Chapter 7

Forensic Duplication

Ed Crowley

Spring 10

Topics

- Response Strategies
- Forensic Duplicates and Evidence
- Federal Rules of Evidence
- What is a Forensic Duplicate?
- Hard Drive Development
- Forensic Tool Development
- Evidence Rules – Case Law
- Safeback

Response Strategy

- Decision of when to perform a forensic duplication based is based, in part, on existing response strategy for the instant situation.
  - For example, many organizations have a policy of creating forensic HD duplicates of all PCs used by executives that leave the organization.

Forensic Duplicates as Admissible Evidence

- Existing legal standards define minimum criteria for an item to be admitted into evidence.
  - Collection process usually under scrutiny as well.

Federal Rules of Evidence

Federal Rules of Evidence (FRE) 1002 state that the item or information presented in court must be the original.

Exceptions: Definitions and Duplicates

- If data are stored by computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.

Admissibility of Duplicates

- A duplicate is admissible to the same extent as an original unless:
  - A genuine question is raised as to the authenticity of the original, or
  - In the circumstances it would be unfair to admit the duplicate in lieu of the original

What is a Forensic Duplicate?

- A file that contains every bit of information from the source in a raw bitstream format.

Tools that create forensic duplicates:

1. dd
2. FTK Imager, Access Data
3. Dfcldd, US DOD Computer Forensics Lab version of the dd comand.

Qualified Forensic Duplicate?

- A file that contains every bit of information from the source, but may be stored in a altered form.
- Tools that create qualified forensic duplicate output files:
  1. SafeBack
  2. EnCase
  3. FTK Imager

Restored Image

- A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium.
- Mismatched drive geometries can cause problems.
  - For example, partition table or mbr problems

HD Development

- When hard drives grew beyond 512MB, the PC-BIOS needed to be updated (to recognize larger drives).
  - …software emulated a modern BIOS.
  - Software pushed all of the real data on the drive down one sector and stored its program and information in sector 2.
  - The real partition table would be at cylinder 0, head 0, sector2.
- Safeback, EnCase, FTK Imager, and dd will create a restored image from the qualified forensic duplicate.
- EnCase and dd images may not need to be restored.
  - Treat images as virtual disks, eliminating the need for restoration.
  - Note, FTK Imager can create images in the EnCase Format.

Mirror Image

- Created from hardware that does at bit for bit copy from one hard drive to another.
  - Requires two identical hard drives
- Doesn’t happen very often.

Tool Requirements: Forensic Duplication

Tool must:

- Create a forensic duplicate or mirror image of the original.
- Handle read errors in a robust and graceful manner.
- Not make any changes to source medium.
- Capable of scientific and peer review.
- Results must be third party repeatable and verifiable.

Legal Issues

- Tools used for forensic duplication must pass the legal tests for reliability.
- Note, when tool is generally accepted by others in the field, it is easier to prove that information was gathered in a reliable, accurate manner.

Frye and Daubert

- 1923, Federal Court decided on set of evidence standards called the Frye test.
- 1993, Daubert v. Merrell Dow Pharmaceuticals shifted the focus from a test for general acceptance to a test of “reliability and relevance”.
  - Lead to the Daubert Criteria

Four Daubert Factors

1. Has scientific theory or technique been empirically tested?
2. Has scientific theory or technique been subjected to peer review and publication?
3. Is there a known or potential error rate?
   - Do standards exist that control the technique's operation?
4. Is there a general acceptance of the methodology or technique in the relevant scientific community?

Kumho Tire v. Carmichael

- Found that the tests set forth in the Daubert standard were insufficient for testing cases where the methodology was not formed on a scientific framework.

Additional Kumho Tests

- Has the technique been created for a purpose other than litigation?
- Does the expert sufficiently explain important empirical data?
- Is the technique based on qualitatively sufficient data?
- Is there a measure of consistency to the technique's:
  1. Process or methods?
  2. Process or methods as applied to the current case?
- Is the technique represented in a body of literature?
- Does the expert possess adequate credentials in the field?
- How did the technique used differ from other similar approaches?

Creating a Forensic Duplicate of a Hard Drive

- dd, part of the GNU software suite.
- dcfldd, from the DOD
- dd utility the most reliable tool for creating a true forensic duplicate image.
- Dd a tool that you should be intimately familiar with before you need to use it on a real investigation.

Process

- Creating Linux boot media
- Start with a precompiled version of Linux.
- Once you have the basic package up and running, disassemble the packages and add your own binaries, such as dcfldd.
- In certain situations, duplications will be stored in a series of files that are sized to fit on a particular media type (such as CDs or DVDs) or file system type (such as files under 2.1 GB).
  - Called a segmented image.
  - Most commercial forensic packages have the ability to process segmented images.

Creating A Qualified Forensic Duplicate

- Never boot from evidence drive.
- In preparation, create a bootable disk
- To prevent compressed disks from loading and changing time stamps, disable the DRVSPACE.BIN driver file
- Hack IO.SYS
  - 4 instances need to be changed

SafeBack

- SafeBack, a small application that is designed to run from a DOS boot floppy
  - Requires a clean DOS environment ready on a boot floppy.
  - Offered by New Technologies Inc. (NTI)

SafeBack

Four operating modes

- Backup function
  - Produces a forensically sound image file for the source media.
- Restore function
  - Restores forensically sound image files.
- Verify function
  - Verifies the checksum values within an image file.
- Copy function
  - Performs the Backup and Restore operations in one action.

Safeback

- Text authors prefer to use the Backup function to create an image file for creating a qualified forensic duplicate.
- SafeBack includes a logging function that records options used for each session.

Questions?

Chapter 8

Collecting Network-based Evidence

Ed Crowley

Spring 10

Topics

- Intro
- Network Monitoring Goals
- Types of Network Monitoring
- Event Monitoring
- Trap and Trace Monitoring
- Full Monitoring
- Setting Up a Network Monitoring System
- Process
- Network Logs

Intro

- Network based evidence:
  1. Full content network monitoring or
  2. Interception of electronic communications.
- The challenge: Extracting meaningful results.
- Analysis of network based evidence includes:
  - Reconstructing network activity
  - Performing low level protocol analysis and
  - Interpreting network activity.

Network Monitoring Goals

- Confirm or dispel suspicions surrounding an incident.
  - Accumulate additional evidence and information
  - Verify that there is a compromise
    - Establish incident's scope.
  - Determine network events timeline
  - Identify any additional involved parties.
- Ensure compliance with a desired activity or policy.

Three Types of Network Monitoring

- Event monitoring
- Trap and trace monitoring
- Full content monitoring

Event Monitoring

- Events are indicators (alerts) that something has occurred.
  - Based on pre-established monitoring rules or thresholds.
- Generated traditionally by IDS
  - Such as Snort.

Trap and Trace Monitoring

- Noncontent monitoring
  - Records session or transaction data
  - Network activity summary.
- Law enforcement refers to such noncontent monitoring as a pen register or a “trap and trace”.
  - Typically, includes header info i.e.
    - Protocol
    - IP address
    - Ports
      - May include flags

Full Content Monitoring

- Yields data including raw packets.
- Includes both header and data

Setting up a Network Monitoring System

Special purpose tools include

- Hardware and software based network diagnostic tools
- IDS sensors
- Packet capture utilities.

- Network diagnostic and troubleshooting tools have several drawbacks that make them unsuitable for performing network surveillance.
  - Including lack of remote management capabilities and proper storage space

Process

1. Determine network surveillance goals.
2. Ensure that you have proper standing to perform monitoring.
3. Acquire and implement proper hardware and software.
4. Ensure platform security, both electronically and physically.
5. Ensure appropriate placement of the network monitor.
6. Evaluate network monitor.

Sample Goals

- Observe traffic to and from a specific host.
  - Reconstruct communications
- Monitor traffic to and from a specific network
- Monitor a specific user's digital actions.
- Verify intrusion attempts.
- Look for specific attack signatures.
- Focus on a specific protocol.

Make sure that policies in place support instant goals.

Choosing Appropriate Hardware

- Organizations with small budgets need to rely on homegrown solutions.
  - Can be customized for situation.
  - CPU, RAM, and HD define potential
- Historically, consultants used laptops for network monitors

Choosing Appropriate Software

Factors include:

- Host O/S?
- Remote access?
- Sniffer desired?
- Portability for capture files?
- Skill levels of operator?
- How much data moves across the network?

Operating System

- Monitoring platform needs to have all applications and processes not essential to the operation of the operating system, sniffer, and administrative functions removed.

Desirable characteristics

- Robust TCP/IP stack
- Secure, remote access (SSH)
- Ability to run on many types of hardware

Other Factors

- Remote Access

Silent Sniffers

- A silent sniffer is a system that will not respond to any packets it receives
- If you don’t disable system from responding to ARP packets, your monitor may be detected.
  - One option, a one way Ethernet Cable i.e. clipped transmit wire

Other Factors

- Data File Formats
- Choosing software that creates files in an open standard format saves many potential headaches.

Network Monitor Deployment

- Modern switches SPAN feature (switched port analysis) allows one switch port to transmit all frames, regardless of whether the switch has detected the presence of the destination address on that port.

Trap and Trace

- Used to capture network noncontent data.
  - Aka pen register
  - Monitors the IP and TCP headers (or other transport layer protocol header), without monitoring any packet data.
  - Extremely helpful in DOS cases
- TCPDump or WinDump can be useful

Trap and Trace Analysis

- When performing a trap and trace, it is simpler to create a permanent output file than it is to view the data live on the console.

Full Content Monitoring

- Simplest way to implement filtering is TCPdump
  - Relies on building Berkeley Packet Filters.
- Two aspects that merit attention:
  1. File naming
  2. File integrity.
- Perform MD5 or SHA hashing of full content data files.

Collecting Network Based Log Files

- Routers, firewalls, servers IDS sensors
- DHCP servers
- Modern firewalls
- IDS sensor may catch a portion of an attack due to a signature recognition or anomaly detection filter
- Host based sensors may detect the alteration of a system library or the addition of a file in a sensitive location

Network Logs

- Remote network logs may be more secure than local logs.

Questions?