

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice



NIJ

NOV. 09



Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders

www.ojp.usdoj.gov/nij

**U.S. Department of Justice
Office of Justice Programs**

810 Seventh Street N.W.
Washington, DC 20531

Eric H. Holder, Jr.
Attorney General

Laurie O. Robinson
Acting Assistant Attorney General

Kristina Rose
Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.ojp.usdoj.gov/nij

Office of Justice Programs
Innovation • Partnerships
Safer Neighborhoods
www.ojp.usdoj.gov

NIJ

NOV. 09

**Electronic Crime Scene
Investigation: An On-the-Scene
Reference for First Responders**

**Cover photograph
copyright© 2001
PhotoDisc, Inc.**

NCJ 227050



Kristina Rose
Acting Director
National Institute of Justice

This flipbook is a companion piece to *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. Use the flipbook only after you have reviewed the contents of the Guide at <http://www.ojp.usdoj.gov/nij/pubs-sum/219941.htm>.

The flipbook was updated by the Electronic Crime Partnership Initiative (ECPI), a program established by the National Institute of Justice to build the capacity of state and local law enforcement to prevent, investigate and prosecute electronic crime and identify, collect, preserve and examine digital evidence.

This publication does not create, is not intended to create, and may not be relied upon to create any rights, substantive or procedural, enforceable as law by any party in any matter civil or criminal. Opinions or points of view expressed in this document represent a consensus of ECPI members and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

Contents

Introduction	vi
Electronic Devices: Types, Description and Potential Evidence	1
Computer Systems	1
Storage Devices	2
Handheld Devices	3
Peripheral Devices	3
Computer Networks	4
Sources of Potential Digital Evidence in Electronic Devices	5
Securing and Evaluating the Scene	6
Preliminary Interviews	8
Documenting the Scene	9
Evidence Collection	11
Assess the Situation	12
Packaging and Transporting Digital Evidence ..	21
Packaging Procedures	21
Transportation Procedures	22

Electronic Crime and Digital Evidence	
Considerations by Crime Category	23
Child Abuse and/or Exploitation	23
Computer Intrusion.	24
Counterfeiting.	25
Death Investigations.	26
Domestic Violence, Threats and Extortion	27
E-mail Threats, Harassment and/or Stalking.	28
Gambling	29
Identity Theft	30
Narcotics.	31
Online Fraud and/or Economic Fraud	32
Prostitution	33
Software Piracy	34
Telecommunication Fraud	35
Terrorism (Homeland Security)	36
Other Potential Sources of Evidence	37
Information to Document to Assist the	
Forensic Examination	40

Introduction

This flipbook is intended as a quick reference for first responders who may be responsible for identifying, preserving, collecting and securing evidence at an electronic crime scene. It is a companion piece to *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, from which it is excerpted.



Use this flipbook only after you have reviewed and familiarized yourself with the contents of *Electronic Crime Scene Investigation*, which is available for free download at <http://www.ojp.usdoj.gov/nij/pubs-sum/219941.htm>.

Consider agency protocols; federal, state and local laws; and prevailing technology when applying the information in this flipbook.

Electronic Devices: Types, Description and Potential Evidence

Computer Systems

- Laptops
- Desktop systems
- Tower computers
- Rack-mounted systems
- Minicomputers
- Mainframe systems

A computer system's hardware is likely to include:

- A case containing circuit boards, microprocessors, hard drive, memory and interface connections.
- A monitor or video display device.
- A keyboard and mouse.
- Peripheral devices such as external hard drives, modems, printers, scanners, routers and docking stations.

Storage Devices

- Hard drives (whether loose or connected to the system).
- External hard drives (generally require a power supply and a connection to the computer system).
- Removable media, e.g., cartridges or disk-based data storage devices.
- Thumb or flash drives: Small, lightweight, removable data storage devices with USB connections. Can be found as part of, or disguised as, any number of common or unique devices, e.g., wrist-watch or Swiss Army Knife.
- Memory cards: Small data storage devices commonly used with digital cameras, computers, mobile phones, digital music players, personal digital assistants (PDAs) and video game consoles.

Handheld Devices

- PDAs
- Digital multimedia devices
- Pagers
- Digital cameras
- Global positioning satellite (GPS) receivers
- Mobile and smart phones

Peripheral Devices

Equipment that can be attached or connected to a computer.

- Modems
- Routers
- Printers
- Scanners
- Docking stations

Computer Networks

- Two or more computer systems linked by data cables or by wireless connections to enable them to share resources and data.
- Often include printers and data-routing devices such as hubs, switches and routers.

Sources of Potential Digital Evidence in Electronic Devices

- The device and its components.
- The function(s) it performs or facilitates.
- Software, documents, photos, image files, e-mail and attachments, databases, financial information, Internet browsing history, chat logs, buddy lists and event logs.
- Information stored on the device regarding its use, e.g., incoming and outgoing phone and fax numbers and recently scanned, faxed or printed documents.
- Identifying information associated with the computer system, e.g., Internet protocol (IP) and local area network (LAN) addresses, broadcast settings, and media access card (MAC) or network interface card (NIC) addresses.



Electronic devices also may hold latent evidence such as fingerprints, DNA or other physical evidence that should be preserved.

See page 37 for other potential sources of evidence.

Securing and Evaluating the Scene

Document, photograph, and secure digital evidence at the scene as soon as possible.

When securing and evaluating the scene:

- Do not alter the state of an electronic device. If a computer or an electronic device is off, leave it off.
- Remove all unauthorized persons from the area where evidence is to be collected.
- Identify, seize and secure all electronic devices, including personal or portable devices.
- Recognize potential digital evidence in telephones, digital video recorders, other household appliances and motor vehicles.

If the computer is on or the power state cannot be determined:

- Look and listen for indications that the computer is on — e.g., fans running, drives spinning and lit light-emitting diodes (LEDs).
- If you cannot determine the power state of the computer, observe the monitor to determine if it is on, off or in sleep mode.
- Check display screen for signs of data destruction. Look out for words such as “delete,” “format,” “remove,” “copy,” “move,” “cut” or “wipe.”
- Look for indications that the computer is being accessed remotely and/or signs of ongoing communications with other computers or users — e.g., Instant Messaging (IM) windows or chat rooms.
- Take note of all cameras and determine whether they are active.

Proceed to page 12.

Preliminary Interviews

Separate and identify all adults of interest and record the location they occupied when you entered the scene. Obtain the following information from interviewee(s):

- Purpose of computers and devices.
- All users of the computers and devices.
- Type of Internet access and Internet service provider.
- Computer and Internet user information — e.g., login names, user account names and passwords, and Instant Message screen names.
- E-mail and Web mail (Web-based e-mail) accounts and personal Web pages.
- Account information for online social networking Web sites — e.g., MySpace, Facebook.
- All security provisions, data access restrictions, destructive devices or software in use.
- Any automated applications in use.
- Any other relevant information.

Documenting the Scene

Your documentation should include:

- The type, location, position, condition and power status of the device.
- A record of all activity and processes visible on the display screen(s).
- A record of all physical connections to and from the computers and other devices.
- A record of any network and wireless components capable of linking devices to each other and the Internet.
- The type, condition and power status of the device's Internet and network access.
- Video, photos, notes and sketches to assist in recreating/conveying the details of the scene.



Some computer systems and electronic devices — and the information they contain — may be protected under applicable laws, agency policies or other

factors, that may prohibit collection of these devices or components. However, do include the location, condition and power state of these devices in your documentation.



Movement of a running computer or electronic device may cause changes or damage to the computer or device or the digital evidence it contains. Computers and electronic devices should not be moved until it is determined that they are powered off.

Evidence Collection

Handling digital evidence correctly is essential to preserving the integrity of the physical device as well as the information or data it contains. Turning off the power to a computer or other electronic device may cause the information or data stored on it to be damaged or lost.

If you are not trained in handling digital evidence —

- Do not attempt to explore the contents of a computer or other electronic device or to recover information from it.
- Do not alter the state of a computer or other electronic device.
- Do not press any keys or click the mouse.
- If the computer or device is off, leave it off.
- Do not move a computer or other electronic device that is powered on.

- Do not accept offers of help or technical assistance from unauthorized persons.
- **DO request technical assistance** from personnel with advanced equipment and training in digital evidence collection. See <http://www.ecpi-us.org/Technicalresources.html> for a list of available resources.

Assess the Situation

Before seizing digital evidence, make sure you have the legal authority to do so. **Improper access to information or data stored on electronic devices may violate provisions of federal laws.**

After securing the scene and identifying the computer's power status (p. 6), follow the steps listed below for the situation most like your own.

Situation 1: Monitor is on. Program, application, work product, picture, e-mail or Internet site is displayed.

1. Photograph screen and record information displayed.
2. Proceed to **"If the Computer Is ON"** (p. 19).

Situation 2: Monitor is on. Screen saver or picture is visible.

1. Move mouse slightly without depressing buttons or rotating wheel if present.
2. Note any onscreen activity that causes a change in the display.
3. Photograph screen and record information displayed.
4. Proceed to **“If the Computer Is ON”** (p. 19).

Situation 3: Monitor is on. Display is blank.

1. Move mouse slightly without depressing buttons or rotating wheel if present.
2. Display changes to login screen, work product, or other visible display.
3. Note change in display.
4. Photograph screen and record information displayed.
5. Proceed to **“If the Computer Is ON”** (p. 19).

Situation 4a: Monitor is off. Display is blank.

1. If monitor's power switch is in off position, turn monitor on.
2. **Display changes** to a login screen, work product or other visible display.
3. Note change in the display.
4. Photograph screen and record information displayed.
5. Proceed to **"If the Computer Is ON"** (p. 19).

Situation 4b: Monitor is off. Display is blank.

1. If monitor's power switch is in off position, turn monitor on.
2. **Display does not change. Screen remains blank.**
3. Note that the display does not change.
4. Photograph blank screen.
5. Proceed to **"If the Computer Is OFF"** (p. 16).

Situation 5: Monitor is on. Display is blank.

1. Move mouse slightly without depressing any buttons or rotating the wheel if present.
2. If display does not change, confirm that power is supplied to the monitor.
3. If display remains blank, check computer case for active lights and listen for fans spinning or other indications computer is on.
4. If computer case gives no indication that it is powered on, proceed to **"If the Computer Is OFF"** (p. 16).

If the Computer Is OFF

For **desktop, tower and minicomputers** follow these steps:

1. Document, photograph, and sketch all wires, cables, and devices connected to the computer.
2. Uniquely label and photograph the power supply cord and all cables, wires or USB drives attached to the computer and the connection each of these occupies on the computer.
3. Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip or battery backup device.
4. Disconnect and secure all cables, wires and USB drives from the computer and document the device or equipment connected at the opposite end.
5. Place tape over the floppy disk slot if present. Ensure that the CD or DVD drive trays are retracted into place and tape across the drive tray to prevent it from opening.
6. Place tape over the power switch.

If the Computer Is OFF (continued)

7. Record the make, model, serial numbers and any user-applied markings or identifiers.
8. Record or log computer and all cords, cables, wires, devices and components according to agency procedures.
9. Carefully package all evidence collected 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.
2. Uniquely label and photograph all wires, cables and devices connected to the laptop and the connection each occupies.
3. Remove and secure the power supply and all batteries from the laptop computer.
4. Disconnect and secure all cables, wires, and USB drives from the laptop and document the equipment or device connected at the opposite end.
5. Place tape over the floppy disk slot if present. Ensure that the CD or DVD drive trays are retracted into place and tape across the drive tray to prevent it from opening.
6. Place tape over the power switch.
7. Record the make, model, serial numbers and any user-applied markings or identifiers.
8. Record or log the laptop computer and all cords, cables, wires, devices and components according to agency procedures.
9. Carefully package all evidence collected to prevent damage or alteration during transportation and storage.

If the Computer Is ON


Removing the power supply is generally the safest option. If evidence of a crime is visible on the computer display, however, request assistance from personnel with experience in volatile data capture and preservation (see <http://www.ecpi-us.org/Technicalresources.html>).

Immediate disconnection of power is recommended when —

- Information or activity on screen indicates that information or data is being deleted or overwritten.
- A destructive process appears to be in progress on the computer's data storage device(s).
- The system is powered on in a typical Microsoft Windows® environment. Pulling the power supply cord from the back of the computer will preserve information about the last user account logged in, login time, most recently used documents, most recently used commands, and other valuable information.

 **Immediate disconnection of power is NOT recommended when —**

- Information or data of apparent evidentiary value is in plain view onscreen. Seek assistance from personnel with advanced training in digital evidence collection.
- Indications exist that any of the following are active or in use: Chat room(s), text documents, remote data storage, Instant Messaging (IM), child pornography, contraband, financial documents, data encryption and obvious illegal activities.
- The device is a mobile or smart phone. Leave mobile and smart phones in the power state in which they were found.

 Improper shutdown of mainframe computers, servers or a group of networked computers may result in the loss of data, loss of evidence and potential civil liability. Secure the scene and request assistance from personnel with advanced training in digital evidence collection of large or complex computer systems (see <http://www.ecpi-us.org/Technicalresources.html>).

Packaging and Transporting Digital Evidence

Packaging Procedures

- Ensure that all digital evidence collected is properly documented, labeled, marked, photographed, video recorded or sketched and inventoried. Properly label connections and connected devices to facilitate reassembly of the system later.
- Protect any latent, trace or biological evidence contained on the digital evidence. Photograph digital evidence before conducting latent, trace or biological evidence processes on the evidence.
- Pack all digital evidence in antistatic packaging. Plastic bags and containers can produce static electricity and allow the development of humidity and condensation that can damage or destroy digital evidence.
- Package digital evidence in a manner that will prevent it from being bent, scratched or otherwise deformed. Label all containers properly.

- Leave phones in the power state in which they were found. Package phones in radio frequency-shielding material to prevent them from accessing communication signals.
- Collect all power supplies and adapters for all electronic devices seized.

Transportation Procedures

- Keep digital evidence away from magnetic fields, e.g., those produced by radio transmitters, car stereo speaker magnets and magnetic mount emergency lights. Other transportation hazards include heated seats and any device or material that can produce static electricity, such as carpet.
- Do not keep digital evidence in a vehicle for extended periods. Heat, cold and humidity can damage or destroy digital evidence.
- Ensure that computers and electronic devices are packaged and secured during transportation to prevent damage from shock and vibration.
- Document the transportation of the digital evidence and maintain the chain of custody.

Electronic Crime and Digital Evidence Considerations by Crime Category

Below are potential sources of digital evidence for different crimes. These lists are not exhaustive.

Child Abuse and/or Exploitation

- Calendars and journals
- Computer games
- Digital photo software
- Printed photographs
- Printers and copiers
- Scanners
- Still cameras and media
- Video cameras and tapes
- Video games and consoles
- Voice over Internet Protocol (VoIP) phones

Computer Intrusion

- Antennas
- Books and references on hacking
- List of computers accessed
- List of IP addresses
- Network devices and components
- Printed computer code
- Wireless network equipment

Counterfeiting

- Checks and money orders
- Credit card information
- Database printouts
- Financial records
- High-quality printers
- Magnetic strip readers
- Online banking software
- Printed computer code
- Reproductions of signatures
- Scanners, copiers, laminators

Death Investigations

- Credit card information
- Financial records
- Medical records
- Online banking software
- Personal writings and/or diaries
- Recently printed material
- Reproductions of signatures
- Telephone records and/or telephone bills
- Will-making software

Domestic Violence, Threats and Extortion

- Caller ID records
- Financial records
- Legal documents
- Personal writings and/or diaries
- Protection orders
- Telephone records/telephone bills

E-mail Threats, Harassment and/or Stalking

- Caller ID records
- Financial records
- Legal documents
- Maps, directions, GPS equipment
- Personal Web sites
- Personal writings and/or diaries
- Telephone records

Gambling

- Accounting software
- Cash
- Client lists
- Database printouts
- Electronic money transfers
- Financial records
- Forged documents
- Lists of online gambling sites
- References to odds and/or lines
- Sports betting statistics

Identity Theft

- Accounting software
- Cash
- Checks and money orders
- Credit card information
- Database printouts
- Electronic money transfers
- Financial records
- Forged documents
- High-quality printers
- Mail in victim's name
- Online banking software
- Reproductions of signatures
- Scanners, copiers, laminators
- Web site transaction records

Narcotics

- Cash
- Countersurveillance equipment
- Credit card information
- Database printouts
- Electronic money transfers
- Fictitious identification
- Financial records
- Forged documents
- GPS devices and maps
- Online banking software
- Photographs of drugs and accomplices
- Police scanners
- Unfilled prescriptions

Online Fraud and/or Economic Fraud

- Accounting software
- Cash
- Checks and money orders
- Credit card information
- Database printouts
- Electronic money transfers
- Financial records
- Forged documents
- Online banking software
- Reproductions of signatures

Prostitution

- Appointment logs
- Calendars and/or journals
- Cash
- Client lists
- Credit card information
- Database printouts
- Electronic money transfers
- Financial records
- Forged documents
- Lists of online escort sites
- Medical records
- Online banking software
- Printed photos

Software Piracy

- Cash
- CD and DVD burners and labelers
- Credit card information
- Electronic money transfers
- Financial records
- Forged documents
- Software activation codes
- Software duplication equipment

Telecommunication Fraud

- Boot loader devices
- Cash
- Credit card information
- Database printouts
- Electronic money transfers
- EPROM burner
- Financial records
- Forged documents
- Online banking software
- Phone cables
- SIM card reader
- Stolen phones

Terrorism (Homeland Security)

- Cash
- Credit card information
- Database printouts
- Electronic money transfers
- Fictitious identification
- Financial records
- GPS equipment and/or maps
- Phone cables
- Stolen phones
- VoIP phones

Other Potential Sources of Evidence

- Answering machines
- Audio recorders
- Blank pads of paper with impressions from prior writings
- Calendars
- CDs and CD burners
- Cell phones/smart phones
- Computer processors (chips)
- Computer-printed material
- Contact lists
- Copy machines
- Cordless landline telephones
- Digital cameras
- DVDs and DVD burners
- DVD/CD players
- External data-storage devices

Other Potential Sources of Evidence (continued)

- Fax machines
- GPS equipment and accessories
- Handwritten notes
- Hard drive duplicators
- Hardware and software manuals
- Information on steganography
- Internet activity records
- Laptop power supplies and accessories
- Microphones
- MP-3 players, e.g., iPods
- Multifunction machines (e.g., printer, scanner, copier, fax combos)
- Pagers
- Pieces of paper with possible passwords
- Printed e-mails and notes
- Printers

Other Potential Sources of Evidence (continued)

- Records of chat sessions
- Removable media
- Scanners
- Screen names and buddy lists
- Smart cards
- Software duplication equipment
- Telephone caller ID units
- User names and passwords
- Video cassette recorders (VCRs) and VCR tapes
- Web cameras
- Wireless access points

Information to Document to Assist the Forensic Examination

- Authorization to examine evidence
- Case summary
- Investigation point of contact
- Keyword lists
- Passwords
- Preliminary reports and documents
- Suspect information and nicknames
- Suspected criminal activity

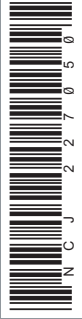
The National Institute of Justice is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, DC 20531

Official Business
Penalty for Private Use \$300



PRESORTED STANDARD
POSTAGE & FEES PAID
DOJ/NIJ
PERMIT NO. G-91

