

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 4

Processing Crime and Incident Scenes





Objectives (1 of 2)

- 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 (2 of 2)

- 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 (1 of 2)

- **Digital evidence**

- Can be any information stored or transmitted in digital form
- 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



Identifying Digital Evidence (2 of 2)

- 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 while processing a criminal or incident scene must be done systematically



Understanding Rules of Evidence (1 of 7)

- Consistent practices help verify your work and enhance your credibility
- Comply with your state's rules of evidence or with the Federal Rules of 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 (2 of 7)

- Data you discover from a forensic examination falls under your state's rules of evidence
 - Or the Federal Rules of Evidence (FRE)
- 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
- Another concern when dealing with digital records is the concept of hearsay
 - Hearsay is secondhand or indirect evidence



Understanding Rules of Evidence (3 of 7)

- Business-record exception
 - Allows “records of regularly conducted activity,” such as business memos, reports, records, or data compilations
- Business records are authenticated by verifying that they were created
 - “at or near the time by, or from information transmitted by, a person with knowledge”
- Business records are admissible
 - “if the record was kept in the course of a regularly conducted business activity, and it was the regular practice of that business activity to make the record”
- Computer records are usually divided into:
 - **Computer-generated records**
 - **Computer-stored records**



Understanding Rules of Evidence (4 of 7)

- Computer-generated and computer-stored records must be shown to be authentic and trustworthy
 - To be admitted into evidence
- Computer-generated records are considered authentic if the program that created the output is functioning correctly
 - Usually considered an exception to hearsay rule
- Collecting evidence according to approved steps of evidence control helps ensure that the computer evidence is authentic



Understanding Rules of Evidence (5 of 7)

- 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
- Follow the steps starting on page 150 of the text to see how to identify file metadata



Understanding Rules of Evidence (6 of 7)

- 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 file is required
- Federal Rules of Evidence
 - Allow a duplicate instead of originals when it is produced by the same impression as the original



Understanding Rules of Evidence (7 of 7)

- 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



Collecting Evidence in Private-Sector Incident Scenes (1 of 6)

- Private-sector organizations include:
 - Small to medium businesses, large corporations, and non-government organizations (NGOs)
- Non-government organizations (NGO) must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws
 - And make certain documents available as public records
- FOIA allows citizens to request copies of public documents created by federal agencies



Collecting Evidence in Private-Sector Incident Scenes (2 of 6)

- A special category of private-sector businesses includes ISPs and other communication companies
- ISPs can investigate computer abuse committed by their employees, but not by customers
 - Except for activities that are deemed to create an emergency situation
- Investigating and controlling computer incident scenes in the corporate environment
 - Much easier than in crime scenes
 - Incident scene is often a workplace



Collecting Evidence in Private-Sector Incident Scenes (3 of 6)

- Typically, businesses have inventory databases of computer hardware and software
 - Help identify the computer forensics tools needed to analyze a policy violation
 - And the best way to conduct the analysis
- Corporate policy statement about misuse of digital assets
 - Allows corporate investigators to conduct covert surveillance with little or no cause
 - And access company systems without a warrant



Collecting Evidence in Private-Sector Incident Scenes (4 of 6)

- Companies should display a warning banner and publish a policy
 - Stating that they reserve the right to inspect computing assets at will
- Private-sector 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 (5 of 6)

- If a private-sector investigator finds that an employee is committing or has committed a crime
 - Employer can file a criminal complaint with the police
- Employers are usually interested in enforcing company policy
 - Not seeking out and prosecuting employees
- Private-sector investigators are mainly concerned with protecting company assets



Collecting Evidence in Private-Sector Incident Scenes (6 of 6)

- 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

(1 of 2)

- 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**
 - 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



Processing Law Enforcement Crime Scenes

(2 of 2)

- 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



Understanding Concepts and Terms Used in Warrants (1 of 3)

- **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 (2 of 3)

- **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 into 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



Understanding Concepts and Terms Used in Warrants (3 of 3)

- 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



Preparing for a Search

- Preparing for a computer search and seizure
 - Probably the most important step in digital investigations
- 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
- 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 OS or Digital Device

- For law enforcement
 - This step might be difficult because the crime scene isn't controlled
- If you can identify the OS or device
 - 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



Determining Whether You Can Seize Computers and Digital Devices (1 of 2)

- The type of case and location of the evidence
 - Determine whether you can remove digital evidence
- 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 (2 of 2)

- 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



Getting a Detailed Description of the Location

- Get as much information as you can about the location of a digital crime
- Identify potential hazards
 - Interact with your **HAZMAT** (hazardous materials) team
- HAZMAT guidelines
 - Put the target drive in a special HAZMAT bag
 - HAZMAT technician can decontaminate the bag
 - Check for high temperatures



Determining Who Is in Charge

- Private-sector computing investigations
 - Usually require only one person to respond to an incident
- Law enforcement agencies
 - Typically handle large-scale investigations
- Designate lead investigators in large-scale investigations
 - Anyone assigned to the scene should cooperate with the designated leader to ensure the team addresses all details when collecting evidence



Using Additional Technical Expertise

- Determine whether you need specialized help to process the incident or crime scene
- You may need to look for specialists in:
 - 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 (1 of 5)

- Prepare tools using incident and crime scene information
- 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



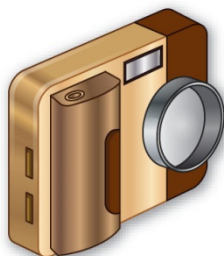
Determining the Tools You Need (2 of 5)



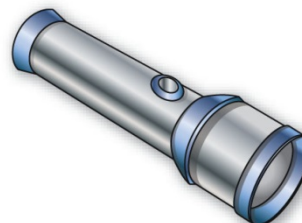
Digital forensics kit



Laptop computer



Digital camera



Flashlight

Figure 4-4 Items in an initial-response field kit



Determining the Tools You Need (3 of 5)

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

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	Set of Japanese Industrial Standard (JIS) screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wrist bands
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



Determining the Tools You Need (4 of 5)

Table 4-1 Tools in an initial-response field kit (*continued*)

Number needed	Tools
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	USB drives (or a portable hard drive)



Determining the Tools You Need (5 of 5)

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	Set of JIS screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wristbands
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
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 USB drives for data acquisition



Preparing the Investigation Team

- Before initiating the search:
 - Review facts, plans, and objectives with the investigation team you have assembled
- Goal of scene processing
 - To collect and secure digital evidence
- Digital evidence is volatile
 - Develop skills to assess facts quickly
- Slow response can cause digital evidence to be lost



Securing a Computer Incident or Crime Scene (1 of 2)

- Goals
 - Preserve the evidence
 - Keep information confidential
- Define a secure perimeter
 - Use yellow barrier tape
 - Legal authority for a corporate incident includes trespassing violations
 - For a crime scene, it includes obstructing justice or failing to comply with a police officer



Securing a Computer Incident or Crime Scene (2 of 2)

- **Professional curiosity** can destroy evidence
 - Involves police officers and other professionals who aren't part of the crime scene processing team
- **Automated Fingerprint Identification System (AFIS)**
 - A computerized system for identifying fingerprints that's connected to a central database
 - Used to identify criminal suspects and review thousands of fingerprint samples at high speed
- Police can take elimination prints of everyone who had access to the crime scene



Seizing Digital Evidence at the Scene

- Law enforcement can seize evidence
 - With a proper warrant
- Corporate investigators might have the authority only to make an image of the suspect's drive
- When seizing digital evidence in criminal investigations
 - Follow U.S. DOJ standards for seizing digital data
- Civil investigations follow same rules
- Consult with your attorney for extra guidelines



Preparing to Acquire Digital Evidence (1 of 2)

- 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 (2 of 2)

- Ask your supervisor or senior forensics examiner in your organization the following questions (cont'd):
 - 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 (1 of 4)

- 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
 - Pay attention to details
 - Sketch the incident or crime scene
 - Check state of computers as soon as possible



Processing an Incident or Crime Scene (2 of 4)

- Guidelines (cont'd)
 - Don't cut electrical power to a running system unless it's an older Windows 9x or MS-DOS system
 - 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 (3 of 4)

- Guidelines (cont'd)
 - 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 (4 of 4)

- Guidelines (cont'd)
 - Look for information related to the investigation
 - Passwords, passphrases, PINs, bank accounts
 - Collect as much personal information as possible about the suspect or victim
 - 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 (1 of 2)

- 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



Using a Technical Advisor (2 of 2)

- 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
 - 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
- Your 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 or a SAN
 - 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 (1 of 2)

- The media you use to store digital evidence usually depends on how long you need to keep it
- CDs, DVDs
 - Lifespan: 2 to 5 years
- Solid-state USB drives
 - Optimum choice
 - More durable
- Magnetic tapes - 4-mm DAT
 - Capacity: 40 to 72 GB
 - Slow read and write speeds
 - Lifespan: 30 years



Storing Digital Evidence (2 of 2)

- Super Digital Linear Tape (Super-DLT or SDLT)
 - Specifically designed for large RAID data backups
 - Can store more than 1 TB of data
- Smaller external SDLT drives can connect to a workstation through a SCSI card
- 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 (1 of 2)

- 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



Evidence Retention and Media Storage Needs (2 of 2)

Evidence Activity Log

This form is for tracking access by examiners of evidence items. Use one form for each piece of evidence.

Case Number:				
Evidence Number:				
Evidence Description:				
Examiner's Name	Date Logged Out	Time	Date Logged In	Time

Figure 4-5 A sample log file



Documenting Evidence (1 of 2)

- 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 (2 of 2)

- 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 (1 of 4)

- **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 (2 of 4)

- 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)**
 - Another hashing algorithm
 - Developed by the **National Institute of Standards and Technology (NIST)**



Obtaining a Digital Hash (3 of 4)

- In both MD5 and SHA-1, collisions have occurred
- Most digital 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



Obtaining a Digital Hash (4 of 4)

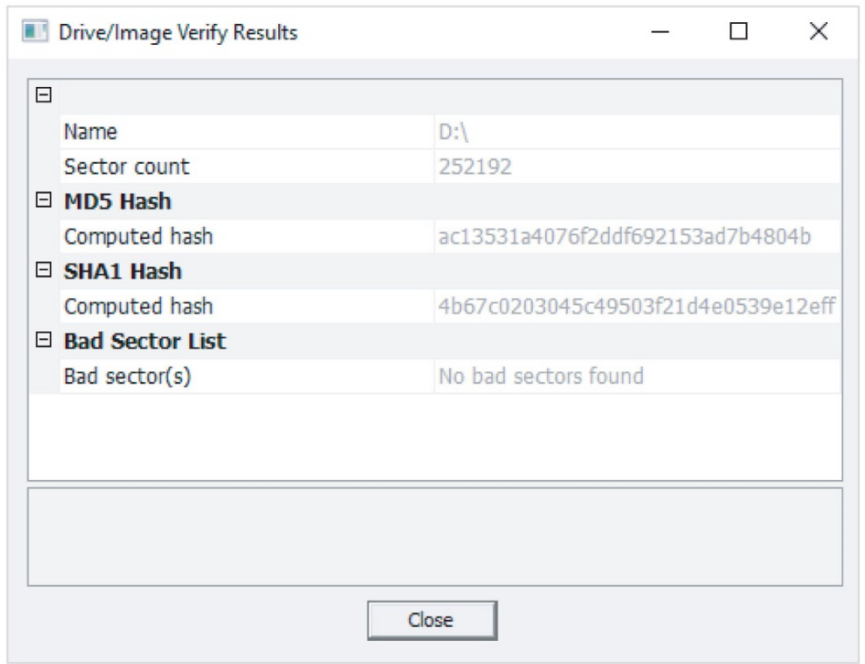


Figure 4-6 Using FTK Imager Lite to verify hash values

Source: AccessData Group, Inc.



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



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



An example of a Criminal Investigation (1 of 2)

- Computer crimes examples
 - Fraud
 - Check fraud
 - Homicides
- Need a warrant to start seizing evidence
 - Limit searching area



An example of a Criminal Investigation (2 of 2)

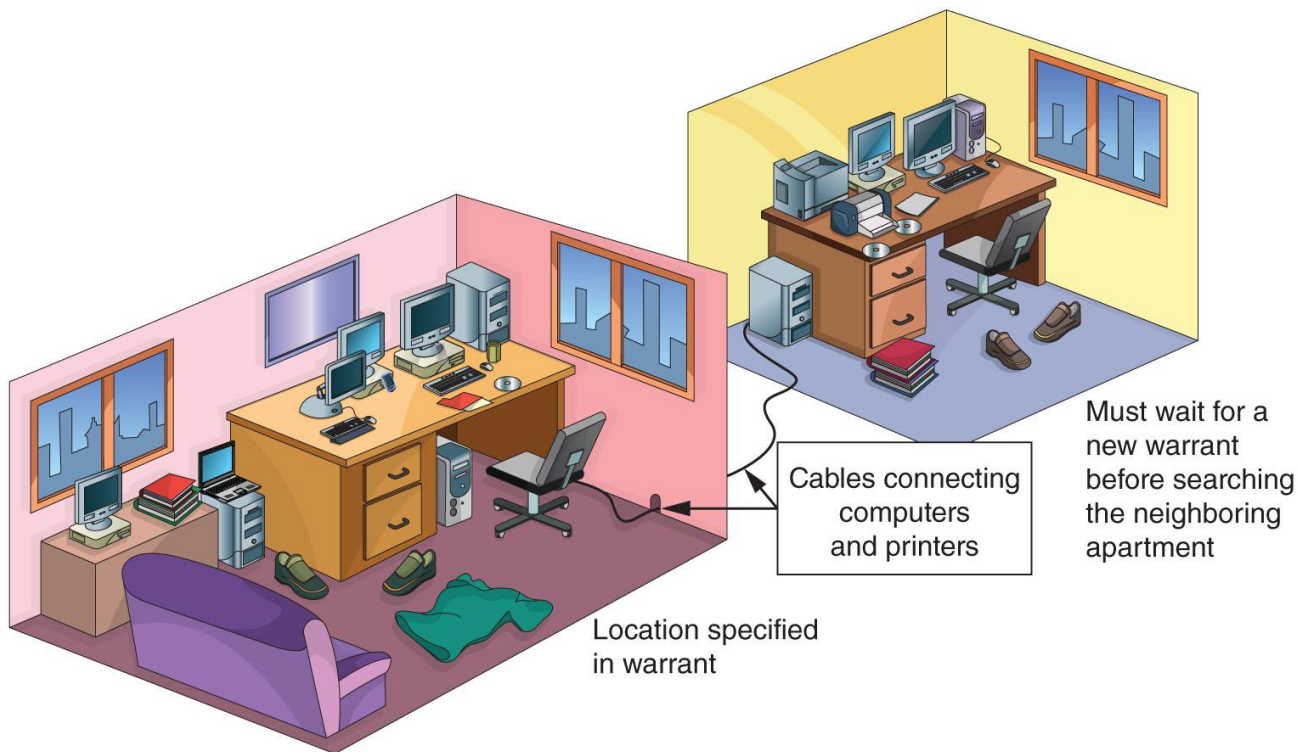


Figure 4-7 Search warrant limits



Reviewing Background Information for a Case

- Throughout the book, you use data files from the hypothetical M57 Patents case
 - A startup company doing art patent searches
 - A computer sold on Craigslist was discovered to contain “kitty” porn
 - It was traced back to M57 Patents
 - An employee is suspected of downloading the porn



Planning the Investigation

- Background information on the case
 - Main players:
 - Pat McGoo, CEO
 - Terry, the IT person
 - Jo and Charlie, the patent researchers
- Police made forensic copies of:
 - The image of the computer sold on Craigslist
 - Images of five other machines found at M57
 - Images of four USB drives found at M57
 - RAM from the imaged machines
 - Network data from the M57 Patents servers



Conducting the Investigation: Acquiring Evidence with OSForensics

- Follow the steps outlined on pages 182-186 of the text
 - To use OSForensics to analyze an image file



Summary (1 of 3)

- 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
 - Require warrants



Summary (2 of 3)

- Protect your safety and health as well as the integrity of the evidence
- Follow guidelines when processing an incident or crime scene
 - Security perimeter
 - 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 (3 of 3)

- 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