

## What is computer forensics?

The preservation, recovery, analysis and reporting of digital artifacts including information stored on computers, storage media (such as a hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network.

## Where is computer forensics used?

- Criminal and civil investigations
- Divorce cases
- Insurance investigation
- Corporate investigations

## Principles of computer forensic investigations

1. Your actions should not affect the integrity of the evidence
  - a. You should minimize any changes to the evidence. If changes are made, make sure the reason and impacts are documented.
2. Take notes on everything
3. Analyze all evidence collected
4. Report your findings

## Tools

### A case for open source

- Verifiable
- Available
- Scriptable
- Large community support
- Cutting edge
- Opportunity to give back to the community

### Linux

Linux makes an extremely powerful forensic workstation and acquisition environment. In addition to all the reasons listed above, Linux has the following advantages:

- Support many file systems natively
- Forensic community heavily uses Linux and much of what you can find or read will be based on Linux
- Linux is very powerful and utilizes all the assets of your computer system

### Helix

Helix is maintained by e-fense and is a “customized distribution of Ubuntu Linux” that “has been modified very carefully to NOT touch the host computer in any way and it is forensically sound”. Helix has both a live side for Incident Response as well as a forensic environment.

## The Sleuth Kit and Autopsy Forensic Browser

TSK and Autopsy are authored by Brian Carrier. He is also the author of File System Forensic Analysis, a very important book for any forensic analyst. TSK 3.0 and Autopsy 2.20 were released on October 2008.

## Open source/free tools

The following is a list of some of the most used and important open source/free tool for computer forensic:

- dd/dcfld/dc3dd (<http://dcfldd.sourceforge.net/> <http://dc3dd.sourceforge.net/>)
  - Disk Duplicator and/or Disk Destroyer and various updates versions
- Foremost (<http://foremost.sourceforge.net/>)
  - File/data carving
  - Built-in file types, can be expanded with configuration file (i.e. iPhone forensics)
- Lazarus (<http://www.porcupine.org/forensics/tct.html>)
  - Part of TCT, attempts to reconstruct files or data from raw data
  - Very slow but very powerful
- Sorter (<http://www.sleuthkit.org/>)
  - Runs file command on all files, deleted and undeleted
  - Sorts based on file type, looks for mismatched extensions
  - Can utilize hash databases for known good or known bad files
- nc/cryptcat (<http://netcat.sourceforge.net/> <http://sourceforge.net/projects/cryptcat/>)
  - networking utility which reads and writes data across network connections, using the TCP/IP protocol.
- Sysinternals (<http://technet.microsoft.com/en-us/sysinternals/default.aspx>)
  - suite of utilities to help you manage, troubleshoot and diagnose Windows systems and applications
  - Company was bought by Microsoft in 1996 and the tools remain free and ever expanding
- VMWare workstation
- Liveview (<http://liveview.sourceforge.net/>)
  - Java-based graphical forensics tool that creates a VMware virtual machine out of a raw (dd-style) disk image or physical disk
- Wireshark (<http://www.wireshark.org/>)
  - Formerly Ethereal, allow for network capture (via pcap) and analysis of network traffic
- Volatility Framework (<https://www.volatilesystems.com/default/volatility>)
  - Emerging project for the analysis of memory dumps

## Commercial Tools

- EnCase (<http://www.guidancesoftware.com/>)
- FTK (<http://www.accessdata.com/>)

## Concepts

### Cryptographic hashing

- Purpose
- Hashes
  - MD5

- SHA1
- Collision concerns

### Hash databases

- NSRL/Hashkeeper
- Roll your own
- Child Pornography

### Live vs. dead analysis

- Incident response
- Encrypted file systems

## Technical introduction

### Physical media (hard drives, usb drives, etc.)

- Big-Endian vs. Little-Endian
- Sectors and clusters
- Blocks and inodes

### Layers of a file systems

- Physical Layer (fsstat)
- File System Layer (mmls,mmstat)
- Data Content Layer (dls)
  - Sectors -> Clusters/blocks
  - Allocated or unallocated, addressable
- Meta Data Layer (ils)
  - Add structure to the data, like a card catalog
  - Inodes/MFT Entry/FAT Directory Entry
  - Allocated or unallocated, addressable
  - Points to Data Content Layer
- File Name Layer (fls)

### HPA

- Host Protect Area explained
- disk\_stat, disk\_sreset, dmesg
  - # disk\_stat /dev/hdb
  - Maximum Disk Sector: 120103199
  - Maximum User Sector: 118006047
  - \*\* HPA Detected (Sectors 118006048 - 120103199) \*\*

### Disk images vs. partitions

### Special considerations for raw/unstructured data

- Swap space
- Memory

## Volatility of data

- CPU registers
- Memory
- Network connections
- Processes
- Hard drive
- Removable media

## Basic methodology for a computer forensic investigation

The US DOJ has many resources for digital forensics. Particularly useful is their document “Forensic Examination of Digital Evidence: A Guide for Law Enforcement” (<http://www.ojp.usdoj.gov/nij/pubsum/199408.htm>). This document contains their suggested methodology for digital forensics.

1. Verify the incident
2. Evidence Assessment
3. Evidence Acquisition
4. Evidence Examination
  - Physical Extraction
    - Keyword searching
    - File carving (foremost, lazarus)
  - Logical Extraction
    - Extract slack space, unallocated space, allocated space and deleted files
    - Identify known good or known bad via hash databases
  - Analysis of extracted data
    - Timeline analysis
    - Data hiding analysis
    - Application and file analysis
    - Ownership and possession
5. Documenting and Reporting
  - Document as you go!
  - Make notes with full context for further analysis later or reporting

## Live demonstration

I will perform a step by step analysis of a USB drive.

## Suggestion for forensic education

- Image your own hard drive
- Purchase a hard drive from eBay and analyze
- Analyze your cell phone

## Areas of active development

- Memory analysis

- Mobile device forensics
- Encrypted file systems

## References/Resources

- Books
  - File System Forensic Analysis by Brian Carrier
  - Windows Forensics: The Field Guide for Corporate Computer Investigations by Chad Steel
- Websites
  - Forensics Wiki - [http://www.forensicswiki.org/wiki/Main\\_Page](http://www.forensicswiki.org/wiki/Main_Page)
  - Forensic Incident Response - <http://forensicir.blogspot.com/>
  - Windows Incident Response - <http://windowsir.blogspot.com/>
  - The Electronic Evidence Information Center - <http://e-evidence.info/>
  - Computer Forensics, Malware Analysis & Digital Investigations - <http://www.forensickb.com/>
  - Forensic Focus - <http://www.forensicfocus.com/>