OPERATIONAL GUIDE TO WHITE-COLLAR CRIME ENFORCEMENT

A Report of the National Center on White-Collar Crime

THE INVESTIGATION OF COMPUTER CRIME

by Jay Becker, Director
National Computer Crime Data Center
Office of the District Attorney
Los Angeles, California

Battelle
Law and Justice Study Center
4000 N.E. 41st Street
Seattle, WA 98105

The National Center on White-Collar Crime, operated by the Battelle Law and Justice Study Center, is a criminal justice improvement project established by the Enforcement Division, Office of Criminal Justice Programs, Law Enforcement Assistance Administration, U.S. Department of Justice.

OPERATIONAL GUIDE TO WHITE-COLLAR CRIME ENFORCEMENT

A Report of the National Center on White-Collar Crime

Title: The Investigation of Computer Crime

Author: Jay Becker, Director
National Computer Crime Data Center
Office of the District Attorney
Los Angeles, California

Law and Justice Study Center
4000 N.E. 41st Street
Seattle, WA 98105

This project was supported by Grant Number 77-TA-99-0008 awarded to the Battelle Memorial Institute Law and Justice Study Center by the Law Enforcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions stated 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.

THE INVESTIGATION OF COMPUTER CRIME

by

Jay Becker

TABLE OF CONTENTS

	Page
Introduction	1
I. INITIATION: GETTING REPORTS OF COMPUTER CRIME	1
A. UNIQUE ASPECTS OF COMPUTER CRIME	1
1. Low Reporting Rates	1
2. Different Sources of Information	2
B. APPROACHES TO THESE PROBLEMS	2
1. High Profile	2
2. Becoming Familiar with the Different Sources of Information	3
II. PRELIMINARY PLANNING: GETTING READY TO APPROACH THE COMPUTER	4
A. UNIQUE ASPECTS	4
1. The Combination of Complexities	4
2. The Necessity for Expert Assistance	4
B. APPROACHES TO THESE PROBLEMS	5
1. Develop a Framework for Understanding Computer Crime	5
2. Be Aware of Applicable Law	7
3. Develop a Written Investigation Plan	7
III. COLLECTION: GATHERING THE EVIDENCE	8
A. UNIQUE ASPECTS	8
1. The Nature of Computerized Evidence	8
2. The Nature of the System	8
3. Other Problems	9
4. Legal Difficulties	9
B. HOW TO MEET THE PROBLEMS	10
1. The Nature of Computerized Evidence and the Computer System	10
2. Possible Solutions to Legal Difficulties	12

TABLE OF CONTENTS, Cont.

Page

IV. PRESERVATION: WHAT TO DO WITH THE EVIDENCE ONCE YOU HAVE GOT IT 15

A. UNIQUE ASPECTS 15

1. Technical 15

2. Legal Requirements 15

B. POSSIBLE SOLUTIONS 16

1. Technical 16

2. Possible Solutions to Legal Problems . . 17

V. PRESENTATION: MAKING SURE THE CASE IS NOT THROWN OUT BECAUSE OF SOME FAULT IN THE EVIDENCE 17

A. WHAT MAKES THE AREA UNIQUE 17

1. The Lack of Technical Expertise in the Trier of Fact 17

B. VOLUME 17

C. FOUNDATION REQUIREMENTS 17

D. POSSIBLE SOLUTIONS TO THESE PROBLEMS 18

1. Repetition of the Investigative Process . 18

2. "Librarianship" 18

3. Foundation Requirements 19

BIBLIOGRAPHY 20

APPENDIX 1 - Groups Interested in Computer Crime . . . 21

APPENDIX 2 - Computer Crime Complexities 22

APPENDIX 3 - Characteristics and Responsibilities of EDP Functions 23

APPENDIX 4 - Specimen Checklist for Auditors 24

APPENDIX 5 - Search Warrant 32

ABOUT THE AUTHOR

Jay J. Becker is Chief of the Antitrust Section, Los Angeles County District Attorney's Office, and Director of the National Computer Crime Data Center. He was recently a lecturer at the FBI course on Computer Crime at the Florida Institute of Law Enforcement. He has also taught at the Annual Seminar of the American Society for Industrial Security, and at the 1978 National Computer Conference. Mr. Becker has published articles on computer crime in Crime and Delinquency, the Washington Post, Prosecutor's Brief, and Law Office Economics and Management.

THE INVESTIGATION OF COMPUTER CRIME

by Jay Becker

Introduction

The investigator faced with a computer crime allegation faces two contrasting difficulties. On the one hand, if he or she has not conducted such an investigation before, the computer is a mysterious instrument. Many people, including investigators, believe that computers and their operation can never be understood. On the other hand, a thorough investigation of a computer crime does require an appreciation of the many unique characteristics of a computer.

Consequently, the approach of this operational guide is twofold. First we list, in as great detail as possible, the aspects of the investigative process which are unique features of a computer. Secondly, we try to offer practical solutions to those unique problems. No pretense of final or ideal solutions to these problems should be inferred from these suggestions. The most important aspect of the manual is to alert the investigator to the variety of problems which he or she may face. Although we believe that the suggestions offered will prove useful, and often have proven useful to other investigators, an investigator using his or her own common sense, experience, or intuition may find that all the circumstances dictate a solution different than that which we have suggested.

I. INITIATION: GETTING REPORTS OF COMPUTER CRIME

A. UNIQUE ASPECTS OF COMPUTER CRIME

1. Low Reporting Rates

Non-reporting represents a serious problem in the area of computer crime--far more than is even the case with white-collar crime in general. IBM and the U.S. Chamber of Commerce estimate that no more than 15% of all computer crime is reported.

Several reasons appears to lie at the base of this non-reporting. A primary one is the fear on the part of businesses that admitting their computer's fallibility will have a severe effect on their customers' confidence in the business operations. Additionally, businesses may well assume that local law enforcement agencies do not have the expertise to deal with computer crimes. The third possible factor is the absence of the usual "old boy" networks through which company security personnel might become familiar with local law enforcement officers who are interested and experienced in investigating computer crime cases.

2. Different Sources of Information

From the law enforcement side, part of the problem in determining the existence of computer crime offenses is the fact that different professional people are likely to be the source of reports of potential computer crime cases. Systems analysts, auditors, and programmers--people seldom seen in a police station--have an important role in communicating both the possibility of a computer crime and the dimensions of that crime.

B. APPROACHES TO THESE PROBLEMS

1. High Profile.

If your office has an interest in investigation of computer crime cases because of its belief that the business community and the consumers (who bear the business community's losses) deserve this protection, let your community know it. Press releases about your completion of a course in white-collar crime investigation, which includes the investigation of computer crime, are just one of many ways to alert the public to your office's new computer crime investigation capabilities. There are a variety of organizations whose membership can provide valuable leads in the investigation of computer crime.* These include the ACM (Association for Computer Machinery); DPMA (Data Processing Management Association); AICPA (American Institute of Certified Public Accountants); ASIS (American Society for Industrial Security); ASA (Association of Systems

* See Appendix 1 for addresses of these associations.

Analysts), and of particular importance, the EDP Auditors Association. These groups may have subcommittees which are addressing themselves to issues involving computer crime.

2. Becoming Familiar with the Different Sources of Information

The systems analyst and the internal auditor have unique contributions to make in the investigation of computer crime. Appendix 2, the chart describing the complexity of computer crime cases, indicates in summary form the areas of assistance of internal auditors, systems analysts, and the businessman himself.

The internal auditor is an employee of a business who has as his main function the establishment of management controls for the business systems. Often this responsibility extends to the company's computer system. "Controls" is the word used in the auditing profession to denote rules and practices whereby the business component parts run smoothly. Thus it is the internal auditor's task to see that the computer system is not being used to commit crimes and that it is reasonably secure from attempts to use it to commit crimes. To do this, an auditor has a variety of testing procedures to apply to the systems. Appendix 4 demonstrates the extensive attention that an internal auditor should pay to the computer system. As a result of this attention, the auditor may well be able to detect irregularities in the system before the businessman has discovered any loss.

The external auditor works for an accounting firm, and he is customarily called in by a company to provide impartial analysis of its systems. Where the internal audit capacity is undeveloped in a company, or where there is a question as to the honesty of an internal auditor, an investigator may want to call upon an external auditor to help analyze a suspect computer system operation.

The systems analyst also has a concern for the efficiency of the computer system. His concern is less with the detailed checks than an internal auditor uses, and more with the ability of the computer system to accomplish its computing tasks in as

accurate and economical way as possible. The systems analyst usually has substantially more understanding of the machinery of the computer system. His help will probably be necessary to fully explain the computer mechanisms through which the irregularities detected by the auditor have been accomplished.

Appendix 3 summarizes the areas of concern of the different kinds of specialized EDP personnel.

II. PRELIMINARY PLANNING: GETTING READY TO APPROACH THE COMPUTER

A. UNIQUE ASPECTS

1. The Combination of Complexities

A computer crime investigation is difficult not only because it involves a computer, but also because the effect of the computer is often to severely complicate every other aspect of the investigation. One needs to understand something about the complex mechanisms of programming, the internal workings of the machine, and the methods by which it is connected to any remote input or output devices. One must also understand and deal with business and legal problems which are also much more complex than when only manual systems are involved.

2. The Necessity for Expert Assistance

One can no more investigate a complex computer crime case by himself than one could investigate an art forgery, a securities swindle, or accusation of death resulting from medical malpractice. The combination of complexities means that other experts may be needed to explain the computer context, the business context, or even the legal context. It is important that the investigator know where to find these experts, what sorts of questions they can be expected to help him answer, and how to understand their responses.

B. APPROACHES TO THESE PROBLEMS

Appendix 2 demonstrates the interaction of legal, business, and computer complexities and the personnel who may be relied on to assist the investigator in winding his way through this maze of complexities.

1. Develop a Framework for Understanding Computer Crime

In order to best understand experts who describe the mechanisms and the effects of computer crimes, and also to develop your own sense of whether a computer crime has taken place, it is important to have a clear understanding of the context of computer crime. This understanding should include a working knowledge of each of the following:

(a) What are the vulnerable points of a computer system?

There are a number of vulnerable points in computer systems, each of which is subject to attack by computer criminals. Some of the major ones are discussed in Chapter 4 of Users Guide to Computer Crime by Liebholz and Wilson. (see Bibliography, p. 20 of this guide)

(b) What are the threats at each vulnerable point?

The discussion in Chapter 4 also indicates the types of acts which can be committed at each vulnerable point.

(c) What are the dynamics of software development?

It is important to keep in mind that changes in a computer program may result from any of a number of steps in the development of the program. Before a program is actually put into operation, the following steps may take place:*

1. A programmer writes a module (or segment) of the program.
2. The programmer's manager inspects the program and signs a sheet which accompanies the program.
3. A central testing group tests the module in a variety of situations. (In a small installation, the programmer may do his own checking.)

---

* This list tends to apply mainly to a larger computer user which has remote terminals as part of its machinery.

4 An "Application Control Group" approves the module and gives permission for it to be placed in a file of live programs.

5. An "Operations Group" enters the module into the live program file (that is, into the computer itself).

6. The module is tested as part of the computer system.

7. A "Functional Group" checks the operation of the module to insure that it does what they want it to do.

8. Terminal users use the new module to insure that it is satisfactory for users.

From this detailed description, the possibilities for both fraud and its detection should appear to be numerous. A wide variety of employees will have access to the computer program, as it is developing. They may inject their own dishonest programming or that of others. In trying to ascertain how illegitimate parts of the program got to be there, one may well have to go through each of the steps outlined above to find the initial source of the program change.

(d) Be aware of the variety of "Documentation" in a computer system.

"Documentation" is defined as a detailed description of a computer procedure or set of procedures. It may specify the files and programs required for input, the files and reports a system produces, the criteria for the system, or instructions for action to be taken in response to any unanticipated efforts.

In planning a computer investigation, a thorough awareness of the types of documents used in the business in question is vital, since these records will often demonstrate more clearly how the system should work.

The investigator should be aware of five types of documentation:

1. Program Problem Definition
2. System Documentation
3. Program Documentation
4. Computer Operation Documentation
5. User Documentation

A computer application may well have the following sorts of documentation: (1) a written statement of the problem which the application seeks to solve; (2) a flow chart, indicating the information flow which the application will follow; (3) record layouts, or descriptions of where information will be found in the records used by the system; (4) data editing requirements; (5) program flow charts, which break down the system into the subdivisions of the system and detail the manner in which these subdivisions work; (6) program source listing; (7) test data; (8) operators instructions; (9) summary of controls; (10) approval and change records; (11) examples of input documents; and (12) samples of output reports.

Each company has its own documentation system. A first step in investigation is to get a list of the documentation used by the company involved.

2. Be Aware of Applicable Law

To investigate a computer crime, like any other crime, it is necessary to know the elements of the crime one seeks to prove. Although most computer crimes will fit into the general area of theft, difficult questions concerning the property value of information may arise. The investigator should be aware of any state laws specifically related to computer crime, and whether any federal laws apply. Presently, pending before the U.S. Senate is the "Computer Systems Protection Act," which would create a wide variety of federal crimes involving computers. The investigator would also want to check other applicable federal statutes such as those relating to mail fraud and securities fraud in appropriate cases.

3. Develop a Written Investigation Plan

More than in the ordinary investigation, a written plan for the conduct of the computer crime investigation is a necessity. The plan should involve the names of the areas, person, documents, files, and other relevant aspects of this case which are to be

investigated. It should include investigation of the company's background, prior crime problems it has experienced, provisions to gather organization charts, functional flow charts, the job descriptions of its employees, the company's financial statements, and its personnel files.

The plan should be as complete and as organized as possible. The investigator should be aware of the possibility of using this document as evidence when the case goes to trial, and thus should attempt to make it clear enough for a juror or judge to understand how the investigation was initiated.

III. COLLECTION: GATHERING THE EVIDENCE

A. UNIQUE ASPECTS

1. The Nature of Computerized Evidence

Several aspects of computerized evidence have direct bearing on the investigator's task. Evidence in a computer is much more "dense" than in any other information system. That is, a single computer tape can contain as much information as a shelf full of books. Consequently, the ease of destroying the information is much greater and the value of the information to a potential thief is greater as well. Furthermore, much of the information is not visible without the use of some device to translate it from electronic symbology to print. Being invisible, the information is also more subject to "booby traps" or illegitimate programming designed to destroy the information should an investigator attempt to reproduce it.

2. The Nature of the System

The computer system itself is dynamic: it consists of information and programs within a computer that is usually in operation. It may not be possible to gather the information one wants out of the computer without shutting down the business operation which the computer

has been set up to run. Furthermore, the data on the magnetic tapes, disks, and other storage media cannot be used to produce the hard copy reports that were produced except through use of the same programs and hardware. And while there are many areas of computer compatibility, one cannot in general obtain any information off tape or disk unless one has compatible systems and usually a similar computer model. A further practical problem for the investigator is the enormous volume of evidence that a computer center may contain. In the Equity Funding case, some 3,000 reels of computer tapes were potential evidence.

3. Other Problems

The type of evidence which the investigator will want to look at and possibly seize are different than in the normal investigation. Documentation is the most common form of evidence, other than the computer tapes, disks, and other storage media. In unusual cases, the equipment itself might be required. The complexity of the computer case may well make it much more difficult to specify the instrumentality of a computer crime before an investigation has begun. Thus, a certain amount of "fishing" may be necessary to understand how it is that the crime in question was committed. Likewise, the complexity of the crime involved may make it hard to determine who the potential defendants are in certain cases. Thus, the investigator must gather information without tipping off the defendants and enabling them to cover their tracks.

4. Legal Difficulties

Each of the approaches to evidence collection described below has its difficulties:

(a.) Consent Searches: Where the complexity of the case makes the identity of the crime perpetrators hard to discern, a request for a consent search may be counter-productive if it affords the criminal the opportunity to destroy evidence.

(b.) Search Warrant: Where surprise is desired, a search warrant may seem preferable to a consent search. Few judges have ever signed a search warrant involving the technical proof of probable cause which may well be presented in a search warrant for a computer system. Additionally, judges have seldom had the opportunity to fashion a search warrant with the sorts of provisions needed to protect evidence once the investigator has gone to the location of a computer system. The requirement that the items to be searched must be narrowly and specifically defined may require an enormous amount of description for the investigator in order to cover each component of the computer system which he seeks to inspect or seize. The affiant in an application for a search warrant will often be a technician and his affidavit may well be written technically.

(c.) Right to Privacy: Whatever the method used to gather evidence from the computer system, the right to privacy in personal information contained in the computer system may present additional problems.

B. HOW TO MEET THE PROBLEMS

1. The Nature of Computerized Evidence and the Computer System

The major investigative technique is simple awareness. Keeping in mind the problems outlined in Part A of this section, particularly those of a technical nature, will often be sufficient to dictate the appropriate response in a computer crime investigation.

Variables such as whether the complaining witness is someone who can be trusted, whether the employees working in the computer center can be trusted, whether the existence of a law enforcement investigation is already known to many individuals in the company, all will have a significant effect on the course of action one takes when going to actually seize the evidence in question. Nonetheless, some general procedures may be suggested:

- Check with the victim and find out to what extent there are back-up copies of the tapes or other data storage media which you seek to inspect or to seize. It cannot be assumed that the back-up copies are identical to those presently in use, since there would probably be little motivation for a computer thief to change the back-up copies, as well as the original copies. The back-up copies are useful, however, to allow the computer system to continue in operation while those copies which were actually in use in the system are removed to be duplicated or seized.

- It may often be desirable, if not necessary, to duplicate the controls of each of the information-storing devices in the computer system, be they tapes, disks, cards, etc., so that subsequent changes in the system do not impair the investigation. When such duplication takes place, make sure that the foundation requirements referred to below in Sections 4 and 5 are strictly observed.

Despite the enormous size of the Equity Funding data base--more than 3,000 rolls of computer data--a copying project was undertaken, and a duplicate of every tape on the premises was prepared as one of the first steps in the investigation. All copying was done on the Equity Funding computer equipment. The originals were transported to a vault away from the Equity Funding scene, and the business was allowed to continue with the duplicate tapes.

Where a large volume of tapes or other media are likely to be seized, preparation should be made ahead of time for the removal and storage of these tapes. (See the discussion below concerning preservation of evidence for further suggestions as to what sort of preparations are appropriate.)

The dynamic nature of the computer system necessitates keeping as many employees whose possible involvement in the crime is unclear away from the computer system for as long as

possible. This may be easily accomplished in a small system where the seizure can be completed fairly quickly. In a major investigation, one must consider the possibility of furloughs or other enforced leaves for those employees who are not cleared, and if necessary, convincing the victim to bring in temporary help to run the computer operation while the investigation is ongoing. It may often be necessary to pinpoint those areas of greatest sensitivity and deploy law enforcement personnel to secure these areas when it is not possible to segregate out all those employees who may have some role in the computer fraud. Special control systems may be appropriate when a large number of suspect personnel are allowed to continue at work in the computer center. These might include the audit trail with the requirement that no input be made into the machine without a hard copy being produced at the same time.

2. Possible Solutions to Legal Difficulties

(a.) Consent Searches: Where the element of surprise is required, a request to perform a consent search may be accompanied by a prepared search warrant. Thus, if consent is granted, the consenting party will not have time to destroy evidence, and if consent is not granted, the search warrant can be immediately served and no loss of time will accrue.

In such cases, the consent should be written. The investigator should thus come with a prepared search consent form which is as extensive in its scope as possible. Cases are quite clear that search pursuant to consent can be no more extensive than the consent. It is far preferable to have written proof of the scope of the consent rather than to chance an adverse determination by a trier of fact (i.e., judge or jury) as to whether the consent covered certain specific areas. The search consent form should generally

be as specific as possible, perhaps couched in the same terminology as the request for a search warrant, as well as containing several general provisions enabling the investigator to search in those areas that he or she has not been able to adequately and specifically define. The purpose of the specificity is to preclude the subsequent argument that the person giving consent did not understand the language of the consent to extend to those specific areas which the investigator has searched.

(b.) Search Warrants: It is necessary to exercise great care in preparing a search warrant in a computer crime case, mainly because this is a technical area often new and unfamiliar to judges. The investigator should have a detailed affidavit which covers all the technical bases, but which is comprehensible to someone who knows nothing about computers. The technical affiant should be available for questioning by the magistrate being asked to sign the search warrant.

Specificity is important wherever possible. Limit the time period to which the records sought to be seized pertain, as well as the number of persons whose records are sought, wherever this can be done without jeopardizing the investigation.

A copy of an actual state search warrant is included in Appendix 5.

Where appropriate, request permission to shut down the operation of the business for a reasonable time to protect the evidence as part of the search warrant. Such permission is unusual and will require extensive justification, both factually

and legally. Facts must be brought before the court to show that anything short of this drastic step will severely endanger the investigation. Legal authorities, which will have to be provided by the prosecutor assisting in the preparation of the search warrant, will have to show that under these unusual factual circumstances the remedy sought is appropriate.

Additional permission will probably be required before an expert is allowed to touch the victim company's computer. Again, a similarly detailed and persuasive factual and legal argument will be needed before a magistrate grants this unusual permission. Even where the search warrant does provide for the expert's operation of the computer system, it is better to have the consent of the victim and the victim's attorney, where possible, before such operation is begun. There is always a danger that at a later data an objection will be raised along the line that the data was changed by the expert's "meddling" with the victim's system.

(c.) Right to Privacy: Where the information sought relates to individual clients or customers of the victim company, it will be well to get a consent from the victim company to the search based on the company's belief that it is a victim of a crime and that it requires the search of the evidence in question to protect itself from loss resulting from this crime. The specific requirements of this consent will depend on the individual jurisdiction's definition of the right to privacy in such business records and its definition of an exception to this right where the records are maintained by a company which believes itself to be the victim of a crime.

(d.) Administrative and Grand Jury Subpoenas: Where an industry is regulated, or is otherwise the subject of an administrative or grand jury subpoena, consideration should be given to the use of either of these approaches as well.

(e.) Emergency Seizure: Where an investigator believes that evidence is being destroyed or a crime is being committed while

he is in the process of serving a warrant or conducting a consent search, or just is involved in a general investigation, he may go beyond the authority he had to search previously, and seize evidence to prevent the commission of that crime or the destruction of that evidence.

IV. PRESERVATION: WHAT TO DO WITH THE EVIDENCE ONCE YOU HAVE GOT IT

A. UNIQUE ASPECTS

1. Technical

(a.) The Possibility that Evidence Cannot be Moved: Although few cases fit into this category, it is possible that the evidence of the commission of a computer crime is not to be found in the programming or the data storage media, but in the machinery itself, perhaps involving communication gear. It may not always be possible to remove the machinery from its location. Nor may it be possible to keep the machinery from being used.

(b.) Maintenance Requirements of the Evidence: It will not be self-evident to the investigator how a computer tape can be preserved. Improper storage may result in warpage or other damage, rendering the tapes unreadable.

(c.) Volume: Closely related to the general maintenance requirements for computer tapes and other data preservation media, are the problems presented by the enormous volume of evidence that may present itself to the investigator at the conclusion of a major seizure.

(d.) Visual Fungibility: Computer tapes are not necessarily distinguishable to the human eye. It is necessary to develop permanent marking systems to keep track of the evidence which is seized.

2. Legal Requirements

A basic requirement for the admission of evidence is proof that "The condition of the object is substantially unchanged." (McCormick, Evidence, pp. 527-528 , 1972.)

B. POSSIBLE SOLUTIONS

1. Technical

(a.) Immovability of Evidence: Where the mountains of evidence cannot be brought to the custodian of evidence, the custodian must be brought to the mountains of evidence. In this rare sort of case, either through consent of the parties involved or by way of court order, one might consider establishing a 24-hour guard in the office of the victim company to safeguard the evidence in question. This procedure was used in the Equity Funding case.

(b.) Expert assistance should be sought whenever there is any question as to the storage of materials gained through a seizure of evidence. Such simple matters as how tapes are to be stacked, the ranges of safe temperature to maintain them in, and possible magnetic, electrical, or other dangers to the security of the data must be considered.

(c.) & (d.) All items which are seized must be carefully indexed. A 5-step approach has been suggested to deal with the problems of keeping track of large volumes of computer evidence:*

1. The investigator's initials and the date should be scratched onto each tape reel. The tape canisters which are usually marked to identify computer tapes they contain are too easily interchanged.
2. Magnetic disks should be identified with the investigator's initials and date being scratched onto the metallic bottom of the disk.
3. The tape identification number should be scratched onto the tape or disk as well.
4. The computer center may have a perforator which can make a "permanent" marking on the tape itself. The tape normally has considerable "leader" or blank tape.
5. Some storage media (e.g., some disks) may not be readily removable. To perpetuate the data in such

---

* See Coughran, Computer Abuse and Criminal Law, pp. 29-61.

a system, it would be necessary to have a print-out made of the data stored in the memory component.

2. Possible Solutions to Legal Problems

To establish that the evidence is substantially unchanged, the investigator must be ready to prove a complete chain of custody. Where the seriousness of the case warrants it, a 24-hour guard over the evidence locker with strict logging procedures whenever the evidence is removed is ideal. In any case, a system must be developed which carefully maintains evidence of the chain of custody. From the beginning of the search, careful indexing must be maintained of all the evidence which is seized.

The expert assistance that is used to make sure that the evidence is not damaged in storage should be kept available for testimony to that effect, should there be any challenge to the contents of the information at the time of trial.

V. PRESENTATION: MAKING SURE THE CASE IS NOT THROWN OUT BECAUSE OF SOME FAULT IN THE EVIDENCE

A. WHAT MAKES THE AREA UNIQUE

1. The Lack of Technical Expertise in the Trier of Fact

Whether judge or jury, the trier of fact is unlikely to have any depth of understanding of the components of a computer system.

B. VOLUME

In many computer cases, the volume of tapes which are in evidence can be staggering.

C. FOUNDATION REQUIREMENTS

In order to gain admission into evidence, the computer tapes which have been seized must be shown to meet the following requirements:

1. They were made in the ordinary course of business.
2. The information was placed in the computer within a reasonable time after the act or transaction to which they relate.

3. The source of the information contained in the evidence must be one in which is reliable and one which can be communicated to the trier of fact.
4. The methods and circumstances of the preparation of the evidence must be such as to provide reason for the trier of fact to believe that the evidence is reliable.*

Although representing a careful and extensive treatment of the problem of the admission of computerized documents into evidence, the Genser decision is only the decision of the court in one jurisdiction. The foundation requirements will vary from state to state.

D. POSSIBLE SOLUTIONS TO THESE PROBLEMS

1. Repetition of the Investigative Process

The investigator who began his case as less than an expert in computers and the detection of computer crime can turn his initial inexperience to an advantage by maintaining the records of his investigation through each step from initial planning to the completion of the gathering of evidence. Then, in testimony, before the court of jury, he should be able to refer to extensive notes and explain exactly what he did in the investigation of the crime. If the investigator cannot explain what he did to a traffic dispatcher, a secretary, or someone else equally untrained, he or she will have difficulty making an effective presentation to the trier of fact.

2. "Librarianship"

Effective investigation of a computer crime case will take on certain elements of librarianship. Where the investigator has seized hundreds of reels of tape, he must have made detailed notes at the time of the seizure, and be able to translate those notes for the trier of fact in such a way as to minimize his

---

* These four criteria are those specified in the case of Monarch Federal Savings & Loan Assn. v. Genser, 383 Atlantic 2d 475 (1977).

exposure to the cross-examiner's attempt to cast doubt as to the accuracy of his records.

3. Foundation requirements will be met by testimony from the individuals in the victim's company responsible for the maintenance of the computer. The Genser case indicates that the specific individual responsible for placing information into the computer need not testify, so long as someone can testify that the information was ordinarily entered into the computer in the ordinary course of business. It is important to line up witnesses who can testify to the following information, however:

a. What is the original source of the computer program? That is, the witness must be able to explain sources and meanings of any calculations, formulas or abbreviations appearing in the computer printout.

b. Can the printouts be verified from the sources of the information?

c. Were the computer operators competent? That is, did they understand the operation of the computing equipment, and was it their regular duty to operate the equipment?

d. Was the type of computer used one which is accepted in the field as standard and efficient equipment?

e. Was the procedure for the input and output of information reliable, based on the controls and the test and checks for accuracy and reliability of the system?

f. Were the mechanical operations of the machine such as to insure that the machine operated properly?

g. What is the meaning and identity of the records themselves?

In response to these requirements, it is clear that the investigator, in cooperation with the prosecutor of the case, may have to spend a considerable amount of time in conversation with the victim company's personnel to ascertain that each of the foundation requirements can be met. A technically sophisticated defense lawyer may well have a field day challenging these requirements where the prosecution is not ready to bring forth evidence that each of them has been met.

BIBLIOGRAPHY

Books

August Bequai, Computer Crime, D.C. Heath & Company, (1978), Chapters 10, 13, 14.

John Carroll, Computer Security, Security World Publishing, (1977), Chapters 1, 2, 18, 20.

Edward Coughran, Computer Abuse and Criminal Law, Computer Center, University of California, San Diego, (1976), Pages 29-61.

Stephen Liebholz and Louis Wilson, User's Guide to Computer Crime, Chilton Book Company, (1974), Chapters 12, 13, 14.

William Maier, Computer Control and Audit, Institute of Internal Auditors, (1978), Chapters 6-10.

James Martin, Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall Publishing Company, (1973), Chapters 33, 34-39, and Appendices 3, 9, 15, 23, 29, 31.

Donn Parker, Crime by Computer, Scribner's, (1976), Chapters 7, 13.

Thomas Whiteside, Computer Capers, Thomas Y. Crowell Company, (1978), Chapter 5.

APPENDIX 1

GROUPS INTERESTED IN COMPUTER CRIME

1. ACM - Association for Computing Machinery
   1133 Avenue of the Americas
   New York, NY 10036

2. AICPA - American Institute of Certified Public Accountants
   1211 Avenue of the Americas
   New York, NY 10036
   Wallace E. Olson, President

3. ASIS - American Society for Industrial Security
   2000 "K" Street N.W.
   Suite 651
   Washington D.C. 20006
   O.P. Morton, Executive Director

4. DPMA - Data Processing Managers Association
   c/o Carl Spencer - Membership Director
   Price Waterhouse
   1880 Century Park East
   Los Angeles, CA 90067

5. EDPAA - EDP Auditors Association
   c/o Leon F. Olsen - Vice President
   427 West Dryden Street, # 214
   Glendale, CA 91202

6. EDPAF - EDP Auditors Foundation
   P.O. Box 8184
   Fountain Valley, CA 92708
   J. Friou, President

7. IIA - Institute of Internal Auditors
   249 Maitland Avenue
   Altamonte Springs, FL 32701

8. NCCDC - National Computer Crime Data Center
   Office of the District Attorney
   320 West Temple Street, Rm. 540
   Los Angeles, CA 90012
   Jay Becker, Director

APPENDIX 2

COMPUTER CRIME COMPLEXITIES

Computer crimes have three aspects: (1) Business, (2) Computing, and (3) Law. The auditor, the systems analyst, and the businessman can help the investigator in a variety of ways including the following:

ASPECT OF CRIME

Who can Help?	Business	Computer	Crime
Auditor	1. What is proper business procedure? 2. How has criminal subverted this procedure? (i.e., where did money or other asset go?)	1. What are procedures and safeguards against this sort of crime? 2. Were they followed?	1. Could subversion of the system have been innocent? 2. Is this a common M.O. he has seen in this company or elsewhere?
Systems Analyst	Same as Auditor	Same as Auditor --Also: 1. What is system configuration? 2. What is available documentation?	Same as Auditor --Also: 1. Who had most opportunity to commit crime? 2. What other physical evidence is available?
Businessman	1. What is effect of crime on victim company?	1. What will happen if computer is down (for one day, one week)? 2. What is history of system?	1. Who are likely suspects? a. Personnel b. Competitors c. Ex-employees

Appendix 3

Maier, W. Computer Control and Audit. Altamonte Springs: Institute of Internal Auditors, Inc., 1978.

APPENDIX 3

CHARACTERISTICS AND RESPONSIBILITIES OF EDP FUNCTIONS *

FUNCTIONAL GROUPINGS	FUNCTIONS INCLUDED	GROUP CHARACTERISTICS	RESPONSIBILITIES
INFORMATION PROCESSING FUNCTIONS	Operation of computer and related equipment Data conversion Library Control group	Highly repetitive work loads predictable and subject to scheduling Operations routine require supervision Instructions necessary Operations subject to performance measurement Visible results for users Quality of controls, readily determinable	Achieve efficiency for group as a whole Maintain committed schedules High level of accuracy for data processed Maintain quality consciousness for group as a whole
PROJECT FUNCTIONS	Systems development Procedures and forms Quantitative analysis Programming	Only nominally repetitive Long duration Projects with structured activities for visible interim results High level of interpersonal skills Numeric orientation (quantitative analysis) Systems analysis skills necessary	Understand objectives, responsibilities and functioning of user organization Improve effectiveness of user through application of EDP processing
TECHNICAL SERVICES FUNCTIONS	Equipment selection Software and operating system selection Program maintenance Quality assurance	Highly technical Results may have low user visibility	Technical support to operating and project functions Improve efficiency and effectiveness of operating and project functions Development and maintenance of standards for computer operations Monitor compliance with standards

* From Computer Control and Audit by William Maier, Copyright 1978 by the Institute of Internal Auditors, Inc., 249 Maitland Avenue, Altamonte Springs, Florida, 32701. Reprinted with permission.

Appendix 4

Martin, J. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs: Prentice-Hall Publishing Co., 1974

APPENDIX 4

Checklists and Summaries

Table D.29. Specimen Checklists for Auditors*

The following checklists are based on actual questionnaires that are in effective use in several different organizations.

Checklists for accuracy control, control of terminal operators, physical theft protection, file construction software features, and control of classified documents are not included as these are dealt with at length in the earlier tables.

1. CONTROLS ON PERSONNEL	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
Are responsibilities divided so that fraud cannot be carried out without collusion?						
Are departments and close associates separated so as to minimize the likelihood of collusion?						
Are personnel handling the corporation's assets entirely separate from personnel involved in data processing?						
Are background checks performed on all new hires?						
Are critical personnel bonded?						
Do managers know their subordinates sufficiently well to detect disgruntled employees, or employees who are in trouble; who might be a threat to the installation?						
Can employees who constitute a threat be transferred or dismissed immediately?						
Are critical jobs rotated periodically?						
Are employees cross-trained so that if any critical employee becomes unable to do his job another can immediately take it over?						
Is the level of training sufficiently high?						
Is there a continuing education program?						
Is security included in this program?						
Do all personnel take security seriously?						
Are casual practices—such as leaving classified documents unlocked—to be found?						
Is a "clean desk" policy enforced?						
Controls on programmers—See Table D.19						

* From James Martin, Security, Accuracy, and Privacy in Computer Systems (Prentice-Hall Publishing Company, 1974) Reproduced with permission.

Table D.29. (continued)

2. SENSITIVE PROGRAMS	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
Definition of a "sensitive" program: A sensitive program is one in which a programmer can, by changing program instructions *only*, misappropriate company assets and conceal the act even though adequate administrative processing controls are in place. They are the programs in the system where important internal control tests are made. The more sensitive areas have been identified as Payroll, Accounts Payable, Fixed Assets, Purchasing, and Inventory Control. (Note: Although there may be many programs in a given system, such as Accounts Payable, only a small number may contain internal control tests. These should be identified as the sensitive programs. The other programs should not be identified as such. To identify all programs in Payroll, Accounts Payable, etc, as sensitive defeats the purpose of the control which is to establish reasonable protection from programming fraud without burdening the location. Controls over unnecessary programs make the controls costly and less effective.)							
1. Is there a control list for sensitive programs identifying the responsible programmer and his manager?						
2. Is there adequate separation of maintenance responsibility for sensitive programs between programmers?						
3. Are programs and documentation stored in a secure location to prevent unauthorized access? Each storage area should maintain a log that shows the program requestor's name, date, and authorization reference.						
4. Is unauthorized patching and changing of sensitive programs prevented, or could a programmer or operator bypass the safeguards?						
5. Does an independent party review all requests for updates to sensitive programs, and advise management of questionable changes?						
6. Is there controlled maintenance of a history of assembled programs? Local management discretion should be used on the number of documented changes to be maintained, since frequency of change will vary by program.						
7. Are there sufficiently frequent unannounced periodic audits of program changes for authorization and documentation?						

Table D.29. (continued)

4. INPUT/OUTPUT CONTROLS	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
1. What controls exist for input of sensitive data from point of origin?						
2. What controls exist for the distribution of output to designated areas?						
3. Are controls established for point of origin review of rejected sensitive transactions?						
4. What type of controls are established for correcting errors in input/output with the point of origin?						
5. Are predetermined totals or item counts maintained within the DP operation and compared with keypunch, unit record, or computer output prior to being sent to the customers? The person maintaining the controls should not be involved in processing the data.						
6. Keypunching–are all important data fields subject to mechanical verification by operators using verifier machines?						
7. Are limit checks included in appropriate programs? On input? On output? Is appropriate action taken when limit checks are violated?						
8. Review the controls listed in Tables D.8 and D.12. Should any of these be added to the controls currently in existence?						
9. Is appropriate segregation of duties in effect for persons who handle sensitive data?						
10. Are data control personnel provided with schedules listing the dates that programs will be run, the due in and due out times, the dates for customers providing input data and the date for distribution of output. Schedulers should monitor the flow of work. *Note:* This will facilitate the flow of work to the computer and reduce idle time awaiting input.						
11. Is the backlog of jobs reasonable? Review for excessive delays.						
12. Is rerun time due to error by operator, programmer, or other Information Systems personnel segregated and charged to department overhead?						

Table D.29. (continued)

4. INPUT/OUTPUT CONTROLS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
13. Has responsibility been established for following up all input errors to ensure that they are properly corrected and returned for processing?						
14. Are the exceptions (or significant events) logged by Machine Operators reviewed by management and is action taken?						
15. Are reasons determined and corrective action taken for rerun hours (machine-operator-input-program)?						
16. Are all significant deviations from targets established for "hands on" time rerun checked?						
17. What is done about low utilization machines and overload situations?						
18. To test the system's validation controls, the auditor should feed in invalid transactions and see what the system does with them.						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
1. Have computer center operating procedures been written?						
(a) Are they sufficiently descriptive in detail to guide the organization and operation?						
(b) Are they kept up-to-date?						
(c) Does the computer center operate independent of the programming area?						
2. Do operators' instructions for running each job include:						
(a) Identification of all machine components used and purpose?						
(b) Identification of all input/output forms?						
(c) Explanation of purpose of run?						
(d) Detailed input and output disposition instructions?						
(e) Identification of all possible programmed halts and prescribed restart instructions?						
3. Is an operating log maintained to record any significant events and action taken by the operator? (Proper recording would indicate whether operators were following instructions for halts in programs, etc.)						
4. Is the operator log inspected daily by management?						
5. Are the pages of the operator log prenumbered, or is some other method used to ensure total accountability?						
6. Are data control center personnel and operators' assignments rotated? (This not only aids in cross-training, it helps avoid fraudulent manipulation of jobs.)						
7. Are logs maintained to record the CPU meter readings (for both customer and CE meters) at the start and end of each shift? Are variances explained?						
8. Are CE maintenance logs kept current? (These logs are especially important when recording reruns caused by machine failures. This time should be claimed against any additional billable time.)						
9. Are trouble reports prepared when processing is interrupted because of operator or program(mer) error or machine failure? (The reports should indicate what caused the problem and what action was taken.)						
10. Are computer room personnel the only individuals allowed to operate the machines?						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
11. If programmers operate the machine, is this time controlled?						
(a) Are programmers required to obtain written permission from their department manager for all "hands on" time?						
(b) Is management able to determine whether programmers are making excessive tests and assemblies due to poor programming techniques? Is control adequate?						
(c) Are targets for reasonable "hands on" time rerun due to operator or programmer error established?						
12. Are operators denied access to program flow charts, source decks, program listings, etc.? (The operator does not need access to these items to perform his duties. Consequently these items should be maintained outside of the computer room to prevent changes to programs or operation by computer operators.)						
13. Do programmers test their programs with "live data"? Are there procedures in effect to control this?						
14. Are adequate safeguards exercised to ensure that only authorized persons are permitted in computer or machine areas? Are these safeguards effective in practice?						
15. Do operators know what to do when an unauthorized person does come into the machine room and is intent upon stealing something or doing harm?						
16. Do the operators know what to do in the event of fire or other emergency?						
17. Is there a surveilling escort for all visitors?						
18. Are demonstrations controlled?						
19. Are computer operating staff adequately screened before hiring?						
20. Are all computer runs supported by a work request or other written authorizations? (This includes scheduled and nonscheduled production assemblies and tests.)						
21. Are the above approved by management? If not, are there other controls to ensure that *all* computer runs are justified?						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
22. Are there provisions for scheduling of jobs on the system? These provisions would include:						
(a) Due dates of input and output						
(b) Records covering delays in receipt of input; processing of data; delivery of output						
(c) Establishment and adherence to priorities						
23. Is all input data accompanied by control totals, or other control information (such as number of cards, reels of tape and records per tape, etc.)?						
24. Are control totals produced independently by the tape/disk/drum loading program?						
25. Are input, load, and output totals reconciled after processing?						
26. Input errors; Are the users provided with data error listings that report on the accuracy of their input data?						
27. Are there procedures to extend document control to such items as blank checks, stock certificates, etc.?						
28. Is adequate control maintained over the input and output data? (Trace the flow of operational data through the computer and/or machine room.)						
29. Are system utilization and usage reports distributed to management for their review of:						
(a) Operating system reporting						
(b) Productive time						
(c) Program test and assembly						
(d) Operating system generation (Sysgen)						
(e) CE maintenance time						
(f) Programmer "hands on" time						
(g) Demonstration time						
(h) Rerun time						
(i) Idle time						
(j) Power off time						
(k) Other (other location backup, etc.)						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
30. Is "productive time" broken down into scheduled and nonscheduled production? (Periodic comparison of productive to nonproductive time and scheduled to nonscheduled production is necessary to ensure reasonability. The Utilization Reports are also needed to evaluate system effectiveness and profitability; help plan manpower and hardware work loads; provide a basis for scheduling new job capacity.)						
31. Are "turn-around" (time on and time off the system) reports distributed for Management review?						
32. Are procedures for billing charges for computer usage and/or cost allocations, if applicable, based upon operating records?						
(a) Can departmental charges be reconciled back to the usage/utilization reports or turn-around reports?						
(b) Is rerun time caused by programmer, operator, systems personnel or machine error segregated and charged to overhead rather than to the using department?						
(c) If using departments are not charged for computer time, is there a procedure to ascertain the need for regularly scheduled production jobs?						

IN THE

MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT,

COUNTY OF SANTA CLARA, STATE OF CALIFORNIA.

SEARCH WARRANT

THE PEOPLE OF THE STATE OF CALIFORNIA

To any Sheriff, Constable, Marshal, Policeman, or Peace Officer in the County of Santa Clara:

Proof, by affidavit, having been made before me this day by TERENCE GREEN that there is just, probable and reasonable cause for believing that: evidence of the commission of a felony, to wit: Theft of Trade Secrets, described in Section 499c of the Calif. Penal Code, more particularly described below, will be located where described below.

You are therefore commanded, in the daytime or nighttime, to make immediate search of the University Computing Corp., 260 Sheridan Avenue, Palo Alto; the residences of Hugh Jeffrey Ward at 128 Dunsmuir, Menlo Park, and at 228 O'Conner Street, Menlo Park; a 1966 Porsche, Calif. Lic. ZHW 977, registered to said Hugh Jeffrey Ward; and the person of Hugh Jeffrey Ward

located at the addresses noted above, County of Santa Clara, State of California, for the personal property described as follows: 1) Key punch computer cards, punched with the Information Systems Design remote plotting programs; 2) Computer printout sheets with printouts of Information Systems Design remote plotting programs; and 3) Computer memory bank or other data storage devices magnetically imprinted with Information Systems Design remote, plotting computer programs;
and if you find the same or any part thereof, to hold such property in your possession under Calif. Penal Code Section 1536.

Given under my hand this 19th day of February, 1971.

/s/
Judge of the Municipal Court

WPH:nas

Becker - 32

IN THE

MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT

COUNTY OF SANTA CLARA, STATE OF CALIFORNIA

STATE OF CALIFORNIA)
) ss.
COUNTY OF SANTA CLARA)

AFFIDAVIT IN SUPPORT
OF SEARCH WARRANT

Personally appeared before me this 19th day of February 19 71, TERENCE GREEN who, on oath, makes complaint, and deposes and says that there is just, probable, and reasonable cause to believe, and that he does believe, that there is now in the possession of HUGH JEFFREY WARD and UNIVERSITY COMPUTING CORPORATION, on the premises located at University Computing Corp., 260 Sheridan Avenue, Palo Alto, Calif., and residences of HUGH JEFFREY WARD at 128 Dunsmuir, Menlo Park, Calif., and 228 O'Conner Street, Menlo Park, California, which premises consist of: University Computing Corp., a business, and said WARD's residences occupied by said HUGH JEFFREY WARD; a 1966 Porsche, Calif. Lic. ZHW 977, registered to HUGH JEFFREY WARD; and the person of HUGH JEFFREY WARD;
personal property described as follows:

1) Key punch computer cards, punched with the Information Systems Design remote plotting programs;

2) Computer printout sheets with printouts of Information Systems Design remote plotting programs; and

3) Computer memory bank or other data storage devices magnetically imprinted with Information Systems Design remote plotting computer program.

Affiant, Terence Green, is a Sergeant of Police attached to the Fraud Detail of the Oakland Police Department and is engaged in the apprehension of persons engaged in the theft of trade secrets and commercial property.

Affiant was advised on February 4, 1971, by Mr. George Steeley, President of Information Systems Design, a corporation with offices at 7817 Oakport Road, Oakland, that he had discovered a set of key

punch cards at a terminal electrically connected to a computer owned and operated by his corporation, which terminal is located on the premises of the Shell Corporation in Emeryville, Alameda County. That his personal examination indicated that the key punch cards relate exclusively to a program on the computer of his corporation which program gave the computer the capability of producing remote plotting. That the remote plotting capability is a program which was designed and developed by his corporation and was used and regarded by them as a trade secret. That the value of this program in the data processing industry is estimated by him at $15,000.00. That his examination of the key punch cards shows that the computer was implemented by use of an access code to that particular program, which code was regarded by his corporation as confidential, and was not released by them except to persons authorized by them. Further that the production of the program was further initiated through use of the site number assigned to the Shell Corporation facilities. That Mr. Steeley has confirmed with officers of the Shell Corporation that the implementation was not made by them or at their request. This affiant has further contacted Mr. Jerry Helmuth, special agent with the Pacific Telephone Corporation and is apprised by Mr. Helmuth that a telephone call was made to the telephone number then exclusively leased to the Information Systems Design computer from a number then exclusively leased to the University Computing Corporation at 260 Sheridan Avenue in the City of Palo Alto. That that call lasted 11 minutes and 32 seconds. That Mr. Keith Marcelius, an

employee of Information Systems Design, has examined their computer and has advised affiant that the computer was used for the purpose of printing the confidential program at the same time that the telephone call was placed from the University Computing Corporation.

That Mr. Marcelius, who is employed by Information Systems Design as an expert in the functioning and operation of the UNIVAC 1108 computer, has advised your affiant that the confidential remote plotting program would have been reproduced at the terminal which he personally knows to be located at the premises of University Computing Corporation.

Affiant is further advised by Mr. Keith Marcelius that, prior to the 19th of January, 1971, and thereafter, a Mr. HUGH JEFFREY WARD was employed by University Computing Corporation. Mr. Marcelius has further advised affiant that MR. WARD had been a representative of University Computing Corporation in utilizing the computer installation to the Shell facilities. The use of which installation was shared with Information Systems Design. That affiant is further advised that MR. WARD had access to both the Shell site number and the access code to the Information Systems Design confidential program, but that he had not been authorized to utilize the latter.

Mr. Marcelius further advised affiant that the program, the property of Information Systems Design, could now be held in various forms: 1) In the form of key punch computer cards as were discovered at the Shell facilities; and/or 2) in the form of computer printout sheets; and/or 3) could exist in an intangible form as a program in a computer, which program, consisting of a series of

accessible electrical and/or magnetic impulses, could be disclosed only through interrogation of such computer and any data storage device. That in either key punch card or computer printout sheet form this program would be readily moveable.

Mr. James Verner, Manager of Customer Support for Information Systems Design, advised affiant that he was personally acquainted with MR. WARD, that to his personal knowledge MR. WARD knew of the existence of the Information Systems Design, and further that MR. WARD had represented generally that he was able to get into the Information Systems Design computer.

Your affiant has contacted the Department of Motor Vehicles of California and from them has been advised that MR. HUGH JEFFREY WARD is the registered owner of a 1966 Porsche, license number ZHW 977, which vehicle is currently registered to him at 128 Dunsmuir in the City of Menlo Park. Affiant is further advised by Mr. Steeley that MR. WARD's current address is 228 O'Connor Street in the City of Menlo Park.

Mr. Keith Marcelius has furnished affiant with a series of key punch computer cards punched with the Inforamtion Systems Design remote plotting programs and a printout sheet with a printout of the Information Systems Design remote plotting programs and is accompanied by Mr. Keith Marcelius, an expert in the use of said cards, printouts, and the manner in which magnetic information is stored in computers, as well as the Information Systems Design remote plotting program.

Affiant believes that the personal property first above described will constitute evidence of the commission of a felony, to wit: Theft of Trade Secrets, as described in Section 499c of the Calif. Penal Code, and that said evidence will be in the possession of University Computing Corporation at its address and business first above described, and in the possession of HUGH JEFFREY WARD at his residences above described and in a 1966 Porsche automobile above described.

Affiant desires to search at night because he has ascertained that said University Computing Corporation operates its business both day and night, and it is now approximately 5:00 pm, and it may well be dark by the time affiant can obtain a signature of the magistrate to this warrant and conduct the aforementioned search.

Further, affiant has been informed by Mr. Keith Marcelius that said magnetic impulses in the computer can be altered or destroyed in a matter of a few minutes.

That based upon the above facts, your affiant prays that a Search Warrant be issued with respect to the above location for the seizure of said property, and that the same be held under California Penal Code Section 1536 and disposed of according to law.

/s/

TERENCE GREEN

WPH:nas

Subscribed and sworn to before
me this 19th day of February, 1971.

/s/

Judge of the Municipal Court

IN THE MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT
COUNTY OF SANTA CLARA, STATE OF CALIFORNIA

PROPERTY RECEIPT

Inventory of items taken pursuant to Search Warrant issued by the Honorable Louis C. Doll, Judge of the Municipal Court, upon the affidavit of Sergeant Terence Green, Oakland Police Department, on February 19, 1971.

1. Total directory of all files on Fastrand at University Computer Corp., hereinafter UCC, at 260 Sheridan Avenue, Palo Alto, California, consisting of continuous print-out sheets.

2. Abbreviated as to description directory of files of Fastrand at UCC, at same address, as of 0730 19 February 1971, consisting of continuous print-out sheets.

3. Abbreviated as to description directory of files "dumped" from Fastrand to paper at 2300 hours, 19 February 1971.

4. Nine (9) tapes, the result and product of the "dumping", item 3, supra.

5. List of nineteen (19) tapes of UCC, the property of UCC, assigned by UCC to Hugh Jeffrey Ward for him to use on UCC business.

6. Program listing of a computer run, 2 February 1971, from 12:05:08, sequence #180.

7. Nineteen tapes, each in a plastic container, referred to in item 5, supra.

8. White binder, consisting of a number of listings of computer runs, labeled "Aerojet-General J Ward", binder approximately 12" x 15" x 1".

9. Olive desk file folder, metal mounts, containing:
   a) six handwritten pages, paper clipped, labelled ISD Message Format
   b) ISD Univac 1108 Users Guide 1 April 1969, bound
   c) ISD Univac 1108 Users Guide 1 April 1969, two copies, xeroxed, unbound. (approximately 70 pages each)

10. A manila file folder, labelled "Plot Packages" containing:
   a) CALCOMP Operation Manual Model 611 Offline Dataphone ... Part No. 10037-901-001-0, dated November 1969, blue binder
   b) CALCOMP Operation Manual for Model 663 Plotter, dtd March 1970, blue binder
   c) California Computer Products, Inc. Manual, Programming Calcomp Pen Plotters, dtd June 1968, labelled WARD
   d) CII Applications Software, Pub No 585b, July 1969, yellow softbound, labelled WARD

11. Olive desk file folder, metal mounts, labelled PLOTTING.

12. Manila file folder, labelled AEROJET-GENERAL, containing
   a) 35 reproduced pages
   b) 3 handwritten pages

13. Manila file folder, labelled AEROJET-CALCOMP, containing
   a) five xeroxed pages labelled ISD
   b) three unlabelled xerox pages
   c) seven handwritten sheets

IN THE MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT
COUNTY OF SANTA CLARA, STATE OF CALIFORNIA

PROPERTY RECEIPT
Continuation

14. Mottled grey binder, consisting of a number of listings of computer runs, labelled ISD, approximately 12" x 18" x 1/2".

////////////////////////// Nothing Follows //////////////////////////////////

Received, pursuant to Property Security Agreement made this date with University Computer, Corp.

/s/

END