Processing Law Enforcement Crime Scenes

Processing Law Enforcement Crime Scenes

- You must be **familiar with criminal rules** of search and seizure
- You should also **understand how a search warrant works** and what to do when you process one
- Law enforcement officer may search for and seize criminal evidence only with **probable cause**
  - Probable cause refers to the **standard** specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest
  - With probable cause, a police officer can obtain a search warrant from a judge that authorizes a search and the seizure of specific evidence related to the criminal complaint.

Processing Law Enforcement Crime Scenes

- The Fourth Amendment states that only warrants “particularly describing the **place** to be searched, and the **persons** or things to be seized” can be issued

Understanding Concepts and Terms Used in Warrants

- **Innocent information**
  - Unrelated information
  - Often included with the evidence you're trying to recover
- Judges often issue a **limiting phrase** to the warrant
  - Allows the police to separate innocent information from evidence

Understanding Concepts and Terms Used in Warrants

- **Plain view doctrine**
  - Objects falling in plain view of an officer who has the right to be in position to have that view
    - Are subject to seizure without a warrant and may be introduced in evidence
- **“Knock and announce”**
  - With few exceptions, warrants require that officers knock and announce their identity
    - When executing a warrant

Preparing for a Search

Preparing for a Search

- Preparing for a computer search and seizure
  - Probably the most **important step** in computing investigations
- To perform these tasks
  - You might need to get answers from
    - **the victim**
    - **an informant**
      - could be a police detective assigned to the case, a law enforcement witness, or a manager or coworker of the person of interest to the investigation

Preparing for a Search

- **Identifying the Nature of the case**
- **Identifying the Type of Computing**
- **Determining Whether You Can Seize a Computer**
- **Obtaining a Detailed Description of the Location**
- **Determining Who Is in Charge**
- **Using Additional Technical Expertise**
- **Determining the Tools You Need**
- **Preparing the Investigation Team**

Identifying the Nature of the Case

- Start by identifying the nature of the case
    - Including whether it involves the private or public sector
- The **nature of the case dictates how you proceed**
    - – And what types of assets or resources you need to use in the investigation

Identifying the Type of Computing System

- Difficult step because the crime scene isn’t controlled
  - might not know what kinds of computers were used to commit a crime or how or where they were used
- If you can identify the computing system
  - Estimate the size of the drive on the suspect’s computer
  - And how many computers to process at the scene
  - Determine which OSs and hardware are involved

Determining Whether You Can Seize a Computer

- Seizing the computers and taking them to your lab for further processing depend on the type of case and location of the evidence
- Law enforcement investigators need a warrant
- If removing the computers will irreparably harm a business
  - The computers should not be taken offsite

Determining Whether You Can Seize a Computer

- An additional complication
  - files stored offsite that are accessed remotely
  - online data storage services that rent space, which essentially can’t be located physically
- If you aren’t allowed to take the computers to your lab
  - Determine the resources you need to acquire digital evidence and which tools can speed data acquisition

Obtaining a Detailed Description of the Location

- More information about the location - more efficient evidence
- **Identify potential hazards**
  - Interact with your **HAZMAT team**
- HAZMAT guidelines
  - A HAZMAT technician may need to acquire the image, following your instructions
  - You may need to put the target drive in a special HAZMAT bag
  - HAZMAT technician can decontaminate the bag
  - Check for high temperatures

Determining Who Is in Charge

- **Corporate** computing investigations
  - Require only one person to respond
- **Law enforcement** agencies
  - Handle large-scale investigations
  - Designate lead investigators

Using Additional Technical Expertise

- Look for specialists
  - OSs
  - RAID servers
  - Databases
- Finding the right person can be a challenge
- Educate specialists in investigative techniques
  - Prevent evidence damage

Determining the Tools You Need

- Prepare tools using incident and crime scene information
- Initial-response field kit
  - Lightweight
  - Easy to transport
- Extensive-response field kit
  - Includes all tools you can afford

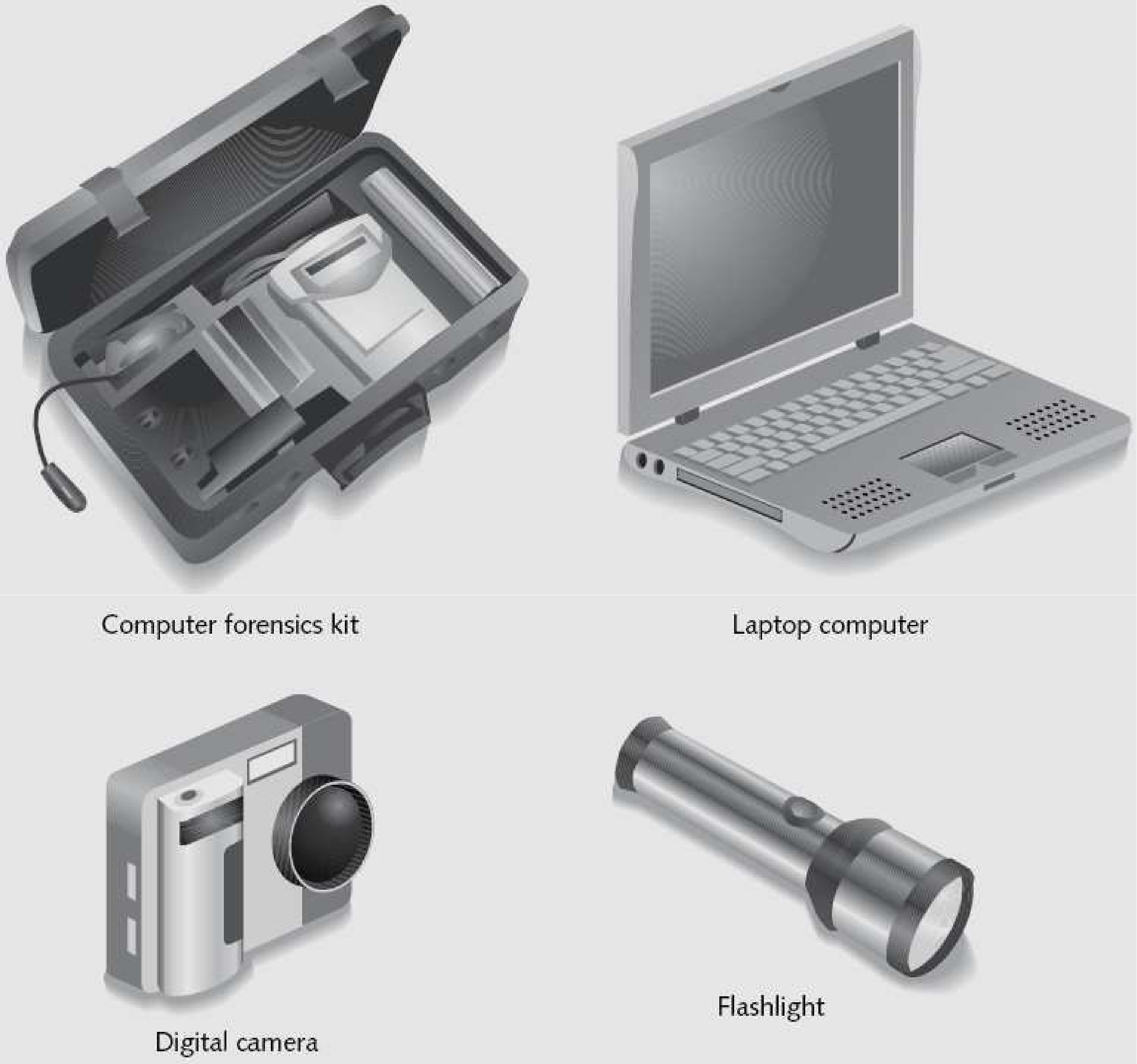


Figure 5-5 Items in an initial-response field kit

Table 5-1 Tools in an initial-response field kit

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	IDE ribbon cable (ATA-33 or ATA-100)
1	SATA cable
1	Forensic boot media containing your preferred acquisition utility
1	Laptop IDE 40- to 44-pin adapter, other adapter cables
1	Laptop computer
1	FireWire or USB dual write-protect external bay
1	Flashlight
1	Digital or 35mm camera with film and flash
10	Evidence log forms
1	Notebook or dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marker
10	External USB devices, such as a thumb drive, or a larger portable hard drive

Table 5-2 Tools in an extensive-response field kit

Number needed	Tools
Varies	Assorted technical manuals, ranging from OS references to forensic analysis guides
1	Initial-response field kit
1	Portable PC with SCSI card for DLT tape drive or suspect's SCSI drive
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Leather gloves and disposable latex gloves (assorted sizes)
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from suspect's interior CPU cabinet
10	USB thumb drives of varying sizes
2	External hard drives (200 GB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives for data acquisition

Preparing the Investigation Team

- Review facts, plans, and objectives with the investigation team you have assembled
- Goals of scene processing
  - Collect evidence
  - Secure evidence
- Slow response can cause digital evidence to be lost

Securing a Computer Incident or Crime Scene

Securing a Computer Incident or Crime Scene

- Goals
  - **Preserve** the evidence
  - Keep information **confidential**

- Define a secure perimeter
  - Use yellow barrier **tape**
  - Legal authority: keep **unnecessary people out** but don’t obstruct justice or fail to comply with police officers
- Professional curiosity can destroy evidence
  - Involves police officers and other professionals who aren’t part of the crime scene processing team

Seizing Digital Evidence at the Scene

Seizing Digital Evidence at the Scene

- Law enforcement can seize evidence
  - With a proper warrant
- Corporate investigators rarely can seize evidence
- When seizing computer evidence in criminal investigations
  - Follow standards
- Civil investigations follow same rules
  - Require less documentation though

Preparing to Acquire Digital Evidence

- The evidence you acquire at the scene depends on the nature of the case
  - And the alleged crime or violation
- Ask your supervisor or senior forensics examiner in your organization the following questions:
  - Do you need to take the entire computer and all peripherals and media in the immediate area?
  - How are you going to protect the computer and media while transporting them to your lab?
  - Is the computer powered on when you arrive?

Preparing to Acquire Digital Evidence

- Ask your supervisor or senior forensics examiner in your organization the following questions :
  - Is the suspect you’re investigating in the immediate area of the computer?
  - Is it possible the suspect damaged or destroyed the computer, peripherals, or media?
  - Will you have to separate the suspect from the computer?

Processing an Incident or Crime Scene

- Guidelines
  - Keep a journal to document your activities
  - Secure the scene
    - Remove people who are not part of the investigation
  - Take video and still recordings of the area around the computer
    - Pay attention to details (cables and their connections)
  - Sketch the incident or crime scene (components and their distance between them)
  - Check computers as soon as possible

Handling a Running Computer

- Old rule: pull the plug
  - Don’t cut electrical power to a running system unless it’s an older Windows 9x or MS-DOS system
- Perform a live acquisition if possible
- When shutting down Win XP or later, or Linux/Unix, perform a normal shutdown, to preserve log files
- Save data from current applications as safely as possible
- Record all active windows or shell sessions
- Photograph the screen

Handling a Running Computer

- Make notes of everything you do when copying data from a live suspect computer
- Save open files to an external hard drive or a network share
  - If that is not possible, save them with new names
- Close applications and shut down the computer

Processing an Incident or Crime Scene

- Guidelines
  - Bag and tag the evidence, following these steps:
    - Assign one person to collect and log all evidence
    - Tag all evidence you collect with the current date and time, serial numbers or unique features, make and model, and the name of the person who collected it
    - Maintain two separate logs of collected evidence
    - Maintain constant control of the collected evidence and the crime or incident scene

Processing an Incident or Crime Scene

- Guidelines
  - Look for information related to the investigation
    - Passwords, passphrases, PINs, bank accounts
    - Look at papers, in drawers, in trash cans
  - Collect documentation and media related to the investigation
    - Hardware, software, backup media, documentation, manuals

Processing Data Centers with RAID Systems

- Sparse acquisition
  - Technique for extracting evidence from large systems
  - Extracts only data related to evidence for your case from allocated files
    - And minimizes how much data you need to analyze
- Drawback of this technique
  - It doesn’t recover data in free or slack space

Using a Technical Advisor

- Technical advisor
  - Can help you list the tools you need to process the incident or crime scene
  - Person guiding you about where to locate data and helping you extract log records
    - Or other evidence from large RAID servers
  - Can help create the search warrant by itemizing what you need for the warrant

Technical Advisor Responsibilities

- Know aspects of the seized system
- Direct investigator handling sensitive material
- Help secure the scene
- Help document the planning strategy for search and seizure
- Conduct ad hoc trainings
- Document activities
- Help conduct the search and seizure

Documenting Evidence in the Lab

- Record your activities and findings as you work
  - Maintain a journal to record the steps you take as you process evidence
- Goal is to be able to reproduce the same results
  - When you or another investigator repeat the steps you took to collect evidence
- A journal serves as a reference that documents the methods you used to process digital evidence

Processing and Handling Digital Evidence

- Maintain the integrity of digital evidence in the lab
  - As you do when collecting it in the field
- Steps to create image files:
  - Copy all image files to a large drive
  - Start your forensics tool to analyze the evidence
  - Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash
  - Secure the original media in an evidence locker

Storing Digital Evidence

Storing Digital Evidence

- The media you use to store digital evidence usually depends on how long you need to keep it
- CD-Rs or DVDs
  - The ideal media
  - Capacity: up to 17 GB
  - Lifespan: 2 to 5 years
- Magnetic tapes
  - Capacity: 40 to 72 GB
  - Lifespan: 30 years
  - Costs: drive: $400 to $800; tape: $40

Storing Digital Evidence

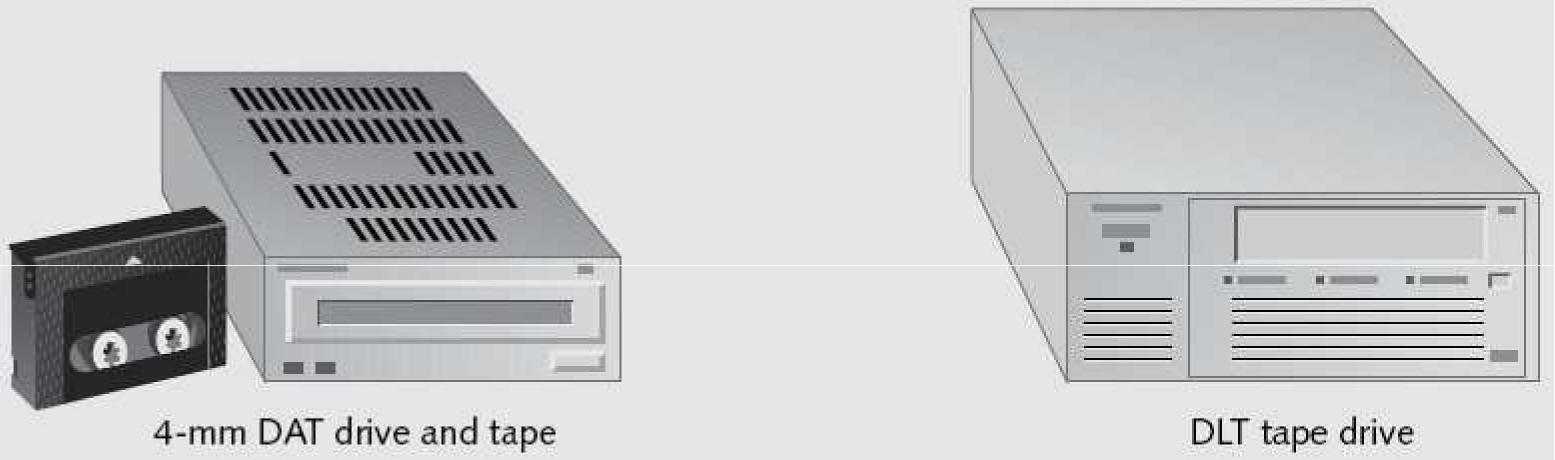
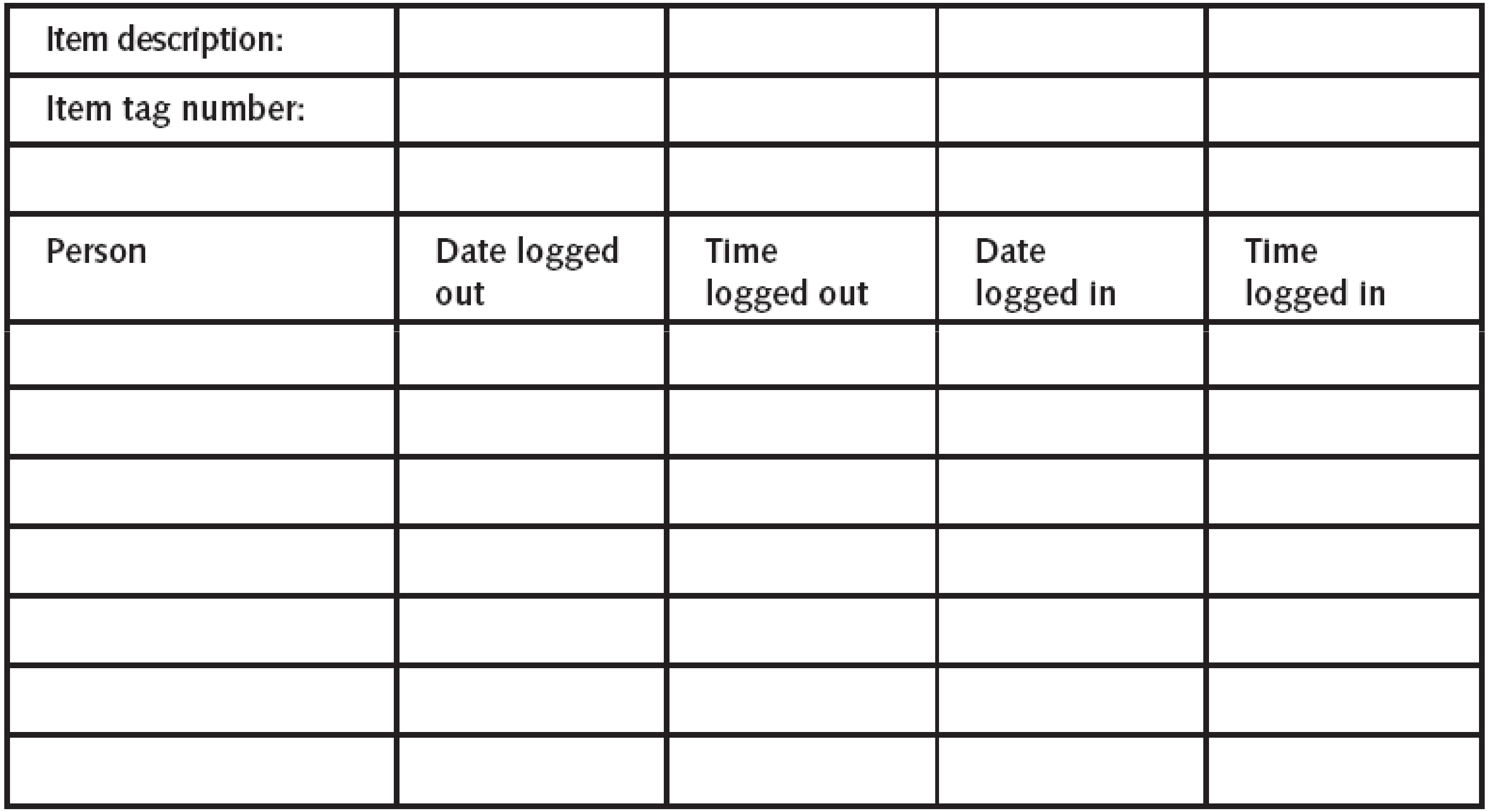


Figure 5-6 4-mm DAT and DLT tape drives

Evidence Retention and Media Storage Needs

- To help maintain the chain of custody for digital evidence
  - Restrict access to lab and evidence storage area
- Lab should have a sign-in roster for all visitors
  - Maintain logs for a period based on legal requirements
- You might need to retain evidence indefinitely
  - Check with your local prosecuting attorney’s office or state laws to make sure you’re in compliance
  - You cannot retain child pornography evidence, however

Evidence Retention and Media Storage Needs



Item description:				
Item tag number:				
Person	Date logged out	Time logged out	Date logged in	Time logged in

Figure 5-7 A sample log file

Documenting Evidence

- Create or use an evidence custody form
- An evidence custody form serves the following functions:
  - Identifies the evidence
  - Identifies who has handled the evidence
  - Lists dates and times the evidence was handled
- You can add more information to your form
  - Such as a section listing MD5 and SHA-1 hash values

Documenting Evidence

- Include any detailed information you might need to reference
- Evidence bags also include labels or evidence forms you can use to document your evidence

Obtaining a Digital Hash

Obtaining a Digital Hash

- **Cyclic Redundancy Check (CRC)**
  - Mathematical algorithm that determines whether a file's contents have changed
  - Most recent version is CRC-32
  - Not considered a forensic hashing algorithm
- **Message Digest 5 (MD5)**
  - Mathematical formula that translates a file into a hexadecimal code value, or a hash value
  - If a bit or byte in the file changes, it alters the **digital hash**

Obtaining a Digital Hash

- Three rules for forensic hashes:
  - You can’t predict the hash value of a file or device
  - No two hash values can be the same
  - If anything changes in the file or device, the hash value must change
- **Secure Hash Algorithm version 1 (SHA-1)**
  - A newer hashing algorithm
  - Developed by the **National Institute of Standards and Technology (NIST)**

Obtaining a Digital Hash

- In both MD5 and SHA-1, collisions have occurred
- Most computer forensics hashing needs can be satisfied with a **nonkeyed hash set**
  - A unique hash number generated by a software tool, such as the Linux md5sum command
- **Keyed hash set**
  - Created by an encryption utility's secret key
- You can use the MD5 function in FTK Imager to obtain the digital signature of a file
  - Or an entire drive