

U.S. Department of Justice
Federal Bureau of Investigation



DIGITAL EVIDENCE FIELD GUIDE:
**WHAT EVERY
PEACE OFFICER
MUST KNOW**

Continuing Education Series 1.1



Properly handling digital evidence can be complicated—but doing it right is key to ensuring it can be used to effectively support your investigation. This Field Guide was created to help you—the Peace Officer and First Responder—properly collect, preserve, and transport this type of evidence. The FBI's Operational Technology Division's Digital Evidence Section, which includes the Regional Computer Forensics Laboratory (RCFL) Program and the Computer Analysis Response Team (CART), are dedicated to sharing their knowledge about digital forensics with their colleagues throughout the law enforcement community. It is a product of the RCFL Program's Continuing Education Series—an online initiative that provides you with helpful news and information about the latest happenings in the digital forensics world. This Guide's authors, all seasoned law enforcement professionals and digital forensics RCFL/CART Examiners, hope that the information presented here and in future updates, serves as a valuable resource for years to come.

5 Key Facts You Should Know About Digital Evidence

- 1** Many types of crime involve digital evidence.
- 2** Every crime scene is a digital evidence crime scene. Investigators must apply the same level of care, custody, and control to ensure their personal safety and to preserve all types of evidence.
- 3** Digital evidence can be fragile. If not handled properly, heat, cold, and magnets can destroy it. Digital evidence can also be damaged by dropping it.
- 4** Digital evidence can be easily altered. If a computer is off, leave it off. Just turning it on or taking a quick peek at the files can change the data. If the computer is on, perform a proper shutdown or ask a digital forensics Examiner for assistance. When in doubt, leave the device “off.”
- 5** Never assume that digital evidence is destroyed. RCFL/CART Examiners have extracted digital evidence from burned out computers and devices found at the bottom of a lake. Play it safe—always bring the device to a certified digital forensics Examiner for further study.

SECTION 1: CRIMINAL USES OF DIGITAL EVIDENCE

Digital information is created, stored, processed, and/or translated by an electronic device. To better understand how digital information can be a factor in a criminal investigation, Peace Officers should know that—

- A computer* or digital evidence item may play a role in a crime. Therefore, during the investigation, it's necessary to determine the item's role in order to handle and treat it properly.
- Digital evidence could play any or all of three roles in a crime—
 1. Target of a crime
 2. Instrument of a crime
 3. Repository of evidence that documents the crime itself.

* Throughout this Guide, the term “computer” refers to a digital device in the form of a cell phone, laptop, personal digital assistant (PDA), thumb drive, or any other electronic device capable of storing digital information.



Computers as the Target of a Crime

The computer or system can be vulnerable to attack from outside—stealing or destroying information, depending on the criminal's intent. The types of crimes can include—

- Child Exploitation
- Corporate Espionage
- Cyber Terrorism
- Identity Theft/Internet Fraud
- Intrusion
- Phishing.

Computers as the Instrument of a Crime

When a computer system is the target of a crime, it can also be an instrument of the intrusion or attack. In these situations, the computer can become a roadmap to a criminal's activities. Handle these devices with great care—your investigation may depend on it. The types of crimes include—

- Child Exploitation
- Child Solicitation
- Corporate Espionage
- Counterfeiting
- Credit Card Fraud
- Cyber Terrorism
- Identify Theft/Internet Fraud
- Intrusion (Hacking)
- Phishing/Social Engineering
- Theft of Intellectual Property.

Computer as the Repository of Evidence

When a computer contains evidence of crime, it may take several different forms, e.g., files, programs, e-mail, etc. that are obvious, hidden, or “erased.” The following types of crimes often involve a computer as a repository of the digital evidence—

- Fraud and Embezzlement
- Child Pornography
- Child Solicitation (saving chat, e-mail, webcam recordings)
- Narcotics Trafficking
- Intrusion or Hacking Storage Platform for Tools and Programs
- E-mail or Chat with Accomplices Regarding Traditional Crimes Such as Homicide, Robbery, or Burglary.

Generally, two types of evidence pertain to computers as repositories. The following descriptions are not all-inclusive lists, but provide common examples of the types of evidence in each category—

UNIVERSAL—The following types of evidence are universal to criminal cases involving digital evidence—

- Chat Logs
- E-mail
- Internet Browsing: Favorites, Temporary Files, History, Activity Logs
- Financial Records/Programs
- Photos and Movies
- My Documents
- Registry Information.



CASE SPECIFIC—Evidence can also be classified by case-specific categories, such as—

- **Child Exploitation/
Child Pornography**
 - ▶ File Sharing Programs/Peer-to-Peer (P2P)
 - ▶ News Group Links
 - ▶ Photo Editing Software
 - ▶ Screen Names
 - ▶ Webcam Recordings (digital photos and movies)
- **Cyber Terrorism/Network Intrusion**
 - ▶ Encryption Software, e.g., Passwords and Public/Private Key Sets
 - ▶ Internet Links or Programs That Make the User Anonymous
 - ▶ Internet Protocol (IP) Addresses and Connection Logs
 - ▶ Proprietary Programs
 - ▶ Source Code
 - ▶ System Configuration Logs
- **Financial Fraud/Counterfeiting**
 - ▶ Check-Making Software
 - ▶ Credit Card Numbers
 - ▶ Customer Databases
 - ▶ Digital Photos for False IDs
 - ▶ Financial Records
 - ▶ Photo Editing Software
 - ▶ Template Graphics for False IDs

■ Homicide

- ▶ Alibi Planning (with accomplices)
- ▶ Identification of Accomplices
- ▶ Internet Research (about the victim and/or activities, and similar crimes)

■ Identity Theft

- ▶ Backdrops
- ▶ Scanners and Software
- ▶ Stolen Mail
- ▶ ID Templates and Blanks

■ Narcotics Investigation

- ▶ Price Lists
- ▶ Spreadsheets



While interviewing a subject(s), there are a number of general and computer/-specific questions the investigator should ask, such as—

- User names/User Accounts
- Passwords/Pass Phrases
- Screen Names
- Internet Provider.

For a full list of investigative questions, go to www.rcfl.gov and click the **Continuing Education Series—Field Guide** link under **Training**.

Image Scan

The Image Scan tool was developed by the CART Unit and allows an investigator to preview a suspect's graphics image files during a consent search—without altering any data on the computer system. Image Scan is not meant to replace a professional computer forensics examination; however, once it's deployed, it can detect the drives and partitions on a computer and search for graphics image files in a write-protected manner. Law enforcement agencies can obtain the Image Scan tool by



completing a 1-day training course offered by the RCFL/CART Programs. After completing the course, students receive the Image Scan kit, which includes a CD-Rom and 2 GB thumb drive. For more information or to request training, send an e-mail to ImageScan@rcfl.gov.

SECTION 2: IDENTIFYING DIGITAL EVIDENCE

Digital evidence typically falls into four distinct categories:

1. Commonplace

Traditional digital media that often hides in plain view. Commonplace digital media can include—

- Cell Phones
- Thumb Drives
- Digital Cameras
- DVD/CDs
- MP3 Players
- Flash Memory Cards



2. Obscure

Non-traditional digital media that are present during the execution of a digital search warrant—but are often not noticed, thought of, or identified as an item containing usable or relevant digital media. Obscure digital media can include—

- Printers with Smart Media or Internal Memory
- Digital Video Recorder (i.e., DVRs, aka “TiVo®”)
- Answering Machines
- GPS Receivers (e.g., Garmin devices)
- Game Consoles (e.g., Xbox, Playstation)
- Digital Voice Recorders.



3. Protected

Non-traditional digital media that include those meant to prevent unauthorized access or to conceal data through either encryption or biometric verification.

- Biometric Protected Devices:
 - ▶ Iris Scanners
 - ▶ Fingerprint Readers
- Mechanically Protected Devices:
 - ▶ Access Cards
 - ▶ Dongles



4. Concealed

Digital media designed to disguise or conceal their true purpose and are easily hidden and/or transported on one's person. If law enforcement personnel do not conduct a thorough and proper search, they very likely won't recover concealed media, which can include—

- Computers disguised as boxes or bottles
- USB flash drives disguised as—
 - ▶ Wristbands
 - ▶ Pens
 - ▶ Watches
 - ▶ Earrings
 - ▶ Pocket knives
 - ▶ Credit cards
 - ▶ Toys
 - ▶ Everyday objects



SECTION 3: LEGAL CONSIDERATIONS

Because electronic devices are containers of digital evidence—law enforcement is permitted to conduct a lawful search. Three options are available to you:

- 1 Search Warrant**—If possible, do your advance work before conducting the actual search to determine whether a computer specialist should be present. Also, Peace Officers should confirm that the warrant names the items for collection as well as the electronic information contained therein. Be thorough and detailed—below are some key questions the investigator should ask while preparing the search warrant—
 - ▶ Are networks involved?
 - ▶ How many computers will be at the scene?
 - ▶ Is the subject/user technically sophisticated?
- 2 Consent to Search**—“Consent to Search” forms should include language pertaining to the actual seizure and the digital forensics examination that will occur at a later date. A downloadable copy of a generic Consent to Search form is available at www.rcfl.gov.
- 3 Plain View**—In these situations, the Peace Officer can seize contraband if he/she is lawfully in a position to view such items, and/or the incriminating or evidentiary nature of the items are readily apparent to the officer. Items not in plain view are inadmissible without a warrant or consent.

- Consult your legal advisor when obtaining your warrant or when dealing with any privacy issues—better safe than sorry.
- You're searching not only for computers—but for the information contained therein. Note that in the warrant.
- Warrants must be executed during a specific time frame, e.g., 10 days, but digital forensics examinations often take longer. Therefore, note this in the warrant or affidavit. Also, if you are sending the seized equipment to a digital forensics laboratory for examination outside your jurisdiction, include this information in your search warrant or affidavit as well.



For more tips on preparing a search warrant, visit www.rcfl.gov—“Continuing Education Series.”

SECTION 4: EXECUTING THE DIGITAL SEARCH WARRANT

PRIORITY #1: Officer Safety—Always secure the crime scene.

PRIORITY #2: Protect the Evidence from Harm—Remind investigators to keep all non-law enforcement personnel away from computers because—

- They could be attempting to arm themselves—Peace Officers are reporting an increase in instances of weapons within easy reach of the keyboard.
- Suspects may try to destroy evidence.

1 Executing the Digital Search Warrant

It is recommended that Peace Officers use the following procedures to safely execute the digital search warrant:

- **Isolate the Computer**—To isolate the computer and protect the evidence from harm or destruction—
 - ▶ **Remove the Network Connection**—This disconnects the computer from remote access.
 - ▶ **Identify Wireless Access Points**—If you encounter them, pull the power plug from the access point.
 - ▶ **Disconnect Recording Devices**—Such as webcams. Pull the connection from the computer or place something over the camera until the connection can be safely terminated.



If you suspect that destructive programs are running, immediately pull the power cord from the back of the computer.



2 Documenting the Scene

A. Take Notes—Notes are essential and will assist—

- ▶ The computer forensics Examiner, investigator, prosecutor, and court in showing where each piece of evidence was found
- ▶ You, the Peace Officer, both in preparing your final report and in testifying in court.

Your overall notes should record—

- ▶ **Who**—Took photos, secured the digital crime scene and what methods they used, marked the computers, prepared the sketch, seized the computers, and took exit photos
- ▶ **Times**—When you entered the scene, took control of the computers, and you left the scene
- ▶ **Description of the Computer**—When describing the computer, some important points to note are—
 - What was on the screen
 - What peripherals were attached to the computer.

B. Sketch the Scene—Your notes should include a diagram of the crime scene showing where the digital evidence was located. After drawing the initial sketch, add detail to the diagram such as the serial number(s) of the computer(s). While artistic ability is helpful—accuracy is essential.



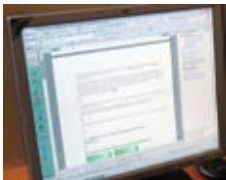
Identifying Evidence with Number Tents

- Desktop and tower computers
- Laptop computers
- PDAs/portable computers
- Free-standing hard drives
- Flash and other free-standing media such as CDs, DVDs, Zip Disks, etc.



C. Take Digital Photographs—In addition to taking detailed notes and completing a seizure work sheet*, you should photographically document the entire crime scene showing the location of every digital device. Begin the process by photographing—

- ▶ **Active Screen**—Photograph the computer's active screen if it's on.
 - Do **not** turn the computer on for this purpose.
 - Check the task bar to check whether any active programs are running.
- ▶ **Passwords**—People frequently have passwords written down within reach of the keyboard, on the mouse pad, in drawers, or pencil trays, or on a Rolodex. Photograph any passwords you find.
- ▶ **Books**—Check the bookcases around the scene—their contents provide an excellent idea of the subject's computer knowledge. Take a picture of any computer books you find.
- ▶ **Back of the Computer**—Photograph the back of the computer noting the cord and cable locations.



*For copies of the RCFL Program's *Seizure Work Sheet*, visit www.rcfl.gov.



D. Shut Down System if Necessary—There are times when a Peace Officer must shut down a system. Prior to doing so, you must first determine whether the computer is on or off by checking the following:

- ▶ If the computer appears to be off or if the monitor is dark, perform the “Bump/Shift/Feel” test—
 - Bump the mouse by clicking it or moving the device
 - Depress the shift key
 - Feel the fan.

After Performing the Bump/Shift/Feel Test—If text or images appear on the monitor, then the computer is still on. If nothing appears on the monitor and if the fan is cool and not moving, then the computer is off.

If you determine that the computer is on, there are two approaches for shutdown:

- 1 Hard Shutdown**—If the computer is on and you are concerned about the destruction of evidence, perform a hard shutdown by pulling the power cord from the electrical source OR removing the battery from the laptop. Before performing this procedure, consider that hard shutdowns may—

- Preserve some system files
- Prevent:
 - ▶ Destructive program activation on shutdown
 - ▶ Changes to time stamp
 - ▶ Changes to file attributes
- Corrupt operating system and open documents
- Lose unsaved open files.



2 Graceful Shutdown—With a graceful shutdown, you close the system in the recommended manner. It's important to note that shutdown methods for different operating systems vary. Graceful shutdowns may—

- + Help locate network connections
- + Identify and close open files
- + Ensure a more successful boot of the computer
- Lose some system files
- Activate destructive programs at shutdown.

**1**

Some computers are running Windows Vista. If the computer is using this operating system, look for the shutdown icon, which can be customized by the user, but is usually located in the lower left-hand corner of the screen. See the Vista Work Sheet on www.rcfl.gov.

2

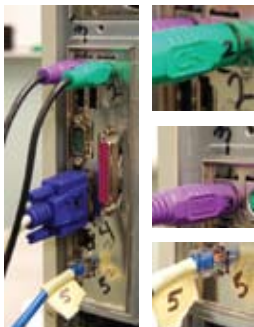
While at a search scene, other law enforcement personnel may assume that you're a digital forensics expert when you start taking computer systems or computer networks down. If that's not the case, know your limits and don't take on more than you can handle.

SECTION 5: PACKAGING AND TRANSPORTING DIGITAL EVIDENCE

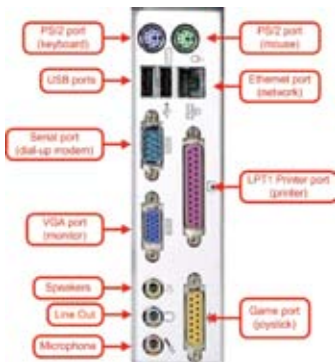
Once you properly document the scene and shut down the system, you are ready to package and transport the digital evidence. Below are some tips to safely complete these processes.

Dismantling the Computer

- Start by “direct marking” a number for each cable and the corresponding port on the computer.
- Record what each cable is attached to (e.g., the mouse, monitor, or printer) on your worksheet or in your notes.
- If the cable is too small to direct mark, wrap a piece of tape around it and mark the number on the tape.
- Once you’ve marked the cables with numbers, photograph them.
- Finally, remove the cables from the back of the computer.



Shown here is the back of a typical computer with common ports and their names.



Packaging the Computer

- 1** Begin the process of packaging the computer by placing tamper-resistant evidence tape over the power port and the edge of the computer case. This ensures that the computer cannot be powered up or the case opened without the tape being torn.
- 2** Print your name, initials, and date on the tape—overlapping onto the evidence. Some agencies require a second person to place his/her initials on the seal as well.
- 3** While the computer can be impounded like this, for additional protection you can place it inside a paper bag or anti-static bag.
- 4** As with any evidence placed in a bag, write your name, initials, and date on the tape that seals the bag.



1




2



3



4




TIP

When transporting laptops, don't forget to include the power converter/adaptor and the case.



Packaging Cell Phones/PDAs



TIP

These items may be small, but they can contain the subject's most treasured, and valuable data. When packaging these devices, remember to seize the power sources, e.g., synchronization cradles or cables.



Transporting Digital Evidence

When packaging the evidence for transport:

- Check the floppy drive and CD-ROM for any loose media.
- Use:
 - ▶ Plastic tubs
 - ▶ Cardboard boxes
 - ▶ The original box for the computer
 - ▶ Store and transport loose hard drives in anti-static bags, bubble wrap, or drive cases.
 - ▶ Try to transport in the back seat if possible and place the device in a secure tub or container that won't move easily.
 - ▶ Keep equipment away from LMR radios—they emit a magnetic field that could damage digital evidence.
 - ▶ Transport in a safe, dry, and preferably cool area such as the passenger compartment (not the trunk). Also, avoid high heat (leaving the device in a car during the summer).
 - ▶ Consider loading it last and transporting immediately
 - Place peripheral devices in the back seat—wrap and tape the cables to avoid “cable spaghetti.”
 - ▶ Avoid packing peanuts because they can become lodged in computer orifices.



Definitions

Boot—The process the computer uses when it is started up to load the operating system.

Computer Forensics—Science involving the identification, preservation, extraction, documentation, and interpretation of computer data for presentation in court.

Dongle—A device attached to a computer (usually a USB device) that is used to authenticate a particular software package or application.

Encryption—The process of scrambling or encoding data so only the intended users can gain access to it.

IP Address—The numerical sequence that serves as an identifier for an Internet server. An IP address appears as a series of four groups of numbers separated by dots.

Personal Digital Assistant (PDA)—Handheld devices that provide phone, e-mail, internet access, camera, music player, and other computing functions.

Peer-to-Peer (P2P)—Process whereby computers can directly trade information between each other without the assistance of a third-party network (e.g., Limewire, Napster, Bearshare).

Removable Media—Devices that store data and can easily be removed and concealed, such as floppy discs, CDs, DVDs, flash cards, and USBs.

Router—A computer networking device that interconnects separate networks allowing them to exchange data. Available in both wired and wireless models.

Webcam—A digital camera capable of downloading images to a computer for transmission over the Internet or other network.

Wireless Access Point (WAP)—A device that connects wireless communication devices together to form a wireless network.

Write-Protected—To modify (a file or disk) so that its data cannot be edited or erased.


RCFL/CART CONTACTS

RCFL and CART personnel comprise the largest digital forensics laboratory network in the country. They are available to the law enforcement community 24/7 to answer questions and offer assistance. Below is their contact information.

RCFL National Program Office

 www.rcfl.gov
 703-985-3677



CART Headquarters

 703-985-3326



Chicago RCFL

 www.cgrcfl.org
 312-431-1751



Greater Houston RCFL

 www.ghrcfl.org
 713-316-7878


Heart of America RCFL

 www.harcrfl.org
 816-584-4300



Intermountain West RCFL

 www.iwrcfl.org
 801-456-4800 (Salt Lake City)
 208-433-3527 (Boise)
 406-896-3257 (Billings)

Kentucky RCFL

 www.krcfl.org
 502-852-4369

Miami Valley RCFL

 www.mvrcfl.org
 937-512-1924

New Jersey RCFL

 www.njrcfl.org
 609-631-8777



North Texas RCFL

 www.ntrcfl.org
 972-559-5800



Northwest RCFL

 www.nwrcfl.org
 503-249-3750

Philadelphia RCFL

 www.phrcfl.org
 610-975-3691


Rocky Mountain RCFL

 www.rmrcfl.org
 303-649-7900

San Diego RCFL

 www.rcfl.org
 858-499-7799

Silicon Valley RCFL

 www.svrcfl.org
 650-289-3000

Western New York RCFL

 www.wnyrcfl.org
 716-362-8600

