Processing Scenes

CSC 388

Objectives

- Explore how to collect and control evidence
- Review collecting and validating hashes
- Demonstrate network acquisitions

Identification of Digital Evidence

Introduction

- **Digital Evidence:** any information stored or transmitted in digital form
  - US courts accept digital evidence as physical evidence (a tangible object)
- Standards set by numerous groups including the **Scientific Working Group on Digital Evidence (SWGDE)**

Tasks to Perform

- 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

Rules of Evidence

- 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
- Remember: it may be easier to accidentally damage or modify digital evidence than other types of evidence

Hearsay

- **Hearsay:** information received from other people that one cannot adequately substantiate; rumor/secondhand info

- Existence of files or digital evidence can’t be disputed, but the contents require testimony or corroborating evidence

Hearsay Exceptions

- 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 Generated v. Computer Stored Records

- **Computer Generated Records:** data maintained by the system (logs, etc.)
  - Program that creates the records must be functioning correctly for records to be accepted into evidence

- **Computer Stored Records:** data that a person creates and stores on a computer or other device (documents, etc.)
  - Stored records accepted into evidence if they qualify for a hearsay exception

Challenging Digital Evidence

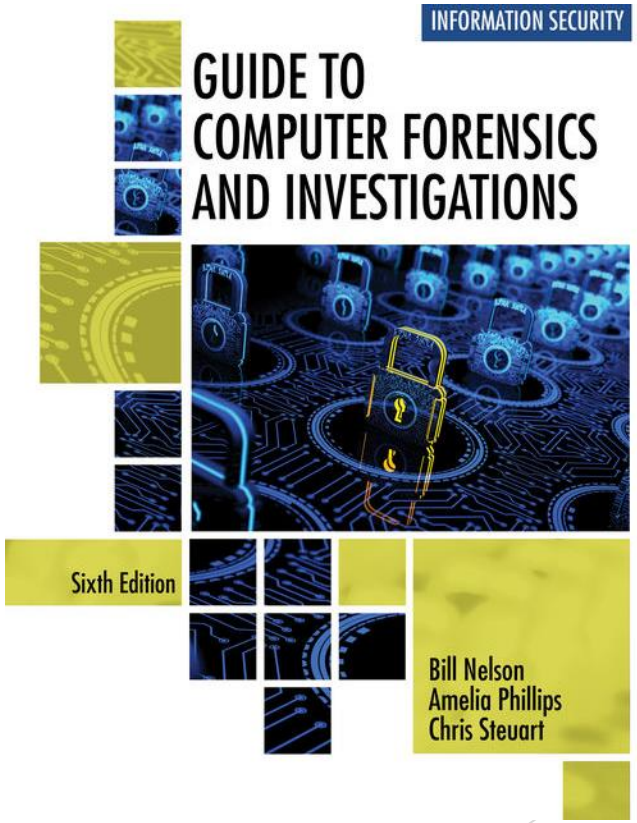
- Attorneys can raise the issue of whether a computer-generated record was altered or damaged
  - Defend position by showing who created the file and when using metadata (there's a task from the book on page 150)

Best Evidence

- **Best Evidence:** to prove the content of a written document, recording, or photograph, ordinarily the original file is required
  - This also applies to digital evidence
  - There may be cases when you must prepare to explain why best evidence isn't immediately available (returned to user & changed, failed hardware, etc.)
  - Federal Rules of Evidence allows duplicate instead of originals when produced by the same impression as original

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Incident Scene Types

Corporate v. Law Enforcement

Business Types & Considerations

- Small to medium businesses
- Corporations
- Non-government organizations (that are funded by the government)
  - May have to comply with FOIA
- ISPs can monitor their employees but not customers unless permitted under law for emergency situations

Corporate Scenes v. Crime Scenes

- Workplace entry/exit controlled by the business
- Inventory databases (hopefully) note what is present
- Policies and roles may designate what evidence is to be collected
  - Is the user a developer? Do you force a certain web browser? Etc.

Corporate Policy

- Policies and warning banners must be in place to
  - alert users that there is no privacy expected otherwise other rules (such as the 4th amendment) apply
  - determine who can initiate an investigation
  - formalize communication with law enforcement as necessary

- If a crime is found
  - Inform management & legal counsel
  - Stop investigation outside bounds of original inquiry
  - Work with counsel to field requests from law enforcement

Law Enforcement Scenes

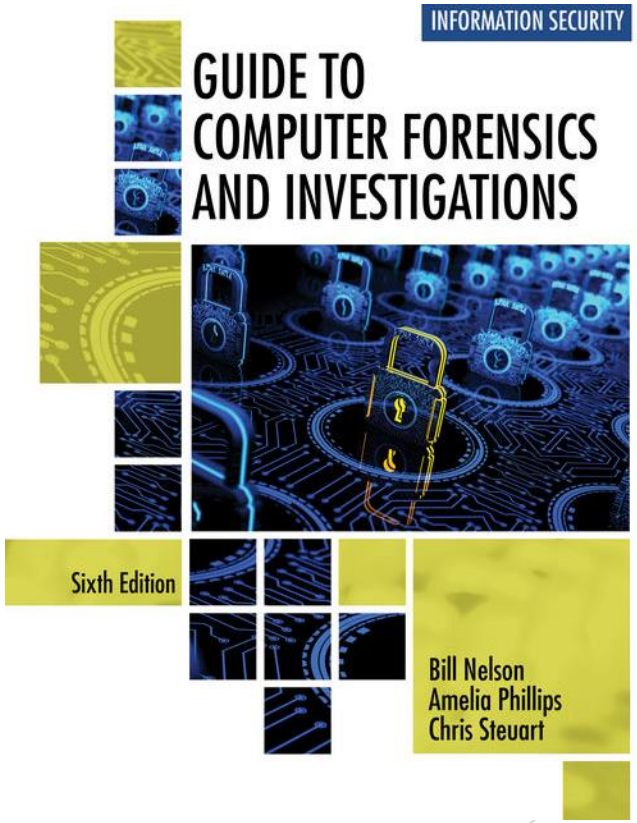
- Be familiar with the rules of search and seizure
  - You'll likely have a mentor or point of contact for a particular investigation
- **Probable cause:** standard specifying whether law enforcement has the right to make an arrest, conduct a search, or obtain a warrant
  - Required to search and seize evidence
- **Search Warrant:** authorizes a search and seizure of specific evidence related to a criminal complaint
  - Broader wording is often allowed for digital evidence (ex: all storage media, all computers, etc.)
  - 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

Warrant & Legal Terms

- **Innocent Information:** Unrelated to case; included with what's recovered
- **Limiting Phrase:** describes how to separate innocent information from evidence
- **Plain View Doctrine:** objects an officer can see from a position they're allowed to be are subject to seizure without a warrant if:
  - Officer is where he or she has a legal right to be
  - Ordinary senses aren't enhanced (no binoculars, etc.)
  - Any discovery must be by chance
- Plain view is often rejected for digital forensics

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Preparing to Respond

First Steps

- Work with LE or your corporate contact to determine facts of the case
  - Always assume there will be more, slower devices than you're informed of
- Gather your kit (will be more difficult for LE)
  - How many devices?
  - What kind of devices? OS? Size?

Seizure Preparation

- Can you take the evidence?
  - Certain cases are focused on gathering single artifacts
  - Others require capturing the original evidence and providing a copy back to the user
- Irreparable harm to a business shouldn't be done
  - Case examples in text
- Are there remote/cloud file shares?

Location Notes

- Document the entire scene of the incident
  - You have the duration of your analysis at the lab to review the digital evidence, you likely only have limited access to the incident scene
  - Bring a notebook & camera
- Scene Safety
  - What hazards are there to be aware of?
- Designate someone to lead the forensics collection effort

Additional Technical Expertise

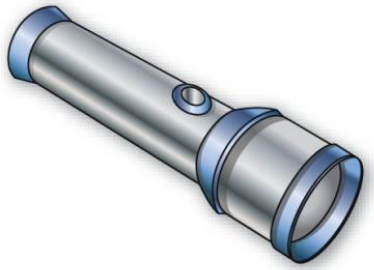
- You may need specialized help in varied
  - OSs
  - Storage devices
  - Applications
  - Databases
- If using external help untrained in forensics, teach the basics and observe collection when practical

Your Kit

Digital forensics kit

Laptop computer

Digital camera



Flashlight

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

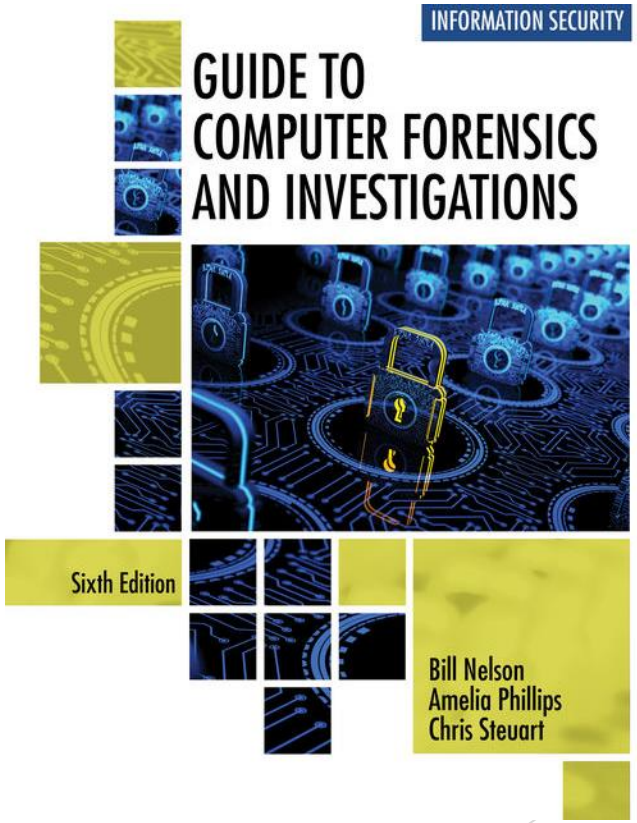
- **Initial response kit:** lightweight & easy to transport; practical for collecting 1 or 2 systems
- **Extensive response kit:** includes everything you can afford to bring with you

Last Steps

- Bring together the team you've gathered (LE/system experts/analysts/etc.)
  - Review the facts and plan
  - Clarify any questions and execution steps

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Processing a Scene

Securing the Scene

- Goals
  - Preserve evidence
  - Keep information confidential
- Perimeter security
  - Corporate
    - Security: watchful eyes or a locked door during acquisition
    - Enforcement: trespassing violations
  - Criminal
    - Security: Yellow barrier tape & LE
    - Enforcement: obstruction or failure to comply

Securing the Scene (Cont.)

- Beware of **professional curiosity**
- Example: found fingerprints

Processing the Scene

- Document your activities using your standard forms or a journal
  - Take photos and video when appropriate
  - Measure items and sketch to include with your report and photos
  - Inspect state of the computing devices as soon as practical
- Maintain scene security while being courteous

Processing the Scene (Cont.)

- Running systems
  - Photograph and log the state (screenshot if allowed by your SOPs)
  - Capture memory
  - If encrypted, capture logical image
  - Save data from running applications
  - Make notes of **everything** you do to the running system
  - Shutdown safely (unless your SOPs suggest pulling power)

Processing the Scene (Cont.)

- Proximity search
  - Near the system seek passwords, PINs, other account information
  - Collect any relevant documentation to the systems & media collected

RAID

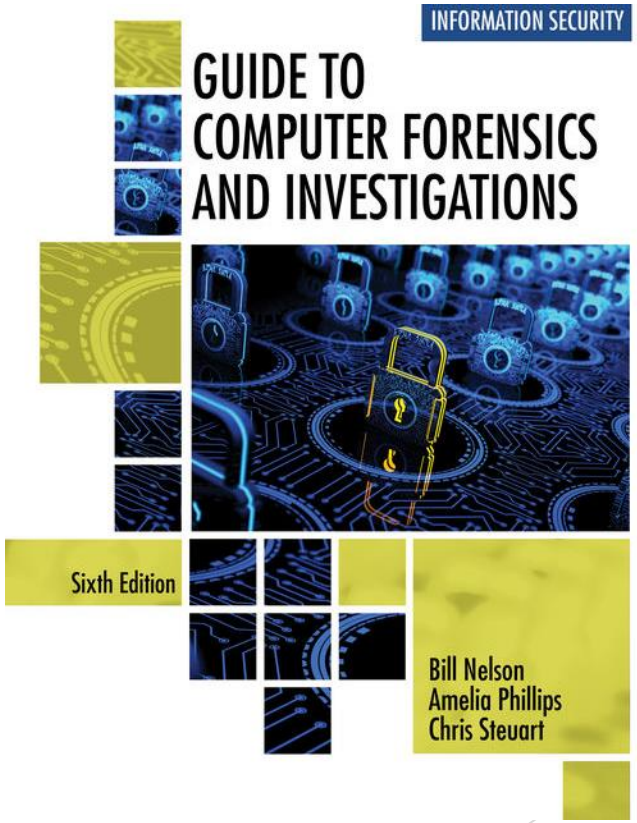
- Sparse acquisition likely required if storage at scale is unavailable or imaging of the volume isn't practical
  - Certain storage systems aren't necessarily going to be readable by your forensic tools; particularly SANs
- Consult with the operator the storage system as practical to determine the best method to capture your evidence

Technical Advisors

- 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

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Evidence Storage & Case Review

Documentation

- Record your activities and findings as you work
  - Maintain a journal to record the steps you take as you process evidence
  - If you have an official form required; use that
- Your goal is to be able to reproduce the same results
  - When you validate the case internally
  - If the case is validated externally or during a legal matter
- Use the required forms to track your evidence
  - Single evidence form, chain of custody, etc.

Documentation (Cont.)

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

Evidence Handling

- Maintain the integrity of digital evidence in the lab
  - Follow the same rules to protect the evidence as you would in the field
  - Access control, defense in depth, logging, etc.
- Steps to store image files:
  - Copy all image files to a large drive, SAN, or other NAS
  - Start your forensics tool to analyze the evidence
  - Hash the image using the forensic tool to verify it matches your original acquisition notes
  - Secure the original media in an evidence locker
- Consider media lifetimes when choosing long term storage

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

Hashing Activity

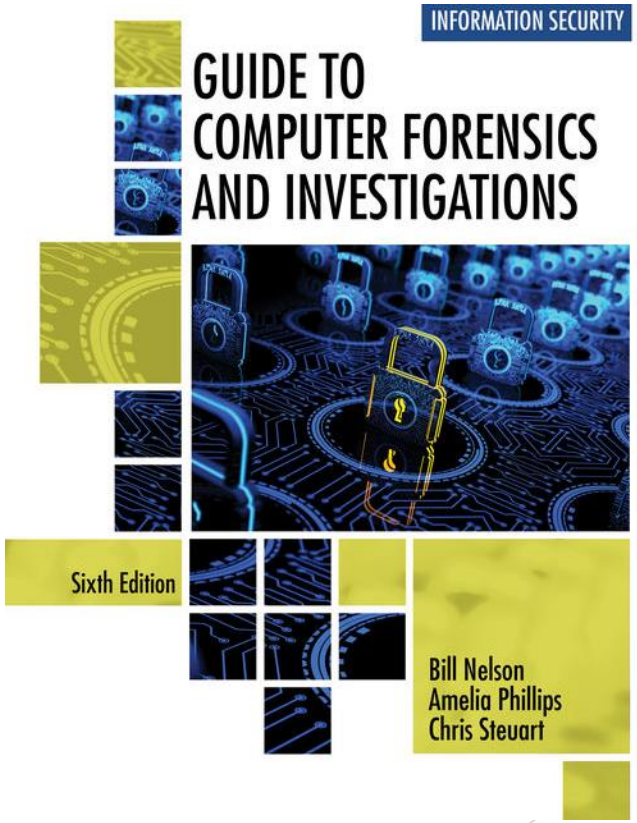
- Attempt the activity on page 177 of the text
  - Requires FTK imager (linked in previous module) or another imaging tool
  - Not scored

Example Cases

- Pages 179-186 of the text
  - OSForensics is configured on ForensicWks in the vApp

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Network Acquisition

Using GRR

Our Example Network

- 2-3 client machines
- 1 Network Forensics Server (GRR Rapid Response)
- 1 Forensic Workstation
- 1 Router (mostly for DHCP/DNS)

Setting Up Clients

- Typically, not done by the forensic investigator in an enterprise
- Simple as downloading a client and installing as administrator
  - Security of client management is important
  - In our environment, client software is at http://grrserver:8000
  - GRR includes all connection information in the binary

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*