NIJ

APR. 08

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

Chapter 7. Electronic Crime and Digital Evidence Considerations by Crime Category

Cover photographs copyright© 2001 PhotoDisc, Inc.

NCJ 219941

Chapter 7. Electronic Crime and Digital Evidence Considerations by Crime Category

The lists of electronic crime and digital evidence considerations presented in this chapter are not exhaustive, but are intended to assist a first responder identify sources of potentially valuable digital evidence by crime category. Depending on the complexity of the scene and the situation, the first responder may need to request more advanced technical assistance.

In some circumstances, trace, latent, or biological evidence such as fingerprints or DNA that may be important to the investigation may be present on computers and their components or on other electronic devices. First responders should follow agency procedures for collecting such evidence. Any destructive processes associated with recovering or analyzing trace, latent, biological, or other evidence should be postponed until after the digital evidence has been recovered for examination and analysis.

To assist in the forensic examination, the first responder should document the following information when possible:

- A summary of the case.
- Passwords to digital evidence seized.
- Investigation point-of-contact information.
- Preliminary reports and documents.
- Keyword lists.

- Suspected criminal activity.
- Suspect information including nicknames.

Child Abuse or Exploitation

Potential digital evidence in child abuse or child exploitation investigations includes:

- Computers.
- Scanners.
- Mobile communication devices.
- Video and still photo cameras and media.
- Calendars or journals.
- Digital camera software.
- Internet activity records.
- Photo editing and viewing software.
- Printed e-mail, notes, and letters and maps.
- Printed images or pictures.
- Notes or records of chat sessions.
- Web cameras and microphones.
- Computer games.
- Printers and copiers.
- Information regarding steganography.
- Removable media.
- External data storage devices.
- Videotapes.

- Video game consoles, games, and expansion packs.
- References to user-created folders and file names that classify images.

Computer Intrusion

Potential digital evidence in computer intrusion investigations includes:

- Computers.
- Network devices, routers, switches.
- Handheld mobile devices.
- Antennas.
- Removable media.
- External data storage devices.
- Web camera(s).
- Wireless network equipment.
- Lists of contacts and address books.
- Lists of Internet protocol addresses.
- Lists or records of computer intrusion software.
- Records of Internet chat sessions.
- Printed e-mail, notes, and letters.
- Printed computer program code.
- Executable programs.
- Lists of computers accessed.
- Notes or records of Internet activity.
- Usernames and passwords.

Counterfeiting

Potential digital evidence in counterfeiting investigations includes:

- Computers.
- Handheld mobile devices.
- PDAs or address books.
- Information regarding Internet activity.
- Information regarding checks, currency, and money orders.
- Removable media and external data storage devices.
- Credit card magnetic strip reader.
- Online banking software.
- Calendar(s).
- Reproductions of signatures.
- Customer information or credit card data.
- False identification.
- Printed e-mail, notes, and letters.
- False financial transaction forms.
- Information regarding financial records.
- Printouts of databases.

Death Investigation

Potential digital evidence in death investigations includes:

- Computers.
- Internet service bills.

- Removable media.
- External data storage devices.
- Mobile communication devices.
- PDAs.
- Address books and contact information.
- Telephone records.
- Personal writings and diaries.
- Medical records.
- Printed e-mail, notes, and letters.
- Financial or asset records.
- Recently printed material.
- Information regarding legal documents.
- Information regarding Internet activity.
- Will-making software or references.

Domestic Violence, Threats, and Extortion

Potential digital evidence in domestic violence, threats, and extortion investigations includes:

- Computers.
- Removable media.
- User names and accounts.
- External data storage devices.
- Mobile communication devices.
- Telephone records.

- PDAs or address books.
- Financial or asset records.
- Personal writings and diaries.
- Information regarding Internet activity.
- Printed e-mail, notes, and letters.
- Legal documents.
- Caller ID units.

E-mail Threats, Harassment, and Stalking

Potential digital evidence in e-mail threat, harassment, and stalking investigations includes:

- Computers.
- Handheld mobile devices.
- PDAs and address books.
- Telephone records.
- Diaries or records of surveillance.
- Evidence of victim background research.
- E-mail, notes, and letters.
- Financial or asset records.
- Printed photos or images.
- Legal documents.
- Information regarding Internet activity.
- Printed maps.

Gambling

Potential digital evidence in gambling investigations includes:

- Computers.
- Removable media.
- PDA, address books, or contact lists.
- External data storage devices.
- Customer database and bettor records.
- Information regarding Internet activity.
- Electronic money transfers.
- Online banking software.
- Calendars.
- Sports betting statistics.
- Customer information or credit card data.
- Financial asset records.
- Printed e-mail, notes, and letters.
- References to online gambling sites.

Identity Theft

Potential digital evidence in identity theft investigations includes:

- Computers.
- Mobile devices.
- Records of online purchases.
- Removable media.

- External data storage devices.
- PDAs, address books, contact lists.
- Online banking software.
- Information regarding Internet activity.
- Financial asset records.
- Electronic money transfers.
- Laminator(s).
- Calendars or journals.
- Forged documents and false identification.
- Victim information and credit card data.
- Copies of signatures.
- Printed e-mail, notes, and letters.
- ID pictures.
- Check cashing cards.
- Scanner(s).

Narcotics

Potential digital evidence in narcotics investigations includes:

- Computers.
- Handheld mobile devices.
- Removable media.
- External data storage devices.
- PDAs, address books, and contact information.

- Forged identification.
- Databases.
- Information regarding Internet activity.
- Drug receipts.
- Blank prescription forms.
- Printed e-mail, notes, and letters.
- Financial asset records.
- GPS devices.

Online or Economic Fraud

Potential digital evidence in online or economic fraud investigations includes:

- Computers.
- Removable media.
- Mobile communication devices.
- External data storage devices.
- Online auction sites and account data.
- Databases.
- PDAs, address books, and contact lists.
- Printed e-mail, notes, and letters.
- Calendars or journals.
- Financial asset records.
- Accounting or recordkeeping software.
- Printed photos and image files.

- Records or notes of chat sessions.
- Information regarding Internet activity.
- Customer credit information.
- Online banking information.
- List(s) of credit card numbers.
- Telephone numbers and call logs.
- Credit card magnetic strip reader.
- Credit card statements or bills.
- Printers, copiers, and scanners.

Prostitution

Potential digital evidence in prostitution investigations includes:

- Computers.
- Handheld mobile devices.
- Removable media.
- External data storage devices.
- Address books and client lists.
- Customer database or records.
- Calendars or datebooks.
- Forged identification.
- Information regarding Internet activity.
- Financial asset records.
- Printed e-mail, notes, and letters.

- Information regarding Web site.
- Medical records.
- Web camera(s).

Software Piracy

Potential digital evidence in software piracy investigations includes:

- Computers.
- Handheld mobile devices.
- Removable media.
- External data storage devices.
- Information regarding chat sessions.
- Information on cracking software.
- Printed e-mail, notes, and letters.
- References to copyrighted software.
- Forged software certificates.
- Lists of software activation codes.
- Information regarding Internet activity.
- Software duplication and packing material.

Telecommunication Fraud

Potential digital evidence in telecommunication fraud investigations includes:

- Computers.
- Handheld mobile devices.

- Removable media.
- External data storage devices.
- Phone programming software and cables.
- Multiple mobile phones.
- Subscriber identity module (SIM) card reader.
- Hacker boxes and cables.
- Lists of customer database records.
- Stolen telephones.
- Printed e-mail, notes, and letters.
- Financial asset records.
- Information regarding Internet activity.
- Telephone programming manuals.
- Erasable programmable read-only memory (EPROM) burner.

Terrorism (Homeland Security)

Potential digital evidence in terrorism investigations includes:

- Computers.
- Handheld mobile devices.
- Removable media.
- External data storage devices.
- Communication devices.
- Network components, routers, and switches.
- Voice over Internet Protocol (VoIP) equipment.

- GPS equipment.
- Information regarding Internet activity.
- Information regarding steganography.
- Printed e-mail, notes, and letters.