FM 3-19.13

LAW ENFORCEMENT INVESTIGATIONS

JANUARY 2005

Headquarters, Department of the Army

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Chapter 11

Computer Crimes

Computer crimes are among the fastest growing crimes in our society today. Electronic devices can be used to commit a crime, can contain the evidence of the crime, and can even be the targets of crime. Understanding the role and nature of electronic evidence that may be found and how to process the crime scene containing potential electronic evidence are crucial issues facing all law enforcement personnel. Due to a rapid increase and the serious nature of these crimes, several federal agencies have organized special units that investigate computer crimes. The Computer Crime Investigation Unit (CCIU) and USACIL are the primary supporting agencies for military law enforcement investigators with regard to electronic evidence.

OVERVIEW

11-1. Technology is advancing at such a rapid rate that the procedures described in this chapter must be examined through the prism of current technology and the practices adjusted, as appropriate. Electronic evidence can be found in many new electronic devices available to today's consumers. *Appendix C* describes a wide variety of the types of electronic devices commonly encountered in crime scenes. It provides a general description of each type of device, describes its common uses, and presents the potential evidence that may be found in each type of equipment.

ELECTRONIC EVIDENCE

11-2. Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device (see *Appendix D*). As such, electronic evidence is latent just as DNA and fingerprints are latent. In its natural state, we cannot see the evidence that the physical object holds. Equipment and software are required to make the evidence visible. Testimony may be required to explain the examination process and any process limitations.

11-3. Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. This chapter suggests methods that will help preserve the integrity of such evidence.

11-4. When dealing with electronic evidence, general forensic and procedural principles should be applied to include the following:

- Actions taken to secure and collect electronic evidence should not change that evidence.
- Persons conducting the examination of electronic evidence should be trained for that purpose.
- Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.

11-5. This evidence is acquired when data or physical items are collected and stored for examination purposes. The following are characteristics of electronic evidence:

- It is often latent just as fingerprints and DNA are latent.
- It can transcend borders with ease and speed.
- It is fragile and can be easily altered, damaged, or destroyed.
- It is sometimes time sensitive.

11-6. Precautions must be taken in the collection, preservation, and examination of electronic evidence. Handling electronic evidence at the crime scene normally consists of—

- Recognition and identification of the evidence.
- Documentation of the crime scene.
- Collection and preservation of the evidence.
- Packaging and transportation of the evidence.

INVESTIGATIVE TOOLS AND EQUIPMENT

11-7. Special tools and equipment may be required to collect electronic evidence. Experience has shown that advances in technology may dictate changes in the tools and equipment required. Preparations should be made to get the equipment required to collect electronic evidence. Investigative agencies should have general crime scene processing equipment, such as cameras, notepads, sketch pads, evidence forms, crime scene tape, and markers. Each aspect of the process (documentation, collection, packaging, and transportation) dictates tools and equipment. The following are additional items that may be useful to have in a tool kit at an electronic crime scene:

- Documentation tools such as—
  - Cable tags.
  - Indelible felt-tip markers.
  - Stick-on labels.
- Disassembly and removal tools in a variety of nonmagnetic sizes and types that include—
  - Flat-blade and cross-tip screwdrivers.
  - Hex-nut and secure-bit drivers.
  - Star-type nut drivers.
  - Needle-nose and standard pliers.

    - Small tweezers.
    - Specialized screwdrivers (manufacturer specific).
    - Wire cutters.
- Packaging and transporting supplies such as—
    - Antistatic bags and bubble wrap.
    - Cable ties.
    - Evidence bags.
    - Evidence and packing tape.
    - Packing materials (avoid materials that can produce static electricity, such as foam peanuts).
    - Sturdy boxes of various sizes.
- Other items such as—
    - Evidence tags.
    - Evidence tape.
    - Forms (keystroke or mouse click log, photograph log, *DA Forms 4137 [Evidence/Property Custody Document]*, and *DA Forms 4002).*
    - Gloves.
    - A hand truck.
    - Large rubber bands.
    - A list of contact telephone numbers for assistance.
    - A magnifying glass.
    - Printer paper.
    - A seizure disk.
    - A small flashlight.
    - Fully-formatted floppy diskettes (3 inch and 5 1/4 inch).

CRIME SCENE SECURITY AND EVALUATION

11-8. The investigator should take steps to ensure the safety of all persons at the crime scene and protect the integrity of all evidence, both traditional and electronic. All activities should be in compliance with Army policy and federal, state, and local laws.

11-9. After securing the scene and all persons on the scene, the investigator should visually identify potential evidence (both physical and electronic) and determine if perishable evidence exists. He should then evaluate the scene and formulate a search plan.

SECURE AND EVALUATE THE CRIME SCENE

11-10. The investigator should secure and evaluate the crime scene by—

- Following jurisdictional policy for securing the crime scene. This would include ensuring that all persons are removed from the immediate area where evidence is to be collected. At this point in the investigation, do not alter the condition of any electronic devices. If it is off, leave it off. If it is on, leave it on.

- Protecting perishable data (physical and electronic). Perishable data may be found on pagers, caller identification (ID) boxes, electronic organizers, cell phones, and other similar devices. The first responder should always keep in mind that any device containing perishable data should be immediately secured, documented, and/or photographed.
- Identifying telephone lines attached to devices such as modems and caller ID boxes. Document, disconnect, and label each telephone line from the wall rather than the device, when possible. There may also be other communications lines present for local area network (LAN), wide area network (WAN), or other network technologies. Consult the appropriate personnel or agency in these cases.
- Preserving the computer mouse, keyboard, diskettes, compact disks (CDs), or other components that may have latent fingerprints or other physical evidence. Chemicals used in processing latent fingerprints can damage equipment and data. Therefore, latent prints should be collected after the completion of electronic evidence recovery.

CONDUCT PRELIMINARY INTERVIEWS

11-11. The investigator should conduct preliminary interviews by—

- Separating and identifying all individuals (witnesses, subjects, or others) at the scene and recording their location at the time of entry.
- Being consistent with departmental policy and applicable laws in obtaining information from these individuals, such as—
  - Passwords and user names of owners and/or users of electronic devices found at the crime scene and the Internet service provider (ISP). Obtain any passwords required to access the system, software, or data. An individual may have multiple passwords, such as basic input-output system (BIOS), system login, network ISP, application files, encryption pass phrase, e-mail, access token, scheduler, or contact list.
  - The purpose of the system.
  - Any unique security schemes or destructive devices.
  - Any off-site data storage.
  - Any documentation explaining the hardware or software installed on the system.

CRIME SCENE DOCUMENTATION

11-12. Documentation of the crime scene creates a permanent historical record of the crime scene. Documentation is an ongoing process throughout the investigation. It is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence. Moving of a computer system while the system is running may cause changes to system data. Therefore, the system should not be moved until it has been safely powered down. The initial documentation of the physical crime scene should include—

- Observing and documenting the physical crime scene, such as the position of the mouse and the location of components relative to each other (a mouse on the left side of the computer may indicate a left-handed user).
- Documenting the condition and location of the computer system, including the power status of the computer (on, off, or in sleep mode). Most computers have status lights to indicate that the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, it may also indicate that it is on or was recently turned off.
- Identifying and documenting related electronic components that will not be collected.
- Photographing the entire scene to create a visual record as noted by the first responder. The complete room should be recorded with 360° coverage, when possible.
- Photographing the front of the computer, monitor screen, and other components. Take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity.
- Performing additional documentation of the system during the collection phase.

AUTHORIZATION TO SEIZE ELECTRONIC EVIDENCE

11-13. Search authorization may be obtained from a US magistrate, a civilian judge at the state or federal level, or the property owner is required. However, in almost all cases, courts have held a relatively high standard with regard to the specificity of computer-related search authorizations. Investigative personnel seeking search authorization must be able to articulate specific and recent information pertaining to the individual items cited on the affidavit and authorization in order to establish probable cause. In many instances, information that is several months old cannot in and of itself be used to generate probable cause. More recent information, gained through “pretext” phone calls or online undercover operations, may be required to develop current and reliable information (see *Appendix E* for a sample affidavit and authorization). Additionally, if during the conduct of a search for one offense, evidence of an unrelated or different type of offense is identified, the scope of the search authorization must be expanded accordingly. If probable cause cannot be developed, consideration should be given to requesting a consent search. However, this may make the suspect aware of law enforcement interest and cause investigators to lose potential evidence.

11-14. When information is required from private business computers, investigators must take the appropriate measures to avoid any financial liability to the government by determining if the seizure of these computers will cause the business to lose money in any way. If it is determined that the seizure will create liabilities to the government, coordination must be made with CCIU or USACIL to have an expert image the appropriate drive information on the site. Additionally, investigators must take reasonable steps to determine if copyrighted information is contained on a computer to be seized. If a determination is made that such data is stored on a target computer, consult with CCIU or USACIL, as appropriate, to seize the required information without collecting the copyrighted information. Failure to comply with this requirement will likely result in the suppression of all collected evidence from courtroom presentation and could possibly leave the Army legally liable.

EVIDENCE COLLECTION

11-15. Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation. Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields, such as those generated by static electricity, magnets, radio transmitters, and other devices.

11-16. Electronic evidence should be collected according to departmental guidelines. In the absence of departmental procedures for electronic evidence collection, use the procedures outlined below.

NONELECTRONIC EVIDENCE COLLECTION

11-17. Recovery of nonelectronic evidence can be crucial in the investigation of electronic crimes. Take proper care to ensure that such evidence is recovered and preserved. Items relevant to subsequent examination of electronic evidence may exist in other forms (written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs) and should be secured and preserved for future analysis. These items are frequently in close proximity to the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with departmental procedures.

STAND-ALONE AND LAPTOP COMPUTER EVIDENCE COLLECTION

11-18. Multiple computers may indicate a computer network. Likewise, computers located at businesses are often networked. In these situations, specialized knowledge about the system is required to effectively recover evidence and reduce your potential for civil liability. When a computer network is encountered, contact the forensic computer expert in your department or an outside consultant identified by your department for assistance. Computer systems in a complex environment are addressed later in this chapter.

11-19. A stand-alone personal computer (PC) is a computer that is not connected to a network or another computer. Stand-alones may be desktop machines or laptops.

11-20. Laptops incorporate a computer, monitor, keyboard, and mouse into a single portable unit. Laptops differ from other computers in that they can be powered by electricity or a battery source. Therefore, they require the removal of the battery in addition to stand-alone, power-down procedures.

11-21. If the computer is on, document existing conditions and call your expert or consultant. If an expert or consultant is not available, document all actions taken and any changes observed in the monitor, computer, printer, or other peripherals that result from actions taken. Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

- **Situation 1:** The monitor is on and the work product and/or desktop are visible.

  Step 1. Photograph the screen and record the information displayed.

  Step 2. Proceed to situation 3, step 3.

- **Situation 2:** The monitor is on and the screen is blank (sleep mode) or the screensaver (picture) is visible.

  Step 1. Move the mouse slightly (without pushing buttons). The screen should change and show the work product or request a password.

  Step 2. Do not perform any other keystrokes or mouse operations if mouse movement does not cause a change in the screen.

  Step 3. Photograph the screen and record the information displayed.

  Step 4. Proceed to situation 3, step 3.

- **Situation 3:** The monitor is off.

  Step 1. Make a note of the "off" status.

  Step 2. Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.

  Step 3. Regardless of the power state of the computer (on, off, or sleep mode), remove the power source cable from the computer, not from the wall outlet. If dealing with a laptop, in addition to removing the power cord, remove the battery pack. The battery is removed to prevent any power to the system. Some laptops have a second battery in the multipurpose bay instead of a floppy drive or CD drive. Check for this possibility and remove that battery as well.

  Step 4. Check for outside connectivity (telephone modem, cable, integrated services digital network [ISDN], and digital subscriber line [DSL]). If a telephone connection is present, attempt to identify the telephone number.

  Step 5. Avoid damage to potential evidence by removing any floppy disks that are present, packaging the disk separately, and labeling the package. If available, insert either a seizure disk or a blank floppy disk. Do not remove CDs or touch the CD drive.

  Step 6. Place tape over all the drive slots and over the power connector.

  Step 7. Record the make, model, and serial numbers.

  Step 8. Photograph and diagram the connections of the computer and the corresponding cables.

Step 9. Label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly at a later time. Label unused connection ports as "unused." Identify laptop computer docking stations in an effort to identify other storage media.

Step 10. Record or log evidence according to departmental procedures.

Step 11. Package any components as fragile, if transport is required.

COMPUTERS IN A COMPLEX ENVIRONMENT

11-22. Business environments frequently have multiple computers connected to each other, to a central server, or both. Securing and processing a crime scene where the computer systems are networked poses special problems, because an improper shutdown may destroy data. This can result in loss of evidence and potential severe civil liability. When investigating criminal activity in a known business environment, the presence of a computer network should be planned for in advance, if possible, and the appropriate expert obtained. It should be noted that computer networks can also be found in a home environment and the same concerns exist.

11-23. The possibility of various operating systems and complex hardware configurations requiring different shutdown procedures make the processing of a network crime scene beyond the scope of this chapter. However, it is important that computer networks be recognized and identified, so that an expert can be obtained if one is encountered.

11-24. Indications that a computer network may be present include

- Multiple computer systems.
- Cables and connectors running between computers or central devices, such as hubs.
- Any information provided by informants or individuals at the scene.
- Network components.

EXAMINATION REQUEST

11-25. At the point when the USACIL laboratory request is prepared, the initial report and all documentation related to the efforts undertaken by the investigator should be forwarded to USACIL with the items of evidence. It is important that all actions, including every keystroke and mouse click, be recorded by the investigator to ensure that the laboratory examiner can fully appreciate what impact the investigator's actions could have had on the operating system. Additionally, special consideration should be undertaken when shipping computer-related items to USACIL; they should be containerized separate from fungible evidence that will require special treatment, such as refrigeration.

ON-SITE SEARCHES WITHOUT SEIZURE AUTHORIZATION

11-26. In some instances, investigative personnel will find themselves in a situation where there is an authorization to search a computer, but the agent lacks the authorization to seize it. Typically, this occurs in one of two situations. The first is when consent to search is authorized by a suspect who agrees to allow the investigator to search the computer; however, he does not agree to allow the investigator to seize or ship it to the laboratory for examination. The second situation frequently results when a commander suspects that criminal activity has been committed using a government computer, but he has no means to verify it and does not want to deprive the organization of the use of the computer while it is awaiting examination. Investigators in the field should never conduct a search of a computer or open electronic files under any circumstance other than when it is impossible or impractical to seize the device for laboratory examination.

11-27. If an investigator conducts a consent type search of a computer, based on the scenario indicated above, it is essential for him to terminate the search as soon as the first file containing evidence of a crime is identified. At this point, probable cause has been met, and a formal search authorization should be obtained from a competent authority. The subsequent seizure of the computer is not based on the consent to search, but rather the evidence identified during the search and the authority of a formal search authorization or warrant. The investigator must then document all of his activities including every keystroke and mouse click that led to the discovery of the criminal material. It is important that additional files not be accessed, because the date-time group of the accessed file are modified and will likely result in the suppression of them in the prosecutorial process.

EVIDENCE PACKAGING, TRANSPORTING, AND STORING

11-28. Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and magnetic sources. Therefore, special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain the chain of custody of electronic evidence, document its packaging, transporting, and storing.

PACKAGING

11-29. If multiple computer systems are collected, label each system so that it can be reassembled as found (system A: mouse, keyboard, monitor, and main base unit; system B: mouse, keyboard, monitor, and main base unit).

11-30. When packaging evidence at a crime scene—

- Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packing.
- Pay special attention to latent or trace evidence and take action to preserve it.
- Pack magnetic media in antistatic packaging (paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags.
- Avoid folding, bending, or scratching computer media, such as a diskette, compact disk-read only memory (CD-ROM), or tape.
- Ensure that all containers used to hold evidence are properly labeled.

TRANSPORTING

11-31. Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt. When transporting evidence—

- Keep all electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- Maintain the chain of custody on all evidence transported.

STORING

11-32. Ensure that evidence is inventoried according to *AR 195-5*. Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.

11-33. Be aware that potential evidence, such as dates, times, and system configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (such as the evidence custodian, laboratory chief, and forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

FM 3-19.13
10 JANUARY 2005

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

Sandra R. Riley

SANDRA R. RILEY
Administrative Assistant to the
Secretary of the Army
0434205

DISTRIBUTION:

Active Army, Army National Guard, and US Army Reserve: To be distributed in accordance with initial distribution number 110139, requirements for FM 3-19.13.