Current Digital Forensics Tools

Software & Hardware

Objectives

- Explain how to evaluate needs for digital forensics tools
- Describe available digital forensics software tools
- List some considerations for digital forensics hardware tools
- Describe methods for validating and testing forensics tools

Evaluating Your Needs

What Tools Work for You?

- Open-source tools will often provide the most features for the lowest price (free)
- Proprietary tools may have better support & wider recognition in the courtroom
- Questions to ask:
  - What OS's do you need to support for analysis? What OS will your tools run on?
  - Can the tool analyze more than one file system? Do you need to analyze more than one file system?
  - Is scripting of some type supported by your tool?
  - Does the vendor provide support consistently?

Task Categories from CFTT / ISO 27037

- NIST has established the **Computer Forensics Tool Testing** (CFTT) program
  - We'll explore a subset of those categories

- Acquisition
- Validation & Verification
- Extraction
- Reconstruction
- Reporting

Acquisition

- Making a copy of an original medium (drives or other media)
- Most important factor in acquisition is using the **proper** tool for the task **correctly**
- There are both hardware and software components to acquisition if a forensic bridge is used
- There are pros and cons to various acquisition formats
  - Ex: size vs ease of access / unallocated capture vs speed

Validation & Verification

- **Validation:** confirming a tool works as intended
- **Verification:** proving that two sets of data are identical or that an output matches what's expected
  - Example: hash verification between image and source
  - Examples: filtering
    - Ignoring what's known (KFF / NSRL)
    - File type verification by header
- Both can be tested using existing images
  - Ex: CFReDS: https://www.cfreds.nist.gov/

Extraction

- **Extraction:** the part of the investigation where data is recovered from evidence

- Subfunctions of extraction:
  - Data viewing
  - Keyword searching
  - Decompressing or uncompressing
  - Carving
  - Decrypting
  - Bookmarking or tagging

Extraction (Cont.)

- Carving and decompression are typically automated
  - Determining what should be carved or decompressed is usually configurable by file type
- Decryption is supported by tools but will require recovery keys or different types of password attacks
  - **Dictionary attack:** using words related to the suspect to create a list of passwords for attempted access to files, volumes, etc
  - **Brute-force attack:** generating a sequence of passwords until determining the right password
    - Works 100% of the time, provided infinite time

Reconstruction

- **Reconstruction:** recreating a suspect drive to demonstrate what happened during an incident

- Most suites have this built-in, but it can always be done manually provided an image
  - FTK Imager only captures images
  - FTK can write out images

- Many methods listed in the text – the idea is copying your acquired image/clone to another image/clone for additional testing or verification

Reporting

- **Reporting:** collection of relevant information from your investigation
  - Tool report: generated automatically (generally from bookmarks)
  - Full report: prepared by an investigator but often references a tool report

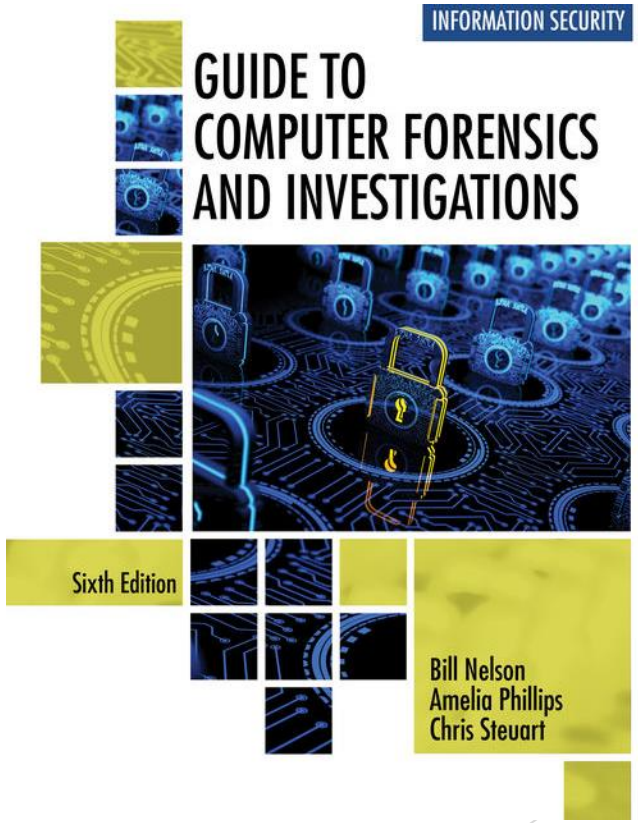
- Subfunctions:
  - Bookmarking or tagging
  - Log reports
  - Timelines
  - Report generator

Comparing Available Suites

- Text has a table comparing features between 4 common tool suites on page 282 (Table 6-1)
- Consider making something similar when determining your needs in forensic tooling
- Flexibility, reliability, and future support/expandability are all factors
  - Every shop will have different needs
- Consider keeping all tools for an extended period if allowed by license terms

References

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



Software Tools

Command Line Tools

- Historically – system administration tools were manually used for forensics
- Norton DiskEdit is a command line tool
- Command line tools are lightweight to run, but can have a higher learning curve than GUI tools
- The text calls out the **`dir`** command with the **`/q`** flag to get file owner as an example of a quick look that's built-in to Windows

Linux Tool Examples

- SMART from ASR Data (only for LE/Military)
- Helix 3 from e-fense ($239/yr membership)
- Kali Linux (free includes Autopsy and Sleuth Kit)
- Autopsy & Sleuth Kit (free)
  - Kali includes the original web version of Autopsy for operating The Sleuth Kit
  - There is a new Java based Autopsy available that runs on Windows & Linux
- Countless other open-source projects
  - This list has been updated recently: https://github.com/cugu/awesome-forensics

GUI Tools

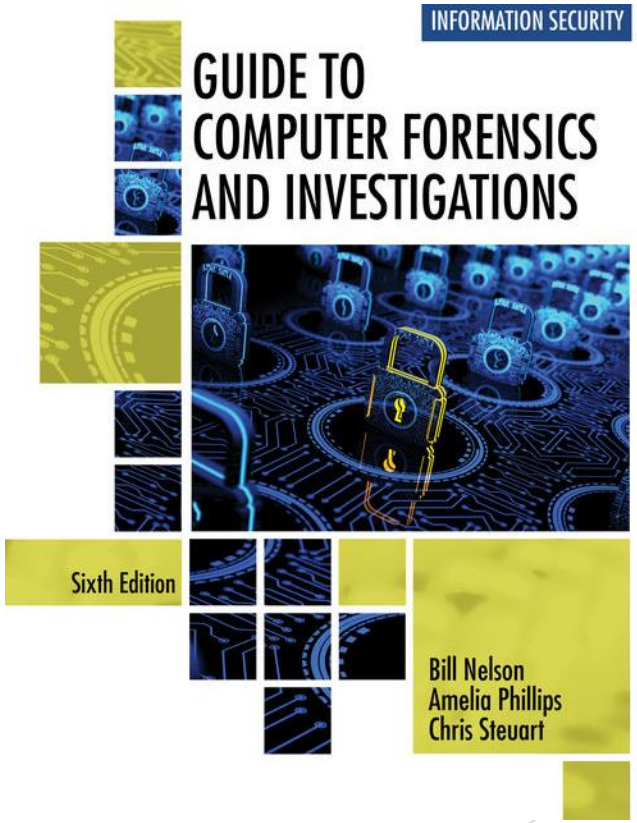
- **Graphical User Interface** (GUI) forensics tools can simplify digital forensics investigations
  - Additionally, simplify training for beginning examiners
- Most (not all) GUI tools are provided as suites
  - We'll use FTK in this course – CSC 419 explores Axiom from Magnet Forensics

GUI Tools (Cont.)

- Advantages
  - Ease of use
  - Multitasking
- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies

References

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



Autopsy / The Sleuth Kit via Kali

Exploring NSRL / KFF

Index Search In FTK

Reconstruction with FTK

Reporting with FTK

Hardware Tools

Workstation Types

- **Stationary Workstation:** desktop machine with several bays and connectivity for external devices / peripherals
- **Portable Workstation:** mobile machine (typically a large laptop) with a similar amount of connectivity as a stationary workstation
- **Lightweight Workstation:** A more basic laptop with fewer connectivity options
- If you have the budget (and need) for it, it's likely more practical to have multiple systems that support diverse cases
  - Private orgs likely can streamline to what they deploy to their users

Building vs. Buying

- Most of you already noted this in your previous labs, but there are pros and cons to building your own forensic workstations

- Pros
  - Save money
  - Customized to your exact needs

- Cons
  - No actual support

Critical Components

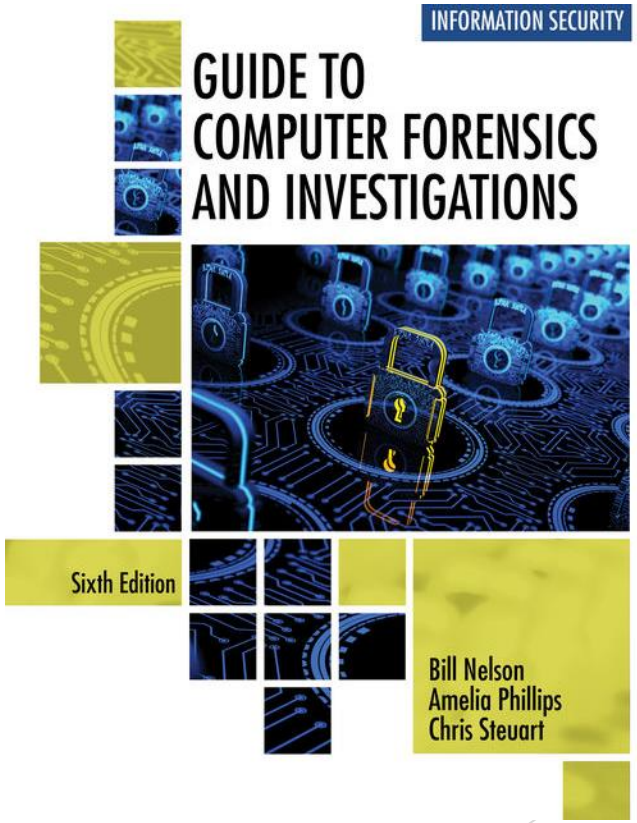
- **Write Blocker / Forensic Bridge:** prevents writes to a disk
  - Can also use live CD/DVDs that support software write blocking (if allowed)
- Large amounts of storage, processing power, and memory
  - Unless you're only doing very targeted investigations

Overall - YMMV

- Your mileage may vary…
- Every shop is going to have different needs

References

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



Validation & Testing

Why?

- It is important to make sure the evidence you recover and analyze can be admitted in court
- You must test and validate your software to prevent damaging the evidence

Using NIST Tools for Testing/Validation

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software
- Computer Forensics Tool Testing (CFTT) project
  - Manages research on forensics tools
- NIST has created criteria for testing forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards

Criteria for Testing

- ISO 5725 - specifies results must be repeatable and reproducible

- **Establish Categories for Tools:** group software according to categories of artifacts they retrieve or similar
- **Identify Category Requirements:** describe the technical features a tool must have to be in that category
- **Develop Test Assertions:** Find/create cases that can be verified in existing tools and use them to test new tools
- **Document a Test Method:** document how to test the tool
- **Report Test Results:** describe the results in a format that complies with ISO 5725

Validate All Tools You Use

- Always verify your results by performing the same tasks with other similar forensics tools
- You don’t have redo every case in an additional tool
  - You should verify each artifact types in different tools
  - Spot checking is good too (quality assurance measures in certain accreditations can drive this)

Examination Protocol

1. Perform the investigation with one tool
2. Verify your results with a disk editor (or another qualified tool)
3. Compare outputs of both tools

Upgrade Protocol

- Test at any
  - New tool releases
  - OS patches and upgrades
- If you find a problem, report it to forensics tool vendor
  - Do not use the forensics tool until the problem has been fixed
- Use a test disk for validation purposes
- Check the Web for new editions, updates, patches, and validation tests for your tools

References

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