Guide to Computer Forensics and Investigations Sixth Edition

Chapter 3
Data Acquisition

Objectives

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to use acquisition tools

Objectives (Cont)

- Explain how to validate data acquisitions
- Explain how to use remote network acquisition tools
- List other forensic tools available for data acquisitions

Data Acquisition recap…

Forensic Data Acquisition

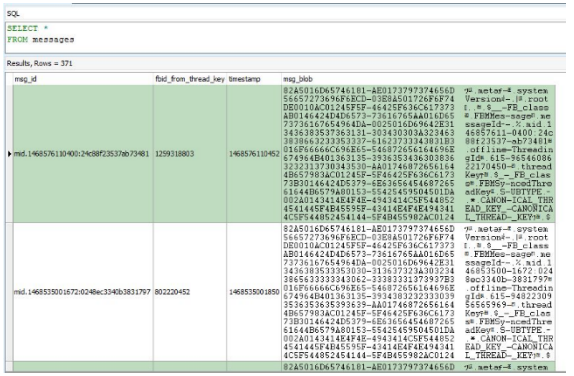
- Before we can analyze data, we have to secure it.
- The goal of forensic data acquisition is to create a forensic copy of a piece of media that is suitable for use as evidence in a court of law.

Understanding **Storage Formats** for Digital Evidence

- Data in a forensics acquisition tool is stored as an **image file**
  - *Basically, the image file can be in one of* the three formats
    - Raw format
    - Proprietary formats
    - Advanced Forensics Format (AFF) – *Newer*

Raw Format

- Makes it possible to write bit-stream data to files (*Sequence flat file*)
  - *In the past we only do bit by bit copy to media same size or bigger to create evidence…*



https://sandersonforensics.com

- Advantages
  - Fast data transfers
  - Ignores minor data read errors on source drive
  - Most computer forensics tools can read raw format (i.e *.dd)
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors – *due to low threshold of retry reads on weak media spots on a drive*

Proprietary Formats

Most forensics tools have their own formats…

- Features offered
  - Option to compress or not compress image files – *save space*
  - Can split an image into smaller segmented files – *provide integrity check for split data*
  - Can integrate metadata into the image file
- Disadvantages
  - Inability to share an image between different tools/*vendors*
  - File size limitation for each segmented volume – *typically 650MB, can adjust up or down at a limit of 2GB*
- The Expert Witness format is unofficial standard - *default for Guidance Software EnCase (i.e ex01, e01)*

Advanced Forensics Format (AFF)

- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format

http://forensics.luizrabelo.com.br/

- Design goals
  1. Provide compressed or uncompressed image files
  2. No size restriction for disk-to-image files
  3. Provide space in the image file or segmented files for metadata
  4. Simple design with extensibility
  5. Open source for multiple platforms and Oss
  6. *vendors will have no implementation restrictions on this format. Possible the future standard*
  7. Internal consistency checks for self-authentication

Advanced Forensics Format (Cont)

- File extensions include **.afd** for segmented image files and **.afm** for AFF metadata

- AFF is open source

https://www.hackread.com

Determining the Best Acquisition Method

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**

- Four methods of data collection
  - Creating a disk-to-image file
  - Creating a disk-to-disk
  - Creating a logical disk-to-disk
  - Creating a sparse data copy of a file or folder

- Determining the best method depends on the circumstances of the investigation!!

Determining the Best Acquisition Method (Cont)

- 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
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLookIX – *Tools that perform disk-to-image file copy. These programs read the disk-to-image file as though it were the original disk.*

- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk's geometry (track, sectors etc) configuration
  - EnCase, SnapCopy, SafeBack

Determining the Best Acquisition Method (Cont)

- **Logical acquisition** or **sparse acquisition** (*Collect evidence from a large device can take several hours*). *Reasons for using these acquisition methods are:-*
  - Use when your time is limited
    - **Logical acquisition** captures only specific files of interest to the case. – *i.e only want to investigate email outlook*
    - **Sparse acquisition** collects fragments of unallocated (deleted) data
  - For large disks
  - For PST or OST mail files, RAID servers (*can be up to a several TByte*)

Determining the Best Acquisition Method (Cont)

When making a copy, consider:

- **Size of the source disk**
  - Lossless compression might be useful (*does not permanently remove data, original data can be reconstructed*) – *Target does not need to be so big*
  - Use digital signatures for verification
- When working with large drives, an alternative **is using tape backup systems** (*i.e SDLT. Can be slow if data is large*)
- **Whether you can retain the disk** : *Sometime after copy, the original disk may need to return to owners.*

Contingency Planning for Image Acquisitions

- Create a duplicate copy of your evidence image file
  - *In case of failure but can be time consuming*
- Make **at least two images** of digital evidence
  - Use different tools (*Encase/Prodiscover*) or techniques
- Copy **host protected area** (***HPA*** - *An area not visible for OS on drive*) of a disk drive as well
  - Consider using a hardware acquisition tool that can access the drive at the BIOS level so as to access HPA
- Be prepared to deal with encrypted drives
  - **Whole disk encryption** feature in Windows called **BitLocker** makes static acquisitions more difficult
  - May require user to provide decryption key – *suspect may not want to corporate*

Using Acquisition Tools

- Acquisition tools for Windows
  - Advantages
    - Make acquiring evidence from a suspect drive more **convenient**
      - Many Tools developed for Windows platform
      - Especially when used with hot-swappable devices (*i.e USB, Fireware*)
  - Disadvantages

    - Must protect acquired data with a well-tested write-blocking hardware device
    - Tools can't acquire data from a disk's host protected area
    - Some countries haven't accepted the use of write-blocking devices for data acquisitions (*Need to check with legal*)

Capturing an Image with ProDiscover Basic

- Connecting the suspect's drive to your workstation
  - Document the chain of evidence for the drive
  - Remove the drive from the suspect's computer
  - Configure the suspect drive's jumpers as needed
  - Connect the suspect drive to write-blocker device
  - Create a storage folder on the target drive

- Using ProDiscover's Proprietary Acquisition Format
  - Refer to "*Guide To Computer and Forensics Anc Investigations*" for details to start ProDiscover Basic and configure settings for acquisition!!

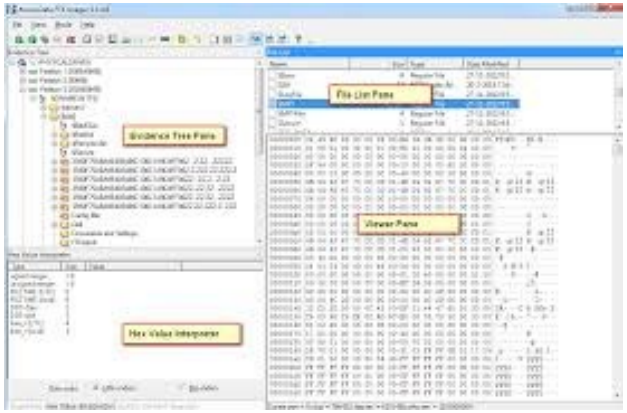
Capturing an Image with ProDiscover Basic (Cont)

- Using ProDiscover's Proprietary Acquisition Format (con't)
  - ProDiscover creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)
  - If the compression option was selected, ProDiscover uses a .cmp rather than an .eve extension on all segmented volumes

Capturing an Image with AccessData FTK Imager Lite

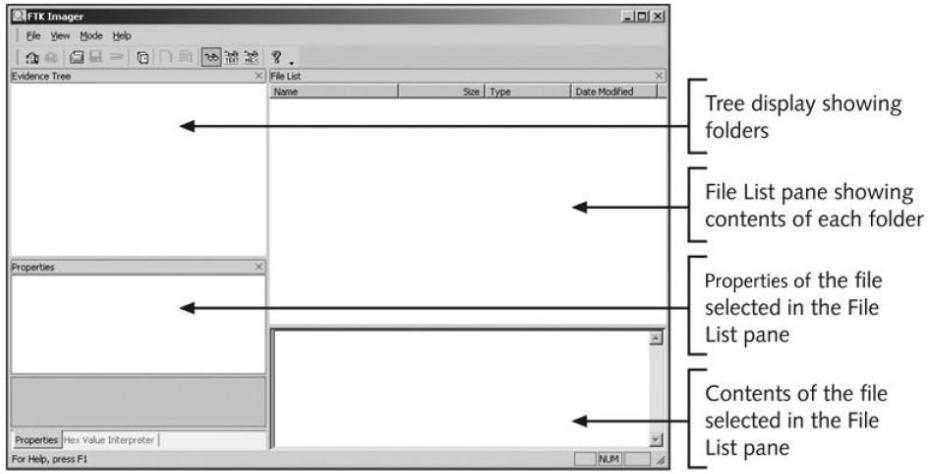
Another New Forensic Tools!

- *FTK Imager is windows data acquisition tool that* Included with AccessData Forensic Toolkit
- Designed for viewing evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a hardware write-blocking device
  - Or run from a Live CD, such as Mini-WinFE



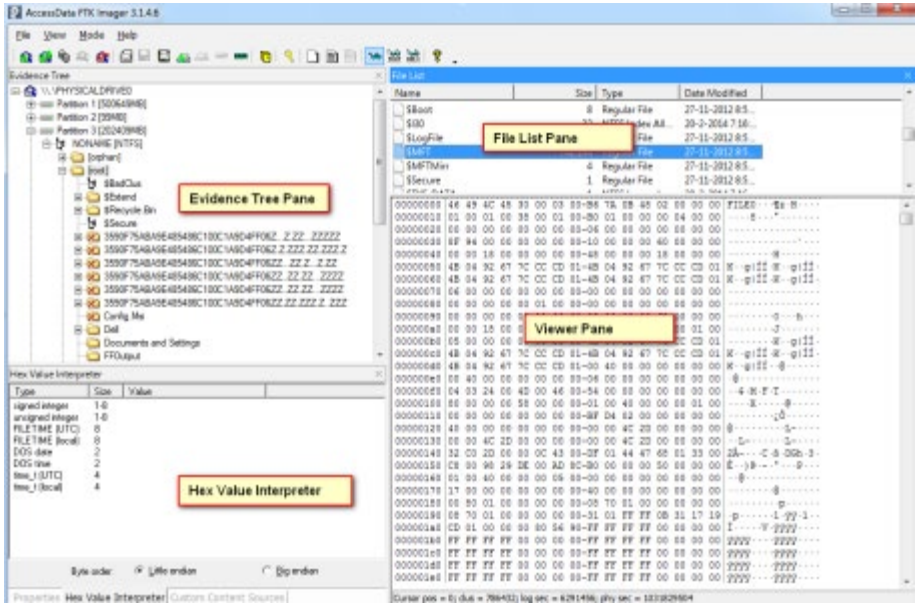
https://eforensicsmag.com

Capturing an Image with AccessData FTK Imager Lite (Cont)



https://eforensicsmag.com

Figure 4-6 The FTK Imager main window



Capturing an Image with AccessData FTK Imager Lite (Cont)

- FTK Imager can't acquire a drive's host protected area (HPA)

- Use a write-blocking device and follow these steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk to write-blocker
  - Start FTK Imager Lite
  - Create Disk Image - use Physical Drive option

Validating Data Acquisitions

- Validating evidence may be the most critical aspect of computer forensics
- Requires using a **hashing algorithm utility**
- Validation techniques
  - **CRC-32, MD5, and SHA-1 to SHA-512**

https://eforensicsmag.com

Windows Validation Methods

- Windows has no built-in hashing algorithm tools for computer forensics
  - Third-party utilities can be used : *hexadecimal editors such as Win Hex*

- Commercial computer forensics programs have built-in validation features
  - Each program has its own validation technique
  - ProDiscover's .eve files contain metadata in the acquisition file or segmented files, including the hash value for the suspect drive or partition.

- Raw format image files don't contain metadata
  - Separate manual validation is recommended for all raw acquisitions

Using Remote Network Acquisition Tools

- You can remotely connect to a suspect computer via a network connection and copy data from it
- Remote acquisition tools vary in configurations and capabilities
  - *i.e Some require manual intervention on remote suspect computers to initiate the data copy*
- Many tools such as Encase, Prodiscover allow remote acquisition.
- Drawbacks
  - Antivirus, antispyware, and firewall tools can be configured to ignore remote access programs – *access could be blocked!*
  - Suspects could easily install their own security tools that trigger an alarm to notify them of remote access intrusions

Remote Acquisition Tool

- Being able to connect to a suspect's computer directly allows the following capabilities:
  1. Preview a suspect's drive remotely while it's in use or powered on.
  2. Perform a live acquisition (also called a "smear" because with an active computer, disk data is being altered) while the suspect's computer is powered on.
  3. Encrypt the connection between the suspect's and examiner's computers.
  4. Copy the suspect computer's RAM while the computer is powered on.
  5. Use the optional stealth mode to hide the remote connection from the suspect while data is previewed or acquired.

Remote Acquisition Tool

- Other functions may include:
  1. Capture volatile system state information.
  2. Analyze current running processes on a remote system.
  3. Locate unseen files and processes on a remote system that might be running malware or spyware.
  4. Remotely view and listen to IP ports on a compromised system.
  5. Run hash comparisons on a remote system to search for known Trojans and rootkits.
  6. Create a hash inventory of all files on a system remotely (a negative hash search capability) to establish a baseline if it gets attacked.

Using Other Forensics-Acquisition Tools

- Other commercial acquisition tools
  - **Magnet Axiom**
  - PassMark Software ImageUSB
  - ASRData SMART
  - Runtime Software
  - ILookIX Investigator IXimager
  - SourceForge Projects Repository

Magnet Axiom

- Like many forensics tool, MA is able to recover digital evidence from most sources, including smartphones, cloud services, computers, IoT devices and third-party images.

- The examination tool help forensics professionals find most relevant data and **visualize** it for better analysis.

- This tool is gaining popularity as users based increases.

MAGNET FORENSICS®

https://www.cybersecurityweek.nl

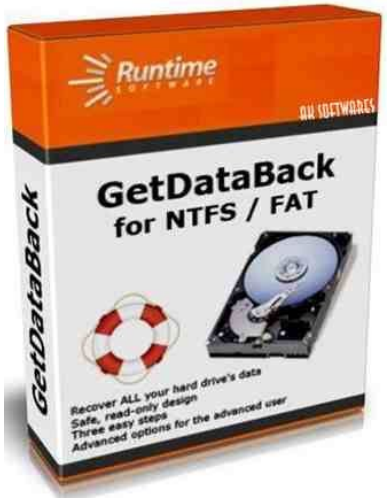
PassMark Software ImageUSB

- PassMark Software has an acquisition tool called ImageUSB for its OSForensics analysis product
- **ImageUSB** downloaded from the OSForensics Web site
- **ImageUSB** is a free utility
  - You can write an image concurrently to multiple USB Flash Drives

Runtime Software

- Runtime Software offers shareware programs for data acquisition and recovery:
  - DiskExplorer for FAT and NTFS

- Features:
  - Create a raw format image file
  - Segment the raw format or compressed image for archiving purposes
  - Access network computers' drives



http://sdxpsoft.blogspot.sg

SourceForge

- SourceForge provides several applications for security, analysis, and investigations
  - *Was preferred source code repository and distribution platform for free and open source software (FOSS) projects*

- For a list of current tools, see:
  - http://sourceforge.net/directory/security-utilities/storage/archiving/os:windows/freshness:recently-updated

Summary

- Forensics data acquisitions are stored in three different formats:
  - Raw, proprietary, and AFF

- Data acquisition methods
  - Disk-to-image file
  - Disk-to-disk copy
  - Logical disk-to-disk or disk-to-data file
  - Sparse data copy

Summary

- Several tools available
  - Lossless compression is acceptable
- Plan your digital evidence contingencies
  - Make a copy of each acquisition
- Write-blocking devices or utilities can be used with GUI acquisition tools
- Always validate acquisition