel Garrabrant	HQ/C-13	(973) 622-9287	(973) 456-9244
NH	Lisa Tutty	HQ/Squad 8	(203) 630-5948	(203) 630-5998
NH	Thomas Veivia	North RA	(203) 630-5912	(203) 630-5998
NO	Barbara O'Donnell	HQ/Squad 5	(504) 592-8179	(504) 595-5749
NO	Niki Williams	Monroe RA	(318) 387-0773	(318) 387-6704
NY	Shelley Doherty	HQ/Squad C-20	(212) 384-1000	(212) 384-4104
NY	Brenda Heck	HQ/Squad C-20	(212) 384-1000	(212) 384-4104
NY	Cynthia Leonardatos	HQ/Squad C-20	(212) 384-1000	(212) 384-4104
NF	Patricia Coureas	HQ/Squad 6	(757) 455-2641	(757) 455-2647
NF	Paul Gray	Peninsula RA	(757) 727-7933	(757) 727-8233
OC	Mike Beaver	HQ/Squad 5	(405) 290-3658	(405) 290-3961
OC	Robert Nixon	Tulsa RA	(918) 665-5218	(918) 665-5235

FO	Name	Squad or RA	Telephone	Fax
OM	Scott McMillion	HQ/Squad 5	(402) 492-3757	(402) 492-3799
PH	Kathleen E. Canning	HQ/Squad 10	(215) 418-4158	(215) 418-4160
PH	Matthew L. Mullin	Lansdale RA	(215) 368-6550	(215) 368-9549
PH	Stephen D. Ford	Lansdale RA	(215) 368-6550	
PX	Mike Conrad	HQ/Squad 7	(602) 650-3082	(602) 650-3078
PX	Robin Andrews	Tucson RA	(520) 791-6862	(520) 791-6883
PG	John Paul Bokal, Jr.	Charleston, WV RA	(304) 346-3232	(304) 346-9303
PG	Denise R. Valentine	HQ/Squad 6	(412) 456-9312	(412) 456-9166
PG	Gregory Curtis	Erie RA	(814) 452-4516	(814) 453-6536
PG	Raymond West	Martinsburg RA	(304) 263-3421	(304) 267-5824
PD	Adrienne Sparrow	HQ/Squad 3	(503) 224-4181	(503) 423-9746
PD	Donald McMullen	Salem RA	(503) 362-6601	(503) 585-5667
RH	Jean Lees Wyant	HQ/Squad 3	(804) 261-1044	(804) 261-8077
RH	John Jerome Kuhn	Fredericksburg RA	(540) 373-2862	(540) 373-6883
SC	William Nicholson	HQ/VC	(916) 977-2248	(916) 977-2300
SC	Jeff Rinek	HQ/VC	(916) 977-2265	(916) 977-2300
SL	Dennis Rice	HQ/VCMO	(314) 589-2500	(314) 589-2636
SL	Jan Hartman	HQ/VCMO	(314) 589-2534	(314) 589-2636
SU	Augustus M. Fennerty	HQ/Squad C-2	(801) 579-4435	(801) 579-4500
SU	Mary Martin	Boise RA	(208) 344-7843	(208) 344-7847
SA	Nancy Fisher	HQ/Squad 5	(210) 978-5354	(210) 302-8676
SA	Nancy Houston	Austin RA	(512) 794-3048	(512) 346-5265
SA	Tamara White	McAllen RA	(956) 928-4027	(956) 687-8715
SD	Kay Baker	HQ/Squad 6	(619) 514-5544	(619) 514-5881
SD	David Bowdich	HQ/Squad 6	(619) 514-5714	(619) 514-5881
SF	Jerry Webb	Oakland RA	(510) 251-4154	(510) 451-1660
SF	Sean Wells	San Jose RA	(408) 998-5633	(408) 535-4696
SJ	Sandra Blain	HQ/Squad 4	(787) 277-7008	(787) 277-7000

FO	Name	Squad or RA	Telephone	Fax
SJ	Hector G. Gonzalez	HQ/Squad 4	(787) 277-7010	(787) 277-7000
SE	Faye Greenlee	HQ/Squad 4	(206) 667-0153	(206) 667-0189
SE	Diane Drake	HQ/Squad 8	(206) 521-5763	(206) 521-5783
SI	Terry Moody	HQ	(217) 535-4418	(217) 535-4400
SI	Donald Freese	Fairview Hts RA	(618) 624-6248	(618) 624-7285
TP	Diane Farrington	HQ/Squad 4	(813) 273-4566	(813) 272-8019
TP	Francis Jarrett	HQ/Squad 4	(813) 272-8141	(813) 272-8019
WF	Kathleen Murphy	HQ/Squad C-4	(202) 278-2375	(202) 278-2609
WF	Karen Nester	HQ/Squad C-4	(202) 278-2393	(202) 278-2609

NCAVC - INNOCENT IMAGES PROFILERS

James Clemente	CIRG	(540) 720-4700	(540) 720-4790
Jennifer Eakin	CIRG	(540) 720-4700	(540) 720-4790

NEWS

Department of the Treasury
U.S. CUSTOMS SERVICE

FOR IMMEDIATE RELEASE
September 2, 1998
98-105

CONTACT: Bill Anthony
(202) 927-0549

U.S. CUSTOMS CONDUCTS 32 RAIDS IN 22 STATES IN WORLDWIDE CHILD PORNOGRAPHY INVESTIGATION

The U.S. Customs Service today executed 32 Federal search and seizure warrants in 22 states around the United States to search for evidence in an investigation of a worldwide child pornography trading ring that involves more than 100 suspects in 14 countries around the world. Search warrants and arrests are taking place simultaneously around the globe today. The investigation is part of a global investigation that stems from information the U.S. Customs Service developed during a highly publicized 1996 investigation of a child pornography trading and molestation ring.

"The people who exploit children in this way think they can hide in cyberspace," said Raymond W. Kelly, Commissioner of the U.S. Customs Service. "They are wrong. We will find them and bring them to justice."

During Customs' 1996 investigation, intelligence information led to the discovery of several international participants in that ring. Information on the international participants was turned over through U.S. Customs Attache offices to the appropriate law enforcement authorities in those countries, including the United Kingdom, Australia, Canada and Finland. The investigation and subsequent arrests of the British suspects in 1997 and 1998 led police to another larger and more sophisticated international child pornography trading ring. The British police opened an investigation into the ring and began finding subjects throughout the world – more than 100 in 14 countries to date. Each member had to have multiple images of child pornography in order to join, some as many as 10,000. Most of those subjects were in the United States, and information on these subjects was turned over to the U.S. Customs Service.

The U.S. Customs Service opened the U.S. portion of the investigation, to investigate U.S. suspects. The challenges of coordinating an international investigation in which suspects could tip each other off if contacted individually by police, coupled with evidence that active molestations may have been taking place, has placed this investigation on the fast track for law enforcement agencies throughout the world, giving rise to today's simultaneous worldwide activity.

Customs opened the first federal law enforcement investigation into computer child pornography in 1989 and the first federal law enforcement investigation into Internet child pornography in 1993. Since then, Customs has become a recognized leader in Internet and other computer-related child pornography investigations.

(more)

From the beginning of Fiscal Year (FY) 1998 on October 1, 1997 to July 31, 1998 (the most current data available), the U.S. Customs Service has arrested 183 individuals on charges relating to the possession, manufacture and/or distribution of child pornography. 189 individuals have been convicted so far during this fiscal year, and 181 indictments have been returned. During FY-1997, Customs arrested 173 individuals on child pornography charges. There were 158 indictments and 178 convictions in FY-97. (Figures do not correspond on a one-to-one basis due to the multi-year nature of investigations, arrests, and the judicial process of prosecution.)

###

DIRECTORY of SAiCs offices with associated RAiCs & RAs
5/19/99 10:37 AM

SAiC BALTIMORE, MD (410) 962-2620

RAiC Philadelphia, PA	(215) 597-4305
RAiC Pittsburgh, PA	(412) 395-4970
RA Harrisburg, PA	(717) 782-4050
RAiC Washington, DC	(703) 709-9700

SAiC BOSTON, MA (617) 565-7400

RAiC Bangor, ME	(207) 942-7239
RAiC Portland, ME	(207) 771-3628
RAiC Burlington, VT	(802) 951-6200
RAiC Derby Line, VT	(802) 873-3277
RAiC New Haven, CT	(203) 773-2155

SAiC BUFFALO, NY (716) 551-4375

RAiC Albany, NY	(518) 431-4031
RAiC Rouses Point, NY	(518) 297-6661
RA Alexandria Bay, NY	(315) 482-3747
RA Massena, NY	(315) 769-3739

SAiC NEW YORK, NY (212) 637-3900

Assoc. AiC JFK Airport	(718) 553-1824
Assoc. AiC Long Island, NY	(516) 471-2099
Assoc. AiC Newark, NJ	(973) 776-5500

SAiC ATLANTA, GA	(770) 994-4200
RAiC Charleston, SC	(843) 745-9290
RAiC Charlotte, NC	(704) 679-6140
RAiC Greenville, SC	(864) 235-0519
RA Columbia, SC	(803) 765-5430
RAiC Norfolk, VA	(757) 441-6533
RAiC Savannah, GA	(912) 652-4341
RAiC Wilmington, NC	(910) 815-4899
SAiC MIAMI, FL	(305) 597-6000
RAiC Fort Lauderdale, FL	(954) 356-7383
RAiC Fort Pierce, FL	(561) 461-1293
RAiC Key Largo, FL	(305) 664-5380
RAiC Key West, FL	(305) 294-3877
RAiC West Palm Beach, FL	(561) 659-4606
SAiC TAMPA, FL	(813) 348-1881 SAC/TA
RA Sarasota, FL	(941) 747-4800
RAiC Cocoa Beach, FL	(407) 452-3700 RAC/CB
RAiC Ft. Myers, FL	(941) 461-3114
RAiC Jacksonville, FL	(904) 232-2611
RAiC Tallahassee, FL	(850) 942-8802
RA Panama City, FL	(850) 763-8418
RA Pensacola, FL	(850) 434-6648
RAiC Orlando, FL	(407) 648-6847
SAiC SAN JUAN, PR	(787) 729-6975
Air/Marine Smuggling Div	(787) 882-3530
RAiC Fajardo, PR	(787) 860-7000
RAiC Mayaguez, PR	(787) 831-3346
RAiC Ponce, PR	(787) 841-3108
RAiC St. Thomas, USVI	(340) 693-2250

SAIC Chicago, IL 312-353-8450

RA Milwaukee, WI	(414) 297-3231
RAIC Chicago O'Hare, IL	(773) 825-6029
RAIC Cincinnati, OH	(606) 578-4600
RAIC Cleveland, OH	(216) 522-4292
RAIC Columbus, OH	(614) 469-5705
RAIC Indianapolis, IN	(317) 248-4151
RAIC Kansas City, MO	(816) 374-6426
RAIC Minneapolis, MN	(612) 348-1300
RAIC St. Louis, MO	(314) 539-6740

SAIC DETROIT, MI (313) 226-3166

RAIC Grand Rapids, MI	(616) 235-3936

SAIC NEW ORLEANS, LA (504) 670-2416

RAIC Baton Rouge, LA	(225) 389-0433
RAIC Birmingham, AL	(205) 731-0077
RAIC Gulf Shores, AL	(334) 981-5711
RAIC Gulfport, MS	(228) 864-1274
RA Jackson, MS	(601) 965-5234
RAIC Houma, LA	(504) 851-0179
RAIC Lafayette, LA	(318) 262-6619
RAIC Lake Charles, LA	(318) 477-2112
RAIC Little Rock, AR	(501) 225-2291
RAIC Memphis, TN	(901) 544-4140
RAIC Mobile, AL	(334) 441-6146
RAIC Nashville, TN	(615) 781-5473
RAIC Shreveport, LA	(318) 676-3350

SAiC SAN ANTONIO, TX (210) 308-4571

RAiC Austin, TX	(512) 916-5888
RAiC Brownsville, TX	(956) 542-7831
RAiC Del Rio, TX	(830) 703-2000
RAiC Eagle Pass, TX	(830) 773-7877
RAiC Falcon Dam, TX	(956) 848-5243
RAiC Laredo, TX	(956) 726-2213
RAiC McAllen, TX	(956) 682-1366
RAiC San Angelo/Midland	(915) 942-6900

SAiC EL PASO, TX (915) 633-7200

PDN-OI office, El Paso	
RAiC Albuquerque, NM	(505) 821-0433
RAiC Alpine, TX	(915) 837-5889
RAiC Deming, NM	(505) 546-2759
RAiC Las Cruces, NM	(505) 527-6944
RAiC Presidio, TX	(915) 229-3960

SAiC HOUSTON, TX (281) 985-0500

RAiC Beaumont/Port Arthur	(409) 839-2401
RAiC Corpus Christi, TX	(512) 888-3501
RAiC Dallas, TX	(214) 880-9800
RAiC Galveston, TX	(409) 766-3791
RAiC Oklahoma City, OK	(405) 319-6437

SAiC TUCSON, AZ (520) 670-6026

RAiC Ajo, AZ	(520) 387-7640
RAiC Bisbee, AZ	(520) 342-7827
RAiC Douglas, AZ	(520) 364-1218
RAiC Naco, AZ	(520) 432-5349
RAiC Nogales, AZ	(520) 377-3100
RAiC Phoenix, AZ	(602) 640-2036
RAiC Sells, AZ	(520) 383-2711
RAiC Sierra Vista, AZ	(520) 458-7528
RAiC Three Points, AZ	(520) 822-1808
RAiC Yuma, AZ	(520) 344-0088

SAiC DENVER, CO (303) 784-6480

RAiC Anchorage, AK	(907) 271-2880
RAiC Astoria, OR	(503) 325-4644
RAiC Portland, OR	(503) 326-2711

SAiC LOS ANGELES, CA (310) 514-6231

RAiC Las Vegas, NV	(702) 388-6732
RAiC Los Angeles Airport	(310) 215-2200
RAiC Oxnard, CA	(805) 988-8690
RAiC Riverside, CA	(909) 276-6664
RAiC Irvine, CA	(714) 836-2293

SAiC SAN DIEGO, CA (619) 744-4600

RAiC El Centro, CA	(760) 353-9090
RAiC Oceanside, CA	(760) 722-6616
RAiC San Ysidro, CA	(619) 671-4500

SAiC SAN FRANCISCO, CA (415) 705-4070

RA Fresno, CA	(559) 487-5353
RAiC Agana, Guam	(671) 472-7265
RAiC Honolulu, HI	(808) 541-2623
RAiC Reno, NV	(775) 784-5727
RAiC Sacramento, CA	(916) 498-5728
RAiC Salt Lake City, UT	(801) 524-5884
RAiC San Jose, CA	(408) 535-5155
RAiC San Francisco Airport	(650) 876-2837

SAiC SEATTLE, WA (206) 553-7531

Sea-Tac, Seattle SAiC	
RAiC Bellingham, WA	(360) 734-7557
RAiC Blaine, WA	(360) 332-6725
RAiC Grand Forks, ND	(701) 746-1157
RAiC Great Falls, MT	(406) 727-8750
RAiC Port Angeles, WA	(360) 452-4122
RAiC Spokane, WA	(509) 353-3130
RAiC Tacoma, WA	(253) 383-7932

fact sheet

Department of the Treasury / United States Customs Service / Washington, D.C. 20229

CUSTOMS CYBER SMUGGLING CENTER

Every crime that can be committed in the "real" world can be committed or facilitated using computers and the Internet. From money laundering and child pornography, from drug smuggling to trafficking in weapons of mass destruction, from copyright fraud to economic terrorism, even to planning murder and kidnaping, the criminal underworld saw early on the criminal potential of computers and the Internet and has taken full advantage of that vast potential.

The U.S. Customs Service began investigating crimes committed on computers in 1989, when it opened the first federal law enforcement investigation into child pornography transmitted via computer. Customs realized then that computer crimes were the criminal wave of the future, and began preparing to deal with that wave. That first investigation led to the drafting of the first federal warrant to search a computer for child pornography, and began setting precedents for computer investigations worldwide.

As the Customs Service gained more expertise in investigating computer and Internet child pornography crimes, agents began to see the potential for other criminal activity on the Internet. Customs had set the standard for computer investigations with the battle against computer child pornography, and Customs reached to set the standard for the move of federal law enforcement into cyberspace.

In August, 1997, the Customs Service formally expanded its Internet investigations with the creation of the Customs CyberSmuggling Center. The CyberSmuggling Center brings together all Customs Service assets dedicated to the investigation of international criminal activity conducted on, or facilitated by, the Internet.

Customs CyberSmuggling Center's areas of responsibility, in addition to child pornography investigations, include international money laundering, international drug trafficking, intellectual property rights violations (including music and software), trafficking in environmental contaminants, illegal arms trafficking and traffic in weapons of mass destruction, and international economic espionage.

fact sheet

Department of the Treasury / United States Customs Service / Washington, D.C. 20229

SAVING CHILDREN:
U.S. CUSTOMS CHILD PORNOGRAPHY PROGRAM

Children have always been vulnerable to all types of exploitation -- economic, social, and sexual. Pedophiles, child molesters, sexual deviants, purveyors and consumers of child pornography continue to try and find new ways to practice their deviant habits by exploiting vulnerable children. While the traffic in hardcopy video and print child pornography has decreased in the last decade, these criminals have increasingly turned to computers to find children to abuse and child pornography to use. The quantum increase in the availability of home computers to households around the country has given the purveyors and consumers of child pornography a new and -- they believe -- relatively anonymous avenue to pursue this illegal traffic.

The U.S. Customs Service has always been the front line of defense against the illegal trafficking and distribution of child pornography into and throughout the United States. Before 1977, the Customs Service seized child pornography entering the United States under obscenity statutes. In 1977, Congress enacted the first anti-child-pornography law, but the authority to seize was still under obscenity statutes. In 1984, Congress enacted the Child Protection Act of 1984 which gives the Customs Service the authority to investigate any cases which involve the receipt, transmission, manufacture, or possession of child pornography which has been shipped in foreign commerce. In 1988, Congress passed a law outlawing the use of computer to transmit, manufacture or possess child pornography which has been shipped in foreign commerce, thus opening the door to Customs computer investigations, the first of which was launched in 1989.

The U.S. Customs Service created its first anti-child-pornography program in 1985. The Child Pornography Enforcement Program provided administrative, programmatic, and operational support to all U.S. Customs field offices and Customs Attaches. The Program established close working relationships that continue today with Department of Justice, Child Exploitation and Obscenity Section, the National Center for Missing and Exploited Children, the FBI, the U.S. Postal Inspection Service, and various military investigative commands. The Program also worked closely and successfully with Customs Office of Field Operations in finding methods used by pornographers to smuggle child pornography into the United States.

Although Customs' efforts in keeping hard copy print and video child pornography from entering the United States were largely successful, the advent of the easily-affordable home computer changed the equation. In 1989, the Customs Service opened the first federal law enforcement investigation into the illegal transmission of child pornography via computer, after

recognizing that the computer was increasingly becoming the venue of choice for pedophiles, child molesters, and other purveyors of child pornography to gain wider, easier and safer access to child pornography and to children.

Customs investigations into computer child pornography expanded in the early 1990s to include child pornography transmitted via the Internet, as pedophiles discovered the ease with which they could traffic in child pornography on the information superhighway. To further combat both traditional and computer-based forms of child pornography and exploitation, Customs created the U.S. Customs Service International Child Pornography Investigation and Coordination Center (ICPICC) in April 1996. Staffed by special agents with expertise in child pornography cases and computers, the Center provides guidance, support and coordination to the field in the investigation of cases involving child pornography violations. The Center also coordinates the U.S. Customs Service international efforts to combat child pornography, and trains state, local and foreign law enforcement officials in child pornography investigations. The Center compiles and analyzes child pornography related intelligence, and coordinates Customs child pornography investigations in the field in order to make maximum use of scarce resources.

In August, 1997 the U.S. Customs Service formally expanded its Internet investigations to all types of Internet criminal activity under Customs jurisdiction with the creation of the Customs CyberSmuggling Center, which incorporates the child pornography investigation program.. Customs CyberSmuggling Center brings together all U.S. Customs assets dedicated to the investigation of international criminal activity conducted on, or facilitated by, the Internet.

Customs CyberSmuggling Center's areas of responsibility, in addition to child pornography investigations, include international money laundering, international drug trafficking, intellectual property rights violations (including music and software), trafficking in environmental contaminants, illegal arms trafficking and traffic in weapons of mass destruction, and international economic espionage.

U/C Caller_____ Time started_____
Date_____ Time ended _____
Recorded Yes/No

Uplink Network Corporation, P.O.Box 4000 Bridgeton, Mo.63044-9718

Survey questionnaire

Hello, my name is Cathy of the Uplink Network Corporation. We are offering ten free hours of Online service on any of the commercial online service of your choice (PRODIGY, DELPHI, COMPUSERVE or AMERICA ONLINE) for answering our questions. It will only take about two minutes of your time and we will send you via mail our software with the ten free hours of usage for your input.

1. What type of computer do you own ?
   A.

2. Do you own a modem, if so what baud speed?
   A. Internal or external
   B. What brand

3. Do you own any other type of computer such as a lap top?
   A. Does it have a modem/what speed

4. Who in your household uses the computer most frequently?

5. Which computer do you utilize most frequently?

6. Do any of your computers have multimedia capability?

7. Is it utilized for business, childrens homework, entertainı

8. Are you a member of any online service? If so which?

9. What do you like most about your online service?

10. What do you dislike most of your online service?

11. Do you own or are a Systems Operator of any bulletin b

12. What times do you use your computer most frequently; afternoon hours?

13. Do you most frequently use it at home or at work?

14. What is your occupation?

15. And, what software would you like to have sir/mam? We have Delphi, America Online, Compuserve, Prodigy and Imagination Network.

16. Where can I mail the software to? (Be sure to get his/her name with the address!)

Thank you for assisting us in our survey and your software should arrive within 12 to 14 work days.

"VICTIMS OF INNOCENCE"

Child Pornography and the Sexual Exploitation of Children: A Perspective From The United States of America

Prepared By: *Raymond C. Smith*
U.S. Postal Inspector - Program Manager
U.S. Postal Inspection Service
Office of Criminal Investigations
475 L'Enfant Plaza West, SW
Washington, DC 20260-2166

INTRODUCTION TO CHILD PORNOGRAPHY

The sexual exploitation of children through pornography is a continuing tragedy that crisscrosses all social and economic classes, with little regard for the enduring grief and trauma it brings to its victims. We have come to realize that child pornography is not simply an "art form." It is, rather, the end product of deviant behavior resulting in the sexual molestation and abuse of children.

During the past several years, the public has become increasingly more aware of the proliferation of sexually oriented materials involving the abuse of children. These materials graphically depict children, sometimes as young as two years of age, engaged in a variety of explicit homosexual and heterosexual activities appearing in full-color magazines, slides, photographs, movie films, video tapes, and now, picture quality computer images.

Due to public outcry, and a series of well-publicized incidents involving child exploitation and abuse, state and local law enforcement efforts in the United States have all but eliminated the over-the-counter sale and viewing of child pornography throughout the country. Child pornographers and pedophiles now use the United States Mail and computers to traffic in this insidious material because they can buy, sell, trade, and remain somewhat anonymous. It is this cloak of anonymity and the compulsive nature of the pedophiles need to not only amass greater quantities of child pornography, but also to validate their behavior with others that has given the child pornographer the drive to engage in this criminal activity.

Child pornography is a permanent record of the sexual abuse and exploitation of children. The dangers of child sexual exploitation cannot and should not be minimized. This most despicable of crimes -- a crime against children -- results in physical and emotional suffering, ruined lives, and shattered dreams. Only through public awareness, vigorous investigation, certain prosecution and just sentencing can we hope to reduce this horrible crime.

THE U.S. POSTAL INSPECTION SERVICE

The U.S. Postal Inspection Service is the law enforcement arm of the United States Postal Service responsible for investigating crimes involving the U.S. Mail, including all child pornography and child sexual exploitation offenses. Postal Inspectors specially trained to conduct these investigations are assigned to each of its 30 field divisions nationwide. U.S. Postal Inspectors, as federal law enforcement agents, carry firearms, serve warrants and subpoenas, and possess the power of arrest.

Recognizing that preferential child molesters and child pornographers[1] often seek to communicate with one another through what they perceive as the security and anonymity provided by the U.S. Mail, Postal Inspectors have been involved extensively in child sexual exploitation and pornography investigations since 1977. Since the enactment of the federal Child Protection Act of 1984, Postal Inspectors have conducted over 2,500 child pornography investigations, resulting in the arrests and convictions of more than 2,200 child pornographers and preferential child molesters.

Postal Inspectors in the United States utilize an established, nationwide network of intelligence in implementing a wide variety of undercover programs designed to uncover suspects and develop prosecutable cases. These undercover operations recognize the clandestine nature of the targets and the inherent need of many offenders to validate their behavior. The techniques utilized in these programs include placement of contact advertisements in both national and local publications, written contacts and correspondence with the subject, and more recently, contact via computer bulletin boards. Postal Inspectors are ready to assist in any related investigation involving child sexual exploitation.

---

1. Child pornographers are not always active child molesters. Conversely, many child molesters are not involved in child pornography. Both types of offenders may use the U.S. Mail to correspond with others who share their interests.

The Postal Inspection Service has had specific responsibility for investigating the mailing of obscene matter for over a century (Title 18 U.S. Code, Section 1461). While over the years child pornography was, as a matter of course, investigated along with the obscenity matters, increased public concern over this material resulted in the United States Congress enacting the Sexual Exploitation of Children Act in 1977 (Title 18 U.S. Code, Section 2251-2253). The Child Protection Act of 1984 (18 USC 2251-2255) amended the 1977 Act by:

1. Eliminating the obscenity requirement.
2. Eliminating the commercial transaction requirement.
3. Changing the definition of a minor from a person under age 16 to one under age 18.
4. Adding provisions for criminal and civil forfeiture.
5. Amending the federal wiretap statute to include the Child Protection Act.
6. Raising the potential maximum fines from $10,000 to $100,000 for an individual and to $250,000 for organizations.

On November 7, 1986, Congress enacted the Child Sexual Abuse and Pornography Act of 1986 (18 USC 2251-2256) which amended the two previous acts by:

1. Banning the production and use of advertisements for child pornography.
2. Adding a provision of civil remedies for personal injuries suffered by a minor who is a victim.
3. Raising the minimum sentences for repeat offenders from imprisonment of not less than two years to imprisonment of not less than five years.

On November 18, 1988, the United States Congress enacted the Child Protection and Obscenity Enforcement Act of 1988 (18 USC 2251-2256). These amendments:

1. Make it unlawful to use a computer to transmit advertisements for, or visual depictions of, child pornography.

2. Prohibit the buying, selling, or otherwise obtaining temporary custody or control of children for the purpose of producing child pornography.

More recently, on November 29, 1990, Congress enacted an additional amendment (18 USC 2252), making it a Federal crime to possess three or more pieces of child pornography.

THE U.S. CUSTOMS SERVICE

The U.S. Customs Service, Office of Enforcement, has Special Agents in every field office responsible for conducting child exploitation investigations. In addition, the Customs Service has foreign mail facilities in 22 U.S. cities that intercept illegal mailings. Every port of entry to the United States is staffed by Customs Inspectors whose responsibilities include interdicting child pornographic contraband and related articles. Customs Agents are currently involved in pro-active, undercover investigations to identify and infiltrate computer bulletin boards used for exchanging child pornography where border crossings are involved.

The Customs Service is authorized to award up to $250,000 to any individual who can provide information leading to a significant seizure or arrest in a child exploitation investigation.

Special Resources:

The Treasury Enforcement Communication Systems (T.E.C.S.) is a computer system that contains reports of investigations, arrests and seizures, and information on border-crossing from around the world. The T.E.C.S. is utilized by Customs' Special Agents on a daily basis to assist in the investigation of sexual exploitation cases.

The U.S. Customs Service also maintains a seizure list containing information about prohibited pornographic materials which have been seized at the border.

Data bases maintained by the U.S. Customs Service are accessible by other federal investigative agencies and by state and local law enforcement agencies with permission.

THE FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation (FBI) is responsible for investigating suspected cases of child sexual exploitation involving interstate commerce.

The FBI assigns particular attention and priority to investigations indicating organized criminal activity, commercialized prostitution, and the manufacture or distribution of child pornography. FBI investigations have also identified computer networks and bulletin boards, both national and international in scope, in which child pornography is transmitted to clients or other members of the network.

Within the FBI there are agents who are specially trained to investigate cases of child sexual exploitation. There is also extensive technology to enhance investigations, including lab testing of fingerprints and body fluids, video enhancement, and technology targeted to computer crimes. The Bureau also has special expertise in behavioral analysis, such as offender profiling.

CHILD PORNOGRAPHERS AND THEIR COLLECTIONS

Unlike commercial adult obscenity dealers, domestic child pornographers rarely, if ever, openly advertise or solicit new business. Their operations are underground and restricted, in many instances, to dealing with known pedophile customers. In fact, child pornography exists only for the the pedophile. A pedophile is defined as one whose erotic imagery and fantasy are focused on children. Pedophiles have an abnormal sexual desire for children; and, as a group, they are the major producers, distributors, and consumers of child pornography. Reduced to its simplest form: no pedophiles -- no child pornography.

Child pornographers and pedophiles come from all walks of life. The occupations of some of the offenders arrested in the United States include: doctors, teachers, lawyers, law enforcement officers, clergymen, and businessmen. Some have occupations bringing them into frequent contact with children. Many hold respected positions in their community and have concealed their interest in child pornography for years. The hobbies of offenders include little league baseball and football coaching, dance instructing, scout leading, baby-sitting, volunteer firemen, and amateur photography.

When, during the course of an investigation, sufficient probable cause has been developed to indicate that a suspect has violated the child pornography statutes, a federal search warrant may be sought for the suspect's residence. Execution of search warrants usually leads to the recovery of child pornography, sexually oriented correspondence, and, quite often, the identification of child victims.

To the child pornographer, his collection is one of the most important things in his life. Why else would he risk fines, disgrace, and jail? The child pornographer's collection is never complete; he must always add to it. To acquire it, he usually

uses the United States Mail, computer systems, or produces it himself. As he acquires it, he organizes his collection carefully, for he will keep it as long as he can. In most cases, because he knows what he does is illegal, the child pornographer carefully conceals his collection. Although the pedophile's collection of child pornography is oftentimes "hidden" from the casual observer, it is almost always readily accessible to him, for it is from this collection of child pornography that the pedophile derives his own sexual gratification.

More recently, over the past several years, we have seen a significant increase in computer usage by these child pornographers through computer bulletin board networks and commercially available telecommunication systems. Today's computer technology allows for the electronic transfer of picture quality images at the touch of a button and makes "letter writing" much easier. Even though the computer, in some cases, is replacing traditional correspondence, our experience has shown these computer literate child pornographers still rely heavily on the mails to exchange video tapes and computer diskettes containing the child pornography.

Of late, it has not been uncommon for law enforcement authorities to seize personal computers and related materials that hau been used to store data bearing on the identities of other pedophiles with whom the offenders have been in contact. Recent investigations, however, have revealed that pedophiles employ personal computers for purposes extending far beyond the mere storage of data. They are using them to carry out "private" conversation with persons of similar proclivities in communicating their sexual interest in and activities with children. Even more alarming today, many pedophiles are now using the computer to carryout these "private" conversations directly with children and, oftentimes, are successful in persuading the child to engage in sexual conduct with them.

Use of the mails and computers in the distribution of child pornography perpetuates the sexual abuse and exploitation of the children involved. Pedophiles believe there is nothing wrong with what they are doing, so naturally they are looking for other individuals who support their thinking. A pedophile will use "kiddie porn," both private, original material and commercial material, to seduce other children into participating in sexual activity with them. Once the pedophile seduces the child, he uses the pornography to blackmail the child into continuing the relationship or keeping their "secret" from others. The pornographer also exchanges the material with other pedophiles.

Who are the victims? Despite a popular notion that runaways and children from broken homes are the main targets of pedophiles, that is not the total answer. In most cases, the victim is the child "down the street" who has been seduced into a relationship by a trusted adult and then hides the fact because of guilt, shame, blackmail, or, in some instances, because, for the first time in their life, they have received attention and what is interpreted to be affection from an adult.

Few crimes, if any, are more heinous and detrimental to our society than the sexual exploitation of children. Governments and their respective law enforcement agencies should not have a "blind eye" toward individuals trafficking in child pornography. Through years of investigating this unlawful activity, it has become clearly evident, the most effective means to identify these individuals is through the development and implementation of pro-active undercover investigations. Generally speaking, this crime does not come "knocking at your door." It can be said, the easiest way to convince yourself that this criminal activity isn't occurring in your community is quite simple, don't look for it. In case after case, had it not been for the work of law enforcement agencies in the United States and our pro-active undercover investigative efforts, these offenders, arrested for violating U.S. laws and sexually abusing children, in all likelihood, would have never been identified and would still be abusing and exploiting children today and well into the future.

It is now time for all international governments and law enforcement agencies to unite and work together in a cooperative spirit. Our goal should be to eradicate child pornography, and in so doing, we will reduce the far too many incidents of child sexual exploitation. Only by combining our efforts, resources, and knowledge in a team approach to this hideous crime can we make a difference.

Child Sexual Abuse Kills:

The story of Justin and Matthew Wilke

In May 1985, Justin Wilke and his brother Matthew attended Camp Puh'Tok in Monkton, MD. There they met 23-year-old camp counselor Peter Dudley Albertsen II. Albertsen, ponytailed and mustachioed, befriended the youngsters, aged 9 and 11. The boys looked up to Albertsen, a seven-year veteran of the camp, who was studying to become a teacher. Pete played the dulcimer and taught arts and crafts.

Albertsen continued his friendship with Justin and Matt after camp was over. He became friends with the boys' parents, who thought of him as a wonderful "older brother" and "role model" for their boys. Albertsen began spending a large amount of time, sometimes even staying overnight, at the Wilke's residence in Upperco, MD. The parents began entrusting the boys to Albertsen's care for overnight visits at his home in Baltimore.

"This was the life," Justin would later write. "This was any kid's dream. I wanted to be as mature as Pete. And in my mind I was. I would do anything to keep the relationship. I knew that he was the best friend any kid could ever have ... so I thought."

Matt Wilke at age 12 and Justin Wilke at age 10.

During one of the weekend visits to Baltimore, Albertsen began to sexually abuse the boys.

Justin's story

It started with tickling and play wrestling. That went on for about a year. Then Albertsen began to separate the boys and play games with them in private.

One hot summer evening in 1987, Pete persuaded Justin to play a new game — Pete would be the photographer and Justin would be the model. Albertsen, who had already painted a picture of 11-year-old Justin, told the boy he wanted to do a series of pictures: one with Justin wearing jeans, then wearing just his underwear, and

then wearing nothing at all. Justin didn't like it, but Pete was his friend and he went along with it.

Albertsen set up a video recorder on a tripod to film the young boy. As Justin began to take off his clothes in front of the video recorder, Albertsen took still photographs with another camera. At some point he stopped taking pictures and began to touch Justin. He told Justin it was okay because he loved him, and that it was an expression of his love. Later, Pete took Justin out for his favorite meal of hot dogs and burritos.

Albertsen continued to abuse Justin Wilke for three years. The abuse involved making Justin participate in certain sexual acts. Albertsen often photographed Justin during these episodes.

Matthew's story

Albertsen also abused Justin's brother, Matthew Wilke, at his Baltimore home. Matt didn't tell anyone about it for a long time. Albertsen continued to abuse Matt until the boy was 13.

Matt finally confronted Albertsen. He knew what Pete was doing was wrong, and he told him so in a letter in 1988:

"I've been doing lots of thinking lately, looking over your letters. I've decided to stop coming over to your house. I saw a TV show on child pornography, and that's what started me thinking. I've also noticed that you have a book on that ... I read your poems in your book, which sounded to me like it was written for me to read. I had thought you learned from camp to stop. Obviously not. I really don't need that pressure on all the other pressure I have ..."

Albertsen responded to the 13-year-old with a letter describing his attraction to young boys. Albertsen said he "recognized" the pressure he put on Matt. He even suggested the molestation had some value. Albertsen wrote:

"As for my book on pornography, I don't have one, I have many, and before I am done I will have many more. I have never tried to hide either my feelings or my attraction to you. Throughout my life I have walked along a trail that is very close to being that of a child molester and I have been warned, reminded and reprimanded every step of the way. Why do I follow a trail that so many people have insisted that I shouldn't? Because after looking at all sides, I made up my own mind that there is something of value on that trail, something that is important to me, but also something that is important to you and Justin and something that is important to all people."

Matt wrote again to Albertsen, expressing his anger over Albertsen's abuse and telling him that he couldn't sleep because he couldn't stop thinking about what Albertsen had done to him. Albertsen responded with another letter, suggesting that Matt may have been abused by the letter of the law:

Peter Dudley Albertsen in 1990, at the time of his first arrest.

"I had no idea that this would affect our lives so badly and so completely ... I am angry at myself because I wasn't listening to the ways you were trying to tell me to stop ...

I am definitely wrong because you did not want me touch you and I did when I shouldn't have, more than for than any reason, I was wrong because now you feel molested. I don't know what that means to you. I do know that it is making you feel hurt. By the letter of the law, you can absolutely say that you were molested. Now we have to figure out what that means. You cannot say that you let it happen as you tried to stop it and it happened anyway."

Matt stopped visiting Pete, but the letters, and some contact, continued. Matthew wished he could help his brother, who was still going to see Pete at his Baltimore home, but he didn't know how to do it.

Albertsen had often told Matt that he would never have a normal relationship with a woman and that he would grow up to be a child molester himself. Matt was terrified by Albertsen's warnings. His fear only worsened when he later began to do volunteer work with abused children.

A small revenge

Pete Albertsen graduated from Towson State College in 1990. Over the years he had taught troubled children at the Children's Guild, an nonprofit center in Baltimore, and worked as a substitute teacher at Medfield Heights Elementary. After graduation, he left the states to accept a job in England tutoring fourth-graders.

While Pete was out of the country, Matt got up the courage to talk to his mother. She confronted Pete when he returned from London, and he admitted his guilt. He said he was in love with Justin. She told him to stay away from her boys.

When she found out that Pete had contacted Justin again, Mrs. Wilke went to the police. A Baltimore City grand jury indicted Peter Albertsen on charges of fondling and having oral sex with Justin, and fondling Matt.

Albertsen pleaded guilty to, and was convicted on, only one charge, a third-degree sex offense for abusing Justin. He convinced the court psychologist it was an isolated incident that would never be repeated, and that the boys had nothing to fear from him.

Albertsen got a three-year suspended sentence and five years' probation.

He was ordered to undergo therapy and have no contact with Justin or Matt.

The stalking begins

The Wilke family enrolled in counseling sessions, but quit after six visits. They weren't comfortable talking about Pete. They decided to bury the problem and keep it a secret. Mental health experts say this is the worst possible way to handle trauma.

Despite the restriction placed by the courts, Albertsen continued to pursue Justin. He began a writing campaign, mailing dozens of cards and letters to Justin, unsigned and postmarked from different places to throw off Justin's parents. He left love letters, poems and notes on Justin's car and on the cars of Justin's friends. Albertsen began secretly watching Justin and showing up at events he knew Justin would be attending.

In May 1994, Pete called Justin and told him he had watched his high school graduation from a hidden spot in the trees. He mailed Justin a letter every day for a month before his eighteenth birthday and said he would be standing in Justin's driveway that day. Included in one letter was a refrigerator magnet that spelled "Happy Birthday, Justin."

On the weekend of his birthday, Justin and a girlfriend left town. Justin was afraid that Pete would be watching him. He believed Pete would kill him if he couldn't have him.

Shortly after Justin's birthday, Albertsen left the United States for Germany on a student visa.

Coping with the damage

When Matthew and Justin attended Loyola High School in Baltimore, they were required to perform volunteer work in the community. First Matt, and later Justin, decided to volunteer at St. Vincent's Center for abused and neglected children in Baltimore County.

At St. Vincent's, the boys met and worked with children who had been sexually abused. Matt and Justin worked under the direction of Father Ray Chase, who became their friend. They told Father Ray about their abuse at the hands of Peter Albertsen.

According to Father Ray, Matt's work with one of the children at St. Vincent's, helping the child cope with the emotional consequences of his history, was wonderful. Justin worked for a year with two small girls, with whom he developed close and nurturing relationships. While the boys never discussed specifics about their own stories, Matt let Father Ray know he had told Albertsen to stay away from his brother.

Father Ray knew that Matt's chief concern was to protect Justin from Albertsen. Matt often told Father Ray he felt he had failed to protect Albertsen from abusing Justin when they were young.

In the fall of 1993, after graduating from Loyola and enrolling in college, Matt attempted suicide, but was unsuccessful. He told Father Ray, who visited him in the hospital, that he felt that the world "would be better off with him gone."

Matt feared that, because he had been abused, he would either be perceived as, or actually become, a pedophile — just as Albertsen had predicted.

Father Ray assured Matthew that this was not an automatic consequence of child abuse, but Matt didn't seem to believe him.

Painting his pain

Like his older brother, Justin never discussed specifics about his abuse by Albertsen, but he did tell Father Ray that Albertsen was stalking him and that he was afraid that Pete would kill him.

After graduating from Loyola, Justin enrolled at the Maryland Institute, College of Art. He began to develop into a skilled artist and started expressing himself in writing. Father Ray suggested a project for Justin: to create a series of paintings and writings that would depict his abuse as a child and the effect it had on him and his family. It would be a way to help others heal their wounds from sexual abuse.

Matt Wilke in 1992. He was an avid mountain biker and photographer.

Justin Wilke in 1994. He was a skilled painter, music fan and car mechanic.

Justin's first painting dealt with the pain and vulnerability of being abused. A second painting depicted Justin's dehumanizing experiences with Albertsen. A third revealed the effect of Peter Albertsen's abuse on the Wilke family. The fourth painting was intended to express to others his current state of mind, years after the abuse.

Justin finished the paintings in October 1994. He wrote three pieces to accompany his artwork, and dedicated the series to Matthew:

"This story is dedicated to my brother, two years my elder. May this help you understand me, for you are the one with whom I silently endured this trail of emotion. May these writings and artwork open a door through which we can both reflect on what has happened to us and what will happen in the future. Please try to understand me, and help me lift this wall of silence between us ... I love you, bro."

The first painting was accompanied by a short story he titled "Solitude." It revealed that Justin still viewed Albertsen as his best friend — a best friend who had betrayed him:

"I remember confusion. I remember emptiness and the sickening feeling of helplessness. I can remember the way I felt when he looked at me with that glassy stare. I can picture it. I can remember trying to imagine why Pete would want to take videotapes of me undressing. It may seem like that is an obvious sign of someone that is not mentally stable, but to an eleven-year-old, it is a bit more confusing.

I can remember how I felt physically ill after he touched me. I still remember him taking me out for hot dogs and burritos afterward as if nothing had ever happened. I can still remember him saying he loved me. I can remember hating him.

I still hate him ...."

In Justin's second painting and poem, he describes Pete's calculated actions, lies and deception. Justin's third piece, accompanied by a letter in which he prays to God to help him, describes

Father Ray Chase and Matt Wilke in April 1996.

Albertsen's impact on the Wilke family: Albertsen is depicted as Satan clutching the neck of Justin's mother, Susan, and Albertsen's house is shown with a red light in the window. In the letter, Justin speaks of Albertsen's impact on his life and the life of Justin's family.

Justin's fourth painting was completed in the fall of 1995, and portrayed the theft of his youth at Albertsen's hands. The event had reduced his childhood to a vague memory. The writing accompanying the painting revealed the devastating impact the abuse had on Justin's self-esteem.

"I cannot pinpoint the demise of my self-esteem or the fading of my concentration on life ....

I sometimes try to think of what I was or where I was before Pete. I want to know if I was happy then, but for some reason, before I was 13, I cannot remember much. Maybe I can remember smatterings of things, but nothing very solid ....

Short-term memory and attention deficit haunts me every day. The hazy image of what I once was lingers over me like a tattered tent, full of vague holes and cold drafts of unpleasant childhood memories ....

My brother, father and I do share at least one thing in common. We all hate Pete and we would give up everything we had to turn back time and avoid the hell that seemed to create the paths of the rest of our lives for us."

About one year later, St. Vincent's Center began exhibiting Justin's paintings to professionals and others in the field of child sexual abuse. It was intended to be part of a process to help people explore and understand, through Justin's art, the emotional devastation caused by child sexual abuse from the perspective of an abused child.

In 1993, Matt tried, unsuccessfully, to kill himself again, using a gun he took from a neighbor's house. When he came home from the hospital 10 days later, he found out his mother and father were separating.

A prohibited mailing

Although Pete Albertsen was in Germany on a student visa, he continued to "stalk" Justin Wilke — this time by mail.

In May 1995, Justin received a package from Germany. It was timed to coincide with his birthday.

Justin recognized the handwriting and the postmark and knew instantly who had mailed it.

In the package was a birthday card; two sealed letters, marked "A" and "B"; two photographs of Albertsen; and a videotape. The video was in a format that could not be viewed on American equipment.

Justin panicked. He was afraid the videotape contained sexually explicit scenes Albertsen had taped of him years earlier.

In the "A" letter, Albertsen told Justin the "proverbial ball is in your court," and he asked him to respond to his letter. "No answer is an answer, and in this case I will define it as 'no.' So if I don't hear 'Wait for me, I don't know, or f— off, (silence = go to hell),' next year around your birthday, I will send one last birthday card and say good-bye."

Letter "B" was 22 pages long. Albertsen went into great detail describing their relationship, including the sexual acts he had performed on Justin. Albertsen knew the letter would cause problems and wrote, "If you are still in the middle of school exams it may be better to wait until you have finished the semester before you deal with this letter."

Albertsen asked in the letter:

"Did I injure you? What is the extent and nature of the injury? Did I destroy you? What was the mechanism of the destruction? Were my actions careless? Were they criminal?"

Justin never viewed the videotape. He gave the package to Father Ray, who surrendered it to an attorney employed by the Maryland Department of Social Services. The attorney interviewed Justin and Matthew, who hired him to handle their claim against Peter Albertsen as a result of harassment and other objectionable actions.

The attorney viewed the tape and was relieved to find Justin was not on it.

"The tape contained images of children under the age of 18 engaged in sexually explicit conduct. Its mailing constituted a federal crime."

The tape contained images of children under the age of 18 engaged in sexually explicit conduct. Its mailing constituted a federal crime.

The attorney contacted the U.S. Postal Inspection Service and U.S. Customs Service.

Pete Albertsen at the time of his second arrest, the day after Christmas, 1996.

Child abuse kills

In the months following receipt of the package, Justin became anxious and depressed. Justin's father, Donald Wilke, wanted to pay for any costs associated with stopping Albertsen from stalking his son. He felt he had failed to protect his sons.

Donald was depressed about his sons' problems and his own failed marriage. On November 30, 1995, Justin found his father's body in the family car. Donald had taken his life by carbon monoxide poisoning.

Justin and Matt were traumatized by their father's suicide. Matt became quiet and kept to himself. Justin, normally an easy-going kid, was agitated and withdrawn, and he stopped talking to friends.

Justin blamed Pete Albertsen for the death of his father, at least in part, and felt he had lost his last line of defense against Albertsen's stalking. He spoke of feeling trapped.

Within a month of his father's death, Justin created a fifth painting, his last artwork. There was no writing to accompany the piece. The painting depicted his father dead in the car, just as Justin had found him. It included a photo of a pair of outstretched hands holding a baby rabbit. Justin told Father Ray that he wanted people to know that child abuse kills.

I hate you Pete

On February 8, 1996, Justin Wilke was found dead in a car behind a service station in Cockeysville, MD. The station was next to the funeral home that had handled his father's funeral. Justin had died at his own hands, by carbon monoxide poisoning. On the passenger seat next to his body was a note that read:

"Sell everything I have and donate the money to St. Vincent's. I love you all — Justin.

I hate you Pete! F— off."

Matthew Wilke was destroyed by the suicides of his brother and father. He felt he had failed miserably to protect his brother from the abuse and continued stalking by Peter Albertsen.

Matt wanted to see Albertsen brought to justice. He met and agreed to cooperate with Postal Inspectors and agents from the U.S. Customs Service to lure Albertsen back into the country. But he could not fight his sadness, his loneliness and his fear of being left alone.

On August 15, 1996, a farmer working in his field found Matt's body in a car. Like his father and brother, he had committed suicide by carbon monoxide poisoning.

Matt left a note saying that he hoped everyone would forgive him, but he could not go through a fall or winter without his father and brother. Along with the note was a teddy bear he had received as a child, a gift from his father.

Five days later, Peter Albertsen was officially charged with trafficking in child pornography via the U.S. Mail.

On December 21, 1996, U.S. Customs received information that Albertsen might have re-entered the country. Postal Inspectors and Customs agents conducted a surveillance of Albertsen's mother's home during the Christmas holidays. On December 26, 1996, Albertsen was arrested.

In an interview with Inspectors and Customs agents, Albertsen admitted that he knew Justin and Matt had committed suicide. He was sad, but did not feel responsible for the deaths.

The tragedy comes full circle

On March 21, 1997, Peter Albertsen pleaded guilty to one count of mailing child pornography to the United States.

Sentencing was set for July 11. In an emotional four-and-a-half-hour hearing, the government called only two witnesses. Postal Inspector Tom Boyle testified to the overall investigation, arrest and post-arrest interview of Peter Albertsen. Father Ray took the stand and spoke about the victims and the terrible impact Peter Albertsen had on their lives. He dimmed the lights in the courtroom, illuminated Justin's paintings and read aloud the dead boy's words. There were sobs in the audience.

The tragedy had come full circle. The one positive thing Justin had gained from his relationship with Peter Albertsen — his art — was the very thing Justin was able to use to show others his abuse and damage.

Peter Albertsen offered a few words, too, but they were not what anyone had expected. Rather than express remorse, Albertsen offended the judge and the courtroom, declaring that he had loved Justin and Matt. He said he was the only one who would remember them in 10 years' time.

U.S. District Judge William Nickerson sentenced Peter Albertsen to 10 years in prison, the statutory limit. The judge stated that the sentence was inadequate for the crime.

The unconscionable actions of Peter Albertsen had triggered the suicides of Donald, Justin and Matthew Wilke. But Albertsen's actions also sealed his own fate: If Pete had never mailed Justin the videotape of child pornography, he might never have been brought to justice.

Postal Inspectors have heard too many tales like this one. It's why the U.S. Postal Inspection Service remains committed to aggressively pursuing those who use the mail to exploit children.

Postscript

In October 1997, Albertsen admitted he had violated the terms of his original, suspended three-year sentence by mailing Justin the letters and the child pornography videotape in 1995. The three-year sentence was therefore reinstated, and added on to the ten-year sentence Albertsen is already serving.

Preventing Child Abuse

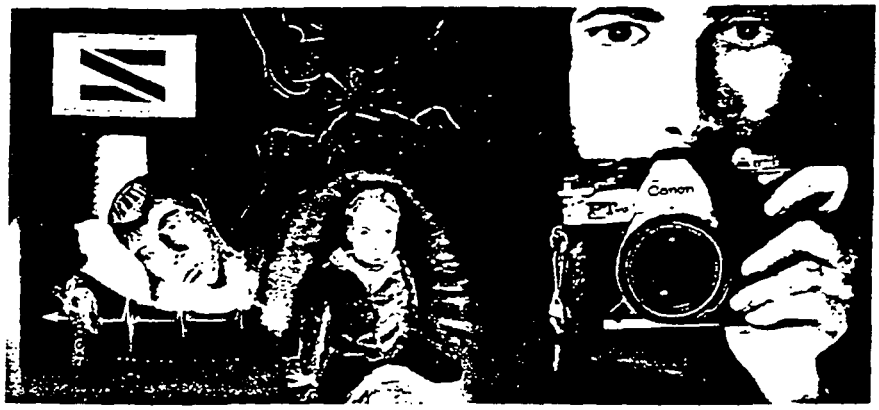
If you are interested in securing Justin's artwork for a presentation or training session for professionals in the field of child abuse, or would like to contribute to a fund Justin established to nurture the use of art with abused children and for programs related to the prevention of child sexual abuse, please call Father Ray at St. Vincent's Center in Baltimore, MD, at (410) 252-4000, ext. 1607.

This article was a joint collaboration of Special Agent Lisa Ward, U.S. Customs Service, Baltimore, MD; Assistant U.S. Attorney Andrew C. White, Baltimore, MD; Assistant U.S. Attorney Christain Manuelian, Baltimore, MD; and Postal Inspector Thomas E. Boyle, Baltimore Domicile, Washington Division.

The first painting

Justin represented himself as a young girl in this pen-and-ink work. His strongest reason for using this image was his concern that people would be less sensitive to a man's pain, as society does not "allow" men to be victims without also being accomplices in their victimization or deficient as men.

Nearly hidden in the lower folds of the girl's skirt, a child screams as a hand closes around her throat — sexual abuse is experienced as an attempt to murder, or kill. The girl's legs are drawn close to her body, self-protectively, but her hand is deformed, revealing Justin's sense of vulnerability and his inability to protect himself from Pete and further victimization. In this bleak image, Justin shows that most people are in the darkness about child sexual abuse: They are rarely aware when it occurs, so its young victims are left defenseless and in pain.



The second painting

At left, Justin lies awake, unable to sleep. His thoughts are trapped in the prison-like hurt of his abuse. Both the heart and its rhythms are reversed in the picture: Justin is confused about himself and his feelings for Pete. The words below, "Keep the secret until I die," reveal the internal and external messages that caused Justin to continue to be terrorized. He depicts himself as a young girl, surrounded by the golden glow of innocence as she looks at a book with a picture of a jester crying. The jester weeps for the child, who is dressed in harlequin colors, indicating she will play the fool. Her spread legs indicate the vulnerability of childhood. One hand is held behind her in a gesture of helplessness, and the other rests in the flowing red of the evil that is child sexual abuse.

The white figure being pulled by its limbs may indicate how Justin felt torn apart by Pete, who sometimes felt like his best friend and other times his worst enemy. The man behind the camera is Pete, who took pictures of Justin, making him feel exposed. Pete is painted without ears; he wasn't interested in what Justin had to say and wouldn't or couldn't listen to how his actions affected Justin. The figures that appear at the side of Pete's head are math calculations — Pete's actions were well planned. The rectangle at the upper left is an actual postcard Justin received from Pete before he went to Germany. It contains lines from a haiku verse written by a Japanese poet, Issa.

The painting is expressed as a strip of film: Pete "exposed" Justin to abuse, and Justin is exposing Pete's abuse through his art. In the lens of the camera, which Justin fashioned to jut out of the painting in 3-D, is a photo of a half-nude boy.

Father Ray, of St. Vincent's Center, exhibits Justin's paintings and writings to educate professionals and others in the field of child sexual abuse about the experience of abuse from a child's perspective.

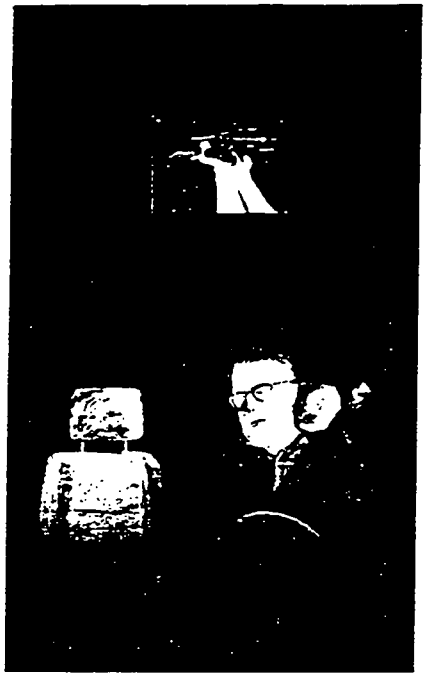
The third painting

Pete is depicted as the devil, clutching the boys' mother by the neck, indicative of how Susan Wilke was victimized by her trust in Pete. She is painted as a pale figure, without hands, powerless. The building in the background was Pete's home in Baltimore, and the room with the red shade is where Justin and Matt were abused. A girl, who is meant to be a composite of the brothers, is staring away from a photo album of a childhood the boys never had. The ghostly man, seated and holding his head in his hands, is Donald Wilke, the father. The image projects his sense of helplessness and inadequacy in protecting his sons. No one in the picture is on the same linear plane; the family members are isolated from one another.

The fourth painting

Justin painted this picture in response to a question about how he was doing, years after the abuse. The old woman is Justin, who felt old when he looked back at his lost youth. Justin attached a photo of a young woman just above the figure of the older one, as if the girl is an image in the older woman's thoughts. Justin didn't want to find himself an old man still grieving over his lost youth. He painted this picture on a bed linen primarily with his fingers, possibly intending that the black paint would gradually fade, as indeed it has. At the left side of the painting is an image of Christ. Oddly, although the rest of the picture is fading, the image of Christ has retained its brightness.

Justin wanted this painting to be illuminated from the front when shown. He intended it to be more hopeful than the others. The golden light, which covers more than half of the painting, is a positive image: Christ watches over the woman in the light that washes across her. Even the young woman is painted in gold, indicating that Justin was beginning to come out of the "darkness" and his lost childhood was beginning to shine through.



The last painting

Justin painted this picture less than a month after finding his father dead in the family car; the painting duplicates the exact scene of the death. Justin worked in a frame shop and framed all of his artwork. He used non-glare glass to frame this picture, which meant that, to see it clearly, the viewer is forced to stand directly in front of it, just as Justin was forced to see his father's death. An actual photograph, which was left on the dashboard of the car where Justin found his father, is mounted on the painting and shows a pair of outstretched arms holding a baby rabbit. Justin said that if people showed the same compassion for abused children as shown towards this rabbit, these terrible events would never have happened.

Justin never wrote anything about this painting, although he wrote about all the other paintings in the series. When asked what he wanted people to "take" from the painting, he said: "I would say that child abuse can kill."

PROJECT SPECIAL DELIVERY

Postal Inspectors Bust Child Porn Ring — and its Patrons

It's hard to believe that Postal Inspector Dave Austrum's response to a postal customer's complaint in December 1993 would lead Inspectors to shut down the largest commercial child pornography ring ever encountered by U.S. law enforcement. Project Special Delivery, a pro-active, undercover investigation conducted by the U.S. Postal Inspection Service, not only shattered an international cartel of child pornographers, it went after its customers as well. It's the customers' demand for this illicit material that creates a market for child pornography, a crime that victimizes children around the world.

Project Special Delivery began when inspector Dave Austrum learned that a Minneapolis man received an unsolicited videotape of child pornography from a mail-order company called Overseas Male (OSM). The video was actually a promotional tape, referred to by OSM as a "video catalog," featuring short previews of young, underage boys engaged in various sexual acts, and ordering information for full-length features. The return address placed the business in San Diego, so Dave forwarded the tape and some OSM advertising brochures to Postal Inspector Don Trutna of the former San Diego Division.

Inspector Trutna tracked down OSM's business address to a mail drop (commercial mail receiving agency) in San Ysidro, CA, a community on the U.S.-Mexican border: you can see the Tijuana International Airport from the street in front of the mail drop. The owners of the mail drop company told Inspector Trutna that OSM received high volumes of mail, which they forwarded several times a week to another mail drop in Mexico. OSM was using a fake return address on its videotape mailings.

Using the undercover mail drop of Postal Inspector Karen Cassatt from the Phoenix Division as a return address, we ordered some of the OSM videos. Inspector Cassatt soon sent us our purchases. All of the material was graphic child pornography, with

obviously underage children including starring roles.

Inspector Trutna called OSM in Mexico, using one of the numbers listed in its literature. The man who answered called himself "Jose." Jose assured us that some models in the videos were under 18. He said that was why OSM was in Mexico.

The real work begins

On June 29, 1994, inspectors from U.S. Customs arrested James Kemmish for currency violations upon his re-entry to the United States from Mexico. Customs Inspectors found over $16,000 in undeclared cash and money orders in Kemmish's possession. They also found videotapes, disguised as audiotapes, containing child pornography. And business records for Overseas Male.

U.S. Customs Special Agent Shirley Harris, a member of an interagency child exploitation task force in San Diego, remembered that Inspector Don Trutna was working a case involving Overseas Male and called him for help. The two spent the next day with Assistant U.S. Attorney Barbara Major drafting a search warrant for Kemmish's San Diego apartment. They executed the warrant with members of the San Diego Police Department and Sheriff's Office. What they found at Kemmish's place stunned them.

From the outside, Kemmish's home looked like any other beach area apartment. Inside, however, was a state-of-the-art production facility used to duplicate videotapes. There were tapes of children having sex with other children and with adults, children as young as seven years old. High-end Super VHS recorders, Hi-8 decks and 20 industrial duplicating machines flanked stacks of high-quality, master videotapes of child pornography. And more than 2,000 solicitations from Overseas Male ready to mail to addresses across the United States.

Inspectors noted the quality of the images and sophisticated effects used in their production. These were not old copies of tapes transferred to video, but state-of-the-art productions from around the world. There weren't many business records in the apartment, but there was a fax machine with printouts of the latest orders from Mexico.

James Leroy Kemmish

The ink had barely dried on the search warrant when Don and Team Leader Andy Thomas called Program Manager Ray Smith at National Headquarters and briefed him on the results of the search. Their decision was unanimous: It was an ideal opportunity to set up an undercover operation — a "reverse sting" — following the business practices of Overseas Male. Using intelligence gathered from the investigation, we would target OSM customers who had been relying on the U.S. Postal Service to deliver child pornography. Our company would be called "Island Male."

Inspector Ray Smith began meeting regularly with members of the Child Exploitation and Obscenity Section (CEOS) at the Department of Justice (DOJ) in Washington, DC, a group that specializes in child exploitation investigations. We worked hand-in-hand with DOJ attorneys to develop an investigative strategy that would be legally sound and withstand any claims of entrapment or outrageous government conduct. Even Attorney General Janet Reno was personally briefed on the initiative, and gave her department's full support.

We were able to expand our customer base when Inspector Smith received additional names of suspects in the United States from a Belgian colleague at a meeting of Interpol's Standing Working Party of Offenses Against Minors in Lyon, France. The names were found after John Stamford was charged in Brussels with depravity of youth and child prostitution. Stamford founded Spartacus International, Ltd., a worldwide organization which distributed publications such as *PAN (Paedo Alert News)*, a magazine about sexual relations between men and boys.

Building the case

Within weeks of the takedown, Inspectors called Jose to complain about an unfilled order. We learned

OSM was in trouble due to "a major catastrophe" (meaning Kemmish, his distributor, was out of commission). But we received brochures again a few weeks later from other companies offering tapes from OSM's catalog. Our undercover purchases confirmed this.

We fine-tuned Project Special Delivery with CEOS at the Department of Justice throughout the fall and into the winter of 1995. Inspector Trutna left the group when he was transferred to work with the Revenue and Asset Protection Program (RAPP) Team. The San Diego portion of Special Delivery and the Kemmish-Jose investigation was passed on to me.

We added more customers to our Island Male mailing list, this time compliments of the Vancouver Police Department in British Columbia. The Vancouver police found that a number of U.S. citizens were buying child pornography through the mail from "Out in the West Productions," a commercial distributor they had recently shut down. We also knew that two companies based in California were distributing OSM's material.

It was now evident that if Project Special Delivery was to succeed we had to close down these satellite businesses and neutralize Jose; otherwise, OSM's customers — now our customers — would know something was up.

As we continued building our case against Jose and OSM, we got a crucial lead: "Jose" was Troy Anthony Frank. The investigation suddenly became far more disturbing.

An evil man

Troy Frank began his career in child pornography in Greeley, CO, where he was arrested by local police and later convicted for child molestation. He was sentenced to probation on state charges. Frank moved on to San Diego and continued producing his videos, meeting James Kemmish there in the late 1980s.

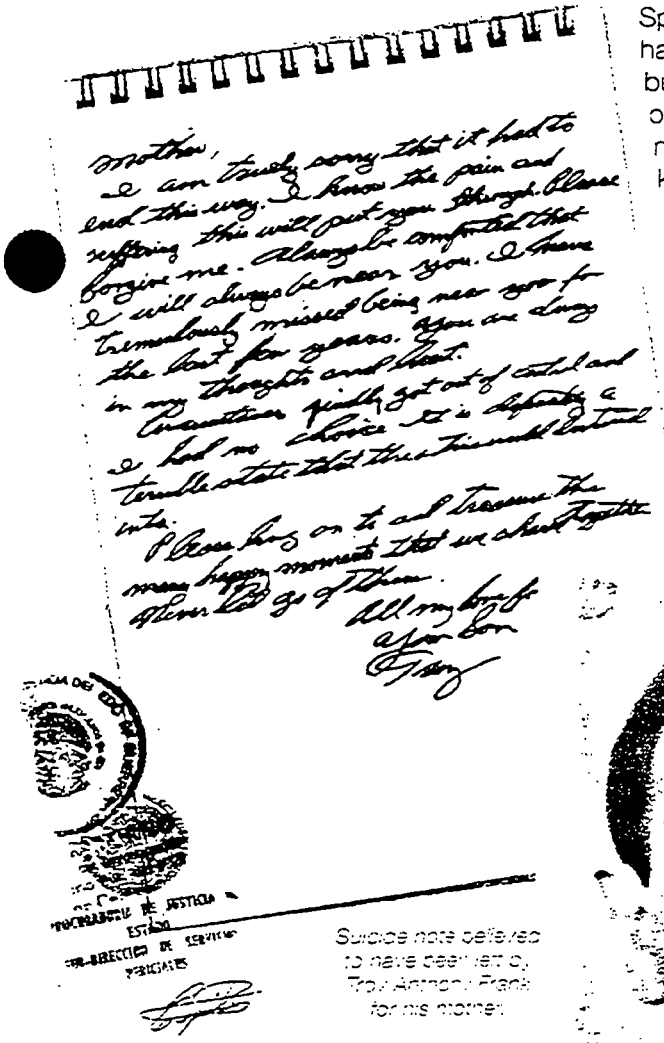
Just as the San Diego police were about to shut down Frank's operation, he fled to the Netherlands via Mexico. Frank again eluded authorities in Amsterdam, when they shut down a major child pornography operation in the area with ties to Frank. He returned to Mexico using the alias of a deceased Colorado police officer.

Meanwhile, Colorado police issued a state arrest warrant against Frank for child molestation, and the Department of State obtained a federal arrest warrant against him for passport fraud. U.S. Customs officials began working with high-level Mexican authorities in 1994 and 1995 to track down Troy Frank, without success.

Full speed ahead

On July 10, 1995, Inspectors led by Ron Higa of the Los Angeles Division and Fred Renfro of the San Francisco Division executed nearly simultaneous federal search warrants at businesses we believed were involved with OSM. Inspectors Andy Thomas and Karen Cassatt initiated actions to stop mail being delivered to Frank's mail drops in San Ysidro, CA, and Phoenix, AZ. With the full approval of the Department of Justice, Project Special Delivery was cleared to go.

The next day we mailed our first "Island Male" solicitations to suspects from the Kemmish, Spartacus and Out in the West Productions investigations. Only days later I received requests for information. I mailed this group a second letter, graphically



Suicide note believed to have been left by Troy Anthony Frank for his mother.

describing Island Male's products and enclosing order forms. Some of the orders for child porn came back faster than requests for information, but the child pornographers would have to wait until we were fully ready to deliver our product.

Project Special Delivery was running at full speed. On some days I received over 150 responses. The only problem was Frank, still at large in Mexico. On the evening of July 18, 1995, we played our last card.

We called Jose. "We know who you are," we told Troy Frank, "and we know where you are in Acapulco. We have federal and state arrest warrants ready for you."

We offered Frank three options: He could surrender himself to Special Agent Ed Lennon at the Embassy in Mexico City, he could surrender himself to us at the border or he could take his chances with the Mexican authorities. Frank said he'd think about it and call us back.

That was the last we heard from Frank. No one answered his phone, and the service was finally disconnected.

A pauper's grave

Acapulco police burst into Frank's bedroom on August 3, 1995. Besides a rotting body slumped in a chair, they found Frank's video equipment, OSM business records, child pornography tapes, a passport and a suicide note.

Servants identified the body as Frank's based on the gold Rolex watch on its wrist and other clothing, and the American Consulate identified him based on documents found at the scene, including a passport and birth certificate. By the time Agent Lennon and Mexican federal authorities arrived, the medical examiner had ruled the death a suicide, and the body was placed in a pauper's grave.

But Mexican officials carried the case as an open homicide. The body was placed face down in the grave, following local superstition that it would induce the murderer to return to the site.

A Postal Inspector makes a controlled delivery of child pornography videotapes to an Island Male customer.

Ed Lennon, however, believed that Frank had committed suicide. He was also fairly certain the body was Frank's, as there weren't many Anglo bodies to be found in Acapulco. Trial Attorney Georgiann Cerese at the Department of Justice's Child Exploitation and Obscenity Section and Assistant U.S. Attorney Barbara Major in San Diego wanted to indict Frank. We just didn't know for sure if the body found at the Acapulco villa was truly his.

The sting continues

On September 6, 1995, Postal Inspectors conducted the first five controlled deliveries of child pornography videotapes to Island Male customers.

One of our first arrests was Robert LaFond, a San Diego businessman who greeted us at his front door with a loaded semi-automatic pistol after accepting an Island Male package from Postal Inspector Yvonne Gurrero. We secured LaFond and his residence and then found his stash of child pornography. LaFond told us he had cultivated a sexual interest in children for over 20 years and admitted he had purchased child pornography through the mail, but he claimed he never hurt a child.

I spoke with AUSA Barb Major on my cellular phone during the search. After uncovering Polaroids of a young boy in a sexual act, I told her I had more questions for LaFond and I'd call her back. When confronted with the photos, LaFond admitted he had molested the boy, who lived in the neighborhood, as well as others. AUSA Major said, "Bring him in."

We dropped off LaFond at the Metropolitan Correctional Center and called San Diego Police Child Abuse detectives; they located and interviewed a young victim that day. LaFond was convicted of child molestation. He'll have to wait to go to state prison until he finishes up his time in the federal penitentiary for receiving child pornography through the mail.

Is he or isn't he?

Inspector Pat Carr of the Denver Division was also briefed on the investigation, and he interviewed Frank's mother, who broke the news of his death to her other son, Keith. Keith was troubled when he heard about the medical examiner's report.

Troy Frank was found dead wearing a pair of shorts, and he had used his right hand to shoot himself. But Troy was left-handed, said Keith, and he absolutely never wore shorts: it could be 100 degrees in the shade and Troy would wear slacks and a shirt. Keith also told Inspector Carr that Troy's business partner bore a striking resemblance to his brother. Recent photos and a family video, both taken in Mexico, confirmed Keith's statements.

I decided to run the case by my old mentor, Detective J.B. Boyd of the San Diego Police Department's homicide team. What he and fellow homicide detectives told me wasn't reassuring. Two extra bullet holes were found in Frank's bedroom, besides the one which had killed him. One of the bullet holes could be written off as a ricochet, but the other one?

"Test shots" were not unheard of, but were uncommon in suicides, said Boyd. He postulated that an inexperienced medical examiner could misdiagnose a contact wound as being an exit wound; exit wounds are usually larger than entry wounds due to muzzle blast. The detectives had other questions which made me uneasy.

Trial Attorney Georgiann Cerese and AUSA Barb Major were itching to indict Frank — if he was still alive. We realized we'd have to confirm the identity of the body now buried, face down, in an Acapulco grave.

A steady stream of orders

More bad news came in early fall 1995 from Inspector Tom Kochman of the Philadelphia Division: Project Special Delivery had been "outed" in the *North American Man Boy Love Association (NAMBLA) Bulletin.* NAMBLA advocates consensual sexual relations between adults and children. The group had printed an altered version of one of our Island Male letters, along with an inaccurate and damaging article.

November brought better news. We received over 50 new orders from Island Male customers and even more repeat business, despite the NAMBLA article and the continuing arrests and indictments of Special Delivery subjects. AUSA Major indicted Kemmish on additional charges related to using the mail to distribute child pornography. Postal Inspectors across the country were working significant cases from the operation.

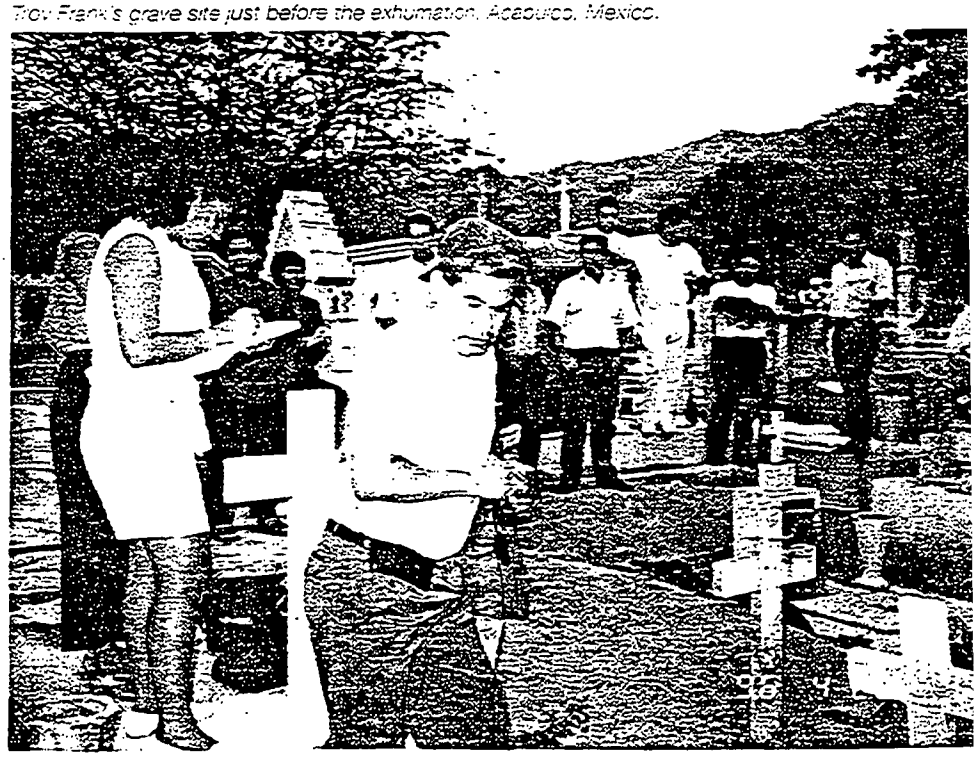
Inspector Karen Cassatt's suspect, Ray Opfer, was a prime example.

Opfer ordered tapes from Island Male. A background check revealed that Opfer, a scout leader, had a previous child molestation conviction hidden in his past and was on probation. Inspector Cassatt traveled to Reno, NV, to make a controlled delivery to Opfer with Inspector Kerry Fisher of the Phoenix Division.

Ray Opfer had a large collection of child pornography. Photographs found during the search revealed he was molesting young neighborhood boys. Opfer pleaded guilty to crimes related to child sexual abuse. After an emotionally charged hearing in which the victim's mother was allowed to speak on the witness stand, the judge sentenced Opfer to three consecutive terms of life imprisonment.

In January 1996, days before his

Troy Frank's grave site just before the exhumation, Acapulco, Mexico.



trial. Kemmish agreed to the government's final offer. Kemmish pleaded guilty to all charges, accepting even the prospect of an upward departure from the sentencing guidelines.

Getting the green light

Meanwhile, the "Frank mystery" remained open. My job was to work with the Mexican authorities and the U.S. Embassy in Mexico City to coordinate an exhumation of the body found in Acapulco. Keith Frank gave us permission to have his brother's remains exhumed and identified. Inspector Carr tracked down Frank's dental X-rays, as we didn't expect to find the body in good condition after months underground.

Postal Inspector Ron Higa of the Los Angeles Division obtained Frank's dental records for the exhumation and had them transferred to me. My team comprised Detective Miguel Penalosa, from the homicide team at the San Diego Police Department, and Dr. Norman "Skip" Sperber, a world-renowned forensic specialist and a pioneer in forensic dentistry. Dr. Sperber developed a dental identification system for the state of California after the crash of a PSA jet in San Diego, a system now used nationally. Both Miguel and Skip had previously worked on homicide investigations in Mexico.

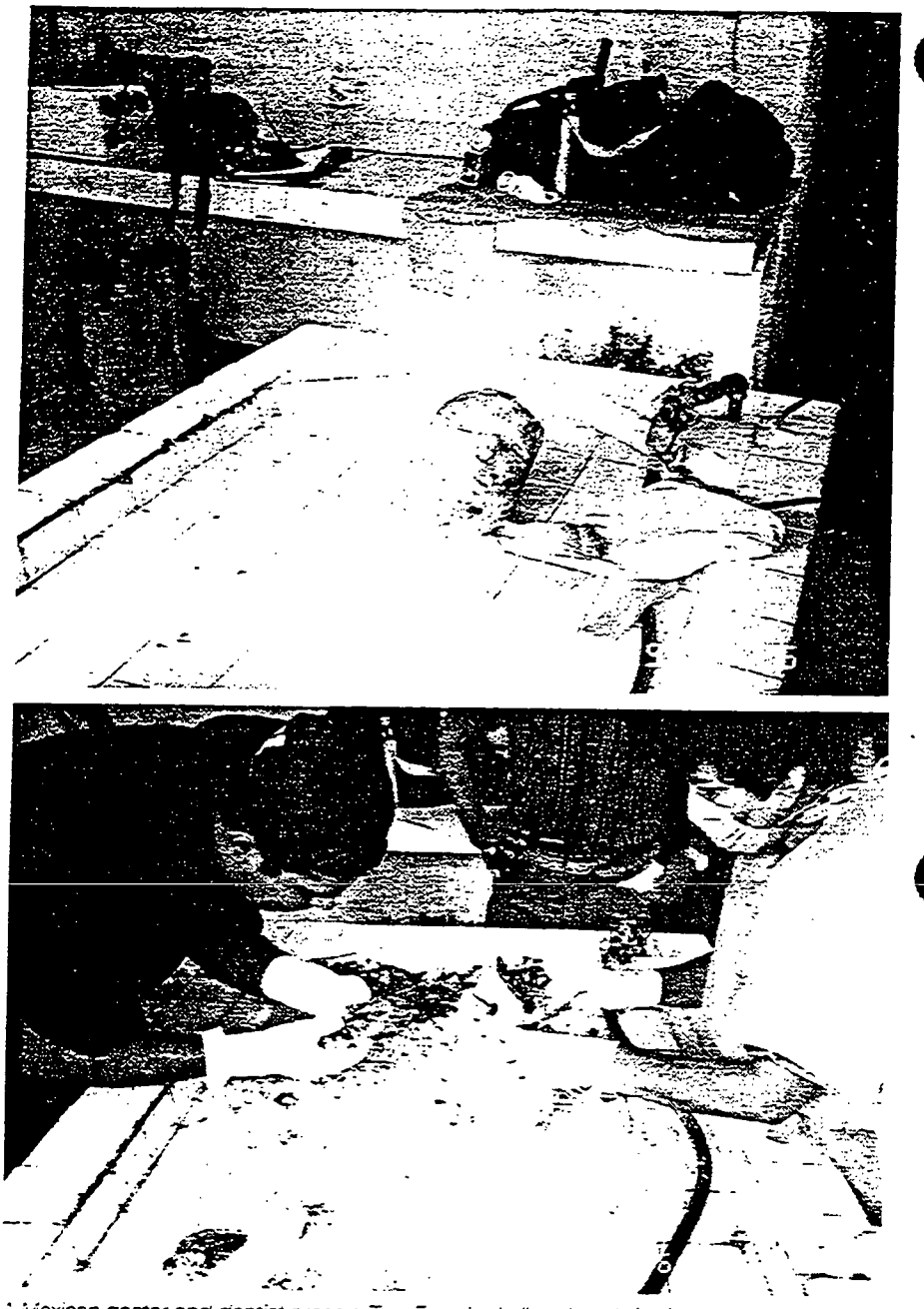
Just before leaving, Ed Lennon set me up with the fourth member of our team and his right-hand man, Senior Foreign Service National Investigator Mario Gonzales. Mario worked for the American Embassy in Mexico for over 20 years as a criminal investigator; he knew how to get things done in that country.

The Mexican way

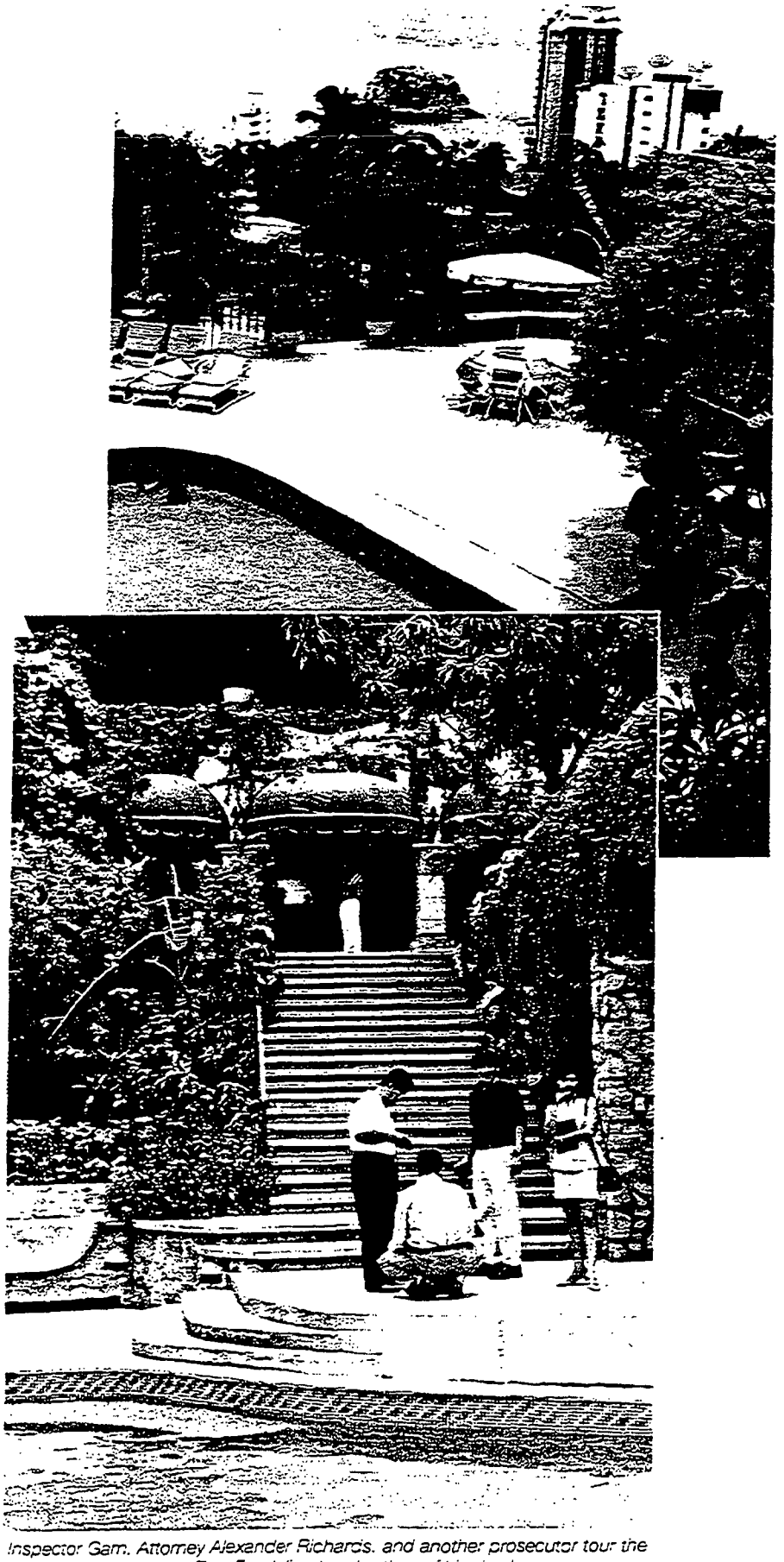
We were met at the airport in Acapulco by a delegation of prosecutors from the State Attorney General's office, and traveled by motorcade to the main police station.

Prosecutors at the station trotted out voluminous evidence of a worldwide child pornography operation. Working late into the night, we pored over business records showing sales of over $50,000 a month; customer lists, with familiar names from the OSM investigation and Project Special Delivery; reams of false identification documents; and photographs of hundreds of young victims of child exploitation.

The next day, the prosecutors took my team to Troy Frank's magnificent villa overlooking Acapulco Bay. They guided us through the



A Mexican doctor and dentist prepare Troy Frank's skull and teeth for further examination.



The view from the garden level of Frank's residence overlooking Acapulco Bay in Mexico.

Inspector Garn, Attorney Alexander Richards, and another prosecutor tour the villa in Acapulco where Troy Frank lived at the time of his death.

multilevel mansion, from the four-car, iron-gated garage and pool with deck, to the video production room and bedroom on the fourth level. They pointed out the bullet holes and the fractured door frame of the bedroom, where in August 1995 detectives found the decomposed body, two weeks old, with a solid gold Rolex on its wrist. That night we worked with a team of doctors, dentists, prosecutors and even anthropologists preparing for the exhumation.

We exhumed the body just as the mercury passed the 90-degree mark, removing the head and right thumb at the grave site and returning to the medical examiner's office via our now-familiar motorcade. A ceiling fan whirred overhead, flies buzzed and the temperature climbed as a doctor and dentist removed remaining flesh from the skull in preparation for the X-rays. Some of the teeth had fallen out and were stuck back in place with a hot glue gun from the Acapulco Wal-Mart. Using his bare hands, the medical examiner rolled the lone thumb on index cards for prints.

Unfortunately, one of the front teeth, which had a unique filling, was missing. Dr. Sperber told me the tooth was probably lost during the first autopsy in August 1995. He said that Frank had a lot of dental work done since the X-rays taken during the 1980s, so he was unable to positively identify the body without an X-ray of the skull.

We moved on to the medical lab for new X-rays. By comparing the orientation of the teeth and other features of the jaw in the new X-rays to the older set from Colorado, Dr. Sperber positively identified the remains. The body that had been buried in a pauper's

Inspector Phil Gam (left) presents Ramon Almonte-Borja, a prosecutor from the State Attorney General's office, with a Los Angeles Division cap and pin. Alexander Richards, a Mexican attorney, (right) translates.

grave was indeed that of Troy Anthony Frank.

The sanctity of the seal

Orders for Island Male videos waited to be filled back in San Diego. Even after eight months and over 120 searches nationwide, customers were still eager for our product. We continued receiving orders the same week Chief Hunter held a press conference in Washington, DC, announcing the results and huge success of Project Special Delivery.

Island Male still hasn't quite closed its doors — quite a few cases await final resolution. As of August 1996, after 133 searches, 57 subjects have been prosecuted and many more are waiting in the wings as Inspectors wade through mountains of evidence. Postal Inspector Steve Sadowitz of the Detroit Division claims he has reviewed more videos than Siskel and Ebert this year.

Child pornographers from all walks of life were identified through Project Special Delivery: four members of the clergy, six NAMBLA devotees, two Boy Scout leaders, one Big Brother, seven school teachers, a retired Army Lieutenant Colonel, several active and former police officers, an attorney, a history professor, a medical doctor, an electrical engineer, a computer programmer and a school counselor. Many were regarded as upstanding citizens in their communities— but they were secretly abusing children.

And there were other, unforeseen, benefits of our work. Robert H. Ellison, another customer of Island Male investigated by Postal Inspector Bob Williams of the Chicago Division, was found to have sexually abused a number of young children in his neighborhood some 35 years earlier. Now adults, these victims came forward, encouraged by the media attention we generated, to tell Postal Inspectors about the man's terrible deeds. Ellison will be spending the next several years behind bars in federal prison and will be registered with the state of Illinois as a sex offender for the rest of his life.

As a result of outstanding work by Postal Inspectors across the nation, from new students like Inspector Rey Santiago at the Ft. Worth Division and Inspector Rhonda Bowie at the Phoenix Division, to "old hands" like Inspector John Dunn in Boston and Inspector Beryl Hedrick in Alabama, Project Special Delivery was a huge success.

We struck a major blow against those who believed they could use the U.S. Postal Service as an unwitting accomplice to sexually exploit and victimize our nation's children. To those who abused the "sanctity of the seal," we proved once again the value of our work: For over 200 years, Postal Inspectors have protected the mail and the citizens of this country, ensuring that confidence in the U.S. Mail is not undermined. ■

ABOUT THE AUTHOR

Postal Inspector Phil Gam earned his B.A. in Psychology from the University of Virginia. He served as an officer in the Naval Reserve until 1990, and entered the Postal Service as a letter carrier in 1985, later supervising mail processing, delivery and finance operations. Inspector Gam was appointed as a Postal Inspector in 1990, and was assigned to the External Crimes Team of the former San Diego Division. Since 1994, he has worked in the areas of prohibited mailings-narcotics, internal crimes-narcotics and prohibited mailings-obscenity. Inspector Gam currently is assigned to the Los Angeles Division's Fraud and Prohibited Mailings Team based in San Diego. ■

UNITED STATES POSTAL INSPECTION SERVICE

CHILD EXPLOITATION CASE HIGHLIGHTS FOR FISCAL YEAR 1998

Since the enactment of the federal Child Protection Act of 1984, U.S. Postal Inspectors have conducted over 3,200 child exploitation investigations resulting in the arrests and convictions of more than 2,700 child molesters and pornographers.

During FY 1998, U.S. Postal Inspectors arrested 167 individuals for child sexual exploitation offenses related to the mail. Often, during the course of the investigation and incident to the search of the suspect's property, Postal Inspectors find evidence that the target of the investigation is a child molester. During FY 1998, 69 child molesters and 100 child victims were identified as a result of our work. Following are a few examples of case activity during FY 1998.

Phoenix, AZ

A child pornographer was sentenced to 17 years in state prison and lifetime probation for sexual exploitation of minors. He admitted to engaging in sex acts with more than 200 youth. He was identified as a result of Project Special Delivery, an undercover operation conducted by the Postal Inspection Service that resulted in over 130 searches nationwide.

Aquilla, TX

Four individuals were indicted by a federal grand jury for crimes related to sexual abuse and the exploitation of children. The four individuals were part of a child sex ring that recruited minor males in the Waco, TX, area to produce child pornography videotapes, which were sold by mail using post office boxes throughout the country. Eleven child victims were identified. Four other suspects were charged by the local district attorney for the aggravated sexual assault of minors. One child victim lost his life as a result of the ring. The four federal defendants have been convicted and received substantial prison sentences.

Harrisburg, PA

A man who produced child pornography when he photographed a 3-year old girl and mailed the undeveloped film to a commercial film developer was sentenced to six years and five months in federal prison, to be followed by 3 years of supervised release. The investigation determined the man had also molested the 7-year old sister of the girl in the photographs. State charges were filed on the molestation.

Gainesville, FL

A child pornographer was sentenced in federal court to ten years in prison and three years' of supervised release for enticing juvenile females to perform sex acts with an adult male in child pornography movies he produced and mailed. The children were offered $20 a minute to perform the acts.

Pittsburgh, PA

A child molester and pornographer, who drugged his young victims before abusing them and videotaping the acts, was sentenced in federal court to 15 years, 8 months in prison.

Newport News, VA

An individual was sentenced to 12 years and 7 months in federal prison and 3 years' probation for child pornography violations involving the mail. Postal Inspectors discovered the man had molested several neighborhood children, including a six-year old girl and nine-year old boy, and produced child pornography of these criminal acts. He also pled guilty to 19-related state charges.

Macon, GA

The former principal of a Macon, GA elementary school and his co-defendant, the former assistant superintendent of Monroe County, GA, schools, were sentenced in federal court to 37 and 42 months' imprisonment, respectively, and 3 years' probation each. The men were also ordered to forfeit their house, car, and the video equipment they used to record their sexual molestation of young boys.

Seattle, WA

A former Christian Brother, teacher and youth coach from Seattle, WA was sentenced to 3 years and 10 months in federal prison and 3 years' probation. He used the mail to lure as many as 17 boys from the Czech Republic for the purpose of criminal sexual activity.

New Orleans, LA

Postal Inspectors and Customs Agents arrested a former New Orleans police officer and head of the New Orleans Child Abuse Unit for receiving child pornography in the mail. The individual was previously arrested by New Orleans Postal Inspectors in 1987 while he was employed with the police department, at which time he was convicted and served five years and six months of a ten-year sentence for mailing child pornography. Following the most recent arrest, four children that he molested were identified.

Anaheim, CA

Postal Inspectors arrested a paroled murderer for mailing child pornography and traveling across state lines to sexually abuse a minor. As a result of these charges and the parole violation, the offender now faces life in prison.

Chesterfield County, VA

A former second-grade elementary school teacher was sentenced in federal court to a term of 10-years and 1-month imprisonment, the maximum allowable under federal sentencing guidelines. Our investigation revealed this man traveled to an Ohio water theme park where he molested and photographed two young boys. The children are now receiving victim services and the state of Ohio has lodged separate warrants against him.

Hammond, IN

A man who frequently traveled to Mexico in order to have sex with young boys was convicted following a four-day trial in federal court. He now faces 30 years to life in prison. This child sex offender, convicted for similar crimes in 1977 and again in 1987, was the subject of a joint investigation conducted by the Postal Inspection Service and the U.S. Customs Service after he purchased child pornography videotapes through the mail.

UNITED STATES POSTAL INSPECTION SERVICE

CHILD EXPLOITATION SPECIALISTS

ATLANTA DIVISION

Beryl Hedrick
U.S. Postal Inspector
(205) 326-2921

Birmingham Field Office
PO Box 2767
Birmingham, AL 35202-2767

CINCINNATI DIVISION

Greely Smith
U.S. Postal Inspector
(513) 684-8045

895 Central Avenue
Suite 400
Cincinnati, OH 45202-5748

Jeff Kahn
U.S. Postal Inspector
(513) 684-8043

895 Central Avenue
Suite 400
Cincinnati, OH 45202-5748

GULF COAST DIVISION

Bruce Beckham
U.S. Postal Inspector
(713) 238-4417

Houston Field Office
PO Box 1276
Houston, TX 77251-1276

Gary Johnson
U.S. Postal Inspector
(504) 589-1211

New Orleans Field Office
PO Box 51690
New Orleans, LA 70151-1690

MEMPHIS DIVISION

David Dirmeyer
U.S. Postal Inspector
(901) 576-2135

PO Box 3180
Memphis, TN 38173-0180

MIAMI DIVISION

William Bonney
U.S. Postal Inspector
(954) 436-7268

3400 Lakeshore Drive
6th Floor
Miramar, Florida 33027-3242

MICHIANA DIVISION

Paul Durand
U.S. Postal Inspector
(313) 226-8017

Detroit Field Office
PO Box 330119
Detroit, MI 48232-6119

Steve Sadowitz
U.S. Postal Inspector
(317) 328-2520

Indianapolis Field Office
7188 Lakeview Parkway West
Indianapolis, IN 46268-4104

MID-ATLANTIC DIVISION

Charley Wehner
U.S. Postal Inspector
(919) 501-9311

Raleigh Field Office
PO Box 26956
Raleigh, NC 27611-6956

MID-ATLANTIC DIVISION
(Continued)

Les Lauziere
U.S. Postal Inspector
(804) 418-6122

Richmond Field Office
PO Box 25009
Richmond, VA 23260-5009

MIDWEST DIVISION

Becky Powers
U.S. Postal Inspector
(314) 539-9441

St. Louis Field Office
1106 Walnut Street
St. Louis, MO 63199-2201

Rich Lawson
U.S. Postal Inspector
(816) 502-0450

Kansas City Field Office
3101 Broadway
Suite 850
Kansas City, MO 64111-2416

Randy Miskanic
U.S. Postal Inspector
(515) 253-2671

Des Moines Field Office
PO Box 566
Des Moines, IA 50302-0566

MIDWEST DIVISION
(Continued)

Dan Kakonis
U.S. Postal Inspector
(414) 287-2244
Milwaukee Field Office
350 W. St. Paul Avenue
#301
Milwaukee, WI 53203-3009

Pam Durkee
U.S. Postal Inspector
(402) 392-8825
Omaha Field Office
9140 W. Dodge Road
Suite 100
Omaha, NE 68114-3342

NEW YORK METRO DIVISION

Jean Wright
U.S. Postal Inspector
(212) 330-3527
PO Box 555
James A. Farley Building
New York, NY 10116-0555

NEWARK DIVISION

John Johnson
U.S. Postal Inspector
(973) 693-5473
PO Box 509
Newark, NJ 07101-0509

NORTHEAST DIVISION

John Dunn
U.S. Postal Inspector
(617) 464-8022
Boston Field Office
425 Summer Street
7th Floor
Boston, MA 02210-1736

NORTHEAST DIVISION
(Continued)

Rich Irvine
U.S. Postal Inspector
(617) 464-8047
Boston Field Office
425 Summer Street
7th Floor
Boston, MA 02210-1736

Terry Loftus
U.S. Postal Inspector
(518) 449-4176
Albany Field Office
PO Box 557
Albany, NY 12201-0557

Tom Lambert
U.S. Postal Inspector
(203) 294-6776
Wallingford Field Office
PO Box 1700
Wallingford, CT 06492-1300

NORTHERN CALIFORNIA DIVISION

Ben Derderian
U.S. Postal Inspector
(415) 778-5924
PO Box 882528
San Francisco, CA 94188-2528

NORTHERN ILLINOIS DIVISION

Bob Williams
U.S. Postal Inspector
(312) 983-6225
433 W. Harrison
Chicago, IL 60669-2201

NORTHWEST DIVISION

Paul Groza
U.S. Postal Inspector
(503) 279-2074
Portland Field Office
921 SW Washington
Suite 790
Portland, OR 97205-2898

Mike Erdahl
U.S. Postal Inspector
(509) 624-1432
Spokane Field Office
PO Box 1464
Spokane, WA 99210-1464

PHILADELPHIA METRO DIVISION

Tom Kochman
U.S. Postal Inspector
(717) 257-2343
Harrisburg Field Office
PO Box 60035
Harrisburg, PA 17106-0035

ROCKY MOUNTAIN DIVISION

Paul Tirjan
U.S. Postal Inspector
(303) 313-5305
Denver Field Office
1745 Stout Street
Suite 900
Denver, CO 80202-3034

Rhonda Bowie
U.S. Postal Inspector
(602) 223-3259
Phoenix Field Office
PO Box 20666
Phoenix, AZ 85036-0666

SAN JUAN DIVISION

Jose Cottes
U.S. Postal Inspector
(787) 749-7600
PO Box 363667
San Juan, PR 00936-3667

SOUTHERN CALIFORNIA DIVISION

Ron Higa
U.S. Postal Inspector
(213) 830-2544
Los Angeles Field Office
PO Box 2000
Pasadena, CA 91102-2000

Phil Garn
U.S. Postal Inspector
(619) 531-8231
San Diego Field Office
PO Box 2110
San Diego, CA 92112-2110

SOUTHWEST DIVISION

Bob Adams
U.S. Postal Inspector
(972) 456-2094
Ft. Worth Field Division
PO Box 162929
Ft. Worth, TX 76161-2929

Mitchell Webb
U.S. Postal Inspector
(501) 945-6720
Little Rock Field Office
PO Box 15058
Little Rock, AR 72231-5058

ST. PAUL DIVISION

Ron Miller
U.S. Postal Inspector
(651) 293-3220
PO Box 64558
St. Paul, MN 55164-0558

TAMPA DIVISION

Lee Edwards
U.S. Postal Inspector
(813) 281-5209
PO Box 22526
Tampa, FL 33622-2526

WASHINGTON METRO DIVISION

Keith Hayden
U.S. Postal Inspector
(410) 347-4400
PO Box 1856
Baltimore, MD 21203-1856

WESTERN ALLEGHENY DIVISION

Tom Clinton
U.S. Postal Inspector
(412) 359-7945
Pittsburgh Field Office
1001 California Avenue
Pittsburgh, PA 15290-9000

WESTERN ALLEGHENY DIVISION *(Continued)*

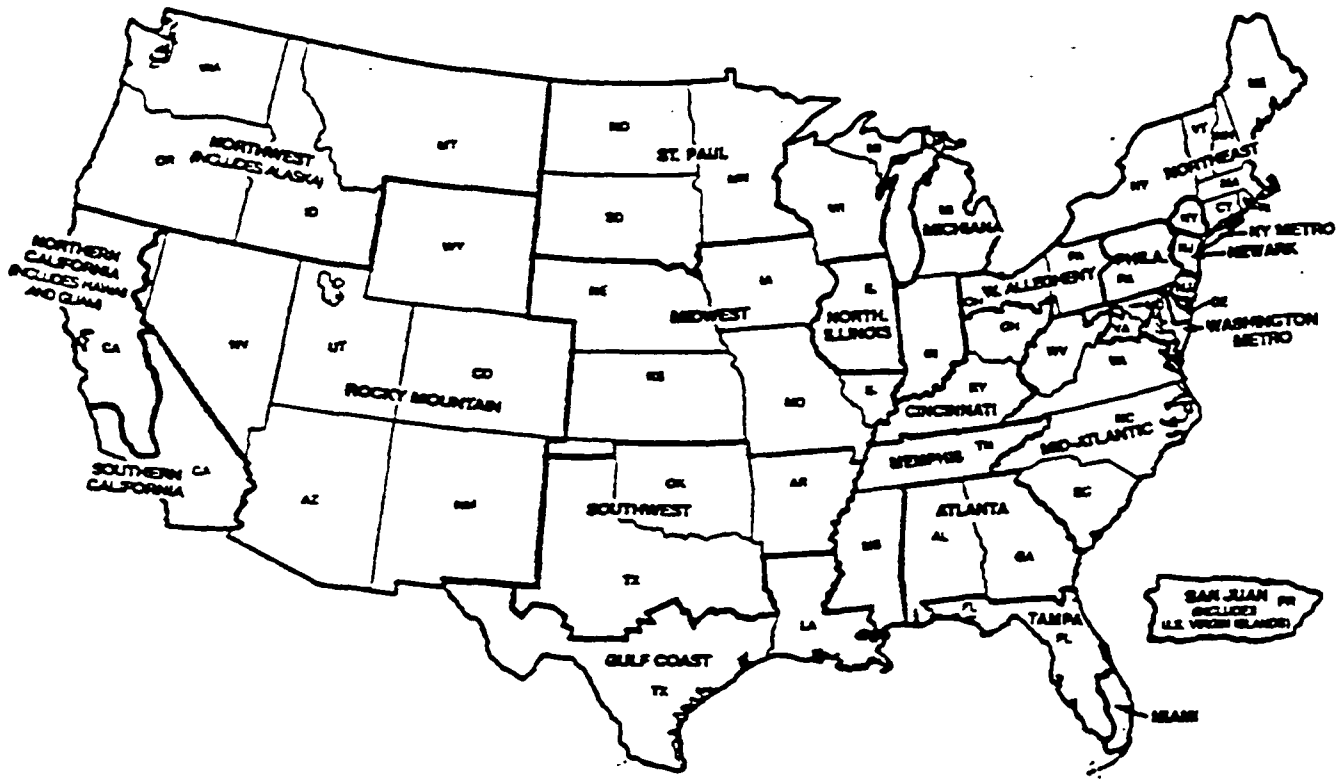
John Campisi
U.S. Postal Inspector
(216) 443-4463
Cleveland Field Office
PO Box 5726
Cleveland, OH 44101-0726

NATIONAL HEADQUARTERS

Ray Smith
U.S. Postal Inspector
(202) 268-4286
U.S. Postal Inspection Service
475 L'Enfant Plaza, SW
Washington, DC 20260-2166

Robert Northrop
U.S. Postal Inspector
(301) 586-4407
11700 Beltsville Drive
Suite 200
Calverton, MD 20705-3103

FYI



For assistance with postal-related problems of a law enforcement nature, please contact the nearest Inspection Service Division.

Atlanta Division
P.O. Box 16489
Atlanta, GA 30321-0489
404/608-4500
Fax: 404/608-4505

Cincinnati Division
895 Central Ave., Ste. 400
Cincinnati, OH 45202-5748
513/684-8000
Fax: 513/684-8009

Gulf Coast Division
P.O. Box 1276
Houston, TX 77251-1276
713/238-4400
Fax: 713/238-4460

Memphis Division
P.O. Box 3180
Memphis, TN 38173-0180
901/576-2077
Fax: 901/576-2085

Miami Division
3400 Lakeside Dr., 6th Fl.
Miramar, FL 33027-3242
954/436-7200
Fax: 954/436-7282

Michiana Division
P.O. Box 330119
Detroit, MI 48232-6119
313/226-8184
Fax: 313/226-8220

Mid-Atlantic Division
P.O. Box 3000
Charlotte, NC 28228-3000
704/329-9120
Fax: 704/357-0039

Midwest Division
1106 Walnut Street
St. Louis, MO 63199-2201
314/539-9300
Fax: 314/539-9306

New York Metro Division
P.O. Box 555
New York, NY 10116-0555
212/330-3844
Fax: 212/330-2720

Newark Division
P.O. Box 509
Newark, NJ 07101-0509
973/693-5400
Fax: 973/645-0600

Northeast Division
425 Summer St., 7th Fl.
Boston, MA 02210-1736
617/464-8000
Fax: 617/464-8123

Northern California Division
P.O. Box 882528
San Francisco, CA 94188-2528
415/778-5800
Fax: 415/778-5822

Northern Illinois Division
433 W. Harrison St., Rm. 50190
Chicago, IL 60669-2201
312/983-7900
Fax: 312/983-6300

Northwest Division
P.O. Box 400
Seattle, WA 98111-4000
206/442-6300
Fax: 206/442-6304

Philadelphia Division
P.O. Box 7500
Philadelphia, PA 19101-9000
215/895-8450
Fax: 215/895-8470

Rocky Mountain Division
1745 Stout St., Ste. 900
Denver, CO 80202-3034
303/313-5320
Fax: 303/313-5351

San Juan Division
P.O. Box 363667
San Juan, PR 00936-3667
787/749-7600
Fax: 787/782-8296

Southern California Division
P.O. Box 2000
Pasadena, CA 91102-2000
626/405-1200
Fax: 626/405-1207

Southwest Division
P.O. Box 162929
Ft. Worth, TX 76161-2929
817/317-3400
Fax: 817/317-3430

St. Paul Division
P.O. Box 64558
St. Paul, MN 55164-0558
651/293-3200
Fax: 651/293-3384

Tampa Division
P.O. Box 22526
Tampa, FL 33622-2526
813/281-5200
Fax: 813/289-8003

Washington Metro Division
P.O. Box 96096
Washington, DC 20066-6096
202/636-2300
Fax: 202/636-2287

Western Allegheny Division
1001 California Ave., Rm. 2101
Pittsburgh, PA 15290-9000
412/359-7900
Fax: 412/359-7682

USPS PROCEDURES

MAIL COVER REQUESTS

RESTRICTED INFORMATION

No portion of this document may be reproduced

Publication 55, July 1995

Publication 55
USPS Procedures: Mail Cover Requests [DATE]

1. EXPLANATION

This publication provides instructions to law enforcement agencies requesting a mail cover as part of a criminal investigation. All conditions and procedures contained in these instructions must be met before a mail cover can be authorized.

2. DISTRIBUTION

a. Initial. Headquarters, Inspection Service Operation Support Group (ISOSG) Managers and Inspectors in Charge (INC) receive initial copies.

b. Additional Copies. Only those receiving initial distribution may order extra copies from the Material Distribution Centers (MDCs) on Form 7380, MDC Supply Requisition. Only the Inspection Service may issue copies to law enforcement agencies on a case-by-case basis.

3. PROTECTION

Publication 55 is a "Restricted Use" publication. All persons in possession of this document must ensure that it is secured at all times. Its reproduction is prohibited.

4. COMMENTS

Address comments and questions to:

COUNSEL
OFFICE OF THE CHIEF INSPECTOR
US POSTAL INSPECTION SERVICE
WASHINGTON DC 20260-2181

This publication is effective upon receipt.

Kenneth J. Hunter
Chief Postal Inspector

Contents

I. Summary 4

A. Policy Statement 4

B. Definition 4

C. Purpose 4

D. Authority 5

II. Restrictions 6

A. Cover Categories 6

B. Mail Contents and Disclosure 6

C. Regulations Enforcement 6

D. Submission Requirements 6

III. Preparation 7

A. Mailing Instructions 7

B. Mandatory Information 7

1. Cover Justification 7

2. Subject Identity 7

3. Mail Classification 8

4. Time Frame 8

5. Criminal Violation 8

6. Legal Representation 9

7. Daily Documentation 9

8. Special Instructions 9

C. Signature Block 9

Exhibits:

1. Title 39, Code of Federal Regulations, Section 233.3 10
2. Inspection Service Operations Support Group Managers 16
3. Sample Request (Letter/Memo) - Criminal Violation 18
4. Sample Request (Letter/Memo) - Forfeiture 21
5. Sample Request (Letter/Memo) - Fugitive 24
6. Form 2009, Information Concerning Mail Matter 27

A. Policy Statement

It is the policy of the Postal Inspection Service to maintain close control and supervision of mail covers as a sensitive law enforcement investigative technique, in accordance with applicable federal laws and regulations (Title 39, United States Code, Section 410; Title 39, Code of Federal Regulations, Section 233.3). Requesting agencies must treat mail covers as restricted and confidential information. To the extent possible, mail covers should not be introduced as evidence in criminal or civil proceedings. Since mail cover information is recorded by postal employees in the postal facility responsible for delivery of the mail, the implementation of the mail cover may be subject to operational restrictions established at this facility. The failure of a requestor to comply with these requirements and conditions may result in a suspension of future mail cover requests.

B. Definitions

"Inspection Service Operations and Support Groups (ISOSGS)" are the five (5) primary administrators of the mail cover program with defined geographical areas of responsiblity.

"Mail cover" is the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law. The information provided by a mail cover may only be used to: (i) protect national security; (ii) locate a fugitive; (iii) obtain evidence of commission of a crime; and/or (iv) assist in the identification of property, proceeds or assets forfeitable under law.

"Sealed class of mail" is mail which under postal laws and regulations is not subject to opening and inspection without a federal warrant and includes First-Class mail, Express Mail, Priority Mail, international letter mail, and mailgram messages.

"Unsealed class of mail" is mail which under postal laws or regulations is subject to inspection without a federal warrant and includes Second-Class (newspapers and magazines), Third-Class (bulk business advertising and small parcels), and Fourth-class mail (parcel post and international parcel post mail).

C. Purpose

This publication contains the guidelines which law enforcement agencies must use in preparing mail cover requests. Mail covers are implemented only when all requirements are met in a written request to the Inspection Service. In emergency situations, a mail cover may be initiated based on a verbal request which is confirmed by a written request within three (3) working days. Mail cover information will not be released until the written request is approved. In exigent circumstances, the mail cover information may be provided to the

request prior to the receipt of the written request

D. Authority

The United States Postal Inspection Service (Inspection Service) has sole regulatory authority to authorize mail covers. Title 39 of the Code of Federal Regulations, Section 233.3, authorizes and prescribes the manner in which mail covers are conducted (see Exhibit 1).

Requests are approved by the Chief Postal Inspector and, by delegation, to each of the five ISOSG Managers. In emergencies, local Inspectors in Charge may also approve cover requests.

Mail covers are issued only to agencies empowered by statute or regulation to conduct criminal investigations and are strictly controlled to assure proper use. They are not to be used as the sole or initial investigative step.

Mail covers are restricted to the following categories of investigations:

1. To protect national security against actual or potential threats to the U.S. by a foreign power or its agents. (Note: Only those agencies with national security investigative authority may request covers in this category.)

2. To locate a fugitive.

3. To acquire evidence of a commission or attempted commission of a crime punishable by one year or more in prison (felony violations).

4. To assist in the identification of property, proceeds or assets forfeitable under law.

B. Mail Contents and Disclosure

Approved mail covers authorize the recording of information from the outside wrappers or envelopes of sealed and unsealed classes of mail. Mail covers do not authorize the opening of any class of mail. Mail in USPS custody may be seized and its contents examined only under authority of a properly executed federal search warrant. Only postal personnel are authorized to record mail cover information and may disclose such information at the express direction of the Inspection Service. The disclosure of mail cover information to other law enforcement agencies assisting in an investigation also requires Inspection Service approval.

C. Regulations Compliance

Each request is reviewed to ensure that it contains enough information to stand alone as full justification for the cover and fully complies with all regulation requirements. Requests for time extensions of approved mail covers must state the investigative benefits gained from the original request or anticipated to be obtained from the extension. A mail cover will be extended beyond the initial time period of the original where sufficient justification is provided.

D. Submission Requirements

Once a request is approved, mail cover data is provided on PS Form 2009, Information Concerning Mail Matter. These forms remain USPS property and must be returned to the ISO/SCI Manager within 60 days after the termination date of the cover. Reproduction of these forms is prohibited.

III. Preparation

A. Mailing Instructions

Request the mail cover on agency letterhead addressed to the ISOSG Manager, Attn.: Mail Cover Specialist, and send to the Inspection Service Operational Support Group (ISOSG) which has jurisdiction over the postal facility where the information will be recorded. A list of ISOSGs and the geographical area they cover is provided as Exhibit 2. Endorse the request and envelope RESTRICTED INFORMATION. Seal the request in the envelope, place it in a second envelope, and mail to the ISOSG.

B. Mandatory Information

There is certain information which **must** be furnished to determine if a mail cover can be approved. The items in this section are numbered to correspond to those shown in parentheses on the sample mail cover requests provided as Exhibits 3, 4 and 5. These sample requests identify the information required for a mail cover in a criminal case (Exhibit 3), a forfeiture case (Exhibit 4) and a fugitive case (Exhibit 5).

1. Cover Justification. State your purpose for requesting a mail cover and explain how the cover will provide evidence of a crime. A mail cover should **not** be used as merely a **routine** "investigative tool." Specify how information from the mail cover will assist the criminal investigation. Provide reasonable grounds that demonstrate the basis of the criminal investigation and the need to obtain this information from the mail. (For example, reasonable grounds might be based on information from a confidential informant, public complaint, previous investigation, etc.) Be specific and concise in outlining the reasonable grounds element.

Reminders:

a. Mail covers are not authorized for exploratory purposes or for crimes punishable by less than one year imprisonment (misdemeanors).
b. Requests referencing federal grand jury material covered by Rule 6(e) of Federal Rules of Criminal Procedure are returned without action.
c. The request is a permanent part of the mail cover file and will be made available through proper disclosure procedures, including criminal or civil discovery actions.

2. Subject Identity. Identify each person or business to be covered by full name, address, and ZIP Code. If the request specifies "all other names at the subject address," it must justify the broader scope. Examples of such justification could include the known use of aliases by the subject, agency experience in similar cases which indicate that different names are normally used, or information that a spouse, family member, or roommate is involved in the suspected criminal activity.

Information regarding the persons residing at or receiving mail at a particular address should be obtained prior to submitting the mail cover request. This information can normally be requested from the local Postal Inspector's office. Be careful to insure that the cover is limited only to the persons required for the investigation and that the information provided establishes a basis to show the involvement of each subject in the matter under investigation. As an example, a mail cover request for all names at a building address which contains multiple dwellings (i.e., an apartment building), without adequate justification, will be rejected.

Reminders:

a. State whether all mail delivered to this address is intended for the cover subject.
b. Identify anyone else who receives mail at the same address but is not a subject of your investigation, so that person's mail can be excluded from the cover.

3. **Mail Classifications**. The class of mail (see definition section) to be covered must be stated. Usually, only sealed mail will be covered. If it is necessary to add unsealed mail, specify the reasons for its inclusion.

4. **Time Frame**. State the amount of time needed for the mail cover. Covers are usually authorized for 30 days, with three 30-day extensions allowed, not to exceed a maximum of 120 days.

Reminders:

A request for an extension of the mail cover must include the following information:

a. Subject of the mail cover;
b. Mail cover security number;
c. The information developed from the original mail cover;
d. The contributions obtained from the original mail cover; and
e. The additional information that the extension may provide.

5. **Violation**. In a case where the cover is being requested to develop information for a criminal investigation, cite the specific applicable statute, with a description of the violation, and the penalty provided under the code (e.g., Title 18, United States Code, Section 1343, Wire Fraud, Penalty is five (5) years imprisonment and/or $1,000 fine).

Ordinarily, a mail cover will not be approved for a criminal investigation purpose where the subject has already been indicted. The only exceptions to this prohibition are where the subject is a fugitive or where the mail cover information will be used for a forfeiture investigation. In the case where the mail cover is being requested to locate a fugitive, clearly identify the fugitive and the specific statute which the fugitive violated, including title, section and penalty. State whether the person has been indicted, an arrest warrant is outstanding, and if the person's whereabouts are known or unknown.

In those cases where information is being sought in furtherance of a forfeiture, specify both the legal basis of the forfeiture (facts which describe the forfeiture investigation) and applicable statutes which authorize the forfeiture by the requesting agency (forfeiture statute and the agency's forfeiture authority).

If the subject is formally charged by indictment or information while the mail cover is in effect, notify the ISOSG Manager immediately to terminate the cover. Except in fugitive and forfeiture cases, mail covers are not continued if the person is indicted for the crime upon which the mail cover was requested. In these instances, a new mail cover request must be submitted which states as its basis the identification of assets for forfeiture purposes or the location of the suspect as a fugitive.

6. Legal Representation. Give the name and address of the subject's attorney or state if the attorney is unknown to you. If the purpose of the cover is to locate a fugitive, identify known legal counsel for both the subject of the cover and the fugitive. Mail covers exclude any mail between subjects and their attorneys.

7. Daily Documentation. Cover information is documented daily on Forms 2009 and sent to you at the end of the authorized time frame. If you need these forms during the course of the cover period, specify in your request that the forms are to be submitted on a weekly basis. Return all Forms 2009 to the ISOSG Manager within 60 days of the mail cover termination date (see Exhibit 6).

Reminders:

a. All Forms 2009 are USPS property.
b. Reproduction of forms is prohibited.
c. Use of forms as evidence, or reference to mail covers in criminal, civil or administrative proceedings, should be avoided to the extent possible.
d. Requesting official must ensure security of forms and their return.

8. Special Instructions. Note any additional circumstances relevant to your investigation, such as particular mail the subject receives or name of the local Postal Inspector if liaison has been established.

C. Signature Block

Provide your name, title, department, and commercial phone number. Sign above typed name.

Exhibit 1

39 CFR, Section 233.3

233.3 MAIL COVERS

(a) **Policy.** The U.S. Postal Service maintains rigid control and supervision with respect to the use of mail covers as an investigative technique for law enforcement or the protection of national security.

(b) **Scope.** These regulations constitute the sole authority and procedure for initiating a mail cover, and for processing, using and disclosing information obtained from mail covers.

(c) **Definitions.** For purpose of these regulations, the following terms are hereby defined.

(1) **"Mail cover"** is the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law, to obtain information in order to: (i) Protect national security; (ii) Locate a fugitive; (iii) Obtain evidence of commission or attempted commission of a crime; (iv) Obtain evidence of a violation or attempted violation of a postal statute, or (v) Assist in the identification of property, proceeds or assets forfeitable under law.

(2) **For the purposes of 233.3, "record"** is a transcription, photograph, photocopy or any other facsimile of the image of the outside cover, envelope, wrapper, or contents of any class of mail.

(3) **"Sealed mail"** is mail on which appropriate postage is paid, and which under postal laws and regulations is included within a class of mail maintained by the Postal Service for the transmission of mail sealed against inspection, including First-Class Mail, Express Mail, international letter mail, and mailgram messages.

(4) **"Unsealed mail"** is mail on which appropriate postage for sealed mail has not been paid and which under postal laws or regulations is not included within a class of mail maintained by the Postal Service for the transmission of mail sealed against inspection. Unsealed mail includes second-, third-, and fourth-class mail, and international parcel post mail.

(5) **"Fugitive"** is any person who has fled from the United States or any State, the District of Columbia, territory or possession of the United States, to avoid prosecution for a crime, to avoid punishment for a crime, or to avoid giving testimony in a criminal proceeding.

(6) **"Crime"**, for the purposes of this section, is any commission of an act or the attempted commission of an act that is punishable by law by imprisonment for a term exceeding one year.

(7) **"Postal statute"** refers to a statute describing criminal activity, regardless of the term of imprisonment, for which the Postal Service has investigative authority, or which is directed against the Postal Service, its operations, programs, or revenues.

(8) **"Law enforcement agency"** is any authority of the Federal Government or any authority of a State or local government, one of whose functions is to: (i) Investigate the commission or attempted commission of acts constituting a crime, or (ii) Protect the national security.

(9) **"Protection of the national security"** means to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents: (i) An attack or other grave, hostile act; (ii) Sabotage, or international terrorism; or (iii) Clandestine intelligence activities, including commercial espionage.

(10) **"Emergency situation"** refers to circumstances which require the immediate release of information to prevent the loss of evidence or in which there is a potential for immediate physical harm to persons or property.

(d) **Authorizations** - Chief Postal Inspector.

(1) The Chief Postal Inspector is the principal officer of the Postal Service in the administration of all matters governing mail covers. The Chief Postal Inspector may delegate any or all authority in this regard to not more than two designees at Inspection Service Headquarters.

(2) Except for national security mail covers, the Chief Postal Inspector may also delegate any or all authority to the Manager, Inspection Service Operations Support Group, and, for emergency situations, to Inspectors in Charge. The Manager, Inspection Service Operations Support Group, may delegate this authority to no more than two designees at each Operations Support Group.

(3) All such delegations of authority shall be issued through official, written directives. Except for delegations at Inspection Service Headquarters, such delegations shall only apply to the geographic areas served by the Manager, Inspection Service Operations Support Group, or designee.

(e) **The Chief Postal Inspector**, or his designee, may order mail covers under the following circumstances:

(1) When a written request is received from a postal inspector that states reason to believe a mail cover will produce evidence relating to the violation of a postal statute.

(2) When a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to: (i) Protect the national security; (ii) Locate a fugitive; (iii) Obtain information regarding the commission or attempted commission of a crime, or (iv) Assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.

(3) When time is of the essence, the Chief Postal Inspector, or designee, may act upon an oral request to be confirmed by the requesting authority in writing within three calendar days. Information may be released by the Chief Postal Inspector or designee, prior to receipt of the written request, only when the releasing official is satisfied that an emergency situation exists.

(f) (1) **Exceptions.** A postal inspector, or a postal employee acting at the direction of a postal inspector, may record the information appearing on the envelope or outer wrapping, of mail without obtaining a mail cover order, only under the circumstances in paragraph (f)(2) of this section.

(2) The mail must be: (i) Undelivered mail found abandoned or in the possession of a person reasonably believed to have stolen or embezzled such mail; (ii) Damaged or rifled, undelivered mail, or (iii) An immediate threat to persons or property.

(g) **Limitations.**

(1) No person in the Postal Service, except those employed for that purpose in dead-mail offices, may open, or inspect the contents of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise Non-mailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute.

(2) No employee of the Postal Service shall open or inspect the contents of any unsealed mail, except for the purpose of determining: (i) Payment of proper postage, or (ii) Mailability.

(3) No mail cover shall include matter mailed between the mail cover subject and the subject's known attorney.

(4) No officer or employee of the Postal Service other than the Chief Postal Inspector, Manager, Inspection Service Operations Support Group, and their designees, are authorized to order mail covers. Under no circumstances may a postmaster or postal employee furnish information as defined in Title 39, Code of Federal Regulations, Section 233.3(c)(1) to any person, except as authorized by a mail cover order issued by the Chief Postal Inspector or designee, or as directed by a postal inspector under the circumstances described in Title 39, Code of Federal Regulations, Section 233.3(f).

(5) Except for mail covers ordered upon fugitives or subjects engaged, or suspected to be engaged, in any activity against the national security, no mail cover order shall remain in effect for more than 30 days, unless adequate justification is provided by the requesting authority. At the expiration of the

mail cover order period, or prior thereto, the requesting authority may be granted additional 30-day periods under the same conditions and procedures applicable to the original request.

The requesting authority must provide a statement of the investigative benefit of the mail cover and anticipated benefits to be derived from its extension.

(6) No mail cover shall remain in force longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or designees at National Headquarters.

(7) Except for fugitive cases, no mail cover shall remain in force when an information has been filed or the subject has been indicted for the matter for which the mail cover is requested. If the subject is under investigation for further criminal violations, or a mail cover is required to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law, a new mail cover order must be requested consistent with these regulations.

(8) Any national security mail cover request must be approved personally by the head of the law enforcement agency requesting the cover or one designee at the agency's headquarters level. The head of the agency shall notify the Chief Postal Inspector in writing of such designation.

(h) **Records.**

(1) All requests for mail covers, with records of action ordered thereon, and all reports issued pursuant thereto, shall be deemed within the custody of the Chief Postal Inspector. However, the physical storage of this data shall be at the discretion of the Chief Postal Inspector.

(2) If the Chief Postal Inspector, or his designee, determines a mail cover was improperly ordered, all data acquired while the cover was in force shall be destroyed, and the requesting authority notified of the discontinuance of the mail cover and the reasons therefor.

(3) Any data concerning mail covers shall be made available to any mail cover subject in any legal proceeding through appropriate discovery procedures.

(4) The retention period for files and records pertaining to mail covers shall be 8 years.

(i) **Reporting to requesting authority.** Once a mail cover has been duly ordered, authorization may be delegated to any employee in the Postal Inspection Service to transmit mail cover reports directly to the requesting authority.

(j) **Review.**

(1) The Chief Postal Inspector, or his designee at Inspection Service Headquarters shall periodically review mail cover orders issued by the Manager, Inspection Service Operations Support Group or their designees to ensure compliance with these regulations and procedures.

(2) The Chief Postal Inspector shall select and appoint a designee to conduct a periodic review of national security mail cover orders.

(3) The Chief Postal Inspector's determination in all matters concerning mail covers shall be final and conclusive and not subject to further administrative review.

(k) **Military postal system.** Title 39, Code of Federal Regulations, Section 233.3 does not apply to the military postal system overseas or to persons performing military postal duties overseas. Information about regulations prescribed by the Department of Defense for the military postal system overseas may be obtained from the Department of Defense.

Exhibit 2

Inspection Service Operations Support Group Managers

Geographical jurisdictions are shown by state. When a state is split between ISOSGs, the first 3 digits of ZIP Codes are shown by asterisk(*).

Newark ISOSG: INSPECTION SERVICE OPERATIONS SUPPORT GROUP

Two Gateway Center - 9th Floor

Newark, NJ 07175-0001

Jurisdiction: CT, MA, ME, NH, NJ, NY, RI, VT, Puerto Rico, Virgin Islands

---

Bala Cynwyd ISOSG: INSPECTION SERVICE OPERATIONS SUPPORT GROUP

POB 3000

Bala Cynwyd PA 19004-3609

Jurisdiction: DC, DE, KY, MD, NC, *NJ, OH, PA, SC, VA, WV

*ZIP Codes 080-086 only

Chicago ISOSG: INSPECTION SERVICE OPERATIONS SUPPORT GROUP

222 S. Riverside Plaza - Suite 1250

Chicago IL 60606-6100

Jurisdiction: CO, IA, IL, IN, KS, MI, MN,MO, NE, ND, SD, UT, WI, WY

Memphis ISOSG: INSPECTION SERVICE OPERATIONS SUPPORT GROUP

225 N. Humphreys Blvd., 4th Floor South

Memphis TN 38161-0009

Jurisdiction: AL, AR, FL, GA, LA, MS, OK, TN, TX

San Bruno ISOSG: INSPECTION SERVICE OPERATIONS SUPPORT GROUP

PO Box 9000

South San Francisco CA 94083-9000

AK, AZ, CA, HI, ID, MT, NV, NM, OR, WA

Exhibit 3. Sample Request - Criminal Violation

(Letter/Memo)

(Numbers in parentheses correspond to instructions in III-B.)

Department of Justice

Drug Enforcement Administration

[DATE]

ISOSG MANAGER

US POSTAL INSPECTION SERVICE

PO BOX 9000

SOUTH SAN FRANCISCO CA 94083-9000

ATTN: MAIL COVER SPECIALIST

Restricted Information

(1-Justification - Brief case description and purpose)

This is a request for a mail cover to acquire evidence of a commission or attempted commission of a crime. Our informant advised that a sizable quantity of cocaine will be mailed to John Doe, 1234 Main Street, San Francisco, CA 12345-6789 from Tucson, AZ, on or about June 6. The suspect shipment was ordered on or about June 1. The mail cover will provide information regarding the source of the drugs and also information concerning financial assets the subject may have that were derived from the above described drug activity which may be subject to forfeiture under law.

(2-Subject)

The cover subject is:

JOHN DOE (AND ALL OTHER NAMES)

1234 MAIN STREET

SAN FRANCISCO CA 12345-6789

The subject of this request was convicted in 1988 and again in 1992 for drug trafficking, and our informant has personally made two buys from him.

All other names should be covered because recidivists often use aliases. Mail delivered to this address is intended for John Doe and, to our knowledge, no one else receives mail at the same address.

(3-Mail Class)

The mail cover should include information from both sealed and unsealed mail since past experience indicates that drugs are transported by both of these mail categories.

(4-Time Frame)

Cover is requested for 30 days, to begin as soon as possible.

(5-Violation)

Our investigation concerns a possible violation of 21 USC, 841(a), Possession of a Controlled Substance, punishable by up to 15 years in prison. Doe has not been indicted, but if he is formally charged during the 30 days requested, you will be promptly notified to terminate the mail cover.

(6-Attorney)

We are unaware of any legal representation for Doe. However, if this information becomes available, the name of his attorney will be relayed to you at once.

(7-Documentation)

Forms 2009, Information Concerning Mail Matter, will be needed on a weekly basis. We will not copy these forms. They will be returned to you within 60 days of the mail cover completion date.

(8-Special Instructions)

Postal Inspector J. Smith has been contacted regarding this case. (Provide complete name, address and phone number for case agent if different than requester).

(Signature)

R. Jones

Supervising Agent

Drug Enforcement Administration

Phone: (000)123-1234

Exhibit 4. Sample Request - Forfeiture

Department of Treasury

Internal Revenue Service

[DATE]

ISOSG MANAGER

US POSTAL INSPECTION SERVICE

PO BOX 9000

SOUTH SAN FRANCISCO CA 94083-9000

ATTN: MAIL COVER SPECIALIST

Restricted Information

(1-Justification)

This is a request for a mail cover to assist in the identification of property, proceeds or assets forfeitable under law. Our investigation has developed evidence that the subject J. Doe, 123 Main Street, San Francisco, CA 12345-6789 is engaged in money laundering.

(2-Subject)

The cover subject is:

J. Doe (AND ALL OTHER NAMES)

123 MAIN STREET

SAN FRANCISCO CA 12345-6789

All other names should be covered because the information developed in this investigation indicates that Doe is using different names to facilitate his money laundering operation. This address is a single family house. Mail delivered to this address is intended for J. Doe and, to our knowledge, no one else receives mail at the same address.

(3-Mail Class)

The mail cover should include information from sealed mail.

(4-Time Frame)

Cover is requested for 30 days, to begin as soon as possible.

(5-Violation)

Our investigation has disclosed evidence that Doe is engaged in money laundering activity in violation of 18 U.S.C., 1956 and this cover will help identify proceeds and other assets which are subject to forfeiture under 18 U.S.C., 981, Civil Forfeiture. Doe has not been indicted, but if he is formally charged during the 30 days requested, you will be promptly notified to terminate the mail cover.

(6-Attorney)

We are unaware of any legal representation for Doe. However, if this information becomes available, the name of his attorney will be relayed to you at once.

(7-Documentation)

Forms 2009, Information Concerning Mail Matter, will be needed on a weekly basis. We will not copy these forms. They will be returned to you within 60 days of the mail cover completion date.

(8-Special Instructions)

Information concerning accounts with banks or other financial institutions will be especially helpful.

(Provide complete name, address and phone number for case agent if different than requester.)

(Signature)

T. Smith, Director

Criminal Division

Internal Revenue Service

Phone: (000)123-1234

Exhibit 5 Sample Request - Fugitive

Oregon State Police

[DATE]

ISOSG MANAGER

US POSTAL INSPECTION SERVICE

PO BOX 9000

SOUTH SAN FRANCISCO CA 94083-9000

ATTN: MAIL COVER SPECIALIST

Restricted Information

(1-Justification)

The Oregon State Police is presently conducting a fugitive investigation involving R. Doe who has failed to surrender for disposition of sentence.

(2-Subject)

The subject of this mail cover request is Jane Doe, who is R. Doe's mother and is believed to be in contact with the fugitive. She lives at 123 Broadway, Anytown, USA. This address is the focus of the Mail

Cover request because it is believed that the fugitive may be communicating with his mother by mail. A mail cover is necessary to attempt to locate the fugitive.

The cover subject is:

JANE DOE

123 BROADWAY

ANYTOWN, USA 12345-6789

(3-Mail Class)

The mail cover should include information from sealed mail.

(4-Time Frame)

Cover is requested for 30 days, to begin as soon as possible.

(5-Violation)

R. Doe was originally charged with distribution of narcotics. A warrant for R. Doe's arrest has been issued by the authority of Oregon Statute 3146 (A2), Penalty for failure to appear. This offense is a felony punishable by imprisonment for a term of 15 years or more. The subject, Jane Doe, has not been indicted, but if she is formally charged during the 30 days requested, you will be promptly notified to terminate the mail cover.

(6-Attorney)

It is unknown if the fugitive R. Doe or the subject Jane Doe are represented by counsel at this time. However, if this information becomes available, the name of the attorney will be relayed to you at once.

(7-Documentation)

Forms 2009, Information Concerning Mail Matter, will be needed on a weekly basis. We will not copy these forms. They will be returned to you within 60 days of the mail cover completion date.

(8-Special Instructions)

(Provide complete name, address and phone number for case agent if different than requester.)

(Signature)

T. Jones

Oregon State Police

Phone: (000)123-1234

Exhibit 6. Form 2009

Information Concerning Mail Matter

RESTRICTED INFORMATION

U.S. POSTAL SERVICE INFORMATION CONCERNING MAIL MATTER	YOUR FILE NO. 951249	FILE DATE
TO (*Name of Postal Inspector*) INSPECTION SERVICE OPERATION SUPPORT GROUP	FROM (*Post Office*) MEMPHIS, TN	DATE 5/22/
ADDRESS (*City, State and ZIP Code*) PO BOX 6667 MEMPHIS TN 38161-0011	The delivery of mail was not delayed while obtaining this info POS	

THE FOLLOWING INFORMATION IS FURNISHED IN COMPLIANCE WITH YOUR REQUEST

ADDRESSEE	SENDER	RETURN ADDRESS	PLACE AND DATE OF POSTMARK	METER NUMBER	CLA OF M
JOHN DOE	JANE TREE	123 N. FRONT ST. MEMPHIS, TN 38166-1234	3RD STREET PO 5-9-95	7231154	FIRST CL

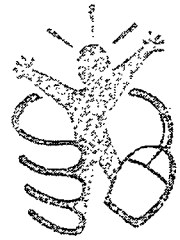
SAMPLE

MAIL THIS FORM IN TWO, OPAQUE ENVELOPES. DO NOT USE WINDOW ENVELOPES.
THE INNER ENVELOPE MUST BE MARKED "RESTRICTED INFORMATION."

PS Form 2009
June 1981

RESTRICTED INFORMATION

Exploited Child Unit



CYBERTIPLINE

www.cybertipline.com

The Public's Resource for Protecting Children Online

The National Center for Missing and Exploited Children

PCO-UC-Resources-1

Exploited Child Unit

- How many children are on the Internet?
- Dangers to Children Online
- Resources for Parents
- CyberTipline (www.cybertipline.com)
- Resources for Law Enforcement

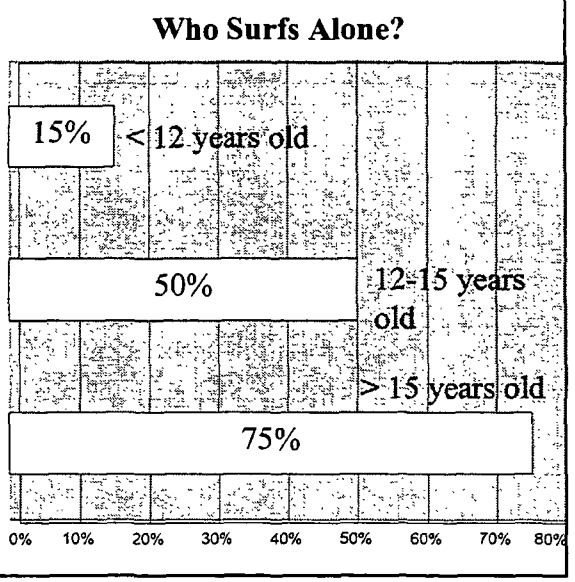
PCO-UC-Resources-2

Kids and the Internet

The majority of US children over the age of 12 are allowed to surf the Web unsupervised, according to a recent survey by Greenfield Online.

The study found that only 5 percent of parents with children over the age of 16 attempt to monitor their online activities, with just 20 percent of parents using software to control the type of material their children can access online.

Greenfield estimates that 55 percent of children aged 11 and over use the Net for school work, while 20 percent of parents with children in this age group say that they are more interested in the Net than in TV.

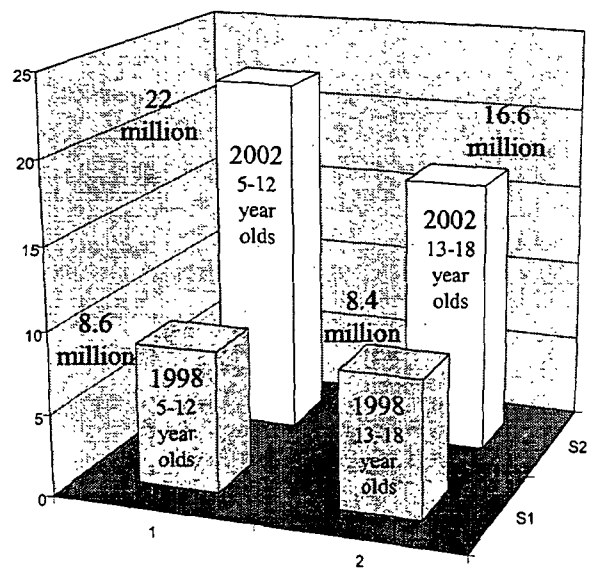


PCO-UC-Resources-3

Kids and the Internet

KIDS ONLINE

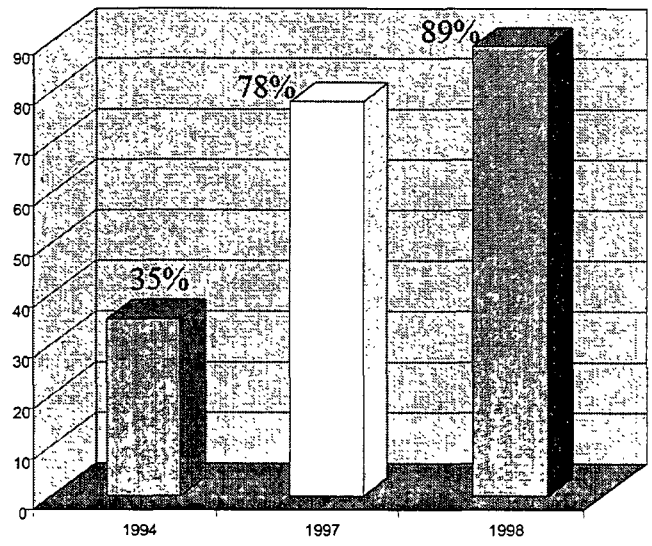
Last year, about 8.6 million kids ages 5 to 12 and 8.4 million ages 13 to 18 were online; Jupiter predicts the numbers will be 22 million and 16.6 million, respectively, by 2002.



PCO-UC-Resources-4

Classrooms Online

From 1997 to 1998, Web connectivity in public schools increased to 89 percent.

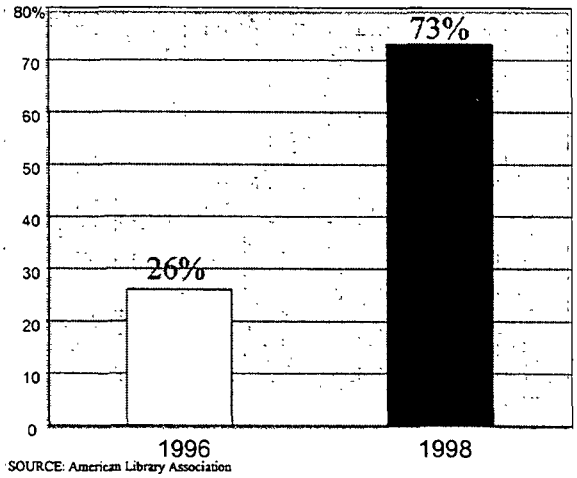


PCO-UC-Resources-5

Libraries and the Internet

The Internet is an ideal tool for research and education. In just a few years many public libraries have incorporated this new medium into their everyday service for patrons. The American Library Association released a study that shows 73 percent of public libraries offer Net terminals.

Net Access at Libraries has Increased

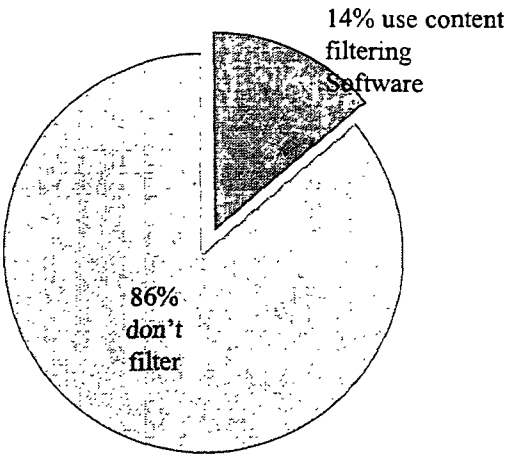


SOURCE: American Library Association

PCO-UC-Resources-6

Libraries and the Internet

Unfortunately, few of these libraries currently filter content. The ability to place filters on library computers is a top topic. In early 1998, a federal district court barred the Loudoun County public library from using filtering software to block access to Net porn.



SOURCE: American Library Association

PCO-UC-Resources-7

Dangers on the Internet

Access to Inappropriate Material

SPAM

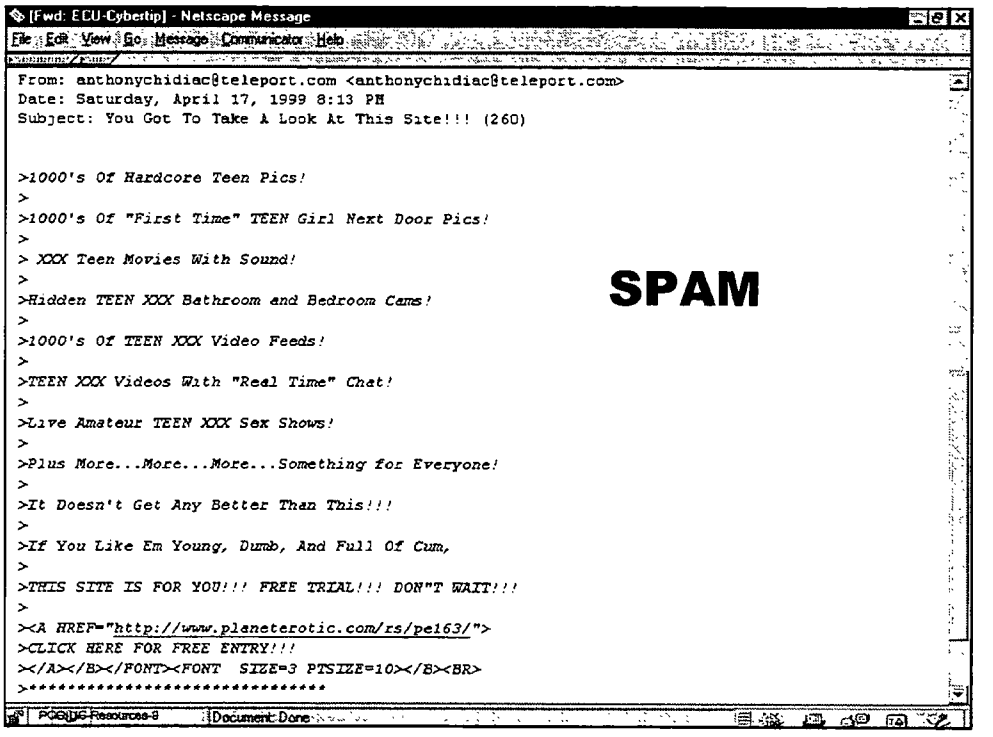
Child Pornography

Fraud

Online Enticement

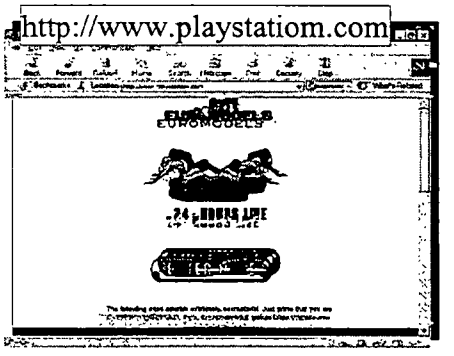
Stalking

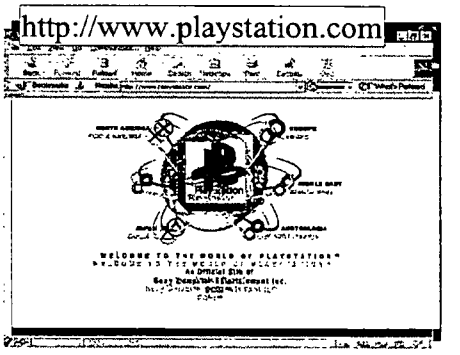
PCO-UC-Resources-8



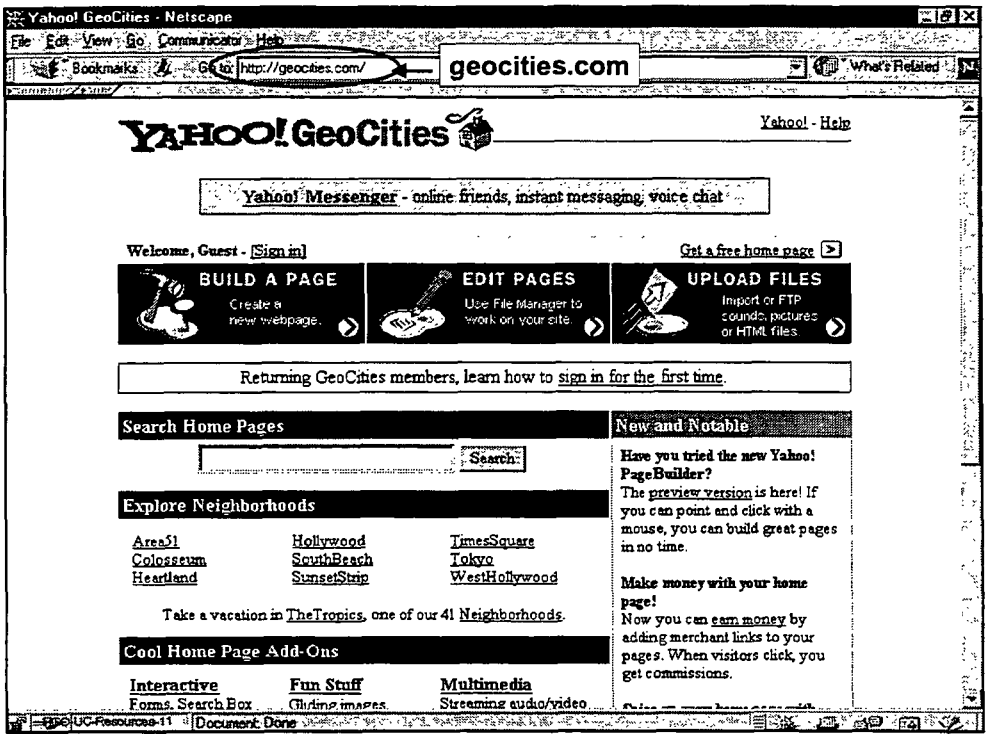
SPAM

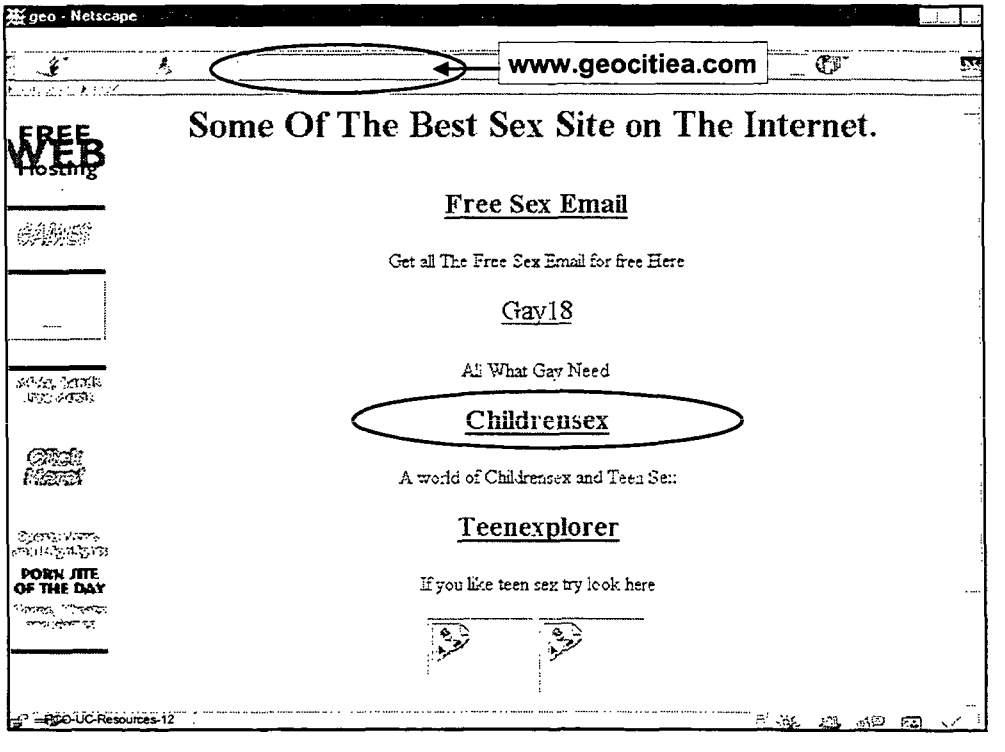
Dangers Online

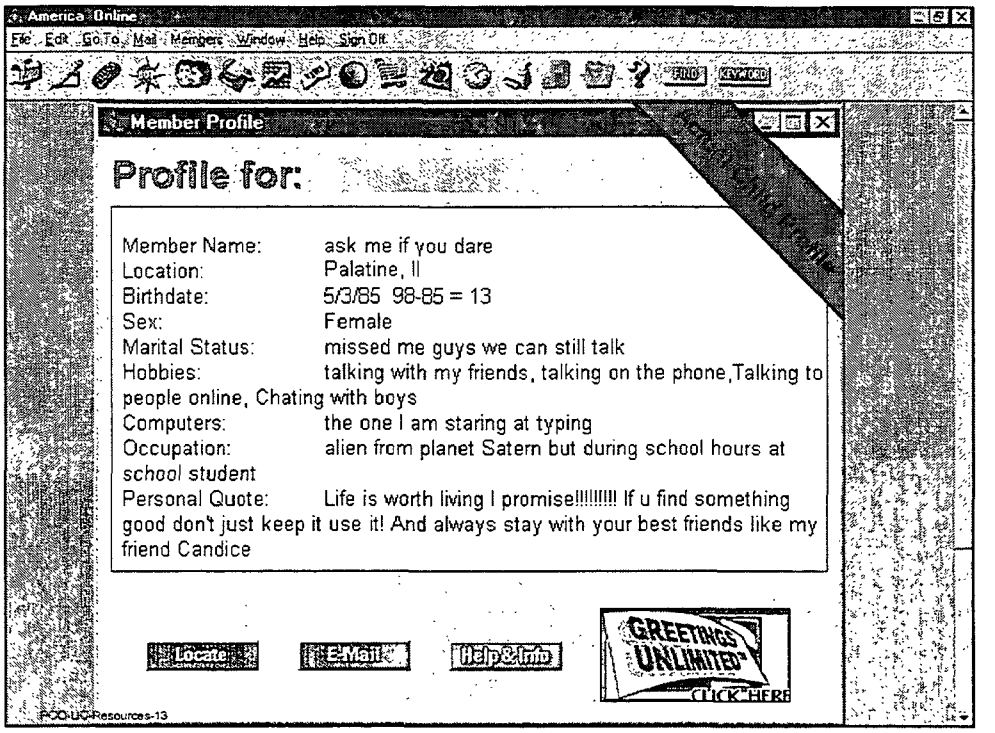


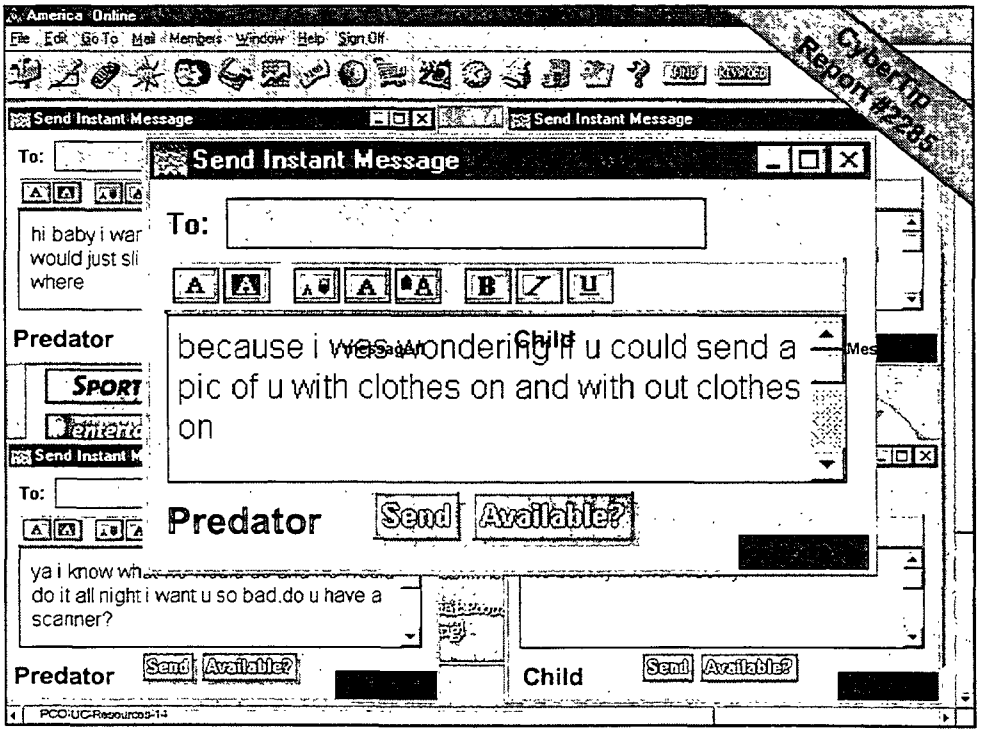


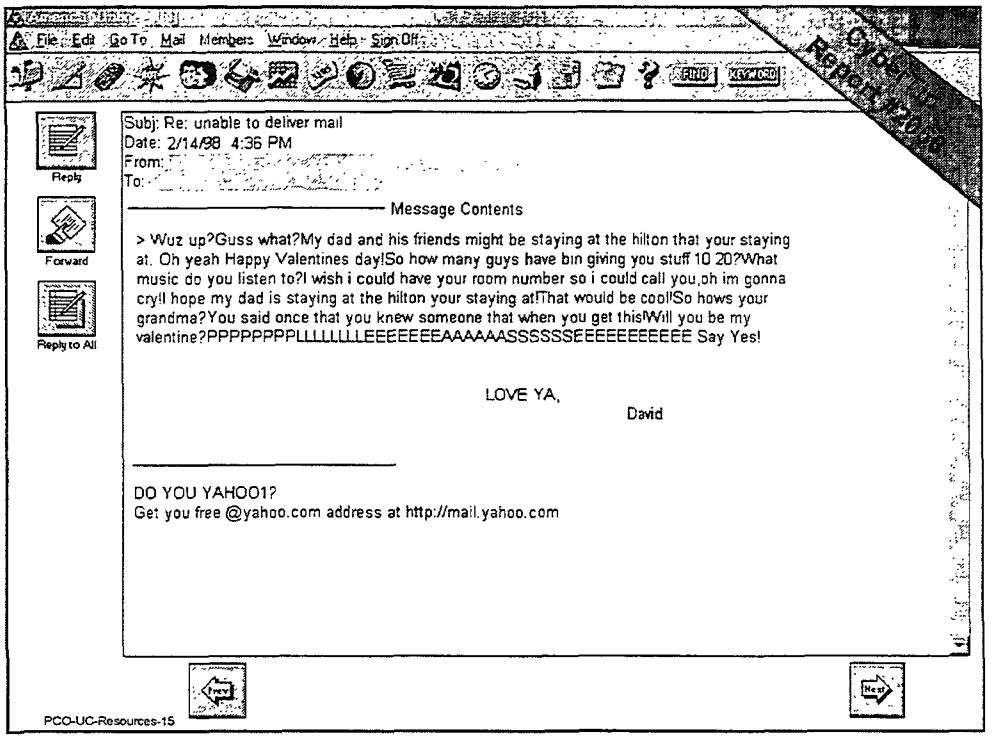
There are approximately 4 million pornographic websites, newsgroups and chatrooms on the Internet.

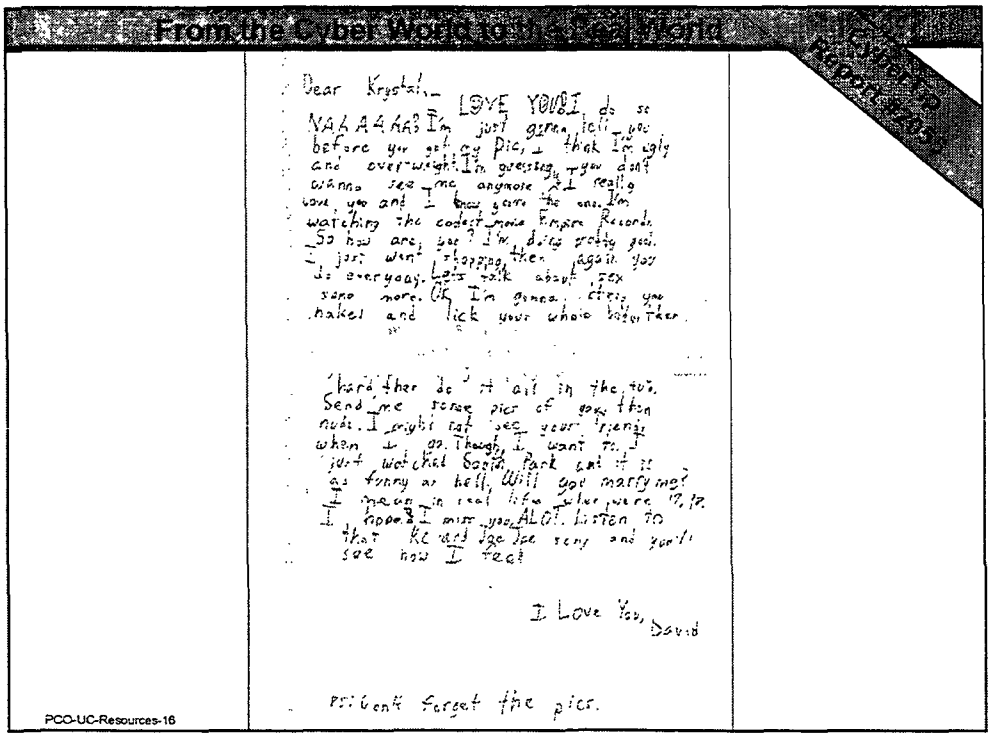

Yahoo! GeoCities - Netscape
File Edit View Go Communicator Help
Bookmarks Go to: http://geocities.com/
geocities.com
What's Related
YAHOO! GeoCities
Yahoo! - Help
Yahoo! Messenger - online friends, instant messaging, voice chat
Welcome, Guest - [Sign in]
Get a free home page
BUILD A PAGE
Create a new webpage.
EDIT PAGES
Use File Manager to work on your site.
UPLOAD FILES
Import or FTP sounds, pictures or HTML files.
Returning GeoCities members, learn how to sign in for the first time.
Search Home Pages
Search:
Explore Neighborhoods
Area51
Colosseum
Heartland
Hollywood
SouthBeach
SunsetStrip
TimesSquare
Tokyo
WestHollywood
Take a vacation in TheTropics, one of our 41 Neighborhoods.
Cool Home Page Add-Ons
Interactive
Forms, Search Box
Fun Stuff
Gliding images
Multimedia
Streaming audio/video
New and Notable
Have you tried the new Yahoo! PageBuilder?
The preview version is here! If you can point and click with a mouse, you can build great pages in no time.
Make money with your home page!
Now you can earn money by adding merchant links to your pages. When visitors click, you get commissions.
UC-Resources-11
Document: Done


geo - Netscape
www.geocitiea.com
FREE WEB Hosting
Some Of The Best Sex Site on The Internet.
Free Sex Email
Get all The Free Sex Email for free Here
Gay18
All What Gay Need
Childrensex
A world of Childrensex and Teen Sex
Teenexplorer
If you like teen sex try look here
PORN SITE OF THE DAY
UC-Resources-12


America Online
File Edit Go To Mail Members Window Help Sign Off
Member Profile
Profile for:
Member Name: ask me if you dare
Location: Palatine, Il
Birthdate: 5/3/85 98-85 = 13
Sex: Female
Marital Status: missed me guys we can still talk
Hobbies: talking with my friends, talking on the phone,Talking to people online, Chating with boys
Computers: the one I am staring at typing
Occupation: alien from planet Satern but during school hours at school student
Personal Quote: Life is worth living I promise!!!!!!!! If u find something good don't just keep it use it! And always stay with your best friends like my friend Candice
Locate
E-Mail
Help&Info
GREETINGS UNLIMITED
CLICK HERE
PCO-UC-Resources-13


America Online
File Edit Go To Mail Members Window Help Sign Off
CyberTip Report #2285
Send Instant Message
To:
hi baby i war
would just sli
where
Predator
Send Instant Message
To:
because i wonder if u could send a pic of u with clothes on and with out clothes on
Child
Predator
Send
Available?
ya i know wh
do it all night i want u so bad.do u have a scanner?
Predator
Send
Available?
Child
Send
Available?
PCO-UC-Resources-14


File Edit Go To Mail Members Window Help Sign Off
Cyber Tip Report #2000
Reply
Forward
Reply to All
Subj: Re: unable to deliver mail
Date: 2/14/98 4:36 PM
From:
To:
Message Contents
> Wuz up?Guss what?My dad and his friends might be staying at the hilton that your staying at. Oh yeah Happy Valentines day!So how many guys have bin giving you stuff 10 20?What music do you listen to?I wish i could have your room number so i could call you,oh im gonna cry!I hope my dad is staying at the hilton your staying at!That would be cool!So hows your grandma?You said once that you knew someone that when you get this!Will you be my valentine?PPPPPPPPLLLLLLLLEEEEEEEAAAAAASSSSSSEEEEEEEEEEE Say Yes!
LOVE YA,
David
DO YOU YAHOO!?
Get you free @yahoo.com address at http://mail.yahoo.com
Prev
Next
PCO-UC-Resources-15


From the Cyber World to the Real World
Cyber Tip Report #2000
Dear Krystal,
LOVE YOU!
I do so
NAAAAAA? I'm just gonna tell you
before you get my pic, I'm ugly
and over-weight. I'm guessing you don't
wanna see me anymore :(I really
love you and I know you're the one. I'm
watching the coolest movie Empire Records.
So how are you? I'm doing pretty good.
I just went shopping then again you
do everyday. Let's talk about sex
some more. Ok I'm gonna strip you
naked and lick your whole body then
Then do it all in the tub.
Send me some pics of you then
nude. I might not see your friends
when I go. Though I want to.
just watched Sarah Park and it is
so funny as hell. Will you marry me?
I mean in real life where we're 18 yr.
I hope. I miss you ALOT. Listen to
that KC and Jojo song and you'll
see how I feel
I Love You, David
P.S. don't forget the pics.
PCO-UC-Resources-16

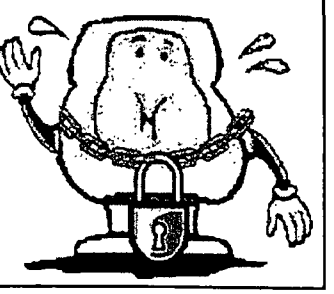
Prevention/Awareness Resources

CYBERTIPLINE
The Public's Resource for Protecting Children Online
www.cybertipline.com

Exploited Child Unit
The National Center for Missing and Exploited Children

Online Safety Kit

- **Filters**
- **Monitors**
- **Kid-Browser**
- **Kid-safe search engines**
- **Proxy Servers**

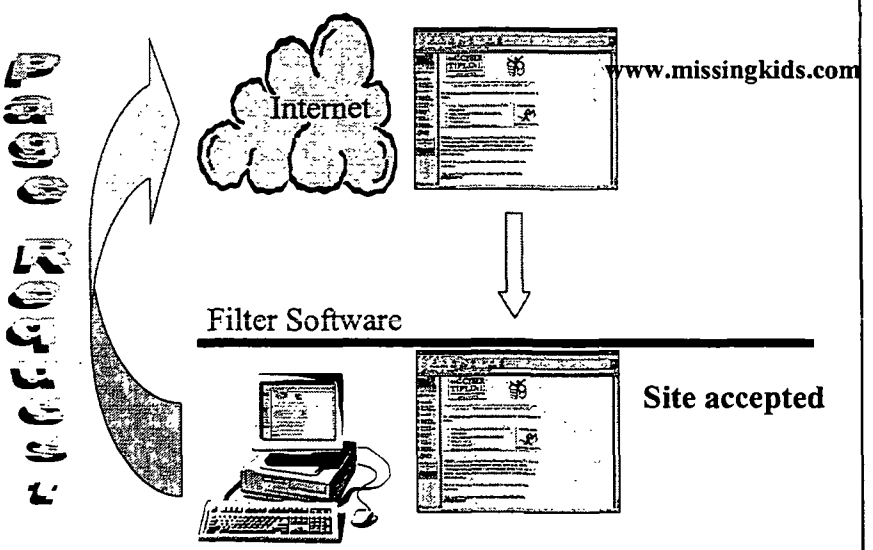


Filters

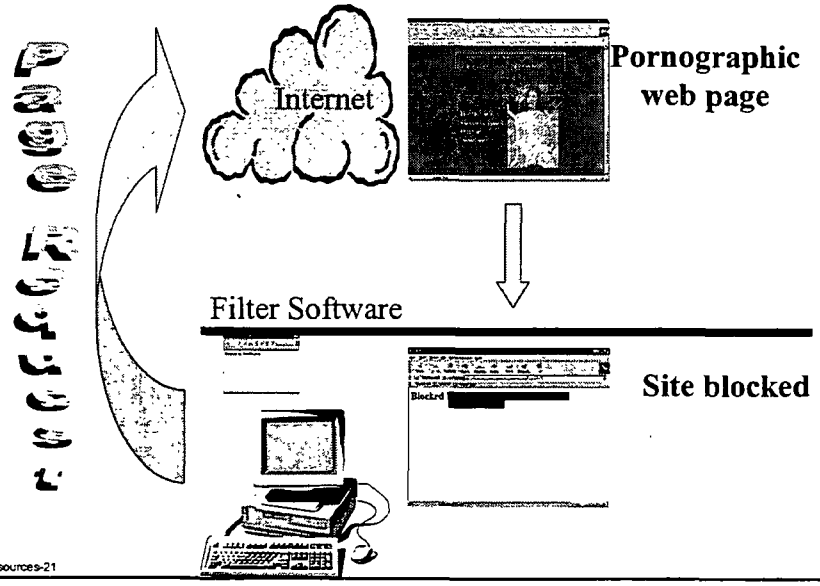
Filters are software programs that prevent users from viewing material found on the Internet. This process has two components.

- **Rating**
- **Filtering**

Filter Sequence of Events

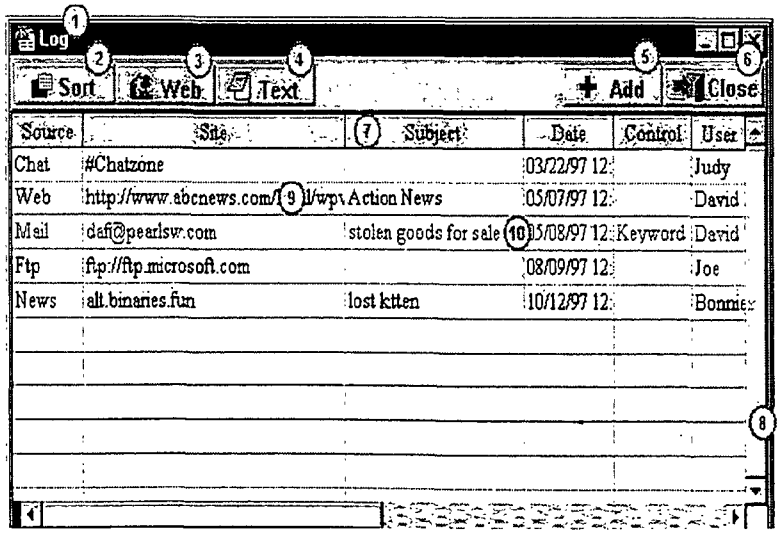


Filter Sequence of Events

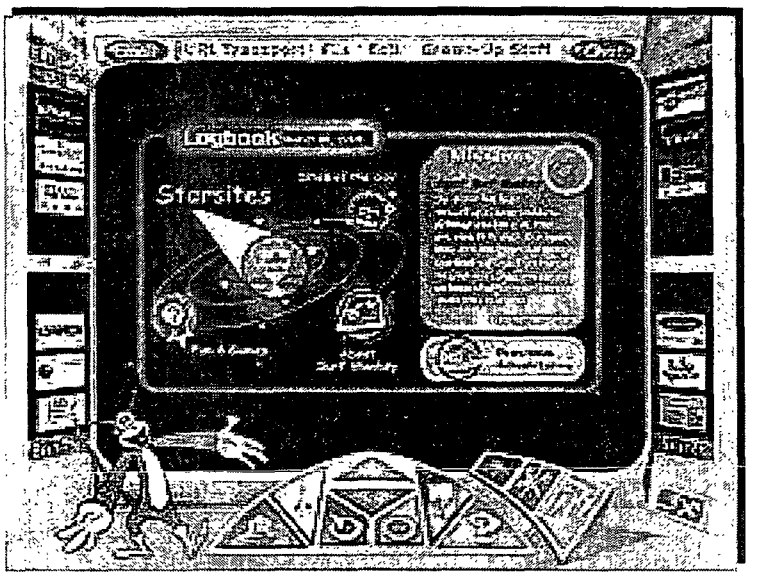


PCO-UC-Resources-21

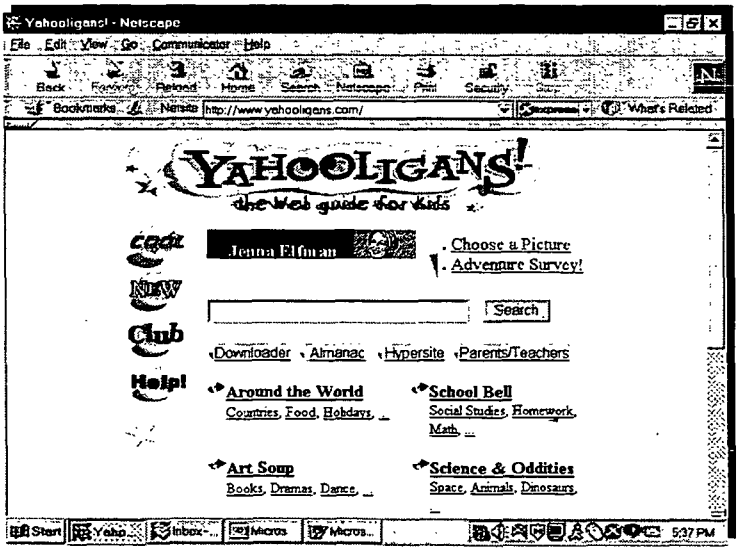
Monitors



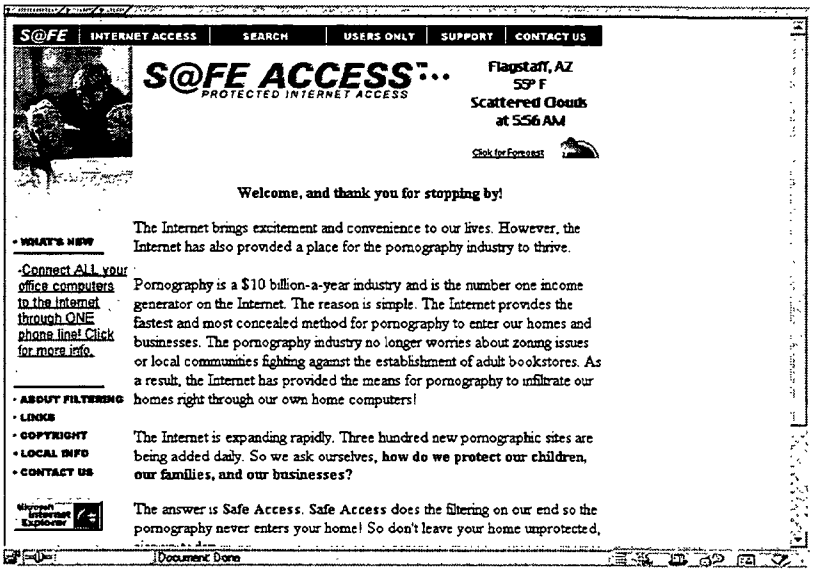
Web Browsers for Children



Search Engines for Children

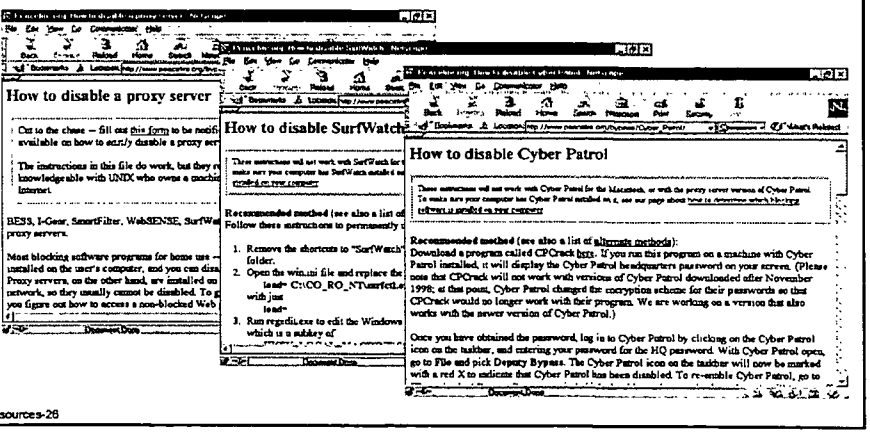


ISPs Offering Filter Technology



Technology is NO Substitute

The majority of parental control products can be defeated.



#1 Rule

GET INVOLVED: Supervise your children when they're online, just as you do during other activities. Software, the government, standards organizations-none can replace Mom or Dad as co-pilot.

Child Safety on the Information Highway

http://www.missingkids.com

- What Are The Risks?
- How Parents Can Reduce The Risks
- Guidelines For Parents
- My Rules For Online Safety

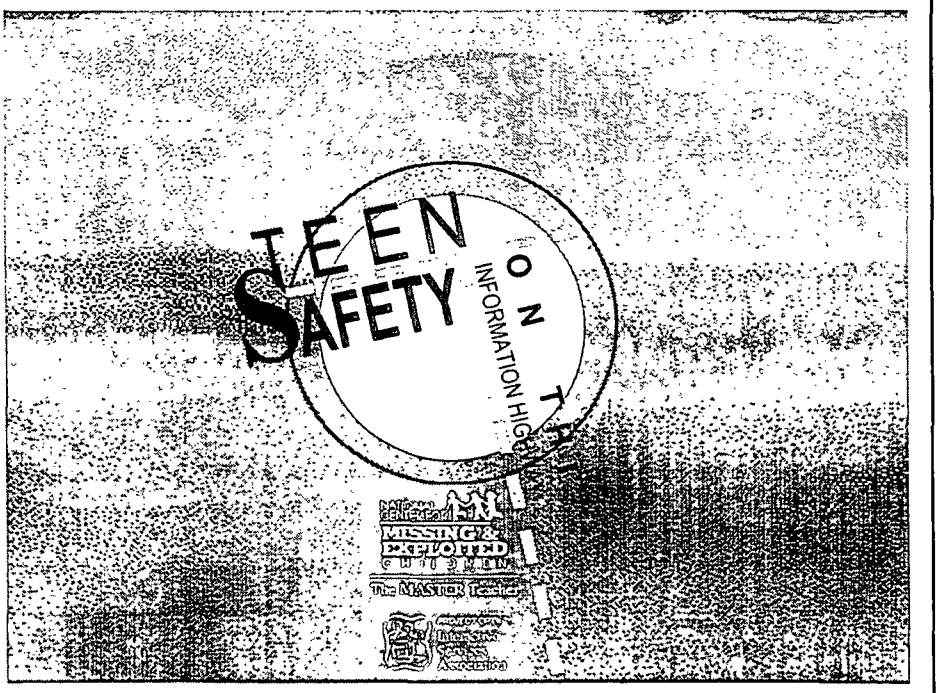
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

INTERACTIVE SERVICES ASSOCIATION

Enticement or Runaway Cases

- A statistical review of NCMEC data indicates that in the cases where children are lured or voluntarily runaway because of a relationship or friendship developed online, 83% of that population is 15 years or older, and 75% of that same population is female.

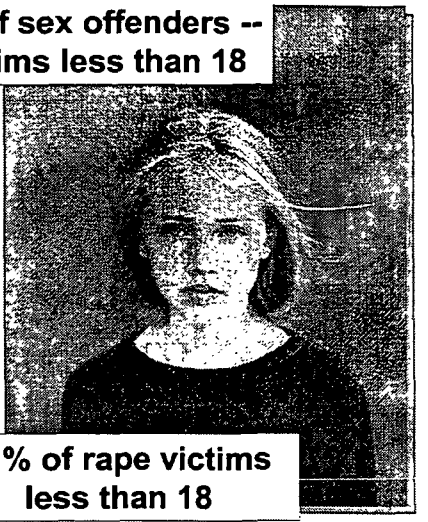
PCO-UC-Resources-29



PCO-UC-Resources-30

Teenage Victims

2/3 of sex offenders -- victims less than 18



61% of rape victims less than 18

✳Teenage girls are the most frequent victims of sexual assault.

PCO-UC-Resources-31

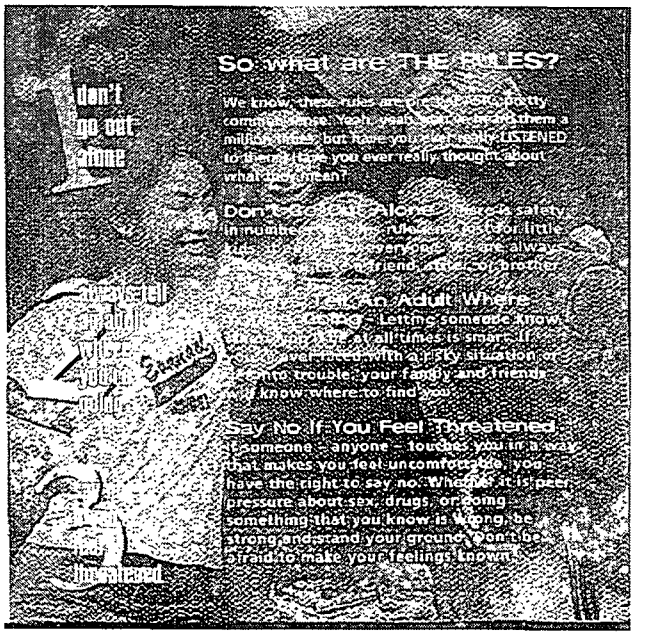
Child Empowerment Campaign

THE RULES

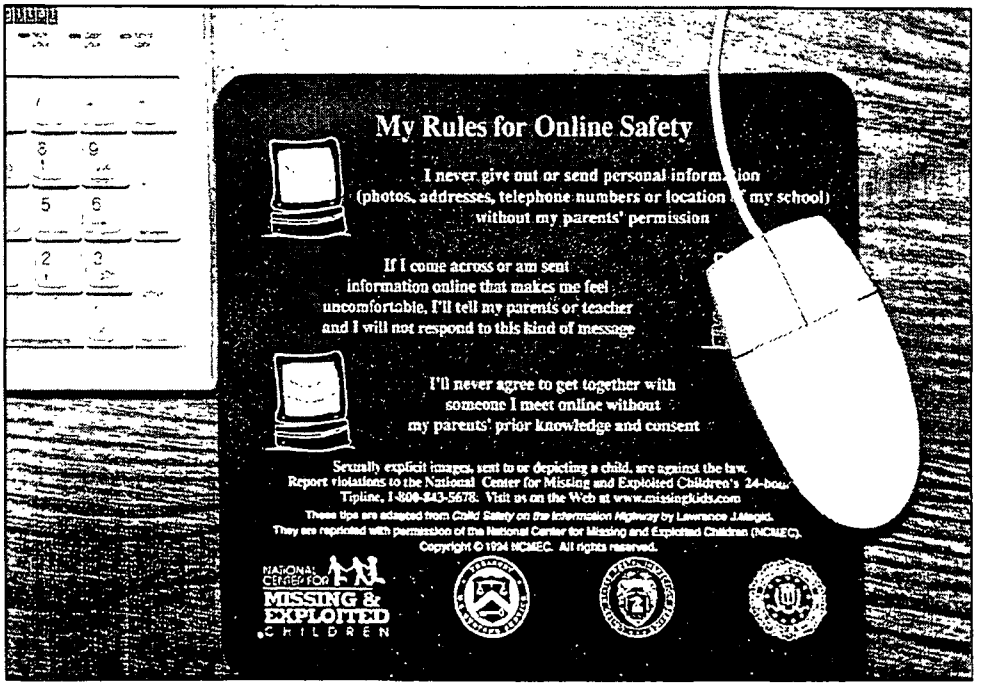
1. Don't go out alone

2. Always tell an adult where you're going

3. Say no if you feel threatened



PCO-UC-Resources-33



You're one click away ...

Mor you're one click away...

GetNetWise

Safety Guide | Tools | Reporting Trouble | Kid Sites | Glossary | About GetNetWise

The Internet offers kids many opportunities for learning, constructive entertainment, and personal growth. At the same time, parents are concerned about the risks kids face online. The challenge for parents is to educate themselves and their children about how to use the Internet safely. GetNetWise can help.

Online Safety Guide

Learn about the risks kids face online, based on age levels or types of activities. Also: Quick tips for kids, teens, and families.

Tools for Families

Search or browse for Internet safety products, including those that filter explicit or violent content, monitor a child's Internet access, or limit time online. See sample contracts for kids' Internet use.

Reporting Trouble

How Can GetNetWise Help?

GetNetWise is a resource for families and caregivers to help kids have safe, educational, and entertaining online experiences. We include a glossary of Internet terms, a guide to online safety, directions for reporting online trouble, a directory of online safety tools, and great sites for kids to visit.

What's This All About?

GetNetWise is a public service

The CyberTipline:

Your Resource for Reporting the Sexual Exploitation of Children

The Internet has created an exciting new world of information and communication for anyone with access to online services. While this world offers unparalleled opportunities for children and adults to learn about the universe we live in, some risks and dangers exist for children as they travel through Cyberspace. This may include access to illegal content on the web or receiving inappropriate and unsolicited E-mail or chat messages. In addition, individuals who prey on children have quickly adapted to the online environment of the Information Age and often use computer technology to seek unsupervised access to and contact with children.

To better safeguard children while online, key public- and private-sector leaders joined with the National Center for Missing & Exploited Children® (NCMEC) on March 9, 1998, to launch the CyberTipline. The CyberTipline was created for individuals to report incidents of child-sexual exploitation including:

- Possession, manufacture, and distribution of child pornography
- Online enticement of children for sexual acts
- Child prostitution
- Child-sex tourism
- Child-sexual molestation (not in the family)

SEVEN DAYS PER WEEK, 24 HOURS PER DAY, NCMEC IS FULLY STAFFED TO HANDLE LEADS AND THEN DISTRIBUTE THOSE LEADS TO THE APPROPRIATE LAW-ENFORCEMENT AGENCIES.

HOW DOES THE CYBERTIPLINE WORK?

- When children believe that someone is trying to entice them for sexual or illegal purposes or that they have found child pornography online, they tell their parents.
- The parents and child look to the CyberTipline, www.cybertipline.com, and fill out an online report form for child-sexual exploitation.
- NCMEC CyberTipline Operators retrieve and prioritize each lead. Then the report is immediately reviewed and analyzed by NCMEC's Exploited Child Unit (ECU). This may include visiting a reported web site or newsgroup posting, contacting the complainant to gather additional information, and conducting searches using various Internet tools. The report is made available online to the Federal Bureau of Investigation; U.S. Customs Service; U.S. Postal Inspection Service; and, when known, forwarded to the state and local law-enforcement agency where the incident occurred.

YOU CAN HELP

Cyberspace is being used in a number of ways to target and sexually victimize children. The best way to reduce the risks in Cyberspace is to understand the potential dangers, watch for abuses, and immediately report them. Using the CyberTipline will help tremendously in the fight against child-sexual exploitation on the Internet.

SUCCESS STORIES

The CyberTipline has received thousands of leads from parents, teachers, clergy, law enforcement, and many other concerned people who want to better safeguard children while they are exploring on the Internet. Many of these leads have taken children out of harm's way.

- The CyberTipline received a lead about the location of a runaway who was involved in child prostitution. The lead was forwarded to local law enforcement in Des Moines, Iowa, and the child was recovered.
- NCMEC credited a local resident and law enforcement in Orange County, Florida, for their quick response and resourcefulness in reporting information to the CyberTipline that resulted in the recent arrest of a 63-year-old Ruskin, Florida, man who was charged with 50 counts of sexual activity with a minor.
- The CyberTipline received a report from a mother in Helena, Montana, whose 16-year-old daughter ran away from home. The mother suspected that her daughter had taken a bus to Kansas City, Missouri, to visit with an adult she "met" via the Internet. NCMEC's ECU contacted the FBI, which in turn contacted its Kansas City field office. The child arrived in Kansas City and was greeted by federal agents. The suspect—a divorced male in his thirties—was also apprehended.
- The CyberTipline received a report regarding a web site that contained hundreds of images of child pornography. NCMEC's ECU contacted the U.S. Postal Inspection Service and they worked with local law enforcement who made an arrest in the case.

WHO WE ARE

The National Center for Missing & Exploited Children was established in 1984 as a private, nonprofit organization and serves as a clearinghouse of information on missing and exploited children per federal statutes 42 USC § 5771 and 42 USC § 5780. The 24-hour, toll-free Hotline and CyberTipline are open for those who have information on missing and exploited children at 1-800-THE-LOST (1-800-843-5678) and www.cybertipline.com.

In 1998 the U.S. Congress established the Exploited Child Unit within NCMEC. ECU is not an investigative agency, but rather a resource center and clearinghouse for parents, law enforcement, public and private agencies, legislators, and other professionals offering services including:

- Public awareness and prevention materials for law enforcement and parents on Internet safety and the issue of child-sexual exploitation
- Queries and database searches for law enforcement on cases of child-sexual exploitation
- Publications, training, and technical assistance for law enforcement on cases of child-sexual exploitation

FOR MORE INFORMATION ON THE SERVICES AND RESOURCES OFFERED BY NCMEC'S EXPLOITED CHILD UNIT, PLEASE VISIT WWW.CYBERTIPLINE.COM OR CALL 1-800-843-5678.

MISSING & EXPLOITED CHILDREN

CYBERTIPLINE

www.cybertipline.com

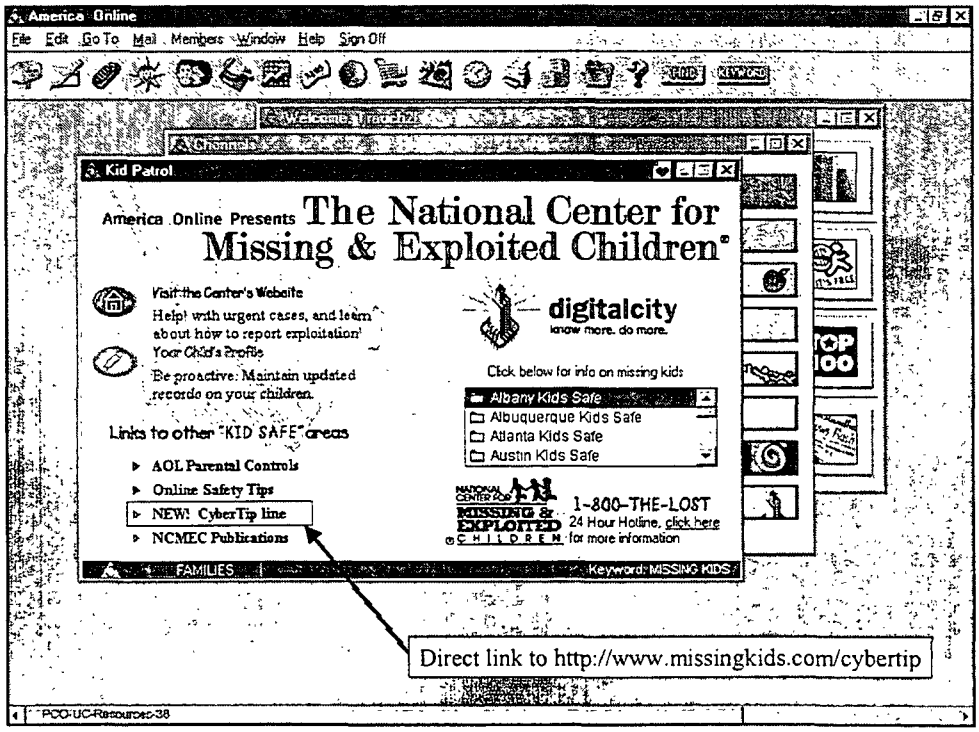
The Public's Resource for Protecting Children Online

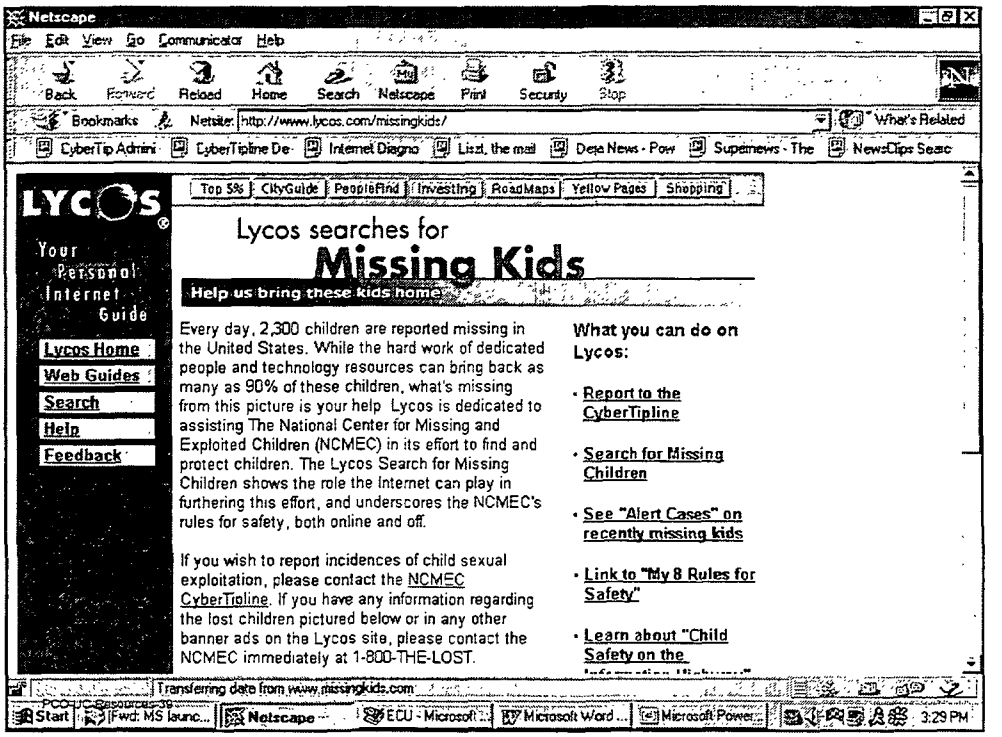
1-800-843-5678

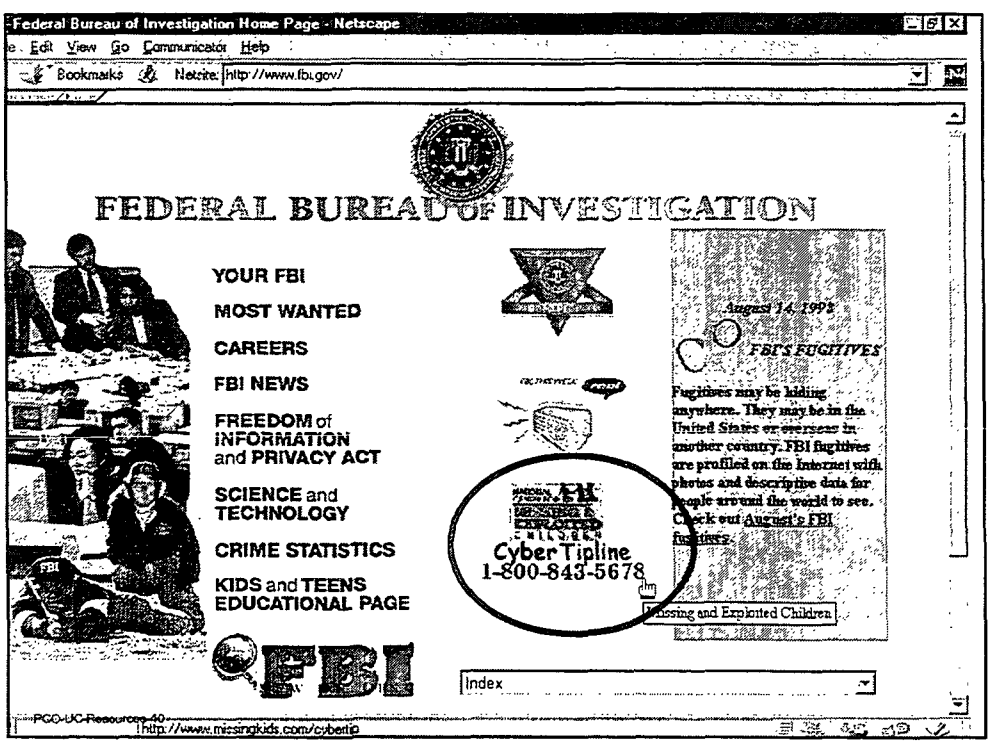
CyberTipline

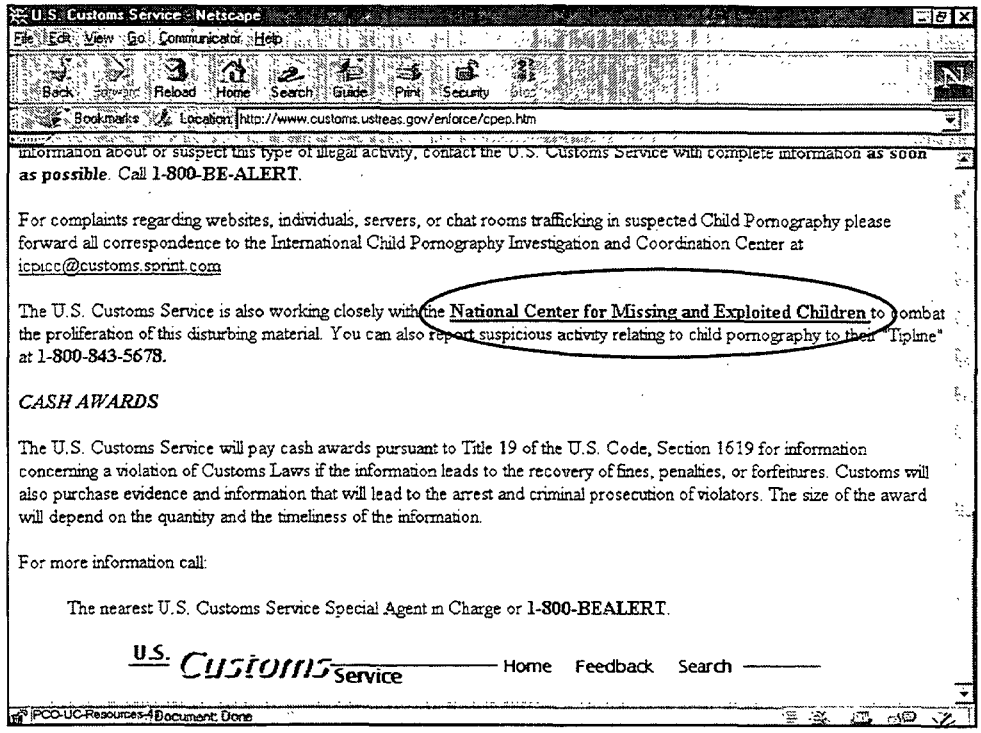
Public Service Announcement (PSA)

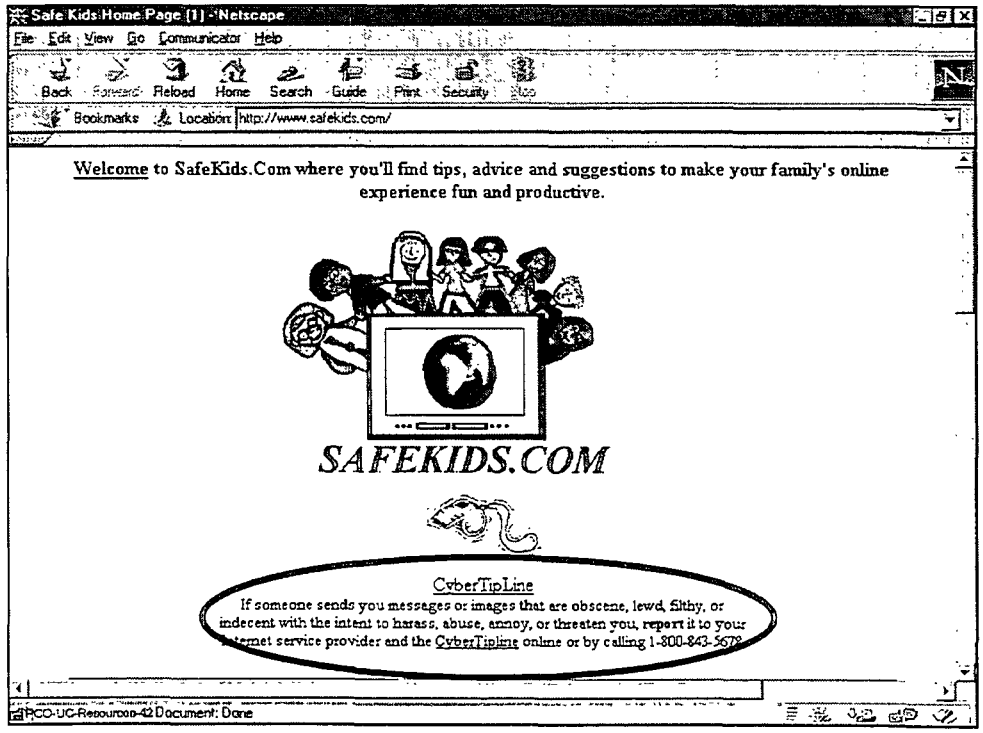
PCO-UC-Resources-37

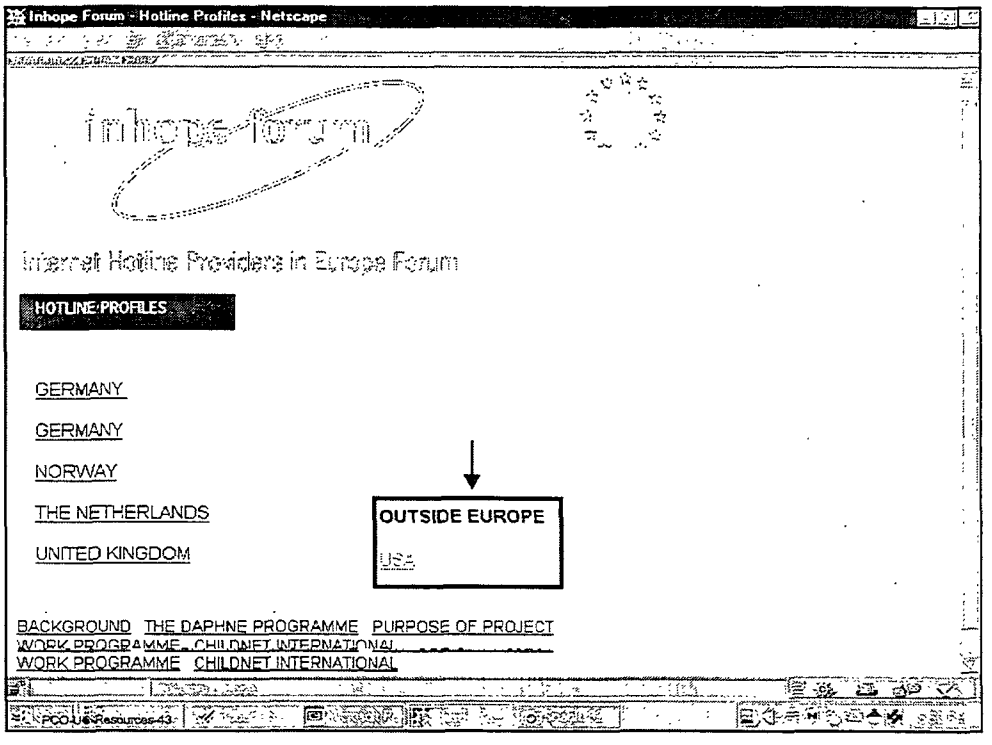


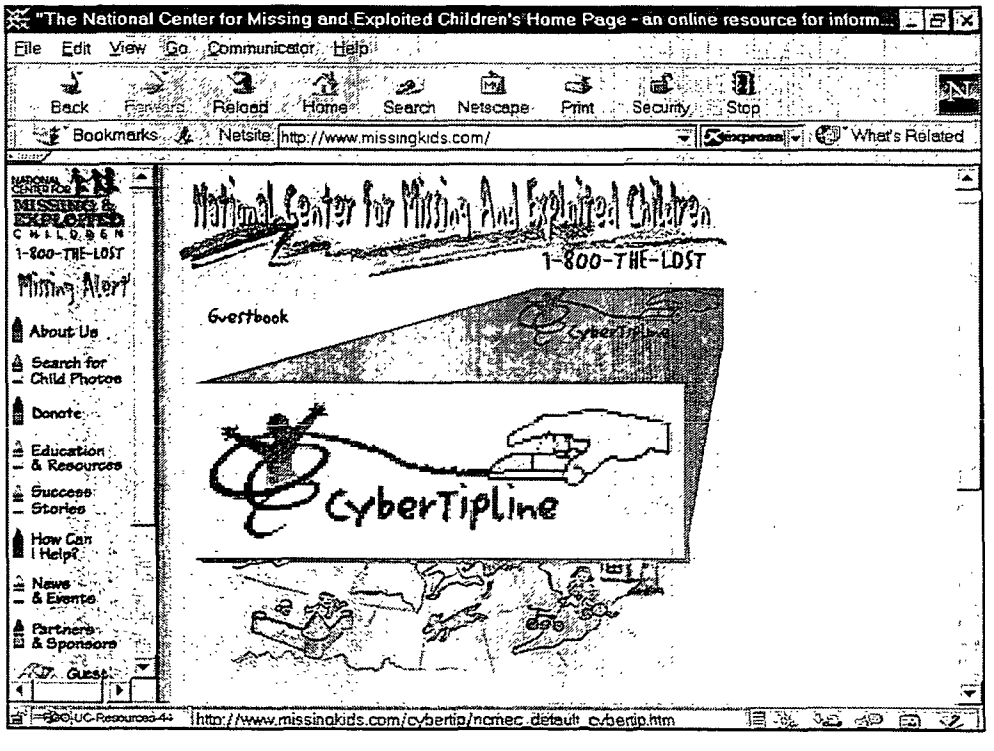

Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: http://www.lycos.com/missingkids/
What's Related
CyberTip Admini CyberTipline De Internet Diagno Lizst, the mail Dejа News - Pow Supernews - The NewsClips Searc
LYCOS
Your Personal Internet Guide
Lycos Home
Web Guides
Search
Help
Feedback
Top 5% CityGuide PeopleFind Investing RoadMaps Yellow Pages Shopping
Lycos searches for
Missing Kids
Help us bring these kids home
Every day, 2,300 children are reported missing in the United States. While the hard work of dedicated people and technology resources can bring back as many as 90% of these children, what's missing from this picture is your help. Lycos is dedicated to assisting The National Center for Missing and Exploited Children (NCMEC) in its effort to find and protect children. The Lycos Search for Missing Children shows the role the Internet can play in furthering this effort, and underscores the NCMEC's rules for safety, both online and off.
If you wish to report incidences of child sexual exploitation, please contact the NCMEC CyberTipline. If you have any information regarding the lost children pictured below or in any other banner ads on the Lycos site, please contact the NCMEC immediately at 1-800-THE-LOST.
What you can do on Lycos:
Report to the CyberTipline
Search for Missing Children
See "Alert Cases" on recently missing kids
Link to "My 8 Rules for Safety"
Learn about "Child Safety on the
Transferring data from www.missingkids.com
Start Fwd: MS launc... Netscape ECU - Microsoft ... Microsoft Word ... Microsoft Power... 3:29 PM

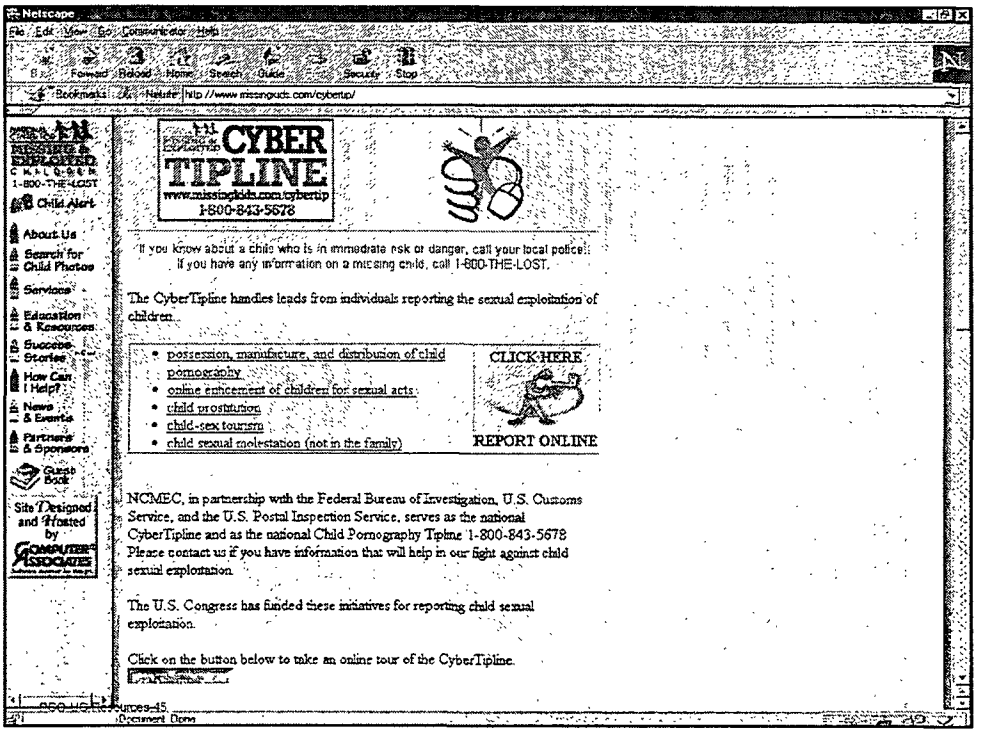

Federal Bureau of Investigation Home Page - Netscape
Edit View Go Communicator Help
Bookmarks Netsite: http://www.fbi.gov/
FEDERAL BUREAU OF INVESTIGATION
YOUR FBI
MOST WANTED
CAREERS
FBI NEWS
FREEDOM of INFORMATION and PRIVACY ACT
SCIENCE and TECHNOLOGY
CRIME STATISTICS
KIDS and TEENS EDUCATIONAL PAGE
FBI
August 14, 1998
FBI'S FUGITIVES
Fugitives may be hiding anywhere. They may be in the United States or overseas in another country. FBI fugitives are profiled on the Internet with photos and descriptive data for people around the world to see. Check out August's FBI fugitives.
CyberTipline
1-800-843-5678
Missing and Exploited Children
Index
http://www.missingkids.com/cybertip

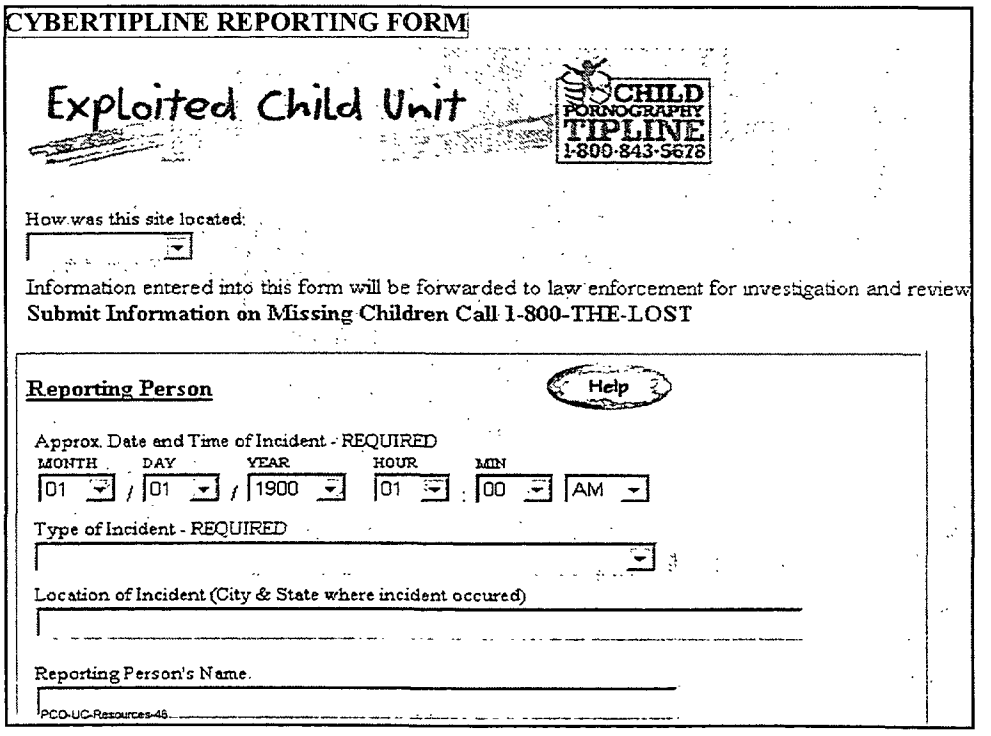

U.S. Customs Service - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.customs.ustreas.gov/enforce/cpep.htm
information about or suspect this type of illegal activity, contact the U.S. Customs Service with complete information as soon as possible. Call 1-800-BE-ALERT.
For complaints regarding websites, individuals, servers, or chat rooms trafficking in suspected Child Pornography please forward all correspondence to the International Child Pornography Investigation and Coordination Center at icpicc@customs.sprint.com
The U.S. Customs Service is also working closely with the National Center for Missing and Exploited Children to combat the proliferation of this disturbing material. You can also report suspicious activity relating to child pornography to their "Tipline" at 1-800-843-5678.
CASH AWARDS
The U.S. Customs Service will pay cash awards pursuant to Title 19 of the U.S. Code, Section 1619 for information concerning a violation of Customs Laws if the information leads to the recovery of fines, penalties, or forfeitures. Customs will also purchase evidence and information that will lead to the arrest and criminal prosecution of violators. The size of the award will depend on the quantity and the timeliness of the information.
For more information call:
The nearest U.S. Customs Service Special Agent in Charge or 1-800-BEALERT.
U.S. Customs Service
Home Feedback Search
PCO-UC-Resources-4 Document: Done

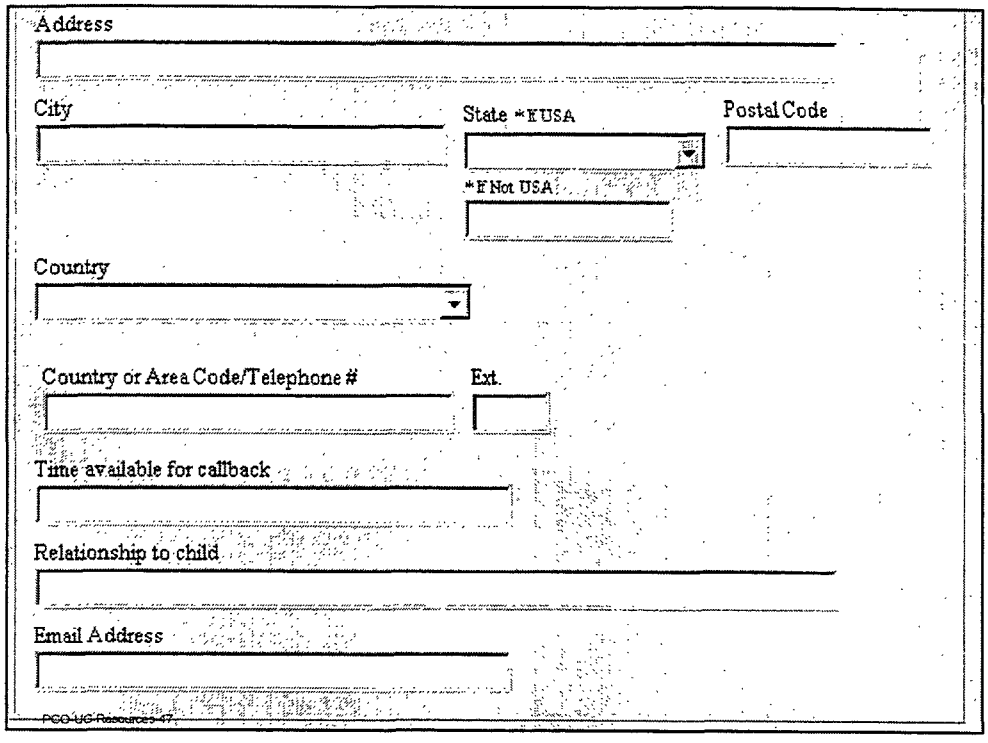

Safe Kids Home Page [1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.safekids.com/
Welcome to SafeKids.Com where you'll find tips, advice and suggestions to make your family's online experience fun and productive.
SAFEKIDS.COM
CyberTipLine
If someone sends you messages or images that are obscene, lewd, filthy, or indecent with the intent to harass, abuse, annoy, or threaten you, report it to your Internet service provider and the CyberTipline online or by calling 1-800-843-5678
PCO-UC-Resources-42 Document: Done

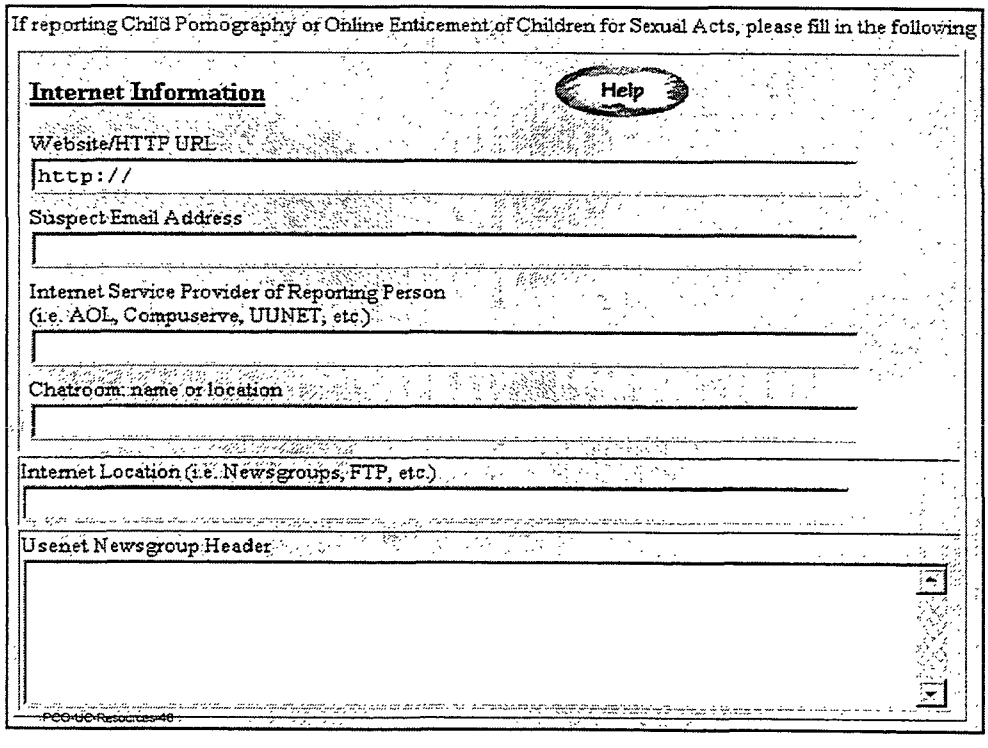

Inhope Forum - Hotline Profiles - Netscape
inhope-forum
Internet Hotline Providers in Europe Forum
HOTLINE PROFILES
GERMANY
GERMANY
NORWAY
THE NETHERLANDS
UNITED KINGDOM
OUTSIDE EUROPE
USA
BACKGROUND THE DAPHNE PROGRAMME PURPOSE OF PROJECT
WORK PROGRAMME CHILDNET INTERNATIONAL
WORK PROGRAMME CHILDNET INTERNATIONAL

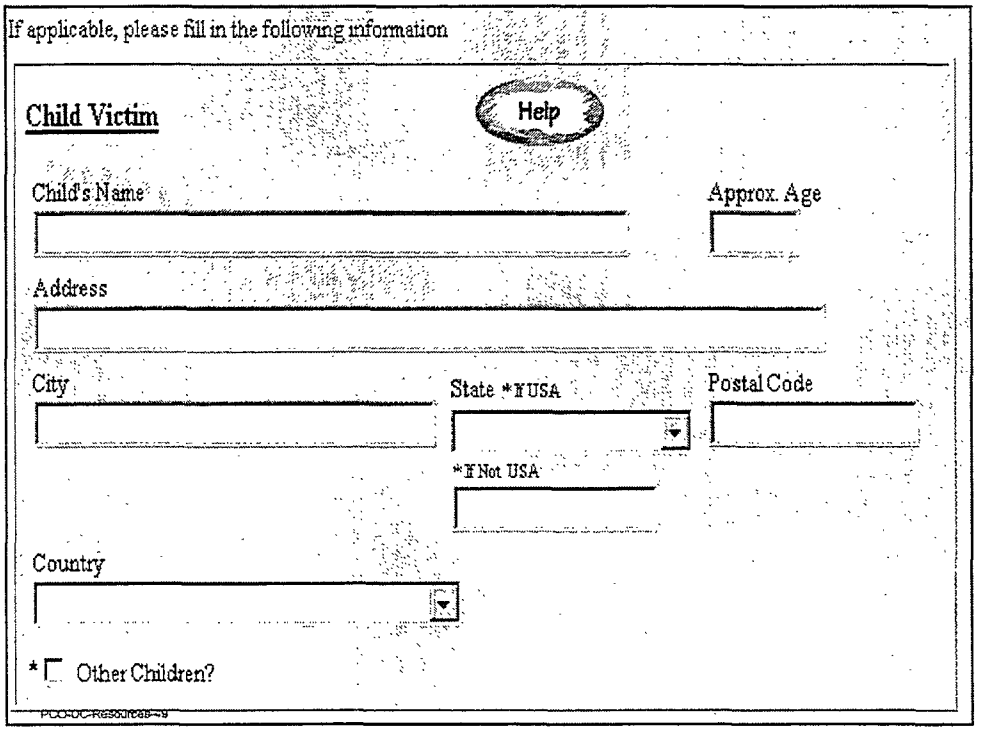

"The National Center for Missing and Exploited Children's Home Page - an online resource for inform...
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: http://www.missingkids.com/
What's Related
National Center for Missing And Exploited Children
1-800-THE-LOST
Missing Alert
About Us
Search for Child Photos
Donate
Education & Resources
Success Stories
How Can I Help?
News & Events
Partners & Sponsors
Guest
Guestbook
CyberTipline
http://www.missingkids.com/cybertip/ncmec_default_cybertip.htm

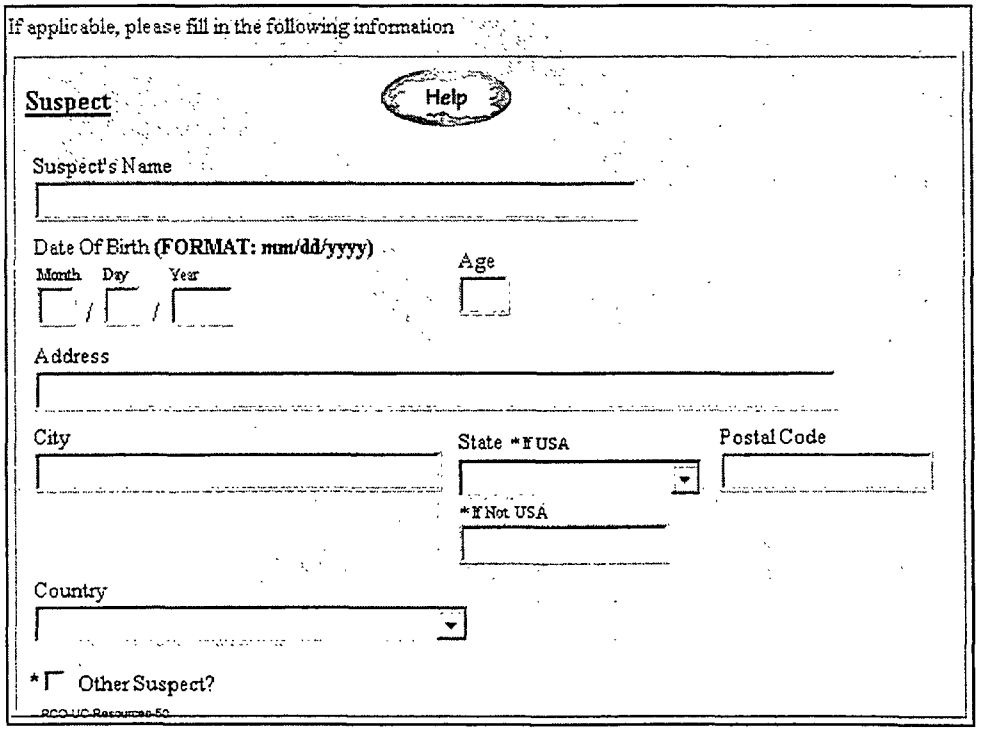

Netscape
CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678
If you know about a child who is in immediate risk or danger, call your local police.
If you have any information on a missing child, call 1-800-THE-LOST.
The CyberTipline handles leads from individuals reporting the sexual exploitation of children.
possession, manufacture, and distribution of child pornography
online enticement of children for sexual acts
child prostitution
child-sex tourism
child sexual molestation (not in the family)
CLICK HERE
REPORT ONLINE
NCMEC, in partnership with the Federal Bureau of Investigation, U.S. Customs Service, and the U.S. Postal Inspection Service, serves as the national CyberTipline and as the national Child Pornography Tipline 1-800-843-5678. Please contact us if you have information that will help in our fight against child sexual exploitation.
The U.S. Congress has funded these initiatives for reporting child sexual exploitation.
Click on the button below to take an online tour of the CyberTipline.
Site Designed and Hosted by Computer Associates


CYBERTIPLINE REPORTING FORM
Exploited Child Unit
CHILD PORNOGRAPHY TIPLINE
1-800-843-5678
How was this site located:
Information entered into this form will be forwarded to law enforcement for investigation and review
Submit Information on Missing Children Call 1-800-THE-LOST
Reporting Person
Help
Approx. Date and Time of Incident - REQUIRED
MONTH DAY YEAR HOUR MIN
01 / 01 / 1900 01 : 00 AM
Type of Incident - REQUIRED
Location of Incident (City & State where incident occured)
Reporting Person's Name
PCO-UC-Resources-45


Address
City
State *If USA
Postal Code
*If Not USA
Country
Country or Area Code/Telephone #
Ext.
Time available for callback
Relationship to child
Email Address
PCO UC Resources 47


If reporting Child Pornography or Online Enticement of Children for Sexual Acts, please fill in the following
Internet Information
Help
Website/HTTP URL
http://
Suspect Email Address
Internet Service Provider of Reporting Person
(i.e. AOL, Compuserve, UUNET, etc.)
Chatroom name or location
Internet Location (i.e. Newsgroups, FTP, etc.)
Usenet Newsgroup Header
PCO UC Resources 48


If applicable, please fill in the following information
Child Victim
Help
Child's Name
Approx. Age
Address
City
State *If USA
Postal Code
*If Not USA
Country
* Other Children?


If applicable, please fill in the following information
Suspect
Help
Suspect's Name
Date Of Birth (FORMAT: mm/dd/yyyy)
Month
Day
Year
Age
Address
City
State *If USA
Postal Code
*If Not USA
Country
* Other Suspect?

Additional Information

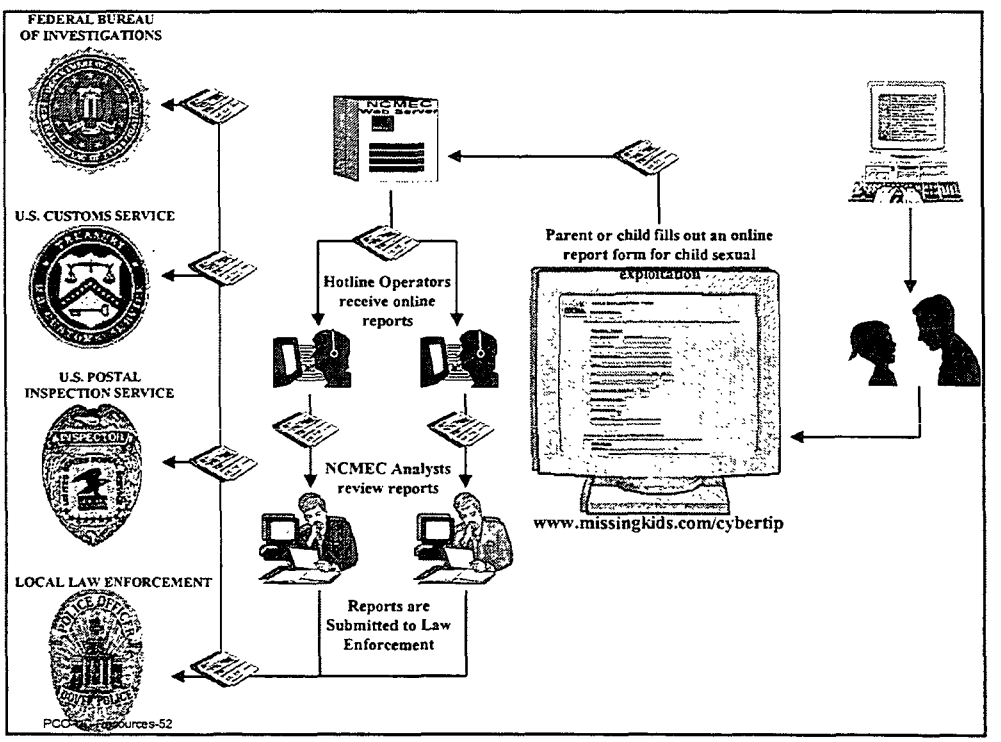
Help

Please provide additional information or description (be specific)

*other victims or suspects should be listed in this section

Report Exploitation

PCO-UC-Resources-51



PCO-UC-Resources-52

National Center for Missing and Exploited Children

Recent

Success Stories

www.missingkids.com/cybertip

CYBERTIPLINE

October 20, 1998

CyberTipline #2033

Law Enforcement makes an arrest from the information gathered through the CyberTipline

On the 12th of August, a person alleging he had seen child pornography on the Internet made a report online to the CyberTipline. An ECU staff person confirmed the site contained over five hundred photographs of child pornography and conducted a query on "allwhois" to determine where the site was registered. The report was referred by US Postal Service to a local law enforcement agency. On the 2nd of September they called to inform ECU the person administering the site was arrested. The FBI was also called in to assist in recovering the forensic computer evidence that may lead to additional arrests in the future.

CyberTipline #2240

Four Hours after CyberTipline report child is returned home after traveling to meet an adult met on-line

A report was made to NCMEC on the 25th of August about a 16 year-old child who had runaway from her home to meet someone she corresponded with on-line. The child had access to the Internet for eleven days and in that time she met the suspect, who paid for a Greyhound bus ticket and wired it to her home. The child was due to arrive in Missouri on the same day the report was made, so the child's mother and Innocent Images were contacted immediately. Several FBI agents and the thirty year-old male suspect were at the Greyhound station when the child arrived later that evening.

Law Enforcement Resources

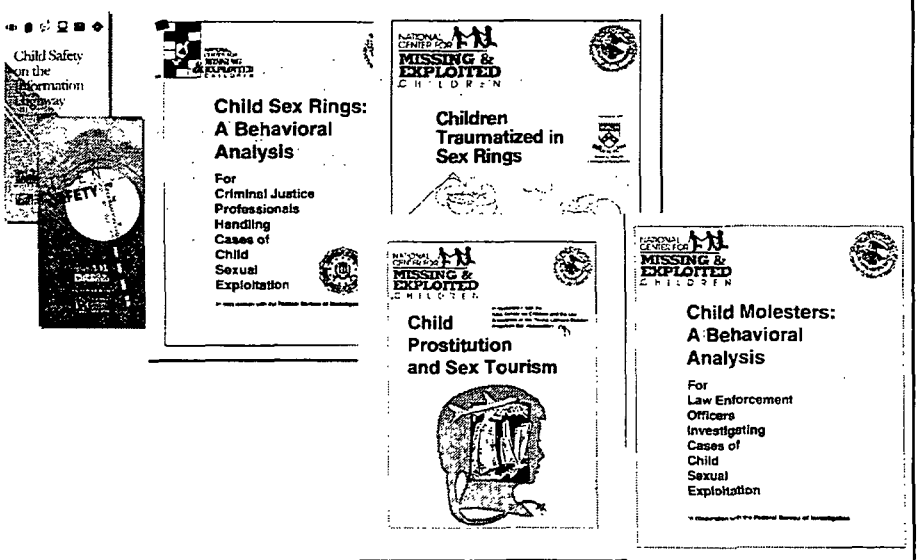
CYBERTIPLINE

The Public's Resource for Protecting Children Online

www.cybertipline.com

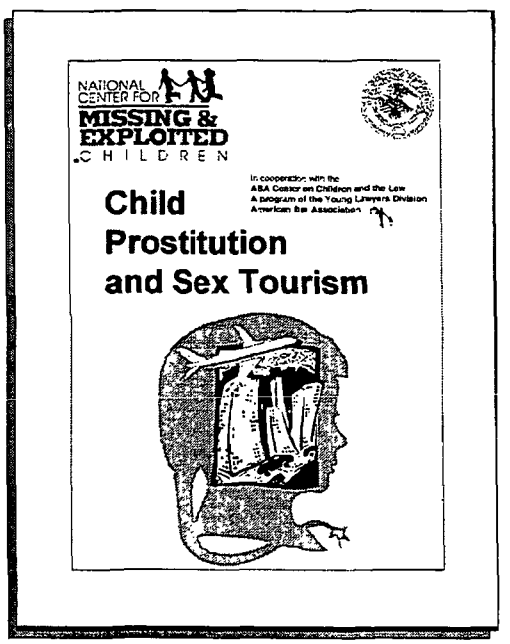
Exploited Child Unit
The National Center for Missing and Exploited Children

Publications



PCO-UC-Resources-55

ABA Children and the Law report on child prostitution and sex tourism provides information on the current state of the problem and reviews domestic laws and international responses.

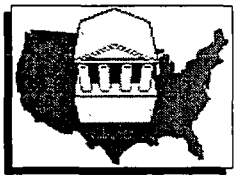


PCO-UC-Resources-56

State and Federal Task Forces

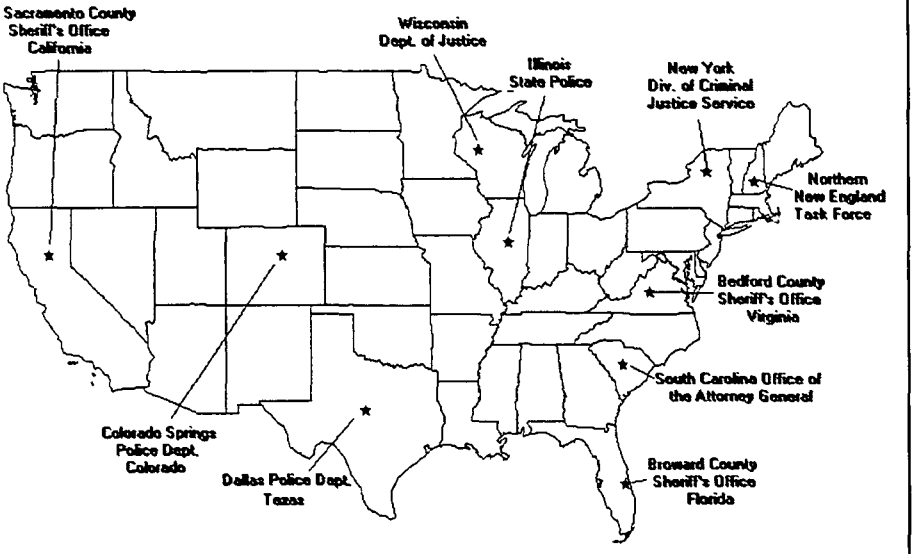
ECU maintains a database of federal, State, and local agencies and task forces that deal with Internet crimes against children.

14 individual task forces



State and Local Task Forces

OJJDP Internet Crimes Against Children's Program



Law Enforcement Contacts Database

Identifying individual contacts worldwide that deal with the crimes against children issues.

4586 records

Public/Private Records Databases

Availability to search public records databases (CDB Infotek, Autotrak, Lexis-Nexis, FinCEN) on leads pertaining to crimes against children.

Investigative Databases

Credit Bureau Info

County assessor records

Address changes

Licensing files

SSN tracking

Public Information Records

Business records

Publishing mailing lists

Marriage/divorce files

MVB records

Telephone listings

Court filings

Birth/death records

PCO-UC-Resources-61

Additional Resources

PCO-UC-Resources-62

Secret Service Resources

Forensic Services Division

Forensic Services Division (FSD) plans, directs, and coordinates forensic science activities within the Secret Service and make available their resources to assist State and Local law enforcement investigate crimes against children.

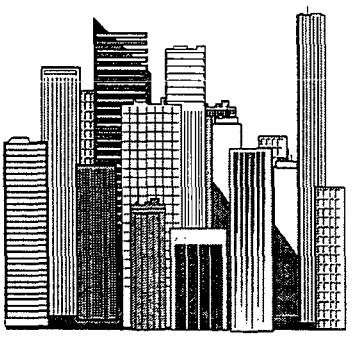
- **Fingerprint and Handwriting Analysis**
- **Polygraph Examinations**
- **Audio and Video Enhancement**

PCO-UC-Resources-63

Private/Public Sector Resources

A database of private companies and organizations that deal with education and additional resources to law enforcement.

•SEARCH
•HTCIA
•National White Collar Crimes Center
•FACCI
•FLETC (US Customs)



PCO-UC-Resources-64

Training Programs

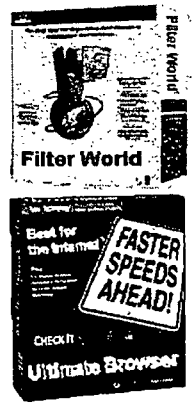
NCMEC offers training programs for law enforcement on the issues of child sexual exploitation, missing children, and investigating crimes against children on the Internet.

- **PCO Investigator Course**
- **Unit Comdr. Course**
- **T/F Certification and Policy Course**

PCO-UC-Resources-65

Applications and Software Evaluation

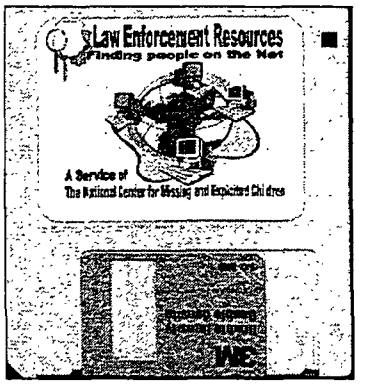
Identifying software and other applications (spiders, webcrawlers, intelligent agents) that may be of assistance to law enforcement officers investigating crimes against children via the Internet.



PCO-UC-Resources-66

Applications and Software Development

Developing programs that aid law enforcement officers obtain information available on the Internet.

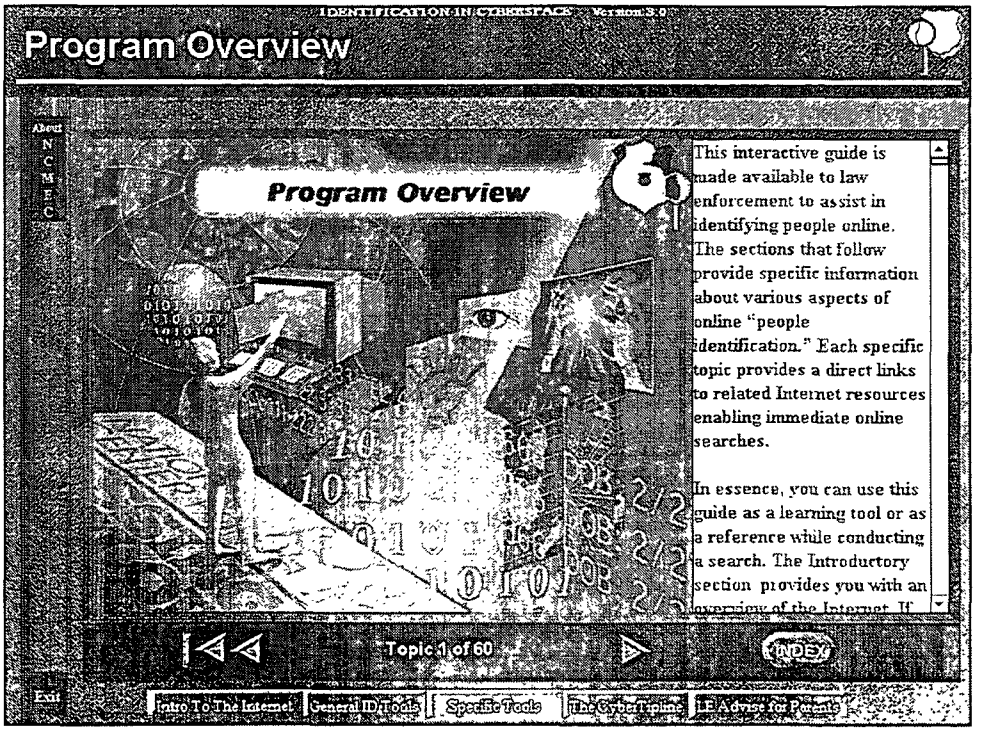


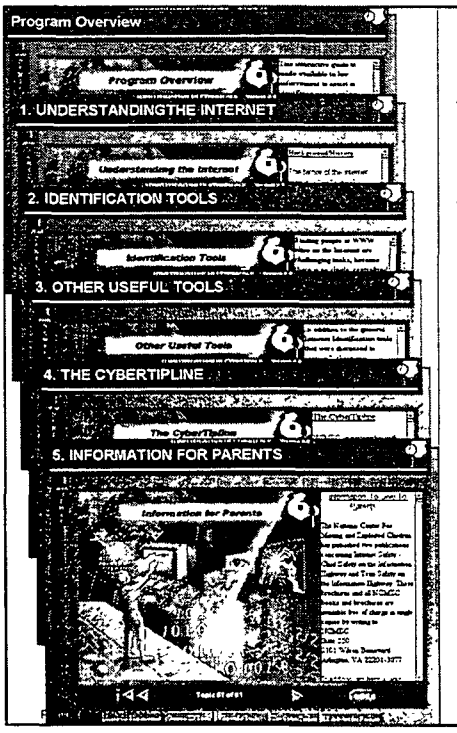
PCO-UC-Resources-67

IDENTIFICATION IN CYBERSPACE

A Law Enforcement Resource For Finding People On The Internet

PCO-UC-Resources-68





Section 1: The Internet and Its Components

Statistics, E-Mail, FTP, Newsgroups, IRC, The Web

- **Section 2: General Identification Tools**

  Finger, Whois, Searching Newsgroups and the Web, Web Directories, Meta-Search Engines

- **Section 3: Other Useful Tools (Specific Tools)**

  State Sex Offender Lookup, Public Records Searches, Surfing the Web Undercover, Web Page Translator, Accessing Hidden Sites, Social Security # Lookup, Mapping and Location Tools, International Yellow and White Pages, Web Meta-Searchers,Identifying Mailing List Participants, E-Mail Aliases, Ping utility, Express Search Engine, CyberLaw Resources, Zip Codes & Postal Identifier, County Court House Directory, Internet Dictionary, Law Enforcement Resources

- **Section 4: The CyberTipline**

  Overview of the CyberTipline, CyberTipline Tour, Contacting CyberTipline Analysts

- **Section 5: Information for Parents**

  Child Safety Tips and Brochures, Child Privacy Tips, Information on Filters and Monitors

Age Progression

2 1/2 years

Stefan Potteiger
Family Abduction
Age at Disappearance: 2 1/2 Years
Aged 2 1/2 to 9 years 7 months

RECOVERED

Age Progressed - 9 years 7 months

Child photo after successful recovery

PCO-UC-Resources-71

Facial Reconstruction

Facial Reconstruction

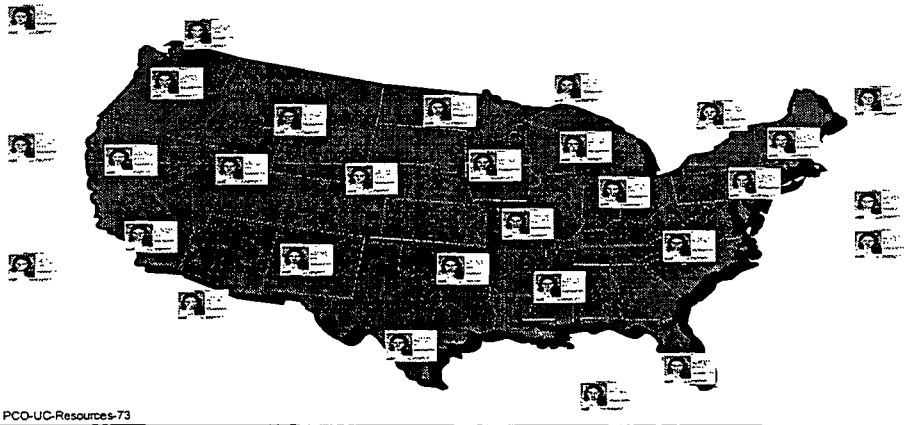
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Jennifer Osborne
age 12

PCO-UC-Resources-72

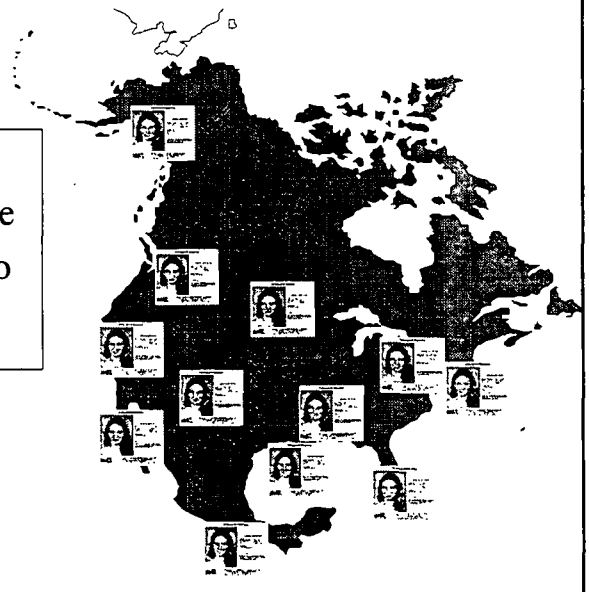
Distribution of Images

Extensive network enables the transfer and posting of child posters worldwide in a matter of minutes utilizing the Internet or being sent via broadcast fax.

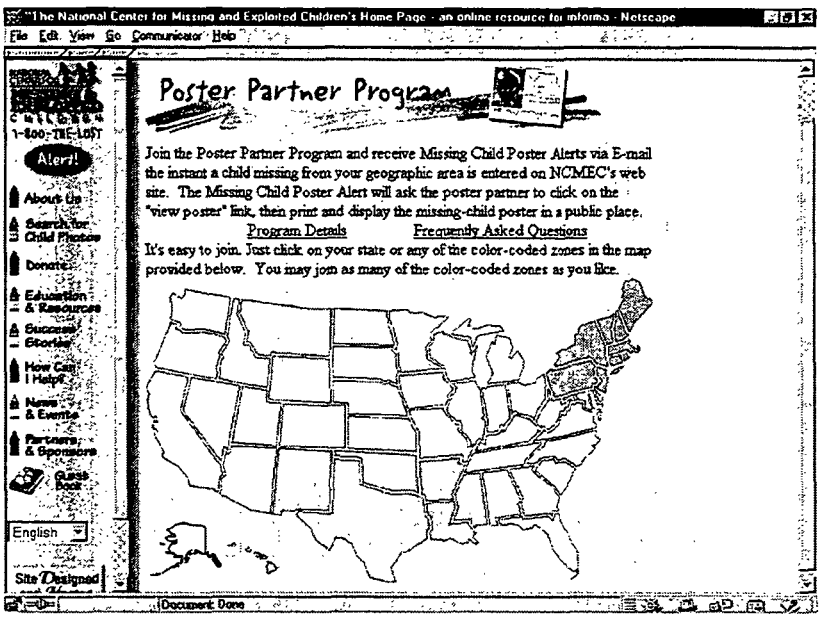


NCMEC Posters & Fliers

Distributed throughout Canada, Mexico and the USA by over 450 Photo Partners



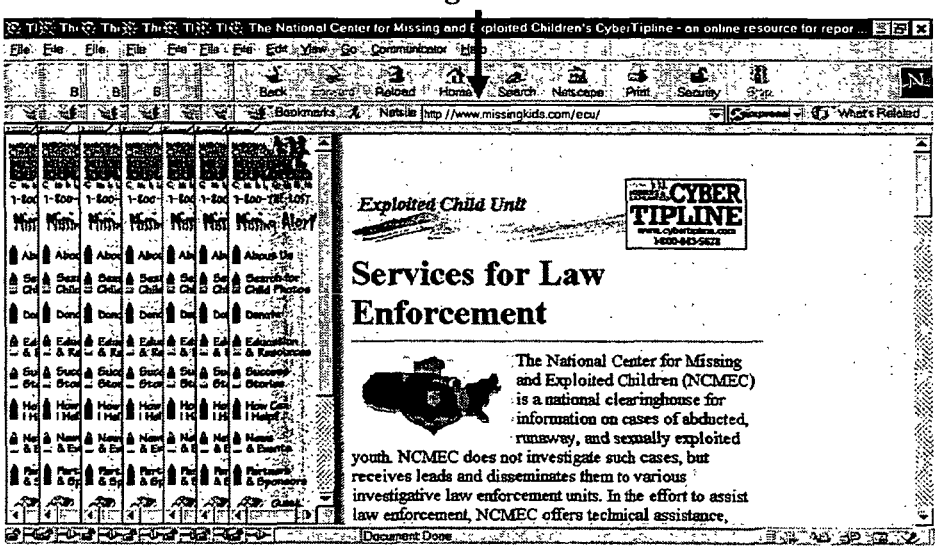
NCMEC Poster Partner Program



PCO-UC-Resources-75

ECU Web Site

www.missingkids.com/ecu



PCO-UC-Resources-76

Contact Information

Ruben D. Rodriguez
Director

Kathy Free
Program Manager

Exploited Child Unit
1 800 843-5678
703 274 2121 fax

rrodriguez@ncmec.org
kfree@ncmec.org

NEW ADDRESS:

Exploited Child Unit
National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314

800/843-5678

Becoming Cyber-Savvy:

An Internet Guide for Parents

Producer: Education Development Center, Inc.

Funder: U.S. Department of Justice
Office of Juvenile Justice and
Delinquency Prevention

Becoming Cyber-Savvy: An Internet Guide for Parents

Authors: **Education Development Center, Inc.**
Newton, MA

This project was supported by Cooperative Agreement No. 98-MC-CX-K014, awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, through the Portsmouth, New Hampshire, Police Department. Points of view in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

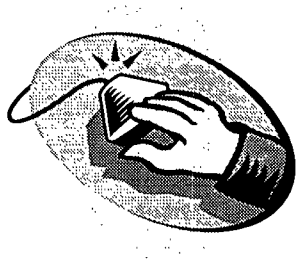
Table of Contents

Introduction 1

Summary of Key Points 2

Glossary of Terms 7

Resources 11



Introduction

Do you know . . .

. . . what the Internet is? . . . what the World Wide Web is?

. . . what a chat room is? . . . what instant messages are?

Do you know what your children do when they're online?

The Internet is at once exciting, vital, and mysterious. At the click of a mouse, computer users of all ages can access an almost limitless array of information or talk to people in every corner of the world. Yet, as with most opportunities in life, there is risk. On their journeys along the "information superhighway," Internet users may be exposed to undesirable content or situations.

Children may be especially vulnerable to these risks. More than 10 million children are already online, and industry experts say there will be 45 million children online by the year 2002. In its first year of operation, the "CyberTipline," managed by the National Center for Missing and Exploited Children, logged more than 9,000 reports of suspicious online activities, including images of child pornography and attempts to engage children in sexual relationships.

In many homes, children are far more cyber-savvy than their parents. Parents are unsure how to supervise and protect their children online. Does this sound familiar to you?

The key to promoting your children's safety online is educating yourself. There are things you can do to help your children enjoy all the benefits of the Internet without falling prey to the risks. This handbook, and the accompanying videotape, draws from the experience of parents, children, and law enforcement experts to help you guide your children safely as they travel through cyberspace.

For more information, contact your local police department or
The National Center for Missing and Exploited Children
1-800-843-5678
www.missingkids.com/cybertip

Summary of Key Points

Disclosing Information

✓ **Children feel safe when they are online.**

They know not to identify themselves by giving their name, address, or age.

At the same time, they may inadvertently give clues that can lead to their identities. They may mention the name of their school or a friend, a local sports team or shopping mall, or community events. Over time, someone could gather these clues, do a little research, and find out who these children are.

Also, some Internet service providers (ISPs) keep "member profiles" that are available to everyone who registers with their service. These profiles may contain a great deal of identifying information. But cyber-savvy kids know the profiles are not mandatory, and many kids intentionally enter false information.

Check with your ISP to see if member information is made available to other users. If so, remove your child's identifying information or choose another ISP.

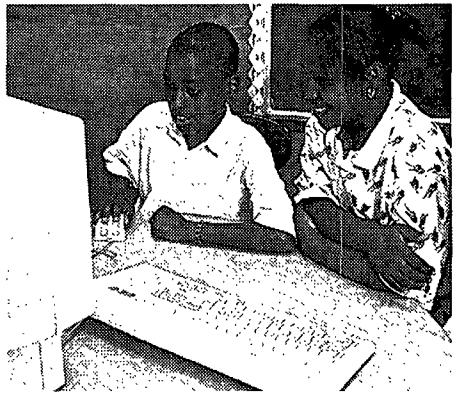
✓ **People online may not be who they say they are.**

The 15-year-old baseball fan may in fact be a 51-year-old computer programmer or ballet instructor. Conversely, the 21-year-old fashion model may really be a 12-year-old child. Whether an adult poses as a child, or a child poses as an adult, there is potential for trouble.

Remind your children that no matter how much their online "buddies" seem like best friends they are still strangers. Also, caution your children against pretending to be someone they're not.

Going Places

✓ **Children go to chat rooms when they're bored, have no one to talk to, have few friends who are online, and because they can be fun.**



Chat rooms are very popular among teens—about 80% of teens who answered a *Newsweek* telephone poll said they use the Internet for things like e-mail and chat rooms. Although chat rooms usually have names that indicate special interests (such as movies or popular music groups), the actual content can include anything. Sexual predators often visit chat rooms to strike up relationships with unsuspecting children.

Encourage your children to use the Internet to visit interesting websites and to correspond with people they know. But expect that, sooner or later, children will experiment. Reinforce the guiding rule of Internet use: "Don't talk to strangers."

✓ **Almost any search of the Internet can lead to pornography or other undesirable content.**

Even the most innocent, legitimate topics can somehow be related, or linked, to something offensive.

Ask your children to show you how they use the Internet. See for yourself the results of searches for typical homework assignments. Ask your children's teachers how they help their students use the Internet safely.

Monitoring Use

✓ **Do not assume that your older teen requires no supervision on the Internet.**

72% of the Internet-related missing children cases known to the National Center on Missing and Exploited Children involved children 15 or over.

Be alert to changes in your children's behavior. Do they spend long hours on the computer? Do they spend less time with their friends? Do they receive mail or telephone calls from people you don't know?

✓ **Blocking and filtering programs may help you control your children's access to certain kinds of information.**

Blocking and filtering tools may limit your children's access to many useful websites as well as undesirable ones. Remember, too, that your children probably use other computers—at school, in the library, at friends' homes—that may not be equipped with blocking or filtering tools.

Even if you choose to install one of these programs, explain to your children the concerns you have and your expectations that they will use the Internet wisely—no matter where they are.

✓ **Rules help children feel safe.**

Keep the computer in a common area of the home. Set limits on when your children may use the computer and for how long. Once you have set the rules, enforce them!

Staying Connected

✓ **Children need privacy, too.**

You probably don't listen to your children's telephone conversations or read their personal mail. Why should you need to see their e-mail correspondence? Unless you've seen dramatic negative changes in their behavior, it's not fair to assume your children are doing "something bad" if they won't let you see the computer screen.

By setting reasonable rules for computer and Internet use and talking with your children about your concerns and expectations, you should be able to trust that they are using the computer safely.

✓ **Be available to help your children if the need arises.**

Children should know that their parents will help them find solutions to problems. Remember that your children are growing in many ways and may take a wrong turn now and then.

Let your children know that you will listen when they are concerned, and work with them to solve the problem. Solutions may be as simple as changing a user name or moving an account to another Internet service provider.

If you believe your child is in danger, call your local police.

Keeping Your Perspective

✓ **There have always been opportunities for children to take risks.**

The Internet is different because it brings these opportunities into your home. Children no longer need to "borrow" an adult's magazine collection to see pornography. Sex offenders no longer need to approach children in playgrounds or shopping malls. But the same rules apply, with certain modifications.

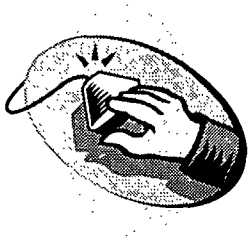
Don't talk to strangers—*but remember that the person in the chat room who seems to share your interests and understand your problems is still a stranger.*

If you've gone somewhere that feels wrong or unsafe—LEAVE. Whether it's an adult movie theater or a pornographic website, ***you don't have to go there.***

✓ **Keeping children safe on the Internet is a community concern.**

Children use computers in many locations—in their own homes and in schools, libraries, community centers, and their friends' homes. Internet safety must be a shared concern.

Parents, educators, and community leaders have a responsibility to understand how children use the Internet and to find ways to ensure their safety online.



Glossary of Terms

Address. The unique location, or name of a computer host, of a site on the Internet (for example, a webpage; see "URL"), a specific file location, or an electronic mail user.

Blocking Software. Special programs that attempt to prevent access to certain sites on the Internet.

Bookmark. A record of an address stored in your browser that allows you to access sites directly by clicking on an icon.

Browser. A software program, such as Netscape Navigator or Microsoft's Internet Explorer, that enables you to find, see, and hear material on the World Wide Web.

Bulletin Board System (BBS). A central computer, or set of computers, accessed via modem that enables you to carry on discussions with people who may or may not be connected to the computer at the same time. Most BBSs offer files, programs, and other information that you can download to your own computer.

Chat Room. Also called discussion groups. They allow you to communicate with others in "real time." A user enters a chat room, types a message, and sends it, and it is displayed to other users in the room, or can be limited to just one other user.

Commercial Online Service (COS). General term for online services, such as America Online, Earthlink, Microsoft Network, and Prodigy. These services have lots of information attractively organized and may also offer access to the Internet.

Cookies. A piece of information unique to you that your browser saves and sends back to a Web server when you visit a website. Cookies contain information such as log-in or registration information, online "shopping cart" information (your online buying patterns in a certain retail site), user preferences, what site you came from last, etc.

Cyberspace. A term generally used to describe the range of information services available on the Internet.

Download. To copy a file from one computer system to another over a modem.

E-Mail (Electronic Mail). A way of sending messages, usually text, from one computer to another.

Flaming. Directing insulting or derogatory comments at someone through e-mail, newsgroups, or chat rooms.

Freenet. A community network that provides free online access, usually to local residents, and often includes its own forums and news.

Hardware. The nuts, bolts, and wires of computer equipment and the actual computer and related machines.

Home Page. The site that is the starting point for your browser on the World Wide Web or a particular main page for a group or organization's website.

HTML (Hypertext Markup Language). The coding language used to create all webpages. Text documents must be converted to HTML in order to be readable on the Web.

Hyperlink. An easy method of accessing information by choosing highlighted words in text on the screen. The link will take you to related documents or sites.

Hypertext Transfer Protocol (HTTP). A standard that provides instructions for moving text, images, sound, video, and other multimedia files across the Internet from one webpage to another.

Instant Message. A chat-like technology on an online service that notifies a user when a friend is online, allowing for simultaneous communication (like talking on the phone, only with text).

Internet. A worldwide collection of computer networks, connected by cables and satellites, that allows people to find and use information and communicate with others.

ISP (Internet Service Provider). A generic term for any company that can connect you directly to the Internet (as compared to COS).

Modem. A device that allows computers to communicate with each other over telephone lines or other delivery systems.

Newbie. Somebody new to the Net.

Net, The. A colloquial term often used to refer to the entirety of cyberspace, the Internet, commercial services, Usenet, etc.

Netiquette. The rules of cyberspace civility such as not typing a message in capital letters, which is equivalent to shouting.

Newsgroups. The name for discussion groups on Usenet.

Online Service. A company such as America Online (AOL) or Prodigy that provides its members access to the Internet through its own special user interface as well as additional services such as chat rooms, children's areas, travel planning, and financial management.

Posting. The process of sending a message to a newsgroup, BBS, or other public message area. The message itself is called a post.

Profile. Information provided to an ISP that may be accessed by other users of the same ISP. Typical profile information includes name, age, date of birth, address, interests, hobbies, clubs, secondary e-mail accounts, and phone numbers. Some profiles can even include photographs.

Search Engine. A program that performs keyword searches for information on the Internet.

Spamming. Inappropriate use of a mailing list by sending the same unsolicited message to a large number of people.

URL (Uniform Resource Locator). The World Wide Web address of a site on the Internet. For example, the address for the White House is http://www.whitehouse.gov.

Usenet Newsgroups. A system of thousands of special interest groups to which readers can "post" and read messages. These messages are then distributed to other computers on the network. Usenet registers newsgroups, which are available through ISPs.

UserId (User ID). The unique name given to a user on a system for her/his account.

Virus. A piece of programming code that causes some unexpected and usually undesirable event, such as lost or damaged files. Viruses can be transmitted by downloading from another diskette or be present on the diskette programs.

Website. A location on the World Wide Web that incorporates graphics, sounds, and links to other sites. Websites are identified by an online address.

WWW (World Wide Web). A hypertext-based navigation system that allows you to browse through a variety of linked Internet resources organized by colorful, graphics-oriented home pages. Also known as the Web.

Sources:

Aftab, Parry. *A Parents' Guide to the Internet.* SC Press, Inc., 1997.

Lazarus, Wendy & Laurie Lipper. *The Parents' Guide to the Information Superhighway.* The Children's Partnership, September 1996.

Parents Guide to the Internet. U.S. Department of Education, November 1997.

Resources*

Online Information

JuniorNet is a commercial-free online service for children ages 3–12. It does not allow access to the larger Internet.
www.juniornet.com

GetNetWise is a coalition that wants Internet users to be just "one click away" from the resources they need to make informed decisions about their family's use of the Internet. Some information available to families includes: Online Safety Guide, Tools for Families, Reporting Trouble, and Web Sites for Kids.
www.getnetwise.org

The National Center for Missing and Exploited Children
699 Prince Street
Alexandria, VA 22314-3175
703-274-3900
703-274-2220 (fax)
hotline: 1-800-THE-LOST (800-843-5678)
www.missingkids.org

Books/Manuals

Aftab, P. (1997). *A Parents' Guide to the Internet.*

Dixon, P. (1996). *The Dummies Guide to Family Computing: Take Charge Computing for Teens and Parents.* Framingham, MA: IDG Books Worldwide.

**The resources listed here are not endorsements.*

Leadership and Technology: What School Board Members Need to Know. (1995). Annapolis Junction, MD: National School Boards Association.

Making the Net Work for You: How to Get the Most Out of Going Online. (1996). Silver Spring, MD: Interactive Services Association and National Consumers League.

Marsh, M. (1995). *Everything You Need to Know (But Were Afraid to Ask Kids) About the Information Highway.* Palo Alto, CA: Computer Learning Foundation.

Mohta, V. (1996). *The Dummies Guide to Family Computing: The World Wide Web for Kids and Parents.* Framingham, MA: IDG Books Worldwide.

Polly, J.A. (1997). *The Internet Kids & Family Yellow Pages.* Berkeley, CA: Osbourne McGraw-Hill.

Wolff, M. *Kids Rule the Net: The Only Guide to the Internet Written by Kids.* Wolf New Media.

Brochures/Booklets

American Library Association. *The Librarian's Guide to Cyberspace for Parents & Kids.* Chicago, IL: ALA Public Information Office. (800-545-2433 x2148). Free online at www.ala.org/parentspage/greatsites.

Childnet International. (1997). *Global Information Networks—The Agenda for Children.* London. Free online at www.childnet-int.org.

Library of Congress. *Internet Guides, Tutorials, and Training Information.* Online address is lcweb.loc.gov/global/internet/training.html.

National Coalition for the Protection of Children & Families (NCPCF). (1997). *Protecting Your Family in Cyberspace.* Cincinnati, OH. Online address is www.nationalcoalition.org.

U.S. Department of Education. (1997). *Parents Guide to the Internet.* Washington, DC: U.S. Department of Education, Office of Educational Research and Improvement, Media and Information Services. Available online at www.ed.gov.

Blocking/Filtering/Monitoring Software

Access Management Engine (www.bascom.com)

America Online Parental Controls (www.aol.com)

BESS (www.n2h2.com)

Bonus.com the SuperSite for Kids (www.bonus.com)

Cyber Patrol (www.cyberpatrol.com)

Cyber Snoop (www.pearlsw.com)

CYBERsitter (www.solidoak.com)

EdView Channel Lock (www.edview.com)

GuardiaNet (www.guardianet.net)

I-Gear (www.urlabs.com)

McAfee-virus protection (www.mcafee.com)

Microsoft Plus! For Kids (www.microsoft.com/kids)

Neosoft (www.neosoft.com/parental-control)

Net Nanny (www.netnanny.com)

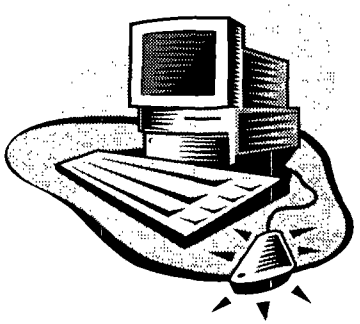
Planet View (www.planetview.com)

SafeSurf Internet Filtering Solution (www.safesurf.com)

SmartFilter (www.smartfilter.com)

Surf Watch (www.surfwatch.com)

X-Stop (www.xstop.com)



Investigation of Internet Crimes against Children

Model Policy

Policy Purpose: The purpose of this policy is to establish responsibilities and guidelines regarding this agency's response to reports of the exploitation of children, and the possession and distribution of child pornography using computers.

II. Policy Statement: It shall be the policy of this agency to adhere to strict guidelines with respect to investigations of computer related child exploitation. The standards adopted pursuant to this policy mirror those prescribed by Office of Juvenile Justice and Delinquency Prevention's (OJJDP) Internet Crimes Against Children (ICAC) Task Forces, and ensure compliance with those protocols accepted by the Federal Bureau of Investigations (FBI), U.S. Customs, and the U.S. Postal Inspectors' Office.

III. Definitions:

A proactive investigation is designed to identify, investigate and prosecute offenders, which may or may not involve a specific target, and requires online interaction and a significant degree of pre-operative planning.

A reactive investigation involves the investigation and prosecution of a known target(s), and where the need to proceed with the investigation is urgent. It also includes a response within the community or area of jurisdiction to a specific complaint brought to you attention by another law enforcement agency, a reputable source of information such as the Cyber-Tipline at the National Center for Missing & Exploited Children or a large Internet Service Provider such as America On-Line. Finally we must also respond to complaints made by citizens, schools, libraries or business who believe illegal material has been transmitted or potentially dangerous situations, such as child lure attempts have been communicated through the internet.

The term Internet Crimes against Children (ICAC) includes both proactive and reactive investigative activities as outlined above

An investigation is deemed to be urgent when there is a reasonable belief that the target presents an imminent threat to the well being of potential victims.

IV. Procedures:

Case Management

A. Workspace and Equipment

1. Internet Crimes Against Children (ICAC) computers and software shall be reserved for the exclusive use by agency designated ICAC personnel. When possible, undercover computers, software, and online accounts shall be purchased covertly. No personally owned equipment shall be used in ICAC investigations and all software shall be properly acquired and licensed.

2. Absent exigent or unforeseen circumstances, all ICAC online investigations shall be conducted in government workspace as designated by the agency.

B. Case Predication and Prioritization

1. Cases may be initiated by referrals from the CyberTipline, Internet service providers, or other law enforcement agencies, and by information gathered through subject interviews, documented public sources, direct observations of suspicious behavior, public complaints, or by any other source acceptable under agency policies.

2. ICAC supervisors are responsible for determining investigative priorities and selecting cases for investigation. Assuming the information is deemed credible, that determination should begin with an assessment of victim risk and then consider other factors such as jurisdiction and known offender behavioral characteristics. The following prioritization scale was established by the ICAC Task Forces and will apply to the assignment of cases within the agency:

   a) A child is at immediate risk of victimization;
   b) A child is vulnerable to victimization by a known offender;
   c) Known suspect is aggressively soliciting a child(ren);
   d) Traders of images that appear to be home photography with domiciled children;
   e) Aggressive, high-volume child pornography traders who either are commercial distributors, repeat offenders, or specialized in sadistic images;
   f) Traders and solicitors involved in high-volume trafficking or belong to an organized child pornography ring that operates as a criminal conspiracy;
   g) Traders in previously known images;
   h) Traders in digitally altered images.

C. Recordkeeping

ICAC investigative units shall be subject to the existing agency incident reporting procedures and case supervision systems. Investigators will obtain a case number

at the outset of each case and fully document their activities through the completion of initial and supplemental reports. Reports will be completed and reviewed by a supervisor in a timely fashion. As with any other type of investigation case management activities will occur in accordance with existing departmental policies and procedures. Closeout reports will indicate the manner in which a case has been resolved with copies forwarded to the prosecutor's office and/or the law enforcement agency continuing the investigation where applicable.

D. UNDERCOVER INVESTIGATIONS *(THIS SECTION LIMITED TO THOSE AGENCIES WHO DECIDE TO ENGAGE IN THESE ACTIVIES)*

1. Carefully managed undercover operations conducted by well-trained officers are among the most effective techniques available to law enforcement for addressing ICAC offenses. Undercover operations, when executed and documented properly, collect virtually unassailable evidence regarding a suspect's predilection to sexually exploit children. However, these investigations can trigger serious legal and ethical considerations because of concern that inappropriate government conduct may induce an otherwise innocent citizen into committing a crime.

2. All undercover investigations shall be conducted in a manner consistent with the principles of due process. Investigators shall avoid unlawful inducement of any individual not otherwise disposed to commit the offenses being investigated, and will not engage in conduct that is shocking or offensive to notions of fundamental fairness as described in applicable caselaw. See, for example, *Jacobson v U.S.*, 503 U.S. 540 (1992); *U.S. v. Archer,* 486 F.2d (2nd Cir.1973).

3. Investigators should always be aware that their actions, in addition to those of the offender, may be at issue in deciding if charges are brought, whether referrals to other law enforcement agencies are acted upon, and in determining the guilt or innocence of the offender at trial. Therefore, it is critical that you work closely with local or federal prosecutors when investigating ICAC offenses.

4. Accordingly the following **minimum standards** apply to all undercover investigations:

   a) Only sworn, on-duty investigative personnel shall conduct ICAC investigations in an undercover capacity. Private citizens shall not be asked to seek out investigative targets nor shall they be authorized to act as police agents in an online undercover capacity.

   b) Employees shall not, under any circumstances, upload, transmit, or forward pornographic or sexually explicit images.

   c) Other than photographs of law enforcement officers who have provided their informed written consent, no human images shall be uploaded, transmitted, or forwarded by ICAC Task Force personnel.

d) Other than authorized above, images considered for uploading shall be approved by a supervisor and reviewed by the local prosecutor. Images uploaded for investigative purposes shall be nonhuman and encrypted. Sexually suggestive titles shall not be used.

e) During online dialogue, undercover officers should allow the investigative target to set the tone, pace, and subject matter of the online conversation. Image uploading shall be initiated by the target.

E. EVIDENCE PROCEDURES

1. All undercover online activity, shall be recorded and documented. Any deviations from this policy due to unusual circumstances, shall be documented in the relevant case file and reviewed by an ICAC Task Force supervisor.

2. The storage, security, and destruction of investigative information shall be consistent with existing evidentiary policy and procedures. Access to investigative files and any evidence collected should be restricted to authorized personnel with a legitimate need to know.

3. Supervisors must ensure that qualified personnel who have received specific training in this field conduct forensic examinations of computers and related evidence.

I. Information Sharing

a) Conventional boundaries are virtually meaningless in the electronic world of the Internet and the usual constraints of time and distance do not apply. These factors increase the possibility of investigators targeting one another, investigating the same subject, or inadvertently disrupting an ongoing investigation. To foster coordination, collaboration, and communication, investigators are required to contribute basic case information to a common database. Federal Guidelines have been established through the Department of Justice's ICAC Task Force Information Sharing Working Group. The (*Insert Agency Name)* has adopted the Federal Guidelines and therefore requires that investigators adhere to the information sharing procedures listed below.

   a) Investigators shall contribute basic and case update information on all cases (local, interstate, reactive and proactive) to the Child Pornography Pointer System (CPPS) maintained by the FBI Innocent Images Task Force.

   b) Basic case information shall include, but is not limited to:

      1) Submitting Task Force
      2) Person submitting information
      3) Telephone number for verification purposes

4) Date of submission
5) Brief synopsis of investigation
6) Offender screen name(s)
7) Identifiers (URL, FTP, newsgroup, IP Address)
8) True name of suspect (if known)
9) Other suspect information (if known)
10) Undercover officer screen names(s)

c) Case update information shall include, but is not limited to:

1) Submitting Task Force
2) Person submitting information
3) Telephone number for verification purposes
4) Date of submission
5) Date investigation initiated
6) Identity of subject(s) including address, date of birth, social security number, address (when available)

d) The ICAC Supervisor shall designate a primary and secondary staff contact for the CPPS. Contact will be made by telephone and/or the information can be forwarded to CPPS using the attached data form. CPPS staff will verify each caller's identity through a return telephone call to the Investigator. While 24-hour access is not currently available, it is anticipated that this capacity will be available via dial-up connection by mid 1999. Once dial-up access capability is achieved, Investigators will use a stand-alone computer to access CPPS.

e) Each Investigator will query CPPS prior to opening an active investigation to determine if there are related active investigations being conducted by other law enforcement agencies.

f) Assuming no other active investigations are discovered and that reasonable suspicion is present to initiate an investigation, the agency will submit case information to CPPS, including an indication that there is no known related investigation underway. Investigators should submit this information within 24 hours if initiating the case or as soon thereafter as possible.

g) If any duplication is found, the initiating Investigator is responsible for contacting the other law enforcement agency. CPPS personnel are not responsible for notifying the parties of duplication beyond alerting the initiating agency to the potential conflict.

h) The *(Insert agency Name)* will utilize the Law Enforcement Online (LEO) e-mail system to facilitate communication among ICAC Task Forces and with the FBI. LEO may also be used to exchange information about training opportunities, target referrals, and investigative strategies. Other topics may include technology developments, recent successes, educational material, and press releases.

i) Additionally, investigators initiating a case should contacting the U.S. Customs Cyber Smuggling Center (703 293-8005) to ensure there is no duplication with regard to their ongoing investigations. Similarly, once an offender has been identified and associated with a known address, contact should be made with the U.S. Postal Inspector responsible for child sexual exploitation offenses where the offender resides.

II. Supervision

1. Existing agency supervisory systems and procedures shall apply, with specific emphasis on observation, documentation, and periodic evaluation of cases assigned to undercover investigators. Given the nature of these investigations, consistent and on-going supervision of these cases and investigative personnel assigned to the unit is essential.

2. At a minimum, management or supervisory practices shall include:

   a) Review of daily ICAC Task Force investigative reports
   b) Periodic review of undercover session records
   c) Direct participation in formulating undercover investigative plans and establishing investigative priorities
   d) Development of work schedules including approval of specific overtime expenditures
   e) Assessment of equipment and training needs
   f) Review and approval of any fiscal matters

III. Selection of ICAC Investigative Personnel

1. While existing agency personnel procedures apply, supervisors should evaluate prospective ICAC investigative candidates for work history that indicates prior investigative experience, court testimony skill, ability to handle sensitive information prudently and a genuine interest in the protection of children.

2. Once assigned, supervisors should ensure that ICAC investigators are computer literate, knowledgeable regarding child exploitation issues, and are familiar with Federal and State statutory and caselaw pertaining to ICAC investigations.

IV. Prevention and Education Activities

1. Prevention and education activities are a critical component of the *(Insert Agency Name)* ICAC Program. Consequently supervisors and investigators are expected to develop and lead prevention programs to foster awareness and provide practical, relevant guidance to children, parents, educators, librarians, and other individuals concerned about child safety issues.

2. Presentations to school staff, parents, and community groups are excellent ways to promote awareness. However, these presentations shall not depict identifiable victims nor shall they use pornographic or sexually explicit images. Presenters shall not discuss investigative techniques.

3. One valuable source of educational information is the Exploited Child Unit of the National Center for Missing and Exploited Children (NCMEC) (800). They can be reached at (800) 843-5678 or through e-mail at exploited@ncmec.org for information on developing and delivering awareness and safety education programs.

V. Media Releases

1. Copies of media releases related to this initiative should be forwarded through the ICAC Supervisor to the *(Name appropriate approving authority for your agency, i.e. Chief of Police, Sheriff, etc)*. Copies of radio or video segments and press clippings will be used to promote and sustain public support for ICAC activities should also be reviewed prior to dissemination.

2. Media releases relating to prosecutions, crime alerts or other matters concerning ICAC investigations should be coordinated (if applicable) with other involved Federal State and local investigative agencies consistent with sound information management and media relations practices.

Inquiries regarding interpretation of this model policy may be directed to Chief Bradley J. Russ Portsmouth Police Department 3 Junkins Ave. Portsmouth, NH 03801 at (603) 427-1500 ext. 403 or by e-mail bruss@pd.cityofportsmouth.com

A GLOSSARY OF INTERNET AND INTERNET RELATED TERMS

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

CYBER TIPLINE

www.missingkids.com/cybertip

1-800-843-5678

THE INTERNET

The Internet is a communication network that is second in size only to the telephone network. Like the telephone network, it matters less to the end user how the technology works, and more how to use the technology. We usually approach the Internet with a goal in mind. That goal is to use the Internet to locate information. Thus the "researcher", often without giving the technology a second thought, uses the Internet to communicate with other computers to find desired information. On any given day there are roughly 40 million people using the Internet throughout the world.

The Internet traditionally encompasses several tools, some of which are electronic mail (e-mail), file transfer protocol (FTP), Gopher, Telnet and the World Wide Web (WWW). The advent of graphical web browsers has brought the World Wide Web to the forefront and pushed some of the other tools to the background. Exploring these Internet tools is much like checking under the hood of a car. You know the engine is there, but you don't necessarily need (or sometimes even want) to know how it works. In most instances, modern Internet technology makes knowledge of these tools unnecessary, but at the National Center for Missing and Exploited Children it is crucial that we grasp a sound understanding of the basics of this medium.

The quickest way to get on the Internet is to get an account on one of the commercial online services. Some of the major national commercial online services are Prodigy, CompuServe, America Online, Genie, Erols, Delphi and Microsoft. All of these services offer Internet e-mail, and several offer other Internet tools. Also, many offer free trial periods and home-access software. For about $10-20 per month, you can ask questions and electronically look over peoples shoulders to learn about the Internet.

Revisions / February 9, 1998

I have revised the Internet Glossary to include more relevant terms and have withdrew some words that were not needed. The previous version contained 123 terms, this glossary contains 288 terms. I have tried to shorten the definitions and have included a few tables to help explain a few of the terms. In addition I have included a new list of commonly used email and chat room symbols.

Again, it is important to understand that the Internet is constantly growing and thus the language that is associated with it will grow. These lists will continue to be reviewed and updated on a regular basis.

Section 1 **Quick Reference List**
Section 2 **Internet Glossary**
Section 3 **Chat Room and Email Acronyms and Symbols**

INTERNET QUICK REFERENCE LIST

Applet A small Java program that can be embedded in an HTML page. Applets differ from full-fledged Java applications in that they are allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The current rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

Baud In common usage the baud rate of a modem is how many bits it can send or receive per second. Technically, baud is the number o times per second that the carrier signal shifts value - for example a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud (4 x 300 = 1200 bits per second).

BBS (Bulletin Board System) -- A computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. There are many thousands (millions?) of BBS's around the world, most are very small, running on a single IBM clone PC with 1 or 2 phone lines. Some are very large and the line between a BBS and a system like CompuServe gets crossed at some point, but it is not clearly drawn.

Bps (Bits-Per-Second) -- A measurement of how fast data is moved from one place to another. A 28.8 modem can move 28,800 bits per second.

Browser A Client program (software) that is used to look at various kinds of Internet resources.

Cookie The most common meaning of "Cookie" on the Internet refers to a piece of information sent by a Web Server to a Web Browser that the Browser software is expected to save and to send back to the Server whenever the browser makes additional requests from the Server. Depending on the type of Cookie used, and the Browser's settings, the Browser may accept or not accept the Cookie, and may save the Cookie for either a short time or a long time. Cookies might contain information such as login or registration information, online "shopping cart" information, user preferences, etc. When a Server receives a request from a Browser that includes a Cookie, the Server is able to use the information stored in the Cookie. For example, the Server might customize what is sent back to the user, or keep a log of particular user's requests. Cookies are usually set to expire after a predetermined amount of time and are usually saved in memory until the Browser software is closed down, at which time they may be saved to disk if their "expire time" has not been reached. Cookies do not read your hard drive and send your life story to the CIA, but they can be used to gather more information about a user than would be possible without them.

Cyberspace Term originated by author William Gibson in his novel Neuromancer the word Cyberspace is currently used to describe the whole range of information resources available through computer networks.

E-mail
(electronic mail) Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses (mailing lists).

FAQ (Frequently Asked Questions) FAQs are documents that list and answer the most common questions on a particular subject. There are hundreds of FAQs on subjects as diverse as Pet Grooming and Cryptography. FAQs are usually written by people who have tired of answering the same question over and over.

FTP (File Transfer Protocol) Internet protocol (and program) used to transfer files between hosts.

Gopher A widely successful method of making menus of material available over the Internet. Gopher is a Client and Server style program, which requires that the user have a Gopher Client program. Although Gopher spread rapidly across the globe in only a couple of years, it has been largely supplanted by Hypertext, also known as WWW (World Wide Web). There are still thousands of Gopher Servers on the Internet and we can expect they will remain for a while.

Hit As used in reference to the World Wide Web, "hit" means a single request from a web browser for a single item from a web server; thus in order for a web browser to display a page that contains 3 graphics, 4 "hits" would occur at the server: 1 for the HTML page, and one for each of the 3 graphics. "hits" are often used as a very rough measure of load on a server, e.g. "Our server has been getting 300,000 hits per month." Because each "hit" can represent anything from a request for a tiny document (or even a request for a missing document) all the way to a request that requires some significant extra processing (such as a complex search request), the actual load on a machine from 1 hit is almost impossible to define.

Home Page (or Homepage) Several meanings. Originally, the web page that your browser is set to use when it starts up. The more common meaning refers to the main web page for a business, organization, person or simply the main page out of a collection of web pages

e.g. "Check out so-and-so's new Home Page." Another sloppier use of the term refers to practically any web page as a "homepage," e.g. "Tha web site has 65 homepages and none of them are interesting."

HTML(HyperText Markup Language) a language (or format) used for creating hypertext documents on the World Wide W[illegible] This is the format used to create Web pages..

HTTP (HyperText Transport Protocol) -- an information retrieval mechanism for HTML documents.

Hypergraphic: A graphic image link to other documents containing more information on the same or a related topic. To retrieve the related document, click on the hypergraphic. Similar to an icon in the Mac world.

Hypertext: A text link to other documents containing more information on the same or a related topic. Hypertext links are identified as different coloured text with an underline. To retrieve the related document, or move to the related link, click on the hypertext.

Internet A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network.

IRC (Internet Relay Chat) -- Basically a huge multi-user live chat facility. There are a number of major IRC servers around the world which are linked to each other. Anyone can create a channel and anything that anyone types in a given channel is seen by all others in the channel. Private channels can (and are) created for multi-person conference calls.

ISP (Internet Service Provider) -- An institution that provides access to the Internet in some form, usually for money.

Java Java is a network-oriented programming language invented by Sun Microsystems that is specifically designed for writing programs that can be safely downloaded to your computer through the Internet and immediately run without fear of viruses or other harm to your computer o files. Using small Java programs (called "Applets"), Web pages can include functions such as animations, calculators, and other fancy tricks. We can expect to see a huge variety of features added to the Web using Java, since you can write a Java program to do almost anything a regular computer program can do, and then include that Java program in a Web page.

Listserv The most common kind of maillist, Listservs originated on BITNET but they are now common on the Internet.

Login Noun or a verb. Noun: The account name used to gain access to a computer system. Not a secret (contrast with Password). Verb: The act of entering into a computer system, e.g. Login to the WELL and then go to the GBN conference.

Maillist (or Mailing List) A (usually automated) system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the maillist. In this way, people who have many different kinds of e-mail access can participate in discussions together.

Modem A device that you connect to your computer and to a phone line, that allows the computer to talk to other computers through th phone system. Basically, modems do for computers what a telephone does for humans.

Newsgroup The name for discussion groups on USENET.

Online To be connected, by way of a modem, to the World Wide Web.

Password A code used to gain access to a locked system. Good passwords contain letters and non-letters and are not simple combinations such as virtue7. A good password might be: Hot$1-6

Server A computer, or a software package, that provides a specific kind of service to client software running on other computers. The ter can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, e.g.Our mail server is down today, that's why e-mail isn't getting out. A single server machine could have several different server software packages running on it, providing many different servers to clients on the network.

Terminal A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to b (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

URL (Uniform Resource Locator) -- The standard way to give the address of any resource on the Internet that is part of the World Wide Web (WWW). A URL looks like this: http://www.matisse.net/seminars.html or telnet://well.sf.ca.us or news:new.newusers.questions etc. The most common way to use a URL is to enter into a WWW browser program, such as Netscape, or Lynx.

USENET A world-wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the Internet, maybe half. USENET is completely decentralized, with over 10,000 discussion areas, called newsgroups.

WWW (World Wide Web) -- Two meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers) which are the servers that allow text, graphics, sound files, etc. to be mixed together.

INTERNET RELATED TERMS

A

ac
If a Domain Name includes the characters "ac" then the site is associated with an academic institution e.g www.collegename.ac

Access Provider
A company which provides its customers a service whereby the can access the Internet. The user normally connects to the Access providers computer via a modem using a dial up connection.

Access Time
A standard measure which indicates the level of performance of the Hard Disk. The measure is the actual time that it takes for a piece of Data to be located on the Hard Disk.

AI
Artificial Intelligence.

Alias
An alias is an alternate name used to refer to something or someone.

Animated GIF File
A special type of GIF File. They gives the impression of a video. A collection of GIFS, presented one after the other each picture slightly different from the previous. Same principle as a film.

Anonymous FTP
The mechanism of actually connecting to a remote computer, as an anonymous user, normally to transfer files back to your own PC.

Anonymous FTP Site
If an FTP site does not require the user to have their own specific User ID & password the site is called an Anonymous FTP Site. Basically they can be accessed by anybody.

Anorak
A rather unkind reference to somebody whose life revolves around computers & computer technology.

These people are also stereotyped as being into trainspotting (the real thing not the movie). Someone who spends a lot of time putting together a Glossary of PC & Internet Terminology is not necessarily an Anorak.

ANSI

American National Standards Institute. It is a US business group which sets the standards - it is a voluntary organisation. ANSI is frequently seen in 3 areas:-

- Programming Languages - FORTRAN, COBOL & C conform to ANSI
- SCSI
- ANSI.SYS Device Driver. Available in DOS - it enables the use of ANSI defined commands (using the escape key) to control the screen & the keyboard

Anti Virus Software

A program which is written specifically to locate & remove harmful viruses from your PC. These programs constantly have to be updated to cater for new viruses as they become known.

Applet

An applet is a very small program written in the Java programming Language which can only be used as part of a Web Page. The Browser you are using must be capable of running Java Applets. They are used to bring a Web page to Life.

Application Program

A Program which has been created to perform a specific task which is useful to the user - unlike the operating system which is a program that controls the PC. Most people buy PC's so that they can run application programs. Examples include :-

- Wordprocessor
- Spreadsheet
- Home Finance Package
- Drawing Package

Archie

A Program which enables you to find Files on the Internet which you can transfer to your own PC. Archie searches the internet & provides you with a list of all the locations of the type or name of file that you are looking for. You can then transfer the file that you require using FTP.

The name Archie is derived from the word Archive

Archive

A backup copy of data designed to be kept long term - often for security or audit reasons. The verb for doing this is also archive.

Artificial Intelligence

A computer science which involves making a computer imitate human intelligence - learning as it goes along.

ASCII

American Standard Code for Information Interchange. It is a standard way of representing ordinary text as a stream of binary numbers. A code set of 128 characters. The first 32 characters are control codes & the remaining 96 are upper & lower case letters, numbers, punctuation marks & special characters.

ASCII Text File

The most common File Format found on PC's. They are basically text files which contain no formatting information at all. They do not require special programs to access them

AUTOEXEC.BAT

This is one of the two special Batch Files which **Auto**matically **Exec**ute when the PC is started up - the other being CONFIG.SYS. This File is normally located in the Root Directory. An example AUTOEXEC.BAT is :-

```
@ECHO OFF

CLS

PROMPT $p$g

PATH=C:\DOS;C:\WINDOWS

SET TEMP=C:\DOS
```

"`@ECHO OFF`" stops DOS from displaying each command on screen rather than just its results. "`CLS`" clears the screen. "`PROMPT $p$g`" determines what appears before the flashing cursor, p specifies show the path and g specifies show the ">" sign. "`PATH=C:\DOS;C:\WINDOWS`" tells DOS where to look for a File if it can't find it in the Current Directory. If a version of the file happened to exist in more than one of the Directories in the Path the file in the first directory listed would be the one that was selected. "`SET TEMP=C:\DOS`" tells programs which directory to place any Temporary Files which may be produced.

BABT Approval

Any Modem used in the UK must be approved by the **B**ritish **A**pproval **B**oard for **T**elecommunications. A green circle means approval, a red triangle means it has not been approved.

Back Up

A Back up is a duplicate copy of some data or a disk or some software that is made by the user as a safeguard against the loss of the original information. Should this happen then the information can be recovered by restoring or copying the information back from the backup.

Band Width

The Band Width is basically the maximum speed at which data can be transmitted between computers in a network.

Basic

Beginner's All-purpose Symbolic Instruction Code. A very popular programming language developed by John Kemeny and Thomas Kurtz at Dartmouth College in the 1960's. Their have been a number of implementations of basic over the years including :-

- Tiny Basic
- Microsoft Basic
- CBasic
- Integer Basic
- Applesoft Basic
- GW Basic
- Turbo Basic
- Microsoft QuickBasic

Historically, basic has been the programming language with which most people have got their first experience of programming.

Batch File

A Batch File is a set of DOS commands contained within a single Text File. If this text File has a File Suffix of .BAT then by entering the File name at the DOS Prompt, the DOS commands will be executed one after the other. AUTOEXEC.BAT is an example of a Batch File.

Baud

In common usage the baud rate of a modem is how many bits it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value - for example a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud (4 x 300 = 1200 bits per second).

BBS

Bulletin Board System - a computer which allows the people who subscribe to it to :-

- Copy files to it from their own PC's
- Copy files from it to their own PC's
- Send messages to other users of the Bulletin board
- Play multi-player games.

BBS's are still around in abundance but have generally been superseded by the Internet

Beta Version

Beta Version refers to a version of an Application Program which is available for use but is not the definitive version that the company who developed the product will be releasing as the final product - it carries a warning that it is not 100% reliable - the idea of this is to iron out any unidentified problems before releasing it to the whole world.

Binary

The Base 2 numbering system which has a very high use in PC technology. 10 in Binary is equivalent to 2 in decimal.

BIOS

The PC's Basic Input/Output System stores a set of instructions which tells your PC how to handle input from the keyboard or the mouse & output to the printer or monitor.

Bay

An opening at the front of the PC's Case which is designed to hold a data storage device such as a hard disk or a CDROM

Bit

A bit is the smallest unit of information understood by a computer. A bit can take a value of 0 or 1. A byte is made up of 8 bits which is large enough to contain a single character. For example the character 2 would be equivalent to "00000010" when represented in bits. A Kilobyte is equivalent to 1024 bytes. A Megabyte is equivalent to 1024 Kilobytes. A Gigabyte is equivalent to 1024 Megabytes.

A Megabit is 1048576 bits.

Bit	Byte	Kilobyte	Megabyte	Gigabyte
8	1	-	-	-
8,192	1,024	1	-	-
8,388,608	1,048,576	1,024	1	-
8,589,934,592	1,073,741,824	1,048,576	1,024	1

Bps

(Bits-Per-Second) -- A measurement of how fast data is moved from one place to another. A 28.8 modem can move 28,800 bits per second.

Browser

An application program which interprets HTML & presents the final Web Page. Used to "Surf the WWW". Examples include:-

- Internet Explorer
- Netscape Navigator
- Mosaic

Bus

Data is transmitted to & from the different components of a PC via a bus. Different types of BUS are :-

- CPU/Memory bus
- I/O Bus
- Local Bus

The CPU/Memory bus runs at the same speed as the Processor but the I/O Bus runs at about 8MHz.

Bus Clock Speed

The speed in Megahertz at which the I/O bus runs.

Byte

A Byte is a unit of measure for Data Storage. 1 Byte is equivalent to 8 Bits.

Bit	Byte	Kilobyte	Megabyte	Gigabyte
8	1	-	-	-
8,192	1,024	1	-	-
8,388,608	1,048,576	1,024	1	-
8,589,934,592	1,073,741,824	1,048,576	1,024	1

Cache

A Cache Memory is a small but very fast memory used to store frequently used Data or instructions. It

tries to "guess" what data is going to be needed next by the Processor. The Cache can be:-

- Level 1 (Primary) Cache - part of the processor itself - fast & expensive
- Level 2 (Secondary) Cache - Mounted on the Motherboard slower than Level 1

CCITT

Consultative Committee on International Telegraphy and Telephony is an international committee based in Geneva that sets standards for the whole world on Telecommunications

CD ROM

A CD ROM (Compact Disk - Read only Media) can contain vast amounts of information (over 600Mb) which is accessible via a PC providing it contains a CD ROM Drive. As the name suggests you can only read information from a CD ROM.

CD ROM Drive

A CD ROM Drive is required to enable the PC to read CD ROM's. The power of the CD ROM Drive is determined by its speed. Available on the market nowadays are:-

- Two Speed
- Four Speed (Quad)
- Six Speed
- Eight Speed
- Ten Speed
- Twelve Speed
- Sixteen Speed
- Twenty Speed
- Twenty Four Speed

Central Processing Unit

Refers to the Microprocessor & the Memory of the PC.

CGA

Colour Graphics Adapter Video Apapter introduced by IBM in 1981. A CGA Monitor can display 640 X 200 pixels using 2 different colours or 320 X 200 pixels using 4 colours.

CGI

Common Gateway Interface Scripts are used by Internet Programmers to perform basic functions such as counting the number of times a Web Page is accessed

Client Server

Client/Server distributes the processing of a Computer Application between 2 computers the Client & the Server - the principle being to exploit the power of each. The Client is normally a PC. The

Application Program will access Data & perform processing on the Server & using the data obtained via the server more processing tasks will be performed on the Client. The Application can be used by more than one user.

Clock Speed
The speed at which the PC works measured in Megahertz

CMOS
CMOS stands for Complimentary Metal-Oxide Semiconductor. It is a special RAM Chip which stores vital settings about your PC - such as the size of the Hard Disk & the amount & type of Memory. This information is stored even when the PC is switched off.

Command Interpreter
The command interpreter is a DOS program which executes commands entered at the DOS prompt.

Com Port
1 of up to 4 serial ports on your PC - normally used for a mouse or a modem

Compression
A technique used to considerably reduce the size of a file without loosing any of the original information. The compression process alters the content of the file but this can & is completely recovered by reversing the process.

CONFIG.SYS
This is one of the two special Batch Files which Automatically Execute when the PC is started up - the other being AUTOEXEC.BAT. This File serves the purpose of giving you the opportunity to Configure your System to you own requirements. Commands in your CONFIG.SYS commonly set up your PC to work with other Peripherals such as a CD ROM Drive. This file is normally located in the Root Directory. An example CONFIG.SYS is :-

```
DEVICE=C:\DOS\SETVER.EXE

DEVICE=C:\DOS\HIMEM.EXE

DEVICE=HIGH

FILES=30

SHELL=C:\DOS\COMMAND.COM C:\DOS/P
```

"DEVICE=C:\DOS\SETVER.EXE" fools Software into thinking it is running under an older version of DOS (i.e. upgrading to a new version of DOS does not mean that your old programs can no longer be used - good in theory but does not always work in practice. "DEVICE=C:\DOS\HIMEM.EXE" loads the Extended Memory Manager. "DEVICE=HIGH" saves Conventional Memory by loading Parts of DOS into the High

Memory area above 1Mb. "FILES=30" is the number of Files that can be open at any one time. "SHELL=C:\DOS\COMMAND.COM C:\DOS/P" points to the Command Interpreter. The /P telling it to stay permanently in Memory

Controller

A circuit board which links the Hard Disk & the Motherboard. When access to information on the hard disk is requested by the Operating System, the controller tells the Hard Disk to get to work. With IDE Hard Disks, the controller is built into the Hard Disk itself.

Conventional Memory

The first 640 Kilobytes of Memory. All DOS programs run in Conventional Memory.

Cookie

A file that is written to your Hard Disk when you access certain Web Pages. The file contains certain information, often information that you entered when you displayed the page. The next time you access this page a check is done to see if the Cookie exists. The information within the cookie may well influence what happens next.

CPU

Central Processing Unit.

CPU/Memory Bus

The CPU/Memory bus, also referred to as the System Bus, transmits data between the CPU, Cache & RAM. The CPU/Memory Bus runs at the same speed as the Processor.

Current Directory

The current directory is the DOS Directory at which the user is currently positioned. The current directory can be changed using the "CD" command. For more information type "help" at the DOS prompt

Cursor

A flashing rectangle or line on the screen which shows exactly where the user is working. For example, when using a Word Processor the cursor indicates the point at which the characters being typed by the user will be inserted.

Cyberpunk

Cyberpunk was originally a cultural sub-genre of science fiction taking place in a not-so-distant, dystopian, overindustrialized society. The term grew out of the work of William Gibson and Bruce Sterling and has evolved into a cultural label encompassing many different kinds of human, machine, and punk attitudes. It includes clothing and lifestyle choices as well.

Cyberspace

Term originated by author William Gibson in his novel Neuromancer the word Cyberspace is currently used to describe the whole range of information resources available through computer networks.

Daisy Chain

A Daisy Chain, is when a number of PC's and or Peripherals are connected to each other in a series. When devices are daisy-chained to a PC, the first device is connected to the PC, the second device is connected to the first etc.

Data

The content of a File, e.g. the information contained within a Spreadsheet, the contents of the Records on a Database

Database

A collection of Data organised & designed for easy access. A collection of customer names & addresses may form the content of a database.

Databits

When you send an Email to a friend or colleague the information will be sent (probably using a modem) across a network. As well as sending the content of the Email, information telling the system where it has come from, where it is going to, how much data should be sent e.t.c will also be sent as part of the transmission. Databits refers to the bits of information in this transmission which contain the content of the Email message.

Data Transfer Rate

The speed at which data can be read from the hard disk & delivered to the processor

DDE

Dynamic Data Exchange. When 2 or more programs that support DDE are running simultaneously, they can exchange information and commands. For example, a spreadsheet with a DDE link to a communications program might be capable of keeping stock prices that are displayed in the spreadsheet current with trading information received over the communications channel.

Default Value

A number of programs will require the user to provide information. In some cases if the user chooses not to enter a value a "default value" will be taken. If for instance you have a Database in which you record the names & addresses of all your customers & nearly all of them are based in the UK you can set the database up such that if a country is not entered then it will be defaulted to the UK.

DES

Data Encryption Standard. A commonly used standard method used for Encrypting & Decrypting Data. Encryption is necessary as valuable & sensitive information is often sent from one computer to another via a network which technically can be accessed by anybody. It provides a degree of security should the information fall into the wrong hands. DES was developed by the U.S National Institute of Standards & Technology.

Desk Top Publishing

Using your PC to produce professional publications which can be used to market your products or present useful information to your customers. Software packages which are specifically designed for this purpose include :-

- Microsoft Publisher
- Corel print House

Device Driver

Software that allows the PC to talk to hardware devices such as the printer & the Mouse. If you buy a new Printer it will come complete with a Disk containing the necessary Device Drivers.

Dialog Box

A box displayed on your PC screen by a program including a message normally indicating that something is about to happen or has just happened. The dialog box requires the user to respond to the message before continuing with what it is about to do - normally the response is in the form of a Yes or No & based on the answer the program will carry out the next step or stop what it is doing. An example of this could be within an Email program - you read a message that has been sent to you & you decide to delete the message. After clicking on the delete button a dialog box containing the message "Are you sure you want to remove this message from your PC ? Yes or No" may be displayed.

Dial Up Connection

A temporary connection between two computers via a telephone line normally using a modem - the most common method used to access the internet

A to Z index

Digital camera

A digital Camera is basically a camera which produces photographs which can be saved as files on your PC. These cameras do not require a film to be processed. This is an ideal way to get a picture of anything that you need to include in a web page. The alternative is to take an ordinary photograph & use a scanner to scan the image into a file on your PC.

Digital Video Disk

New Disk Technology. Digital Video Disks can hold over 4 Gigabytes of information - these are predicted to eventually supercede CD's.

DIMMs

Dual In-line Memory Modules. Memory chips which are soldered onto plugs which slot into sockets on the Motherboard of the PC - makes fitting memory much easier than it use to be.

They have 168 pins in two rows. See SIMMs

Directory

A directory is catalog for files stored on the Hard disk of a PC; a mechanism to group the files so that the user is not overwhelmed by a one huge long list of all the files stored on the hard disk. All the filenames belonging to a particular project, for example, might be kept together in one directory. The topmost directory is called the root directory; the directories within a directory are called sub directories.

```
Example

C:\WINDOWS\SYSTEM
```

In this Example "C:\" is the Root Directory, "C:\WINDOWS" is referred to as the WINDOWS directory & "C:\WINDOWS\SYSTEM" is referred to as the SYSTEM directory. This directory is a subdirectory of "C:\WINDOWS".
Windows 95 refers to directories as Folders

Diskette

Another name for a 3.5 inch Floppy Disk.

DLL

Dynamic Link Library - A library of program subroutines which can be shared amongst several different Application Programs - a concept which is extensively used under Windows. Windows programmers do not have to re-invent the wheel each time they want to do something common such as undo the last command or highlight a line of text.

DNS

The Domain Name System is how the Internet links together the thousands of Networks which it is comprised of. The DNS is utilised whenever you send an Email or access a particular Web Page. Each computer on the Internet has a one of more Domain Names such as "fredbloggs.co.uk". The .co indicates a commercial organisation & the .uk indicates that the computer is in the United Kingdom.
Standard conventions used in Domain Names include:-

- ac - Educational institution
- co - Commercial organisation

- com - Commercial organisation
- edu - Educational institution
- gov - Non military government organisations
- int - International Organisations
- mil - Military government organisations
- net - Networks
- org - non profit organisation

You will also see these codes in URL's such as "homepages.enterprise.net/jenko/Glossary/G.htm".

These DNS converts the Domain Names to a unique number known as an IP address (the IP stands for Internet Protocol). You will often see the IP address displayed by your Web Browser when you are connecting to a particular computer.

Domain Name

The Domain Name is a unique name which represents each computer on the Internet. (Some machines do have more than one Domain Name. The DNS converts the Domain Name requested by an Internet User into an IP Address. The location of the machine with this IP address is known & the information being requested can then be found. "www.yahoo.com" is an example of a Domain Name. The "com" indicates that Yahoo is a commercial Organisation. Other codes include:-

- ac - Educational institution
- co - Commercial organisation
- com - Commercial organisation
- edu - Educational institution
- gov - Non military government organisations
- int - International Organisations
- mil - Military government organisations
- net - Networks
- org - non profit organisation

You will also see these codes in URL's such as "homepages.enterprise.net/jenko/Glossary/G.htm".

These Domain Names are converted to a unique number known as an IP address (the IP stands for Internet Protocol). You will often see the IP address displayed by your Web Browser when you are connecting to a particular computer.

DOS

Disk Operating System. oversees such operations as disk input and output, video support, keyboard control, and many internal functions related to program execution and file maintenance.

Download

To copy files from another computer to your own PC via a network or using a modem.

DPI

Dots Per Inch - A measure of the quality of the output from a printer - the greater the number of DPI the better the printer.

DRAM

Dynamic Random Access Memory. It is a type of RAM capable of speeds of about 40MHz. Superceded by EDO RAM.

DTP

Acronym for Desk Top Publishing.

DVD

Digital Video Disk, New Disk Technology. Digital Video Disks can hold over 4 Gigabytes of information - these are predicted to eventually supercede CD's.

DVDROM

Digital Video Disk Read Only Media, Digital Video Disks which can only be read.

EDO RAM

Extended Data Out Random Access Memory. It is a type of RAM capable of speeds of about 50MHz. It holds its last requested data in a cache after releasing it.
Superseded by SDRAM.

edu

If a Domain Name includes the characters "edu" then the site is associated with an academic institution e.g www.collegename.edu

EGA

Enhanced Graphics Adapter Video Adapter introduced by IBM in 1984. A EGA Monitor can display 640 X 350 pixels using 16 different colours from a table of 64 colours.

EIDE

Enhanced Integrated Drive Electronics - protocol which allows for faster data transfer rates & the connection of up to 4 hard disks to a PC - supersedes IDE.

Email

ElectronicMail - a way of sending other people messages from your PC. Widely used facility on the Internet which basically sends addressed messages over a Network. The message normally gets there in a couple of minutes. Internet users refer to the conventional Mail system as "Snail Mail". Who says Anoraks don't have a sense of humour.

Encryption

Encryption is the process of converting data into "unreadable code" so that prying eyes cannot understand the content. Encryption is necessary as valuable & sensitive information is often sent from one computer to another via a network which technically can be accessed by anybody. It provides a degree of security should the information fall into the wrong hands.

Ethernet

Ethernet is a LAN which was developed by Xerox in 1976. The different Nodes on the Network are connected by Coaxial Cable. This cable can be thin (which can connect 2 Nodes up to a distance of about 1000 feet) or thick (which can connect 2 Nodes up to a distance of about 3300 feet). The Ethernet standard has a provision to transmit data at a rate of 10 megabits per second.

Expanded Memory

Physical Memory above 1 Megabyte for PC's with an 8086 or 8088 microprocessor (or simulating these microprocessors). This memory can be accessed using an Expanded Memory Manager.

Expanded Memory Manager

A program which allows DOS to utilise the Expanded Memory.

Expansion Card

A printed circuit card such as a video card that plugs into an expansion slot and adds functionality to the PC.

Expansion Slot

Compartments in a PC into which you can plug expansion cards such as a video or sound card & connect them to the system bus. Most PC's have from 3 to 8 expansion slots.

Extended Memory

Physical Memory above 1 Megabyte for PC's with an 286 or above microprocessor (or simulating these microprocessors).

Extranet

Very similar to an Intranet with the added feature that the information contained can be accessed externally by business partners.

FAQ

Frequently Asked Questions - a term used in magazines & by Software companies to provide users with answers to those questions that we all have to ask.

Fiber Optics

A technology by which data is transmitted using light through glass fibre cable

Finger

An Internet software tool for locating people on other Internet sites. Finger is also sometimes used to give access to non-personal information, but the most common use is to see if a person has an account at a particular Internet site. Many sites do not allow incoming Finger requests, but many do.

File

Data is stored in the form of a file. Files can be program files - contain instructions which allow the PC to perform various tasks under the control of the user or data files which contain information only.

File Format

Defines or categorises files based on the way that the data is stored & presented. Examples include :-

- ASCII Text
- TIFF
- GIF

The format of a file governs which programs can process the file for either update & or display purposes.

Firewall

A combination of specialised hardware & software designed to keep unauthorised users from accessing information within a networked computer system.

Floating Point Calculation

A mathematical method which the processor uses to perform calculations which need a very high degree of accuracy

Floppy Disk

A magnetic disk which is used to store data. They come in 3.5 & 5.25 inch diameter variants. Floppy disks are often used to transfer files from one PC to another or to backup important files.

Flowchart

A Flowchart is a diagram which is produced to show the steps in a particular process. The flowchart will show what are the inputs & outputs in each of the steps. Flowcharts are frequently used to show diagramatically what processes certain computer programs perform.

FTP

File Transmission Protocol - a standard for moving Files from one computer to another. Predominant use on the Internet. This master copy of this document resides on my (Steve Jenkins) home computer. When I make a change to it I use FTP to transfer the updated files to the computer of my Internet Service Provider. I can also use FTP on certain computers on the internet to transfer files to my home computer.

A computer on the Internet which specifically stores files for users to FTP to there own computers is called an FTP Site.

If the FTP site does not require the user to have your own specific User ID & password is called an Anonymous FTP Site.

Function

A Function is similar to a subroutine in that it is part of a program which can be performed a number of times. The difference is that a function has input parameters & output parameters. For example I have developed a function which you pass in the date of your birthday - the function then calculates how many days there are until your next birthday & passes the result of this back to the program - I use this function in a Web Page which displays the number of days until the next birthdays of all the members of my family (except uncle Bert who likes to keep his birthday a secret).

General Protection Fault

A Windows term - Each program running under windows is given its own exclusive area of memory which is protected from other applications & a general protection fault occurs if this exclusive memory is accessed by another program.

Gateway

The technical meaning is a hardware or software set-up that translates between two dissimilar protocols, for example Prodigy has a gateway that translates between its internal, proprietary e-mail forznat and Internet e-mail format. Another, sloppier meaning of gateway is to describe any mechanism for providing access to another system, e.g, AOL might be called a gateway to the Internet.

GIF File

The most common type of image file used on the Internet. These files are compressed so they take up the minimum amount of space & can therefore be downloaded a lot quicker than other graphics file.

GIF files are typically used for:-

- Backgrounds
- Displaying banners
- Advertisements
- Buttons

The files unlike other graphical file types are limited to 256 colours.

GIF Files are stored in a number of different formats such as:-

- 87a
- Interlaced 87a
- 89a
- Interlaced 89a

The interlaced versions are designed to allow the image to be gradually revealed as it is downloaded.

Gopher

An application whose purpose is to locate, retrieve & record information from the Internet. Developed at the University of Minnesota in 1991.

Gopherspace

The information that is available via the Gopher tool set.

Graphic

A picture or non text item within a document. Most Web pages will contain a number of Graphics

GUI

GUI stands for Graphical User Interface. A Graphical User Interface is designed so that the user can perform tasks by using a mouse to point & click on an icon. The user can perform any task with either the mouse of the keyboard.

GIF Files can also be:- 

Hacker

Somebody who deliberately Logs on to other computers by somehow bypassing the Log on security system - this is sometimes done to steal valuable information or to cause irreparable damage.

Hard Disk

The Hard Disk is where the data is stored within the PC. Hard Disks have the capacity to contain several megabytes or even a few gigabytes of data.

Hardware

The physical components of a PC including Peripherals.

Head

The part of the harddisk mechanism which actually reads & writes data to the disk.

Hexadecimal

The Base 16 numbering system which has a very high use in PC technology. The decimal numbers 10 to 15 are represented by the letters A to F. 10 in hexadecimal is equivalent to 16 in decimal.

High Memory Area

The first 64 Kilobytes of Extended Memory.

Hit

This occurs when a web page is accessed by a user or a program accesses the page.
A hit was registered on this particularly web page (the Letter "H" in the Glossary) when you requested to look at the information contained within it.

Home Page

The page by which a user normally enters a web site. If you click on the "A to Z index" below you will display the Home Page of this Glossary Web Site.

Host Computer

A Host Computer is one which provides a particular service to a user. This includes Information or communications.

Hot Java

Hot Java is a Web Browser which can display "executable content" written in the Java Programming Language

HTML

HyperText Markup Language - the text based language used to construct WWW pages. Interpreted by Web Browsers. This delightful masterpiece is a collection of HTML instructions which you can see using the View HTML Source option form your Browsers menu.

HTTP

HyperText Transmission Protocol is a Protocol that Computers on the Internet use to communicate with each other.

Hypermedia

Basically, Hypertext which also contains Multimedia components.

Hypertext

Text which contains links which can be clicked with a mouse. When the user "clicks" the link they are taken to another document or a different section of the current document. This Glossary is a good example of Hypertext.

- Animated - gives the impression of a video. A collection of GIFS, each picture slightly different from the previous. Same principle as a film
- Transparent - Blends in with the background

IAB

Internet Architecture Board - a group of people which makes decisions regarding Internet Standards. IETF & IRTF are subordinate to the IAB.

ICE

Intelligence Concept Extraction - technique used by Search Engines to relate words to ideas, so if you do a search for "camping equipment" you may well find articles specifically about tents.

Icon

An Icon is a small picture which is displayed on the screen. It is intended to depict pictorially a task. By clicking the icon with the mouse will invoke the task. It is an essential component of a Graphical User Interface.

Examples include:-

- A folder with a magnifying glass to depict Windows Explorer
- A book with a question mark to depict a help file
- A blue notepad to depict, believe it or not, Windows Notepad

IDE

Integrated Drive Electronics. Most PC's contain IDE Hard Drives. They normally contain built in controllers.

IEEE

Institute of Electrical & Electronic Engineers. This organization is responsible for many of the accepted communication standards

IETF

Internet Engineering Task Force. A subgroup of volunteers of the IAB that concentrates on technical issues on the Internet. The tactical arm of the IAB.

Image Map

A graphic which is divided into different areas each of which link to different web pages. An example of where this could be used is by an Australian company that has an office in each state capital. The Graphic would be a Map of Australia. If the user clicked on Melbourne the Victoria Web Page would be displayed but If the user clicked on Sydney the New South Wales Web Page would be displayed

Index

An index is something which points at other information - a program will often use an index to locate a particular record on a file - same concept as an index in a book. Most Databases make use of indexes

Install

To add hardware or load a software application onto your PC.

Instruction Set

Basically the set of instructions which a particular Microprocessor can recognise such as add, subtract.

Integer

As in mathematics, a whole number which does not contain any decimals

Internet

The Internet is a world wide computer network through which you can send a letter, chat to people

electronically or search for information on almost any subject you care to think of. Quite simply it is a "network of computer networks". It originated in the 1960's in the USA where the US defence were conscious of having its computer network destroyed by blowing up the central computer. A network was designed around the principle of "unreliable computers" - if one was destroyed or failed the remaining computers could still function. Each computer in the network acknowledges the existence of all of the others.

InterNIC

InterNIC is a group of people who control domain name registration. They also provide various services to all users of the internet.

Intranet

An internal or Company Internet that can be used by anyone who is directly connected to the companies computer network

I/O

Input Output deals with 2 out of 3 of the activities (input, processing, and output) performed by a PC. I/O are complimentary tasks of gathering data for the microprocessor to work with and making the results available to the user through a device such as the monitor or printer. The keyboard and the mouse are input devices that make information available to the computer; the display and printer are output devices with which the computer makes its results available to the user. The Hard Disk is both an input and an output device because it can either provide stored information or store the data after processing

I/O Bus

Input Output Bus - used to transmit data from the Cache & the RAM to the PC disks.

I/O Port

Input Output Port - part of the PC which is used for passing data in and out of a computing device. This is normally located on the back of the PC. The port can be a Serial Port - data is sent/received one bit at a time through a cable containing a single wire, or a Parallel port where the data is sent/received through a cable containing several pieces of wire so that more than one bit at a time can be processed

IP Address

The Internet Protocol address is a unique number which is used to represent every single computer in a Network. All the computers on the internet have a unique IP address. The format of the IP Address is 4 numbers separated by dots e.g. 198.123.456.7.

IRC

Internet Relay Chat is the CB Radio of the Internet. Basically you can "chat" to a number of people by typing simple messages at your keyboard & these are responded to by one or more other people from all over the world who happen to be "chatting" to you via IRC.

IRQ

Interrupt Request. This forces the CPU to stop what it is doing so that it can carry out the task requested as part of the IRQ.

IRTF

Internet Research Task Force. A sub group of the IAB that considers the stratgeic approach to issues with the Internet - creates long term solutions to new challenges which have to be addressed. The strategic arm of the IAB.

ISDN

Integrated Services Digital Network is a fast digital phone line - can be provided by most phone companies. To be able to reap the benefits you will need to add a special card to your PC and your Internet Service Provider must be able to provide an ISDN connection.

ISOC

The Internet SOCiety, worldwide standards organization - sponsor the IAB.

ISP

Internet Service Provider or sometimes referred to as Internet Access Provider (IAP) is a company which provides access to the Internet for people like you & me. The company handles the link from your PC to the rest of the Internet. The ISP's central computer is linked to the rest of the internet so the person using this service only pays the telephone charges to connect from their home computer to the ISP's central computer

Java

Java is a modern Programming Language , first seen in 1995 , & is used to bring Web Pages to life. Java programs are referred to as applets.

Java is an interpreted, object-orientated program language with a syntax & structure similar to C++,

designed specifically for the internet by Sun microsystems

One huge plus for Java is that Java programs can run on many different types of computer (e.g. IBM PC, Apple Macintosh).

Java Applets are always small in size & can be downloaded from the Internet & executed as part of the Web page being displayed.

Once a programmer has completed the Java program it is compiled to produce an executable module. This executable module has instructions written for the "Java virtual machine" - this is designed for the platform on which the module is to be executed. These instructions are interpreted on the platform where the program is being executed. The "Java Virtual Machines" are available for a number of operating environments e.g. Windows, AIX, OS/2.

JavaScript

JavaScript is a Programming Language for developing Client Internet applications. The WEB Browser interprets JavaScript statements embedded in an HTML page. LiveWire is the Server based equivalent which enables you to create applications similar to Common Gateway Interface (CGI) programs.

Joystick

A pointing device mostly used for playing computer games

JPEG

JPEG is a type of image file used on the Internet. Like GIF files, JPEG files are compressed. Unlike GIF files JPEG files cannot be interlaced or transparent.

Kermit

A program developed at Columbia University to transfer files between computers

A to Z index

Keyboard

The Keyboard is the main device that we use for entering data into a PC or giving it an instruction to do something specific. The key arrangements resemble that of a tradition typewriter plus lots more additional keys for specific functions.

A to Z index

Kilobyte

A Kilobyte is a unit of measure for Data Storage. 1 Kilobyte is equivalent to 1024 Bytes or 8192 Bits.

Bit	Byte	Kilobyte	Megabyte	Gigabyte
8	1	-	-	-
8,192	1,024	1	-	-
8,388,608	1,048,576	1,024	1	-
8,589,934,592	1,073,741,824	1,048,576	1,024	1

LAN

A Local Area Network is a group of PC's, Other Computers & Peripheral Devices which are linked together where each device is located in close proximity to all the other devices. LANs typically consist of a number of PC's, shared printers & Shared Directories & Files.

Laptop

A Laptop is a portable PC. The term Laptop has been superseded by Notebook. The original laptops were bulky & quite heavy.

LCD

Liquid Crystal Display - a low power display - frequently used in Laptops

LED

Light Emitting Diode - An electronic device which gives off light when an electric current is passed through it. Most indicator lights, such as the one which comes on when you switch on your PC use an LED.

Level 1 Cache

Cache Memory which is part of the processor itself - fast & expensive.

Level 2 Cache

Cache Memory which is mounted on the Motherboard - slower than Level 1 Cache.

Link

A component of a hypertext document which when clicked with a mouse takes the user to another document or a different section of the current document. The word "mouse" above in this paragraph - which you can probably see in mauve or blue is an example of a link.

Listserv

The most common kind of maillist, Listservs originated on BITNET but they are now common on the Internet.

Local Bus

Local Bus introduced to circumvent the delay due to the vast difference in speeds between the CPU/Memory Bus & the I/O Bus.

Login

This is the term for the process of actually gaining access to the resources on a particular computer - normally this is done by entering a userid & a password.

Log off

The process of actually ending your access to a particular computer.

Log out

The process of actually ending your access to a particular computer.

Mailbox

The file or directory where your incoming email messages are stored on the computer of your Internet Service Provider.

Maillist

(or Mailing List) A (usually automated) system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the maillist. In this way, people who have many different kinds of e-mail access can participate in discussions together.

Megabyte

A Megabyte is a unit of measure for Data Storage. 1 Megabyte is equivalent to 1024 Kilobytes or 1,048,576 Bytes or 8,388,608 Bits.

Bit	Byte	Kilobyte	Megabyte	Gigabyte
8	1	-	-	-
8,192	1,024	1	-	-
8,388,608	1,048,576	1,024	1	-
8,589,934,592	1,073,741,824	1,048,576	1,024	1

Megahertz

The measure of how fast a Chip can work

Memory

Chips which hold information which the PC needs to use. These chips are connected directly to the Microprocessor. There are two types of Memory Chip:-

- Random Access Memory (RAM)
- Read Only Media (ROM)

Menu

A Menu is a list of options presented to the user to enable them to perform a specific task. Each option on the list will perform a different task.

Microprocessor

The Microprocessor is built onto a single piece of silicon, known as a wafer or chip, Its size is about 0.5 cm along one side and no more 0.05 cm thick. It can be programmed to perform a great number of information-handling tasks. It can serve as a general-purpose computer for instructional or word-processing use, to control other machines or industrial processes such as making food products, and for hand-held calculators. Its advent was brought about by the progressive miniaturization of integrated circuits and by advances in semiconductor technology.

A microprocessor may function by itself in a wide range of applications, incorporating from as few as 1000 or as many as several hundred thousand elements on its single chip. It may also serve as the CPU of a PC, when it is combined with support chips containing computer memories and is equipped with

input-output devices. Microcomputers gained great importance in the 1970s and '80s with the growth of the PC.

A microprocessor chip typically contains a read-only memory (ROM)-that is, a memory that can be read repeatedly but cannot be changed-but it may also have some random-access memory (RAM) for holding transient data. Also present are a register for holding computing instructions, a register for holding the "address" of each instruction in turn, similar data registers, and a logic unit. It also has interfaces for connecting with external memories and other systems as needed.

Microprocessors are classified in terms of the number of "bits" of information that can be transferred in parallel and held in their registers. This number has been steadily increasing with the growth of circuit technology. Thus 4-bit, 8-bit, and 16-bit microprocessors are now common, and 32-bit chips have also been developed.

MIDI

Musical Instrument Digital Interface. A standard for connecting computers & musical instruments.

MIME

Multipurpose Internet Mail Extensions - a standard by which people can send each other Email messages which contain pictures, videos or sounds.

MMX

Multi Media eXtensions - a technology which is featured in a number of the latest Processors designed mainly for Multi-Media applications. To benefit form MMX the application running must have been written to take advantage of MMX technology

Modem

Modem comes from the 2 words **Mod**ulation & **Dem**odulation. A Modem converts information from Analog to Digital & vice versa. Digital Information is represented in a series of 1's & 0's. Analog information varies continuously such as a sound wave. Typical when you send an Email, your Modem converts the digital Email message to analog.

Monitor

The Monitor is used to display the images which are generated by a PC's Video Adapter.

Motherboard

The main circuit board containing the vital components of a PC such as the processor & the RAM.

Mouse

A Mouse is a common pointing device used to maximise the benefits of a Graphical User Interface. Generally a mouse has two butons which action various tasks either by a single or a double click. Windows 95 has some features which are activated via a triple click. The mouse also has a pointer on the screen which is moved by moving the mouse up or down or from side to side.

MPEG

Moving Picture Experts Group - a standard used on the World Wide Web for video & audio files - compression techniques are used which enable the files to be transmitted across the internet significantly quicker than other audio & video files. The web browser you are using must be capable of running MPEG files

Multimedia

Multimedia is the presentation of video, sound, graphics, text & animation by Software.

Multitasking

A Multitasking operating system is one which allows a PC to perform more than one task at a time. There are several types of multitasking. Different types include:-

- Context switching - Only the foreground applications utilises the processor
- Cooperative multitasking - Background tasks utilise the processor during idle times
- Time-slice multitasking - Each task utilises the processor's for a fraction of a second.

net

Part of the Domain Name which indicates that the company is an organisation which provides a network service - usually an Internet Service Provider e.g. www.enterprise.net

Netscape

A WWW Browser and the name of a company. The Netscape (trn) browser was originally based on the Mosaic program developed at the National Center for Supercomputing Applications (NCSA).

Netscape has grown in features rapidly and is widely recognized as the best and most popular web browser, Netscape corporation also produces web server software.

Netscape provided major improvements in speed and interface over other browsers, and has also engendered debate by creating new elements for the HTML language used by Web pages -- but the Netscape extensions to HTML are

not universally supported.

The main author of Netscape, Mark Andreessen, was hired away from the NCSA by Jim Clark, and they founded a company called Mosaic Communications and soon changed the name to Netscape Communications Corporation.

Network

A network is basically a series of wires & cables which connect a number of computers. Data is exchanged between computers via these cables. The maximum speed at which the data can be transmitted is called the bandwidth.

Newbie

A term used to describe somebody who is new to the internet.

News group

News groups are one of the many facilities available on the Internet. Like most of the internet, News groups are run voluntarily & co-operatively by people like you & me. A News group is centred around a discussion topic an example being rec.sport.soccer. Within these News groups several discussions or Threads take place on themes within the discussion topic. A news group devoted to the great rock guitarists may have a thread on who is the best guitarist out of Clapton, Beck & Page for instance. If you are having a problem getting something specific to work in a spreadsheet there will definitely be a news group to which you can pose your problem & it won't take long to get many responses. Unfortunately news groups appear to be the vehicle for a majority of the more undesirable topics that pollute the internet. If you see a particular News group of interest you can "subscribe" to it. Once this has been done you "post" your article & eventually it can be seen by anyone else who subscribes to the particular news group.

The categories of News groups (represented by the first 3 or 4 characters of the name followed by a "." are) :-

- rec - recreational activities
- biz - business related groups
- comp - computers including technical discussion & support
- soc - social issues
- sci - scientific discussions
- uk - groups of interest to us English, Scottish, Irish & Welsh
- alt - Alternative groups

Node

A node is any device such as a PC which is connected to a Network

Notebook

A notebook is a PC which is about the same size as a sheet of A4 paper & about 5cm thick. The term Notebooks has superseded the term laptop which generally referred to a portable PC. The original laptops were bulky & quite heavy.

Octal

The Base 8 numbering system which has a very high use in PC technology. 10 in Octal is equivalent to 8 in decimal.

OEM

Original Equipment Manufacturer is the company which actually made the computer equipment - it is quite common for one company to make the equipment & another company to sell it.

Online

To be connected to the Internet

Operating System

The Software which is responsible for running the PC, control & utilisation of the hardware & Peripherals Examples include:-

- DOS
- UNIX
- WINDOWS 95

OS

Operating System

P

Page Impression

A Page Impression occurs every time a particular web page is displayed by someone using the Internet - similar to a Hit except that a Hit is also registered when a spider or similar program accesses the web page.

Password

The password is a code known only by a user to ensure that the individual who is trying to Login to the computer is the actual person that the Userid being used belongs to.
A

Path

Any program which a user tries to execute in DOS without supplying a directory causes DOS to have to find the Directory in which the Program resides. First it tries the Current Directory, If unsuccessful it then goes through in order all the Directories specified in the PATH. The PATH is defined in AUTOEXEC.BAT

PC

PC - The Personal Computer - what this Glossary is all about. Quite Simply a computer designed to be used by one person at a time.

Pentium

The Pentium processor was introduced by Intel in 1993. PC's with this kind of processor are normally referred to as Pentiums. The speed of the Pentium Processor when it was introduced was 60MHz - this increased to 100MHz in 1994, 120MHz in 1995 & 160MHz in 1996. By Mid 1996 Processor speeds were in excess of 200MHz.

intel.

Pentium II

The Pentium II processor was introduced by Intel in the middle of 1997. The speed of the Pentium II Processor when it was introduced was around 300MHz. The Pentium II is basically the Pentium Pro incorporating MMX technology.

Pentium Pro

The Pentium Pro processor was introduced by Intel at the end of 1997. The speed of the Pentium Pro Processor when it was introduced was around 200MHz.

Peripheral

A device which can be attached to a PC & is controlled by its Processor. Examples include:-

- Printer
- Modem
- Joystick

PERL

Practical Extraction & Report Language originally developed by Larry Wall for his personal use. It is now one of the most popular Internet tools. Perl is most often met in the context of the World Wide Web where its basic function is in the manipulating of Files, text & producing Reports. The basic concepts of Hypertext Markup Language are greatly extended by being able to run ancillary programs achieved using the Common Gateway Interface (CGI). This allows programs to be called in response to actions by the Web Client user i.e. something done by use on your PC on a particular Web Page. Almost any Programming Language can be used with Perl being the Most popular. The Perl program sits in between the Web Server & other software such as Databases

PIM

Personal Information Manager - Application programs designed to help you manage your day to day affairs - features included are:-

- Diary
- List of contacts
- Notes
- Reminders

Pixel

Pixel stands for picture element.. It is the smallest element of information that programs can display or print. A picture or image is made up of thousands of pixels. A pixel is sometimes called a pel

Plug-in

A (usually small) piece of software that adds features to a larger piece of software. Common examples are plug-ins for the Netscape(& browser and web server, Adobe Photoshop(& also uses plug-ins.

The idea behind plug-in's is that a small piece of software is loaded into memory by the larger program, adding a new feature, and that users need only install the few plug-ins that they need, out of a much larger pool of possibilities. Plug-ins are usually created by people other than the publishers of the

software the plug-in works with.

POP

Post Office Protocol - standard for exchanging Email between a users PC & their Internet Access Provider.

Port

A Port is part of the PC which is used for passing data in and out of a computing device. This is normally located on the back of the PC. The port can be a Serial Port - data is sent/received one bit at a time through a cable containing a single wire, or a Parallel port where the data is sent/received through a cable containing several pieces of wire so that more than one bit at a time can be processed. Also referred to as the I/O Port.

PPP

Point to Point Protocol - Standard for using a modem & telephone line to connect to the Internet using TCP/IP.

Primary Cache

Another term for Level 1 Cache.

Processor

In the PC field the Processor & Microprocessor are synonimous. Basically it is the brain of the PC which carries out all of the low level "processing" that the PC needs to do - calculating the sum of 2 numbers is a simple example of something that the processor will do. Basically every single task that the PC performs is dependant on the processor doing its stuff.

Program

A Program is basically a series of instructions that causes the PC to do something. The Operating System such as DOS is known as a Systems Program. Application Programs such as a Word Processor or Spreadsheet perform the main tasks for which we use the PC i.e. a letter to Mum or managing the finances.

Programming Language

An artificial language through which a set of instructions can be performed by a PC. Examples are:-

- Basic
- C, C++
- Cobol
- Java
- JavaScript
- Perl
- Visual Basic

People who use programming languages to create a computer program are called programmers.

RAM

Random Access Memory is a temporary storage area which the processor uses to execute Programs & hold Data. Information is put into RAM & held there. Once the RAM becomes full information has to be removed to make space for the current task being performed. A PC with limited RAM will take a long time to perform the simplest task as the information in the RAM is constantly being replaced. RAM requires a constant electric supply to keep the information intact. Should you switch off the PC then you will lose the contents of RAM forever

Different areas of RAM include:-

- Conventional Memory
- Expanded Memory
- Extended Memory
- High Memory Area
- Upper Memory Area

Types of RAM include

- DRAM
- EDO RAM
- SDRAM

RAM Doubler

Software designed to make your RAM go further by allowing you to open more programs or handle more data within a program.

Record

Files are comprised of a number of records. Each record normally has a common set of characteristics. For example at a College a particular File may contain a record of all the students. Each record could contain Student ID, Date of Birth, Year enrolled etc.

ROM

Read Only Media. ROM chips cannot be written to. Therefore they contain information which never changes. All PC's have ROM chips. When the PC is switched on the Information in the ROM chip is used to test the RAM. ROM does not require a constant electric supply to keep the information intact. Information in ROM is retained should you switch the PC off

Root Directory

The highest point in the Directory structure at which a user can access the files. For a typical PC running DOS this is C:\.

Route

The path that data travels along moving from its starting point in a Network to its destination.

Router

A communications device which routes data between Networks.

RS232

The industry standard for the transmission of data between Serial (one bit at a time) Devices. The RS stands for Recommended Standard

Scanner

A scanner is a peripheral device which is used to transer a picture, photograph, image into a file on your PC. The image is scanned & this is converted into a format which the PC can interpret.

SCSI

Small Computer Systems Interface introduced by the American National Standards Institute (ANSI). A SCSI connects PC's to Peripherals & to other PC's & LANs. Up to 7 devices excluding the PC can be attached through a single SCSI connection, linking them together (known as a daisy chain). Only 1 device at a time can transmit through the SCSI connection - the devices are prioritised.

SDRAM

Synchronous Dynamic Random Access Memory. It is a type of RAM capable of speeds of about 55MHz. It has superceded EDO RAM.

Search Engine

One of the most essential tools on the Internet - they help you find web sites relating to a particular subject or the Email address of someone you know or articles posted to a Newsgroup or even companies which have a presence on the Internet. Most of the information provided by search engines is categorised so the search can be considerably refined before you even begin. The search engines are basically huge databases containing millions of records which include the URL of a particular Web pagealong with information relating to the content of the web page which is supplied in the HTML by the author. The search engine obtains this information via a submission from the author or by the search engines doing a "crawl" using "robot crawlers" of the internet for information.
Some search engines use Spiders to obtain information.
The are a number of facilities available on the web which allow authors to submit their web pages to hundreds of web sites at once.
Some search engines use a technique known as ICE to locate information on related topics.
The majority of the people that use this Glossary would have located it by using a Search Engine.
The most popular search engines are :-

- Alta Vista
- Excite
- Hotbot
- Galaxy
- Infoseek
- Lycos
- Webcrawler
- Yahoo

Secondary Cache

Another term for Level 2 Cache.

Shareware

Software that you can obtain for free. The author of the software does request a small fee to pay for registration, documentation etc.

Server

A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, e.g.Our mail server is down today, that's why e-mail isn't getting out. A single server machine could have several different server software packages running on it, thus providing many different servers to clients on the network.

SIMMs

Single In-line Memory Modules. Memory chips which are soldered onto plugs which slot into sockets on the Motherboard of the PC - makes fitting memory much easier than it use to be.

SIMMs come in various speeds & sizes - 1Mb, 4Mb, 16Mb & 32Mb - with speeds of 90, 80, 70 or 60 nanoseconds (60 is faster than 90).

SIMMs can either be 30-pin or 72-pin.

DIMMs, Dual In-line Memory Modules are now available. These have 168 pins in two rows

SLIP

Serial Line Internet Protocol, basically a standard which enables a user to connect to the internet using a modem & a telephone line.

Snail Mail

A term that us Email users use to describe the traditional mail or post office service. A note will take seconds to go from London to Sydney via Email but a number of days via Snail Mail.

Software

Software is basically a series of instructions that causes the PC to do something. The Operating System such as DOS is known as Systems Software. Application Programs such as a Word Processor or Spreadsheet perform the main tasks for which we use the PC i.e. a letter to Mum or managing the finances.

Spam

Basically sending Emails to people who in no way asked you to send that information - normally done in huge numbers to promote a product.

Spider

A search engine which obtains its information by starting at a specified Web Page & visitng each Web Page which has a link to it from the current page that the spider is accessing. This process continues as it moves it way through the WWW.

Spreadsheet

An Application Program where the information is stored in a grid. The spreadsheet has Rows &

Columns. A spreadsheet with 3 rows & 3 columns will have 9 "Cells" where data can be manipulated. Typically they are used for tracking expenses, budgeting etc. The content of a Cell can be based on that of other Cells & the spreadsheet program has a number of built in functions for manipulating Cells e.g. Sum, Average etc. Example Spread sheet programs include:-

- Microsoft Excel
- Lotus 123

SQL

Structured Query Language - a standard for managing, retrieving, changing & deleting records from relational databases.

Subroutine

A subroutine is part of a program which performs a specific task & can be actioned from more than one place within the program. For instance, in a windows program the programmer may write a subroutine to close the current window as this task is likely to be actioned from several different places within the program.

SVGA

Super Visual Graphics Array Video Apapter. A SVGA Monitor can display up to 1280 X 1024 pixels using over 16 million different colours.

T

T-1

T-1 is a leased line Internet connection. The speed at which data can be transmitted is 1.45 megabits per second.

T-3

T-3 is a leased line Internet connection. The speed at which data can be transmitted is 45 megabits per second.

TCP/IP

TCP/IP stands for Transmission Control Protocol/Internet Protocol & is quite simply a standard set of protocols that govern the basic workings of the Internet which was implemented in 1982.

The TCP part is all about ensuring that data is transmitted correctly between 2 computers. If any errors occur these are detected & the data is retransmitted. The data transmitted is split up into small portions called Data packets. The IP part of TCP/IP is how these data packets are moved from one point to another. Each computer on the internet has a unique IP address & the data packets are moved from the source to the destination through many different computers & this is controlled via TCP/IP. This protocol is used on the Internet & also by computers which are part of a LAN.

Telnet

Telnet is program which is part of the TCP/IP protocol. Its purpose is to allow a user to logon to a computer from a remote location.

Temporary Files

These are Files which are set up by a Program because it needs to use them when it runs. For example a spreadsheet program might want to keep a record of the last change that was made by the user to allow the change to be "undone" if required. The program may decide to keep the copy of the changes in a Temporary File. All good programs will delete Temporary Files when they are no longer required.

Terminal

A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

Terminal Server

A special purpose computer that has places to plug in many modems on one side, and a connection to a LAN or host machine on the other side. Thus the terzninal server does the work of answering the calls and passes the connections on to the appropriate node. Most terminal servers can provide PPP or SLIP services if connected to the Internet.

Text File

A common used term used to describe ASCII Text Files.

TIFF

Tagged Image File Format. One of the many different types of File Format used on PC's. This particular type is a graphics file i.e. a picture.

Toolbar

The Toolbar sits across the top or down the side of a particular Window. The toolbar allows the use to perform certain tasks such as opening a file or submitting a print. The toolbar can usually be customised so that the user can add those tasks most regularly performed

TSR

Terminate and Stay Resident These are DOS programs which sit in memory so thay can be run from within other application programs.

UNIX

A Multitasking Operating System developed in 1969. The are many variants of Unix. Written in the C Programming Language it is very portable - running on a number of different computers. Unix is the main operating system used by Internet host computers.

Upload

To copy files from your own PC to another computer via a network or using a modem. Opposite of download.

Upper Memory Area

The 384 Kilobytes of memory immediately above the 640K Conventional memory on a PC.

URL

Uniform Resource Locator - How documents on the WWW are referenced. The URL contains the protocol to be used e.g. HTTP

USENET

A world-wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the Internet, maybe half. USENET is completely decentralized, with over 10,000 discussion areas, called newsgroups.

Userid

Each user that is permitted to use a computer can be allocated an identification code which uniquely

identifies them to the computer. Normally the user will first be asked to enter this code - their userid followed by their password when they Log on to the computer. My Userid to get onto the internet is jenko.

VESA

Video Electronics Standards Association - responsible for graphics & Local Bus Standards.

VGA

Visual Graphics Array Video Apapter introduced by IBM in 1987. A VGA Monitor can display 640 X 480 pixels using 16 different colours or 320 X 200 pixels using 256 colours. These colours can be chosen from a table of up to 262,144 colours.

Video Adapter

Used to generate & send Video signals via a cable to the Monitor. The video adapter can be located on the Motherboard or in an Expansion Slot. Examples include :-

- CGA
- EGA
- VGA
- SVGA

Virtual memory

Hard Disk space on your PC which is used as if it was actual memory. Windows reserves an area of your hard disk which it uses as virtual memory.

Virus

This is a program which can damage the files on your PC - often created intentionally to do so.

Virus Scan

A program which a PC user will invoke in order to check that their PC contains no known viruses.

VMEBus

Versa Module Eurocard BUS. VMEbus is the term used to describe the established standard technology used by many systems developers/ integrators/vendors to serve user communities that require open systems architectures. It is the most utilized bus in real-time applications throughout the world. For More Information Click Here.

VRML

Virtual Reality Modelling Language is a Programming Language which has been designed to build 3D worlds on the World Wide Web. With this language a programmer can create a virtual three dimensional world which the user can explore.

WAIS

(Wide Area Information Servers) -- A commercial software package that allows the indexing of huge quantities of information, and then making those indices searchable across networks such as the Internet. A prominent feature of WAIS is that the search results are ranked (scored) according to how relevant the hits are, and that subsequent searches can find more stuff like that last batch and thus refine the search process.

WAN

Stands for Wide Area Network. Basically a linked Network of LANs. The Internet can be considered to be the largest WAN there has ever been.

Web Browser

An application program which interprets HTML & presents the final Web Page. Used to "Surf the WWW". Examples include:-

- Internet Explorer
- Netscape Navigator
- Mosaic

Web Master

The person who is responsible for looking after a particular Web Site

Web Page

An HTML document which contains information which can be seen on the Internet

Web Site

A group of Web Pages which collectively represent a company, or individual on the WWW. A group of Web pages which have been developed together to present information on a specific subject(s) is also a Web Site - This Glossary falls into that category.

Web Space

The amount of storage space that your Internet Service Provider gives you to use for your own personal web page. Normally between 2 Megabytes & 10 Megabytes.

Windows

Windows is the everyday term for Microsoft Windows which is a multitasking Graphical User Interface which runs under DOS. This user interface is made up of a number of "views" which sit on top of each other - these are the Windows. Tasks are performed by using a mouse to click an Icon, selecting an item from a menu or using the mouse to click on an item on a toolbar.

Windows 95

Microsoft's flagship Operating System introduced to the world in August 1995. The main benefit is that Windows 95 & DOS are one

Word Processor

Word Processors are Application program used mainly for creating text-based documents. Used by everyone to send letters to Mum, do the CV, newsletters, prepare business documentation, Invoices etc. Word Processors have moved on significantly over a short period of time. Nowadays one can insert pictures, check spelling automatically, change the colour of the text. This Glossary was prepared using Microsoft Word.

Examples of Word processors include:-

- Microsoft Word
- Word Perfect
- Ami Pro

WWW

The World Wide Web - The Internet facility that allows you to browse linked web pages.

WYSIWYG

Stands for What You See Is What You Get basically it means that what you can see on the screen is what you will see on paper when you print the screen contents.

ZIF Socket

The Processor in most modern PC's sits in what is called a ZIF (Zero Insertion Force) Socket. The idea is that it is easy to insert a new chip. A lever is pulled to get the chip out, plug in the new chip & throw the lever to lock it in place.

0 to 9

286

386

486

8086

8088

286

The 80286 Microprocessor was introduced by Intel in 1982. PC's with this kind of Microprocessor are normally referred to as 286 Computers.

386

The 80386 Microprocessor was introduced by Intel in 1985. PC's with this kind of Microprocessor are normally referred to as 386 Computers.

486

The 80486 Microprocessor was introduced by Intel in 1989. PC's with this kind of Microprocessor are normally referred to as 486 Computers.

8086

The 8086 Microprocessor was introduced by Intel in 1978.

8088

The 8088 Microprocessor was introduced by Intel in 1978.

COMMONLY USED CHAT ROOM AND E-MAIL ACRONYMS

Most chat rooms have no-profanity rule and some rooms have foul-language filters that screen out inappropriate language. Likewise many parents who have access to their children's e-mail accounts will not permit certain language use by their children.

For these obvious reasons, and many others, some chat room users and e-mailers use a coded language that is based on acronyms. This is a rapidly developing language and complete literacy is very difficult. The Exploited Child Unit of the National Center for Missing and Exploited Children has compiled a list of the most commonly used acronyms. This list will be updated regularly and often.

Acronym	Meaning
adr	address
afaik	As Far As I Know
afk	Away From Keyboard
aka	Also Known As
alol	Actually Laughing Out Loud
aml	All My Love
asap	As Soon As Possible
asl	Age/Sex/Location
aslmh	Age/Sex/Location/Music/Hobbies
atm	At The Moment
awol	Absent Without Leave
bak	Back At Keyboard
bbfn	Bye Bye For Now
bbl	Be Back Later
bbs	Be Back Soon
bbsl	Be Back Sooner or Later
bcnu	Be Seeing You
bfn	Bye For Now
bka	Better Known As
brb	Be Right Back
brt	Be Right There
btw	By The Way
bbiab	Be back in a bit
Bbeg	Big evil grin
bfd	Big f***ing deal
bg	Big grin
brb	Be right back
cul	See you later
cyo	See you online
cy	calm yourself
cya	See You
dl	Download
duct	Did You See That?
eg	Evil grin
emfbi	Excuse me for butting in
el	Evil Laugh
f2f	Face to Face
fawc	For Anyone Who Cares
ftf	Face To Face

Acronym	Meaning
fwiw	For What Its Worth
fya	For Your Amusement
fyi	For Your Information
fla	Four-letter acronym
fomcl	Falling off my chair laughing
fubar	F***ed up beyond all recognition
fud	Fear, Uncertainty, and Doubt
fwiw	For what it's worth
galgal	Give A Little Get A Little
gbh	Great Big Hug
gg	Good Game
ggn	Gotta Go Now
gl	Good Luck
gmta	Great Minds Think Alike
gr8	Great
g	Grin
ga	Go ahead
GOL	Giggling out loud
hih	Hope It Helps
hiliacaclo	Help I Lapsed Into A Coma And Can't Log Off
hth	Hope This Helps
iae	In Any Event
iat	I am Tired
ic	I See
icbw	I Could Be Wrong
idk	I Don't Know
igtp	I Get The Point
ihno	I have no opinion
iir	If I Recall
im	Instant Message
imao	In My Arrogant Opinion
imho	In My Humble Opinion
imo	In My Opinion
iow	In Other Words
irl	In Real Life
ianal	I am not a lawyer (but)
iirc	If I recall/remember/recollect correctly

lu or ily	I love you
mho	In my humble opinion
mnsho	In my not so humble opinion
[illegible]	I'm posting naked
ic	Just in case
jk	Just Kidding
jt	Just Teasing
k	Okay
kotc	Kiss On The Cheek
kotl	kiss on the lips
l8r	Later
lol	Laughing out loud
lmao	Laughing My A** Off
lola	Laugh Out Loud Again
lool	Laughing Outragously Out Loud
lwr	Launch When Ready
lylas (b)	love you like a sister (brother)
msg	Message
nfw	No feasible way or no f*****g way
nl	nice one
nda	Non-Disclosure Agreement
nm	Nevermind
np	No Problem
nrn	No Reply Necessary
oic	Oh, I see
otoh	On the other hand
omg	Oh My God
ooi	Out Of Interest
otoh	On The Other Hand
ousu	Oh, You Shut U
pans	Pretty awesome new stuff
pda	Public Display of Affection
pls	please
pm	Personal Message
ppl	people
pmfjib	Pardon me for jumping in but...
pots	Plain old telephone service
ql	quit laughing!
qs	Quit Scrolling
qt	cutie
rbay	right back at ya
rotfl	Rolling on the floor laughing
rotflmao	Rolling on the floor laughing my a** off
rotflbo	Rolling on the floor laughing my butt off
rtfm	Read the f***ing manual
[illegible]	S***-eating grin
sed	Said Enough Darling
sfete	Smiling From Ear To Ear
smaim	Send Me An Instant Message
somy	Sick of me yet?
snafu	Situation normal, all f***ed up
tfds	That's For Darn (Damn) Sure
Tia	Thanks In Advance
tnc or tic	tongue in cheek
ttfn	Ta-Ta for now
ttyl	Talk to you later
vbg	Very big grin
vbseg	Very big s***-eating grin
w/	with
w/b	Write Back
w/o	without
wad	Without A Doubt
wb	welcome back
wbs	Write Back Soon
weg	Wicked Evil Grin
wtg	way to go
wth	What The Heck (Hell)
wywh	Wish You Were Here
wt?	What/who the ?
wtfru	What the F***! Are You!
xm	excuse me
xme	'EXCUSE' me
xo	hugs, kisses
ygbsm	You got to be s***tin' me!
y	why
yw	Your Welcome
zzz	sleeping, bored, tired

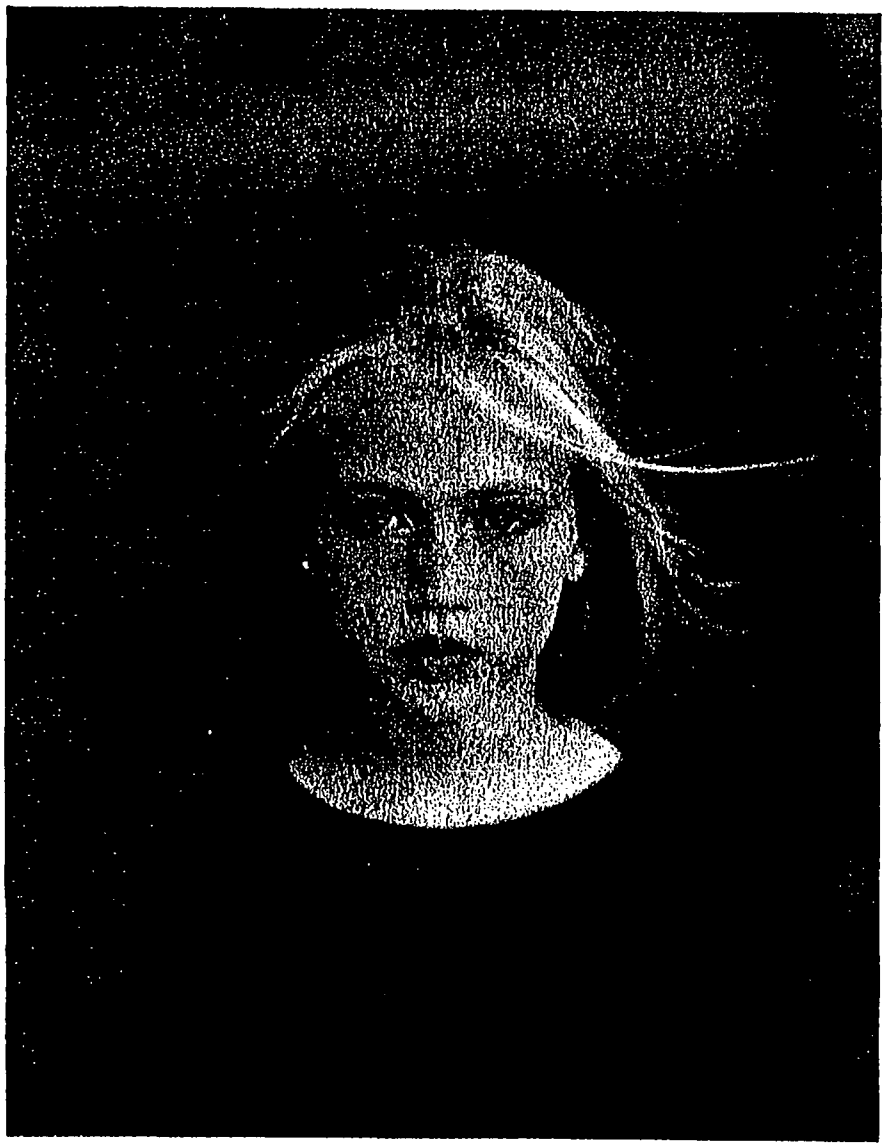
Emotional and Symbolic Acronyms

Acronym	Meaning
:-|	Ambivalent
o:-)	Angelic
>:-(	Angry
|-I	Asleep
(::()::)	Bandaide
:-{}	Blowing a Kiss
\-o	Bored
:-c	Bummed Out
|C|	Can of Coke
|P|	Can of Pepsi
:( )	Can't Stop Talking
:*)	Clowning
:'	Crying
:'-)	Crying with Joy
:'-(	Crying Sadly
:-9	Delicious, Yummy
:->	Devilish
;->	Devilish Wink
:P	Disgusted (sticking out tongue)
:*)	Drunk
:-6	Exhausted, Wiped Out

Acronym	Meaning
:(	Frown
\~/	Full Glass
_/	Glass (drink)
^5	High Five
(((((name))))	Hug (cyber hug)
(( )):**	Hugs and Kisses
:-I	Indifferent
:-#	Lips are Sealed
:~/	Mixed Up
:-O	Mouth Open (Surprised)
( )	Mug (coffee, beer)
@[_]~~	Mug of HOT Coffee or Tea
****	Popcorn
&&&&	Pretzels
@--)--)(--	Rose
:-@	Screaming
:O	Shocked
:)	Smile
^	Thumbs Up
:-&	Tongue Tied
:-\	Undecided
;)	Wink
|-O	Yawning

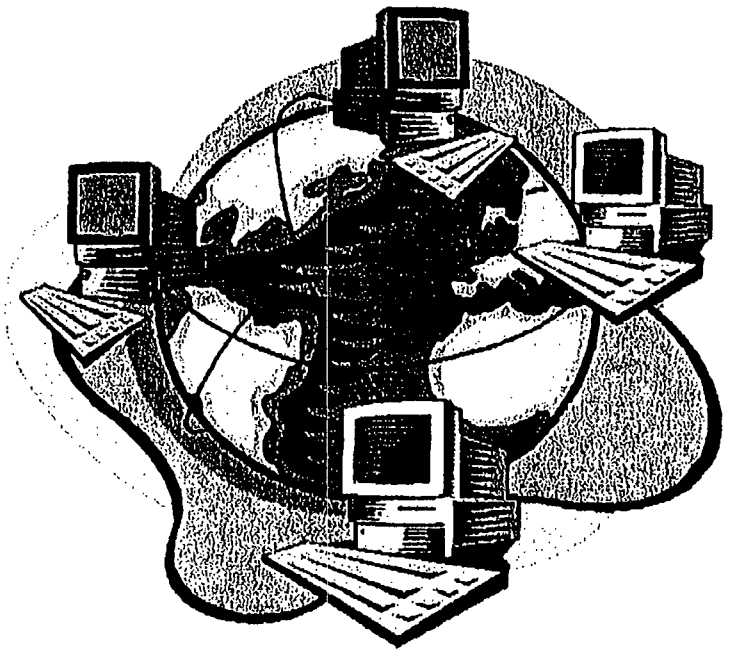
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

The Exploited Child Unit



Protecting and Empowering Our Children

THE INTERNET AND THE CYBERTIPLINE



The National Center for Missing and Exploited Children

Internet Related Reports

Your review of CyberTipline reports has or eventually will lead you to encounter the various components of the Internet. A follow-up to your first training, "Introduction to the Internet," this session will deal with applying your knowledge to your work with the CyberTipline. The topics we will discuss are as follows

- What is ftp?
- What is Listserv?
- What is Usenet and Newsgroups?
- Understanding URLs
- Understanding Email addresses
- Helper Applications & Plug-ins

ECU

Domain Names

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

Several top-level domains (TLDs) are common in the United States:

com	commercial enterprise
edu	educational institution
gov	U.S. government entity
mil	U.S. military entity
net	network access provder
org	usually nonprofit organizations

ECU

Understanding Email Addresses

Since an email address can tell you a lot about an individual, I thought it might be useful to briefly explain email addresses and free email accounts.

Email Basics

An email address has two parts: user_name@domain_name (eg. Trauch@ncmec.org)

The first part is the person's user name. That may be an abbreviated version of their name (eg. Trauch or raucht) or their name in full eg. Terry.Rauch or Terry_Rauch).

The second part is the domain name which tells the email server on which computer the recipient's email account is located. Domain names are usually made up of three parts. The computer name, the high level domain to which the computer forms a part and the country domain.

The format is: [computer_name].[domain_type].[country]

[computer_name] can be any name that the computer's administrator has registered eg. ncmec

[domain_type] will be either "com", "edu", "gov", "mil" or "org".

[country] is a two letter code for each country. eg. "au" for Australia. The only country not to have a code is the United States. Domain names in the United States do not have a [country] on the end. eg www.missingkids.com.

Types of Internet Domains

For the U.S., these are the following classes of Internet domains:

- .edu: an educational institution (ex. jhu.edu: John Hopkins University)
- .org: an organization not seen as being part of the for-profit sector (ex. ncmec.org: National Center for Missing and Exploited Children)
- .com: a commercial enterprise, including a commercial online service (ex. aol.com: America Online)
- .net: An Internet Service Provider (ISP, not really the same as a commercial online service) (ex. charm.net: Charm City's own Charm Net)
- .gov: a governmental body (ex. loc.gov: Library of Congress)
- .mil: a military body (ex. milinet.mil: interagency military network)

For the British Commonwealth countries, there are at least two domain types preceding the country code:

- .ac: an academic organization (ex. oxford.ac.uk: U. of Oxford)
- .co: A commercial organization (ex. blackwell.co.uk: Blackwell Co.)

Free Email (Anonymous Email)

This type of email account allows individuals to send anonymous correspondence all over the world, at no charge. Free email provides access to email from wherever a person is -- at home, at work, while traveling, at the local public library, or at school in the computer lab. You don't need to own a computer to use these accounts. All one needs is a web connection. The email service stores all of the email for subscribers. This is important since a considerable amount of illegal and dangerous email correspondence (child luring and photo transfers) are done by individuals using "fake" emails (anonymous email). Identifying these email accounts might help you in your work.

Large Free Email Providers

Yahoo! Mail: **trauch@yahoo.com.**
Net@ddress: **trauch@usa.net.**
Hotmail: Must use your web browser to Get/Send Mail. **trauch@hotmail.com**
MailCity: Pretty much the same as HotMail. **trauch@mailcity.com.**
Geocities: Gives an E-Mail address with a free web site. **trauch@geocities.com**
RocketMail: Free E-Mail Account. **trauch@rocketmail.com**
Bigfoot: Free E-mail Address when you become a member. **trauch@bigfoot.com**
Juno: They provide software to Get/Send Mail. **trauch@juno.com**

Other Forwarding Email Services

INDOCITIES	@indocities.com	Callsign	@callsign.com
CHURCHUSA	@churchusa.com	Populus	@populus.com
SINGPOST	@singpost.com	Dotcom	@mail.dotcom.fr
FREEYELLOW	@freeyellow.com	GMX	@gmx.net
PLANETALL	@planetall.com	Infomedia	@info-media.de
BIGFOOT	@bigfoot.com	Chez	@chez.com
BROADCAST	@broadcast.net	Cybermail	@cybermail.com
ATLINK	@atlink.com	XTEL	@free.xtel.com
UNI	@uni.de,@mailto.de	PRATOMIC	@pratomic.com
WONDER-NET	@wonder-net.com	Kitznet	@kitznet.at
GEOCITIES	@geocities.com	Onvillage	@onvillage.com
HEREMAIL	@heremail.com	Seguros	@seguros.com.br
YCLUB	@yclub.com	Visitweb	@visitweb.com
FWNB	@fwnb.com	Mailnet	@mailnet.org.uk
Beer.Com	@beer.com	Altern	@altern:org
Stones	@stones.com	Advalvas	@advalvas.be
Copacabana	@copacabana.com	Deneg	@deneg.net
Friends-café	@friends-café.com	Stealthmail	@stealthmail.com

STARMAIL(MYOWNEMAIL), NETFORWARD, FRIENDLY MAIL, INAME, THEBOYS, NETFORWARD

The short list above are email forwarding services that provide numerous domain names. You can not create your own domain name but there are hundreds - possibly thousands to choose from. These names are easily identified because they are descriptive or are statements, for instance trauch@antisocial.com. The domain names always end in ".com" and can describe or make statements about sexual acts, music, TV, movies, sports, celebrities and quotes or funny statements. Examples of such domain names are: @lover-boy.com, @cyberloveplace.com, @onecooldude.com @hehe.com, @metallicafan.com, @thepolice.com, @the-beatles.com, @lover-boy.com, @trust-me.com, @earthcorp.com, @POBoxes.com, @thepentagon.com, @theoffice.net, @writeme.com, @mindless.com, @Themarines.com, @thearmy.com, @collegemail.com, @LAOffice.com, @LondonOffice.com, @fan.theboys.com, @dallas.theboys.com, @phil-collins.com, @rednecks.com, @federalreserve.com, @smileyface.com, @most-wanted.com, @forpresident.com, @cindy-crawford.com,

Anonymous remailer

An anonymous remailer (also called an "anonymous server") is a free computer service that privatizes your e-mail. A remailer allows you to send electronic mail to a Usenet news group or to a person without the recipient knowing your name or your e-mail address.

By using an anonymous remailer, an individual can write to any email and have their true email address STRIPPED AWAY(the header at the top of your e-mail), and have it replaced with a dummy address. The Anonymous remailer or server then forwards your message to wherever you want it to go.

Currently, there are roughly a dozen active, PUBLIC remailers on the Internet. Undoubtedly, there are PRIVATE remailers that restrict who may use them.) Remailers tend to come and go. First, they require equipment and labor to set up and maintain; second, they produce zero revenue.

Nym	config@nym.alias.net
Htp	mixer@htp.org
Cracker	remailer@anon.efga.org
Redneck	config@anon.efga.org
Replay	remailer@replay.com
Squirrel	mix@squirrel.owl.de
jam	remailer@cypherpunks.ca
mix	mixmaster@remail.obscura.com
privacy	remailer@privacynb.ml.org
htuttle	h_tuttle@juno.com
grit	grit_remailer@juno.com
palnu	palnu@juno.com

tea	tea@notatla.demon.co.uk
neva	remailer@neva.org
bureau42	remailer@bureau42.ml.org

What is FTP?

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

Definition: File Transfer Protocol (FTP) is an Internet protocol which allows you to move files from one computer to another. FTP allows you to retrieve publicly accessible files on anonymous FTP servers and transfer them to your local computer account. Publicly accessible FTP servers are called anonymous servers because you log into them with the keyword anonymous.

Searching for FTP files?

Archie is the search engine of anonymous FTP sites. It is easiest to search FTP sites using Web-based Archie search engines. For an example, view the list of FTP search engines at this URL:

http://www.albany.edu/library/internet/engines.html

ECU

What is Listserv

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

Listserv discussion groups are electronic discussion groups relating to specific topics which distribute all messages sent to the list to the e-mail addresses of all the list members. Listserv itself is a software program that allows users to join groups, configure subscription options, and search the archives of previous messages.

Try these directories on the World Wide Web:

LISZT - http://www.liszt.com/
TILE.NET - http://tile.net/

ECU

What is Usenet and Newsgroups?

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

Usenet is a network of computers which exchange electronic mail tagged with predetermined headers. The mail is referred to as articles, the subjects are newsgroups. Usenet is implemented by software that downloads and uploads newsgroup mail. This software implements the Network News Transfer Protocol (NNTP). You can read Usenet articles by the use of a software program called a newsreader.

Newsgroup names begin with a group name identifier which describes the general type of newsgroup: See "Supplemental 1"

ECU

Usenet and Newsgroups Headers

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

When Usenet messages are sent, the predetermined headers are available for all members of the Usenet to see. These headers hold information about the sender, the date and the identifies which newsgroup it is going to.

Subject: Upcoming baseball season
Date: Fri, 27 Feb 1998 17:15:36 -0500
From: janedoe <janedoe@hotmail.com>
Organization: BBallRUs - Ohio
Newsgroups: alt.sports.baseball

-- OR --

Subject: Upcoming Fashion
Date: 27 Feb 1998 03:23:47 GMT
From: johndoe@aol.com (johndoe)
Organization: AOL http://www.aol.com
Newsgroups: society.style.fallfashion

ECU

Understanding URLs

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

URL stands for Uniform Resource Locator. The URL specifies the Internet address of a file stored on a host computer connected to the Internet. Every file on the Internet, no matter what its access protocol, has a unique URL. Web software programs use the URL to retrieve the file from the host computer and the directory in which it resides. This file is then displayed on the user's computer monitor.

URLs are translated into numeric addresses using the Internet Domain Name System (DNS). The numeric address is actually the "real" URL. Since numeric strings are difficult for humans to use, alphneumeric addresses are employed by end users. Once the translation is made, the Web server can send the requested page to theuser's Web browser.

ECU

Anatomy of URLs

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

This is the format of the URL:

protocol://host/path/filename

For example, this is a URL of the Preperation page of the CyberTipline

http://www.missingkids.com/cybertip/cybertipline.html

This URL is typical of addresses hosted in domains in the United States.

Structure of this URL:

1. Protocol: http
2. Host computer name: www
3. Second-level domain name: missingkids
4. Top-level domain name: com
5. Directory name: cybertip
6. File name: cybertipline.html

E C U

Domain Names

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

In addition, dozens of domain names have been assigned to identify and locate files stored on host computers in countries around the world. These are referred to as two-letter Internet country codes, and have been standardized by the International Standards Organization as ISO 3166. For example:

ch	Switzerland
de	Germany
jp	Japan
uk	United Kingdom

ECU

Email Addresses

An email address has two parts: user name@domain name (eg. Trauch@ncmec.org)

The first part is the person's user name. That may be an abbreviated version of their name (eg. Trauch or raucht) or their name in full eg. Terry.Rauch or Terry_Rauch).

The second part is the domain name which tells the email server on which computer the recipient's email account is located. Domain names are usually made up of three parts. The computer name, the high level domain to which the computer forms a part and the country domain.

The format is: [computer_name].[domain_type].[country]
See "Supplemental 2"

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

ECU

Helper Applications and Plug-ins

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

• Software programs may be configured to a Web browser in order to enhance its capabilities. When the browser encounters a sound, image or video file, it hands off the data to other programs, called helper applications, to run or display the file. Many helper applications are available for free.

• Plug-ins are software programs that extend the capabilities of a Web browser in a specific way, such as the ability to play audio files or view video movies from within Navigator. Web browsers are often standardized with a small suite of plug-ins. Additional plug-ins may be obtained at the browser's Web site, at special download sites on the Web, or from the home pages of the companies that created the programs. The number of available plug-ins is increasing rapidly. Nearly 200 plug-ins are available for downloading at the Netscape site.

ECU

Helper Applications and Plug-ins

CYBER TIPLINE
www.missingkids.com/cybertip
1-800-843-5678

• Apple's Quick Time Player downloads files with the .mov extension and displays these as "movies" in a small window on your computer screen. Quick Time files can be quite large, and it may take patience to wait for the entire movie to download into your computer before you can view it.

• The RealPlayer plug-in plays streaming audio and video files. Extensive files such as interviews, speeches and hearings work very well with the RealPlayer. The RealPlayer is also ideal for the broadcast of real-time events. These may include press conferences, live radio and television broadcasts, concerts, etc.

• Shockwave presents another multimedia experience. Shockwave allows for the creation and implementation of an entire multimedia display combining graphics, animation and sound.

ECU

Group Name	Meaning
Alt	alternative groups that are often very free in content
Bit	usually a cross-posting of a listserv discussion group
Comp	computers, computer science, software
Misc	newsgroups that don't fall into any other category
News	general news and topical subjects
Rec	recreational activities, arts, hobbies
Sci	science
Soc	social issues, socializing
Talk	debate-oriented discussions

AVAILABLE TRAINING ON SEIZING AND EXAMINING COMPUTER EVIDENCE

1. Florida Department of Law Enforcement Center for Advanced Law Enforcement Studies
   PO Box 1489
   Tallahassee FL 32302
   (904) 488-1340

2. FBI Academy
   Economic and Financial Crime Training Unit
   SA Ervin Suggs
   Quantico VA 22135
   (703) 640-1156

3. Federal Law Enforcement Training Center
   Carlton Fitzpatrick
   Building 210
   Glynco GA 31524
   (912) 267-2724

4. SEARCH
   7311 Greenhaven Drive, Suite 145
   Sacramento CA 95831
   (916) 392-2550

5. Royal Canadian Mounted Police
   Canadian Police College
   Ottawa, Ontario
   (613) 998-2541

6. IACIS
   PO Box 21688
   Keizer OR 97307-1688
   (503) 557-1506

Federal Resources on Missing and Exploited Children:

A Directory for Law Enforcement and Other Public and Private Agencies

Federal Agency Task Force for Missing and Exploited Children

U.S. Department of Defense
Family Advocacy Program
Legal Assistance Offices

U.S. Department of Education
Office of Elementary and Secondary Education
Safe and Drug-Free Schools Program

U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect

U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/
Missing and Exploited Children's Program
U.S. Immigration and Naturalization Service
U.S. National Central Bureau (INTERPOL)

U.S. Department of State
Office of Children's Issues

U.S. Department of Treasury
U.S. Customs Service
U.S. Secret Service
Forensic Services Division

U.S. Postal Service
U.S. Postal Inspection Service

National Center for Missing and Exploited Children

Federal Resources on Missing and Exploited Children:

A Directory For

Law Enforcement and Other Public and Private Agencies

Federal Agency Task Force for Missing and Exploited Children

Revised Edition - December 1997

This document was prepared by Fox Valley Technical College under Cooperative Agreement 95-MC-CX-K002 from the Office of Juvenile Justice and Delinquency Prevention of the U.S. Department of Justice.

The Office of Juvenile Justice and Delinquency Prevention is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, and the Office for Victims of Crime.

Foreword

Our children are our most important resource, and providing a safe environment for them is our most important responsibility. When a child is reported missing or victimized, our response as a society must be swift, efficient, and effective.

Faced with reduced budgets and high violent crime rates, state and local law enforcement are often unable to actively investigate missing children cases on a long-term basis. In stranger abduction cases, where victim life expectancy often can be measured in hours, local law enforcement is under incredible pressure to recover the child immediately. All missing and exploited children cases, whether short or long-term, can strain the resources of the investigating agency. Consequently, it is critical for information about Federal programs and services to be available so that local law enforcement can request them when needed.

This directory was prepared by the Federal Agency Task Force for Missing and Exploited Children and represents the Task Force's initial efforts to enhance the coordination of the delivery of Federal services to missing and exploited children and their families. Designed to provide information about Federal resources, the directory is a compilation of the many services, programs, publications, and training that address issues of child sexual exploitation, child pornography, child abductions, and missing children cases. The directory contains information ranging from access to specialized forensic resources for an abducted child case, to proactive training and prevention programs.

This second edition of the directory has been prepared to insure that the most up-to-date information is readily available and accessible to law enforcement officials as they investigate cases involving missing and exploited children. It is the Task Force's hope that child-serving professionals and law enforcement will find this publication to be a valuable supplement and that it will enhance their activities and programs for missing and exploited children.

I invite you to make use of this directory as we all work to protect our Nation's children.

Shay Bilchik
Administrator
Office of Juvenile Justice and Delinquency Prevention

Acknowledgments

Compiling a directory of this type is a labor of love. It requires the commitment, dedication, and cooperation of many agencies and many persons within those agencies. The Task Force wishes to thank the following individuals in particular, who gave their time and energy so generously to the development of the first and revised versions of the Resource Directory:

Thomas Andreotta
U.S. Immigration and Naturalization Service
U.S. Department of Justice

Gail Beaumont
Safe and Drug-Free Schools Program
U.S. Department of Education

Joe Bock
Family and Youth Services Bureau
U.S. Department of Health and Human Services

Greg Burns
U.S. Customs Service
U.S. Department of Treasury

Ray Clore
Office of Children's Issues
U.S. Department of State

Emily Cooke
National Center on Child Abuse and Neglect
U.S. Department of Health and Human Services

Richard Dusak
Forensic Services Division
U.S. Secret Service
U.S. Department of Treasury

William Hagmaier, S.S.A.
Child Abduction and Serial Killer Unit
Morgan P. Hardiman Task Force on Missing and Exploited Children
Federal Bureau of Investigation
U.S. Department of Justice

John Hargett
Forensic Services Division
U.S. Secret Service
U.S. Department of Treasury

Don Huycke, S.S.A.
U.S. Customs Service
U.S. Department of Treasury

Margie Kazdin
National Center for Missing and Exploited Children

Richard Laczynski, S.S.A.
U.S. National Central Bureau (INTERPOL)
U.S. Department of Justice

Ronald C. Laney
Missing and Exploited Children's Program
Office of Juvenile Justice and Delinquency Prevention
U.S. Department of Justice

Cynthia J. Lent
Child Abduction and Serial Killer Unit
Federal Bureau of Investigation
U.S. Department of Justice

Terry R. Lewis
Family and Youth Services Bureau
U.S. Department of Health and Human Services

David Lloyd
Family Advocacy Program
U.S. Department of Defense

Terry Lord
Child Exploitation and Obscenity Section
U.S. Department of Justice

George Martinez
Office of Crimes Against Children
Federal Bureau of Investigation
U.S. Department of Justice

Michael Medaris
Missing and Exploited Children's Program
Office of Juvenile Justice and Delinquency Prevention
U.S. Department of Justice

Carolyn O'Doherty
Violent Crimes Unit
Federal Bureau of Investigation
U.S. Department of Justice

Curtis Porter
Family and Youth Services Bureau
U.S. Department of Health and Human Services

James R. Prietsch, S.A.
U.S. National Central Bureau (INTERPOL)
U.S. Department of Justice

John Rabun
National Center for Missing and Exploited Children

Leslie Rowe
Office of Children's Issues
U.S. Department of State

Judy Schretter
Child Exploitation and Obscenity Section
U.S. Department of Justice

Jim Schuler
Office of Children's Issues
U.S. Department of State

Sue Shriner
Office for Victims of Crime
U.S. Department of Justice

Raymond C. Smith
Office of Criminal Investigations
U.S. Postal Inspection Service
U.S. Postal Service

Dan Wright, S.S.A.
Violent Crime and Fugitive Unit
Federal Bureau of Investigation
U.S. Department of Justice

Elizabeth Yore
National Center for Missing and Exploited Children

Jim York
Interpol - U.S. Central Bureau
U.S. Department of Justice

Cynthia Quinn
Interpol - Criminal Division
U.S. Department of Justice

Table of Contents

Foreword iii

Acknowledgments v

Introduction 1

Where To Get Help 3

List of Acronyms 13

Federal Agencies

- U.S. Department of Defense
  - Family Advocacy Program 17
  - Legal Assistance Offices 21
- U.S. Department of Education
  - Office of Elementary and Secondary Education
    - Safe and Drug-Free Schools Program 23
- U.S. Department of Health and Human Services
  - Family and Youth Services Bureau 27
  - National Center on Child Abuse and Neglect 33
- U.S. Department of Justice
  - Child Exploitation and Obscenity Section 35
  - Federal Bureau of Investigation 37
  - Office for Victims of Crime 43
  - Office of Juvenile Justice and Delinquency Prevention/Missing and Exploited Children's Program 47
  - U.S. Immigration and Naturalization Service 51
  - U.S. National Central Bureau (INTERPOL) 53
- U.S. Department of State
  - Office of Children's Issues 57
- U.S. Department of Treasury
  - U.S. Customs Service 61
  - U.S. Secret Service
    - Forensic Services Division 63
- U.S. Postal Service
  - U.S. Postal Inspection Service 65

Organizations

- National Center for Missing and Exploited Children 71

Appendixes

Appendix 1. Department of Defense Investigative Liaisons for Law Enforcement Agencies . . 1-1

Appendix 2. Safe and Drug-Free Schools Comprehensive Regional Centers 2-1

Appendix 3. Family and Youth Services Bureau Regional Centers 3-1

Appendix 4. Organizations Concerned With the Prevention of Child Abuse and Neglect: State Contacts 4-1

Appendix 5. FBI Field Offices 5-1

Appendix 6. FBI Legal Attaches 6-1

Appendix 7. Crime Victims Compensation/Assistance - State Agencies and Programs 7-1

Appendix 8. Interpol State Liaison Offices 8-1

Appendix 9. Office of Children's Issues Abduction and Custody Information Checklist 9-1

Appendix 10. U.S. Customs Service Field Offices 10-1

Appendix 11. U.S. Postal Inspection Service Division Boundaries 11-1

Introduction

Creation of the Federal Agency Task Force for Missing and Exploited Children was announced by Attorney General Janet Reno on May 25, 1995, at the 12th Annual Missing Children's Day. The mission of the Task Force is to coordinate Federal resources and services to effectively address the needs of missing, abducted, and exploited children and their families. The Task Force:

- Serves as an advocate for missing and exploited children and their families.
- Initiates positive change to enhance services and resources for missing and exploited children, their families, and the agencies and organizations that serve them.
- Promotes communication and cooperation among agencies and organizations at the Federal level.
- Serves as the focal point for coordination of services and resources.

The Task Force includes representatives from 16 Federal agencies and one private agency that work directly with cases involving missing, abducted, and exploited children and their families. As used in this guide, the term "missing child" refers to any youth under the age of 18 whose whereabouts are unknown to his or her legal guardian. This includes children who have been abducted or kidnaped by a family member or a nonfamily member, a child who has run away from home, a child who is a throwaway, or a child who is otherwise missing. It also includes both national and international abductions. The term "child exploitation" refers to any child under the age of 18 who has been exploited or victimized for profit or personal advantage. This includes children who are victims of pornography, prostitution, sexual tourism, and sexual abuse.

Members of the Task Force are acutely aware of the tremendous pressure placed on people who handle these types of cases on an ongoing basis. The devastating impact on the child, family, community, and practitioner; the gravity and severity of these offenses; and the overwhelming amount of time required to resolve such cases often place unfair burdens and challenges on those responsible for case investigations. Yet, when a child is missing, abducted, or victimized, an immediate and continual response is key to the successful resolution of a case.

In response to these concerns, the Task Force developed this resource manual to contribute support and to provide real solutions to practitioners when they most need them. This manual contains information on the resources, technical assistance and support, and services that are available during the investigation of cases involving missing and exploited children. The manual describes the role of each Task Force agency in the location and recovery of missing and exploited children, the types of services and support that are available, the procedures for accessing these services, and instructions for obtaining additional information. To make the information accessible, the next section, "Where To Get Help," categorizes the type of assistance offered by each agency. In addition, telephone quick reference cards can be removed and kept where most needed; addresses and phone numbers are correct as of the date of publication.

The information contained in this manual will help to expand the resources that are available, enhance services for children and their families, increase coordination of services for missing and exploited children and their families, and promote positive system change. We hope this manual provides the added tools and information practitioners need to face the many challenges that lie ahead.

The manual is from the Office of Juvenile Justice and Delinquency Prevention's (OJJDP's) Juvenile Justice Clearinghouse, P.O. Box 6000, Rockville, MD 200849-6000, 800-638-8736. The manual is also available through OJJDP's home page at http://www.ncjrs.org/pdffiles/fedredir/pdf.

Where To Get Help

Agencies that provide...

TRAINING

National Center for Missing and Exploited Children
U.S. Department of Education
Safe and Drug-Free Schools Program
U.S. Department of Health and Family Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency
Prevention/Missing and Exploited Children's Program
U.S. Immigration and Naturalization Service
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues
U.S. Department of Treasury
U.S. Customs Service
U.S. Postal Service
U.S. Postal Inspection Service

TECHNICAL ASSISTANCE

National Center for Missing and Exploited Children
U.S. Department of Defense
Family Advocacy Program
U.S. Department of Education
Safe and Drug-Free Schools Program
U.S. Department of Health and Family Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency
Prevention/Missing and Exploited Children's Program
U.S. Department of Treasury
U.S. Secret Service/Forensic Services Division
U.S. Department of State
Office of Children's Issues

LEGAL ASSISTANCE TO CHILDREN AND FAMILIES

National Center for Missing and Exploited Children
U.S. Department of Defense
Legal Assistance Offices

LITIGATION ASSISTANCE

U.S. Department of Justice
Child Exploitation and Obscenity Section

PUBLICATIONS

National Center for Missing and Exploited Children
U.S. Department of Defense
Family Advocacy Program
U.S. Department of Education
Safe and Drug-Free Schools Program
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. Department of State
Office of Children's Issues
U.S. Department of Treasury
U.S. Secret Service/Forensic Services Division

RESEARCH AND EVALUATION

U.S. Department of Education
Safe and Drug-Free Schools Program
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Federal Bureau of Investigation
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program

Agencies that provide services to...

MISSING AND EXPLOITED YOUTH AND THEIR FAMILIES

National Center for Missing and Exploited Children
U.S. Department of Defense
Family Advocacy Program
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of State
Office of Children's Issues

FEDERAL PROSECUTORS

U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues
U.S. Department of Treasury
U.S. Customs Service
U.S. Postal Service
U.S. Postal Inspection Service

STATE AND LOCAL PROSECUTORS

National Center for Missing and Exploited Children
U.S. Department of Justice
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues
U.S. Department of Treasury
U.S. Customs Service
U.S. Postal Service
U.S. Postal Inspection Service

LAW ENFORCEMENT AGENCIES

National Center for Missing and Exploited Children

U.S. Department of Defense

Family Advocacy Program

U.S. Department of Justice

Federal Bureau of Investigation

Office for Victims of Crime

Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program

U.S. Immigration and Naturalization Service

U.S. National Central Bureau (INTERPOL)

U.S. Department of State

Office of Children's Issues

U.S. Department of Treasury

U.S. Customs Service

U.S. Secret Service/Forensic Services Division

U.S. Postal Service

U.S. Postal Inspection Service

STATE AND LOCAL GOVERNMENT AGENCIES

National Center for Missing and Exploited Children

U.S. Department of Health and Family Services

National Center on Child Abuse and Neglect

U.S. Department of Justice

Federal Bureau of Investigation

Office for Victims of Crime

Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program

U.S. Department of State

Office of Children's Issues

U.S. Department of Treasury

U.S. Customs Service

U.S. Postal Service

U.S. Postal Inspection Service

NATIVE AMERICAN TRIBES

U.S. Department of Health and Family Services

National Center on Child Abuse and Neglect

U.S. Department of Justice

Federal Bureau of Investigation

Office for Victims of Crime

Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program

DIRECT SERVICE PROVIDERS AND YOUTH SERVICE AGENCIES

U.S. Department of Education
Safe and Drug-Free Schools Program
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program

NONPROFIT ORGANIZATIONS

National Center for Missing and Exploited Children
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. Department of State
Office of Children's Issues

GENERAL PUBLIC

National Center for Missing and Exploited Children
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. Department of State
Office of Children's Issues
U.S. Department of Treasury
U.S. Customs Service

Agencies that provide assistance on cases involving...

PARENTAL KIDNAPING

National Center for Missing and Exploited Children
U.S. Department of Defense
Legal Assistance Offices
U.S. Department of Justice
Federal Bureau of Investigation
U.S. Immigration and Naturalization Service
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues

RUNAWAY CHILDREN

National Center for Missing and Exploited Children
U.S. Department of Health and Human Services
Family and Youth Services Bureau
U.S. Department of Justice
U.S. National Central Bureau (INTERPOL)
U.S. Department of Treasury
U.S. Secret Service Forensic Services Division

MISSING AND EXPLOITED CHILDREN

National Center for Missing and Exploited Children
U.S. Department of Defense
Family Advocacy Program
U.S. Department of Health and Human Services
Family and Youth Services Bureau
National Center on Child Abuse and Neglect
U.S. Department of Justice
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. Immigration and Naturalization Service
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues
U.S. Department of Treasury
U.S. Customs Service
U.S. Secret Service/Forensic Services Division
U.S. Postal Service
U.S. Postal Inspection Service

CHILD SEXUAL EXPLOITATION

National Center for Missing and Exploited Children
U.S. Department of Defense
Family Advocacy Program
U.S. Department of Health and Family Services
National Center on Child Abuse and Neglect
U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. National Central Bureau (INTERPOL)
U.S. Department of Treasury
U.S. Customs Service
U.S. Secret Service/Forensic Services Division
U.S. Postal Service
U.S. Postal Inspection Service

CHILD PROSTITUTION

National Center for Missing and Exploited Children
U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
U.S. National Central Bureau (INTERPOL)

CHILD PORNOGRAPHY

National Center for Missing and Exploited Children
U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
Office of Juvenile Justice and Delinquency Prevention/ Missing and Exploited Children's Program
U.S. National Central Bureau (INTERPOL)
U.S. Department of Treasury
U.S. Customs Service
U.S. Secret Service/Forensic Services Division
U.S. Postal Service
U.S. Postal Inspection Service

SEXUAL TOURISM

National Center for Missing and Exploited Children
U.S. Department of Justice
Child Exploitation and Obscenity Section
Federal Bureau of Investigation
Office for Victims of Crime
U.S. Department of Treasury
U.S. Customs Service
U.S. Secret Service/Forensic Services Division

INTERNATIONAL ABDUCTION

National Center for Missing and Exploited Children
U.S. Department of Defense
Legal Assistance Offices
U.S. Department of Justice
Federal Bureau of Investigation
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues

INTERNATIONAL ADOPTION

U.S. Department of Justice
U.S. National Central Bureau (INTERPOL)
U.S. Department of State
Office of Children's Issues

Agencies that provide 24-hour information and referral sources to children and their families...

National Center for Missing and Exploited Children
U.S. Department of Health and Human Services
Family and Youth Services Bureau
U.S. Department of State
Consular Affairs Duty Officer (when an international abduction is in progress)

Agencies that provide compensation to crime victims...

U.S. Department of Justice
Office for Victims of Crime

Agencies that provide forensic services...

National Center for Missing and Exploited Children
U.S. Department of Justice
Federal Bureau of Investigation
U.S. Department of Treasury
U.S. Secret Service/Forensic Services Division

List of Acronyms

AFIS -- Automated Fingerprint Identification System

BCP -- Basic Center Program

CASKU -- Child Abduction and Serial Killer Unit

CCR -- Community Crisis Response

CEOS — Child Exploitation and Obscenity Section

CI -- Children's Issues

CIRG -- Critical Incident Response Group

CJA -- Children's Justice Act

DoD -- Department of Defense

FBI -- Federal Bureau of Investigation

FISH -- Forensic Information System for Handwriting

FYSB -- Family and Youth Services Bureau

JJDP — Juvenile Justice and Delinquency Prevention

NCB -- National Central Bureau

NCCAN -- National Center on Child Abuse and Neglect

NCFY -- National Clearinghouse on Families and Youth

NCIC -- National Crime Information Center

NCJRS -- National Criminal Justice Reference Service

NCMEC -- National Center for Missing and Exploited Children

OVC -- Office for Victims of Crime

OJJDP -- Office of Juvenile Justice and Delinquency Prevention

RICO -- Racketeer Influenced and Corrupt Organizations

SOP -- Street Outreach Program

TECS -- Treasury Enforcement Computer System

TLP -- Transitional Living Program

USNCB -- U.S. National Central Bureau (INTERPOL)

VICAP -- Violent Criminal Apprehension Program

VOCA -- Victims of Crime Act

FEDERAL AGENCIES

U.S. Department of Defense

Family Advocacy Program

Agency Description

The Family Advocacy Program of the Department of Defense (DoD) is designed to prevent and treat child and spouse abuse in accordance with DoD Directive 6400.1, Family Advocacy Program. DoD maintains a central registry of reports of alleged child and spouse abuse. Allegations of child sexual abuse that occur in out-of-home care settings, such as in child care centers, family day care homes, schools, or recreation programs, must also be reported within 72 hours to the Service Family Advocacy Program for inclusion in the central registry and to the DoD Assistant Secretary (Force Management Policy) or to his or her designee. Criminal prosecution is the primary goal of intervention in cases involving multiple victim child sexual abuse in an out-of-home care setting.

Services

If more than one child is a victim of sexual abuse in an out-of-home care setting, the Service may convene a multidisciplinary technical assistance team for the installation at the request of the installation commander, or the Assistant Secretary of Defense (Force Management Policy) may deploy a joint service multidisciplinary team of specially trained personnel from the four Services to provide technical assistance. Technical assistance may include law enforcement investigations, forensic medical examinations, forensic mental health examinations, and victim assistance to the child and family.

The primary recipients at the installation are the Family Advocacy Program Manager, the investigators of the installation law enforcement agency, and the physicians and mental health professionals at the military treatment facility or those who provide services under contract.

For cases involving missing and exploited children, appendix 1 lists the investigative liaisons for law enforcement agencies.

Availability of Services

Services are available to: (1) members of the Armed Services who are on active duty and their family members who are eligible for treatment in a military treatment facility, and (2) members of a reserve or National Guard component who are on active duty and their family members who are eligible for treatment in a military treatment facility.

At the request of the installation commander, a multidisciplinary team is convened by the Family Advocacy Program Manager for a particular Service. A joint Service team is deployed by the Office of the Assistant Secretary (Force Management Policy) at the request of the installation

commander. These services are directed to cases in which multiple children are victims of sexual abuse in an out-of-home care setting.

Publications

Copies of the following publications are available from the Military Family Resource Center:

- DoD Directive 6400.1, "Family Advocacy Program."
- DoD Instruction 6400.2, "Child and Spouse Abuse Report."
- DoD Instruction 6400.3, "Family Advocacy Command Assistance Team."
- DoD Directive 5525.9, "Compliance of DoD Members, Employees, and Family Members Outside the United States With Court Orders."

Publication orders should be directed to:

Military Family Resource Center
4040 N. Fairfax Drive, 4th Floor
Arlington, VA 22203-1635
Telephone: (703) 696-9053
Fax: (703) 696-9062

Agency Contact

For further information, contact the appropriate Department of Defense Family Advocacy Program Manager listed below:

Army

Army Family Advocacy Program Manager
HQDA, CFSC-FSA
Department of the Army
Hoffman #1, Room 1407
Alexandria, VA 22331-0521
Telephone: (703) 325-9390
Fax: (703) 325-5924

Navy

Director
Family Advocacy Program
BUPERS 661
Department of the Navy
Washington, DC 20370-5000
Telephone: (703) 697-6616/8/9
Fax: (703) 697-6571

Air Force

Chief
Family Advocacy Division
HQ AFMOA/SGPS
8901 18th Street, Suite 1
Brooks Air Force Base, TX 78235-5217
Telephone: (210) 536-2031
Fax: (210) 536-9032

Marine Corps

Marine Corps Family Advocacy Program Manager
Headquarters USMC
Human Resources Division (Code MHF)
Washington, DC 20380-0001
Telephone: (703) 696-2066 or 696-1188
Fax: (703) 696-1143

Defense Logistics Agency

Family Advocacy Program Manager
Quality of Life Program CAAPQ
Defense Logistics Agency
8725 John J. Kingman Road, STE 2533
Fort Belvoir, VA 22060-6221
Telephone: (703) 767-5372
Fax: (703) 767-5374

U.S. Department of Defense

Legal Assistance Offices

Agency Description

The Army, Navy, Air Force, and Marine Corps legal assistance offices serve as the point of contact for inquiries concerning the legal issues in the abduction of a child by a parent or other family member either on active duty with that Armed Service or accompanying such a Service member. They are also the point of contact for the State Department in cases of international abduction of the children of Service members.

Services

Responsibility for ensuring a Service member's compliance with child custody orders is placed with that Service member's commander. Legal assistance offices provide advice to active-duty and retired Service members and their family members on personal civil legal matters, but do not provide representation in civilian court. The legal assistance offices listed below can provide assistance in locating a Service member and will coordinate with the local legal office where that Service member is stationed. That local legal office provides legal assistance to the Service member's commander. The legal assistance offices listed below are also the points of contact for the State Department in cases of international abduction of the children of Service members.

Availability of Services

Legal advice is available to active-duty and retired Service members and their family members who are parents of children who have been abducted. In all other cases, services are limited to assistance in locating the Service member and coordinating with the local legal office or commander. Representation in civilian court is not provided. Services may be obtained directly by a parent at the Service's legal assistance agency or through the legal office where the Service member is stationed. The parent seeking assistance must have a valid court order for custody or visitation.

Publications

Copies of the following publication are available from the Military Family Resource Center:

DoD Directive 5525.9, "Compliance of DoD Members, Employees, and Family Members Outside the United States With Court Orders."

Publication orders should be directed to:

Military Family Resource Center
4040 N. Fairfax Drive, 4th Floor
Arlington, VA 22203-1635
Telephone: (703) 696-9053
Fax: (703) 696-9062

Agency Contact

For further information, contact the appropriate Department of Defense Legal Assistance Office listed below:

Army

DAJA-LA
Office of the Judge Advocate General
Room 2C463
Pentagon
Washington, DC 20310-2200
Telephone: (703) 697-3170

Air Force

AFLSA/JACA
1420 Air Force Pentagon
Washington, DC 20330-1420
Telephone: (202) 697-0413

Navy

Legal Assistance (Code 36)
Office of the Judge Advocate General
Department of the Navy
9S25 Hoffman II Building
200 Stovall Street
Alexandria, VA 22332-2400
Telephone: (703) 325-7928

Marine Corps

Legal Assistance Office
Judge Advocate Division
Headquarters, USMC
301 Henderson Hall
Southgate Road and Orme Street
Arlington, VA 22214
Telephone: (703) 614-1266

U.S. Department of Education

Office of Elementary and Secondary Education
Safe and Drug-Free Schools Program

Agency Description

The Safe and Drug-Free Schools Program supports initiatives to meet the seventh National Education Goal, which provides that by the year 2000 all schools will be free of drugs and violence and the unauthorized presence of firearms and alcohol and will offer a disciplined environment that is conducive to learning. These initiatives are designed to prevent violence in and around schools and to strengthen programs that prevent the illegal use of alcohol, tobacco, and drugs; that involve parents; and that are coordinated with related Federal, State, and community efforts and resources.

Services

Programs and activities supported by the Safe and Drug-Free Schools Program are primarily prevention efforts. The Program provides funding for formula grants to States to support local educational agencies and community-based organizations in developing and implementing programs to prevent drug use and violence among children and youth. The Program also provides funding for national leadership activities that meet identified needs and that directly support classroom teaching. Examples of such activities include:

- Development and implementation of comprehensive drug and violence prevention programs for all students from preschool through grade 12 that include health education, early intervention, pupil services, mentoring, rehabilitation referral, and related activities.
- Strategies to integrate services, such as family counseling and early intervention to prevent family dysfunction, from a variety of providers to enhance school performance and boost attachment to school and family.
- Dissemination of drug and violence prevention materials for classroom use.
- Professional training and development for school personnel, parents, law enforcement officials, and other community members.
- Support for "safe zones of passage" for students between home and school through enhanced law enforcement, neighborhood patrols, and similar measures.
- Interagency initiatives that coordinate Federal efforts to achieve safe and drug-free schools.

- Direct services to schools and school systems afflicted with especially severe drug and violence problems.

Availability of Services

Training and technical assistance for States, school districts, schools, community-based organizations, and other recipients of funds under the Improving America's Schools Act are available by contacting the appropriate Comprehensive Regional Center listed in appendix 2. Information about programs for elementary and secondary students that are provided by local schools and school districts can be obtained by contacting local Safe and Drug-Free Schools coordinators. State coordinators for Safe and Drug-Free Schools can provide information about statewide programs operated by State education agencies and governors' offices.

Publications

The publications listed below can be obtained by calling 1-800-624-0100:

Art of Prevention (1994).

Creating Safe and Drug Free Schools: An Action Guide (1996).

Drug Prevention Curricula: A Guide to Selection and Implementation (1988).

Growing Up Drug Free: A Parent's Guide to Prevention (1991).

Learning To Live Drug Free: A Curriculum Model for Prevention (1991).

Manual to Combat Truancy (1996).

Success Stories From Drug-Free Schools (1994).

What Works: Schools Without Drugs (revised 1992).

Youth and Alcohol: Selected Reports to the Surgeon General (1994).

Youth and Tobacco: Preventing Tobacco Use Among Young People, A Report of the Surgeon General (1995).

Legislative Citations

- Safe and Drug-Free Schools and Communities Act of 1994, Title IV of the Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 2701 *et seq.*).

- Gun-Free Schools Act of 1994, enacted in March 1994, reauthorized as part of the Improving America's Schools Act in October 1994.

- Pro-Children Act of 1994, enacted as part of the Goals 2000 Educate America Act, March 1994.

- Comprehensive Regional Assistance Centers program, Title XIII of the Improving America's Schools Act.

- Safe Schools Act of 1994 enacted as Title VII of the Goals 2000: Educate America Act.

Agency Contact

For further information about services, contact:

Safe and Drug-Free Schools Program
U.S. Department of Education
Portals Building
600 Independence Avenue SW.
Room 604
Washington, DC 20202-6123
Telephone: (202) 260-3954
Fax: (202) 260-7767
e-mail: http://www.ed.gov/offices/OESE/SDFS

U.S. Department of Health and Human Services

Family and Youth Services Bureau

Agency Description

The Family and Youth Services Bureau (FYSB) is an agency within the Administration on Children, Youth and Families, Administration for Children and Families. FYSB provides national leadership on youth-related issues and helps individuals and organizations to provide comprehensive services for youth in at-risk situations, as well as for their families. The primary goals of FYSB programs are to provide positive alternatives for youth, ensure their safety, and maximize their potential to take advantage of available opportunities. FYSB programs and services support locally based youth services.

Services

There are six major FYSB programs that relate to missing and exploited children: the Basic Center Program (BCP), the Transitional Living Program (TLP) for Homeless Youth, the Street Outreach Program (SOP), the National Runaway Switchboard, the National Clearinghouse on Families and Youth (NCFY), and the Runaway and Homeless Youth Training and Technical Assistance System.

Basic Center Program

FYSB's Basic Center Program supports agencies that provide crisis intervention services to runaway and homeless youth who are outside the traditional juvenile justice and law enforcement systems. The goal of the Program is to reunite youth with their families, whenever possible, or to find another suitable placement when reunification is not an option. Discretionary grants are awarded to Basic Center projects each year on a competitive basis.

There are 350 Basic Center projects across the country. More than three-quarters of these projects are operated by community-based organizations. Some of the projects are freestanding, single-purpose emergency shelters, while others are multipurpose youth service agencies. All Basic Center projects are required to provide a set of essential core services to runaway and homeless youth, including the following:

- Short- and long-term emergency shelter.
- Individual, group, and family counseling for youth and families.
- Aftercare services to stabilize and strengthen families and to ensure that additional assistance is available, if necessary.
- Recreation programs for youth.

- Linkages to other local providers for services that are not available through the Basic Center Program.

- Outreach efforts to increase awareness of available services.

Transitional Living Program for Homeless Youth

TLP helps homeless youth, ages 16 through 21, make a successful transition to self-sufficient living. The goal is to help young people avoid long-term dependency on social services. Discretionary funds are awarded to local agencies that provide youth with comprehensive services in a supervised living arrangement. The first TLP projects were funded in fiscal year 1990. To date, 86 projects have been funded.

Most local agencies operating TLP's are multipurpose youth service organizations, of which more than half also receive FYSB funds to operate temporary shelter and counseling services for runaway and homeless youth. TLP project staff provide the following services:

- Safe, supportive living accommodations in group homes, host family homes, or supervised apartments.

- Mental and physical health care.

- Education in basic living skills.

- Development of an individual transitional plan.

- Educational advancement assistance.

- Employment preparation and job placement.

Street Outreach Program for Runaway and Homeless Youth

The primary focus of the Street Outreach Program for Runaway and Homeless Youth is the establishment and building of relationships between staff of local youth service providers and street youth, with the goal of helping young people leave the streets. The local grantee programs provide a range of services directly to or through collaboration with other agencies, specifically those working to protect and treat young people who have been, or who are at risk of being, subjected to sexual abuse or exploitation. Those services include the following:

- Street-based education and counseling.

- Emergency shelter.

- Survival aid.

- Individual assessment.
- Treatment and counseling.
- Prevention and education activities.
- Information and referral.

National Runaway Switchboard

The National Runaway Switchboard is a confidential, 24-hour, toll-free hotline (1-800-621-4000) that provides assistance to runaway and homeless youth and helps them to communicate with their families and service providers. The switchboard provides the following services to at-risk youth and their families:

- Message delivery.
- Crisis intervention counseling.
- Information and referral services.

The switchboard uses a computerized national resource directory that includes more than 9,000 resources. In addition, the switchboard maintains a management information system for local switchboard staff and conducts an annual conference for local switchboard service providers.

Since early 1970 the switchboard has responded to approximately 120,000 crisis intervention calls. In 1990 the switchboard provided 7,000 referrals to youth service organizations. Through a collaborative agreement with the SONY Corporation, public service announcements are run on SONY's giant video screen in New York City's Times Square.

National Clearinghouse on Families and Youth

NCFY is a resource for communities interested in developing effective new strategies to support young people and their families. NCFY serves as a central information source on family and youth issues for youth service professionals, policymakers, and the general public. Services include:

Information Sharing. NCFY distributes information about effective program approaches, available resources, and current activities relevant to the family and youth services fields. The agency uses special mailings, maintains literature and FYSB program databases, and operates a professionally staffed information line.

Issue Forums. NCFY facilitates forums that bring together experts in the field to discuss critical issues and emerging trends and to develop strategies for improving services to families and youth.

Materials Development. NCFY produces reports on critical issues, best practices, and promising approaches in the field of family and youth services, as well as information briefs on FYSB and its programs.

Networking. NCFY supports FYSB's efforts to form collaborations with other Federal agencies, State and local governments, national organizations, and local communities to address the full range of issues facing young people and their families today.

Runaway and Homeless Youth Training and Technical Assistance System

Ten regionally based centers (see appendix 3) provide training and technical assistance to projects funded under the Basic Center Program, the Transitional Living Program, the Drug Abuse Prevention Program, and other programs serving runaway and homeless youth. Training and technical assistance are designed to enhance the skills and increase the effectiveness of youth service providers by facilitating information exchange on programmatic and operational procedures that are critical to runaway and homeless youth programs. The 10 regional centers offer onsite consultations; local, State, and regional conferences; information sharing; and skill-based training.

Availability of Services

Services provided by FYSB are directed to runaway and homeless youth and their families. To locate a service provider in your community or to secure services, contact the regional center serving your area (see appendix 3).

Publications

National Clearinghouse on Families and Youth, *Research Summary: Youth With Runaway, Throwaway, and Homeless Experiences: Prevalence, Drug Use, and Other At-Risk Behaviors* (October 1995).

National Clearinghouse on Families and Youth, *Supporting Your Adolescent: Tips for Parents* (January 1996).

Legislative Citations

The Runaway Youth Act, Title III, Juvenile Justice and Delinquency Prevention (JJDP) Act of 1974 (P.L. 93-415) focused attention on the need to develop a nonpunitive system of social services for vulnerable youth and authorized resources to support shelters for runaway and homeless youth. The 1977 Amendments to the JJDP Act (P.L. 95-115) extended services to "otherwise homeless youth" and authorized support for coordinated networks to provide training and technical assistance to runaway and homeless youth service providers (Basic Center Program). The 1980 JJDP Act Amendments (P.L. 96-509) changed the title to the Runaway and Homeless Youth Act. The Program was reauthorized through 1992 by the Anti-Drug Abuse Act of 1988

(P.L. 100-690) and was subsequently reauthorized through FY 1996 by the 1992 JJDP Act Amendments (P.L. 102-586).

The 1988 Amendments to Title III of the Juvenile Justice and Delinquency Prevention Act (P.L. 100-690) included the Transitional Living Program, which was subsequently reauthorized through 1996 by the 1992 Amendments to the JJDP Act (P.L. 102-586).

Agency Contact

For further information about services, contact any of the agencies listed below:

Family and Youth Services Bureau
U.S. Department of Health and Human Services
P.O. Box 1882
Washington, DC 20013
Telephone: (202) 205-8102
Fax: (202) 260-9333

National Clearinghouse on Families and Youth
P.O. Box 13505
Silver Spring, MD 20911-3505
Telephone: (301) 608-8098
Fax: (301) 608-8721

National Runaway Switchboard Hotline
Telephone: 1-800-621-4000

U.S. Department of Health and Human Services

National Center on Child Abuse and Neglect

Agency Description

The National Center on Child Abuse and Neglect (NCCAN), established by the Child Abuse Prevention and Treatment Act of 1974 (P.L. 93-247), is an agency within the Administration on Children, Youth and Families, Administration for Children and Families. It is the primary Federal agency with responsibility for assisting States and communities in the prevention, identification, and treatment of child abuse and neglect. The Center grants congressionally appropriated funds to States to improve and increase their prevention and intervention efforts. The Center generally coordinates Federal activities in this field.

Services

NCCAN's major activities include: three State grant programs (Basic State Grants, Children's Justice Act [CJA] grants, and Community-Based Family Resource and Support Grants); funding for research, service improvement programs and demonstration projects; the National Child Abuse and Neglect Data System (NCANDS); the National Incidence Study (NIS); the National Clearinghouse on Child Abuse and Neglect Information; and the National Resource Center for Child Maltreatment.

All of these programs relate to missing and exploited children in the sense that all victims of child abuse are exploited in some way. However, in a more specific way CJA grantees are required to improve procedures for the State's investigation and prosecution of child abuse cases, particularly child abuse and exploitation, and to improve the handling of these cases so that additional trauma to the child is limited. Also, the National Resource Center for Child Maltreatment assists States, local agencies, and tribes in developing effective and efficient child protective services (CPS) systems to handle reports of child abuse and neglect.

Availability of Services

The NCCAN Clearinghouse and Resource Center for Child Maltreatment provide information to public and private agency personnel, professionals working in related fields, and members of the general public. See appendix 4 for more information.

Publications

The NCCAN Clearinghouse maintains a complete database of up-to-date information, including all NCCAN publications, on all aspects of child abuse and neglect for professionals and members of

the general public. The Clearinghouse can provide annotated bibliographies on specific topics by request, as well as a copy of the database on CD-ROM.

The ***1997 State Statute Series*** reflects the status of the law as of December 1996. It includes six volumes of State statutes summaries organized according to the following topic areas:

Volume I:	*Reporting Laws*	*Volume IV:*	*Child Witnesses*
Volume II:	*Central Registries*	*Volume V:*	*Crimes*
Volume III:	*Investigations*	*Volume VI:*	*Permanency Planning**

*This latest volume currently includes one topic element: *Termination of Parental Rights.* Please contact the NCCAN Clearinghouse at (800) FYI-3366 for price information.

In addition to the State Statute Series, the NCCAN Clearinghouse has produced the ***1997 Statutes at a Glance Series.*** Available free of charge, this series includes 6-7 page fact sheets on the following topic areas:

Reporting Penalties (1997)
Central Registry Expungement (1997)
HIV Testing of Sex Offenders (1997)
Sex Offender Registration (1997)
Public Notification of the Release of Sex Offenders (1997)

Finally, law enforcement officials may also be interested in the most recent ***User Manuals***, which also are available free of charge:

Crisis Intervention in Child Abuse and Neglect (1995)
Treatment for Abused and Neglected Children: Infancy to Age 18 (1994)

Agency Contact

For further information about services, contact:

National Center on Child Abuse and Neglect
Administration on Children, Youth and Families
U.S. Department of Health and Human Services
P.O. Box 1182
Washington, DC 20013-1182
Telephone: (202) 205-8586
Fax: (202) 260-9351

NCCAN Clearinghouse
P.O. Box 1182
Washington, DC 20013-1182
Telephone: 1-800-FYI-3366
Fax: (703) 385-3206

U.S. Department of Justice

Child Exploitation and Obscenity Section

Agency Description

Established in 1987 and expanded in 1994, the Child Exploitation and Obscenity Section (CEOS) is a group of attorneys who have specialized in the prosecution of obscenity, child exploitation, and child abuse cases, in international child abduction, and in victim-witness issues. CEOS attorneys, who are responsible for the enforcement of Federal laws in these areas, work with Federal law enforcement agencies, other Federal agencies, and U.S. Attorneys around the country. Although CEOS will assist State and local law enforcement agencies upon request, CEOS's jurisdiction is limited to enforcement of Federal statutes; strictly intrastate cases must be handled at the local level. The CEOS chief serves as the legal advisor to the Missing and Exploited Children Task Force.

Services

- Litigation support, including assistance to U.S. Attorney's Offices; legal research; legal assistance to other Federal agencies, task forces, and committees on projects relating to child exploitation and obscenity; and policy development.
- Technical assistance.
- Training for prosecutors and investigators on topics such as interviewing skills, case preparation, and child exploitation law.

Availability of Services

Upon request, CEOS provides litigation support, technical assistance, and training to Federal investigators and prosecutors who work on child sexual exploitation cases, including child pornography, child prostitution, sexual tourism, and sexual abuse occurring on Federal lands. Services are available by contacting the local U.S. Attorney's Office or the FBI field office in the Federal judicial district where the matter arises and requesting that these offices contact CEOS by telephone and/or by writing, and if no response is forthcoming, contacting CEOS directly at the address below.

Legislative Citations

- 18 U.S.C. § 228 Child support.
- 18 U.S.C. § 1204 International parental child kidnaping.

- 18 U.S.C. § 2241 *et seq.* Sexual abuse.
- 18 U.S.C. § 2251 *et seq.* Sexual exploitation and other abuse of children.
- 18 U.S.C. § 2421 *et seq.* Transportation for illegal sexual activity (Mann Act).
- 18 U.S.C. § 3509 Child victims' and witnesses' rights.
- 42 U.S.C. § 5776a Morgan P. Hardiman Task Force on Missing and Exploited Children.

Agency Contact

For further information about services, contact:

Child Exploitation and Obscenity Section
Criminal Division
U.S. Department of Justice
1331 F Street NW.
6th Floor
Washington, DC 20530
Telephone: (202) 514-5780
Fax: (202) 514-1793

U.S. Department of Justice

Federal Bureau of Investigation

Agency Description

The Federal Bureau of Investigation (FBI) exercises its jurisdiction and investigative responsibilities pursuant to Federal statutes addressing various crimes against children including kidnaping and sexual exploitation. Federal law defines children as minors under the age of 18, often referred to as "children of tender years." FBI investigations involving crimes against children generally include violations of Federal statutes relating to child abuse, sexual exploitation of children, interstate transportation of obscene material, computer pornography, interstate transportation of children for sexual activity, parental kidnaping, and violations of the Child Support Recovery Act. In some instances, the RICO (Racketeer Influenced and Corrupt Organizations) statute also may apply. While some of those Federal violations may not necessarily involve the sexual abuse or sexual exploitation of children, such as violations of the International Parental Kidnaping Act, the FBI pursues any child victimization offense within its lawful jurisdiction, often coordinating those investigations with other Federal, State, and local agencies.

Cases related to the sexual abuse and exploitation of children and other crimes against children are given high priority within the FBI. All available and necessary FBI resources are used during these investigations, and each case is aggressively prosecuted. Nonfamily abductions, often referred to as stranger abductions, receive immediate attention. Particular attention is also given to investigations involving organized criminal activity, commercialized child prostitution, and the manufacture and distribution of child pornography. The transmission and exchange of child pornography through computer bulletin boards are aggressively investigated as an insidious form of child sexual exploitation.

The FBI also investigates allegations of sexual assault in Indian country, including the investigation of child abuse and the sexual exploitation of children. The FBI addresses these sensitive investigations by participating with other professionals in a multidisciplinary team approach that enlists the expertise of investigators, social workers, clinical psychologists, victim-witness coordinators, and Federal prosecutors.

Services

Investigative Services and Support

FBI Headquarters. On January 20, 1997, a new unit and two new offices were established within the Violent Crime and Major Offenders Section, Criminal Investigations Division, at FBI Headquarters. These entities, the Office of Crimes Against Children (OCAC) and the Office of Indian Country Investigations (OICI), are managed within the Special Investigations and Initiatives Unit (SIIU), and became operational during March 1997. Staffed by Supervisory Special Agents

and support professionals, these entities were established to specifically focus on crimes against children and crimes in Indian country. The OCAC addresses all crimes under the FBI's jurisdiction that in any way involve the victimization of children, providing program management and field wide investigative oversight of those critical FBI operations. Likewise, the OICI addresses crimes in Indian country, providing program management and investigative oversight of those sensitive FBI operations. The SIIU, OCAC, and OICI work closely with FBI field offices, other FBI components, and various other entities to provide and coordinate operational support to more effectively address crimes against children.

FBI Field Offices. Individual FBI field offices throughout the country serve as the primary point of contact for persons requesting FBI assistance. Special agents assigned as Crimes Against Children Coordinators use all available resources--including investigative, forensic, tactical, informational, and behavioral science--in the investigation of crimes against children. The special agents coordinate their investigations with appropriate local law enforcement agencies, as well as with Federal or State prosecutors. Upon receiving notification that a child has been abducted, FBI Evidence Response Team personnel may be assigned immediately to conduct the forensic investigation of the abduction site and any other appropriate areas, while other special agents typically join law enforcement personnel in coordinating and conducting the comprehensive neighborhood investigation that is vital to the resolution of these cases. A Rapid Start Team may also be deployed immediately to begin the overwhelming task of coordinating and tracking the investigative leads, which often number in the thousands during protracted child abduction investigations. Special Agents will also coordinate child abduction investigations with the National Center for Missing and Exploited Children (NCMEC) and other entities to make full use of all available resources.

Child Abduction and Serial Killer Unit. The Child Abduction and Serial Killer Unit (CASKU) is a rapid response element of the FBI's Critical Incident Response Group (CIRG). The unit has primary responsibility for providing investigative support through profiling, violent crime analysis, technical and forensic resource coordination, and application of the most current expertise available in matters involving the abduction or mysterious disappearance of children and serial murder. (Serial murder involves the killing of two or more victims in separate incidents).

Child abductions are among the most difficult crimes to resolve and require immediate dedication of significant resources. A specialized CASKU staff provides operational assistance to Federal, State, and local law enforcement agencies involved in these important investigations. The unit responds immediately to requests and provides onsite assistance as appropriate. CASKU services include:

- Profiles of unknown offenders.
- Crime analysis.
- Investigative strategies.

- Interview and interrogation strategies.
- Behavioral assessments.
- Trial preparation and prosecutive strategy.
- Expert testimony.
- Coordination of other resources, including FBI Evidence Response Teams and FBI laboratory services.

Case consultations may include any or all of the services listed above. Services are provided by telephone, in writing, or in person. In some cases investigators may travel to Quantico for consultation sessions, or CASKU members may be sent to the area of the crimes.

CASKU can also assist in coordinating the deployment of Rapid Start, a computerized major case management support system. CASKU maintains a close working relationship with NCMEC and can help to arrange the use of their resources, such as poster distribution and age enhancement of photographs.

Another CIRG component, the Violent Criminal Apprehension Program (VICAP), works closely with CASKU and provides automated support. To assist investigators working on cases, VICAP analysts perform standard and ad hoc searches of their databases, as well as other law enforcement databases. The VICAP database contains reports submitted by participating law enforcement agencies concerning certain violent crimes, which can be used to analyze and link multiple cases.

In addition to case consultation services, CASKU conducts research regarding child abduction and serial murder in an effort to develop further understanding of the crimes and criminals. Results of research are applied to cases and shared with the criminal justice community through publications and training.

Morgan P. Hardiman Task Force on Missing and Exploited Children. Created by the Violent Crime Control and Law Enforcement Act of 1994, the Morgan P. Hardiman Task Force on Missing and Exploited Children coordinates Federal law enforcement resources to assist State and local authorities in investigating the most difficult cases of missing and exploited children. The Task Force is composed of at least two members from each of seven Federal agencies: Bureau of Alcohol, Tobacco, and Firearms; Drug Enforcement Administration; FBI; U.S. Customs Service; U.S. Marshals Service; U.S. Postal Inspection Service; and U.S. Secret Service. As legislated by Congress, the FBI manages the Task Force, which is co-located with CASKU and therefore works closely with that unit. The unit chief of CASKU also serves as chief of the Task Force.

FBI Forensic and Technical Support Services

CASKU was created to centralize services in child abduction and serial homicide cases. In addition to providing investigative consultation, CASKU can coordinate the application of all FBI headquarters resources needed in particular cases.

The FBI laboratory is the only full-service Federal forensic science laboratory serving the law enforcement community. The FBI is mandated by Title 28, CFR Section 0.85, to conduct scientific examinations of evidence, free of charge, for any duly constituted law enforcement agency in the United States. Assistance is provided through:

- Evidence response teams.
- Document services.
- Latent fingerprint services.
- Scientific analysis services (including chemistry-toxicology, DNA analysis/serology examinations, explosives, firearms-toolmarks, hairs and fibers, and materials analysis).
- Special projects (including graphic design, photographic processing, special photographic services, structural design, and visual production and video enhancement).
- Forensic science research and training.

Detailed information about these services, including instructions for collecting, preserving, and shipping evidence, can be found in the *Handbook of Forensic Science*, which is available from the Government Printing Office. The FBI's Rapid Start Team, developed since the *Handbook* was last revised, provides onsite information management services to support the handling of crisis situations. The team is capable of operating in a bivouac environment, bringing with them all equipment required.

The Special Techniques Program, established in 1993, is another part of the Information Resources Division/Engineering Section. This group uses geophysical methodology and other remote sensing equipment to search for clandestinely concealed evidence. These techniques are considered as an investigative tool only after more expedient measures have been exhausted.

Criminal Justice Information Services. Criminal justice information services provided by the FBI include a fingerprint repository and the National Crime Information Center (NCIC).

- **Fingerprint repository**. The FBI serves as the Nation's civil and criminal fingerprint repository and responds to the information needs of Federal, State, local, and international members of the criminal justice community. The FBI receives more than 34,000 fingerprint cards each day.

- **National Crime Information Center**. NCIC is a nationwide computer-based inquiry and response information system that was established in 1967 to serve the criminal justice community. NCIC's purpose is to maintain a computerized filing system of accurate, timely, documented criminal justice information that is readily available through a telecommunications network. An average of 1.3 million inquiry-response transactions per day are processed through more than 100,000 NCIC terminals.

The *Handbook of Forensic Science* describes technical services of the Criminal Justice Information Services Division and the Information Resources Division of the FBI.

Training

The FBI offers an extensive training program for the law enforcement community. Training in a broad spectrum of topics is offered to bona fide law enforcement personnel in settings throughout the United States, around the world, and at the FBI Academy. Each FBI field office has a training coordinator. International requests for training can be made through the FBI Legal Attaches at American Embassies.

Victim-Witness Assistance

Each FBI field office has a victim-witness coordinator. The FBI's Victim-Witness Assistance Program operates on a referral basis for victims of Federal violations.

Availability of Services

Recipients of FBI services include law enforcement agencies and the U.S. Government (hence the citizens of the United States). Services can be accessed by a request from a law enforcement agency, either through the Child Abduction and Serial Killer Unit or through the local FBI field office or Legal Attache (see appendix 5 and 6 for a list of these offices and attaches).

Legislative Citations

FBI investigations involving child victimization are based upon violations of Federal statutes, including the crime of kidnaping (Title 18, U.S. Code, Sections 1201 and 1202); International Parental Kidnaping Act (Title 18, U.S. Code, Section 1024); Unlawful Flight to Avoid Prosecution (UFAP) - Parental Kidnaping (Title 18, U.S. Code, Section 1073); crimes committed in Indian country (Title 18, U.S. Code, Section 1153); child sexual abuse (Title 18, U.S. Code, Sections 2241, 2242, 2243, and 2244); sexual exploitation of children (Sections 2251, 2251A, 2252, and 2258); interstate transportation of obscene material (Sections 1462, 1465, and 1466); interstate transportation of children for sexual activity (Sections 2421, 2422, 2423, and 2424); Child Support Recovery Act (Title 18, U.S. Code, Section 228); and in some instances the RICO statute (Title 18, U.S. Code, Section 1961).

Agency Contact

For further information about services or to request immediate FBI assistance, contact one of the local FBI field offices, which are listed in appendix 5 and in local telephone directories, or contact one of the units listed below:

FBI Headquarters
Special Investigations and Initiatives Unit
Office of Crimes Against Children
Office of Indian Country Investigations
935 Pennsylvania Avenue NW.
Washington, DC 20535-0001
Telephone: (202) 324-3666
Fax: (202) 324-2731

Child Abduction and Serial Killer Unit
Federal Bureau of Investigation
Quantico, VA 22135
Telephone: (540) 720-4700
Fax: (540) 720-4790

Morgan P. Hardiman Task Force on Missing and Exploited Children
Federal Bureau of Investigation
Quantico, VA 22135
Telephone: (540) 720-4760
Fax: (540) 720-4792

U.S. Department of Justice

Office for Victims of Crime

Agency Description

The mission of the Office for Victims of Crime (OVC) is to enhance the Nation's capacity to assist crime victims and to provide leadership in order to change attitudes and practices to promote justice and healing for all victims of crime. OVC administers the Crime Victims Fund (hereafter called the Fund), which was authorized by the Victims of Crime Act of 1984 (VOCA). Financing for the Fund comes from criminal fines, forfeited bail bonds, penalty fees, and special assessments collected by U.S. Attorneys, U.S. Courts, and the Federal Bureau of Prisons.

Each year OVC makes awards to State crime victim assistance and compensation programs to supplement State funding for victim services. In addition, OVC provides victim assistance training and technical assistance for criminal justice officials and direct service providers. Exploited children, families of missing and exploited children, practitioners who provide direct services to victim families, and law enforcement personnel who investigate and prosecute such cases are eligible to participate in OVC-sponsored programs.

Services

Crime Victim Compensation

Crime victim compensation is the direct payment to a crime victim or to his or her family to help cover crime-related expenses such as medical treatment, mental health counseling, lost wages, or funeral services. Every State administers a crime victim compensation program. Most of these programs have similar eligibility requirements and offer a comparable range of benefits. Most programs require victims to report crimes to the police in a timely manner and to file claims within a fixed period of time.

Each year OVC uses VOCA funds to supplement State resources. States receive a grant based on 40 percent of the amount of compensation benefits made by the State in a previous year.

Crime Victim Assistance

Crime victim assistance programs provide direct services such as crisis intervention, counseling, emergency transportation to court, temporary housing, and criminal justice support and advocacy. All States receive VOCA victim assistance grant funds, which are then awarded by the States to community-based public and nonprofit organizations that serve crime victims, such as domestic violence shelters, child abuse treatment programs, victim service units in law enforcement agencies and prosecutor's offices, hospitals, and social service agencies. Each State receives a base amount of $500,000, plus a percentage of the amount remaining in the Fund based on population.

Training and Technical Assistance

OVC's Trainers Bureau seeks to improve services to crime victims by providing training and technical assistance to the programs and agencies that serve crime victims. The Trainers Bureau helps Federal, State, and local agencies address training, administrative, and programmatic issues.

Community Crisis Response Program

OVC's Community Crisis Response (CCR) program seeks to improve services to communities that have experienced crimes involving multiple victimizations. The program provides rapid response and limited technical assistance to victim service agencies; Federal, State, and local criminal justice agencies; U.S. Attorney's Offices; Native American tribes; and other agencies that assist crime victims.

Information Dissemination

OVC's Resource Center provides victim-related information to criminal justice practitioners, researchers, policymakers, and crime victims. The OVC Resource Center collects, maintains, and disseminates information on national, State, and local victim-related organizations and on State programs that receive funds authorized by VOCA. The OVC Resource Center is a component of the National Criminal Justice Reference Service (NCJRS), the world's largest criminal justice information clearinghouse.

Availability of Services

OVC services are directed to:

- Missing and exploited children and their families.
- Victims of child pornography.
- Victims of sexual tourism.
- Parents of abducted children.
- Federal, State, and local criminal justice officials and other professionals who handle cases of missing and exploited children.
- Members of the general public who have an interest in child-victim information.

State crime victim compensation applications can be obtained from the appropriate State program. A list of agencies responsible for the administration of crime victims compensation in each State can be found in appendix 7.

Crime Victim Assistance

OVC provides funding to over 2,500 State crime victim assistance programs. A list of local crime victim assistance programs is available from each State VOCA victim assistance administrator (see appendix 7).

Training and Technical Assistance

Programs and agencies can access OVC's Trainers Bureau by submitting a request on agency letterhead that: (1) describes the problem to be addressed and explains why it cannot be funded with existing resources, (2) provides information about the individuals to be trained, (3) estimates the number of hours of training or the number of days of technical assistance needed, (4) details the expected outcome of the assistance, and (5) indicates what special skills or knowledge are required of the trainer or assistance provider. If the request is approved for funding, OVC will match trainers and/or technical assistance providers to the request. For additional information, write to the Trainers Bureau at the OVC address below or call (202) 307-5983.

Community Crisis Response (CCR) Program

Agencies and communities can access OVC's CCR program by submitting a request on agency letterhead that: (1) contains a statement of facts concerning the situation, (2) enumerates the number of victims and describes the impact of the crime on the community, (3) explains why existing resources are inadequate, (4) describes the type of technical assistance requested and the desired outcome, and, if known, (5) lists any special skills required by the consultants. If approved, onsite assistance usually will be short-term, generally from 1 to 3 days. For additional information, write to the CCR program at the OVC address below or call (202) 307-5983.

Information Dissemination

The OVC Resource Center can be accessed through its toll-free number (1-800-627-6872). A list of publications and other information is available.

OVC has initiated an interactive homepage on the Internet -- http://www.ojp.usdoj.gov/ovc/. The new website enables victims, victims advocates, and others interested in victims' rights to obtain information about available services on a state-by-state basis. OVC website visitors can also obtain information about available funding and training and technical assistance opportunities.

Publications

A complete list of OVC publications is available from the OVC Resource Center (1-800-627-6872).

Child Sexual Exploitation: Improving Investigations and Protecting Victims (1995), NCJ 153527.

Crime Victim Compensation: A Good Place to Start (1996, Video, 9.2 minutes), NCJ 162359.

Agency Contact

For further information about services, contact:

Office for Victims of Crime
U.S. Department of Justice
810 7th Street NW.
Washington, DC 20531
Telephone: (202) 307-5983
Fax: (202) 514-6383
Gopher to: ncjrs.aspensys.com
World Wide Web: http://www.ojp.usdoj.gov/ovc/

U.S. Department of Justice

Office of Juvenile Justice and Delinquency Prevention
Missing and Exploited Children's Program

Agency Description

The Juvenile Justice and Delinquency Prevention (JJDP) Act of 1974 (P.L. 93-415), as amended by the Missing Children's Assistance Act of 1984, establishes the Missing and Exploited Children's Program in the Office of Juvenile Justice and Delinquency Prevention (OJJDP). The purpose of the Missing Children's Assistance Act is to develop leadership and provide funding support to address the needs of the Nation's missing and exploited children and their families and to foster coordination of programs and services for this population.

The Missing and Exploited Children's Program conducts research, demonstration, and service programs pertaining to missing and exploited children; provides training and technical assistance; and coordinates various activities. In addition, the Missing and Exploited Children's Program supports the National Center for Missing and Exploited Children, the national resource center and clearinghouse dedicated to missing and exploited children issues.

Since 1984, the Missing Children's Assistance Act has provided for research, training, and technical assistance to support local law enforcement efforts to locate and recover missing children. Each year the Missing and Exploited Children's Program trains more than 3,500 law enforcement officials in the investigation of missing children cases, at no cost to State or local governments.

Services

- Training and technical assistance.
- Demonstration programs.
- Research projects.
- Evaluation studies.
- Publications.
- Funding for the National Center for Missing and Exploited Children.
- Support for nonprofit organizations that work with missing and exploited children.
- Coordination of the Federal Agency Task Force for Missing and Exploited Children.

Availability of Services

Training and technical assistance is available to State and local units of government, nonprofit organizations, and other agencies serving missing and exploited children. Research briefs and other publications are available to the general public. Some materials are restricted to law enforcement personnel.

Training Programs

The following training programs are sponsored by the Missing and Exploited Children's Program. These courses are designed to assist law enforcement officers and other professionals who handle child abuse and exploitation cases.

Responding to Missing and Abducted Children. The aim of this course is to enhance the knowledge and skills of law enforcement officials who investigate cases involving abducted, runaway, and other missing youth.

Child Sexual Exploitation Investigations. This course provides law enforcement officials and other professionals with the knowledge and information they need to understand, recognize, investigate, and resolve cases of child pornography and sexual exploitation.

Child Abuse and Exploitation Investigative Techniques. This course is designed to enhance the skills of experienced law enforcement officials and other professionals who investigate cases involving child abuse, sexual exploitation of children, child pornography, and missing children.

Missing and Exploited Children Comprehensive Action Program (M/CAP). M/CAP is a training and technical assistance program that emphasizes community-wide, interagency collaboration and self-assessment, information sharing, and comprehensive case management to address the needs of and respond to missing and exploited children and their families.

Child Abuse and Exploitation Team Investigative Process. This course focuses on the development of a community interagency protocol that is unique to jurisdictions implementing a collaborative investigative process for child abuse cases.

Publications

The following documents are available from the Missing and Exploited Children's Program. Publications with an NCJ number are also available from the National Criminal Justice Reference Service (1-800-851-3420).

America's Missing and Exploited Children: Their Safety and Their Future (1986), NCJ 100581.

Charging Parental Kidnaping (American Prosecutor's Research Institute, 1995).

Child Sexual Exploitation: Improving Investigations and Protecting Victims - A Blueprint for Action (Education Development Center, Inc., 1995)

Hiring the Right People: Guidelines for the Screening and Selection of Youth-Serving Professionals and Volunteers (Missing and Exploited Children Comprehensive Action Program/Public Administration Service and the National School Safety Center, 1994).

Investigation and Prosecution of Child Abuse, second edition (American Prosecutors Research Institute, 1993).

Law Enforcement Policies and Practices Regarding Missing Children and Homeless Youth (Research Triangle Institute, 1993) NCJ 145644.

Missing, Abducted, Runaway, and Thrownaway Children in America, First Report: Numbers and Characteristics. National Incidence Studies (Full Report and Executive Summary) (1990), NCJ 123668.

Missing and Abducted Children: A Law Enforcement Guide to Case Investigation and Program Management (National Center for Missing and Exploited Children, 1994), NCJ 151268.

National Center for Missing and Exploited Children (OJJDP Fact Sheet, 1995).

Obstacles to the Recovery and Return of Parentally Abducted Children (American Bar Association, 1993), NCJ 144535.

Obstacles to the Recovery and Return of Parentally Abducted Children: Research Summary (American Bar Association, 1994), NCJ 143458.

Parental Kidnaping (OJJDP Fact Sheet, 1995).

Parental Kidnaping, Domestic Violence, and Child Abuse: Changing Legal Responses to Related Violence (American Prosecutor's Research Institute, 1995).

Portable Guides to Investigating Child Abuse: An Overview (Office of Juvenile Justice and Delinquency Prevention, 1997), NCJ 165153.

Sharing Information: A Guide to the Family Educational Rights and Privacy Act (1997).

Using Agency Records To Find Missing Children: A Guide for Law Enforcement (1995), NCJ 154633.

Videos

"Conducting Sensitive Child Abuse Investigations" is a six series video that was produced in 1996 by the Missing and Exploited Children's Program in conjunction with the National Child Welfare Resource Center, Edmund S. Muskie Institute of Public Affairs, University of Southern Maine.

Agency Contact

For further information about services, contact:

Missing and Exploited Children's Program
Office of Juvenile Justice and Delinquency Prevention
810 7th Street, NW.
Washington, DC 20531
Telephone: (202) 616-3637
Fax: (202) 307-2819

U.S. Immigration and Naturalization Service

Agency Description

The Inspections Program of the U.S. Immigration and Naturalization Service (INS) controls and guards the boundaries and borders of the United States at designated Ports-of-Entry (POEs) against the illegal entry of aliens to protect the health, welfare, safety, and security of the public and the nation. Under authority granted by the Immigration and Nationality Act (INA), as amended, an immigration inspector may question any person coming into the United States to determine his or her admissibility. In addition, an inspector has authority to search without warrant the person and effects of any person seeking admission, if there is reason to believe that grounds of exclusion exist which may be disclosed by such search. The INA is based on the law of presumption - an applicant for admission is presumed to be an alien until he or she shows evidence of citizenship, and an alien is presumed to be an immigrant until he or she proves that he or she fits into one of the nonimmigrant classifications.

Persons seeking entry into the United States are inspected at POEs by Immigration Inspectors who determine their admissibility. Inspectors are responsible for determining the nationality and identity of each applicant for admission. United States citizens are automatically admitted on verification of citizenship. Aliens' documents are reviewed to determine admissibility based on the requirements of the U.S. immigration law. Because of this unique status, the Immigration Inspector is usually the first U.S. official encountered by travelers who seek to enter the United States. Within this context, the INS is ideally situated to assist in preventing the movement of missing children across U.S. borders.

Services

Services provided by the INS include:

- Training for common carriers to improve ability of personnel to identify missing or exploited children.
- Interdiction of missing children at United States Ports-of-Entry, when encountered.
- Information dissemination to the public.

Availability of Services

Services available from the INS are directed to law enforcement officials and selected travel industry personnel. Services can be obtained by contacting the INS Office of Inspections.

Agency Contact

For further information about services, contact:

U.S. Immigration and Naturalization Service
Office of Inspections (HQINS)
425 I Street NW
Washington, DC 20536
Telephone: (202) 514-3019
Fax: (202) 514-8345
After Hours: (202) 616-5000 (INS Command Center, 7 x 24)

U.S. National Central Bureau (INTERPOL)

Agency Description

INTERPOL is the international criminal police organization that comprises designated national central bureaus (NCB's) from the law enforcement agencies of its 177 member nations. The primary mission of INTERPOL is:

(a) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the 'Universal Declaration of Human Rights.'

(b) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

By law, INTERPOL is forbidden to undertake any intervention or activities of a political, military, religious, or racial character.

INTERPOL maintains a sophisticated global communications network to coordinate international criminal investigations among its member countries. This network is also used to relay humanitarian requests, such as missing person inquiries. INTERPOL provides a forum for discussions, organizes working group meetings, and stages symposia for law enforcement authorities of member nations to focus attention on specific areas of criminal activity affecting their countries.

Services

Each INTERPOL member country establishes, funds, and staffs a national central bureau, which serves as the point of contact for the international law enforcement community. Every NCB operates within the parameters of its own nation's law and policies and within the framework of the INTERPOL constitution. In the U.S., authority for the INTERPOL function rests with the Attorney General. Authority for administering the U.S. National Central Bureau (USNCB) is shared by the Departments of Justice and Treasury.

The mission of USNCB is twofold:

- To receive foreign requests for criminal investigative assistance and direct them to the appropriate U.S. Federal, State, or local law enforcement or judicial authorities.

- To receive domestic law enforcement requests and direct them to the appropriate NCB abroad.

The USNCB's coordinative services provide Federal, State, and local law enforcement authorities with the most effective means available to secure the assistance of foreign police in matters ranging from a criminal record check to the arrest and extradition of wanted persons.

The USNCB investigative staff includes senior agents who are detailed from more than 16 Federal and State law enforcement agencies and a permanent analytical staff. Agents and analysts work in five investigative divisions: alien/fugitive, criminal, drugs, financial fraud and economic crimes, and State liaison. Cases involving the exploitation of minors are assigned to one of these divisions, depending on the nature of the offense. For example, the Fraud Division investigates sexual abuse against minors, sexual assault against minors, child pornography, and sexual tourism. The Criminal Division is responsible for cases involving missing persons, parental kidnaping, and child abduction.

Through INTERPOL's worldwide telecommunications network, messages can be directed to one country, to an entire region, or to the whole INTERPOL membership. Messages destined for regional or worldwide distribution are referred to as "diffusions." Diffusions inform other NCB's of the circumstances of a case and request their assistance or intervention.

If information is not obtained from other NCB's as a result of a diffusion message, the originating agency can request that a formal notice be issued for worldwide distribution through the INTERPOL Secretariat General Office. INTERPOL notices are categorized (color-coded) according to the circumstances surrounding the request.

- International Red Notices request a subject's provisional arrest with a view toward extradition. A Red Notice provides specific details concerning charges against a subject, along with warrant information, and includes prior criminal history.

- International Blue Notices are designed to collect information about persons. For example, to trace and locate a subject whose extradition may be requested.

- International Yellow Notices are circulated to provide information about persons who are missing, abducted or who are unable to identify themselves, such as children.

Upon receipt of these notices, most member countries enter the information into their databases and border lookout systems.

Availability of Services

Requests for Assistance

To reach the international law enforcement community, USNCB enters information on the child-related crime, subject, victim, abducting parent, or missing child(ren) into the INTERPOL network. Requests can be made immediately following the incident, but they must be made by a U.S. law enforcement agency or judicial authority (see appendix 8 for a listing of USNCB - State Liaison offices). The USNCB **cannot** accept requests for assistance from members of the public, including a victim parent.

Virtually every request normally handled through law enforcement channels can be accommodated by INTERPOL, provided communication is needed within the international law enforcement community. Generally, correspondents on INTERPOL messages are the law enforcement authorities in the respective member countries.

Responses to inquiries are sent to the originating law enforcement agency. Interested parties, such as a victim parent, can ask for a status report directly from the originating law enforcement agency.

When a request is received, a USNCB analyst will search the internal case tracking system to determine if there is any prior correspondence regarding the principals in the investigation. Additional searches will be conducted on a wide range of internal and external computer databases to determine if there are any records that will disclose prior investigative information or if there is any information that will help to locate a missing or abducted child and/or the abducting parent.

A determination is then made as to what action should follow, and a message is usually sent to one or more foreign NCB's through the INTERPOL communications network by the agent or analyst. Because local customs, policies, and laws dictate what the receiving NCB can and will do, USNCB has little or no control over how a message will be handled by a foreign NCB. Most requests from U.S. police entail interviewing witnesses, victims, or subjects of child exploitation crimes who reside in foreign countries or concern efforts to locate missing or abducted children and/or abductors.

Domestic Child Abduction Cases

In domestic child abduction cases, the initial request seeks to confirm if border-entry records can establish the presence of the abductor or the child in the foreign country. Once entry has been established, discreet verification is requested to confirm the exact location of the abductor in the hope of preventing that person from fleeing to another location.

If an NCB confirms the location of an offender, abductor, or child, USNCB notifies the originating police agency, which then coordinates subsequent investigative or retrieval efforts with the prosecuting attorney or the victim parent via the Department of State, Office of Children's Issues. If USNCB messages fail to locate an offender, abductor, or child, USNCB helps the originating

agency complete the application process that will lead to the publication of INTERPOL international notices.

If a child is located abroad. INTERPOL may request protective custody of the child, even in countries that are party to the Hague Convention treaty.

If a subject is charged with a child exploitation offense or parental kidnaping, a request for provisional arrest with a view toward extradition must be sent first through the proper diplomatic channels. Cases resulting in extradition are handled by the Department of Justice's Office of International Affairs, which uses the INTERPOL channel to transmit information pertaining to the extradition process.

Foreign Requests for Assistance

Foreign requests for investigative assistance are handled similarly to domestic cases. USNCB agents or analysts query various law enforcement databases--including the NCIC--to determine whether prior investigative information exists in the United States. The investigative request is then forwarded to the appropriate Federal or State police authority and, oftentimes, is coordinated with NCMEC. The results of such investigative actions are then routed back to USNCB for relay to the requesting country. If another NCB requests such action, USNCB can initiate a border-lookout notice using the Treasury Enforcement Communications System (TECS) database. Such a notice would request that INTERPOL be notified if the subject and/or missing/abducted child(ren) were to attempt to enter the United States.

In foreign origin abduction cases, the names of the abductor and of the child cannot be entered into the NCIC computer system unless a Red Notice has been issued for the abductor and a Yellow Notice for the child. In some cases USNCB can enter the victim child's name into NCIC without the existence of a Yellow Notice, but all efforts to locate the child must have been exhausted previously, and the request for such entries must be made by the National Center for Missing and Exploited Children.

Agency Contact

For further information about services, contact:

U.S. National Central Bureau (INTERPOL)
U.S. Department of Justice
Bicentennial Building Room 600
600 E Street NW.
Washington, DC 20530
Telephone: (202) 616-9000
Fax: (202) 616-8400
NLETS: DCINTER00

U.S. Department of State

Office of Children's Issues

Agency Description

The Office of Children's Issues (CI) is located in the Overseas Citizens Services, Bureau of Consular Affairs, U.S. Department of State. CI formulates, develops, and coordinates policies and programs and provides direction to foreign service posts on international parental child abduction and international adoption. CI also fulfills U.S. treaty obligations relating to international parental abduction of children.

Services

The Office of Children's Issues provides services in two areas: international parental child abduction and international adoption.

International Abduction

CI works closely with parents, attorneys, private organizations, and government agencies in the United States and abroad to prevent and resolve international parental child abductions. Since the late 1970's, the Bureau of Consular Affairs has taken action in more than 8,000 cases of international parental child abduction. In addition, the Office has answered thousands of inquiries concerning international child abduction, enforcement of visitation rights, and abduction prevention techniques.

CI acts as the U.S. Central Authority for the operation and implementation of the Hague Convention on the Civil Aspects of International Child Abduction. Forty-seven countries, including the United States, have joined the Hague Abduction Convention. The Convention discourages abduction as a means of resolving a custody matter by requiring, with a few limited exceptions, that the abducted child be returned to the country where he or she resided prior to the abduction. About 60 percent of applications for assistance under the Hague Abduction Convention involve children abducted from the United States and taken to other countries, and 40 percent involve children who were abducted in other countries and brought to the United States. The countries with the most abduction cases are, in descending order, Mexico, United Kingdom, Canada, Germany, and France. These five countries account for about half of the abduction cases in which CI becomes involved.

Many countries have not yet accepted the Hague Convention. In 1996 CI handled the cases of more than 250 children who were abducted to non-Hague countries. In the event of an abduction to a non-Hague country, one option for the left-behind parent is to obtain legal assistance in the country where the child was taken and to follow the local judicial process. Of non-Hague countries, the

largest number of cases have involved children taken to Egypt, Japan, Jordan, the Philippines, and Saudi Arabia.

For international abduction cases, CI can:

- Provide information in situations where the Hague Convention applies and help parents file an application with foreign authorities to obtain the return of or access to the child.
- Contact U.S. Embassies and consulates abroad and request that a U.S. Consul Officer attempt to locate, visit, and report on a child's general welfare.
- Provide the left-behind parent with information on the legal system, especially concerning family law, of the country to which the child was abducted and furnish a list of attorneys willing to accept American clients.
- Monitor judicial or administrative proceedings overseas.
- Help parents contact local officials in foreign countries or make contact with such officials on the parent's behalf.
- Inform parents of domestic remedies, such as warrants, extradition procedures, and U.S. passport revocations.
- Alert foreign authorities to any evidence of child abuse or neglect.

CI cannot re-abduct a child, help a parent in any way that violates the laws of another country, or give refuge to a parent who is involved in re-abduction. CI also cannot act as a lawyer, represent parents in court, or pay legal expenses or court fees.

International Adoption

CI offers general information and assistance regarding the adoption process in more than 60 countries. In 1996 U.S. citizens adopted more than 11,000 foreign-born children. Because adoption is a private legal matter within the judicial sovereignty of the Nation where the child resides, the Department of State cannot intervene on behalf of an individual U.S. citizen in foreign courts.

For international child adoption cases, CI can:

- Provide general information about international adoption in countries around the world.
- Provide general information on U.S. visa requirements for international adoptions.
- Make inquiries regarding the status of specific adoption cases and clarify documentation and other requirements to the U.S. consulate abroad.

- Make efforts to ensure that U.S. citizens are not discriminated against by foreign authorities or court personnel.

CI cannot become directly involved in the adoption process in another country, cannot act as an attorney or represent adoptive parents in court, and cannot order that an adoption take place or that a visa be issued.

Availability of Services

International Abduction

In cases involving international abduction, services are directed to the parents or the attorneys of children who have been abducted internationally or to those who fear a child may be abducted by another parent abroad. CI promotes the use of civil legal mechanisms to resolve international parental abduction cases. CI also works closely with local and Federal law enforcement agencies, the Department of Justice, and the Department of State Advisors Office, all of which pursue criminal remedies to international parental abduction cases.

General information on international parental child abduction and custody issues is available to any interested person. As the U.S. Central Authority for the Hague Convention on the Civil Aspects of International Child Abduction, CI processes applications from parents seeking access to and the return of abducted children under the Convention. CI coordinates U.S. government assistance in cases involving children abducted abroad. CI works closely with U.S. Embassies and Consulates, and foreign Hague Convention Central Authorities to help resolve international parental child abduction cases. The International Child Remedies Act (52 U.S.C. 11601; P.L. 100-300; 22 CFR Part 94) is the Federal legislation implementing the Hague Abduction Convention in the United States. A Memorandum of Understanding signed by the Departments of State and Justice and by the National Center for Missing and Exploited Children gives NCMEC the authority to process Hague abduction cases involving children taken to the United States.

Although the Convention does not require that requests for services be in the form of an application, CI has created a special form (DSP-105), "Application for Assistance Under the Hague Convention on Child Abduction," to help organize information (see appendix 9). It should be noted that CI does not adjudicate the validity of the application claim for the return of or access to a child; rather, CI provides information on the operation of the treaty and on the issues that the appropriate judicial or administrative body that reviews the application will consider in making a determination.

International Adoption

International adoption services provided by CI are directed to parents seeking to adopt abroad, to agencies involved in international adoption, and to U.S. Embassies or consulates abroad that provide information on the local adoption situation and that issue visas to children to enter the United States. Most services are accessed when a parent calls CI or uses the automated information

system. Any individual, agency, or group wanting information on international adoption may contact CI to obtain information.

Under guidance from CI, Embassies and consulates monitor and report changes in local adoption procedures that may affect U.S. citizens wishing to adopt abroad. The Embassies also inform other governments of the effect that their laws, regulations, and procedures have on Americans who wish to adopt a child who resides in that country.

Agency Contact

For further information about services, contact:

Office of Children's Issues
Room 4811
Overseas Citizens Services
Bureau of Consular Affairs
U.S. Department of State
Washington, DC 20520-4818
Telephone: (202) 736-7000
Fax: (202) 647-2835
Autofax: (202) 647-3000
Consular Affairs Electronic Bulletin Board: (202) 647-9225 (modem number)
Internet Address: http://travel.state.gov

U.S. Department of Treasury

U.S. Customs Service

Agency Description

The U.S. Customs Service is on the frontline of the Nation's defense against the illegal importation and trafficking of child pornography. Long recognized by both the domestic and international law enforcement communities for its knowledge of and skill in the area of child pornography investigations, the U.S. Customs Service aggressively targets importers, distributors, and purveyors of child pornography to prevent the sexual exploitation and abuse of children both in the United States and abroad. The U.S. Customs Service Child Pornography Enforcement Program works closely with the FBI, the Department of Justice's Child Exploitation and Obscenity Section, the U.S. Postal Inspection Service, and the National Center for Missing and Exploited Children.

Through an agreement with NCMEC, the U.S. Customs Service Child Pornography Enforcement Program has assumed primary responsibility for all NCMEC child pornography-related complaints. NCMEC has established a national toll-free child pornography Tipline (1-800-THE LOST, or 1-800-843-5678) for the reporting of information regarding child pornography. NCMEC refers such data directly to the Child Pornography Enforcement Program for dissemination to the appropriate field offices.

Services

- Training for law enforcement officers who are involved in child pornography investigations.
- Investigative support for child pornography investigations.
- Information dissemination to the public.

Availability of Services

Services available through the U.S. Customs Service are directed to law enforcement officials, investigators, and parents involved in cases of child pornography. Services can be accessed by contacting the nearest Customs Service office (see appendix 10).

A training course curriculum is available through the training center in Atlanta, Georgia. All training courses are coordinated through local Customs Service offices (see appendix 10).

Agency Contact

For further information about services, contact:

U.S. Customs Service
International Child Pornography Investigation and Coordination Center
45365 Vintage Park Road, Suite 250
Sterling, VA 20166
Telephone: (703) 709-9700, ext. 353
Fax: (703) 709-8286

U.S. Department of Treasury

U.S. Secret Service
Forensic Services Division

Agency Description

Under Title XXXI of the Violent Crime Control and Law Enforcement Act of 1994, the U.S. Secret Service is mandated to work with the National Center for Missing and Exploited Children to provide forensic and technical assistance to State and local authorities in investigating the most difficult cases of missing and exploited children.

Services

Services provided by the U.S. Secret Service include access to the following:

- The Forensic Information System for Handwriting (FISH) database, which allows handwritten or handprinted material to be searched against previously recorded writings, making possible links or consolidations.
- The Automated Fingerprint Identification System (AFIS), a nationwide network with access to the largest collection of automated fingerprint databases in the United States.
- Polygraph examinations, to help detect deception through physiological means, resulting in investigative leads.
- Visual information services, such as image enhancement, age progression and regression, suspect drawings, video and audio enhancement, and graphic and photographic support.

Availability of Services

Services are directed to local, State, and Federal law enforcement investigators who deal with cases involving missing children, runaways, parental abductions, international abductions, sexual tourism, and child pornography. Services are available at the discretion of the investigating agency when a missing or exploited child case is involved.

Publications

Publications include two brochures: the *Forensic Services Division* brochure, and the *U.S. Secret Service, Forensic Services Division, National Center for Missing and Exploited Children* brochure.

Agency Contact

Further information about services may be obtained from any local Secret Service field office or from:

U.S. Secret Service
Forensic Services Division
1800 G Street NW.
Suite 929
Washington, DC 20223
Telephone: (202) 435-5926
Fax: (202) 435-5603

National Center for Missing and Exploited Children
2101 Wilson Boulevard
Suite 550
Arlington, VA 22201-3052
Hotline: 1-800-THE-LOST (1-800-843-5678)
Telephone: (703) 235-3900
Fax: (703) 235-4067

U.S. Postal Inspection Service

Agency Description

The U.S. Postal Inspection Service is the law enforcement arm of the U.S. Postal Service with responsibility for investigating crimes involving the U.S. mail, including all child pornography and child sexual exploitation offenses. Specially trained postal inspectors are assigned to each of the 28 field divisions nationwide (see appendix 11). As Federal law enforcement agents, U.S. postal inspectors carry firearms, serve warrants and subpoenas, and possess the power of arrest.

Recognizing that child molesters and child pornographers often seek to communicate with one another through what they perceive as the security and anonymity provided by the U.S. mail, postal inspectors have been involved extensively in child sexual exploitation and pornography investigations since 1977. Since the Federal Child Protection Act of 1984 was enacted, postal inspectors have conducted more than 2,800 child pornography investigations, resulting in the arrest and conviction of more than 2,500 child pornographers and preferential child molesters.

Services

Postal inspectors in the United States use an established, nationwide network of intelligence to implement a wide variety of undercover programs designed to identify suspects and develop prosecutable cases. These undercover operations recognize the clandestine nature of their targets and the inherent need of many offenders to validate their behavior. The techniques used in these programs include placement of contact advertisements in both local and national publications, written contacts and correspondence with the subject, and more recently, contact via computer networks and the Internet. Postal inspectors are ready to assist in any related investigation involving child sexual exploitation.

Availability of Services

Investigative assistance by the Postal Inspection Service is available and should be sought under the following circumstances:

- When a subject may be using the U.S. mail to exchange, send, receive, buy, loan, advertise, solicit, or sell child pornography.
- When a subject is believed to be using the U.S. mail to correspond with others concerning child sexual exploitation, child pornography, or child erotica.

- When a subject is believed to be using a computer network or bulletin board to exchange child pornography or child erotica or to correspond with others concerning child sexual exploitation, and the actual exchange or initial contact may involve the U.S. mail.

- When a subject is believed to be clearly predisposed to receive or purchase child pornography and a reverse sting investigative approach appears warranted.

- When there is a need to execute a controlled delivery of child pornography.

- When the activities of a subject warrant further investigation and there is a need for assistance from a postal inspector who is trained in the investigation of child pornography or child sexual exploitation cases.

- When other local investigative leads have been exhausted and a postal inspector is needed to utilize additional resources.

Services and investigative assistance provided by the Postal Inspection Service are available to any local, State, or Federal law enforcement agency. Contact the nearest office of the U.S. Postal Inspection Service for further information.

Legislative Citations

For over a century, the Postal Inspection Service has had specific responsibility for investigating the mailing of obscene matter (Title 18 U.S. Code, Section 1461). While over the years child pornography has been, as a matter of course, investigated along with obscenity matters, increased public concern resulted in the enactment of the Sexual Exploitation of Children Act of 1977 (Title 18 U.S. Code, Section 2251-2253). The Child Protection Act of 1984 (18 U.S.C. 2251-2255) amended the 1977 Act by:

- Eliminating the obscenity requirement.

- Eliminating the commercial transaction requirement.

- Changing the definition of a minor from a person under age 16 to one under age 18.

- Adding provisions for criminal and civil forfeiture.

- Amending the Federal wiretap statute to include the Child Protection Act.

- Raising the potential maximum fines from $10,000 to $100,000 for an individual and to $250,000 for an organization.

On November 7, 1986, Congress enacted the Child Sexual Abuse and Pornography Act (18 U.S.C. 2251-2256), which amended the two previous acts by:

- Banning the production and use of advertisements for child pornography.

- Adding a provision for civil remedies of personal injuries suffered by a minor who is a victim.

- Raising the minimum sentence for repeat offenders from imprisonment of not less than 2 years to imprisonment of not less than 5 years.

On November 18, 1988, Congress enacted the Child Protection and Obscenity Enforcement Act (18 U.S.C. 2251-2256), which:

- Made it unlawful to use a computer to transmit advertisements for or visual depictions of child pornography.

- Prohibited the buying, selling, or otherwise obtaining temporary custody or control of children for the purpose of producing child pornography.

On November 29, 1990, Congress amended 18 U.S.C. 2252, making it a Federal crime to possess three or more depictions of child pornography that were mailed or shipped in interstate or foreign commerce or that were produced using materials that were mailed or shipped by any means, including by computer.

Most recently, a new criminal statute was enacted with the passage of the Telecommunications Act of 1996. Title 18 U.S.C. 2422 makes it a Federal crime for anyone using the mail, interstate or foreign commerce, to persuade, induce, or entice any individual under the age of 18 years to engage in any sexual act for which the person may be criminally prosecuted.

Agency Contact

For further information about the U.S. Postal Inspection Service, contact:

U.S. Postal Inspection Service
Office of Criminal Investigations
475 L'Enfant Plaza West SW.
Room 3141
Washington, DC 20260-2166
Telephone: (202) 268-4286
Fax: (202) 268-4563

ORGANIZATIONS

National Center for Missing and Exploited Children

Agency Description

The mission of the National Center for Missing and Exploited Children (NCMEC) is to assist in the location and recovery of missing children and to prevent the abduction, molestation, sexual exploitation, and victimization of children. A private, nonprofit organization established in 1984, NCMEC operates under a congressional mandate in a cooperative agreement with the Department of Justice's Office of Juvenile Justice and Delinquency Prevention. The goal is to coordinate the efforts of law enforcement personnel, social service agency staff, elected officials, judges, prosecutors, educators, and members of the public and private sectors to break the cycle of violence that historically has perpetuated crimes against children.

Services

NCMEC offers a variety of services to aid in the search for a missing child, including a toll-free hotline; technical case assistance; a national computer network; photograph and poster distribution; age-enhancement, facial reconstruction, and imaging-identification services; a resource directory of nonprofit organizations; recovery assistance; and international case assistance.

Toll-Free Hotline

One of NCMEC's primary activities is its toll-free hotline: 1-800-THE-LOST (1-800-843-5678). The multilingual hotline, which is available throughout the United States, Canada, and Mexico, operates every day of the year, 24 hours a day. It is used by individuals to report the location of a missing child or of other children whose whereabouts are unknown to the child's legal custodian and to learn about the procedures necessary to reunite a child with the child's legal custodian. Reports of missing children are entered immediately into a national missing child database. Reports of sightings of missing children are disseminated directly to the investigative agency handling the case.

Technical Case Assistance

Trained case managers assist citizens and law enforcement officials in filing missing person reports, verify data concerning missing children that have been entered into the FBI's NCIC computer system, and send publications designed to enhance the investigative skills of agency personnel involved in missing child cases.

National Computer Network and Online Services

NCMEC is linked via computer online services to 50 State clearinghouses plus the District of Columbia, the U.S. Department of State Office of Children's Issues, the U.S. National Central Bureau (INTERPOL), the U.S. Secret Service Forensic Services Division, and other Federal

agencies. Internationally, NCMEC is linked to the Australian Police, the Belgium Police, the Netherlands Police, the Royal Canadian Mounted Police, New Scotland Yard, Mexican government contacts, and others. These computer links allow images of and information on missing and exploited children to be transmitted instantly.

In addition, NCMEC has taken the search for missing children to the Internet with the creation of the Missing Children Web Page. This free, publicly available channel allows Internet users to search a database for information on current missing children cases, to view images of missing children, and to obtain safety and resource information. The NCMEC Missing Children Web Page can be found at http://www.missingkids.com.

Photograph and Poster Distribution

NCMEC maintains an up-to-date library of missing children posters on the Internet, CompuServe, and the State Clearinghouse bulletin-board computer network. The organization also places missing child kiosks in high-traffic areas, such as airports and shopping malls. NCMEC simultaneously transmits posters and other case-related information to more than 9,000 law-enforcement agencies throughout the Nation through a broadcast fax dissemination service. NCMEC coordinates national media exposure of missing children cases, including public service announcements for breaking cases. Through a network of private-sector partners that includes major corporations, television networks, and publishers, NCMEC has distributed millions of photographs of missing children.

Age-Enhancement, Facial Reconstruction, and Imaging-Identification Services

Supported by forensic specialists and computer industry leaders, NCMEC provides computerized age-progression of photographs of long-term missing children, reconstructs facial images from morgue photographs of unidentified deceased individuals, provides assistance in the creation of artist composites, and trains forensic artists in imaging applications and techniques.

Resource Directory of Nonprofit Organizations

NCMEC maintains a list of nonprofit organizations located throughout the United States, Canada, and Europe that provide direct services (as stipulated by the Missing Children's Assistance Act) to families of missing and exploited children. This directory is provided as a public service to individuals who are looking for a resource group to help with a missing or exploited child case.

Recovery Assistance

Through NCMEC, several corporations provide lodging and transportation to custodial parents who are recovering their missing children. This service is available to parents or guardians who cannot afford such expenses themselves, provided that established criteria and guidelines are met. To find out if a particular case meets these criteria, call the NCMEC hotline.

International Case Assistance

NCMEC acts on behalf of the U.S. Central Authority in the handling of applications seeking the return of or access to children abducted in the United States. This assistance is provided in compliance with the Hague Convention of the Civil Aspects of International Child Abduction. NCMEC also handles outgoing international abductions.

CyberTipline

Through support from the U.S. congress, NCMEC operates a Federally-mandated CyberTipline aimed at reducing crimes against children occurring on the Internet. Families are encouraged to call its national tollfree hotline at 1-800-843-5678 to report incidences involving child sexual exploitation including online enticement of children for sexual acts; information on the possession, manufacture, or distribution of child pornography; child prostitution; and child-sex tourism. Leads received are immediately forwarded directly to the U.S. Customs Service's Child Pornography Enforcement Program, the U.S. Postal Inspection Service, and the U.S. Department of Justice's Federal Bureau of Investigation. Additionally, online users can report information on the same topics via the Internet. For more information, visit the CyberTipline section of NCMEC's web site at www.missingkids.com/cybertip.

Exploited Child Unit (ECU)

The ECU was created to combat child molestation, pornography and prostitution and raise awareness about child exploitation both nationally and internationally. The ECU seeks to generate leads in cases of child exploitation and forward them to the appropriate investigative agencies; provide technical assistance in these cases to State and local law enforcement; develop tools and resources to assist in the investigation of these cases; and increase awareness about the problem of child exploitation among law enforcement and the general public.

Funding for the ECU is provided by the U.S. Department of the Treasury. Additional partners in this effort include the U.S. Department of Justice and the U.S. Postal Service.

Jimmy Ryce Law Enforcement Training Center

NCMEC, OJJDP, and the FBI have established the Jimmy Ryce Law Enforcement Training Center, housed at NCMEC. Named for a 9-year old boy abducted and murdered out of South Florida, this training and technical assistance program is designed to enhance the investigative response to missing children cases. The Training Center provides training to senior-level law enforcement officers and is broken down into three areas: a two-day intensive seminar for law enforcement officers that focuses on research and policy issues; a five-day regional training that emphasizes investigative resources for local law enforcement working these cases; and two-day training for State control terminal officers on the new National Crime Information Center flagging system that immediately alert NCMEC and the FBI to highly endangered cases.

In addition, the following services are available to law enforcement agencies:

- **Informational Analysis Services**. NCMEC receives thousands of leads and provides law enforcement officials with the most usable, relevant information possible. NCMEC prioritizes its leads and identifies similar patterns in cases across the country, helping to tie cases together and coordinate investigations.

- **Queries and Database Searches**. Through its networked database, NCMEC can search active missing child cases using any series of identifiers. NCMEC also has access to a number of national informational databases, including employment records, motor vehicle records, telephone listings, school registrations, and the Federal Parent Locator Service.

- **Project ALERT (America's Law Enforcement Retiree Team)**. Fourteen national law enforcement associations work with NCMEC to provide free onsite assistance by volunteer retired police officers. This project allows hardpressed local police involved in difficult missing or exploited child cases to benefit from the expertise of the retired officers.

Working closely with crime prevention officers, NCMEC reaches out to the general public with positive, effective child-safety information and services, including:

KIDS AND COMPANY: Together for Safety, a state-of-the-art personal safety curriculum for children in kindergarten through grade six.

Project KidCare, a campaign to ensure that parents have a current photograph as well as descriptive information of their child. A list of safety tips is included in the passport-like booklet.

Kidprint, a program through which families can obtain a free videotape of their child.

Availability of Services

Services provided by NCMEC are directed to:

- Parents and families of missing and exploited children.

- Local, State, and Federal law enforcement investigators and agencies handling cases of missing and exploited children.

- Child care staff, child protection and social service personnel, criminal justice professionals, and legal practitioners who work with missing and exploited children and their families.

- Nonprofit organizations that seek access to a national network of resources and information.

- Members of the general public who have an interest in child safety.

Services are provided for:

- Cases of missing children, including endangered runaways; victims of family and nonfamily abduction; and those who have been lost, injured, or are otherwise missing.
- Reports of sightings of missing children.
- Other cases handled by law enforcement agencies that involve the victimization and possible exploitation of children.
- Reports of child exploitation and child pornography.

For **parents** of missing children, cases are taken in through the hotline when it has been determined that: (1) the child was younger than 18 years of age at the time of disappearance, (2) a missing child report has been filed with the police, and (3) the parent reporting the case has court-awarded custody of the child, unless otherwise noted. These cases include:

- **Voluntary missing (runaway) cases**, which can be taken immediately by NCMEC when the child is 13 or younger or when specific conditions indicate that the child is endangered, such as the existence of a life-threatening medical condition, a serious mental illness, a substance abuse problem, or a belief that the child is with a potentially dangerous individual or in a potentially dangerous situation.
- **Family abduction cases**, which are taken by NCMEC when it is determined that the parent reporting the case has court-awarded custody of the child and that the child's whereabouts are unknown.
- **International family abduction cases**, which are taken by NCMEC when it is believed that the child has been taken out of or brought into the United States and when the child's whereabouts are unknown, or when a child has been brought into the United States and the left-behind parent has made appropriate applications to invoke the Hague Convention on the Civil Aspects of International Child Abduction.
- **Nonfamily abduction cases**, which may involve kidnaping by a stranger or by an acquaintance.
- **Other cases**, in which the facts are insufficient to determine the cause of a child's disappearance. The criteria for intake of a "lost, injured, or otherwise missing" child are the same as for a nonfamily abduction.

For **law enforcement professionals**, requests for resources, technical assistance, and access to NCMEC's database may be obtained by contacting NCMEC's hotline or case management department. All services are free of charge.

For **callers reporting a sighting** of a missing child, the NCMEC hotline will obtain complete information concerning the individual involved and the circumstances surrounding the sighting. A report will be distributed to law enforcement officials.

For **callers reporting specific information concerning child pornography**, the NCMEC hotline also serves as the National Child Pornography Tipline. Reports of alleged child sexual exploitation, including child pornography and prostitution, are forwarded to the U.S. Customs Service, the U.S. Department of Justice, or to the U.S. Postal Inspection Service for verification and investigation.

For **callers reporting instances of possible sexual exploitation**, NCMEC acts as a referring agency and may provide technical assistance, but it does not formally handle such cases. Requests for services in cases of child sexual abuse, incest, and molestation are referred to appropriate law enforcement and child protection agencies.

The resources and services listed above are available to parents of missing children once they have filed a missing person report with the police. There is no waiting period for or time limitation on these services. All other calls and requests for information may be made at any time to NCMEC's hotline. Free publications on child protection and prevention are available upon request.

Resources

Technical Assistance

Safeguard Their Tomorrows is a 4-hour nationally accredited educational program for health care professionals designed to address the prevention and investigation of infant abductions. The program was produced by Mead-Johnson Nutritionals in cooperation with the Association of Women's Health, Obstetric, and Neonatal Nurses; the National Association of Neonatal Nurses; and NCMEC.

NCMEC has joined forces with America's leading law enforcement associations to launch Project ALERT, a national program that uses retired law enforcement professionals as volunteers. Upon request by a law enforcement agency, NCMEC will assign a trained volunteer consultant to provide free, hands-on assistance to agencies struggling with missing child cases, child homicides, and child exploitation issues.

Publications

NCMEC has written and published a number of books, brochures, and pamphlets. Up to 50 copies of most brochures are available free of charge. Single copies of books are available free of charge.

Call NCMEC's hotline at 1-800-THE-LOST (1-800 843-5678) for more information about fees for bulk orders.

Brochures

Child Protection (English/Spanish)
Child Safety on the Information Highway (English)
For Camp Counselors (English)
For Law Enforcement Professionals (English)
Just in Case...Finding Professional Help in Case Your Child Is Missing or the Victim of Sexual Abuse or Exploitation (English, Spanish, Vietnamese)
Just in Case...You Are Considering Daycare (English, Spanish)
Just in Case...You Are Considering Family Separation (English, Spanish, Vietnamese)
Just in Case...You Are Dealing With Grief Following the Loss of a Child (English, Spanish)
Just in Case...You Are Using the Federal Parent Locator Service (English, Spanish)
Just in Case...You Need a Babysitter (English, Spanish)
Just in Case...Your Child Is a Runaway (English, Spanish, Vietnamese)
Just in Case...Your Child Is Testifying in Court (English, Spanish)
Just in Case...Your Child Is the Victim of Sexual Abuse or Exploitation (English, Spanish)
Just in Case...Your Child May Someday Be Missing (English, Spanish, Vietnamese)
My 8 Rules for Safety (English, Spanish, Haitian, Creole, Braille)
National Center for Missing and Exploited Children (English)
Tips to Prevent the Abduction and Sexual Exploitation of Children (Braille)

Books

A Report to the Nation (English)
An Analysis of Infant Abductions (English)
Child Molesters: A Behavioral Analysis (English)
Child Molesters Who Abduct: A Summary of the Case-in-Point Series (English)
Child Sex Rings: A Behavioral Analysis (English)
Children Traumatized in Sex Rings (English)
Family Abduction Guide (English, Spanish)
Female Juvenile Prostitution: Problem and Response (English)
For Health Care Professionals: Guidelines on Prevention of and Response to Infant Abduction (English)
Missing and Abducted Children: A Law Enforcement Guide to Case Investigation and Program Management (English)
My 8 Rules for Safety: Multilingual Child Safety and Prevention Tips (23 languages)
Nonprofit Service Provider's Handbook (English)
Recovery and Reunification of Missing Children: A Team Approach (English)
Selected State Legislation (English)

Also available is a resource list of nonprofit organizations throughout the United States, Canada, and Europe that work on missing and exploited child issues in their communities.

Legislative Citations

42 U.S.C. §§ 5771 and 5780. The National Center for Missing and Exploited Children was established in 1984 as a private, nonprofit organization to serve as a clearinghouse of information on missing and exploited children, to provide technical assistance to citizens and to law enforcement agencies, to offer training programs to law enforcement and social service professionals, to distribute photographs and descriptions of missing children, to coordinate child protection efforts with the private sector, to network with nonprofit service providers and State clearinghouses on missing person cases, and to provide information on effective State legislation to ensure the protection of children. Working in conjunction with the U.S. Postal Inspection Service, the U.S. Customs Service, and the U.S. Department of Justice, NCMEC serves as the National Child Pornography Tipline.

Contact Information

For information about the services provided by NCMEC, contact:

National Center for Missing and Exploited Children
2101 Wilson Boulevard, Suite 550
Arlington, VA 22201-3052
Hotline: 1-800-THE-LOST (1-800-843-5678), for the United States, Canada, and Mexico
Telephone (Business): (703) 235-3900
TTD: 1-800-826-7653
Fax: (703) 235-4067
World Wide Web: http://www.missingkids.com
Internet e-mail: 77431.177@Compuserve.com
CyberTipline: http://www.missingkids.com/cybertip.

Appendix 1

Department of Defense
Investigative Liaisons for Law Enforcement Agencies

Army

Criminal Investigation Command

CIOP-CO
6010 Sixth Street
Fort Belvoir, VA 22060-5506
Telephone: (703) 806-0305
Fax: (703) 806-0307

Criminal Investigation Division District Offices

Area: Georgia

Fort Benning District
Third Military Police Group (CID)
Building 1698
Fort Benning, GA 31905-6200
Telephone: (706) 545-8921
Fax: (706) 545-2509

Area: Hawaii

Hawaii District
Sixth Military Police Group (CID)
Schofield Barracks, HI 96857-5455
Telephone: (808) 655-2396
Fax: (808) 655-2387

Area: Kansas

Fort Riley District
Sixth Military Police Group (CID)
Building 406
Pershing Court
Fort Riley, KS 66442-0365
Telephone: (913) 239-3933
Fax: (913) 239-6388

Area: Kentucky

Fort Campbell District
Third Military Police Group (CID)
Building 2745
Fort Campbell, KY 42223-5637
Telephone: (502) 798-7247
Fax: (502) 798-2479

Area: National Capital Area

Washington, D.C., District
Third Military Police Group (CID)
Building 305
Fort Meyer, VA 22211-5199
Telephone: (703) 696-3496
Fax: (703) 696-6270

Area: New Jersey

Fort Dix District
Third Military Police Group (CID)
Building 6530
Fort Dix, NJ 08640-5780
Telephone: (609) 562-5006
Fax: (609) 562-5853

Area: North Carolina

Fort Bragg District
10th MP Det CID Abn
Third Military Police Group (CID)
Building 8-1221
Fort Bragg, NC 28307-5000
Telephone: (910) 396-7516
Fax: (910) 396-8607

Area: Texas

Fort Bliss District
Sixth Military Police Group (CID)
P.O. Box 6310
Building 13
Fort Bliss, TX 79916-6310
Telephone: (915) 568-5905
Fax: (915) 568-6899

Area: Texas

Fort Hood District
Sixth Military Police Group (CID)
P.O. Box V
Fort Hood, TX 76544-5000
Telephone: (817) 287-5039
Fax: (817) 287-9744

Area: Washington State

Fort Lewis District
Sixth Military Police Group (CID)
P.O. Box 331009
Fort Lewis, WA 98433-1009
Telephone: (206) 967-7859
Fax: (206) 967-4462

Navy and Marine Corps

Naval Criminal Investigative Service Headquarters

Washington Navy Yard
Building 111 (Code 0023B)
901 M Street SE.
Washington, DC 20388-5383
Telephone: (202) 433-9234
Fax: (202) 433-4922

Naval Criminal Investigative Service Field Offices

Area: Northern California, Colorado, Nevada, Utah, and Wyoming

Naval Criminal Investigative Service Field Office
161 Coral Sea Street
Naval Air Station
Alameda, CA 94501-5085
Telephone: (510) 273-4158
Fax: (510) 273-7965

Area: Central California

Naval Criminal Investigative Service Field Office
1317 West Foothill Boulevard
Suite 120
Upland, CA 91786
Telephone: (908) 985-2264
Fax: (908) 985-9763

Area: Southern California, Arizona, New Mexico, and West Texas

Naval Criminal Investigative Service Field Office
Box 368130
3405 Welles Street
Suite 1
San Diego, CA 92136-5050
Telephone: (619) 556-1364
Fax: (619) 556-0999

Area: Georgia, South Carolina, Central America, and South America

Naval Criminal Investigative Service Field Office
2365 Avenue F
Suite A
Charleston, SC 29408-1941
Telephone: (803) 743-3750
Fax: (803) 743-1058

Area: Hawaii and Pacific Islands

Naval Criminal Investigative Service Field Office
P.O. Box 122
Pearl Harbor, HI 96860-5090
Telephone: (808) 474-1218
Fax: (808) 474-1210

Area: Maryland, Northern Virginia, and Washington, D.C.

Naval Criminal Investigative Service Field Office
Washington Navy Yard
Building 200
Washington, DC 20374
Telephone: (202) 433-3658
Fax: (202) 433-6045

Area: Tidewater Virginia

Naval Criminal Investigative Service Field Office
1329 Bellinger Boulevard
Norfolk, VA 23511-2395
Telephone: (804) 444-7327
Fax: (804) 444-3139

Area: New Jersey, New York, and Pennsylvania

Naval Criminal Investigative Service Field Office
Naval Weapons Station
Colts Neck, NJ 07722-1901
Telephone: (908) 866-2235
Fax: (908) 866-1065

Area: North Carolina

Naval Criminal Investigative Service Field Office
H-32 Julian C. Smith Boulevard
Camp LeJeune, NC 28547-1600
Telephone: (910) 451-8017
Fax: (910) 451-8205

Area: Northwest Washington

Naval Criminal Investigative Service Field Office
1010 Skate Street
Suite A
Silverdale, WA 98315-1093
Telephone: (360) 396-4660
Fax: (360) 396-7009

Area: New England and Bermuda

Naval Criminal Investigative Service Field Office
344 Meyerkord Avenue, Third Floor
Newport, RI 02841-1607
Telephone: (401) 841-2241
Fax: (401) 841-4056

Area: North Central United States

Naval Criminal Investigative Service Field Office
Building 2
Second Floor East
Great Lakes, IL 60088-5001
Telephone: (708) 688-5655
Fax: (708) 688-2636

Area: South Central United States

Naval Criminal Investigative Service Field Office
341 Saufley Street
Pensacola, FL 32508-5133
Telephone: (904) 452-4211
Fax: (904) 452-2194

Area: Southeastern United States, Cuba, and Puerto Rico

Naval Criminal Investigative Service Field Office
Naval Station
P.O. Box 280076
Mayport, FL 32228-0076
Telephone: (904) 270-5361
Fax: (904) 270-6050

Air Force

During normal working hours:

Investigative Operations Center
Major Crimes Investigations
Bolling Air Force Base
Washington, DC 20332-5113
Telephone: (202) 767-5192/7760
Fax: (202) 767-5196

After normal working hours:

HQ AFOSI Staff Duty Office
Bolling Air Force Base
Washington, DC 20332-5113
Telephone: (202) 767-5450
Fax: (202) 767-5452

Appendix 2

Safe and Drug-Free Schools Comprehensive Regional Centers

Training and technical assistance for States, school districts, schools, community-based organizations, and other recipients of funds under the Improving America's Schools Act are available through the following Comprehensive Regional Assistance Centers:

Region I: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont

Dr. Vivian Guilfoy, Director
Education Development Center, Inc.
55 Chapel Street
Newton, MA 02158-1060
Telephone: (617) 969-7100, ext. 2201

Region II: New York

Dr. LaMar P. Miller, Executive Director
New York University
32 Washington Place
New York, NY 10003
Telephone: (212) 998-5100

Region III: Delaware, Maryland, New Jersey, Ohio, Pennsylvania, and Washington, D.C.

Dr. Charlene Rivera, Director
George Washington University
1730 North Lynn Street, Suite 401
Arlington, VA 22209
Telephone: (703) 528-3588

Region IV: Kentucky, North Carolina, South Carolina, Tennessee, Virginia, and W. Virginia

Dr. Terry L. Eidell, Executive Director
Appalachia Educational Laboratory, Inc.
P.O. Box 1348
Charleston, WV 25325-1348
Telephone: (304) 347-0400

Region V: Alabama, Arkansas, Georgia, Louisiana, and Mississippi

Dr. Betty Matluck, Vice President
Southwest Educational Development Laboratory
211 East Seventh Street
Austin, TX 78701-3281
Telephone: (512) 476-6861

Region VI: Iowa, Michigan, Minnesota, North Dakota, and Wisconsin

Dr. Minerva Coyne, Director
University of Wisconsin
1025 West Johnson Street
Madison, WI 53706
Telephone: (608) 263-4326

Region VII: Illinois, Indiana, Kansas, Missouri, Nebraska, and Oklahoma

Dr. Hai Tran, Director
University of Oklahoma
1000 ASP - Room 210
Norman, OK 73019
Telephone: (405) 325-2243

Region VIII: Texas

Dr. Maria Robledo Montecel, Executive Director
Dr. Albert Cortez, Site Director
Intercultural Development Research Association
5835 Callaghan Road, Suite 350
San Antonio, TX 78228-1190
Telephone: (210) 684-8180

Region IX: Arizona, Colorado, New Mexico, Nevada, and Utah

Dr. Paul E. Martinez, Director
New Mexico Highlands University
121 Tijeras NE., Suite 2100
Albuquerque, NM 87102
Telephone: (505) 242-7447

Region X: Idaho, Montana, Oregon, Washington, and Wyoming

Mr. Carlos Sundermann, Director
Northwest Regional Educational Laboratory
101 Southwest Main Street, Suite 500
Portland, OR 97204
Telephone: (503) 275-9479

Region XI: Northern California

Dr. Beverly Farr, Director
Far West Laboratory for Educational Research
730 Harrison Street
San Francisco, CA 90242
Telephone: (415) 565-3009

Region XII: Southern California

Dr. Celia C. Ayala, Director
Los Angeles County Office of Education
9300 Imperial Highway
Downey, CA 90242-2890
Telephone: (310) 922-6319

Region XIII: Alaska

Dr. John Anttonen, Executive Director
South East Regional Resource Center
210 Ferry Way
Suite 200
Juneau, AK 99801
Telephone: (907) 586-6806

Region XIV: Florida, Puerto Rico, and the Virgin Islands

Dr. Trudy Hensley, Director
Educational Testing Service
1979 Lake Side Parkway, Suite 400
Tucker, GA 30084
Telephone: (770) 723-7443

Region XV: American Samoa, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Guam, Hawaii, Republic of the Marshall Islands, and Republic of Palau

Dr. John W. Kofel, Chief Executive
Pacific Region Educational Laboratory
828 Fort Street Mall, Suite 500
Honolulu, HI 96813
Telephone: (808) 533-6000

Appendix 3

Family and Youth Services Bureau Regional Centers

Empire State Coalition of Youth and Family Services/Region II
121 Avenue of the Americas, Room 507
New York, NY 10013-1505
Telephone: (212) 966-6477
Fax: (212) 431-9783
EMPSTACOAL@aol.com

Mid-Atlantic Network of Youth and Family Services, Inc.
9400 McKnight Road, Suite 204
Pittsburgh, PA 15237
Telephone: (412) 366-6562
Fax: (412) 366-5407
NancyJMANY@ol.com

MINK - c/o Synergy/Region VII
P.O. Box 14403
Parkville, MO 64152
Telephone: (816) 587-4100
Fax: (816) 587-6691
MINKPAM@aol.com

Mountain Plains Youth Services/Region VIII
221 West Rosser Avenue
Bismarck, ND 58501
Telephone: (701) 255-7229
Fax: (701) 255-3922
MTNPLAINS@aol.com

New England Consortium for Families and Youth/Region I
25 Stow Road
Boxboro, MA 01719
Telephone: (508) 266-1998
Fax: (508) 266-1999
NECFY@aol.com

Northwest Network of Runaway and Youth Services/Region X
603 Stewart Street, Suite 609
Seattle, WA 98101
Telephone: (206) 628-3760
Fax: (206) 628-3746
Northwestnw@aol.com

Southeastern Network of Youth and Family Services/Region IV
337 South Milledge Avenue, Suite 209
Athens, GA 30605
Telephone: (706) 354-4568
Fax: (706) 353-0026
SENCYFS@aol.com

South West Network of Youth Services, Inc./ Region VI
Texas Network of Youth Services
2525 Wallingwood Drive, Suite 1503
Austin, TX 78746
Telephone: (512) 328-6860
Fax: (512) 328-6863
TheresaTod@aol.com

Western States Youth Services Network/ Region IX
1309 Ross Street, Suite B
Petaluma, CA 94954
Telephone: (707) 763-2213
Fax: (707) 763-2704
WSYN@aol.com

Youth Network Council
Illinois Collaboration on Youth
59 East Van Buren Street, Suite 1610
Chicago, IL 60605
Telephone: (312) 427-2710
Fax: (312) 427-3247
YNCICOY@aol.com

Appendix 4

Organizations Concerned With The Prevention of Child Abuse and Neglect: State Contacts

The following organizations can serve as resources for information and materials in the prevention of child abuse and neglect:

- ***"Don't Shake the Baby"*** is a national public awareness campaign, organized in all 50 States, the District of Columbia and Puerto Rico, focused on decreasing the incidence of Shaken Baby Syndrome and thereby decreasing disability and death caused by child maltreatment.

- ***Children's Trust and Prevention Funds*** are State-level organizations that support community prevention programs through policy formation, funding innovative programs, public awareness, and education.

- ***National Committee to Prevent Child Abuse*** is a not-for-profit, volunteer-based organization committed to the prevention of child maltreatment through education, research, public awareness, and advocacy services to community members.

- ***Parents Anonymous*** is a parent self-help program with neighborhood-based support groups throughout the United States and several foreign countries.

"DON'T SHAKE THE BABY" CONTACTS

ALABAMA
Betsy Taff
Alabama Children's Trust Fund
P.O. Box 4251
Montgomery, AL 36103
(334) 242-5710
(334) 242-5711 (fax)

ALASKA
Debra Bruneau/Judy Saha
Rural Community Action Program
P.O. Box 200908
Anchorage, AK 99520
(907) 279-2511
(907) 279-6343 (fax)

ARIZONA
Becky Ruffner
State Coordinator
Arizona Chapter, NCPCA
P.O. Box 442
Prescott, AZ 86302
(602) 445-5038
(602) 778-6120 (fax)

ARKANSAS
Sherri McLemore
AK Child Abuse Prevention
2915 Kavanaugh, Suite 379
Little Rock, AR 72205
(501) 374-9003
(501) 372-5257 (fax)

CALIFORNIA
Margery Winter
Office of Child Abuse Prevention CCDSS
744 P Street, MS 9-100
Sacramento, CA 95814
(916) 445-0456
(916) 445-2898 (fax)

COLORADO
Jacy Showers, Ed.D.
Pueblo City-County Health Department
151 Central Main Street
Pueblo, CO 81003-4297
(719) 583-2000
(719) 583-2004 (fax)

CONNECTICUT
Jane Bourns
Director of Children's Services
Susanne Santangelo
Wheeler Clinic
91 Northwest Drive
Plainville, CT 06062
(203) 747-6801, ext. 244
(203) 793-3520 (fax)

DELAWARE
Karen Derasmo
Delawareans United to Prevent Child Abuse
124CD Senatorial Drive
Greenville Place
Wilmington, DE 19807
(302) 654-1102
(302) 655-5761 (fax)

DISTRICT OF COLUMBIA
Dr. Lavdena Orr
Division of Child Protection
Children's National Medical Center
111 Michigan Avenue, N.W.
Washington, DC 20010-2970
(202) 884-4950
(202) 884-6997 (fax)

FLORIDA
Stephanie Meinke, MSW
President
Parent Network/FCPCA
2728 Pablo Avenue, Suite B
Tallahassee, FL 32308
(904) 488-5437
(904) 921-0322 (fax)

GEORGIA
Pam Brown
GA Council on Child Abuse, Inc.
First Steps Program
1375 Peachtree Street, N.E.
Suite 200
Atlanta, GA 30309-3111
(404) 870-6565
(404) 870-6541 (fax)

HAWAII
Aileen Deese
PREVENT Child Abuse - HI
Hawaii Chapter, NCPCA
1575 S. Beretania Street
Suite 202
Honolulu, HI 96826
(808) 951-0200
(808) 941-7004 (fax)

IDAHO
Anna Sever, Child Protection Program Specialist
FACTS - Third Floor
Children's Service Bureau
450 W. State Street
Boise, ID 83720-0036
(208) 334-5920
(208) 334-6699 (fax)

ILLINOIS
Robyn Gabel, Exec. Director
Illinois Maternal & Child Health Coalition
3411 W. Diversey, Suite 5
Chicago, IL 60647
(312) 384-8828
(312) 384-3904 (fax)

INDIANA
Patti Duwel
Indiana Chapter of NCPCA
Jefferson Plaza
One Virginia Avenue, Suite 401
Indianapolis, IN 46204
(317) 634-9282
(317) 634-9295 (fax)

IOWA
John Holtkamp
Iowa Chapter NCPCA
3829 71st Street, Suite A
Des Moines, IA 50322
(515) 252-0270
(515) 252-0829 (fax)

KANSAS
Michelle Sinclair Lawrence
(Brenda Sharpe)
Child Abuse Prevention
Coalition
6811 W. 63rd Street, Suite 210
Overland Park, KS 66202-4080
(913) 831-2272
(913) 831-0273 (fax)

KENTUCKY
Donna Overbee
Program Director
Kentucky Council on Child
Abuse, Inc.
2401 Regency Road, Suite 104
Lexington, KY 40503
(606) 276-1299
(800) 432-9251
(606) 277-1782 (fax)

LOUISIANA
Jacinta (Jay) Settoon
LA Council on Child Abuse
2351 Energy Drive, Suite 1010
Baton Rouge, LA 70808
(800) 348-KIDS (LA only)
(504) 925-9520
(504) 926-1319 (fax)

MAINE
Cheryl DiCara
Maternal and Child Health
Statehouse Station #11
Augusta, ME 04333
(207) 287-3311
(207) 287-5355 (fax)

MARYLAND
Martha Elliott
Director of Social Work
Mt. Washington Pediatric Hosp.
1708 Rogers Avenue
Baltimore, MD 21209
(410) 578-8600, ext. 4
(410) 466-1715 (fax)

MASSACHUSETTS
Jetta Bernier, Exec. Director
MA Committee for Children
and Youth
14 Beacon Street, Suite 706
Boston, MA 02108
(617) 742-8555
(617) 742-7808 (fax)

MICHIGAN
Janice Long
MI Children's Trust Fund
P.O. Box 30037
Lansing, MI 48909
(517) 373-4320
(517) 335-6177 (fax)

MINNESOTA
Carolyn Levitt, M.D.
Midwest Children's Resource
Center
360 Sherman Street, Suite 200
St. Paul, MN 55102
(612) 220-6750
(612) 220-6770 (fax)

Jane Swenson
Midwest Children's Resource
Center
360 Sherman Street, Suite 200
St. Paul, MN 55102
(612) 220-6750
(612) 220-6770 (fax)

MISSISSIPPI
Regan Marler Painter, Director
MS Children's Trust Fund
State Dept. of Human Services
750 N. State Street
Jackson, MS 39202
(601) 359-4479
(601) 359-4363 (fax)

MISSOURI
Nela Beetem
Social Work Consultant
MO Department of Health
Bureau of Perinatal and Child
Health
1730 E. Elm Street
Jefferson City, MO 65102
(314) 751-6215
(314) 526-5348 (fax)

MONTANA
Maryellen Bindel
Cascade Co. CAP Council, Inc.
2608 Second Avenue, North
Great Falls, MT 59401
(406) 761-1286

NEBRASKA
Terri Segal
NE Dept. of Social Services
301 Centennial Mall South
Lincoln, NE 68509
(402) 471-9196
(402) 471-9455 (fax)

NEVADA
Dr. Paula R. Ford, Exec. Dir.
Nevada NCPCA
We Can, Inc.
3441 W. Sahara, Suite C-3
Las Vegas, NV 89102
(702) 368-1533
(702) 368-1540 (fax)

NEW HAMPSHIRE
Audrey Knight, MSN, CPNP
Child Health Nurse Consultant
Bureau of Maternal & Child
Health
NH Division of Public Health
Services
6 Hazen Drive
Concord, NH 03301
(603) 271-4536
(603) 271-3827 (fax)

NEW JERSEY
Susan White
New Jersey Chapter, NCPCA
35 Halsey Street
Newark, NJ 07012
(201) 643-3710
(201) 643-9222 (fax)

NEW MEXICO
Ellen Novak
Children, Youth & Families Dept.
Child Abuse Prevention Unit
300 San Mateo N.E., Suite 602
Albuquerque, NM 87108-1516
(505) 841-2967
(505) 841-2969 (fax)

NEW YORK
Judith Richards
William B. Hoyt Memorial
Children & Family Trust Fund
40 N. Pearl Street, 11-D
Albany, NY 12243
(518) 474-9613
(518) 474-9617 (fax)

NORTH CAROLINA
Jennifer Tolle, Exec. Director
Prevent Child Abuse - NC
3344 Hillsborough Street
Suite 100D
Raleigh, NC 27607
(919) 829-8009
(919) 832-0308 (fax)

NORTH DAKOTA
Sue Heinze
Children's Hospital MeritCare
720 4th Street North
Fargo, ND 58122
(701) 234-5737
(701) 234-6965 (fax)

OHIO
Sharon Enright, Project Dir.
GRADS
65 S. Front Street, Room 909
Columbus, OH 43215-4183
(614) 466-3046
(614) 644-5702 (fax)

Eve Pearl
Council on Child Abuse of Southern Ohio, Inc.
7374 Reading Road, Suite 105
Cincinnati, OH 45237
(513) 351-8005
(513) 351-0226 (fax)

OKLAHOMA
John Stuemky, MD
Oklahoma Emergency Medical Services for Children Project
Children's Hospital of OK
940 N.E. 13th Street
Oklahoma City, OK
73104-5066
(405) 271-3307
(405) 271-8709 (fax)

OREGON
Donna Merrill
Children's Trust Fund
800 N.E. Oregon Street
Suite 1140
Portland, OR 97232-2161
(503) 731-4782
(503) 731-8614 (fax)

RHODE ISLAND
Ted Whiteside, Exec. Director
Rhode Island Committee to Prevent Child Abuse
500 Prospect Street
Pawtucket, RI 02860
(401) 728-7920
(401) 724-5850 (fax)

SOUTH CAROLINA
Sandra Jeter
Office of Pub. Health/Soc.Work
Department of Health and Environmental Control
Robert Mills Complex
Box 101106
Columbia, SC 29211
(803) 737-3950
(803) 737-3946 (fax)

SOUTH DAKOTA
M erlin Weyer, Prog. Specialist
Joyce Country, Prog. Specialist
Office of Child Protection Svcs.
700 Governor's Drive
Kneip Building
Pierre, SD 57501
(605) 773-3227
(605) 773-6834 (fax)

TENNESSEE
Dora Hemphill
TN Dept. of Human Services
400 Deaderick Street
Nashville, TN 37248
(615) 313-4764
(615) 532-9956 (fax)

TEXAS
Janie Fields, Executive Director
Claire Kriens
Children's Trust Fund of Texas
8929 Shoal Creek Boulevard
Suite 200
Austin, TX 78757-6854
(512) 458-1281
(512) 458-9471 (fax)

UTAH
Marilyn Sandberg
Stacy Iverson
Child Abuse Prevention Council of Ogden
457 26th Street
Ogden, UT 84401
(801) 399-8430
(801) 399-8016 (fax)

VERMONT
Linda Johnson, Exec. Director
Vermont Chapter, NCPCA
141 Main Street
P.O. Box 829
Montpelier, VT 05601
(802) 229-5724
(802) 223-5567 (fax)

VIRGINIA
Diane Bell, Deputy Director
SCAN of Northern Virginia, Inc.
2210 Mount Vernon Avenue
Alexandria, VA 22301
(703) 836-1820
(703) 836-1248 (fax)

WASHINGTON
Carol Mason
Children's Protection Program
Children's Hospital and Medical Center
4800 Sand Point Way, N.E.
P.O. Box 5371, MS CH-76
Seattle, WA 98105-3071
(206) 526-2194
(206) 526-2246 (fax)

Carmen Ray, Exec. Director
WA Council for Prevention of Child Abuse and Neglect
318 First Avenue, South
Suite 310
Seattle, WA 98104
(206) 464-6151
(206) 464-6642 (fax)

WEST VIRGINIA
Victoria Schlak
Children's Reportable Disease Coordinator
1411 Virginia Street, East
Charleston, WV 25301
(304) 558-7996
(304) 558-2183 (fax)

WISCONSIN
Christine Holmes
Child Protection Center
Outpatient Health Center
1020 N. 12th Street
Milwaukee, WI 53233
(414) 277-8980
(414) 277-8969 (fax)

WYOMING
Rick Robb
Wyoming Department of Family Services
Hathaway Building
2300 Capitol Avenue
Cheyenne, WY 82002
(307) 777-7150
(307) 777-3693 (fax)

NATIONAL PROJECT DIRECTOR
Jacy Showers, Ed.D.
SBS Prevention Plus
1907 Northmoor Terrace
Pueblo, CO 81008
(719) 583-2000
(719) 583-2004 (fax)

CHILDREN'S TRUST AND PREVENTION FUNDS

ALABAMA
Kitty Trent
Alabama CTF
P.O. Box 4251
Montgomery, AL 36103
(334) 242-5710
(334) 242-5711 (fax)

ALASKA
Nila Rinehart
Alaska CTF - Children's Cabinet
P.O. Box 112100
Juneau, AK 99811
(907) 465-4870
(907) 465-8638 (fax)

ARIZONA
Valerie Roberson
Arizona CTF
Child Abuse Prevention Fund
P. O. Box 6123, Site Code 940A
Phoenix, AZ 85005
(602) 542-0817
(602) 542-3330 (fax)

ARKANSAS
Sherri McLemore
Arkansas CTF
2915 Kavanaugh, Suite 416
Little Rock, AR 72205
(501) 374-9003
(501) 372-5257 (fax)

CALIFORNIA
Margery Winter
California CTF
Office of Child Abuse Prevention
744 P Street, Mail Station 19-82
Sacramento, CA 95814
(916) 445-2862
(916) 445-2898 (fax)

COLORADO
Joyce Jennings
Colorado CTF
110 16th Street, 3rd Floor
Denver, CO 80202
(303) 446-8860
(303) 640-5289 (fax)

CONNECTICUT
Carol LaLiberte
Connecticut CTF
505 Hudson Street
Hartford, CT 06106
(860) 550-6473
(860) 566-8022 (fax)

DELAWARE
Richard Donges
Delaware CTF
P.O. Box 2363
Wilmington, DE 19899
(302) 836-8550
(302) 836-2960 (fax)

DISTRICT OF COLUMBIA
Carolyn Abdullah
District of Columbia CTF
1730 K Street, N.W., Suite 304
Washington, DC 20006
(202) 296-6656
(202) 296-0942 (fax)

FLORIDA
Admiral Henderson
Florida CTF
Dept. Health and Rehabilitative Services
2811 C Industrial Plaza Drive
Tallahassee, FL 32301
(904) 488-8762
(904) 488-9584 (fax)

GEORGIA
Susan Phillips
Georgia CTF
Two Northside 75, Suite 125
Atlanta, GA 30318
(404) 352-6050
(404) 352-6051 (fax)

HAWAII
Steve Kaneshiro
Hawaii CTF
Hawaii Community Foundation
222 Merchant Street
Honolulu, HI 96813
(808) 537-6333
(808) 521-6286 (fax)

IDAHO
Laura Rappaport
Idaho CTF
P.O. Box 2015
Boise, ID 83701-2015
(208) 386-9317
(208) 334-6699 (fax)

ILLINOIS
Ron Davidson
Illinois CTF
Dept. of Children & Family Services
406 E. Monroe Street
Station #225
Springfield, IL 62701-1498
(217) 524-2403
(217) 524-3966 (fax)

INDIANA
Vernell Miller
Indiana CTF
Child Abuse Prevention Fund
402 W. Washington Street
Room W364
Indianapolis, IN 46204
(317) 232-7116
(317) 232-4436 (fax)

IOWA
Sommai Ung
Iowa CTF
Iowa Dept. Human Services
5th Floor
Hoover State Office Building
Des Moines, IA 50319-0114
(515) 281-5246
(515) 281-4597 (fax)

KANSAS
James Tramill
Kansas CTF
Family & Children's Trust Fund
515 S. Kansas Avenue, Suite A
Topeka, KS 66603
(913) 296-3651
(913) 296-4880 (fax)

KENTUCKY
John W. Patterson
Kentucky CTF
Child Victims' Trust Fund
P.O. Box 2000
Frankfort, KY 40602
(502) 573-5900
(502) 573-8315 (fax)

LOUISIANA
Judy Harrison
Louisiana CTF
P.O. Box 3318
Baton Rouge, LA 70821
(504) 342-2245
(504) 342-2268 (fax)

MAINE
J. Terence Burns, President
Maine CTF
P.O. Box 2850
Augusta, ME 04338
(207) 623-5461

MARYLAND
J.C. Shay
Maryland CTF
301 W. Preston Street
Suite 1502
Baltimore, MD 21201
(410) 225-4160
(410) 333-7492 (fax)

MASSACHUSETTS
Suzin M. Bartley
Massachusetts CTF
294 Washington Street
Suite 640
Boston, MA 02108-4608
(617) 727-8957
(617) 727-8997 (fax)

MICHIGAN
Deborah Strong
Michigan CTF
P.O. Box 30037
Lansing, MI 48909
(517) 373-4320
(517) 335-6177 (fax)

MINNESOTA
Maureen Cannon
Minnesota CTF
444 Lafayette Road
Saint Paul, MN 55155-3839
(612) 296-5436
(612) 297-1949 (fax)

MISSISSIPPI
Regan Marler Painter
Mississippi CTF
Dept. Human Services
750 N. State Street
Jackson, MS 39202
(601) 359-4479
(601) 359-4363 (fax)

MISSOURI
Sarah Grim
Missouri CTF
P.O. Box 1641
Jefferson City, MO 65102-1641
(573) 751-5147
(573) 751-0254 (fax)

MONTANA
Kirk Astroth
Montana CTF
Montana State University
210 Taylor Hall
Bozeman, MT 59717-0358
(406) 994-3501
(406) 994-5417 (fax)

NEBRASKA
Mary Jo Pankoke
Nebraska CTF
Child Abuse Prevention Fund
301 Centennial Mall South
Lincoln, NE 68508
(402) 471-9320
(402) 471-9455 (fax)

NEVADA
Joan Buchanan
Nevada CTF
505 E. King Street, Room 600
Carson City, NV 89710
(702) 687-5761
(702) 687-4733 (fax)

NEW HAMPSHIRE
Fran Belcher
New Hampshire CTF
NH Charitable Foundation
37 Pleasant Street
Concord, NH 03301-4005
(603) 225-6641
(603) 225-1700 (fax)

NEW JERSEY
Donna Pincavage
New Jersey CTF
222 S. Warren Street, CN 700
Trenton, NJ 08625-0700
(609) 633-3992
(609) 984-7380 (fax)

NEW MEXICO
Director
New Mexico CTF
300 San Mateo N.E. - 5th Floor
Albuquerque, NM 87108
(505) 841-6494
(505) 841-6485 (fax)

NEW YORK
Judy Richards
New York CTF
Children & Family Trust Fund
40 N. Pearl Street, 11 Floor
Albany, NY 12243-0001
(518) 474-9613
(518) 474-9617 (fax)

NORTH CAROLINA
Dwight Whitted
North Carolina CTF
301 N. Wilmington Street
Raleigh, NC 27601-2825
(919) 715-1637
(919) 715-0517 (fax)

NORTH DAKOTA
Beth Wosick
North Dakota CTF
600 E. Boulevard Avenue
Bismarck, ND 58505-0250
(701) 224-2301
(701) 224-2359 (fax)

OHIO
Rhonda Reagh, Ph.D.
Ohio CTF
65 E. State Street, Suite 908
Columbus, OH 43266-0423
(614) 466-1822
(614) 728-3504 (fax)

OKLAHOMA
Pamela Rollins
Oklahoma CTF
Child Abuse Prevention Fund
1000 N.E. 10th
Oklahoma City, OK
73117-1299
(405) 271-4471
(405) 271-1011 (fax)

OREGON
Cynthia Thompson
Oregon CTF
800 N.E. Oregon Street
Suite 1140
Salem, OR 97232-2162
(503) 731-4782
(503) 731-8614 (fax)

PENNSYLVANIA
Scott Peters
Pennsylvania CTF
P.O. Box 2675
Harrisburg, PA 17105-2675
(717) 783-7287
(717) 787-0414 (fax)

RHODE ISLAND
Nancy Herrington
Rhode Island CTF
Family & Children's Trust Fund
610 Mount Pleasant Avenue
Building 1
Providence, RI 02908
(401) 457-4519
(401) 457-4511 (fax)

SOUTH CAROLINA
David Havin
South Carolina CTF
Partnership for S.C. Children
2711 Middleburg Drive
Suite 307
Columbia, SC 29204
(803) 929-1013
(803) 779-4160 (fax)

SOUTH DAKOTA
Joyce Country
South Dakota CTF
700 Governor's Drive
Pierre, SD 57501-2291
(605) 773-3227
(605) 773-4855 (fax)

TENNESSEE
Dora Hemphill
Tennessee CTF
Child Abuse Prevention Prog.
400 Deaderick Street
Nashville, TN 37248-9500
(615) 313-4764
(615) 532-9956 (fax)

TEXAS
Janie D. Fields
Texas CTF
8929 Shoal Creek Boulevard
Suite 200
Austin, TX 78757-6854
(512) 458-1281
(512) 458-9471 (fax)

UTAH
Consuelo Alires
Utah CTF
120 N. 200 West, Room 225
Salt Lake City, UT 84103
(801) 538-4535
(801) 538-3993 (fax)

VERMONT
Linda Johnson
Vermont CTF
Children and Family Council
103 S. Main Street
Waterbury, VT 05671-0203
(802) 241-2928
(802) 241-2979 (fax)

VIRGINIA
Phyl Parrish
Virginia CTF
Family & Children's Trust Fund
730 E. Broad Street
Richmond, VA 23219
(804) 692-1823
(804) 692-1869 (fax)

WASHINGTON
Director
Washington CTF
Council for Prevention
318 First Avenue South
Suite 310
Seattle, WA 98104
(206) 464-6151
(206) 464-6642 (fax)

WEST VIRGINIA
Barbara Merrill
West Virginia CTF
Gov. Cabinet on Children
&Families
Building 1, Room 9
1900 Kanawaha Blvd., East
Charleston, WV 25305
(304) 558-1955
(304) 558-0596 (fax)

WISCONSIN
Mary Ann Snyder
Wisconsin CTF
110 E. Main Street, Room 614
Madison, WI 53703
(608) 266-6871
(608) 266-3792 (fax)

WYOMING
Carol Speight
Wyoming CTF
Dept. of Family Services
Third Floor, Hathaway Building
Cheyenne, WY 82002-0490
(307) 777-6081
(307) 777-7747 (fax)

Developing Trust Fund:

PUERTO RICO
Maria Carrillo de Sevilla
Department of the Family
GPO Box 15091
San Juan, PR 00902
(787) 724-7532
(787) 721-1331 (fax)

PARENTS ANONYMOUS, INC.

ARIZONA
Michele Keal,
President and CEO
Parents Anonymous of AZ, Inc.
2701 N. 16th Street, #316
Phoenix, AZ 85006
(602) 248-0428
(602) 248-0496 (fax)
Family Lifeline (800) 352-0528

ARKANSAS
Linda Redden
Parent Anonymous Coordinator
SCAN Volunteer Services
1400 W. Markham
Little Rock, AR 72201
(501) 372-7226
(501) 375-7329 (fax)
Parents Anonymous
(501) 375-7321

CALIFORNIA
Juanita Chavez,
CA Coordinator
Parents Anonymous, Inc.
675 W. Foothill Blvd.
Suite 220
Claremont, CA 91711
(909) 621-6184
(909) 625-6304 (fax)

COLORADO
Laura Fourzan, Coordinator
Pikes Peak Family Connections, Inc.
301 S. Union Boulevard
Colorado Springs, CO 80910
(719) 578-3210
(719) 578-3192 (fax)
Family Connection
(719) 578-3206
or (719) 495-4126

Jennifer Richardson,
Coordinator
Families First
2760-R S. Havana Street
P.O. Box 14190
Aurora, CO 80014
(303) 745-0327
(303) 745-0115 (fax)
Parent Support Line
(303) 695-7996

CONNECTICUT
Jane Bourns, Director
Children's Clinical Services
Wheeler Clinic
91 Northwest Drive
Plainville, CT 06062
(860) 747-6801
(860) 793-3520 (fax)
Parents Anonymous
(800) 841-4314

DELAWARE
JoAnn Kasses & Karen DeRamos, Co-Directors
Delawareans United to Prevent Child Abuse
124 CD Senatorial Drive
Wilmington, DE 19807
(302) 654-1102
(302) 655-5761 (fax)
PATH (302) 654-1102; (302) 674-1112; (302) 856-1737

FLORIDA
Stephanie Meincke, Exec. Dir.
The Family Source of Florida
2728 Pablo Avenue, Suite B
Tallahassee, FL 32308
(904) 488-5437
(904) 921-0322 (fax)
Parent Helpline (800) 352-5683

GEORGIA
Sandra Wood, Exec. Director
GA Council on Child Abuse
1375 Peachtree St. N.E., 200
Atlanta, GA 30309
(404) 870-6565
(404) 870-6541(fax)
Helpline (800) 532-3208

ILLINOIS
Maureen Blaha
Parents Anonymous Director
Children's Home and Aid Society of Illinois
125 S. Wacker Drive, 14th Flr.
Chicago, IL 60606
(312) 424-6822
(312) 424-6800 (fax)
Parents Anonymous
(815) 968-0944; (618) 462-2714; (217) 359-8815; (708) 837-6445; (312) 649-4879

IOWA
Roberta Milinsky,
Dir. of Program Activities
Children & Families of Iowa
1111 University
Des Moines, IA 50314
(515) 288-1981
(515) 288-9109 (fax)
1st Call for Help
(515) 246-6555

KENTUCKY
Mary Smith, Board Chair
Parents Anonymous of Murray-Calloway County
P.O. Box 1302
Murray, KY 42071
(502) 762-4627

LOUISIANA
Marketa Garner, Exec. Director
LA Council on Child Abuse
2351 Energy Drive
Suite 1010
Baton Rouge, LA 70808
(504) 925-9520
(800) 348-KIDS
(504) 926-1319 (fax)

MAINE
Pam Marshall
Parents Anonymous Coord.
Parents Anonymous of Maine
P.O. Box 284
Cape Elizabeth, ME 04107
(207) 767-5506
(207) 767-0995 (fax)
Parent Talk Line
(800) 249-5506

MARYLAND
Frank Blanton, Exec. Director
Parents Anonymous of MD
733 W. 40th Street, Suite 20
Baltimore, MD 21211
(410) 889-2300
(410) 889-2487 (fax)
Parent Stressline
(410) 243-7337

MASSACHUSETTS
Jeannette Atkinson
Executive Director
Parents Anonymous of MA
140 Clarendon Street
Boston, MA 02116
(617) 267-8077
(617) 351-7615 (fax),
call first *Parents Anonymous*
(800) 882-1250

MICHIGAN
Judy Ranger,
Parent Aide Coordinator
Family & Children's Services
1608 Lake Street
Kalamazoo, MI 49001
(616) 344-0202
(616) 344-0285 (fax)

MINNESOTA
Suzann Eisenberg Murray,
Executive Director
Parents Anonymous of MN
1061 Rice Street
Saint Paul, MN 55117
(612) 487-2111
(612) 487-6383 (fax)
Parents Anonymous
(507) 377-7665;
(218) 736-5617

MISSOURI
Joyce Downing
Parents Anonymous of Missouri
10918 Elm Avenue
Kansas City, MO 64134
(816) 765-6600
(816) 767-4101 (fax)
Parent Helpline (800) 844-0192

MONTANA
Jeanne Kemis, Admin. Director
Montana Council for Families
P.O. Box 7533
Missoula, MT 59807
(406) 728-9449
(406) 728-9459 (fax)
Parents Anonymous
(406) 728-5437;
(406) 563-7983;
(406) 252-9799;
(406) 587-3840

NEBRASKA
Vicki Mack, Executive Director
Parents Anonymous of Central Nebraska
P.O. Box 1312
Grand Island, NE 68802
(308) 382-9117
Parent Stressline
(308) 389-0044

Lorena Murray, Chair,
Board of Directors
Hastings Area Parents Anonymous
1832 W. Ninth Street
Hastings, NE 68901
(402) 463-4395

NEVADA
Sandy Soltz,
Parents Anonymous Coord.
WE CAN
3441 W. Sahara, C-3
Las Vegas, NV 89102
(702) 368-1533
(702) 368-1540 (fax)

NEW HAMPSHIRE
Monique Divine,
Director of Communications
New Hampshire Task Force to Prevent Child Abuse
P.O. Box 607
Concord, NH 03302
(603) 225-5441
(603) 228-5322 (fax)
PA Line (800) 750-4494

NEW JERSEY
Kathleen Roe, Executive Dir.
Parents Anonymous of NJ, Inc.
12 Roszel Road, Suite A-103
Princeton, NJ 08540
(609) 243-9779
(609) 243-0169 (fax)
Family Helpline
(800) THE-KIDS

NEW MEXICO
Chris Montano,
Parent Anonymous Coordinator
All Faiths Receiving Home
P.O. Box 6573
Albuquerque, NM 87197
(505) 266-3506
(505) 262-2877 (fax)

NEW YORK
Linda Murphy,
Voc. Ed. Coordinator
Yours, Ours, Mine Community Center, Inc.
152 Center Lane
Levittown, NY 11756
(516) 796-6633
(516) 796-6663 (fax)

Rosemary Taylor, Exec. Dir.
YWCA
44 Washington Avenue
Schenectady, NY 12305
(518) 374-3394
(518) 374-3385 (fax)

NORTH DAKOTA
Beth Wosick, Exec. Dir.
ND Children's Trust Fund
600 East Boulevard
Bismark, ND 58505
(701) 328-2301
(701) 328-2359 (fax)

OHIO
Carolin Kurns
Parents Anonymous of Canton
Families First
142 Arlington, NW
Canton, OH 44708
(330) 456-5470

Karen McCann
Council on Child Abuse
7374 Reading Road, Suite 1-A
Cincinnati, OH 45237
(513) 351-8005
(513) 351-0226 (fax)

Marian Grisdale
Bellflower Center
11701 Shaker Boulevard
Cleveland, OH 44120
(216) 229-2420;
(216) 229-2474

Bill McCulley,
Parents Anonymous Director
Catholic Social Services
155 E. Patterson Avenue
Columbus, OH 43202
(614) 447-9192 (fax)
Parent Connection Line
(614) 447-9400

OREGON
Maureen Rozee, Parents
Anonymous State Director
Waverly Children's Home
3550 S.E. Woodward
Portland, OR 97202
(503) 238-8819
(503) 233-0187 (fax)
Parent Helpline (800) 345-5044

PENNSYLVANIA
Angela Fogle, Exec. Director
Parents Anonymous of PA
2001 N. Front Street
Building 1, Suite 314
Harrisburg, PA 17102
(717) 238-0937
(717) 238-4315 (fax)
Parents Anonymous
(800) 448-4906

RHODE ISLAND
Mildred H. Bauer
324 Oak Hill Avenue
Attleboro, MA 02703
(508) 222-6205
(401) 434-1858 (fax)
Parents Anonymous
(800) 882-1250

SOUTH CAROLINA
Marty Banks, Exec. Director
Parents Anonymous of SC
P.O. Box 80099
Charleston, SC 29416
(803) 529-3200
(803) 529-3211 (fax)
Helpline (800) 326-8621

TEXAS
Rebecca Christie
Executive Director
Parents Anonymous of Texas
7801 N. Lamar, Suite F-12
Austin, TX 78752
(512) 459-5490
(512) 459-3058 (fax)
Texas Heartline
(800) 554-2323

VERMONT
Linda Johnson, Exec. Director
Prevent Child Abuse-Vermont
P.O. Box 829
Montpelier, VT 05601
(802) 229-5724
(802) 223-5567 (fax)
Parent Stressline
(800) 639-4010

VIRGINIA
Karen Schrader,
Director of Programs
Prevent Child Abuse-Virginia
P.O. Box 12308
Richmond, VA 23241
(804) 775-1777
(804) 775-0019 (fax)
Warmline (800) 257-8227

WASHINGTON
Sylvia Meyer, Exec. Director
The Parent Trust for
Washington Children
1305 4th Avenue, Suite 310
Seattle, WA 98101
(206) 233-0156
(206) 233-0604 (fax)
Family Helpline
(800) 932-HOPE

WEST VIRGINIA
Laurie McKeon, Coordinator
Team for West Virginia
Children
824 Fifth Avenue, Suite 208
Huntington, WV 25717
(304) 523-9587
(304) 523-9595 (fax)

WISCONSIN

Sally Casper,
Executive Director
Committee for Prevention of
Child Abuse and Neglect
214 N. Hamilton Street
Madison, WI 53703
(608) 256-3374
(608) 256-3378 (fax); call first

Jackie Maggiore
Executive Director
The Parenting Network
1717 S. Twelfth Street
Suite 101
Milwaukee, WI 53204
(414) 671-5575
(414) 671-1750 (fax)
Parent Stressline (414) 671-0566

NATIONAL COMMITTEE TO PREVENT CHILD ABUSE

ALABAMA

Glenda Trotter, Exec. Director
Greater AL Chapter, NCPCA
AL Council on Child Abuse Inc
P.O. Box 230904
2101 Eastern Boulevard
Suite 26
Montgomery, AL 36123-0904
(334) 271-5105
(334) 271-4349 (fax)
HandsNet: HN4192

Joe Dean, President
Greater AL Chapter, NCPCA
AL Council on Child Abuse Inc
P.O. Box 848
Opelika, AL 36803-0848
(334) 749-5631
(334) 749-5857 (fax)

Naomi Griffith, Exec. Director
N. AL Chapter, NCPCA
Parents and Children Together
P.O. Box 1247
613 Lafayette NE
Decatur, AL 35601
(205) 355-7252
(205) 351-0558 (fax)

Carol Bolding, President
N. Alabama Chapter, NCPCA
Parents and Children Together
P.O. Box 1247
Decatur, AL 35602
(205) 355-7252
(205) 351-0558 (fax)

ALASKA

Elizabeth Forrer, Exec. Dir,
South Central Alaska Chapter,
NCPCA
Anchorage Center for Families
3745 Community Park Loop
Suite 102
Anchorage, AK 99508-3466
(907) 276-4994
(907) 276-6930 (fax)
E-mail: acf@aonline.com

Joe Sonderleiter, President
South Central Alaska Chapter,
NCPCA
670 W. Fireweed Lane
Anchorage, AK 99503
(907) 265-4912
(907) 265-4928 (fax)

Steve Krause, Exec. Director
Fairbanks AK Chapter, NCPCA
Resource Center for Parents and
Children
1401 Kellum Street
Fairbanks, AK 99701
(907) 456-2866
(907) 451-8125 (fax)

Christine Vaughan, President
Fairbanks AK Chapter, NCPCA
Resource Center for Parents
and Children
1401 Kellum Street
Fairbanks, AK 99701
(907) 456-2866
(907) 451-8125 (fax)

ARIZONA

Carole Brazsky, Exec. Director
Arizona Chapter, NCPCA
P.O. Box 63921
Phoenix, AZ 85082-3921
(602) 969-2308
(602) 969-9277 (fax)

Deb Littler, President
Arizona Chapter, NCPCA
c/o Child Crisis Center
P.O. Box 4114
Mesa, AZ 85211
(602) 969-2308
(602) 969-9277 (fax)

CALIFORNIA

Julie Christine, Exec. Director
California Chapter, NCPCA
CA Consortium to Prevent
Child Abuse
926 J Street, Suite 717
Sacramento, CA 95814-2707
(916) 498-8481
(916) 498-0825 (fax)
HandsNet: HN2300
E-mail: ccpca@ix.netcom.com

Cynthia Remmers, President
California Chapter, NCPCA
CA Consortium to Prevent
Child Abuse
c/o Orrick, Herrington &
Sutclifse
400 Capital
Sacramento, CA 95814
(916) 329-7909

COLORADO

Bert Singleton, Exec. Director
Colorado Chapter, NCPCA
Colorado Coalition for the
Protection of Children
950 S. Cherry, Suite 312
Denver, CO 80222
(303) 759-2383
(303) 782-0850 (fax)

Linda Puckett, President
Colorado Chapter, NCPCA
Colorado Coalition for the
Protection of Children
950 S. Cherry, Suite 312
Denver, CO 80222
(303) 782-9337
(303) 782-0850 (fax)

CONNECTICUT

Jane Bourns, Director
Connecticut Chapter, NCPCA
Connecticut Center for
Prevention of Child Abuse
Wheeler Clinic
91 Northwest Drive
Plainville, CT 06062
(860) 747-6801, ext. 244
(860) 793-3520 (fax)
E-mail: ccpca@connix.com

Ronald Bucchi, Chairperson
Connecticut Chapter, NCPCA
Connecticut Center for
Prevention of Child Abuse
Hyde & Bucchi
200 Fisher Drive
Avon Park North
Avon, CT 06001
(860) 678-0155
(860) 676-0213 (fax)

DELAWARE

Karen de Rasmo/JoAnne Kasses
Interim Co-Directors
Delaware Chapter, NCPCA
Delawareans United to Prevent
Child Abuse
Tower Office Park
240 N. James Street, Suite 103
Newport, DE 19804
(302) 996-5444
(302) 996-5425 (fax)
HandsNet: HN2120
E-mail: dupca@aol.com

Gay Lynch, President
Delaware Chapter, NCPCA
Delawareans United to Prevent
Child Abuse
Tower Office Park
240 N. James Street, Suite 103
Newport, DE 19804
(302) 996-5444
(302) 996-5425 (fax)

DISTRICT OF COLUMBIA

Barbara Lautman, Exec.Dir.
Washington, D.C. Chapter,
NCPCA
D.C. Hotline, Inc.
P.O. Box 57194
1400 - 20th Street NW
Washington, DC 20037
(202) 223-0020
(202) 296-4046 (fax)

Robert Yerman, President
Washington, D.C. Chapter,
NCPCA
D.C. Hotline, Inc.
9100 Falls Road
Potomac, MD 20854
(202) 822-4152

FLORIDA

Stephanie Meincke, Exec. Dir.
Florida Chapter, NCPCA
The Family Source
2728 Pablo Street, Suite B
Tallahassee, FL 32308
(904) 488-5437
(904) 921-0322 (fax)
E-mail:
familysource@nettally.com

Mary Oldiges, President
Florida Chapter, NCPCA
c/o Family Resource Center
9500 S. Dadeland Boulevard
Suite 350
Miami, FL 33156
(305) 670-7005
(305) 670-7009 (fax)

GEORGIA

Sandra Wood, Exec. Director
Georgia Chapter, NCPCA
GA Council on Child Abuse Inc
1375 Peachtree Street, N.E.
Suite 200
Atlanta, GA 30309
(404) 870-6565
(404) 870-6541 or 6587 (fax)
HandsNet: HN1537
Website: www.gcca.org

Paul Bowers, President
Georgia Chapter, NCPCA
GA Council on Child Abuse Inc
c/o GA Power Company
P.O. Box 4545
Atlanta, GA 30302
(404) 526-7386
(404) 526-6877 (fax)

HAWAII

Charles Braden, Exec. Director
Hawaii Chapter, NCPCA
Prevent Child Abuse Hawaii
1575 S. Beretania Street
Suite 202
Honolulu, HI 96826
(808) 951-0200
(808) 941-7004 (fax)
E-mail: pcah@aloha.com

Wayne Suehisa, President
Hawaii Chapter, NCPCA
Prevent Child Abuse Hawaii
2880 Kilihau Street
Honolulu, HI 96819
(808) 836-0888
(808) 834-0652 (fax)

ILLINOIS

Don Schlosser, Exec. Director
Illinois Chapter, NCPCA
Prevent Child Abuse Illinois
528 S. 5th Street, Suite 211
Springfield, IL 62701
(217) 522-1129
(217) 522-0655 (fax)

Diana Stroud, President
Illinios Chapter, NCPCA
Prevent Child Abuse Illinois
75 Lincoln Court
Morton, IL 61550
(309) 674-4125
(309) 674-7029 (fax)

Roy Harley, Executive Director
Quad Cities Affiliate, NCPCA
Child Abuse Council
525 - 16th Street
Moline, IL 61265
(309) 764-7017
(309) 757-8554 (fax)
HandsNet: HN4040
E-mail: harley@revealed.net

Larry McCallum, President
Quad Cities Affiliate, NCPCA
Child Abuse Council
1214 Pinehill Road
Bettendorf, IL 52722
(309) 794-7373 or 7300

INDIANA

Andie Marshall, Exec. Director
Indiana Chapter, NCPCA
IN Chapter for Prevention of
Child Abuse
One Virginia Avenue, Suite 401
Indianapolis, IN 46204
(317) 634-9282
(317) 634-9295 (fax)
HandsNet: HN1700

Rebecca Goss, President
Indiana Chapter, NCPCA
IN Chapter for Prevention of
Child Abuse
c/o Eli Lilly & Company
Lilly Corporate Center
Drop Code 1215
Indianapolis, IN 46285
(317) 276-2703
(317) 276-9152 (fax)

IOWA

Steve Scott, Executive Director
Iowa Chapter, NCPCA
3829 - 71st Street, Suite A
Des Moines, IA 50322
(515) 252-0270
(515) 252-0829 (fax)
E-mail: iowancpca@aol.com

Bill Ketch, President
Iowa Chapter, NCPCA
1006 N. "C" Street
Indianola, IA 50125
(515) 246-4068 or 4000
(515) 246-4068 (fax)

KANSAS

Robert L. Hartman, Exec. Dir.
Kansas Chapter, NCPCA
KS Children's Service League
1365 N. Custer Street
P.O. Box 517
Wichita, KS 67201
(316) 942-4261
(316) 943-9995 (fax)

Gwen Sevart, President
Kansas Chapter, NCPCA
KS Children's Service League
9211 Lakepoint
Wichita, KS 67226
(316) 262-6834

Team Leader
Prevention & Early Intervention
Kansas Chapter, NCPCA
KS Children's Service League
1365 N. Custer Street
P.O. Box 517
Wichita, KS 67201
(316) 942-4261
(316) 943-9995 (fax)

KENTUCKY

Jill Seyfred, Executive Director
Kentucky Chapter, NCPCA
Kentucky Council on
Child Abuse, Inc.
2401 Regency Road, Suite 104
Lexington, KY 40503
(606) 276-1299 or 1399
(606) 277-1782 (fax)

Gregory Schaaf, President
Kentucky Chapter, NCPCA
KY Council on Child Abuse Inc
c/o Greenebaum, Doll &
McDonald
P.O. Box 1808
1400 Vine Center Tower
Lexington, KY 40593-1637
(606) 288-4621
(606) 255-2742 (fax)

LOUISIANA

Marketa Garner, Exec. Director
Louisiana Chapter, NCPCA
Louisiana Council on Child
Abuse, Inc.
2351 Energy Drive, Suite 1010
Baton Rouge, LA 70808
(504) 925-9520
(504) 926-1319 (fax)
HandsNet: HN1788

Helen Pope, Chairperson
Louisiana Chapter, NCPCA
Louisiana Council on Child
Abuse, Inc.
P.O. Box 40990
Baton Rouge, LA 70835-0990
(504) 928-1160
(504) 928-1161 (fax)

MAINE

Liz Kuhlman, Exec. Director
Franklin County ME Chapter,
NCPCA
Franklin County Children's
Task Force
69 N. Main Street
Farmington, ME 04938
(207) 778-6960
(207) 778-0171 (fax)

Suc Taylor, Chairperson
Franklin County ME Chapter,
NCPCA
Franklin County Children's
Task Force
P.O. Box 500
W. Farmington, ME 04992
(207) 778-9442

Lucky Hollander, Exec. Dir.
Greater Maine Chapter,
NCPCA
ME Assn. of CAN Councils
P.O. Box 912
211 Cumberland Avenue
Portland, ME 04104
(207) 874-1120
(207) 874-1124 (fax)
HandsNet: HN1113

Sheila Lovell, President
Greater Maine Chapter,
NCPCA
ME Assn.of CAN Councils
c/o Penquis CAP Council
One Summer Street
Dover Foxcroft, ME 04426
(207) 564-7118
(207) 564-2218 (fax)

Marilyn Staples, Exec. Director
York County Chapter, NCPCA
York County Child Abuse &
Neglect Council, Inc.
0 Dental Avenue, P.O. Box 568
Biddeford, ME 04005
(207) 284-1337
(207) 284-1593 (fax)

Bill Hager, President
York County Chapter, NCPCA
York County Child Abuse &
Neglect Council, Inc.
c/o St. Louis Child Care
P.O. Box 645
116 Hill Street
Biddeford, ME 04005
(207) 282-3790

MARYLAND

Gloria Goldfaden, Exec. Dir.
Maryland Chapter, NCPCA
People Against Child Abuse Inc
2530 Riva Road, Suite 3
Annapolis, MD 21401
(410) 841-6599
(410) 224-3725 (fax)

Michael Reichel, M.D.,
President
Maryland Chapter, NCPCA
People Against Child Abuse Inc
7801 York Road, Suite 101
Towson, MD 21204
(410) 821-2810
(410) 821-2804 (fax)

MASSACHUSETTS

Jetta Bernier, Exec. Director
Massachusetts Chapter, NCPCA
Massachusetts Committee for
Children and Youth
14 Beacon Street, Suite 706
Boston, MA 02108
(617) 742-8555
(617) 742-7808 (fax)
HandsNet: HN1126

Eli Newberger, President
Massachusetts Chapter, NCPCA
Massachusetts Committee for
Children and Youth
c/o The Children's Hospital
300 Longwood Avenue
Boston, MA 02115
(617) 355-7982
(617) 355-7979 (fax)
E-mail:
newberger@al.tch.harvard.edu

MICHIGAN

Jean Smith, Executive Director
Michigan Contact
P.O. Box 12096
Lansing, MI 48901
(517) 332-0482

MINNESOTA

Roy Garza, Executive Director
Minnesota Chapter, NCPCA
450 N. Syndicate Street
Suite 290
St. Paul, MN 55104
(612) 641-1568
(612) 641-0404 (fax)

Don Russell, President
Minnesota Chapter, NCPCA
1099 S. Snelling
St. Paul, MN 55116
(612) 582-3630
(612) 582-3680 (fax)

MISSISSIPPI

Donna McLaurin, Exec. Dir.
Mississippi Chapter, NCPCA
Exchange Club Parent/Child
Ctr. 2906 N. State, Suite 200
Jackson, MS 39216
(601) 366-0025
(601) 366-0073 (fax)

Jane Emling, Chairperson
Mississippi Chapter, NCPCA
Exchange Club Parent/Child
Center
1931 Cherokee Drive
Jackson, MS 39211-6509
(601) 362-3995
(601) 366-0073 (fax)

MISSOURI

Lucia Erickson-Kincheloe
Executive Director
Missouri Chapter, NCPCA
Missouri Committee to Prevent
Child Abuse
308 E. High Street, Suite 303
Jefferson City, MO 65101
(573) 634-5223
(573) 635-8499 (fax)
HandsNet: HN2469

Dwain Hovis, President
Missouri Chapter, NCPCA
Missouri Committee to Prevent
Child Abuse
c/o Citibank EBT Services
915 SW Boulevard, Suite L
Jefferson City, MO 65109
(573) 634-2724
(573) 634-3407 (fax)

MONTANA
Jeanne Kemmis
Executive Director
Montana Chapter, NCPCA
Montana Council for Families
P.O. Box 7533
127 E. Main, Suite 209
Missoula, MT 59807
(406) 728-9449
(406) 728-9459 (fax)
HandsNet: HN1780

Jeanne Kemmis, Exec. Director
Jessica Stickney, President
Montana Chapter, NCPCA
Montana Council for Families
2206 Main Street
Miles City, MT 59301
(406) 232-1100
(406) 232-0799, Attn: Dr. Stickney (fax)

NEVADA
Dr. Paula Ford, Exec. Director
Nevada Chapter, NCPCA
We Can, Inc.
3441 W. Sahara, Suite C-3
Las Vegas, NV 89102
(702) 368-1533
(702) 368-1540 (fax)
HandsNet: HN1699

Russell Shoemaker, President
Nevada Chapter, NCPCA
We Can, Inc.
Las Vegas Metro Police Dept.
8265 Hidden Crossing Lane
Las Vegas, NV 89129
(702) 438-3495
(702) 229-3073 (fax)

NEW HAMPSHIRE
Monique Devine, Acting Dir.
NH Chapter, NCPCA
New Hampshire Task Force to Prevent Child Abuse
P.O. Box 607, 44 Warren Street
Concord, NH 03302
(603) 225-5441
(603) 228-5322 (fax)
E-mail: tsmdevine@aol.com

Kevin Hamilton, President
NH Chapter, NCPCA
New Hampshire Task Force to Prevent Child Abuse
c/o Porter, McGee PR
1001 Elm Street
Manchester, NH 03101
(603) 669-8865
(603) 669-8025 (fax)

NEW JERSEY
Sharon Copeland, Exec. Dir.
New Jersey Chapter, NCPCA
Prevent Child Abuse NJ, Inc.
35 Halsey Street, Suite 300
Newark, NJ 07102-3031
(201) 643-3710
(201) 643-9222 (fax)
HandsNet: HN1874

Maura Somers Dughi, President
New Jersey Chapter, NCPCA
Prevent Child Abuse NJ, Inc.
525 Valley Road
Watchung, NJ 07060
(201) 643-3710
(908) 668-4321 (fax)

NEW MEXICO
Lori Campbell, Exec. Director
New Mexico Chapter, NCPCA
Prevent Child Abuse Santa Fe
P.O. Box 15082
Santa Fe, NM 87506
(505) 471-6909
(505) 983-2492 (fax)

Trish Steindler, President
New Mexico Chapter, NCPCA
Prevent Child Abuse Santa Fe
P.O. Box 15082
Santa Fe, NM 87506
(505) 471-6909
(505) 983-1583 (fax)

NEW YORK
James Cameron, Exec. Director
National Chapter, NCPCA
NY Committee to Prevent Child Abuse: NY State
134 S. Swan Street
Albany, NY 12210
(518) 445-1273
(518) 436-5889 (fax)
HandsNet: HN1657
E-mail: ncpcanys@aol.com
Website:
http://child.cornell.edu/ncpca/home.html

William Hayes, President
New York Chapter, NCPCA
National Committee to Prevent Child Abuse: NY State
Bassett Health Care
Atwell Road
Cooperstown, NY 13326
(607) 547-3456

NORTH CAROLINA
Jennifer Tolle, Exec. Director
NC Chapter, NCPCA
Prevent Child Abuse NC
3344 Hillsborough Street
Suite 100D
Raleigh, NC 27607
(919) 829-8009
(919) 832-0308 (fax)
HandsNet: HN2200
Website:
www.pagecreator.com/~pca

Lynn Lewis, President
NC Chapter, NCPCA
Prevent Child Abuse NC
2140 Rolston Drive
Charlotte, NC 27207
(704) 347-2746

NORTH DAKOTA
Kathy Mayer, Exec. Director
North Dakota Chapter, NCPCA
ND Committee to Prevent Child Abuse
P.O. Box 1213
418 E. Rosser, Suite 303
Bismarck, ND 58502-1213
(701) 223-9052
(701) 255-1904 (fax)

Jenny Buell, President
North Dakota Chapter, NCPCA
ND Committee to Prevent Child Abuse
1231 E. Highland Acres Road
Bismarck, ND 58501
(701) 255-7399
(701) 255-7167 (fax)

OHIO
Debbie Sendek, Exec. Director
Ohio Chapter, NCPCA
OH Committee to Prevent Child Abuse
Timken Hall, Suite 130
700 Children's Drive
Columbus, OH 43205
(614) 722-6800
(614) 722-5510 (fax)
E-mail: dsendek@chi.osu.edu

Sandra Mueller, Chairperson
Ohio Chapter, NCPCA
OH Committee to Prevent Child Abuse
10424 Wellington Boulevard
Powell, OH 43065
(614) 766-6743

OKLAHOMA
Debbie Richardson, Exec. Dir.
Oklahoma Chapter, NCPCA
OK Committee to Prevent Child Abuse
Citizen's Tower, Suite 340
2200 Classen Boulevard
Oklahoma City, OK 73106
(405) 525-0688
(405) 525-0689 (fax)
E-mail: ocpca@juno.com

Rev. Mike Albert, President
Oklahoma Chapter, NCPCA
OK Committee to Prevent Child Abuse
c/o Yale Avenue Christian Church
3616 S. Yale Avenue
Tulsa, OK 74135
(918) 747-1304
(918) 747-7175 (fax)

PENNSYLVANIA
Terry Ferrier, Interim Director
Central PA Chapter, NCPCA
Child Abuse Prevention Committee of Central PA
P.O. Box 7664
1917B Olde Homestead Lane
Lancaster, PA 17604
(717) 393-4511
(717) 393-6801 (fax)

Jennifer Goldbach, President
Central PA Chapter, NCPCA
Child Abuse Prevention Committee of Central PA
901 Jade Avenue
Lancaster, PA 17621
(717) 285-5848

Christine Linville, Interim Dir.
Greater Philadelphia Chapter, NCPCA
Child Abuse Prevention Committee of Greater PA
260 S. Broad Street, 18th Floor
Philadelphia, PA 19102
(215) 985-6893
(215) 864-1085 (fax)

Yvonne Ruiz, President
Greater Philadelphia Chapter, NCPCA
Child Abuse Prevention Committee of Greater PA
1738 Pine Street, 4A
Philadelphia, PA 19103
(215) 686-8067

RHODE ISLAND
Ted Whiteside, Exec. Director
Rhode Island Chapter, NCPCA
RI Committee to Prevent Child Abuse
500 Prospect Street
Pawtucket, RI 02860
(401) 728-7920
(401) 724-5850 (fax)

Joe Murray, President
Rhode Island Chapter, NCPCA
RI Committee to Prevent Child Abuse
86 King Phillip Court
Warwick, RI 02886
(401) 732-1224, ext. 354

SOUTH CAROLINA
Janice Bolin, Executive Director
Low Country SC Chapter, NCPCA
Exchange Club Center for Prevention of Child Abuse
5055 Lackawanna Boulevard
North Charleston, SC 29406-4522
(803) 747-1339
(803) 529-3202 (fax)

Lee Stubblefield, President
Low Country SC Chapter, NCPCA
Exchange Club Center for Prevention of Child Abuse
3 Carriage Lane
Charleston, SC 29407
(803) 766-5112
(803) 766-1389 (fax)

Beebe James, Exec. Director
Midlands Chapter, NCPCA
Council on Child Abuse and Neglect
1800 Main Street, Suite 3A
Columbia, SC 29201
(803) 733-5430
(803) 779-7803 (fax)

Sidney Wait, President
Midlands Chapter, NCPCA
Council on Child Abuse and Neglect
c/o Continuum of Care for Emotionally Handicapped Children
220 Stoneridge Drive, Suite 300
Columbia, SC 29210
(803) 253-6272

Russell Smith, Exec. Director
Piedmont Chapter, NCPCA
Piedmont Council for Prevention of Child Abuse
301 University Ridge
Suite 5100
Greenville, SC 29601-3671
(864) 467-7680
(864) 467-7699 (fax)

Jeff Ezell, President
Piedmont Chapter, NCPCA
Piedmont Council for Prevention of Child Abuse
c/o Gibbes & Clarkson, PA
330 Coffee Street
Greenville, SC 29616
(864) 271-9580

TENNESSEE

Lynne Luther, Exec. Director
Tennessee Chapter, NCPCA
Child Abuse Prevention of TN
3010 Ambrose Avenue
Nashville, TN 37207
(615) 227-2273
(615) 227-6846 (fax)

Ed Van Voorhees, President
Tennessee Chapter, NCPCA
Child Abuse Prevention of TN
c/o United Warehouse, Inc.
713 Overton Park
Nashville, TN 37215
(615) 254-3326

TEXAS

Wendell Teltow, Exec. Director
Texas Chapter, NCPCA
TX Committee to Prevent Child
12701 Research, Suite 303
Austin, TX 78759
(512) 250-8438
(512) 250-8733 (fax)

Grace Rank, President
Texas Chapter, NCPCA
TX Committee to Prevent Child
3446 Flour Bluff Road
Corpus Cristi, TX 78418
(512) 289-6501, ext. 110
(512) 289-1867 (fax)

UTAH

Executive Director
Utah Chapter, NCPCA
UT Committee to Prevent Child Abuse
40 E. South Temple,
Suite 350-12
Salt Lake City, UT 84111-1003
(801) 532-3404
(801) 359-3662 (fax)
HandsNet: HN1988
E-mail: ewitker@bitcorp.net
Website: www.bitcorp.net/ucpca

Jeff Hansen, President
Utah Chapter, NCPCA
UT Committee to Prevent Child Abuse
Murdock Travel Management
5383 S. 900 East
Salt Lake City, UT 84117
(801) 267-5831

VERMONT

Linda Johnson, Exec. Director
Vermont Chapter, NCPCA
Prevent Child Abuse Vermont
P.O. Box 829
141 Main Street
Montpelier, VT 05601
(802) 229-5724
(802) 223-5567 (fax)

Bob Donnola, Vice-President
Vermont Chapter, NCPCA
21 Juniper Ridge
Shelburne, VT 05482
(802) 985-1149
(802) 985-2497 (fax)

Gilman Rood, Vice-President
Vermont Chapter, NCPCA
161 Austin Drive
Burlington, VT 05401
(802) 229-5724

VIRGINIA

Barbara Rawn, Exec. Director
Virginia Chapter, NCPCA
Prevent Child Abuse Virginia
P.O. Box 12308
219 E. Broad Street, 10th Floor
Richmond, VA 23241
(804) 775-1777
(804) 775-0019 (fax)
HandsNet: HN1774

Michard Sterret, President
Virginia Chapter, NCPCA
Prevent Child Abuse Virginia
c/o Director, North Hampton County Social Services
P.O. Box 568
Easterville, VA 23347
(804) 678-5153

WASHINGTON

Executive Director
Washington Chapter, NCPCA
Child Abuse Prevention Association of Washington
c/o Board of Directors, CAPAW
Business Office/CAPR
6314 W. 19th Street, Suite 3
Tacoma, WA 98466

Bruce Garner, President
Washington Chapter, NCPCA
CAP Association of Washington
c/o Department of Corrections
1801 Grove Street, Unit D
Marysville, WA 98270
(360) 658-2164

WEST VIRGINIA
Lauri McKeown, Coordinator
West Virginia Contact
P.O. Box 1653
Huntington, WV 25717
(304) 523-9587
(304) 523-9595 (fax)

WISCONSIN
Sally Casper, Exec. Director
Wisconsin Chapter, NCPCA
WI Committee to Prevent Child Abuse
214 N. Hamilton
Madison, WI 53703
(608) 256-3374
(608) 256-3378 (fax)
HandsNet: HN4758
E-mail: wcpca@juno.com

Allen Jacobsen, President
Wisconsin Chapter, NCPCA
WI Committee to Prevent Child Abuse
8001 Excelsior Drive
Madison, WI 53717
(608) 827-6400

WYOMING
Rose Kor, Executive Director
Wyoming Chapter, NCPCA
Prevent Child Abuse Wyoming
1120 Logan Avenue
Cheyenne, WY 82001
(307) 637-8622
(307) 637-8622 (fax)
E-mail: pcawyo@juno.com

Jean Phelan, President
Wyoming Chapter, NCPCA
Prevent Child Abuse Wyoming
1404 E. 17th Street
Cheyenne, WY 82001
(307) 637-6162

Appendix 5

FBI Field Offices

Alabama
Federal Bureau of Investigation
2121 8th Avenue North, Room 1400
Birmingham, AL 35203-2396
Telephone: (205) 326-6166

Federal Bureau of Investigation
One St. Louis Centre
1 St. Louis Street
Mobile, AL 36602
Telephone: (334) 438-3674

Alaska
Federal Bureau of Investigation
101 East Sixth Avenue
Anchorage, AK 99501-2524
Telephone: (907) 276-4441

Arizona
Federal Bureau of Investigation
201 East Indianola, Suite 400
Phoenix, AZ 85012-2080
Telephone: (602) 279-5511

Arkansas
Federal Bureau of Investigation
10825 Financial Centre Parkway, Suite 200
Little Rock, AR 72211-3552
Telephone: (501) 221-9100

California
Federal Bureau of Investigation
Federal Office Building
11000 Wilshire Boulevard, Suite 1700
Los Angeles, CA 90024-3672
Telephone: (310) 477-6565

Federal Bureau of Investigation
4500 Orange Grove Avenue
Sacramento, CA 95841-4025
Telephone: (916) 481-9110

Federal Bureau of Investigation
9797 Aero Drive
San Diego, CA 92123-1800
Telephone: (619) 565-1255

Federal Bureau of Investigation
450 Golden Gate Avenue
San Francisco, CA 94102-9523
Telephone: (415) 553-7400

Colorado
Federal Bureau of Investigation
Federal Office Building
1961 Stout Street, Suite 1823
Denver, CO 80294-1823
Telephone: (303) 629-7171

Connecticut
Federal Bureau of Investigation
Federal Office Building
150 Court Street, Room 535
New Haven, CT 06510-2020
Telephone: (203) 777-6311

Delaware
All queries should be directed to the FBI field office in Baltimore, Maryland.

Florida
Federal Bureau of Investigation
7820 Arlington Expressway, Suite 200
Jacksonville, FL 32211-7499
Telephone: (904) 721-1211

Federal Bureau of Investigation
16320 Northwest Second Avenue
North Miami Beach, FL 33169
Telephone: (305) 944-9101

Florida - continued
Federal Bureau of Investigation
500 Zack Street, Room 610
Tampa, FL 33602-3917
Telephone: (813) 273-4566

Georgia
Federal Bureau of Investigation
2635 Century Parkway Northeast, Suite 400
Atlanta, GA 30345-3112
Telephone: (404) 679-9000

Hawaii
Federal Bureau of Investigation
300 Ala Moana Boulevard, Room 4307
Honolulu, HI 96850-0053
Telephone: (808) 521-1411

Idaho
All queries should be directed to the FBI field office in Salt Lake City, Utah.

Illinois
Federal Bureau of Investigation
E.M. Dirksen Federal Office Building
219 South Dearborn Street, Room 905
Chicago, IL 60604-1702
Telephone: (312) 431-1333

Federal Bureau of Investigation
400 West Monroe Street, Suite 400
Springfield, IL 62704-1800
Telephone: (217) 522-9675

Indiana
Federal Bureau of Investigation
575 North Pennsylvania Street, Room 679
Indianapolis, IN 46204-1524
Telephone: (317) 639-3301

Iowa
All queries should be directed to the FBI field office in Omaha, Nebraska.

Kansas
All queries should be directed to the FBI field office in Kansas City, Missouri.

Kentucky
Federal Bureau of Investigation
600 Martin Luther King Place, Room 500
Louisville, KY 40202-2231
Telephone: (502) 583-3941

Louisiana
Federal Bureau of Investigation
1250 Poydras Street, Suite 2200
New Orleans, LA 70113-1829
Telephone: (504) 522-4671

Maine
All queries should be directed to the FBI field office in Boston, Massachusetts.

Maryland
Federal Bureau of Investigation
7142 Ambassador Road
Baltimore, MD 21244-2754
Telephone: (410) 265-8080

Massachusetts
Federal Bureau of Investigation
One Center Plaza, Suite 600
Boston, MA 02108
Telephone: (617) 742-5533

Michigan
Federal Bureau of Investigation
Federal Office Building
477 Michigan Avenue
Detroit, MI 48226
Telephone: (313) 965-2323

Minnesota
Federal Bureau of Investigation
111 Washington Avenue South, Suite 1100
Minneapolis, MN 55401-2176
Telephone: (612) 376-3200

Mississippi
Federal Bureau of Investigation
100 West Capitol Street, Room 1553
Jackson, MS 39269
Telephone: (601) 948-5000

Missouri
Federal Bureau of Investigation
U.S. Courthouse
811 Grand Avenue, Room 300
Kansas City, MO 64106-1926
Telephone: (816) 221-6100

Federal Bureau of Investigation
1520 Market Street, Room 2704
St. Louis, MO 63103-2686
Telephone: (314) 589-2500

Montana
All queries should be directed to the FBI field office in Salt Lake City, Utah.

Nebraska
Federal Bureau of Investigation
10755 Burt Street
Omaha, NE 68114-2000
Telephone: (402) 493-8688

Nevada
Federal Bureau of Investigation
700 East Charleston Boulevard
Las Vegas, NV 89104-1545
Telephone: (702) 385-1281

New Hampshire
All queries should be directed to the FBI field office in Boston, Massachusetts.

New Jersey
Federal Bureau of Investigation
1 Gateway Center
Market Street
Newark, NJ 07102-9889
Telephone: (201) 622-5613

New Mexico
Federal Bureau of Investigation
415 Silver Street Southwest, Suite 300
Albuquerque, NM 87102
Telephone: (505) 224-2000

New York
Federal Bureau of Investigation
445 Broadway, Fifth Floor
Albany, NY 12207-2963
Telephone: (518) 465-7551

Federal Bureau of Investigation
One FBI Plaza
Buffalo, NY 14202-2698
Telephone: (716) 856-7800

Federal Bureau of Investigation
26 Federal Plaza
New York, NY 10278-0004
Telephone: (212) 384-1000

North Carolina
Federal Bureau of Investigation
400 South Tyron Street, Suite 900
Charlotte, NC 28285-0001
Telephone: (704) 377-9200

North Dakota
All queries should be directed to the FBI field office in Minneapolis, Minnesota.

Ohio
Federal Bureau of Investigation
550 Main Street, Room 9000
Cincinnati, OH 45273-8501
Telephone: (513) 421-4310

Federal Bureau of Investigation
Federal Office Building
1240 East Ninth Street, Room 3005
Cleveland, OH 44199-9912
Telephone: (216) 522-1400

Oklahoma
Federal Bureau of Investigation
50 Penn Place, Suite 1600
Oklahoma City, OK 73118-1886
Telephone: (405) 842-7471

Oregon
Federal Bureau of Investigation
Crown Plaza
1500 Southwest First Avenue
Portland, OR 97201-5828
Telephone: (503) 224-4181

Pennsylvania
Federal Bureau of Investigation
600 Arch Street, Eighth Floor
Philadelphia, PA 19106
Telephone: (215) 418-4500

Federal Bureau of Investigation
U.S. Post Office Building
700 Grant Street, Suite 300
Pittsburgh, PA 15219-1906
Telephone: (412) 471-2000

Rhode Island
All queries should be directed to the FBI field office in Boston, Massachusetts.

South Carolina
Federal Bureau of Investigation
1835 Assembly Street, Room 1357
Columbia, SC 29201-2430
Telephone: (803) 254-3011

South Dakota
All queries should be directed to the FBI field office in Minneapolis, Minnesota.

Tennessee
Federal Bureau of Investigation
710 Locust Street, Suite 600
Knoxville, TN 37902-2537
Telephone: (423) 544-0751

Federal Bureau of Investigation
225 North Humphreys Boulevard
Memphis, TN 38120-2107
Telephone: (901) 747-4300

Texas
Federal Bureau of Investigation
1801 North Lamar, Room 300
Dallas, TX 75202-1795
Telephone: (214) 720-2200

Federal Bureau of Investigation
700 East San Antonio Avenue, Suite C-600
El Paso, TX 79901-7020
Telephone: (915) 533-7451

Federal Bureau of Investigation
2500 East TC Jester, Room 200
Houston, TX 77008-1300
Telephone: (713) 868-2266

Federal Bureau of Investigation
615 East Houston Street, Room 200
San Antonio, TX 78205-9998
Telephone: (210) 225-6741

Utah
Federal Bureau of Investigation
257 East 200 Street South, Suite 1200
Salt Lake City, UT 84111-2048
Telephone: (801) 579-1400

Vermont
All queries should be directed to the FBI field office in Albany, New York.

Virginia
Federal Bureau of Investigation
150 Corporate Boulevard
Norfolk, VA 23502-4999
Telephone: (757) 455-0100

Federal Bureau of Investigation
111 Greencourt Road
Richmond, VA 23228-4948
Telephone: (804) 261-1044

Washington
Federal Bureau of Investigation
915 Second Avenue, Room 710
Seattle, WA 98174-1096
Telephone: (206) 622-0460

Washington, D.C.
Federal Bureau of Investigation
Washington Metropolitan Field Office
1900 Half Street SW.
601 4th Street Northwest
Washington, DC 20535-0002
Telephone: (202) 252-7801

West Virginia
All queries should be directed to the FBI field office in Pittsburgh, Pennsylvania.

Wisconsin
Federal Bureau of Investigation
330 East Kilbourn Avenue, Suite 600
Milwaukee, WI 53202-6627
Telephone: (414) 276-4684

Wyoming
All queries should be directed to the FBI field office in Denver, Colorado.

Puerto Rico
Federal Bureau of Investigation
U.S. Courthouse and Federal Office Building
150 Carlos Chardon Avenue, Room 526
Hato Rey, PR 00918-1716
Telephone: (809) 754-6000

Appendix 6

FBI Legal Attaches

Athens
Legal Attache
American Embassy
PSC 108, Box 45
APO AE 09842
Telephone:(011-30-1) 721-2951 ext.447

Bangkok
Legal Attache
American Embassy-Box 67
APO AP 96546
Telephone:(011-66-2) 205-4366

Bern
American Embassy Bern
Jubilaeumstrasse 93
CH 3005 Bern, Switzerland
Telephone:(011-41-31) 357-7011

Bogota
US Embassy-Bogota
Unit #5124-Legat
APO AA 34038
Telephone:(011-57-1) 315-0811 ext. 2575

Bonn
Off. Of the Legal Attache
PSC 117, Box 310
APO AA 09080
Telephone:(011-49-228) 3391

Bonn, Berlin Suboffice
U.S.Embassy Off. Berlin-Legat
PSC 120, Box 1000
APO AE 09265
Telephone:(011-49-30) 238-5174

Bonn, Frankfurt Suboffice
American Consulate-Frankfurt
Office of Legat Attache
PSC 115
APO AE 09213
Telephone:(011-49-69) 7535-3780

Brazilia
Telephone:(55-61) 321-7272

Bridgetown
Legal Attache
American Embassy
Bridgetown, Barbados
FPO AA 34055
Telephone:(246) 436-4950 ext. 2236

Brussels
Legal Attache
LEG/EMB
PSC 82, Box 002
APO AE 09724
Telephone:(011-32-2)
508-2111 ext. 2551,2552

Budapest International Law Enforcement Agency
Budapest 1126
Böszörményi ùt 21
Hungary
Telephone:(011-36-1) 267-4400

Cairo
American Embassy
Unit 64900, Box 39
APO AE 09839-4900
Telephone:(011-202) 355-7371

Canberra
US Embassy
Legat
APO AP 96549
Telephone:(011-61-6) 270-5000 or
5900 evenings, ext. 862,982

Caracas
American Embassy Unit 4966
APO AA 34037
Telephone:(011-58-2) 977-2011

Hong Kong
Legal Liaison Office
American Consulate
PSC 464, Box 30
FPO AP 96522-0002
Telephone:(011-852) 2841-2282
2356, 2348

Interpol
ICPO-Interpol General Secretariat
200 Charles de Gaulle
69006 Lyon, France
Telephone:(011-33-4) 7244-7213

Islamabad
Legal Attache Office
American Embassy
Unit 62219
APO AE 09812-2219
Telephone:(011-92-51) 826-161 ext.2205

Kiev
American Embassy
Department of State-Kiev
Washington D.C. 20521-5850
Telephone:(011-380) 44-244-7345
ext. 237, 247

London
American Embassy
PSC 801 Box 02
FPO AE 09498-4002
Telephone:(011-44-171) 499-9000
ext. 2478, 2479, 2475

Madrid
PSC 61, Box 0001
APO AE 09642
Telephone:(011-34-1) 587-2200

Manila
American Embassy
Legat Attache
FPO AP 96515
Telephone:(011-63-2) 523-1323

Mexico City
American Embassy
P.O. Box 3087
Laredo, Texas 78044-3087
Telephone:(011-52-5) 211-0042
ext. 3700 through 3703

Mexico City, Guadalajara Suboffice
Telephone:(011-52-38) 25-2998

Mexico City, Monterrey Suboffice
Telephone:(011-52-83) 43-2120
ext. 469

Montevideo
Unit 4503
APO AA 34035
Telephone:(011-598-2) 48-77-77
Ask for Marines

Moscow
American Embassy, Moscow
PSC 77, Legat
APO AE 09721
Telephone:(011-7-095) 252-2459
ext. 5222

Ottawa
US Embassy-Canada
P.O. Box 1711
Ogdensburg, N.Y. 13669
Telephone:(613) 238-5335 ext.206

Panama City
American Embassy Panama
Unit 0945
APO AA 34002
Telephone:(011-507) 227-1777
227-1377 evenings

Paris
Paris Embassy(LEG)
PSC 116, A-324
APO AE 09777
Telephone:(011-33-1) 4312-2222
ext. 2400

Pretoria
American Embassy, Pretoria
U.S. Department of State
Washington, D.C. 20521-9300
Telephone:(011-27-12) 342-1048, ext. 2349

Riyadh
American Embassy
AMEMB, Unit 61340
APO AE 09803-1307
Telephone:(011-966) 1488-3800 ext. 1555

Rome
PSC 59, Box 43
APO AE 09624
Telephone:(011-39-6) 4674-2710
2711, 2392

Santiago
Office of the Legal Attache
American Embassy-Santiago
Unit 4131 (Legat)
APO AA 34033
Telephone:(011-56-2) 232-2600
Ask for Marines

Tallinn
American Embassy
PSC 78, Box T
APO AE 09723
Telephone:(011-372-6) 312-021 ext.210

Tel Aviv
US Embassy
Legat
Unit 7228
APO AE 09830
Telephone:(011-9723) 519-7575

Tokyo
American Embassy
Unit 45004, Box 223
APO AE 96337-0001
Telephone:(011-81-3) 3224-5000

Vienna
American Embassy-Vienna
DOS, Legat
Washington D.C. 20521-9900
Telephone:(011-43-1) 31-339

Warsaw
American Embassy-Warsaw
Department of State
Washington D.C. 20521-5010
Telephone: (011-4822) 628-3041
evenings: 628-0638

Appendix 7

Crime Victims Compensation/Assistance State Agencies and Programs

VICTIM COMPENSATION PROGRAMS

ALABAMA
Randy Helms, Executive Director
Alabama Crime Victims Compensation
100 N. Union Street
P.O. Box 1548
Montgomery, AL 36102-1548
Telephone: (334) 242-4007

ALASKA
Susan Browne, Administrator
Department of Public Safety
Violent Crimes Compensation Board
450 Whittier Street, Room 104
Juneau, AK 99811-1200
Telephone: (907) 465-3040

ARIZONA
Rita J. Yorke, Victim Services Coordinator
Criminal Justice Commission
1501 West Washington, Suite 207
Phoenix, Arizona 85007
Telephone: (602) 542-1928

ARKANSAS
Ginger B. Bailey, Director
Crime Victims Reparations Board
323 Center Street, Suite 200
Little Rock, AR 72201
Telephone: (501) 682-1323

VICTIM ASSISTANCE PROGRAMS

ALABAMA
Gilbert (Doug) Miller, Section Chief
Department of Economic and Community Affairs
Law Enforcement Planning Division
401 Adams Avenue
P.O. Box 5690
Montgomery, AL 36103-5690
Telephone: (334) 242-5843

ALASKA
Jayne E. Andreen, Executive Director
Department of Public Safety
Council on Domestic Violence and Sexual Assault
P.O. Box 111200
Juneau, AK 88911-1200
(907) 465-4356

ARIZONA
Lynn Pirkle, Grant Coordinator
Department of Public Safety
2010 West Encanto Blvd.
Phoenix, AZ 85005-6638
Telephone: (602) 223-2465

ARKANSAS
Jerry Duran, Administrator
Department of Finance & Administration
P.O. Box 3278
Little Rock, AR 72203
Telephone: (501) 682-1071

VICTIM COMPENSATION PROGRAMS

CALIFORNIA
Ted Boughton, Deputy Executive Officer
State of California
State Board of Control
P.O. Box 3036
Sacramento, CA 95814
Telephone: (916) 323-3432

COLORADO
Carol Poole, Deputy Director
Division of Criminal Justice
Department of Public Safety
700 Kipling Street, Suite 1000
Denver, CO 80215
Telephone: (303) 239-4446

CONNECTICUT
Carole R. Watkins, Director
Office of Victim Services
Connecticut Judicial Branch
1158 Silas Deane Highway
Wethersfield, CT 06109
Telephone: (860) 529-3089

DELAWARE
Ann L. DelNegro, Executive Director
Violent Crimes Compensation Board
1500 East Newport Pike, Suite 10
Wilmington, DE 19804
Telephpone: (302) 995-8383

DISTRICT OF COLUMBIA
Laura Banks Reed,Director
Crime Victims Compensation Program
515 5th Street, Suite 503
Washington D.C. 20001
Telephone: (202) 879-4216

VICTIM ASSISTANCE PROGRAMS

CALIFORNIA
Kirby Everhart, Chief
Victim Services & Violence Prevention
Office of Criminal Justice Planning
1130 K Street, Suite 300
Sacramento, CA 95814
Telephone: (916) 327-3687

COLORADO
Candace Grosz, VOCA Administrator
Division of Criminal Justice
Department of Public Safety
700 Kipling Street, Suite 1000
Denver, CO 80215
Telephone: (303) 239-5703

CONNECTICUT
Carole R. Watkins, Director
Office of Victim Services
Connecticut Judicial Branch
1158 Silas Deane Highway
Wethersfield, CT 06109
Telephone: (860) 529-3089

DELAWARE
Corrine Pearson, Program Manager
Criminal Justice Council
Carvel State Office Building
820 North French, 4th Floor
Wilmington, DE 19801
Telephone: (302) 577-3697

DISTRICT OF COLUMBIA
Sandra R. Manning, Director
D.C. Office of Grants Management
717 14th Street N.W., Suite 400
Washington, D.C. 20005
Telephone: (202) 727-6537

VICTIM COMPENSATION PROGRAMS

FLORIDA
Mary Vancore, Chief
Division of Victim Services and
Criminal Justice Programs
Office of the Attorney General
Department of Legal Affairs
The Capitol
Tallahassee, FL 32399-1050
Telephone: (904) 414-3301

GEORGIA
Derek L. Marchman, Program Manager
Crime Victim Compensation Program
503 Oak Place, Suite 540
Atlanta, GA 30349
Telephone: (404) 559-4949

HAWAII
Laraine Koga, Administrator
Office of the Attorney General
425 Queen Street, Room 221
Honolulu, HI 96813
Telephone: (808) 586-1282

IDAHO
Mr. Fran Koch, Director
Crime Victims Compensation Bureau
c/o Idaho Industrial Commission
P.O. Box 83720
Boise, ID 83720-0041
Telephone: (208) 334-6070

ILLINOIS
Katherine Parker, Administrator
Illinois Court of Claims
Crime Victims Division
Attorney General's Office
100 W. Randolph, 13th Floor
Chicago, Illinois 60601
Telephone: (312) 814-2581

VICTIM ASSISTANCE PROGRAMS

FLORIDA
Cynthia Rogers, Chief
Division of Victim Services and
Criminal Justice Programs
Office of the Attorney General
Department of Legal Affairs
The Capitol, PL- 01
Tallahassee, FL 32399-1050
Telephone: (904) 414-3300

GEORGIA
John Cook, Grant Manager
Criminal Justice Coordinating Council
503 Oak Place, Suite 540
Atlanta, GA 30349
Telephone: (404) 559-4949

HAWAII
Adrian Kwock, Planning Specialist
Office of the Attorney General
425 Queen Street, Room 221
Honolulu, HI 96813
Telephone: (808) 586-1282

IDAHO
Celia V. Heady, Executive Director
Department of Health & Welfare
Council on Domestic Violence
450 West State Street, 9th Floor
Boise, ID 83720-0036
Telephone: (208) 334-5580

ILLINOIS
Candice M. Kane, Program Supervisor
Criminal Justice Information Authority
120 S. Riverside Plaza, 10th Floor
Chicago, IL 60606
Telephone: (312) 793-8550

VICTIM COMPENSATION PROGRAMS

INDIANA
Gwendolyn Allen, Program Director
Violent Crime Compensation Fund
Criminal Justice Institute
302 West Washington Street, E209
Indianapolis, IN 46204
Telephone: (312) 233-3383

IOWA
Kelly Brodie, Deputy Director
Department of Justice
Crime Victim Assistance Program
Old Historical Building
1125 East Grand Avenue
Des Moines, IA 50319-0238
Telephone: (515) 281-5044

KANSAS
Frank Henderson, Director
KS Crime Victims Compensation Board
700 SW Jackson Street, Suite 400
Topeka, KS 66603-3756
Telephone: (913) 296-2359

KENTUCKY
Jackie Howell, Executive Director
Crime Victim Compensation Board
115 Myrtle Avenue
Frankfort, Kentucky 40601-3113
Telephone: (502) 564-7986

LOUISIANA
Robert Wertz, Program Manager
Louisiana Commission on Law
Enforcement
1885 Wooddale Boulevard, Suite 708
Baton, Rouge, LA 70806-1511
Telephone: (504) 925-1998

VICTIM ASSISTANCE PROGRAMS

INDIANA
Kimberly I. Howell, Program Director
Criminal Justice Institute
302 West Washington Street, E209
Indianapolis, IN 46204
Telephone: (317) 233-3341

IOWA
Virginia Beane, Administrator
Department of Justice
Crime Victim Assistance Program
Old Historical Building
1125 East Grand Avenue
Des Moines, IA 50319-0238
Telephone: (515) 281-5044

KANSAS
Juliene A. Maska, Director
Office of the Attorney General
301 SW 10th Avenue
Topeka, KS 66612-1597
Telephone: (913) 296-2215

KENTUCKY
Donna Langley, VOCA Program Mngr.
Kentucky Justice Cabinet
Bush Building
403 Wapping Street, 2nd Floor
Frankfort, KY 40601
Telephone: (502) 564-7554

LOUISIANA
Rosanna Marino, Program Manager
Louisiana Commission on Law
Enforcement
1885 Wooddale Boulevard, Suite 708
Baton Rouge, LA 70806-1442
Telephone: (504) 925-1757

VICTIM COMPENSATION PROGRAMS

MAINE
Deborah Shaw-Rice, Director
Office of the Attorney General
Crime Victim Compensation Program
State House Station 6
Augusta, ME 04333
Telephone: (297) 626-8589

MARYLAND
Esther Scaljon, Director
Department of Public Safety
and Correctional Services
Criminal Injuries Compensation Board
6776 Resiterstown Road, Suite 313
Baltimore, MD 21215-2340
Telephone: (410) 764-4214

MASSACHUSETTS
Judith E. Beals, Chief
Office of the Attorney General
Victim Compensation Division
One Ashburton Place
Boston, MA 02108-1698
Telephone: (617) 727-2200

MICHIGAN
Michael J. Fullwood, Administrator
Crime Victims Compensation Board
P.O. Box 30026 - 320 South Walnut
Lansing, MI 48909
Telephone: (517) 373-0979

MINNESOTA
Marie Bibus, Executive Director
Crime Victims Reparations Board
Town Square, Suite 100-C
444 Cedar Street
St. Paul, MN 55101-2156
Telephone: (612) 282-6267

VICTIM ASSISTANCE PROGRAMS

MAINE
Jeannette C. Talbot, Administrator
Department of Human Services
Bureau of Social Services
State House Station 11
Augusta, ME 04333
Telephone: (207) 289-5060

MARYLAND
Adrienne Siegel, Assistant Director
Office of Transitional Services
MD Department of Human Resources
311 West Saratoga Street, Room 272
Baltimore, MD 21201-3521
Telephone: (410) 767-7477

MASSACHUSETTS
Alyssa Kazin, Program Specialist
Victim & Witness Assistance Board
Office for Victims Assistance
100 Cambridge Street, Room 1104
Boston, MA 02202
Telephone: (617) 727-5200

MICHIGAN
Leslie O'Reilly
Grants Management Division
Office of Contract Management
P.O. Box 30026 - 320 South Walnut
Lansing, MI 48909
Telephone: (517) 373-1826

MINNESOTA
Emilie Tan-Graf, Grant Administrator
Department of Corrections
1450 Energy Park Drive
Suite 200
St. Paul, MN 55108-5129
Telephone: (612) 642-0221

VICTIM COMPENSATION PROGRAMS

MISSISSIPPI
Sandra K. Morrison, Hearing Officer
Department of Finance and
Administration
Box 267
Jackson, MS 39205
Telephone: (601) 359-6766

MISSOURI
Sandy Wright, Program Manager
Division of Workers' Compensation
Crime Victims Compensation
P.O. Box 504
Jefferson City, MO 65102
Telephone: (573) 526-3511

MONTANA
Dara Lynn Smith, Program Officer
Board of Crime Control Division
Crime Victims Unit
Scott Hart Building
303 North Roberts, 4th Floor
Helena, MT 59620-1408
Telephone: (406) 444-3653

NEBRASKA
Nancy Steeves, Federal Aid Administrator
Crime Victims Reparation Board
Commission on Law Enforcement
and Criminal Justice
P.O. Box 94946
Lincoln, NE 68509
Telephone: (402) 471-2194

NEVADA*
Bryan Nix, Coordinator
Victims of Crime Program
NV Department of Administration
555 E. Washington, Suite 3200
Las Vegas, NV 89101
Telephone: (702) 486-2740

VICTIM ASSISTANCE PROGRAMS

MISSISSIPPI
Ezzard C. Stamps, Program Manager
Department of Public Safety
Division of Public Safety & Planning
401 North West Street, 8th Floor
Jackson, MS 39225-3039
Telephone: (601) 359-7880

MISSOURI
Vicky Scott, Program Specialist
Department of Public Safety
Truman Building, Room 870
P.O. Box 749 - 301 West High St.
Jefferson City, MO 65102-0749
Telephone: (573) 751-4905

MONTANA
Wendy Sturn, Victim Coordinator
Board of Crime Control Division
Scott Hart Building
303 North Roberts, 4th Floor
Helena, MT 59501
Telephone: (406) 444-3604

NEBRASKA
Nancy Steeves, Federal Aid Administrator
Crime Victims Reparation Board
Commission on Law Enforcement
and Criminal Justice
P.O. Box 94946
Lincoln, NE 68509
Telephone: (402) 471-2194

NEVADA
Chris S. Graham, Program Manager
Department of Human Resources
Division of Child & Family Services
2655 Enterprise Road
Reno, NV 89512
Telephone: (702) 688-1628

VICTIM COMPENSATION PROGRAMS

NEW HAMPSHIRE
Susan Paige-Morgan
NH Department of Justice
33 Capitol Street
Concord, NH 03301-6397
Telephone: (603) 271-3658

NEW JERSEY
Jim Casserly
Victims of Crime Compensation Board
50 Park Place, 5th Floor
Newark, NJ 07102
Telephone: (201) 648-2107

NEW MEXICO
Larry Tackman, Director
Crime Victims Reparation Commission
8100 Mountain Road, N.E., Suite 106
Albuquerque, NM 87110
Telephone: (505) 841-9432

NEW YORK
Patricia Poulopoulos, Administrative Officer
New York Crime Victims Board
845 Central Avenue, South 3, Suite 107
Albany, NY 12206
Telephone: (518) 457-8063

NORTH CAROLINA
Gary B. Eichelberger, Director
Victims Compensation Commission
Department of Crime Control and
Public Safety
P.O. Box 29588 - 512 North Salisbury St.
Raleigh, NC 27611-7687
Telephone: (919) 733-7974

VICTIM ASSISTANCE PROGRAMS

NEW HAMPSHIRE
Gale Dean
NH Department of Justice
33 Capitol Street
Concord, NH 03301-6397
Telephone: (603) 271-7987

NEW JERSEY
Kathleen A. Kauker-Lawrie
Department of Law and Public Safety
Division of Criminal Justice
Office of Victim/Witness Advocacy
25 Market Street, CN 085
Trenton, New Jersey 08625-0085
Telephone: (609) 984-7347

NEW MEXICO
Larry Tackman, Director
Crime Victims Reparation Commission
8100 Mountain Road, N.E., Suite 106
Albuquerque, NM 87110
Telephone: (505) 841-9432

NEW YORK
Peggy Donnelly, Assistant Director
New York Crime Victims Board
845 Central Avenue
Albany, NY 12206
Telephone: (518) 457-1779

NORTH CAROLINA
Barry Bryant, Criminal Justice Planner
Governor's Crime Commission
Department of Crime Control & Public Safety
3824 Barrett Drive
Raleigh, NC 27609-7220
Telephone: (919) 571-4736

VICTIM COMPENSATION PROGRAMS

NORTH DAKOTA
Paul J. Coughlin, Administrator
Division of Parole & Probation
North Dakota Department of Corrections
Crime Victims Reparations
3303 E. Main - Box 5521
Bismarck, ND 58502-5521
Telephone: (701) 328-6195

OHIO
Miles C. Durfey, Clerk
Victims of Crime Compensation Program
Court of Claims of Ohio
65 East State Street, Suite 1100
Columbus, Ohio 43215
Telephone: (614) 466-8439

OKLAHOMA
Suzanne K. Breedlove, Administrator
Crime Victims Compensation Board
2200 Classen Blvd., Suite 1800
Oklahoma City, OK 73106-5811
Telephone: (405) 557-6704

OREGON
Mary Ellen Johnson, Director
Department of Justice
Crime Victims' Compensation Program
1162 Court Street, N.E.
Salem, OR 97310
Telephone: (503) 378-5348

PENNSYLVANIA
Carol Lavery, Director
Pennsylvania Commission on Crime
and Delinquency
Bureau of Victims Services
Victims Compensation Division
P.O.ox 1167
Harrisburg, PA 17108-1167
Telephone: (717) 787-2040

VICTIM ASSISTANCE PROGRAMS

NORTH DAKOTA
Paul J. Coughlin, Administrator
Division of Parole & Probation
North Dakota Department of Corrections
Crime Victim Reparations
3303 E. Main - Box 5521
Bismarck, ND 58502-5521
Telephone: (701) 328-6195

OHIO
Sharon Boyer, Administrator
Ohio Office of the Attorney General
Crime Victim Assistance Office
65 East State Street, 8th Floor
Columbus, OH 43215-4321
Telephone: (614) 466-5610

OKLAHOMA
Suzanne K. Breedlove, Administrator
District Attorneys Council
2200 Classen Boulevard, Suite 1800
Oklahoma City, OK 73106-5811
Telephone: (405) 557-6704

OREGON
Mary Ellen Johnson, Director
Department of Justice
Crime Victims' Assistance Section
1162 Court Street, N.E.
Salem, OR 97310
Telephone: (503) 378-5348

PENNSYLVANIA
John H. Kunkle, Program Manager
Pennsylvania Commission on Crime
and Delinquency
P.O. Box 1167 - 2nd & Chestnut Sts.
Federal Square Station
Harrisburg, PA 17108-1167
Telephone: (717) 787-8559 x 3031

VICTIM COMPENSATION PROGRAMS

RHODE ISLAND
Barbara Boden, Program Administrator
General Treasurer's Office
Crime Victims Compensation Program
49 Fountain Street, 7th Floor
Telephone: (401) 277-2212

SOUTH CAROLINA
Renee Graham, Program Manager
Division of Victim Assistance
Office of the Governor, Room 401
1205 Pendleton Street, Edgar Brown Bldg.
Columbia, SC 29201
Telephone: (803) 734-1930

SOUTH DAKOTA
Ann M. Holzhauser, Administrator
Office of Adult Servicse
Crime Victims' Compensation Commission
700 Governors Drive
Pierre, SD 57501-2291
Telephone: (605) 773-6317

TENNESSEE
Susan P. Clayton, Program Director
Treasury Department
Division of Claims Aministration
9th floor, Andrew Jackson Bldg.
Nashville, TN 37243-0243
Telephone: (615) 741-2734

TEXAS
Richard Anderson, Director
Crime Victims Compensation Division
Office of the Attorney General
P.O. Box 12548, Capitol Station
Austin, TX 78711-2548
Telephone: (512) 936-1200

VICTIM ASSISTANCE PROGRAMS

RHODE ISLAND
Joseph L. Persia, Grant Administrator
Governor's Justice Commission
One Capitol Hill
4th Floor
Providence, RI 02903-5803
Telephone: (401) 277-2620

SOUTH CAROLINA
Barbara Jean Nelson, VOCA Program Coord.
Division of Public Safety Programs
5400 Broad River Road
Columbia, South Carolina 29210
Telephone: (803) 896-8712

SOUTH DAKOTA
Susan Sheppick, Administrator
Department of Social Services
Office of the Adult Services
700 Governors Drive
Pierre, SD 57501-2291
Telephone: (605) 773-4330

TENNESSEE
Cresa L. Bailey, VOCA Specialist
Department of Human Services
400 Deaderick Street
Citizens Plaza Building
Nashville, TN 37248-9500
Telephone: (615) 313-4767

TEXAS
Carol Funderburgh, Program Coordinator
Criminal Justice Division
Office of the Governor
P.O. Box 12428
Austin, TX 78701
Telephone: (512) 463-1919

VICTIM COMPENSATION PROGRAMS

UTAH
Dan R. Davis, Director
Office of Crime Victim Reparations
350 E. 500 South, Suite 200
Salt Lake City, UT 84111
Telephone: (801) 533-4000

VERMONT
Lori E. Hayes, Executive Director
Vermont Center for Crime Victim Services
Crime Victims Compensation Program
103 South Main Street
Waterbury, VT 05671-2001
Telephone: (802) 241-1250

VIRGINIA
Robert W. Armstrong, Director
Division of Crime Victims' Compensation
1000 DMV Drive
Richmond, VA 23220-2036
Telephone: (804) 367-8686

VIRGIN ISLANDS
Ruth D. Smith, Administrator
Criminal Victims Compensation Commission
Department of Human Services
Office of the Commissioner
The Knud Hansen, Complex Building A
1303 Hospital Grounds
Charlotte Amalie, Virgin Islands 00802
Telephone: (809) 774-1166

WASHINGTON
Cletus Nnanabu, Program Manager
Department of Labor & Industries
Crime Victims Compensation Program
7373 Linderson Way, SW - POB 44520
Olympia, WA 98504-4520
Telephone: (360) 902-5340

VICTIM ASSISTANCE PROGRAMS

UTAH
Christine Watters, Program Coordinator
Office of Crime Victim Reparations
350 E. 500 South, Suite 200
Salt Lake City, UT 84111
Telephone: (801) 533-4000

VERMONT
Lori E. Hayes, Executive Director
Vermont Center for Crime Services
103 South Main Street
Waterbury, Vermont 05671-2001
Telephone: (802) 241-1250

VIRGINIA
Mandie Patterson, Program Manager
Department of Criminal Justice Services
805 East Broad Street, 10th Floor
Richmond, VA 23219
Telephone: (804) 786-3923

VIRGIN ISLANDS
Maria Brady, Director
Law Enforcement Planning Commission
8172 Sub Base, Suite 3
St. Thomas, VI 00802
Telephone: (809) 774-6400

WASHINGTON
Susan Hannibal, Program Manager
Department of Social and
Health Services
P.O. Box 45710, 12th & Jefferson
Olympia, WA 98504-5710
Telephone: (206) 753-3395

VICTIM COMPENSATION PROGRAMS

WEST VIRGINIA
Cheryle M. Hall, Clerk
West Virginia Court of Claims
Crime Victims Compensation Fund
Room 6, Building 1, 1900 Kanawha Blvd. E.
Charleston, WV 25305-0291
Telephone: (304) 347-4850

WISCONSIN
Susan Goodwin, Executive Director
Office of Crime Victims Services
Department of Justice
P.O. Box 7951 - 222 State Street
Madison, WI 53707-7951
Telephone: (608) 266-6470

WYOMING
Sylvia Bagdonas, Program Manager
Crime Victims Compensation Commission
Office of the Attorney General
1700 Westland Road
Cheyenne, WY 82002
Telephone: (307) 635-4050

VICTIM ASSISTANCE PROGRAMS

WEST VIRGINIA
Melissa B. Crawford,Program Manager
Criminal Justice & Highway Safety Div.
Dept. of Military Affairs & Public Safety
1204 Kanawha Boulevard, East
Charleston, WV 25301
Telephone: (304) 558-8814

WISCONSIN
Steve Derene, Program Manager
Office of Crime Victims Services
Department of Justice
P.O. Box 7951 - 222 State Street
Madison, WI 53707-7951
Telephone: (608) 267-2251

WYOMING
Sylvia Bagdonas, Program Manager
Office of Crime Compensation Commission
Office of the Attorney General
1700 Westland Road
Cheyenne, WY 82002
Telephone: (307) 635-4050

VICTIM ASSISTANCE TERRITORY PROGRAMS

VICTIM COMPENSATION PROGRAMS	VICTIM ASSISTANCE PROGRAMS
AMERICAN SAMOA No compensation program	**AMERICAN SAMOA** Laauli A. Filoialii, Director Criminal Justice Planning Agency American Samoa Government Pago Pago, AS 96799 Telephone: (011) (684) 633-5221
GUAM No compensation program	**GUAM** Gloria J. Duenas Cruz Department of Law Government of Guam 2-200E Guam Judicial Center 120 West O'Brien Drive Agana, GU 96910 Telephone: (011) (671) 475-3406
NORTHERN MARIANA ISLANDS No compensation program	**NORTHERN MARIANA ISLANDS** Joaquin T. Ogumoro, Executive Director Criminal Justice Planning Agency P.O. Box 1133 CK, Saipan MP Saipan, CM 96950 Telephone: (011) (670) 322-9350
PUERTO RICO No compensation program	**PUERTO RICO** Lizzette Traversoi, Acting Director Department of Justice P.O. Box 192 San Juan, PR 00902 Telephone: (809) 723-4949
PALAU No compensation program	**PALAU** Yusim Sato, VOCA Program Coordinator Ministry of Health P.O. Box 6027 Koror, Palau 96940 Telephone: (680) 488-2813/2553

***Nevada's victim compensation program does not received VOCA funds.

Appendix 8

Interpol State Liaison Offices

A point of contact has been established in each of the 50 States and the District of Columbia for local and State authorities to receive assistance from INTERPOL on international investigations to include child abductions/ kidnapings. This point of contact is known as the INTERPOL State Liaison Office. Local and State law enforcement can forward requests for assistance through the liaison office, which will then forward the request to the USNCB for transmission to appropriate foreign police authorities. The following is a listing of INTERPOL State Liaison Offices through which local/State police authorities can obtain assistance on child abduction investigations:

Alabama/INTERPOL Liaison Office
Alabama Bureau of Investigation
Criminal Information Center
Alabama Department of Public Safety
2720-A West Gunter Park Drive
Montgomery, AL 36109
Telephone: (334) 260-1170
FAX: (334) 260-8788

Alaska/INTERPOL Liaison Office
Alaska State Troopers
101 East 6th Avenue
Anchorage, AK 99501
Telephone: (907) 265-9583
FAX: (907) 274-0851

Arizona/INTERPOL Liaison Office
Arizona Department of Public Safety
P.O. Box 6638
Phoenix, AZ 85005-6638
Telephone: (602) 223-2608
FAX: (602) 223-2911

Arkansas/INTERPOL Liaison Office
Arkansas State Police
Crime Analysis Section
3 Natural Resources Drive
P. O. Box 5901
Little Rock, AR 72215
Telephone: (501) 221-8213
FAX : (501) 224-5006

California/INTERPOL Liaison Office
California Department of Justice
Bureau of Investigation
Organized Crime Unit
P. O. Box 163029
Sacramento, CA 95816-3029
Telephone: (916) 227-4186
FAX: (916) 227-4097

Colorado/INTERPOL Liaison Office
Colorado Bureau of Investigation
Crime Information Center
690 Kipling Street, Suite 3000
Denver, CO 80215-5865
Telephone: (303) 239-4310
FAX: (303) 238-6714

Connecticut/INTERPOL Liaison Office
Central Criminal Intelligence Unit
294 Colony Street
Meriden, CT 06451
Telephone: (203) 238-6561
FAX: (203) 238-6410

Delaware/INTERPOL Liaison Office
Delaware State Police
P.O. Box 430
Dover, DE 19901
Telephone: (302) 739-5998
FAX: (302) 739-2459

District of Columbia/INTERPOL Liaison Office
Washington Metropolitan Police Department
Intelligence Division - Room 5067
300 Indiana Ave., NW
Washington, D.C. 20001
Telephone: (202) 724-1426
FAX: (202) 727-0588

Florida/INTERPOL Liaison Office
Florida Department of law Enforcement
DCI/ISB
P.O. Box 1489
Tallahassee, FL 32302
Telephone: (904) 488-6933
FAX: (904) 488-7863

Georgia/INTERPOL Liaison Office
Georgia Bureau of Investigation
P.O. Box 370808
Decatur, GA 30037-0808
Telephone: (404) 244-2554
FAX:(404) 244-2798

Honolulu/INTERPOL Liaison Office
Department of the Attorney General
425 Queen St.
Honolulu, HI 96813
Telephone: (808) 586-1249
FAX: (808) 586-1371

Idaho/INTERPOL Liaison Office
Idaho State Police
Idaho Bureau of Investigation
P.O. Box #700
Meridian, ID 83680-0700
Telephone: (208) 884-7110
FAX: (208) 884-7191

Illinois/INTERPOL Liaison Office
Illinois State Police
Division of Criminal Investigation
500 Iles Park Place Room 400
Springfield, IL 62718
Telephone: (217) 782-8760
FAX: (217) 785-3328

Indiana/INTERPOL Liaison Office
Indiana State Police
Crime Information Center
100 Senate Avenue
Indianapolis, IN 46206-2404
Telephone: (317) 232-7796
FAX: (317) 232-0652

Iowa/INTERPOL Liaison Office
Iowa Department of Public Safety
Intelligence Bureau
Wallace State Office Building
Des Moines, IA 50319-0049
Telephone: (515) 242-6124
FAX: (515) 281-6108

Kansas/INTERPOL Liaison Office
Kansas Bureau of Investigation
1620 Tyler
Topeka, KS 66612
Telephone: (913) 296-8261
FAX: (913) 296-6781

Kentucky/INTERPOL Liaison Office
Kentucky State Police Intelligence Section
1240 Airport Road
Frankfort, KY 40601
Telephone: (502) 227-8708
FAX: (502) 564-4931

Louisiana/INTERPOL Liaison Office
Louisiana State Police
P.O. Box 66614
Baton Rouge, LA 70896
Telephone: (504) 925-6213
FAX: (504) 925-4766

Maine/INTERPOL Liaison Office
Maine State Police
Gardiner Annex
State House Station 164
Augusta, ME 04333-0164
Telephone: (207) 624-8787
FAX: (207) 624-8765

Maryland/INTERPOL Liaison Office
Maryland State Police
Criminal Intelligence Division
7175 Columbia Gateway Drive, Suite D
Columbia, MD 21045
Telephone: (410) 290-0780
FAX: (410) 290-0752

Massachusetts/INTERPOL Liaison Office
Massachusetts State Police
Criminal Information Section
470 Worcester Road
Framingham, MA. 01702
Telephone: (508) 820-2129
FAX: (508) 820-2128

Michigan/INTERPOL Liaison Office
Michigan State Police
Criminal Intelligence Unit
4000 Collins Road
PO Box 30637
Lansing, MI 48909-8137
Telephone: (517) 336-6235
FAX: (517) 333-5399

Minnesota/INTERPOL Liaison Office
Minnesota State Bureau of Criminal Apprehension
1246 University Avenue
St. Paul, MN 55104-4197
Telephone: (612) 642-0610
FAX: (612) 642-0618

Mississippi/INTERPOL Liaison Office
Mississippi Department of Public Safety
Division of Criminal Investigation
P.O. Box 958
Jackson, MS. 39205
Telephone: (601) 987-1592
FAX: (601) 987-1579

Missouri/INTERPOL Liaison Office
Missouri State Highway Patrol
P.O. Box 568
Jefferson City, MO 65102
Telephone: (573) 751-3452
FAX: (573) 526-5577

Montana/INTERPOL Liaison Office
Montana Department of Justice
Law Enforcement Services Division
P.O. Box 201417
Helena, MT 59620-1417
Telephone: (406) 444-3874
FAX: (406) 444-2759

Nebraska/INTERPOL Liaison Office
Nebraska State Patrol
State House
P. O. Box 94907
Lincoln, NE 68509
Telephone: (402) 479-4957
FAX: (402) 479-4002

Nevada/INTERPOL Liaison Office
Nevada Division of Investigation
555 Wright Way
Carson City, NV 89711-0100
Telephone: (702) 687-3346
FAX: (702) 687-1668

New Hampshire/INTERPOL Liaison Office
New Hampshire State Police
Intelligence Unit
10 Hazen Drive
Concord, NH 03305
Telephone: (603) 271-2663
FAX: (603) 271-2520

New Jersey/INTERPOL Liaison Office
New Jersey State Police
Intelligence Bureau
P. O. Box 7068
West Trenton, NJ 08628-0068
Telephone: (609) 882-2000 x 2642
FAX: (609) 883-5576

New Mexico/INTERPOL Liaison Office
New Mexico Department of Public Safety
Criminal Intelligence Section
400 Gold Ave. SW - Suite 300
Albuquerque, NM 87102
Telephone: (505) 841-8053
FAX: (505) 841-8062

New York/INTERPOL Liaison Office
New York State Police
1220 Washington Avenue - BLDG #30
Albany, NY 12226-3000
Telephone: (518) 485-1518
FAX: (518) 485-2000

Inter-City Correspondence Unit
Police Headquarters
1 Police Plaza, Room 703
New York, NY 10038-1497
Telephone:(212) 374-5030
FAX: (212) 374-2485

North Carolina/INTERPOL Liaison Office
North Carolina State Bureau of Investigation
Intelligence and Technical Services Section
P. O. Box 29500
Raleigh, NC 27626
Telephone: 1-800-334-3000
FAX: (919) 662-4483

N orth Dakota/INTERPOL State Liaison Office
Bureau of Criminal Investigation
P. O. Box 1054
Bismark, ND 58502-1054
Telephone: (701) 221-5500
FAX: (701) 328-5510

Ohio/INTERPOL Liaison Office
Criminal Intelligence Unit
Ohio BCI&I
P.O. Box 365
London, OH 43140
Telephone: (800) 282-3784, Ext. 223
FAX: (614) 852-1603

Oklahoma/INTERPOL Liaison Office
Oklahoma State Bureau of Investigation
6600 N. Harvey, Suite 300
Oklahoma City, OK 73116
Telephone: (405) 848-6724
FAX: (405) 843-3804

Oregon State Police
Criminal Investigation Division
400 Public Service Building
Salem, Oregon 97310
Telephone: (503) 378-3720
FAX: (503) 363-5475

Pennsylvania/INTERPOL Liaison Office
PA Attorney General Intelligence Unit
State Police Headquarters
1800 Elmerton Avenue
Harrisburg, PA 17110
Telephone: (717) 787-0834
FAX: (717) 787-0846

Rhode Island/INTERPOL Liaison Office
Rhode Island State Police Headquarters
P.O. Box 185
N. Scituate, RI 02857
Telephone: (401) 444-1006
FAX: (401) 444-1133

South Carolina/INTERPOL Liaison Office
South Carolina Law Enforcement Division
P. O. Box 21398
Columbia, SC 29221-1398
Telephone: (803) 896-7008
FAX: (803) 896-7041

South Dakota/INTERPOL Liaison Office
Division of Criminal Investigation
Criminal Justice Training Center
E.Hwy. 34 c/o 500 E. Capitol Avenue
Pierre, SD 57501-5070
Telephone: (605) 773-3331
FAX: (605) 773-4629

Tennessee/INTERPOL Liaison Office
Tennessee Bureau of Investigation
Cooper Hall 1148 Foster Avenue
Nashville, TN 37210
Telephone: (615) 741-0430
FAX: (615) 532-8315

Texas/INTERPOL Liaison Office
Texas Department of Public Safety
Special Crimes Service
P. O. Box 4087 N.A.S.
Austin, TX 78773-0001
Telephone: (512) 424-2200
FAX: (512) 424-5715

Utah/INTERPOL Liaison Office
Utah DPS/Division of Investigations
5272 South College Drive - Suite 200
Murray, UT 84123-2611
Telephone: (801) 284-6200
FAX: (801) 284-6300

Vermont/INTERPOL Liaison Office
Vermont State Police
Criminal Division
103 South Main Street
Waterbury, VT 05671
Telephone: (802) 244-8781
FAX: (802) 244-1106

Virginia/INTERPOL Liaison Office
Virginia Department of State Police
808 Moorefield Drive Suite 300
Richmond, VA 23236-3683
Telephone: (804) 323-2493
FAX: (804) 323-2021

Washington/INTERPOL Liaison Office
Washington State Patrol
Investigative Assistance Division
P. O. Box 2347, Mail Stop 42634
Olympia, WA 98507-2347
Telephone: (206) 753-3277
FAX: (360) 586-8231

West Virginia/INTERPOL Liaison Office
West Virginia State Police
725 Jefferson Road
South Charleston, WV 25309
Telephone: (304) 558-3324
FAX: (304) 746-2246

Wisconsin/INTERPOL Liaison Office
Wisconsin Department of Justice
Division of Criminal Investigation
P. O. Box 7857
Madison, WI 53707-7857
Telephone: (608) 266-1671
FAX: (608) 267-2777

Wyoming/INTERPOL Liaison Office
Wyoming Division of Criminal Investigation
316 West 22nd Street
Cheyenne, WY 82002-0150
Telephone: (307) 777-6615
FAX: (307) 777-7252

INTERPOL/U.S. American Samoa
P.O. Box 4567
Pago Pago, American Samoa 96799
Telephone: (684) 633-2827
FAX: (684) 633-2979

INTERPOL-Special Invest. Bureau
Puerto Rico Dept. of Justice
P.O. Box 9023899
San Juan, Puerto Rico 00902-3899
Telephone: (787) 729-2068
FAX: (787) 722-0809

INTERPOL Liaison Office
Virgin Islands Police Department
Insular Investigation Unit
Patrick Sweeney Headquarters
RR 02 Kings Hill
St. Croix, U.S. Virgin Islands 00850
Telephone: (809) 778-6601
FAX: (809) 773-7272

Appendix 9

U.S. Department of State
Bureau of Consular Affairs

Office of Children's Issues
Abduction and Custody Information Checklist

Name: _____
Address: _____
_____

(Please place a check beside your choice)

GENERAL INFORMATION:

____Office of Children's Issues Brochure
____International Parental Child Abduction Booklet*, +
____International Parental Kidnaping Crime Act of 1993
____Tips for Travelers to the Middle East and North Africa*
(Provides country specific information)

HAGUE CONVENTION ON INTERNATIONAL PARENTAL CHILD ABDUCTION:

____Hague Parties (List of Hague Countries)
____Hague Convention - French/English Text
____Hague: Scope of the Convention

COUNTRY SPECIFIC INFORMATION

____Australia
____Canada
____Canada - Legal Aid Act
____Denmark
____Germany*
____Greece
____India
____Iran*
____Islamic Family Law
____Japan
____Jordan*
____Kuwait
____Mexico
____Mexico - Child Custody
____Pakistan
____Pakistan - Child Custody Law
____Pakistan - Sunni Muslim Law
____Philippines*
____Poland
____Portugal
____Saudi Arabia*
____Saudi Arabia = Marriage to Saudis
____Spain
____Sweden
____Syria
____Thailand
____United Kingdom

* - Available by Autofax
+ - Available by Internet

Office of Children's Issues
Adoption Information Checklist

Name: _____
Address: _____
_____

(Please place a check beside your choice)

GENERAL INFORMATION FLYERS:

____International Adoptions*
____The Immigration of Adopted and Prospective Adoptive Children (M-249Y)

COUNTRY SPECIFIC INFORMATION:

____Albania
____Antingua
____Argentina
____Austria
____Bahamas
____Barbados
____Belarus
____Belize
____Bolivia
____Brazil
____Bulgaria
____Chile
____China
____Columbia
____Costa Rica
____Czech Republic
____Dominica
____Dominican Republic
____Ecuador
____El Salvador
____Georgia
____Germany
____Greece
____Grenada
____Guatemala
____Guyana
____Haiti
____Honduras
____Hong Kong
____Hungary
____India
____Iran
____Ireland
____Israel
____Jamaica
____Japan
____Jordan
____Korea
____Latvia
____Lebanon
____Lithuania
____Marshall Islands
____Mexico
____Moldova
____Morocco
____Nepal
____Nicaragua
____Pakistan
____Panama
____Paraguay
____Peru
____Philippines
____Poland
____Portugal
____Romania
____Russia
____Slovakia
____Sri Lanka
____St. Lucia
____St. Kitts
____St. Vincent
____Syria
____Taiwan
____Thailand
____Trinidad
____Ukraine
____Uruguay
____Uzebekistan
____Vietnam
____Former Yugoslavia
____Venezuela

Office of Children's Issues
Overseas Citizens Services
Bureau of Consular Affairs
U.S. Department of State
Washington, D.C. 20520

Telephone: (202) 647-2699
Fax: (202) 647-2835
Autofax (202) 647-3000
Recorded Info:
(202) 647-7000
Internet Address:
http:\\travel.state.gov

Appendix 10

U.S. Customs Service
Field Offices

Alabama	
Birmingham	(205) 290-7193
Gulf Shores	(205) 981-5711
Mobile	(205) 441-6146
Alaska	
Anchorage	(907) 271-2880
Arizona	
Douglas	(602) 364-1218
Flagstaff	(602) 556-7384
Nogales	(602) 761-2075
Phoenix	(602) 640-2036
Sells	(602) 387-7640
Tucson	(602) 670-6026
Yuma	(602) 344-0088
Arkansas	
Little Rock	(501) 324-7345
California	
El Centro	(619) 353-9090
Fresno	(209) 487-5351
Los Angeles	(310) 514-6231
Los Angeles Airport	(310) 215-2200
Oceanside	(619) 722-6616
Orange County	(714) 836-2293
Oxnard	(805) 988-8690
Riverside	(909) 276-6664
Sacramento	(916) 978-4411
San Diego	(619) 557-6850
San Francisco	(415) 705-4070
San Jose	(408) 291-7861
San Ysidro	(619) 428-7115
Colorado	
Denver	(303) 784-6480

Connecticut	
New Haven	(203) 773-2155
District of Columbia	
Washington, D.C.	(703) 709-9700
Florida	
Cocoa Beach	(407) 452-3700
Fort Lauderdale	(305) 590-7384
Fort Myers	(813) 433-7773
Fort Pierce	(407) 461-1293
Jacksonville	(904) 356-4701
Key Largo	(305) 664-2955
Key West	(305) 294-3877
Miami	(305) 597-6000
Naples	(813) 643-4554
Orlando	(407) 648-6847
Panama City	(904) 763-8418
Pensacola	(904) 434-6648
Sarasota	(813) 953-2920
Tallahassee	(904) 942-8802
Tampa	(813) 225-7638
West Palm Beach	(407) 659-4606
Georgia	
Atlanta	(770) 994-2230
Savannah	(912) 652-4341
Illinois	
Chicago	(312) 353-8450
Indiana	
Indianapolis	(317) 248-4151
Louisiana	
Baton Rouge	(504) 389-0433
Belle Chase	(504) 589-2291
Houma	(504) 851-0179
Lafayette	(318) 262-6619
Lake Charles	(318) 477-2112
New Orleans	(504) 589-6499
Shreveport	(318) 676-3350
Maine	
Houlton	(207) 532-6198
Portland	(207) 773-8959

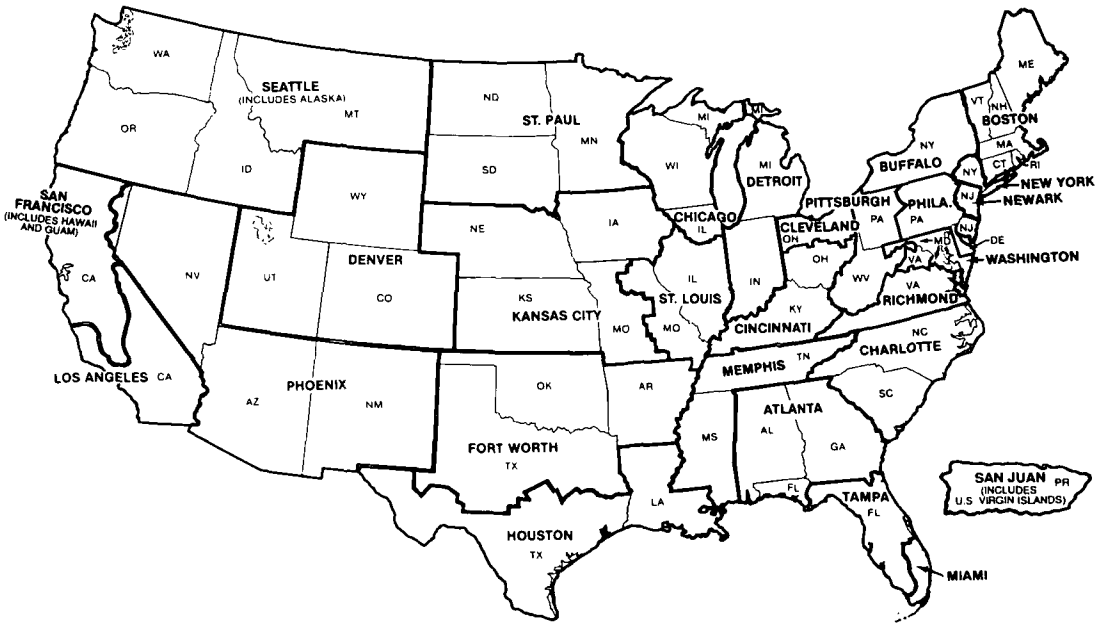
Maryland	
Baltimore	(410) 962-2620
Massachusetts	
Boston	(617) 565-7400
Michigan	
Detroit	(313) 226-3166
Grand Rapids	(616) 235-3936
Minnesota	
Minneapolis	(612) 348-1300
Mississippi	
Gulfport	(601) 864-1274
Jackson	(601) 965-5234
Missouri	
Kansas City	(816) 374-6426
St. Louis	(314) 539-6740
Montana	
Great Falls	(406) 727-8750
Nevada	
Las Vegas	(702) 388-6042
Reno	(702) 784-5727
New Jersey	
Newark	(201) 645-3770
New Mexico	
Albuquerque	(505) 766-2807
Deming	(505) 546-2759
Las Cruces	(505) 526-4643
New York	
Albany	(518) 472-2211
Buffalo	(716) 551-4375
John F. Kennedy Airport	(718) 553-1824
Long Island	(516) 563-3040
New York City	(212) 466-2906
Rouses Point	(518) 297-6661
North Carolina	
Charlotte	(704) 527-0151
Wilmington	(910) 343-4899

North Dakota	
Grand Forks	(701) 746-1157
Ohio	
Cincinnati	(606) 578-4600
Cleveland	(216) 522-4292
Columbus	(614) 469-5705
Oklahoma	
Oklahoma City	(405) 231-4279
Oregon	
Astoria	(503) 325-4644
Coos Bay	(503) 269-7521
Portland	(503) 326-2711
Pennsylvania	
Harrisburg	(717) 782-4047
Philadelphia	(215) 597-4305
Pittsburgh	(412) 644-4970
Rhode Island	
Providence	(401) 528-5025
South Carolina	
Charleston	(803) 745-9290
Columbia	(803) 765-5430
Greenville	(803) 235-0519
Tennessee	
Memphis	(901) 544-4140
Nashville	(615) 781-5473
Texas	
Alpine	(915) 837-5889
Austin	(512) 482-5502
Brownsville	(210) 542-7831
Corpus Christi	(512) 888-3501
Dallas	(214) 767-2011
Del Rio	(210) 703-2000
Eagle Pass	(210) 773-7877
El Paso	(915) 540-5700
Falcon Dam	(210) 848-5243
Galveston	(409) 766-3791
Houston	(713) 985-0500
Laredo	(210) 726-2210
McAllen	(210) 682-1366

Texas - continued	
Port Arthur	(409) 839-2401
Presidio	(915) 229-3960
San Angelo	(915) 942-6900
San Antonio	(210) 229-4561
Utah	
Salt Lake City	(801) 524-5884
Vermont	
Burlington	(802) 863-3458
Derby Line	(802) 873-3609
Virginia	
Norfolk	(804) 441-6533
Washington	
Blaine	(206) 332-6725
Port Angeles	(206) 452-4122
Seattle	(206) 553-7531
Spokane	(509) 353-3130
Wisconsin	
Milwaukee	(414) 297-3231
Bahamas	
Nassau	(809) 325-5322
Guam	
Guam	(700) 550-7265
Puerto Rico	
Fajardo	(809) 865-5303
Mayaquez	(809) 831-3346
Ponce	(809) 841-3108
San Juan	(809) 729-6975
Virgin Islands	
St. Thomas	(809) 774-7409

Appendix 11

U.S. Postal Inspection Service Division Boundaries



For assistance with postal-related problems of a law enforcement nature, please contact your nearest Inspection Service Division.

Atlanta Division
P.O. Box 16489
Atlanta, GA 30321-0489
404/608-4500
Fax: 404/608-4505

Boston Division
425 Summer Street, 7th Floor
Boston, MA 02210-1736
617/464-8000
Fax: 617/464-8123

Buffalo Division
1200 Main Place Tower
Buffalo, NY 14202-3796
716/853-5300
Fax: 716/846-2372

Charlotte Division
2901 South I-85 Service Road
Charlotte, NC 28228-3000
704/329-9120
Fax: 704/357-0039

Chicago Division
433 W. Harrison Street, Room 50190
Chicago, IL 60669-2201
312/983-7900
Fax: 312/983-6300

Cincinnati Division
895 Central Avenue, Suite 400
Cincinnati, OH 45202-5748
513/684-8000
Fax: 513/684-8009

Cleveland Division
P.O. Box 5726
Cleveland, OH 44101-0726
216/443-4000
Fax: 216/443-4509

Denver Division
1745 Stout Street, Suite 900
Denver, CO 80202-3034
303/313-5320
Fax: 303/313-5351

Detroit Division
P.O. Box 330119
Detroit, MI 48232-6119
313/226-8184
Fax: 313/226-8220

Ft. Worth Division
P.O. Box 162929
Ft. Worth, TX 76161-2929
817/317-3400
Fax: 817/317-3430

Houston Division
P.O. Box 1276
Houston, TX 77251-1276
713/238-4400
Fax: 713/238-4460

Kansas City Division
3101 Broadway, Suite 850
Kansas City, MO 64111-2416
816/932-0400
Fax: 816/932-0490

Los Angeles Division
P.O. Box 2000
Pasadena, CA 91102-2000
818/405-1200
Fax: 818/405-1207

Memphis Division
P.O. Box 3180
Memphis, TN 38173-0180
901/576-2077
Fax: 901/576-2085

Miami Division
3400 Lakeside Drive, 6th Floor
Miramar, FL 33027-3242
954/436-7200
Fax: 954/436-7282

Newark Division
P.O. Box 509
Newark, NJ 07101-0509
201/693-5400
Fax: 201/645-0600

New York Division
P.O. Box 555
New York, NY 10116-0555
212/330-3844
Fax: 212/330-2720

Philadelphia Division
P.O. Box 7500
Philadelphia, PA 19101-9000
215/895-8450
Fax: 215/895-8470

Phoenix Division
P.O. Box 20666
Phoenix, AZ 85036-0666
602/223-3660
Fax: 602/258-1705

Pittsburgh Division
1001 California Avenue, Room 2101
Pittsburgh, PA 15290-9000
412/359-7900
Fax: 412/359-7682

Richmond Division
P.O. Box 25009
Richmond, VA 23260-5009
804/418-6100
Fax: 804/418-6150

St. Louis Division
1106 Walnut Street
St. Louis, MO 63199-2201
314/539-9300
Fax: 314/539-9306

St. Paul Division
P.O. Box 64558
St. Paul, MN 55164-0558
612/293-3200
Fax: 612/293-3384

San Francisco Division
P.O. Box 882528
San Francisco, CA 94188-2528
415/778-5800
Fax: 415/778-5822

San Juan Division
P.O. Box 363667
San Juan, PR 00936-3667
787/749-7600
Fax: 787/782-8296

Seattle Division
P.O. Box 400
Seattle, WA 98111-4000
206/442-6300
Fax: 206/442-6304

Tampa Division
P.O. Box 22526
Tampa, FL 33622-2526
813/281-5200
Fax: 813/289-8003

Washington Division
P.O. Box 96096
Washington, DC 20066-6096
202/636-2300
Fax: 202/636-2287

Headquarters
U.S. Postal Inspection Service
475 L'Enfant Plaza SW
Washington, DC 20260-2100
Fax: 202/268-4563

DOCUMENT OF
National Criminal Justice Reference Service (NCJRS)
Box 6000
Rockville, MD 20849-6000

U.S. Department of Defense – Legal Assistance Offices

Army Legal Assistance Office
DAJA-LA
Office of the Judge
Advocate General
Room 2C463
Pentagon
Washington, DC 20310-2200
Telephone: (703) 697-3170

Navy Legal Assistance Office
Legal Assistance (Code 36)
Office of the Judge
Advocate General
Department of the Navy
9S25 Hoffman II Building
200 Stovall Street
Alexandria, VA 22332-2400
Telephone: (703) 325-7928

U.S. Department of Health and Human Services – Family and Youth Services Bureau

Family and Youth Services Bureau
U.S. Department of Health
and Human Services
P.O. Box 1882
Washington, DC 20013
Telephone: (202) 205-8102
Fax: (202) 260-9333

National Clearinghouse on Families and Youth
P.O. Box 13505
Silver Spring, MD 20911-3505
Telephone: (301) 608-8098
Fax: (301) 608-8721

National Runaway Switchboard Hotline
Telephone: 1-800-621-4000

U.S. Department of Justice – Child Exploitation and Obscenity Section

Child Exploitation and Obscenity Section
Criminal Division
U.S. Department of Justice
1331 F Street NW.
6th Floor
Washington, DC 20530
Telephone: (202) 514-5780
Fax: (202) 514-1793

U.S. Department of Justice – Office for Victims of Crime

Office for Victims of Crime
U.S. Department of Justice
810 7th Street NW.
Washington, DC 20531
Telephone: (202) 307-5983
Fax: (202) 514-6383

Gopher to: ncjrs.aspensys.com
World Wide Web:
http://www.ojp.usdoj.gov/OVC/

Air Force Legal Assistance Office
AFLSA/JACA
1420 Air Force Pentagon
Washington, DC 20330-1420
Telephone: (202) 697-0413

Marine Corps Legal Assistance Office
Legal Assistance Office
Judge Advocate Division
Headquarters, USMC
301 Henderson Hall
Southgate Road and Orme St.
Arlington, VA 22214
Telephone: (703) 614-1266

U.S. Department of Defense – Family Advocacy Program

Army Family Advocacy Program
Army Family Advocacy Program Manager
HQDA, CFSC-FSA, Department of the Army
Hoffman #1, Room 1407
Alexandria, VA 22331-0521
Telephone: (703) 325-9390
Fax: (703) 325-5924

Air Force Family Advocacy Program
Chief, Family Advocacy Division
HQ AFMOA/SGPS
8901 18th Street, Suite 1
Brooks Air Force Base, TX 78235-5217
Telephone: (210) 536-2031
Fax: (210) 536-9032

Navy Family Advocacy Program
Director, Family Advocacy Program
BUPERS 661
Department of the Navy
Washington, DC 20370-5000
Telephone: (703) 697-6616/8/9
Fax: (703) 697-6571

U.S. Department of Education – Safe and Drug-Free Schools Program

Safe and Drug-Free Schools Program
U.S. Department of Education
600 Independence Avenue SW.
Room 604, Portals Building
Washington, DC 20202-6123
Telephone: (202) 260-3954
Fax: (202) 260-7767
E-mail: http://www.ed.gov/offices/OESE/SDFS

U.S. Department of Health and Human Services – National Center on Child Abuse and Neglect

National Center on Child Abuse and Neglect
Administration on Children, Youth and Families
U.S. Department of Health and Human Services
P.O. Box 1182
Washington, DC 20013-1182
Telephone: (202) 205-8586
Fax: (202) 260-9351

National Clearinghouse on Child Abuse and Neglect Information
P.O. Box 1182
Washington, DC 20013-1182
Telephone: 1-800-FYI-3366
Fax: (703) 385-3206
E-mail: nccanch@calib.com

U.S. Department of Justice – Federal Bureau of Investigation/ Child Abduction and Serial Killer Unit

Contact your local FBI Office (see inside front cover of your local telephone directory for the number) or:

Child Abduction and Serial Killer Unit
Federal Bureau of Investigation
Quantico, VA 22135
Telephone: (540) 720-4700
Fax: (540) 720-4790

Morgan P. Hardiman Task Force on Missing and Exploited Children
Federal Bureau of Investigation
Quantico, VA 22135
Telephone: (540) 720-4760
Fax: (540) 720-4792

Marine Corps Family Advocacy Program
Marine Corps Family Advocacy Program Manager
Headquarters USMC
Human Resources Division (Code MHF)
Washington, DC 20380-0001
Telephone: (703) 696-2066 or 696-1188
Fax: (703) 696-1143

Defense Logistics Agency Family Advocacy Program
Family Advocacy Program Manager
Quality of Life Program CAAPQ
Defense Logistics Agency
8725 John J. Kingman Road, STE 2533
Fort Belvoir, VA 22060-6221
Telephone: (703) 767-5372
Fax: (703) 767-5374

FBI Headquarters
Special Investigations and Initiatives Unit
Office of Crimes Against Children
Office of Indian Country Investigations
935 Pennsylvania Avenue NW.
Washington, DC 20535-0001
Telephone: (202) 324-3666
Fax: (202) 324-2731

U.S. Department of Justice – Missing and Exploited Children's Program

Missing and Exploited Children's Program
Office of Juvenile Justice and Delinquency Prevention
810 7th Street NW.
Washington, DC 20531
Telephone: (202) 616-3637
Fax: (202) 307-2819
World Wide Web: http://www.ncjrs.org/ojjhome.htm

U.S. Department of State – Office of Children's Issues

Office of Children's Issues
Room 4811
Overseas Citizens Services
Bureau of Consular Affairs
U.S. Department of State
Washington, DC 20520-4818
Telephone: (202) 736-7000
Fax: (202) 647-2835
Autofax: (202) 647-3000

Consular Affairs
Electronic Bulletin Board:
(202) 647-9225
(modem number)
Internet Address:
http://travel.state.gov

U.S. Department of Treasury – U.S. Secret Service

U.S. Secret Service
Forensic Services Division
1800 G Street NW.
Suite 929
Washington, DC 20223
Telephone: (202) 435-5926
Fax: (202) 435-5603

National Center for Missing and Exploited Children

National Center for Missing and Exploited Children
2101 Wilson Boulevard
Suite 550
Arlington, VA 22201-3052
Hotline: 1-800-THE-LOST
(1-800-843-5678), for the United States, Canada, and Mexico

Telephone (Business): (703) 235-3900
TTD: 1-800-826-7653
Fax: (703) 235-4067
World Wide Web:
http://www.missingkids.com
Internet e-mail:
77431.177@Compuserve.com
Cyber Tipline:
http://www.missingkids.com/cybertip

U.S. Department of Justice – INTERPOL

INTERPOL
U.S. National Central Bureau
U.S. Department of Justice
Bicentennial Building
Room 600
600 E Street NW.
Washington, DC 20530

MAIN NUMBER	(202) 616-9000
Deputy Chief	(202) 616-9000
Admin Support	(202) 616-9000
Criminal	(202) 616-7220
Financial Fraud	(202) 616-3850
State Liaison	(202) 616-1051
Chief	(202) 616-9000
General Counsel	(202) 616-7280
Alien/Fugitive	(202) 616-7260
Drug	(202) 616-7230
Invest Support	(202) 616-3900
State Toll-Free	(800) 743-5630
FAX NUMBERS	
Main Fax Number	(202) 616-8400
Interpol Cryptofax	(202) 616-7999

U.S. Postal Service – U.S. Postal Inspection Service

U.S. Postal Inspection Service
Office of Criminal Investigations
475 L'Enfant Plaza West SW.
Room 3141
Washington, DC 20260-2166
Telephone: (202) 268-4286
Fax: (202) 268-4563

U.S. Department of Treasury – U.S. Customs Service

U.S. Customs Service
International Child Pornography Investigation and Coordination Center
45365 Vintage Park Road
Suite 250
Sterling, VA 20166
Telephone: (703) 709-9700, ext. 353
Fax: (703) 709-8286

U.S. Department of Justice - U.S. Immigration and Naturalization Service

U.S. Immigration and Naturalization Service
Office of Inspections (HQINS)
425 I Street NW
Washington, DC 20536
Telephone: (202) 514-3019
Fax: (202) 514-8345
After Hours: (202) 616-5000 (INS Command Center, 7 x 24)