Guide to Computer Forensics and Investigations Fifth Edition

Chapter 4

Processing Crime and Incident Scenes

Objectives

- Explain the **rules** for controlling digital evidence
- Describe how to **collect evidence** at private-sector incident scenes
- Explain **guidelines** for processing law enforcement crime scenes
- List the **steps in preparing for an evidence** search
- Describe how to **secure a computer incident** or crime scene

Objectives (Cont)

- Explain **guidelines** for seizing digital evidence at the scene
- List **procedures** for **storing** digital evidence
- Explain how to **obtain a digital hash**

- Review a case to identify requirements and plan your investigation

Identifying Digital Evidence

- **Digital evidence**
  - Can be any information stored or transmitted in digital form
  - *There is a difference between document evidence and digital evidence. i.e document evidence is always visible on its face*

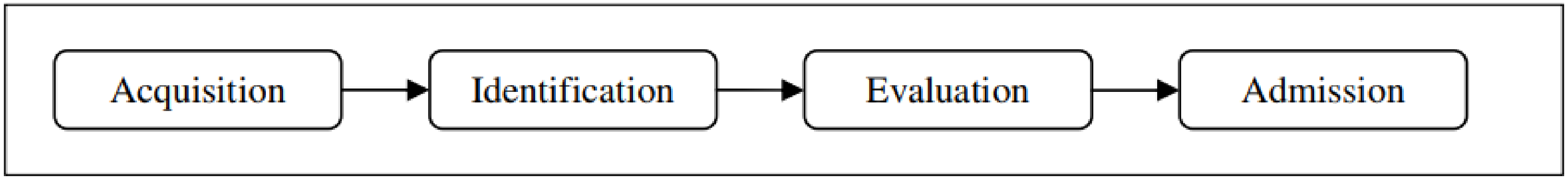
- U.S. courts accept digital evidence as physical evidence
  - Digital data is treated as a tangible object

- Groups such as the **Scientific Working Group on Digital Evidence (SWGDE)** set standards for recovering, preserving, and examining digital evidence

https://www.swgde.org/

Identifying Digital Evidence (Cont)

- General tasks investigators perform when working with digital evidence:
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably



- Collecting digital devices and processing a criminal or incident scene must be done systematically

Understanding Rules of Evidence

- Consistent practices help verify your work and enhance your credibility
  - *must handle all evidence consistently*

- Comply with your state's rules of evidence or with the Federal Rules of Evidence
  - *i.e Security and accountability control for evidence*

- Evidence admitted in a criminal case can be used in a civil suit, and vice versa

- Keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence

Understanding Rules of Evidence (Cont)

- Digital evidence is unlike other physical evidence because it can be changed more easily
  - The only way to detect these changes is to compare the original data with a duplicate. *i.e Hash*

- Most courts have interpreted computer records as hearsay evidence
  - Hearsay is secondhand or indirect evidence
  - *Hearsay - Evidence of a statement made other than by a witness*

Understanding Rules of Evidence (Cont)

- Generally, digital records are considered admissible if they qualify as a business record

- Computer records are usually divided into:
  - **Computer-generated records**
    - *Data maintained by system and not usually data created by human. i.e System logs, proxy log file.*
  - **Computer-stored records**
    - *Electronic data that a person creates and saves on a computer, such as a spreadsheet or word processing document.*

Understanding Rules of Evidence (Cont)

- Computer and digitally stored records must be shown to be **authentic** and **trustworthy**
  - So that it can be admitted into evidence

- Computer-generated records are considered authentic if the program that created the output is functioning correctly. *I.e. No bugs*
  - Usually considered an exception to hearsay rule

- Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic

Understanding Rules of Evidence (Cont)

- When attorneys challenge digital evidence
  - Often they raise the issue of whether computer-generated records were altered or damaged

- One test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records
  - The author of a Microsoft Word document can be identified by using file metadata
    - *May not be easy as records recovered from slack space or unallocated disk space usually don’t identify the author*

Understanding Rules of Evidence (Cont)

- The process of establishing digital evidence’s trustworthiness originated with written documents and the “best evidence rule”

- Best evidence rule states:
  - To prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required
  - Allow a duplicate instead of originals when it is produced by the same impression as the original
    - *No always possible to produce original*

Understanding Rules of Evidence (Cont)

- As long as bit-stream copies of data are created and maintained properly
  - The copies can be admitted in court, although they aren't considered best evidence

- Example of not being able to use original evidence
  - Investigations involving network servers
    - Removing a server from the network to acquire evidence data could cause harm to a business or its owner, who might be an innocent bystander to a crime or civil wrong

Rules of Evidence

- The five properties that evidence must have in order to be useful:
  - **Admissible**
  - **Authentic**
  - **Complete**
  - **Reliable**
  - **Believable**

https://www.avadirect.com

Collecting Evidence in Private-Sector Incident Scenes

- Typically, businesses have inventory databases of computer hardware and software
  - Understand what h/w and s/w help identify the computer forensics tools needed to analyze a policy violation
    - This is also the best way to conduct the analysis

- Corporate policy statement about misuse of digital assets
  - Allows corporate investigators to conduct **covert surveillance** (*surveillance on someone without the person notice it*) with little or no cause
  - And access company systems without a warrant

Collecting Evidence in Private-Sector Incident Scenes (Cont)

- Companies should display a warning banner and publish a policy
  - Stating that they reserve the right to inspect computing assets at will
- Corporate investigators should know under what circumstances they can examine an employee’s computer
  - Every organization must have a well-defined process describing when an investigation can be initiated

Collecting Evidence in Private-Sector Incident Scenes (Cont)

- If a corporate investigator finds that an employee is committing or has committed a crime
    - **Employer** can file a criminal complaint with the police. *As investigator, should immediately report to corporate management*
- Employers are usually interested in enforcing company policy
    - Not seeking out and prosecuting employees
- Corporate investigators are, therefore, primarily concerned with protecting company assets

Collecting Evidence in Private-Sector Incident Scenes (Cont)

- If you discover evidence of a crime during a company policy investigation
  - Determine whether the incident meets the elements of criminal law
  - Inform management of the incident
  - Stop your investigation to make sure you don’t violate Fourth Amendment restrictions on obtaining evidence
  - Work with the corporate attorney on how to respond to a police request for more information

Processing Law Enforcement Crime Scenes (Cont)

- 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 - Reasonable grounds to believe that a particular person has committed a crime, especially to justify making a search or preferring a charge*
  - 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

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

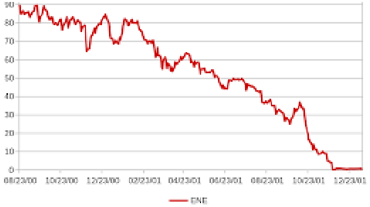
Processing Law Enforcement Crime Scenes (Cont)

- With **probable cause**, a police officer can obtain a search warrant from a judge
  - That authorizes a search and seizure of specific evidence related to the criminal complaint
- 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

https://www.susantperkins.com

Understanding Concepts and Terms Used in Warrants

- **Innocent information**
  - Unrelated information : often included in the information you are looking for. *Need to sort all information to obtain what you need. Sometime amount of data can be up to Terabyte!*
  - *i.e Enron case - by the use of accounting loopholes and poor financial reporting*



- Judges often issue a **limiting phrase** to the warrant
  - Allows the police to separate innocent information from evidence
  - *The warrant must list which items can be seized.*

Understanding Concepts and Terms Used in Warrants (Cont)

- **Plain view doctrine**
  - Objects falling in plain view *(what your eyes can see)* 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
  - Three criteria must be met:
    - Officer is where he or she has a legal right to be
    - Ordinary senses must not be enhanced by advanced technology in any way
    - Any discovery must be by chance

Stu's Views
© Stu All Rights Reserved www.STUS.com
STU
Of course I ate the fish. He was in "plain view". You, of all people, should understand how irresistible that is.

http://4amendment.blogspot.sg/

Understanding Concepts and Terms Used in Warrants (Cont)

- The **plain view doctrine's** applicability in the digital forensics world is being rejected

- Example - In a case where police were searching a computer for evidence related to illegal drug trafficking:
  - If an examiner observes an .avi file and find child pornography, he must get an additional warrant or an expansion of the existing warrant to continue the search for child pornography

https://www.dalesavage.com

Preparing for a Search

- Preparing for a computer search and seizure
  - Probably the most important step in computing investigations
    - *The better you prepare, the smoother your investigation will be*

https://www.dreamstime.com

- To perform these tasks
  - You might need to get answers from the victim and an informant
    - Who 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

Identifying the Nature of the Case

- When you're assigned a digital investigation case
  - Start by identifying the nature of the case
    - Including whether it involves the private or public sector
    - *i.e employee abusing Internet privileges by surfing the Web excessively*

- The nature of the case dictates how you proceed
  - And what types of assets or resources you need to use in the investigation

https://www.flashbackdata.com/

Identifying the Type of OS or Digital Device

- For law enforcement
  - This step might be difficult because the crime scene isn't controlled
    - You 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 OS or device by:-
  - Estimate the size of the drive on the suspect's computer
    - And how many devices to process at the scene
- Determine which OSs and hardware are involved
  - *Microsoft, Linux, UNIX, Macintosh, or mainframe computer*

Determining Whether You Can Seize Computers and Digital Devices

- The type of case and location of the evidence
  - Determine whether you can remove digital evidence
    - *Ideally situation for incident or crime scenes is seizing the computers and taking them to your lab for further processing.*

- Law enforcement investigators need a warrant to remove computers from a crime scene
  - And transport them to a lab

- If removing the computers will irreparably harm a business
  - The computers should not be taken offsite

Determining Whether You Can Seize Computers and Digital Devices

- Additional complications:
  - Files stored offsite that are accessed remotely
  - Availability of cloud storage, which can't be located physically
    - Stored on drives where data from many other subscribers might be stored
- 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

Using Additional Technical Expertise

- Determine whether you need specialized help to process the incident or crime scene
  - *Go look for domain expert, we can't know everything under the sky!*
- You may need to look for specialists in:
  - **OSs**
  - **RAID servers**
  - **Databases**

- Finding the right person can be a challenge
  - *Sometime can be harder than digital forensic!*
- Educate specialists in investigative techniques
  - Prevent evidence damage

Determining the Tools You Need

- Prepare tools using incident and crime scene information
  - *This is after you have gather as much info about the case as possible about the incident or crime scene*

- Create an **initial-response** field kit
  - Should be lightweight and easy to transport

- Create an **extensive-response** field kit
  - Includes all tools you can afford to take to the field
  - When at the scene, extract only those items you need to acquire evidence

Determining the Tools You Need (Cont)

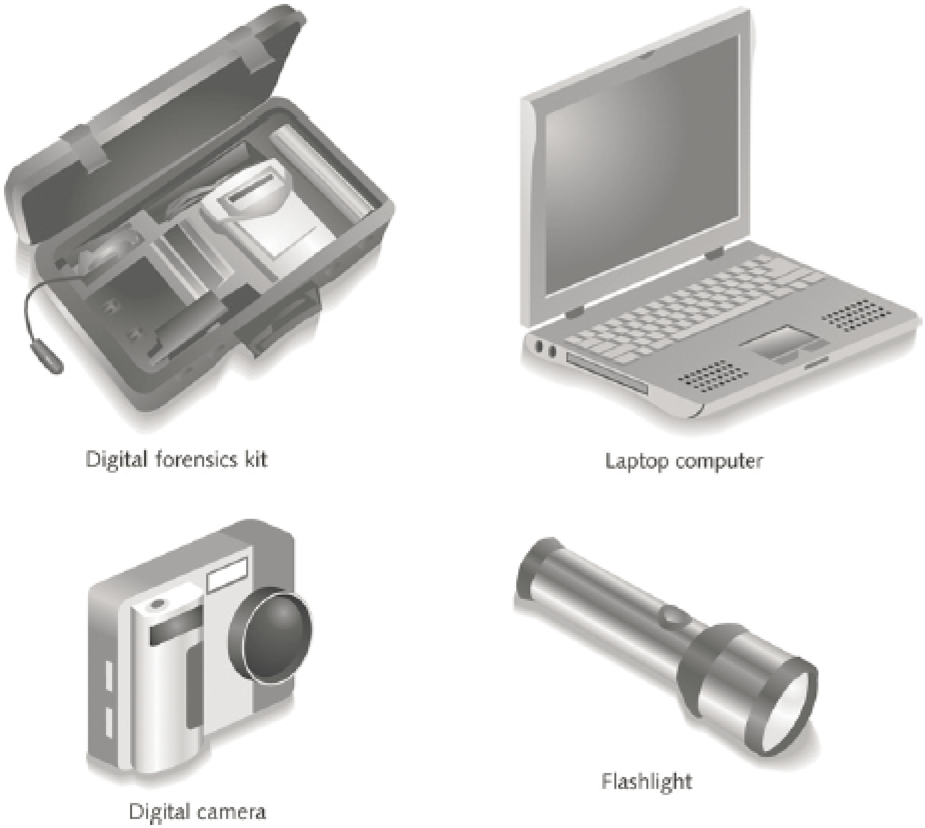


Figure 4-4 Items in an initial-response field kit
© Cengage Learning®

initial-response field kit

Determining the Tools You Need (Cont)

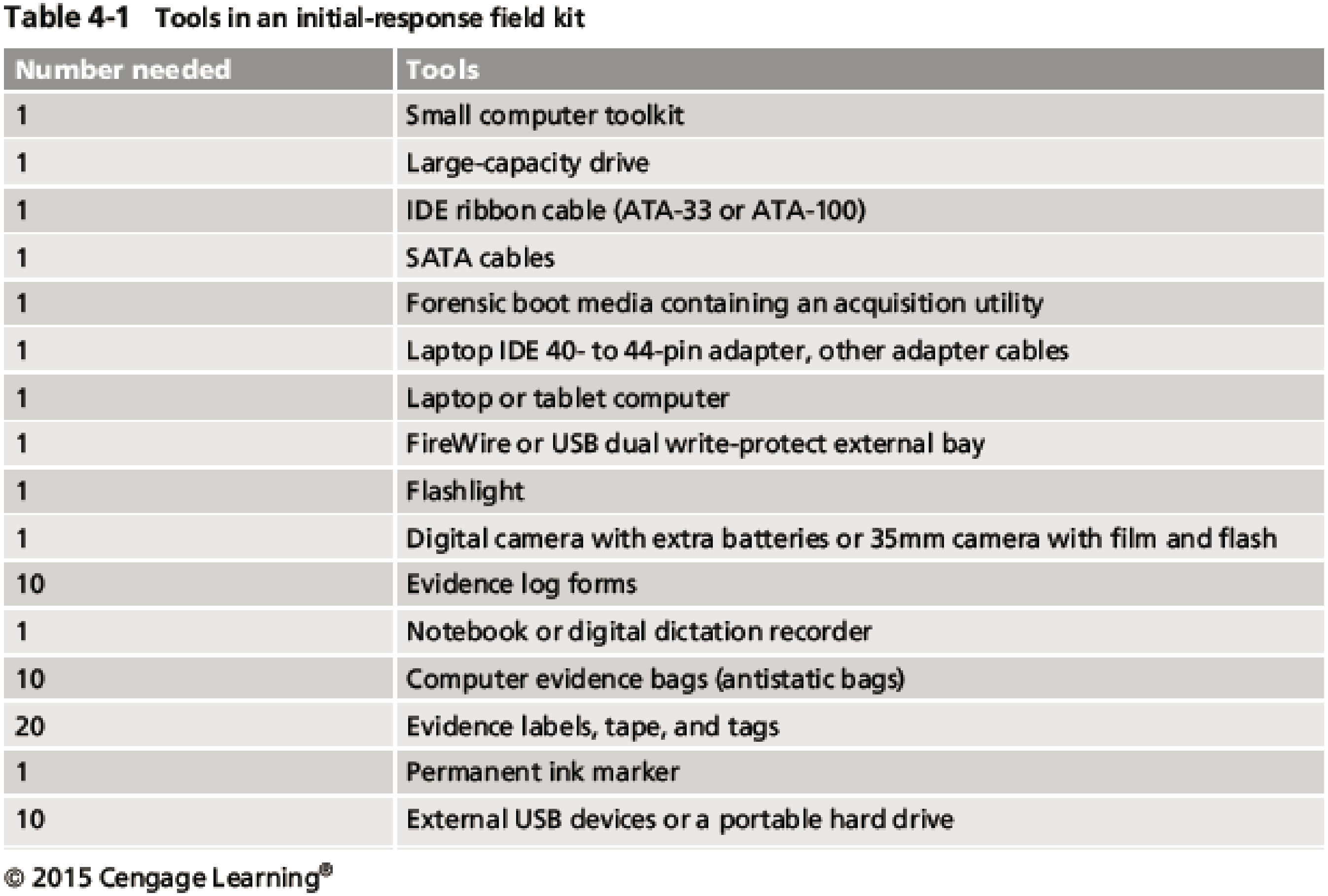


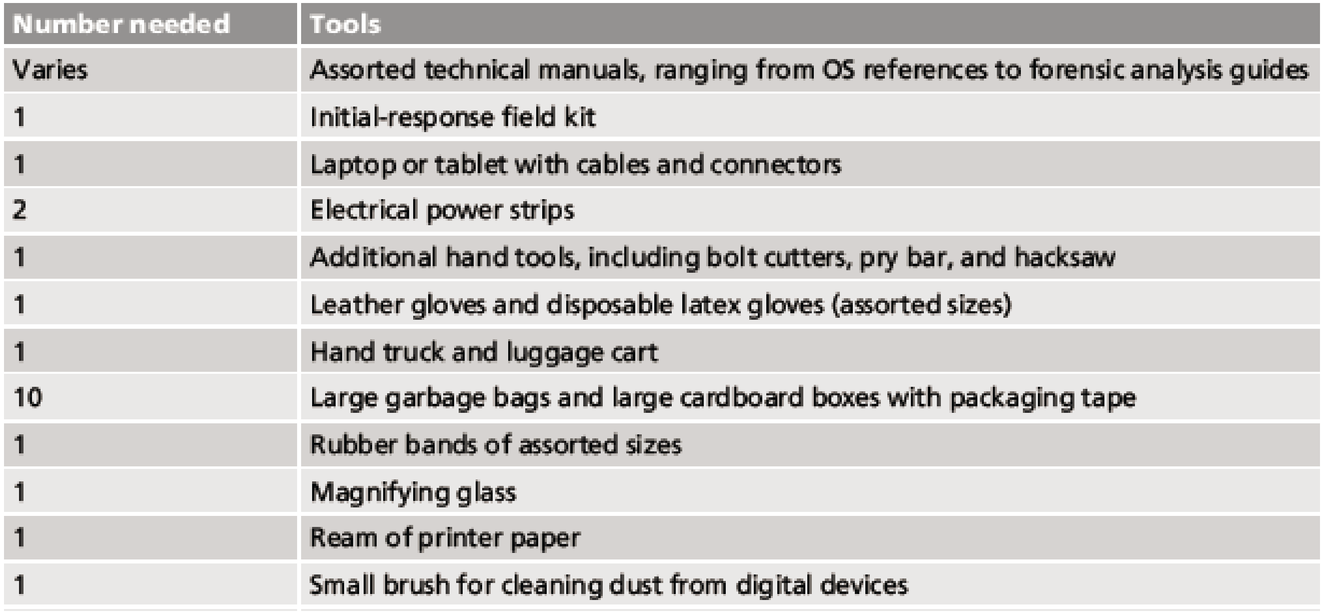
Table 4-1 Tools in an initial-response field kit

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

© 2015 Cengage Learning®

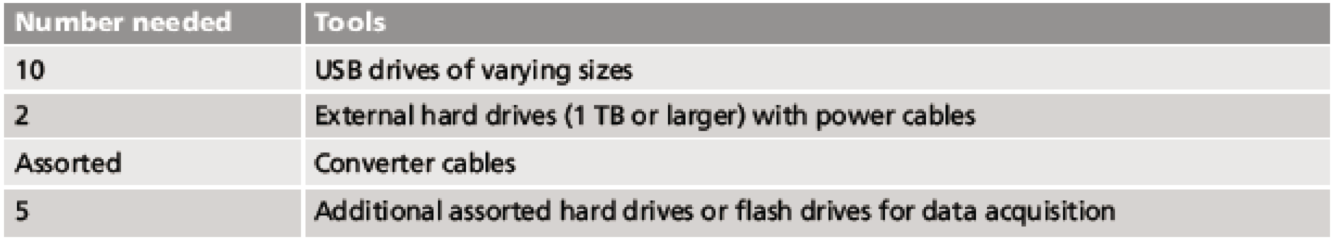
Determining the Tools You Need (Cont)

Table 4-2 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	Laptop or tablet with cables and connectors
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 digital devices

extensive-response field kit



Number needed	Tools
10	USB drives of varying sizes
2	External hard drives (1 TB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives or flash drives for data acquisition

© 2015 Cengage Learning®

http://www.diament.pl/

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?
    - *Data may be lost after machine is powered down*

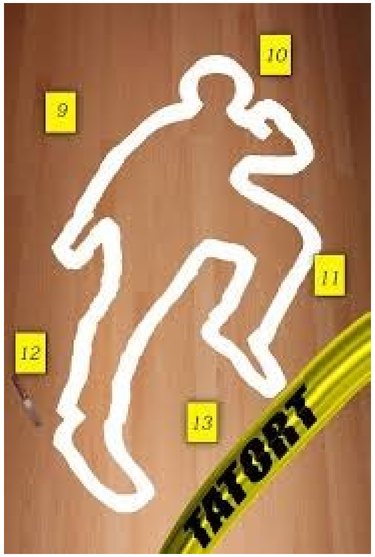
Preparing to Acquire Digital Evidence (Cont)

- *More questions…*

- 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?
    - *Sometime company may not want to employee know investigation is going on*
  - 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
    - Be professional and courteous with onlookers
    - Remove people who are not part of the investigation
  - Take video and still recordings of the area around the computer
    - You want to return belongings to original locations
    - Pay attention to details
  - Sketch the incident or crime scene
  - Check state of computers as soon as possible



Processing an Incident or Crime Scene (Cont)

- More Guidelines…
  - Don't cut electrical power to a running system unless it's an older Windows 9x or MS-DOS system
    - *May lose essential network activity records if power is terminated without a proper shutdown*
  - Save data from current applications as safely as possible
  - Record all active windows or shell sessions
  - Make notes of everything you do when copying data from a live suspect computer
  - Close applications and shut down the computer

Processing an Incident or Crime Scene (Cont)

- More Guidelines…
  - Bag and tag the evidence, following these steps:
    - Assign one person to collect and log all evidence
      - *Minimize the number of people handling evidence to ensure its integrity*
    - 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
      - *For verification and audit purpose*
    - Maintain constant control of the collected evidence and the crime or incident scene

Processing an Incident or Crime Scene (Cont)

- More Guidelines…
  - Look for information related to the investigation
    - Passwords, passphrases, PINs, bank accounts
  - 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

https://www.minitool.com

- **Drawback** of this technique
  - It doesn't recover data in free or slack space

Using a Technical Advisor

- A technical advisor can help:
  - List the tools you need to process the incident or crime scene
  - Guide you about where to locate data and helping you extract log records
    - Or other evidence from large RAID servers
  - Create the search warrant by itemizing what you need for the warrant

http://www.startupspecialistnetwork.com

Using a Technical Advisor (Cont)

- Responsibilities
  - Know all aspects of the seized system
  - Direct investigator handling sensitive material
  - Help secure the scene
  - Help document the planning strategy
  - Conduct ad hoc trainings
    - *On the technologies and components being seized and searched*
  - Document activities
  - Help conduct the search and seizure

"From the looks of you, the problem probably *is* with your set."

https://www.cartoonstock.com

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

- Your goal is to be able to reproduce the same results
  - When you or another investigator repeat the steps you took to collect evidence, *results should be the same!*

- 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!!

https://techubber.blogspot.com

- 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

- The **media** you use to store digital evidence usually depends on how long you need to keep it

- CDs, DVDs, DVD-Rs, DVD+Rs, or DVD-RWs
  - The ideal media
  - Capacity: up to 17 GB
  - Lifespan: 2 to 5 years

https://hubpages.com

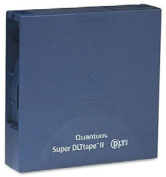
- Magnetic tapes - 4-mm DAT
  - Capacity: 40 to 72 GB
  - Lifespan: 30 years
  - Costs: drive: $400 to $800; tape: $40

Storing Digital Evidence (Cont)

- Super Digital Linear Tape (Super-DLT or SDLT)
  - Specifically designed for large RAID data backups
  - Can store more than 1 TB of data

http://www.unylogix.com

- Smaller external SDLT drives can connect to a workstation through a SCSI card

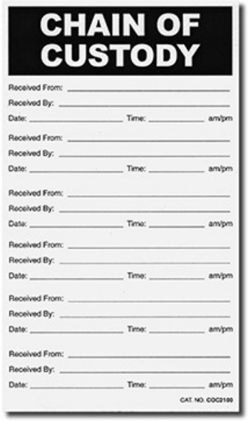


https://www.huntoffice.ie

- Don’t rely on one media storage method to preserve your evidence
  - Make two copies of every image to prevent data loss
  - Use different tools to create the two images

Evidence Retention and Media Storage Needs

- To help maintain the chain of custody (*paper trail that records the sequence of **custody***) for digital evidence
  - Restrict access to lab and evidence storage area



CHAIN OF CUSTODY

Received From: __________
Received By: __________
Date: ________ Time: ______ am/pm

Received From: __________
Received By: __________
Date: ________ Time: ______ am/pm

Received From: __________
Received By: __________
Date: ________ Time: ______ am/pm

Received From: __________
Received By: __________
Date: ________ Time: ______ am/pm

Received From: __________
Received By: __________
Date: ________ Time: ______ am/pm

Received From: __________
Received By: __________
Date: ________ Time: ______ am/pm

CAT. NO. COC2199

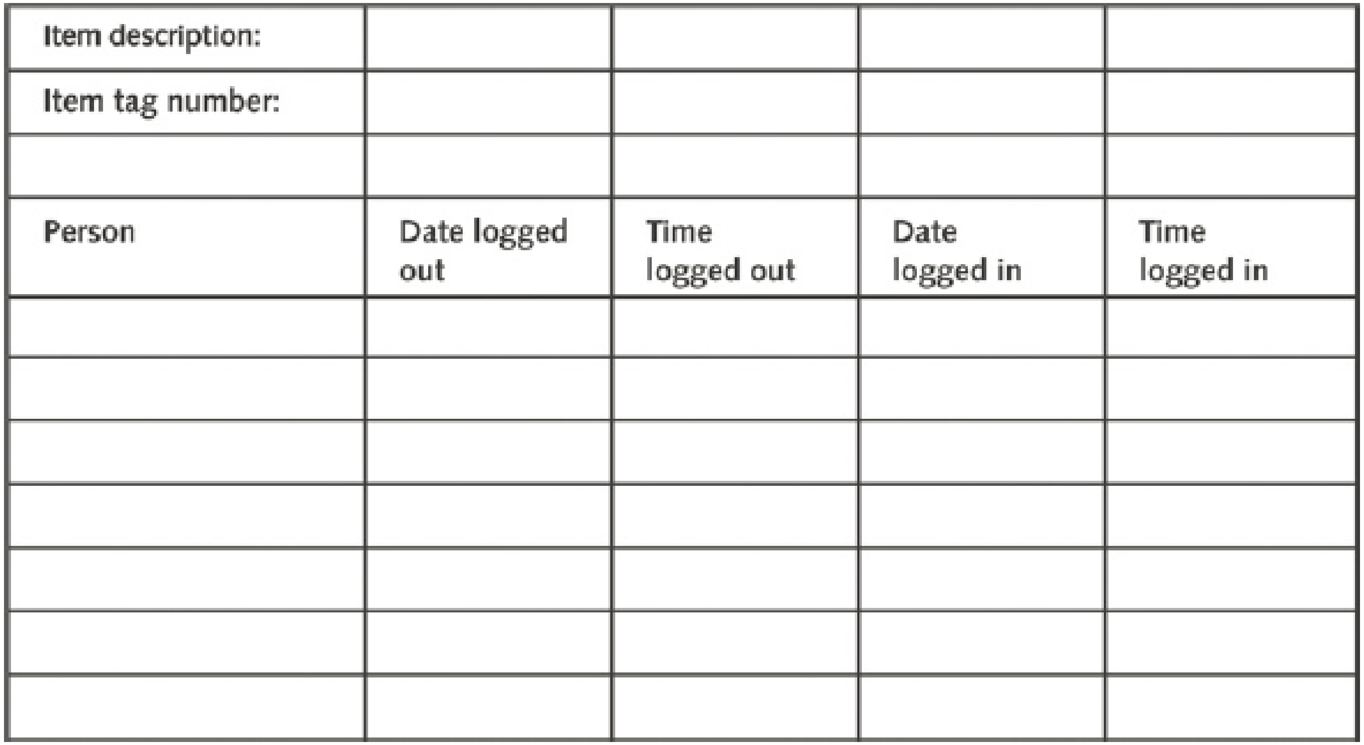
http://www.sirchie.com

- 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

Evidence Retention and Media Storage Needs (Cont)

The evidence custody form should contain an entry for every person who handles the evidence



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

Figure 4-5 A sample log file
© Cengage Learning®

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

Obtaining a Digital Hash

- **Cyclic Redundancy Check (CRC)**
  - Mathematical algorithm that determines whether a file’s contents have changed
  - 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 hash value, which can be used to verify a file or drive has not been tampered with

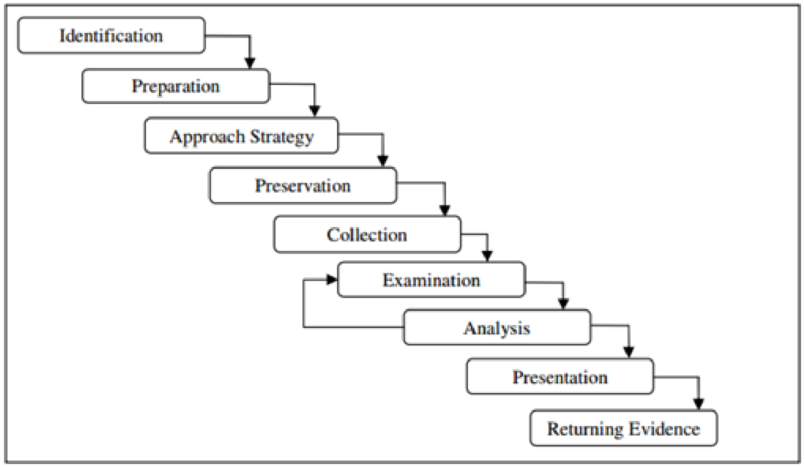
Obtaining a Digital Hash (Cont)

- 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)**
    - *Not secure now!!!*

Reviewing a Case

- General tasks you perform in any computer forensics case:
  - Identify the case requirements
  - Plan your investigation
  - Conduct the investigation
  - Complete the case report
  - Critique the case



http://resources.infosecinstitute.com

Sample Civil Investigation

- Most cases in the corporate environment are considered **low-level investigations**
  - Or noncriminal cases

- Common activities and practices
  - Recover specific evidence
    - Suspect’s Outlook e-mail folder (PST file)
  - **Covert surveillance**
    - Its use must be well defined in the company policy
    - Risk of civil or criminal liability
  - **Sniffing** tools for data transmissions
    - *Wireshark?*

Sample Criminal Investigation (Cont)

- Computer crimes examples
  - Fraud
  - Check fraud
  - Homicides
  - *Others…*

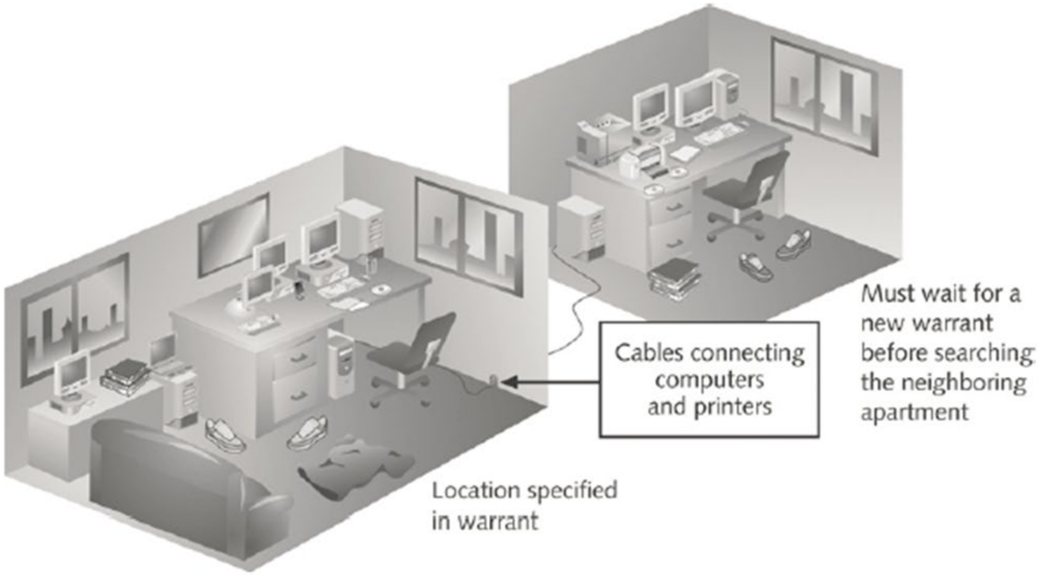

Must wait for a new warrant before searching the neighboring apartment
Cables connecting computers and printers
Location specified in warrant

Figure 4-7 Search warrant limits
© Cengage Learning®

- Need a warrant to start seizing evidence
  - Limit searching area

Summary

- Digital evidence is anything stored or transmitted on electronic or optical media
- In the private sector, incident scene is often in a contained and controlled area
- Companies should publish the right to inspect computer assets policy
- Private and public sectors follow same computing investigation rules
- Criminal cases
  - *Report to company management*
  - Require warrants

Summary (Cont)

- Protect your safety and health as well as the integrity of the evidence
- Follow guidelines when processing an incident or crime scene
  - Security perimeter / *Scope*
  - Video recording
- As you collect digital evidence, guard against physically destroying or contaminating it
- Forensic hash values verify that data or storage media have not been altered

Summary (Cont)

- To analyze computer forensics data, learn to use more than one vendor tool
- You must handle all evidence the same way every time you handle it.
- After you determine that an incident scene has digital evidence, identify the digital information or artifacts that can be used as evidence