MIS 5208 – Lecture 07 – Investigating Theft Acts (Part 2)

Caswell M. Anderson, CISA, CRISC
Caswell.Anderson@temple.edu

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 an Incident or Crime Scene

- 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
- 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
  - Require less documentation though
- Consult with your attorney for extra guidelines

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 (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

- 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

- 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

- 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

- Guidelines (cont’d)
    - 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
- 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

Using a Technical Advisor

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

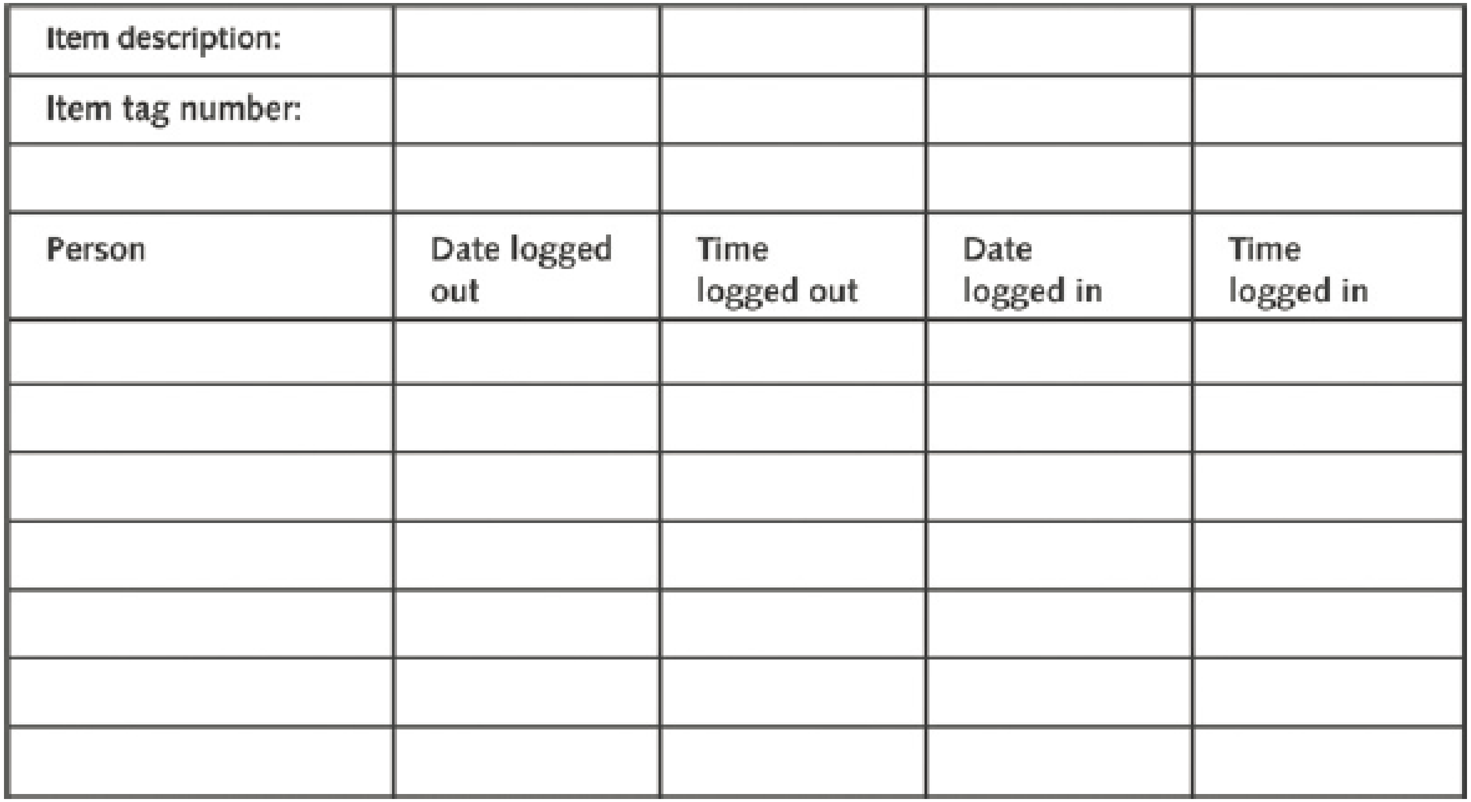
Storing Digital Evidence

- 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

- 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 / Media Storage Needs



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®

TEMPLE
UNIVERSITY

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
  - 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

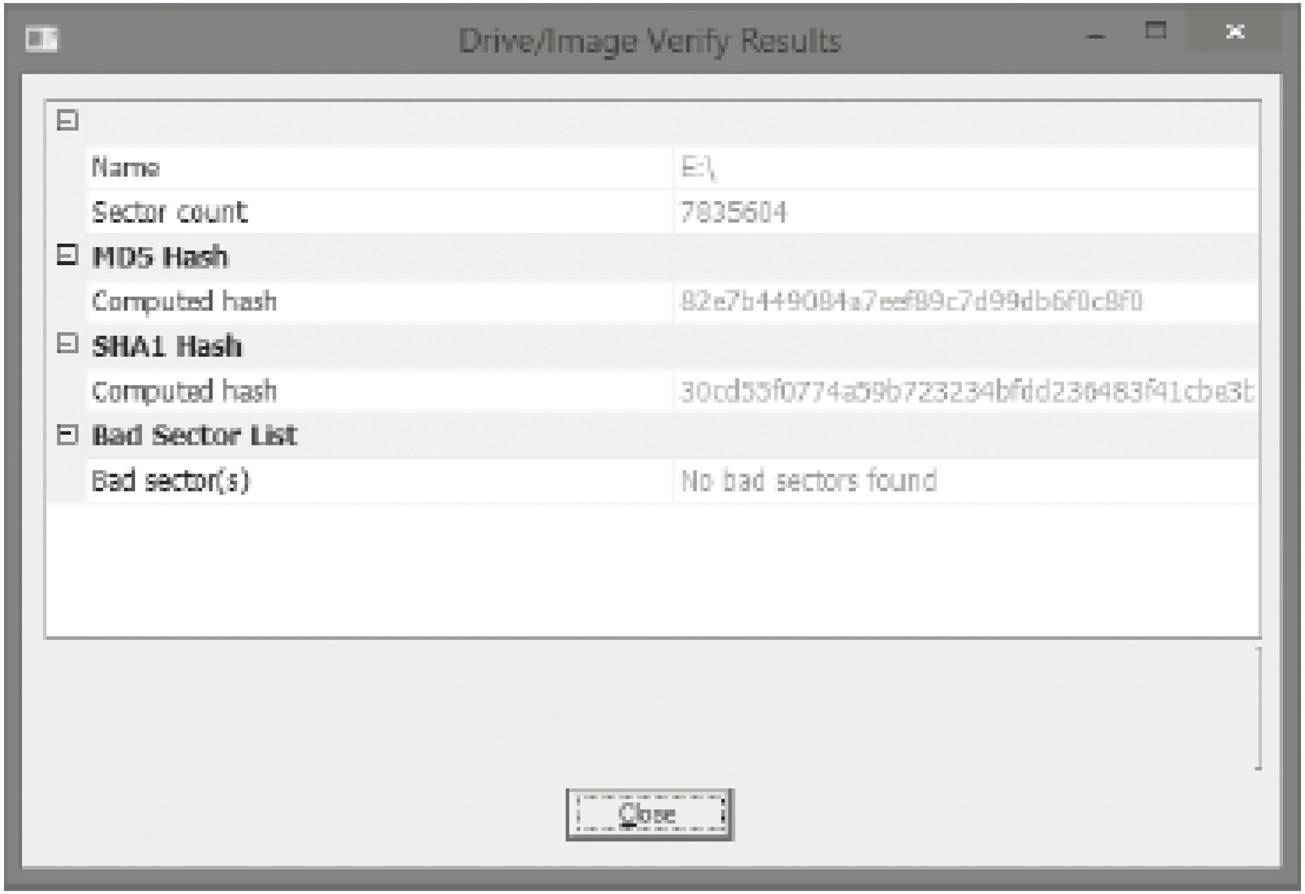
Obtaining a Digital Hash

- 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 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



Drive/Image Verify Results

⊟	
Name	E:\
Sector count	7835604
⊟ **MD5 Hash**	
Computed hash	82e7b449084a7eef89c7d99db6f0c8f0
⊟ **SHA1 Hash**	
Computed hash	30cd55f0774a59b723234bfdd236483f41cbe3b
⊟ **Bad Sector List**	
Bad sector(s)	No bad sectors found

Figure 4-6 Using FTK Imager to verify hash values

Courtesy of AccessData Group, Inc.

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

Sample Criminal Investigation

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

Sample Criminal Investigation

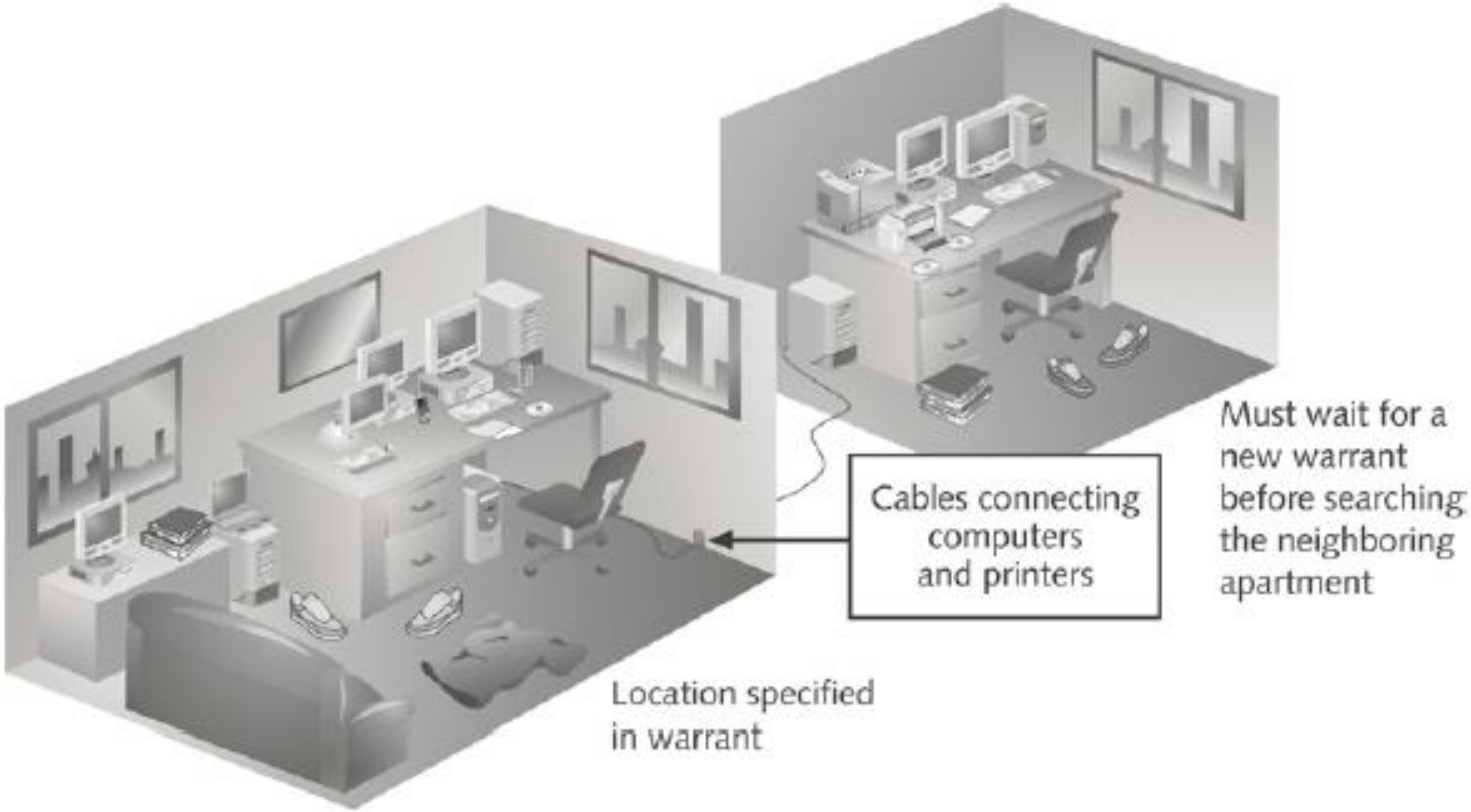

Must wait for a new warrant before searching the neighboring apartment
Cables connecting computers and printers
Location specified in warrant

Figure 4-7 Search warrant limits

© Cengage Learning®

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
  - Require warrants

Summary

- 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

- 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

Thank you