NIJ

APR. 08

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

Chapter 5. Evidence Collection

NCJ 219941

Chapter 5. Evidence Collection

The first responder must have proper authority—such as plain view observation, consent, or a court order—to search for and collect evidence at an electronic crime scene. The first responder must be able to identify the authority under which he or she may seize evidence and should follow agency guidelines, consult a superior, or contact a prosecutor if a question of appropriate authority arises.

Digital evidence must be handled carefully to preserve the integrity of the physical device as well as the data it contains. Some digital evidence requires special collection, packaging, and transportation techniques. Data can be damaged or altered by electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices. Communication devices such as mobile phones, smart phones, PDAs, and pagers should be secured and prevented from receiving or transmitting data once they are identified and collected as evidence.

NOTE: If data encryption is in use on a computer, data storage device, or other electronic device and it is improperly powered off during digital evidence collection, the data it contains may become inaccessible.

Computers, Components, and Devices

To prevent the alteration of digital evidence during collection, first responders should first—

- Document any activity on the computer, components, or devices.

- Confirm the power state of the computer. Check for flashing lights, running fans, and other sounds that indicate the computer or electronic device is powered on. If the power state cannot be determined from these indicators, observe the monitor to determine if it is on, off, or in sleep mode.

Assess the Situation

After identifying the computer's power status, follow the steps listed below for the situation most like your own:

Situation 1: The monitor is on. It displays a program, application, work product, picture, e-mail, or Internet site on the screen.

1. Photograph the screen and record the information displayed.
2. Proceed to "If the Computer Is ON" (see P. 25).

Situation 2: The monitor is on and a screen saver or picture is visible.

1. Move the mouse slightly without depressing any buttons or rotating the wheel. Note any onscreen activity that causes the display to change to a login screen, work product, or other visible display.
2. Photograph the screen and record the information displayed.
3. Proceed to "If the Computer Is ON" (see P. 25).

Situation 3: The monitor is on, however, the display is blank as if the monitor is off.

1. Move the mouse slightly without depressing any buttons or rotating the wheel. The display will change from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
2. Photograph the screen and record the information displayed.

3. Proceed to "If the Computer Is ON" (see P. 25).

Situation 4a: The monitor is powered off. The display is blank.

1. If the monitor's power switch is in the off position, turn the monitor on. The display changes from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
2. Photograph the screen and the information displayed.
3. Proceed to "If the Computer Is ON" (see P. 25).

Situation 4b: The monitor is powered off. The display is blank.

4. If the monitor's power switch is in the off position, turn the monitor on. The display does not change; it remains blank. Note that no change in the display occurs.
5. Photograph the blank screen.
6. Proceed to "If the Computer Is OFF" (see P. 24).

Situation 5: The monitor is on. The display is blank.

1. Move the mouse slightly without depressing any buttons or rotating the wheel; wait for a response.
2. If the display does not change and the screen remains blank, confirm that power is being supplied to the monitor. If the display remains blank, check the computer case for active lights, listen for fans spinning or other indications that the computer is on.
4. If the screen remains blank and the computer case gives no indication that the system is powered on, proceed to "If the Computer Is OFF" (see P. 24).

If the Computer Is OFF

For desktop, tower, and minicomputers follow these steps:

1. Document, photograph, and sketch all wires, cables, and other devices connected to the computer.
2. Uniquely label the power supply cord and all cables, wires, or USB drives attached to the computer as well as the corresponding connection each cord, cable, wire, or USB drive occupies on the computer.
3. Photograph the uniquely labeled cords, cables, wires, and USB drives and the corresponding labeled connections.
4. Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip, or battery backup device.
5. Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end.
6. Place tape over the floppy disk slot, if present.
7. Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
8. Place tape over the power switch.
9. Record the make, model, serial numbers, and any user-applied markings or identifiers.
10. Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.
11. Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

For laptop computers follow these steps:

1. Document, photograph, and sketch all wires, cables, and devices connected to the laptop computer.
2. Uniquely label all wires, cables, and devices connected to the laptop computer as well as the connection they occupied.
3. Photograph the uniquely labeled cords, cables, wires, and devices connected to the laptop computer and the corresponding labeled connections they occupied.
4. Remove and secure the power supply and all batteries from the laptop computer.
5. Disconnect and secure all cables, wires, and USB drives from the computer and document the equipment or device connected at the opposite end.
6. Place tape over the floppy disk slot, if present.
7. Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
8. Place tape over the power switch.
9. Record the make, model, serial numbers, and any user-applied markings or identifiers.
10. Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.
11. Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

If the Computer Is ON

For practical purposes, removing the power supply when you seize a computer is generally the safest option. If evidence of a crime is visible on the computer display, however, you may

need to request assistance from personnel who have experience in volatile data capture and preservation.

In the following situations, immediate disconnection of power is recommended:

- Information or activity onscreen indicates that data is being deleted or overwritten.
- There is indication that a destructive process is being performed on the computer's data storage devices.
- The system is powered on in a typical Microsoft® Windows® environment. Pulling the power from the back of the computer will preserve information about the last user to login and at what time the login occurred, most recently used documents, most recently used commands, and other valuable information.

In the following situations, immediate disconnection of power is NOT recommended:

- Data of apparent evidentiary value is in plain view onscreen. The first responder should seek out personnel who have experience and training in capturing and preserving volatile data before proceeding.
- Indications exist that any of the following are active or in use:
  - Chat rooms.
  - Open text documents.
  - Remote data storage.
  - Instant message windows.
  - Child pornography.
  - Contraband.
  - Financial documents.
  - Data encryption.
  - Obvious illegal activities.

For mainframe computers, servers, or a group of networked computers, the first responder should secure the scene and request assistance from personnel who have training in collecting digital evidence from large or complex computer systems. Technical assistance is available at www.ecpi-us.org/Technicalresources.html.

Other Forms of Evidence

Be alert to the crime scene environment. Look out for pieces of paper with possible passwords, handwritten notes, blank pads of paper with impressions from prior writings, hardware and software manuals, calendars, literature, and text or graphic material printed from the computer that may reveal information relevant to the investigation. These forms of evidence also should be documented and preserved in compliance with departmental policies.

Other Electronic and Peripheral Devices of Potential Evidential Value

Electronic devices such as those listed below may contain information of evidentiary value to an investigation. Except in emergency situations, such devices should not be operated and the information they might contain should not be accessed directly. If a situation warrants accessing these devices and the information they contain immediately, all actions taken should be thoroughly documented. Data may be lost if a device is not properly handled or its data properly accessed.

The following are examples of electronic devices, components, and peripherals that first responders may need to collect as digital evidence:

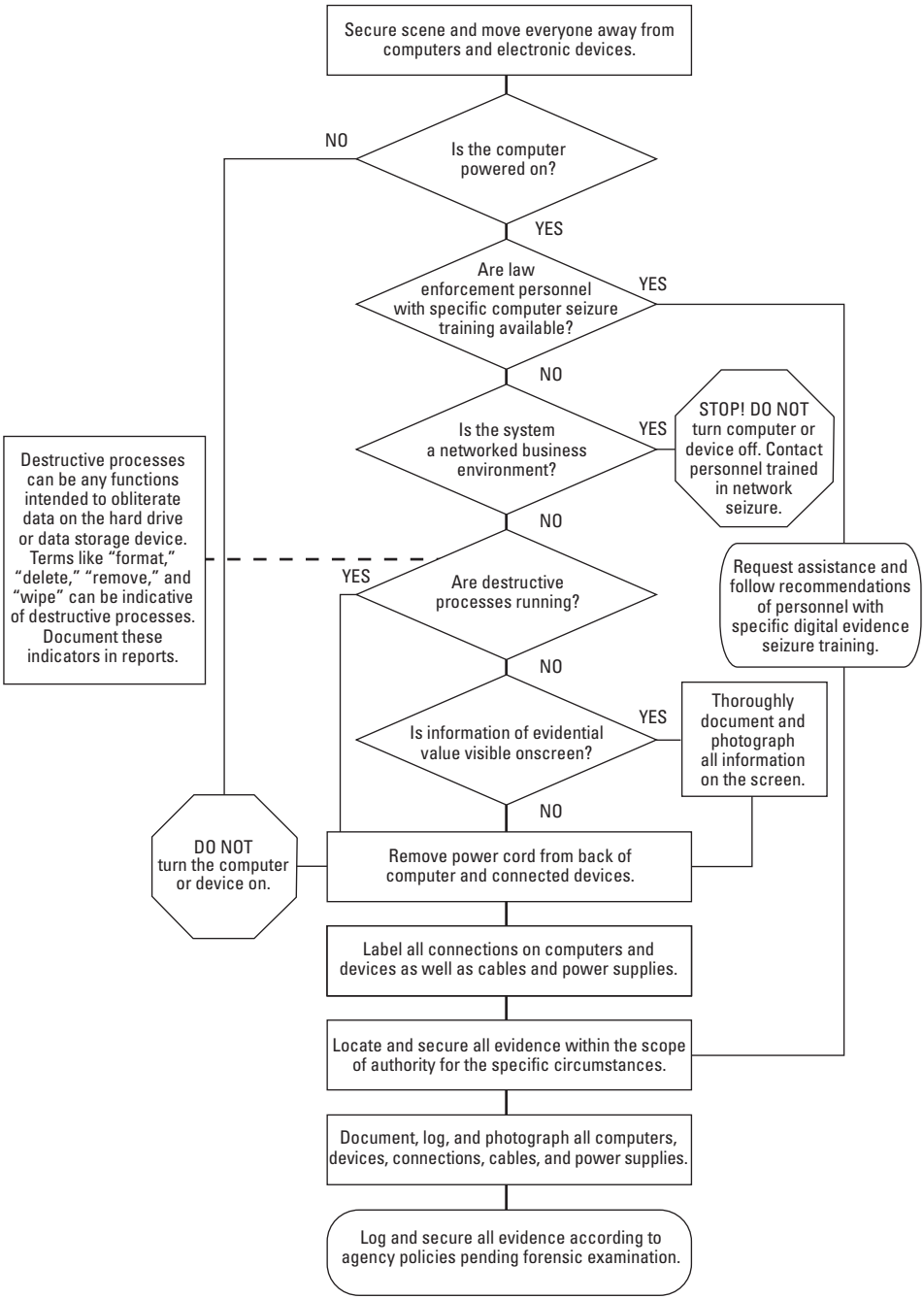
- Audio recorders.
- GPS accessories.
- Answering machines.
- Computer chips.

- Pagers.
- Cordless landline telephones.
- Copy machines.
- Cellular telephones.
- Hard drive duplicators.
- Facsimile (fax) machines.
- Printers.
- Multifunction machines (printer, scanner, copier, and fax).
- Wireless access points.
- Laptop power supplies and accessories.
- Smart cards.
- Videocassette recorders (VCRs).
- Scanners.
- Telephone caller ID units.
- Personal Computer Memory Card International Association (PCMCIA) cards.
- PDAs.

Special handling may be required to preserve the integrity and evidentiary value of these electronic devices. First responders should secure the devices and request assistance from personnel who have advanced training in collecting digital evidence. Refer to www.ecpi-us.org/Technicalresources.html for more information on advanced technical assistance.

NOTE: When collecting electronic devices, components, and peripherals such as those listed above, remember to collect the power supplies, cables, and adapters for those devices as well.

Collecting Digital Evidence Flow Chart



Computers in a Business Environment

Business environments frequently have complicated configurations of multiple computers networked to each other, to a common server, to network devices, or a combination of these. Securing a scene and collecting digital evidence in these environments may pose challenges to the first responder. Improperly shutting down a system may result in lost data, lost evidence, and potential civil liability.

The first responder may find a similar environment in residential locations, particularly when a business is operated from the home.

In some instances, the first responder may encounter unfamiliar operating systems or unique hardware and software configurations that require specific shutdown procedures. Such circumstances are beyond the scope of this guide. For assistance with this type of scene, first responders should refer to www.ecpi-us.org/Technicalresources.html.

Servers