Acquisition

CSC 388

Module Objectives

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to acquire and validate evidence
- Describe RAID acquisition methods
- Explain how to use remote network acquisition tools

Digital Evidence Formats

Format Options

- Data in a forensics acquisition tool is stored as an image file
- Three most common formats
  - Raw format
  - Proprietary formats
  - Advanced Forensics Format (AFF)

Raw Format

- Makes it possible to write bit-stream data to files
- Advantages
  - Fast data transfers
  - Ignores minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors

Proprietary Options

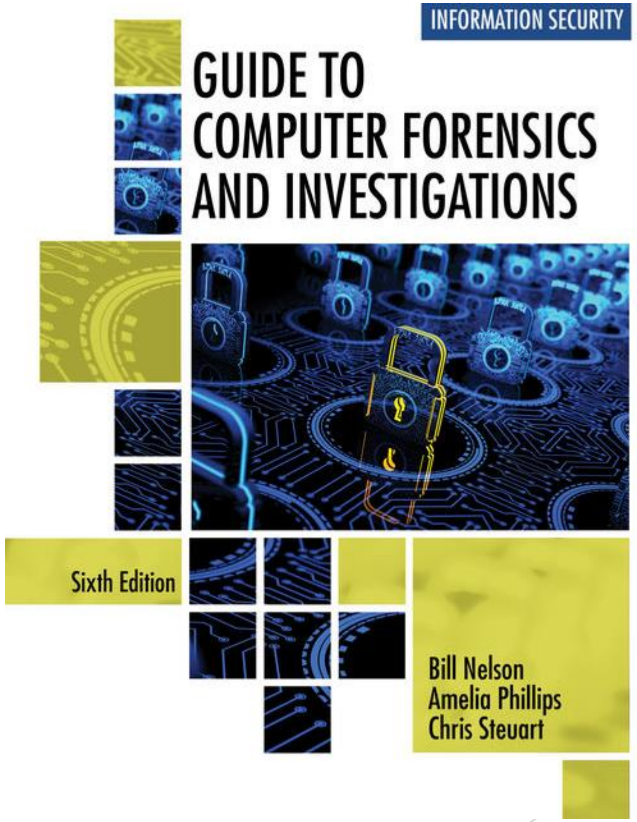
- Most forensics tools have their own formats
- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
  - Can integrate metadata into the image file
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
- The Expert Witness Compression format is unofficial standard

Advanced Forensics Format (AFF)

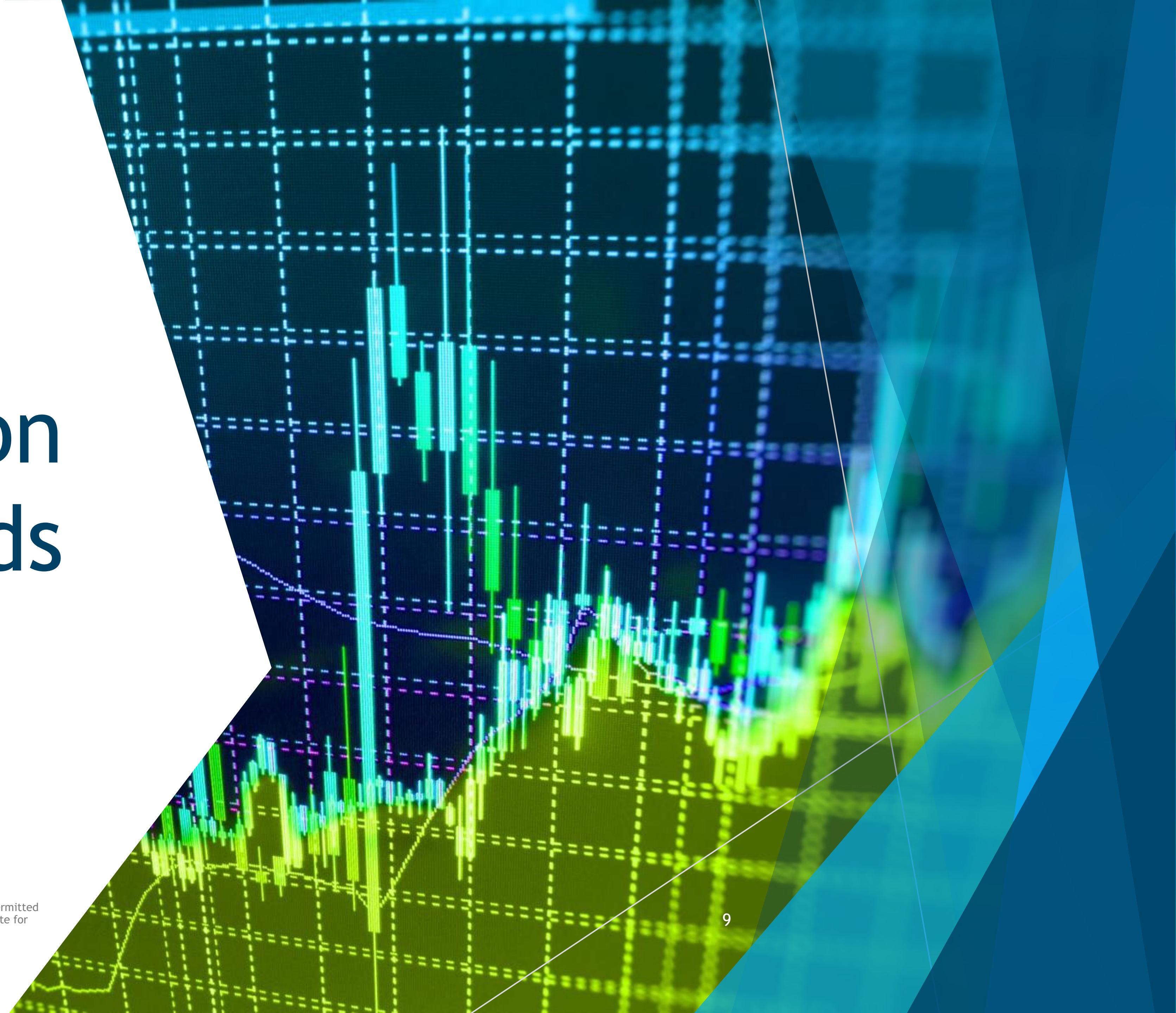
- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format
- Design goals
  - Provide compressed or uncompressed image files
  - No size restriction for disk-to-image files
  - Provide space in the image file or segmented files for metadata
  - Simple design with extensibility
  - Open source for multiple platforms and Oss
  - Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata
- AFF is open source

References

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



Acquisition Methods



Static vs Live Acquisition

- Static Acquisition
  - Also called a dead-box acquisition
  - Image or clone is collected with machine powered off
- Live Acquisition
  - Machine is powered on and there exists a situation where interacting with the machine is valuable
    - Memory acquisition
    - Full disk encryption

Full Disk Methods

- Creating a disk-to-image file
  - Most common method and offers most flexibility
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - Compatible with many commercial forensics tools
- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk’s geometry configuration
  - Tools: EnCase and X-Ways

Logical & Sparse Methods

- Logical Acquisition
  - Only captures specific files of interest to the case
  - Ex: Windows registry, web history, only images or documents
  - Won’t see deleted items this route

- Sparse Acquisition
  - Like logical, but will additionally acquire unallocated (deleted) space on disk

Considerations to Determine Method & Equipment

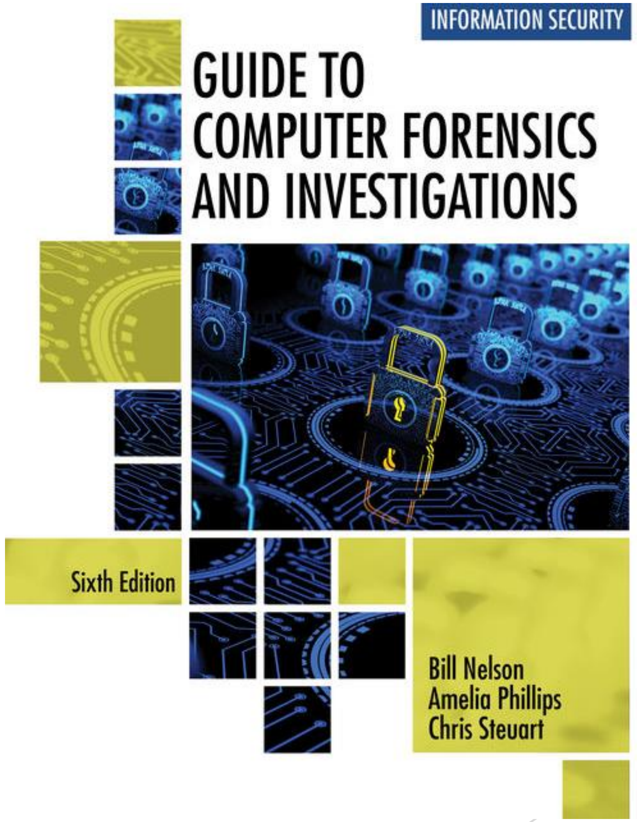
- Size of Disk
  - Lossless compression is useful (built into EWF, others)
- Time to perform acquisition
  - Would a logical acquisition do the job?
- Where the evidence is located

Remember

- Murphy’s Law
  - Always have a duplicate of your image file; particularly when you’re releasing/returning evidence
  - Copy with two different tools (if practical)
- Certain areas of the disk may not be copied by all tools
  - Host Protected Area (HPA) – mostly allows for reporting different disk size information
- If the disk is encrypted AND the machine is powered off, suspect cooperation or other sources may be required

References

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



Acquisition Tools

Acquisition Devices (Disk-to-Disk or Disk-to-Image)

Acquisition Using Windows

- Advantages
  - Collection is convenient
  - Images can immediately be processed
- Disadvantages
  - Tools (generally) can’t see the HPA if that’s suspected to hold data
  - Certain countries don’t accept write blocking bridges for acquisition

Acquisition Using a Live CD/DVD/USB

- Linux Examples (make sure a read-only mode exists / test first; always)
  - Kali
  - Knoppix
  - PALADIN
  - Other spins
- Win-FE
  - https://brettshavers.com/brett-s-blog/entry/mini-winfe-10-and-winfe-10-updated

Basic Linux Commands for Disk Interaction

- **fdisk** lists, creates, deletes, and verifies partition
- **mkfs.<fstype>** formats a file system
- **dd** can be used for bit-for-bit copying of data (be careful…)
  - **dcfldd** is a more forensic centric data dump tool

- Other tools will vary widely by distribution
  - ewfmount/ewfcapture/etc powered by libewf/libyal are very useful in this situation
  - Guymager is a tool on Kali that can capture a well-formed EWF image for use with various forensic tools

Capturing Images in Windows (Live & Static)

- Live w/ FTK Imager
- Static w/ FTK Imager
- *We are operating **without** a write blocker in the lab environment, but when you are able and/or required **always** use a write blocking interface for static acquisitions

Capturing Images in Linux (Static via Live CD/DVD/USB)

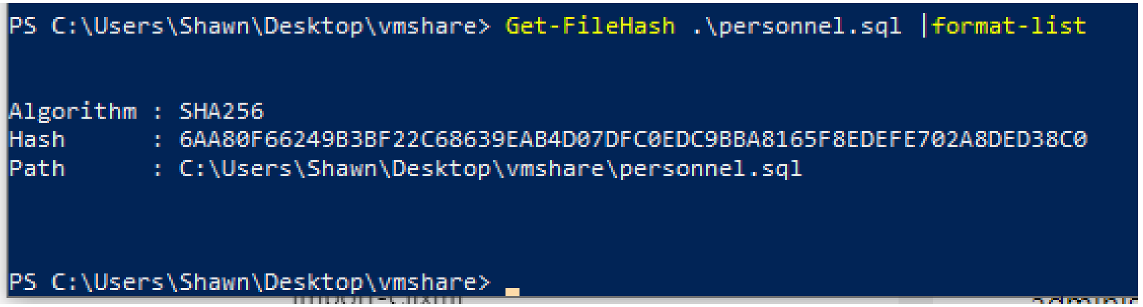
- Static w/ dd
- Static w/ ewfcapture
- *Again, we are operating **without** a write blocker in the lab environment, but when you are able and/or required **always** use a write blocking interface for static acquisitions

Validation Matters

- Validating evidence may be the most critical aspect of computer forensics
- Requires using calculating a hash
    - Identical data always results in the same hash
    - Infeasible to
        - Generate the data that results in a particular hash
        - Find two different messages with same hash value (re: SHAttered)
    - Any change to source data should change hash significantly
- Validation techniques
    - CRC-32, MD5, and SHA-1 to SHA-512

By Collection Tool

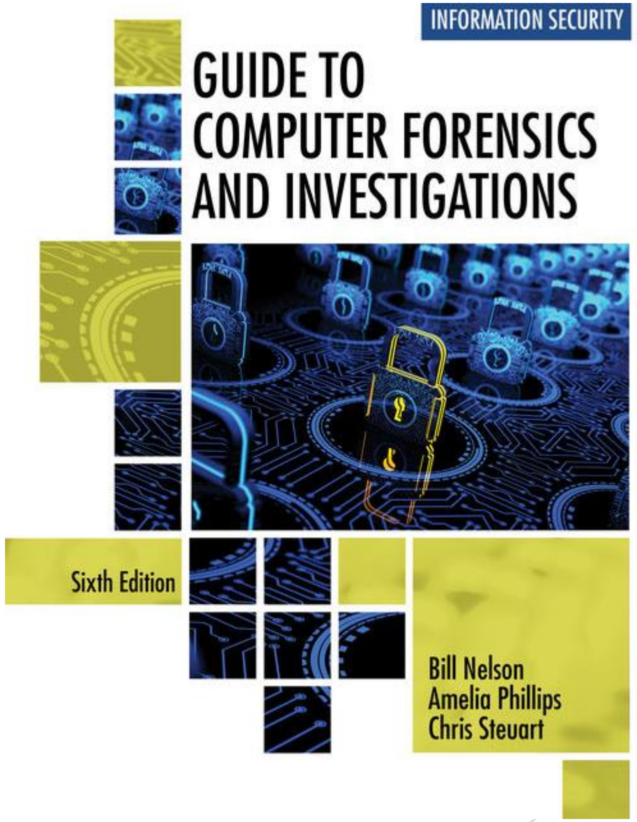
- dd
  - Generic hashing utilities against the file work as the file is an exact copy of the disk
  - Linux: md5sum shasum and sha2sum families of utilities
  - Windows: certutil can calculate certain hashes as can the Get-FileHash cmdlet
- dcfldd
  - Hashing can be included at runtime
  - **hash** option will select algorithm
  - **hashlog** option will store hash outputs
  - **vf** option will compare resulting image hash to original media
- Proprietary formats often include validation metadata



```
PS C:\Users\Shawn\Desktop\vmshare> Get-FileHash .\personnel.sql |format-list


Algorithm : SHA256
Hash      : 6AA80F66249B3BF22C68639EAB4D07DFC0EDC9BBA8165F8EDEFE702A8DED38C0
Path      : C:\Users\Shawn\Desktop\vmshare\personnel.sql



PS C:\Users\Shawn\Desktop\vmshare>
```

References

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



RAID Acquisition

RAID Can Be a Problem

- Acquisition of RAID drives can be challenging and frustrating because of how RAID systems are
  - Designed
  - Configured
  - Sized
- Size is the biggest concern
  - Many large storage systems now have exabytes of data

Key Questions

- How much data storage is needed?
- What type of RAID is used?
- Do you need to have all drives connected?
- Do you have the right acquisition tool?
- Can the tool read a forensically copied RAID image?
- Can the tool read split data saves of each RAID disk?

Available RAID Acquisition Tools

- Vendors offering RAID acquisition or re-construction functions
  - Guidance Software EnCase (ex: blog.1234n6.com)
  - X-Ways Forensics
  - AccessData FTK
  - Runtime Software
  - R-Tools Technologies
- Occasionally, a RAID system is too large for a static acquisition
  - Retrieve only the data relevant to the investigation with the sparse or logical acquisition method

Exploration

- Software RAID today…

References

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