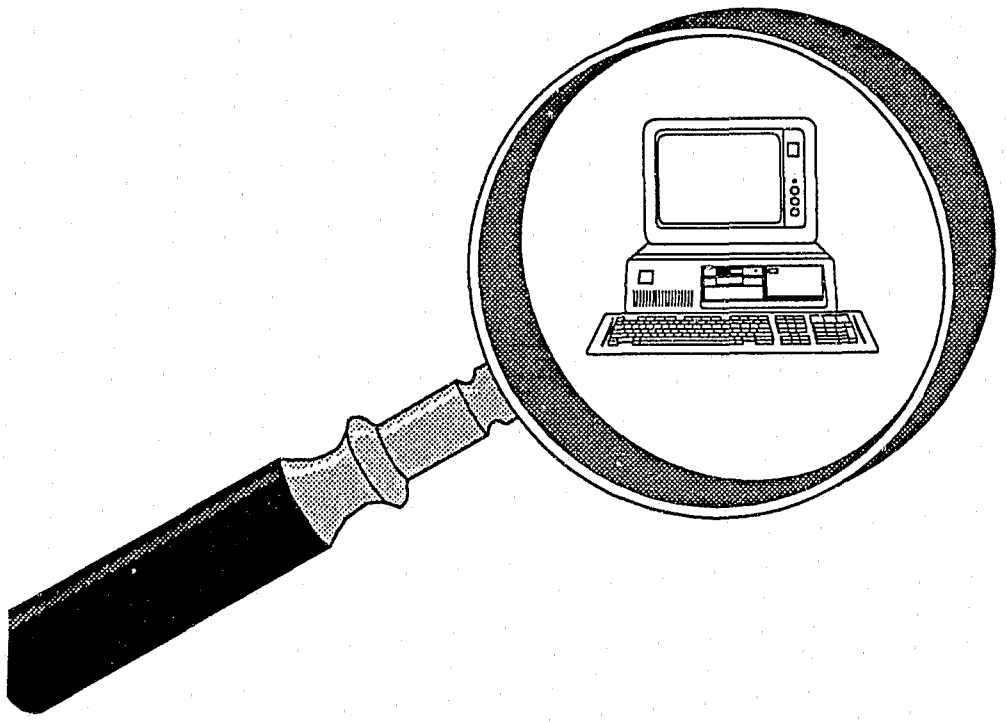
January 1992
Volume 19, No. 1
U. S. Department of Justice
Federal Bureau of Investigation

Crime Laboratory Digest

In This Issue:

DRUGFIRE: Responding to Gang and Drug-Related Shootings

Computer Analysis and Response Team (CART): The Microcomputer as Evidence



CRIME LABORATORY DIGEST

PUBLICATION POLICY

The Crime Laboratory Digest is published quarterly by the FBI Laboratory in cooperation with the American Society of Crime Laboratory Directors (ASCLD). It is intended to serve as a rapid means of communication between crime laboratories, permitting information of interest and value to be disseminated among crime laboratory scientists.

Inclusion of an article in the Crime Laboratory Digest in no way represents an endorsement or recommendation of any part of that article by the Federal Government, the Department of Justice or the FBI. Contributing authors assume total responsibility for the contents and accuracy of their submissions. Questions or requests concerning an article should be directed to the contributing agency.

All submissions are subject to editorial review in accordance with the editorial policy established by the FBI Laboratory and ASCLD. The editorial staff of the Crime Laboratory Digest reserves the right to edit all articles for style, grammar and punctuation. Comments and letters to the editor are encouraged and will be published when appropriate and as space permits. These should be forwarded to:

Crime Laboratory Digest - Editor
FSRTC, FBI Academy
Quantico, Virginia 22135

137561

Contents

CRIME LABORATORY DIGEST Vol. 19, No. 1, January 1992
ISSN NO. 0743-1872

137561

Feature Article

Computer Analysis and Response Team (CART)

The Microcomputer as Evidence

Michael G. Noblett
Laboratory Division
Federal Bureau of Investigation
Washington, D. C. 20535

Just as the business world increasingly relies on computers to perform day-to-day operations, the use of computers as criminal instruments or as devices to store data associated with criminal enterprises is rising. We were reminded of the potential for loss and the frailty of our computer systems when Robert Morris, Jr. placed a program called a worm[1] in an international network of computers and ground the entire system to a halt within hours (Burgess 1990; Markoff 1990). This act of computer fraud and abuse is well documented in both the law enforcement and legal communities. However, for every Robert Morris worm we face, the law enforcement community faces hundreds, perhaps thousands, of cases in which a computer is used incidentally in the crime. In these cases, records vital to the investigation or prosecution of a case are stored on the internal, or hard disk, drive of a computer.

If present trends continue, the use of computers in criminal activities will continue to rise. Likewise, the problems associated with them will continue to trouble investigators, prosecutors, and the computer specialists assigned to examine computer-related evidence. Criminals are using computers to store records regarding drug deals, money laundering, embezzlement, mail fraud, telemarketing fraud, prostitution, gambling matters, extortion and a myriad of other criminal activities. In addition to simply storing records, they manipulate data, infiltrate the computers of financial institutions, illegally use telephone lines charged to unsuspecting businesses, and perform a host of other imaginative scams.

A growing segment of our population considers computers and the data stored within as nothing more than electronic paper. Most people feel very comfortable keeping their records (whether legal or illegal) in this electronic format. In order to reasonably address the legitimate law enforcement need for access to these devices and the information they contain, a structured approach to examining computer evidence is needed. The examination of computer evidence can furnish investigative and intelligence information to the law enforcement community and, at the same time, preserve the information for subsequent admission in the courts.

The following statistics are staggering and suggest that the law enforcement community must act quickly and decisively to meet the challenge presented by the computer:

- Over 4.7 million personal computers were sold in the United States in 1988, as compared with 386,500 in 1980 (Stites 1990).
- There are at least 400 connected networks nationally and internationally. One network alone, Internet, estimates that there could be more than 1 million users (Quarterman 1990).
- $500 million is lost annually through illegal use of telephone access codes (Marsa and Ray 1990).
- $1 trillion is moved electronically each week (Marsa and Ray 1990).
- Only 11% of computer crimes are reported (Stites 1990).

[1] The Morris worm was a program which entered computers on the Internet network and replicated itself. This worm quickly overloaded the systems, making them slow down and ultimately crash. Morris was prosecuted under 18 U.S.C. Sect. 1030.

In the past few years, the FBI Laboratory has seen a phenomenal increase in the submission of computer evidence. Consequently, the FBI Laboratory established a Computer Analysis and Response Team (CART) at FBI Headquarters in Washington, D. C. This team is staffed by both sworn and nonsworn computer professionals with a wide range of experience and proficiency in the examination of computer-related evidence and a sensitivity to the particular needs of the law enforcement community. The CART has a full range of hardware available, as well as unique utility software for forensic examinations of this kind.

The CART's computer examination service is available for any law enforcement agency which is authorized to submit evidence to the FBI for forensic examination. While there is no typical computer case, most fall into the category of White Collar Crime, and the majority of the requests received by the FBI Laboratory are for printouts of the information stored electronically in suspected computers. During the course of these examinations, there are several recurring problems:

1. The preliminary examination is done locally.

When a computer used in criminal activities is seized, immediate action should be taken to protect the data stored on the computer's hard disk and associated floppy diskettes. The investigator often attempts to generate investigative and intelligence information on-site. This approach is reasonable and should be encouraged. However, it is imperative that the computer be protected from the investigator's inadvertently altering the computer's hard disk or floppy diskette files. For instance, many computer systems update files to the current date each time they are retrieved. In order to preserve the evidence in its original condition, appropriate steps must be taken to insure that no dates are changed and no data is added to or deleted from the computer's hard disk or floppy diskettes. Specialized and commercially available software which protects the data on the computer hard disk and floppy diskettes can be purchased, and it should always be used before any examination.

The investigator should also consider that any individual that conducts any type of examination on the evidence may be called upon to testify about the procedures used and the accuracy of the results. Therefore, a documented policy and protocol should be established. This policy does not have to be extensive or detailed, but it must be readily available to whomever is examining the evidence.

2. Supporting software is not seized with the computer.

When a computer is seized, all supporting software and documentation should be confiscated, if it is within the scope of the investigation. This simple action can eliminate numerous problems which may arise during the examination of the computer. It is logical but not necessarily correct to assume that the software which runs on the computer seized is identical to the software used in the investigator's office. This logic is reinforced if the software has the same name, such as WordPerfect, Lotus, etc. As commercial software is developed and marketed, new features are added and modifications are made to correct previously identified problems. The vendor then sells these new upgraded versions of the software; thus, the data seized may not be compatible with the particular version of the identical software in the investigator's office. It is advisable to confiscate all software, documentation, handwritten notes such as instructions or passwords, and any other similar items found near the computer.

3. The entire computer system is not seized.

Many of the devices connected to a seized computer are probably standard pieces of equipment which can be found in any computer facility. However, it only takes one unique, nonstandard or outdated component to render the entire system inoperable in a different office setting. For this reason, it is judicious to seize all the equipment connected to the computer. If it turns out that some of the equipment is not needed for the examination, it can be returned.

The FBI Laboratory does not recommend that the hard disk drive located inside a computer be removed and submitted for examination. While this option would appear to satisfy the needs of a computer specialist in a well equipped laboratory, the manner in which the rest of the computer is set up internally is often crucial to retrieving, displaying and printing the data stored on the hard drive.

Because a decision such as whether or not to seize an entire computer system is based on technical considerations, it may be appropriate to employ an expert as a consultant in the execution of these types of search warrants. This is especially true if the entire computer system is not seized. The concerns regarding incompatibilities of computer systems should be stated in the supporting affidavit as justification if the entire computer system is to be confiscated.

4. **Equipment is not properly packaged for shipment.**

If a computer is shipped to the FBI Laboratory or any other facility for examination, it must be packaged properly. A major reason the FBI Laboratory is sometimes unable to conduct a requested examination quickly and efficiently is because a confiscated computer is damaged in shipment and must be repaired. Likewise, certain precautions must be exercised to ship computer floppy diskettes, magnetic tape and other computer data recording devices. Due to the potential hazard of static electric discharge, these items should not be shipped in plastic evidence envelopes. The evidence should be appropriately labeled to avoid exposure to strong magnetic fields, such as those generated near X-ray machines.

PROCEDURES FOR SUBMISSION AND EXAMINATION OF COMPUTER EVIDENCE

A set of guidelines (Appendix A) has been prepared by the FBI Laboratory which addresses the preservation and submission of computers and related evidence. Although these guidelines are not extensive, they can be used as a basic foundation to insure that evidence is preserved in its original condition for shipment to the FBI Laboratory.

The list of computer equipment and materials in Appendix A represents typical items received by the FBI Laboratory. New storage and peripheral devices are being marketed daily, and no listing could ever be both current and complete. As with all evidence submissions, common sense coupled with the investigator's knowledge and background will usually be enough to insure that the computer specialist is presented with materials suitable for examination.

After the evidence is preserved and submitted to the investigator's laboratory, the examination can proceed. At the FBI Laboratory, the purpose of the examination is to make information contained in the storage media available to the investigator and prosecutor.

All types of evidence, including computer-related evidence, must be maintained so as to preserve the integrity of the evidence while it is in custody. In addition, documentation must be prepared which describes the chain of custody. It has been the experience of many laboratories that computer evidence is assigned for examination to computer specialists who work outside the scope of what is normally considered a forensic environment. These computer specialists are subject matter experts but don't necessarily have a knowledge of the special requirements and considerations for handling evidence. Consequently, it is imperative that each of the individuals assigned cases of this type is aware of these requirements and is provided appropriate training.

Appendix B outlines the basic procedures for the examination of computer evidence.

CONCLUSION

Clearly, the steadily increasing use of computers in society will soon impact every law enforcement investigative program. It is essential that law enforcement agencies be sufficiently educated and have the necessary procedures and guidelines in place to adequately manage the examination of computer-related evidence and records.

In addition to its traditional forensic examination services, the FBI Laboratory's CART can provide on-site field assistance to both FBI field offices and local police departments. Approval for this on-site support is granted on a case-by-case basis, depending upon the resources available and the needs of the requesting agency. Specific information regarding this service is available from the author.

REFERENCES

Burgess, J. (1990). No jail time imposed in hacker case. Creator of "Virus" gets probation, fine, Washington Post, May 5, section 1, page A1.

Markoff, J. (1990). Computer intruder is put on probation and fined $10,000, New York Times, May 5, section 1, page 1, column 1.

Marsa, L. and Ray, D. (1990). Crime bytes back, Omni, August, 12:11:34-36+.

Quarterman, J. S. (1990). The Matrix: Computer Networks and Conferencing Systems Worldwide. Digital Press, Maynard, Massachusetts.

Stiles, C. M. (1990). PCs – personal computers or partners in crime? Law and Order, September, 39:9:161-165.

Appendix A. Guidelines for the Preservation and Submission of Computer Evidence

I. HARDWARE

A. PC/Central Processing Unit (CPU)
1. Determine if system has an internal hard drive. If possible, secure hard drive read/write heads with the appropriate software command. Do not remove the internal hard drive from the computer.
2. Secure read/write heads in the floppy disk drives with a blank floppy diskette.
3. Label cables and ports.
4. Initial and date PC as required by your department's chain of custody procedures.
5. Wrap in plastic and box for shipment to laboratory.

B. Monitor
1. Label cables.
2. Initial and date monitor as required by your department's chain of custody procedures.
3. Wrap in plastic and box for shipment to laboratory.

C. Keyboard
1. Label cables.
2. Initial and date keyboard as required by your department's chain of custody procedures.
3. Wrap in plastic and box for shipment to laboratory.

D. External/Removable Hard Drives
1. Secure hard drive read/write heads, if possible. Some are secured by software commands, and others are secured automatically.
2. Label cables.
3. Initial and date hard drive as required by your department's chain of custody procedures.
4. Wrap in plastic and box for shipment to laboratory.

E. External Floppy Diskette Drives
1. Remove floppy diskette(s) from drive(s).
2. Secure read/write heads with a blank floppy diskette, if possible.
3. Label cables.
4. Initial and date floppy diskette drive as required by your department's chain of custody procedures.
5. Wrap in plastic and box for shipment to laboratory.

F. External Tape Drive
1. Note and record DIP switch settings.
2. Remove tape cartridge from drive.
3. Label cables.
4. Initial and date tape drive as required by your department's chain of custody procedures.
5. Wrap in plastic and box for shipment to laboratory.

G. Printers/Plotters
1. Note and record DIP switch settings.
2. Remove ribbon. Initial and date ribbon canister. (Some computer ribbons may be readable and could provide the most recent text printed on the device).
3. Label cables.
4. Initial and date printer/plotter as required by your department's chain of custody procedures.
5. Wrap in plastic and box for shipment to laboratory.

H. Modems/Acoustic Couplers
   1. Disconnect from telephone.
   2. Label cables and ports.
   3. Initial and date modem/acoustic coupler as required by your department's chain of custody procedures.
   4. Wrap in plastic and box for shipment to laboratory.

I. Cables
   1. Label both ends of each cable, describing connection to PC, printer, etc.
   2. Place in appropriate evidence container.
   3. Box for shipment to laboratory.

II. MAGNETIC MEDIA

A. Floppy Diskettes
   1. Keep away from magnetic fields.
   2. Initial and date using **FELT TIP PEN** as required by your department's chain of custody procedures.
   3. Place in appropriate evidence container. **DO NOT** use plastic envelopes because of the risk of static electric discharge.
   4. Label outside of shipment container **"DO NOT X-RAY"** to warn that evidence should be kept away from magnetic fields, and ship to laboratory.

B. Cartridge Tapes
   1. Keep away from magnetic fields.
   2. Initial and date as required by your department's chain of custody procedures.
   3. Place in appropriate evidence container.
   4. Label outside of shipment container **"DO NOT X-RAY"** to warn that evidence should be kept away from magnetic fields, and ship to laboratory.

III. DOCUMENTATION

A. Manuals/Hand Written Notes, etc.
   1. Handle with gloves to preserve for latent fingerprint examination.
   2. Initial and date all loose sheets, pads, manuals and other paper documents as required by your department's chain of custody procedures.
   3. Place in appropriate evidence container.
   4. Ship to laboratory.

B. Printouts/Listings
   1. Handle with gloves to preserve for latent fingerprint examination.
   2. Initial and date as required by your department's chain of custody procedures.
   3. Place in appropriate evidence container.
   4. Ship to laboratory.

Appendix B. Guidelines for the Examination of Computer Evidence

I. RECEIPT OF EVIDENCE

A. Log evidence into appropriate evidence control system and assign to an examiner.
1. Record date and time received by some unique numbering system.
2. Identify examiner.
3. Prepare documentation for chain of custody from evidence control to the examiner.

B. Transfer evidence to examiner.
1. Determine if other expert analyses such as accounting, drug record analysis, gambling analysis, latent fingerprint examination, etc. are necessary.
2. Prepare chain of custody documentation for other experts as necessary for complete examination.
3. Determine that all pieces of equipment listed as having been submitted are actually present.
4. Mark and initial each piece of evidence as required by your laboratory system and prepare work papers for notes.

II. EXAMINATION OF EVIDENCE

A. Determine if the submitted system is operational.
1. Review submitting communication to determine if system was operational at the time of seizure.
2. Take logical steps to render the system operational.

B. Floppy diskettes
1. WRITE PROTECT ALL DISKETTES.
2. Identify computer to be used for examination.
3. Convert operating system if necessary.
4. Create directory/subdirectory listings.
5. Check for hidden and deleted files using appropriate commercial or custom software.
6. Display and print files.

C. Hard disk systems
1. WRITE PROTECT HARD DISK USING APPROPRIATE SOFTWARE.
2. Create directory/subdirectory listings.
3. Check for hidden and deleted files using appropriate commercial or custom software.
4. Display and print files.

III. REPORTING RESULTS

A. Prepare report, documenting what you did and the results.

B. Send printouts and report to the contributor or subject matter expert for additional analysis.

C. Repack computer and all disks.

D. Return evidence to contributor .