Forensic Data Acquisition

Some Key Issues in E-Discovery

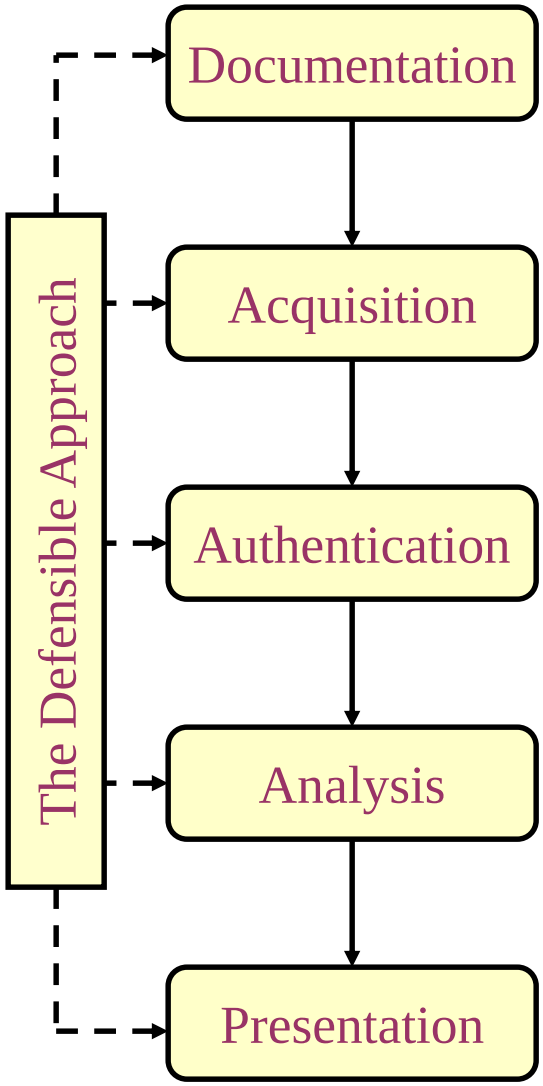
- What is admissible evidence?
- What is electronic evidence?
- Is electronic evidence admissible?
- Why pay the cost of collecting electronic evidence?
- How to preserve electronic evidence?
- What is a defensible approach?
- What is chain of custody?

Computer Forensics Procedure

- Verify Legal Authority
- Search warrants
- Photographing
- Documentation

- Hash verification
- CRC/MD5/SHA1
- Documentation

- Interpret and report
- Present and defend

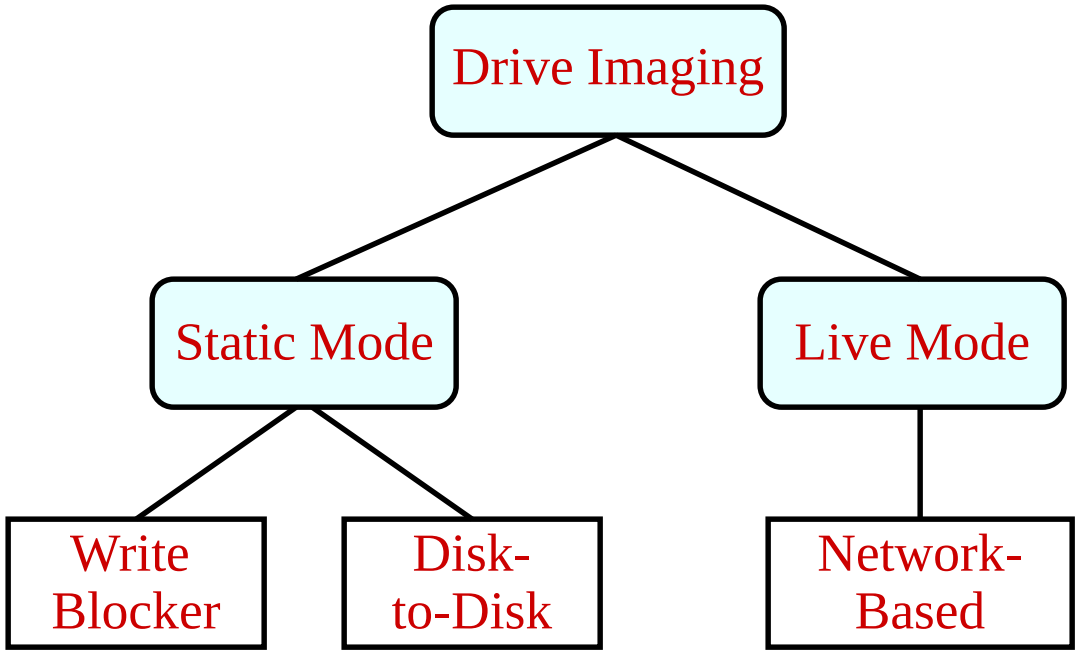


- Location, date, time, witnesses
- System information, status
- Physical evidence collected

- Forensically wipe storage drive
- Bit-stream Imaging
- Documentation
- **Chain of custody**

- Retain the integrity
- Filtering out irrelevant data
- What could/could not have happened
- Be objective and unbiased
- Documentation

Drive Imaging



- Integrity
- Time
- Interrupt Operations
- Equipment
- Personnel

- System is off
- Trusted environment
- Nonvolatile data
- Postmortem analysis

- System is on
- Untrusted environment
- Volatile data
- Hacker attacking

Imaging: Disk to Disk

Step 1:

- Assumes the scene and system have been properly secured.
- Remove suspect hard drive from suspect system
- Place the suspect drive in forensic system

or

- Connect power cable and ribbon from forensic computer to suspect drive

Step 2:

- Boot the forensic computer
- Ensure that the suspect drive is recognized
- Start the forensic tool

Imaging: Disk to Disk

Step 3:

- Create bitstream image of the suspect drive

Step 4:

- Ensure integrity of source and image (MD5)

Step 5:

- Disconnect suspect drive
- Shut down forensic computer
- Make detailed notes

Imaging – Network based

Step 1:

- Connect cross over cable or hub to suspect & forensic computers
- Boot suspect system from forensic boot disk
- Start up the forensic computer
- Set IP addresses for both systems
  - ifconfig eth0 10.1.1.2 netmask 255.255.255.0
  - ifconfig eth0 10.1.1.3 netmask 255.255.255.0
- Ping the one system to ensure connectivity
- Verify the date & time reported on the suspect & forensic systems

Imaging – Network based

Step 2:

- Listening host (MFS) run netcat in listening mode
  - nc –l –p 10000 > /forensics/images/case1.dd
  - -l = listening mode
  - -p = port address
  - > pipes the input to the specified file
- Suspect Host
  - **dd bs=1024 < /dev/hda1 | nc 10.1.1.3 10000 –w 3**
  - Run dd set block size to 1024
  - Pipe the dd input (/dev/hda1) through netcat to the ip address 192.168.1.2 on port 10000

Imaging – Network based

Step 3:

- Ensure integrity of source and image (md5sum)
- Hash totals should match

Step 4:

- Shut down the forensic and the suspect system
- Remove forensic boot disk
- Disconnect cables etc.
- Make detailed notes.

Drive Imaging – Live System

- Assumptions for our example
  - Suspect system is a UNIX filesystem
- Document everything!
- Use statically linked binaries
  - Diskette, CD-ROM
  - http://www.incident-response.org/irtoolkits.htm
- Tools = dd & Netcat

Tools - Netcat

- Designed in 1995 as a network debugging tool
- Some of the features of netcat are:
  - Outbound or inbound connections, TCP or UDP, to or from any ports
  - Full DNS forward/reverse checking, with appropriate warnings
  - Ability to use any local source port
  - Ability to use any locally-configured network source address
  - Built-in port-scanning capabilities, with randomizer
  - Built-in loose source-routing capability
  - Can read command line arguments from standard input
  - Slow-send mode, one line every N seconds
  - Optional ability to let another program service inbound connections

Drive Imaging – Live System

Step 1:

- Connect cross over cable or hub to suspect & MFS
- Start up the MFS
- Set IP addresses for both systems
  - ifconfig eth0 10.1.1.2 netmask 255.255.255.0
  - ifconfig eth0 10.1.1.3 netmask 255.255.255.0
- Ping the one system to ensure connectivity
- Verify the date & time reported on the suspect & MFS systems (Why is this NB)
- Mount CD with statically linked binaries
  - #/mount /dev/hdc /mnt

Drive Imaging – Live System

Step 2

- Use netcat & dd to image systems
- Netcat syntax:
  - Listening host (system we are going to store the image on)
    - nc –l -p 10000 > /forensics/images/case1.dd
    - -l = listening mode
    - -p = port address
    - > pipes the input to the specified file
  - Suspect host (system we want to image)
    - From the CDROM!
    - nc <ip address of listening host> <port number> -w 3
    - nc 10.1.1.3 10000 –w 3
    - -w is timeout value (in our example 3 seconds)

Drive Imaging – Live System

- Combining Netcat & dd
  - Listening host
    - nc –l -p 10000 > /forensics/images/case1.dd
  - Suspect host
    - **dd bs=1024 < /dev/hda1 | nc 10.1.1.3 10000 –w 3**
      - Run dd set block size to 1024
      - Pipe the dd input (/dev/hda1) through netcat to the ip address 10.1.1.3 on port 10000
      - If no data transmitted for 3 seconds then end the process
  - Our suspect image is now safely on our system and is called case1.dd

Drive Imaging – Live System

- Step 3
  - Ensure integrity of source and image (md5sum)
  - Hash totals should match
- Step 4
  - Shut down the MFS
  - Disconnect cables etc.
  - Make detailed notes.

Summary

- Acquiring an exact copy of the suspect media is difficult. Bitstream copies are acceptable as long as you can demonstrate the integrity of the images.
- Acquiring digital evidence should adhere to the second principle of digital forensics (actions should be taken not to change the evidence)
- There are several open source tools that can be used
- If possible avoid obtaining a image from a live system.
- Be conscious of volatile data on live systems

Summary

- Use a forensic boot disk
- Make detailed notes as the procedures you follow need to be both auditable and replicable.
- Test and validate all tools on a known system
- Re-test after upgrading to newer version
- Conduct "Before and After" comparisons
- Be prepared to testify to your methodology