DIGITAL EVIDENCE LOCATIONS & COMPUTER FORENSICS INTRODUCTION

Professor Donald R. Mason

OBJECTIVES:

After this session, you will be able to:
1. Define “digital evidence” and identify types;
2. Describe how digital evidence is stored in computers;
3. Identify devices and locations where digital evidence may be found;
4. Define basic computer and digital forensics; and
5. Identify and describe the essential principles, tools and trends in digital forensics

REQUIRED READING:

Donald R. Mason, Digital Evidence Locations & Introduction to Computer Forensics (Jan. 2011) [NCJRL PowerPoint] ........................................................................................................................................1
Digital Evidence Locations & Introduction to Computer Forensics

Don Mason
Associate Director

Objectives

After this session, you will be able to:

- Define “digital evidence” and identify types
- Describe how digital evidence is stored in computers
- Identify devices and locations where digital evidence may be found
- Define basic computer and digital forensics
- Identify and describe the essential principles, tools and trends in digital forensics

Special Acknowledgments

- Justin T. Fitzsimmons
  Senior Attorney, NDAA National Center for Prosecution of Child Abuse
- Sergeant Josh Moulin
  Commander, Southern Oregon High-Tech Crimes Task Force
Advancing Technology

Computer / Digital Technology
- Personal computers, at work and at home
- Digital cameras
- Webcams
- Camera and video cam cell phones
- Document and image scanners
- Digital recording and duplicating devices
- Large digital storage capacities
- Portable media

How Digital Data is Stored
- Data is written in binary code – 1’s and 0’s
- These 1’s and 0’s are grouped together in blocks of 8, called “bytes.”
- For example, the sequence “10001111” represents the letter “O”.

Digital Evidence Locations: Computer Forensics Introduction
Handling Child Pornography Cases, February 17-18, 2011
Copyright © 2011 National Center for Justice and the Rule of Law – All Rights Reserved
Digital Evidence
Information of probative value that is stored or transmitted in binary form and may be relied upon in court.

Information stored in binary format but convertible to:
- e-mail, chat logs, documents
- photographs (including video)
- user shortcuts, filenames
- web activity logs

Easily modified, corrupted, or erased
Correctly made copies indistinguishable from original

User-created
- Text (documents, e-mail, chats, IM's)
- Address books
- Bookmarks
- Databases
- Images (photos, drawings, diagrams)
- Video and sound files
- Web pages
- Service provider account subscriber records
Digital Evidence

- Computer-created
  - Dialing, routing, addressing, signaling info
  - Email headers
  - Metadata
  - Logs, logs, logs
  - Browser cache, history, cookies
  - Backup and registry files
  - Configuration files
  - Printer spool files
  - Swap files and other "transient" data
  - Surveillance tapes, recordings

Forms of Evidence

- Files
  - Present / Active (doc's, spreadsheets, images, email, etc.)
  - Archive (including as backups)
  - Deleted (in slack and unallocated space)
  - Temporary (cache, print records, internet usage records, etc.)
  - Encrypted or otherwise hidden
  - Compressed or corrupted

- Fragments of Files
  - Paragraphs
  - Sentences
  - Words

Sources of Evidence

- Offender’s computer
  - accessed and downloaded images
  - user log files
  - Internet connection logs
  - browser history and cache files
  - email and chat logs

- Hand-held devices (embedded computer systems)
  - digital cameras
  - PDAs
  - mobile phones
More Sources of Evidence

- Servers
  - ISP authentication user logs
  - FTP and Web server access logs
  - Email server user logs
  - LAN server logs
- Online activity
  - IP addresses of chat room contributors

Digital Devices / Locations Where Digital Evidence May be Found

Computer Hardware
And Still More

More

More
Evidence Containers?

More Containers
Computer Forensics

- “Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis”
- Usually pre-defined procedures followed but flexibility is necessary as the unusual will be encountered
- Was largely “post-mortem” but is evolving

What’s on His Hard Drive?

How Data is Stored

Track
Sector
Clusters are groups of sectors
Digital Knowledge and Intent Evidence

- Evidence that the CP files were purposely collected
  - CP found in computer’s allocated space?
  - In folders assigned to particular “user” of the computer?
  - Files organized, given relevant folder/file titles?
  - Default settings of the computer’s software changed?

- Evidence that CP was obtained via Web browsing
  - Evidence in the Index.dat files of web searches for CP?
  - CP found in the Temporary Internet Files?
  - Any CP-related Bookmarks/Favorites saved?

- Evidence that the CP was viewed by a user
  - Any Recent Files/Link Files to the CP?
  - Windows Registry list other devices (scanners, thumb drives, etc.) recently connected to the computer?
  - Any Thumbs.db files containing CP?
  - Any CP videos listed in Windows Media Player/Real Player histories?

Computer/Digital Forensics

- Sub branches / activities / steps
  - Computer forensics
  - Network forensics
  - Live forensics
  - Software forensics
  - Mobile device forensics
  - “Browser” forensics
  - “Triage” forensics

Basic Computer Forensics

- **Seizing** computer evidence
  - bagging & tagging
- **Imaging** seized materials
- **Searching** the image for evidence
- **Presenting** digital evidence in court

Digital Evidence Locations; Computer Forensics Introduction
Handling Child Pornography Cases, February 17-18, 2011
Copyright © 2011 National Center for Justice and the Rule of Law – All Rights Reserved
Basic steps – 3 A’s

- Acquiring evidence without altering or damaging original
- Authenticating acquired evidence by showing it’s identical to data originally seized
- Analyzing the evidence without modifying it

Myth v. Fact

**Myth**
- A computer forensic analyst can recover any file that was ever deleted on a computer since it was built.

**Fact**
- The analyst can recover a deleted file, or parts of it, from unallocated file space until the file system writes a new file or data over it.

Myth v. Fact

**Myth**
- Metadata ("data about data") is the all knowing, all seeing, end all piece of info on a file.

**Fact**
- Metadata does contain useful information about a file but it is limited.
  - E.g.:
    - Author
    - MAC times
    - File name, size, location
    - File properties
    - Might contain revisions, comments, etc.
EXIF Data

- Exchangeable Image File Format
- Embeds data into images containing camera information, date and time, and more

Acquiring the Evidence

- Seizing the computer: Bag and Tag
- Handling computer evidence carefully
  - Chain of custody
  - Evidence collection
  - Evidence identification
  - Transportation
  - Storage
- Making at least two images of each evidence container
  - Perhaps third in criminal case – for discovery
- Documenting, Documenting, Documenting

Preserving Digital Evidence

The “Forensic Image” or “Duplicate”

A virtual “snapshot” of the entire drive
- Every bit & byte
- “Erased” & reformatted data
- Data in “slack” & unallocated space
- Virtual memory data
Write Blockers

Hard drives are imaged using hardware write blockers

Authenticated the evidence

- Proving that evidence to be analyzed is exactly the same as what suspect/party left behind
  - Readable text and pictures don’t magically appear at random
  - Calculating hash values for the original evidence and the images/duplicates
    - MD5 (Message-Digest algorithm 5)
    - SHA (Secure Hash Algorithm) (NSA/NIST)

What is a Hash Value?

An MD5 Hash is a 32 character string that looks like:

Acquisition Hash:
3FDSJO90UI43IJVJU904FRBEWH

Verification Hash:
3FDSJO90UI43IJVJU904FRBEWH

The Chances of two different inputs producing the same MD5 Hash is greater than:

1 in 340 Unidecillion: or 1 in 340,000,000,000,000,000,000,000,000,000,000,000,000,000
Hashing Tools – Examples

- http://www.fileformat.info/tool/md5sum.htm

- Also, AccessData’s FTK Imager can be downloaded free at http://www.accessdata.com/downloads.html

MD5 Hash

- 128-bit (16-byte) message digest – a sequence of 32 characters
- “The quick brown fox jumps over the lazy dog”
  9e107d9d372bb6826bd81d3542a419d6
- “The quick brown fox jumps over the lazy dog.”
  e4d909c290d0fb1ca068ffaddf22cb0


More Examples of Hash Values
What Happens When You Rename a File?
Or Rename the Extension

“Hashing” an Image

MD5 021509c96bc7a547718950e78a7a371
SHA1 77fe03b07c0063cf35dc268b19f5a449e5a97386

(single pixel changed using Paint program)

MD5 ea8450e5e8cf1a17c6effc965b484
SHA1 01f57f330fb06c16d5872f5c1decdf6b88b69cbbc
Analyzing the evidence

- Working on bit-stream images of the evidence; never the original
  - Prevents damaging original evidence
  - Two backups of the evidence
    - One to work on
    - One to copy from if working copy altered
- Analyzing everything
  - Clues may be found in areas or files seemingly unrelated

Popular Automated Tools

Encase
Guidance Software

Forensic Tool Kit (FTK)
Access Data

Validation of Computer Forensics Tools

Subjecting EnCase to Daubert analysis
1. Subject to testing criteria
   - Lab-specific testing
2. Subject to peer review and publication
   - Featured in a number of articles and forensics/incident response books
3. High known or potential rate of error?
Validation of Computer Forensics Tools

4. General acceptance within the scientific community

Case law/judicial notice of prior Daubert hearings in other jurisdictions

Use in law enforcement and corporate/private sectors
Taught in academic institutions

EnCase and Legal Challenges


Analysis (cont.)

- Existing Files
  - Mislabeled
  - Hidden
- Deleted Files
  - Trash Bin
  - Show up in directory listing with σ in place of first letter
    - "taxes.xls" appears as "@axes.xls"
- Free Space
- Slack Space
- Swap Space
Free Space

- Currently unoccupied, or “unallocated” space
- May have held information before
- Valuable source of data
  - Files that have been deleted
  - Files that have been moved during defragmentation
  - Old virtual memory

Slack Space

- Space not occupied by an active file, but not available for use by the operating system
- Every file in a computer fills a minimum amount of space
  - In some old computers, this is one kilobyte, or 1,024 bytes. In most new computers, this is 32 kilobytes, or 32,768 bytes
  - If you have a file 2,000 bytes long, everything after the 2000th byte is slack space

How “Slack” Is Generated

Slack space: the area between the end of the file and the end of the storage unit
Recall How Data is Stored

Other Sources Mined for Transient Data
- Browser cache, history, cookies
- Residual chat data
- Activity logs
- Registry & registry backup files

Sources of Digital Gold
- Internet History
- Temp Files (cache, cookies etc...)
- Slack/Unallocated space
- Buddy Lists, chat room records, personal profiles, etc...
- News Groups, club listings, postings
- Settings, file names, storage dates
- Metadata (email header information)
- Software/Hardware added
- File Sharing ability
- Email
Selected “Trends” in Digital Forensics

“Browser” Forensics

“Triage” Forensics

Browser Forensics

Web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox, Safari, Opera) maintain histories of recent activity, even if not web related.

Internet History

- Computers store Internet history in a number of locations including:
  - Temporary Internet files
  - Windows Registry
  - Browser / Search Term history
  - Cookies
- This information is browser specific
“Triage” Forensics
- “Rolling” forensics, or “on-site preview”
- Image scan
- Especially useful in “knock & talk” consent situations, screening multiple computers to determine which to seize, or probation or parole monitoring
- Not all agencies equipped or trained yet to do this.

“Triage” Forensics
- Increasingly important, as the number and storage capacities of devices rapidly grow.
- But does NOT enable a comprehensive forensically sound examination of any device on the scene.
- “When is enough enough?”

Evolving Tools
“Triage” Forensics - Steps

- Attach/Install write-blocking equipment
- Turn on target device
- Scan for file extensions, such as:
  - .doc
  - .jpg (.jpeg)
  - .mpg (.mpeg)
  - .avi
  - .wmv
  - .bmp

“Triage” Forensics - Steps

- Pull up thumbnail views - 10-96 images at a time
  - Right click on image, save to CD or separate drive.
- Determine file structure or file path.

Resources

- https://blogs.sans.org/computer-forensics/
- http://craigball.com/
Questions?

662-915-6898
drmason@olemiss.edu
www.ncjrl.org