Objectives

After this session, you will be able to:

- Define and describe "digital evidence"
- Identify devices and locations where digital evidence may be found
- Identify and describe the basic principles, practices, and tools of digital forensics
- Describe selected trends and challenges in digital forensics

From the “old days” to …
Evolving technology in ...

The "Digital age" with ...

"Computers"?

"Portal Devices"
Computers = Digital Devices

- A computer is like a light switch.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Computer</th>
<th>Binary Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>signal present</td>
<td>1</td>
</tr>
<tr>
<td>OFF</td>
<td>no signal present</td>
<td>0</td>
</tr>
</tbody>
</table>

- Each 0 or 1 is a BIT (for BINARY DIGIT): 00000001 = 1, 0000010 = 2 (2+0), 0000011 = 3 (2+1).

- An 8-bit sequence = 1 byte = a keystroke: 01000001 = A

Roles of Digital Devices

- Computer as Target
  - Unauthorized access, damage, theft
  - Spam, viruses, worms
  - Denial of service attacks

- Computer as Tool
  - Fraud
  - Threats, harassment
  - Child exploitation

- Computer as Container
  - From drug dealer records to how to commit murder

Challenges

- Increasing ubiquity and convergence of digital devices
- Increasing data storage capacity
- Shrinking devices and media
- Growing use of solid state devices
### Digital Evidence

- Information of probative value that is stored or transmitted in binary form and may be relied upon in court

- **Two types**

<table>
<thead>
<tr>
<th>User-created</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Text (documents, e-mail, chats, IM’s)</td>
</tr>
<tr>
<td>- Address books</td>
</tr>
<tr>
<td>- Bookmarks</td>
</tr>
<tr>
<td>- Databases</td>
</tr>
<tr>
<td>- Images (photos, drawings, diagrams)</td>
</tr>
<tr>
<td>- Video and sound files</td>
</tr>
<tr>
<td>- Web pages</td>
</tr>
<tr>
<td>- Service provider account subscriber records</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer-created</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Email headers</td>
</tr>
<tr>
<td>- Metadata</td>
</tr>
<tr>
<td>- Activity logs</td>
</tr>
<tr>
<td>- Browser cache, history, cookies</td>
</tr>
<tr>
<td>- Backup and registry files</td>
</tr>
<tr>
<td>- Configuration files</td>
</tr>
<tr>
<td>- Printer spool files</td>
</tr>
<tr>
<td>- Swap files and other “transient” data</td>
</tr>
<tr>
<td>- Surveillance tapes, recordings</td>
</tr>
</tbody>
</table>
Sources of Evidence

- Offender’s computer
  - accessed and downloaded images
  - documents
  - chat sessions
  - user log files
  - Internet connection logs
  - browser history and cache files
  - email and chat logs
  - passwords & encryption keys

Sources of Evidence

- Servers
  - Internet Protocol addresses
  - ISP authentication user logs
  - FTP and Web server access logs
  - Email server user logs
  - Subscriber account information
  - LAN server logs
  - “Cloud” storage
  - Web pages
  - Social media

Data Generated in 2010

- 1200 trillion gigabytes (1.2 zettabytes)
- 89 stacks of books each reaching from the Earth to the Sun
- 22 million times all the books ever written
- Would need more than 750 million iPods to hold it
- 107 trillion emails sent in 2010
Projection

- In 2020: 35 zettabytes will be produced
  - All words ever spoken by human beings, written 7 times

How Much in Real Cases?

- One recent example:
  - 17 terabytes
  - 24+ million images
  - 17,000 movies
  - 4600+ CVIP hits (known CP images)

"inside the box, outside the box"
Inside the Box
What the computer owner actually has possession of
- Computer’s hard drive and other memory
  - Documents
  - Pictures
  - Outlook Emails
  - Internet Cache
- CD’s and floppy disks
- iPods
- Cell Phones
- External Hard Drives

Inside the Box
What the computer owner actually has possession of

Outside the Box
What is not stored on the owner’s computer
- Online Email Accounts (Gmail and Yahoo)
- Internet Shopping Accounts
- Social Networking Accounts
- Backups of text messages
- Cell Site Location Data
- Using Pen/Trap for Internet “DRAS” information
- Subscriber account records
- Contents of Websites
Outside the Box
What is not stored on the owner's computer

Variety of “Boxes”
More

More

More
More

Vehicle “black boxes”
- Event data recorders
- Sensing and diagnostic modules
- Data loggers
Computer Forensics

Or “Digital Forensics”

Computer Forensics

- Obtaining,
- Processing,
- Authenticating, and
- Producing
digital data/records for legal proceedings.

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 headers; EXIF data; etc.)
- Software/hardware added
- File sharing ability
- Email
Digital Knowledge & 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? (Win XP)
  - Any CP videos listed in Windows Media Player/Real Player histories?

Computer Forensics

- Usually pre-defined procedures followed but flexibility necessary
- Was largely "post-mortem"
  - "What's on the hard drive?"
  - AKA "dead box" forensics
- Rapidly evolving
  - Ex:
    - From "Cut the power immediately" to "Don’t power down before you know what’s on it"

Popular Automated Tools

- Encase
- Guidance Software
- Forensic Tool Kit (FTK)
- Access Data
Skills / Expertise Required
- Technical
  - Data processing and production
- Investigative
  - Understanding computer evidence
  - Building a case
- Legal
  - Maintaining chain of custody
  - Managing digital evidence per the rules

Certifications
- Various offered
  - IACIS's "CFCE"
  - Guidance Software’s “Encase CE”
  - ISFCE’s “CCE”
- Some states require P.I. licenses
- Growing number of schools offering certificate and degree programs
- But no uniform, accepted standards

Branches, Trends
- Network forensics
- "Live" forensics
- "Remote" forensics
- Software forensics
- Image forensics
- "Browser" forensics
- "Triage" forensics
- Mobile device forensics
Basic Steps

Acquiring (and preserving) evidence without altering or damaging original data

Authenticating acquired evidence by showing it’s same as data seized

Analyzing (searching) the evidence without modifying it

Acquiring the Evidence

- “Forensically sound manner”
- Securing and seizing computer (“bag and tag”)
- Handling computer evidence carefully
  - Chain of custody
  - Evidence identification
  - Evidence collection (including volatile memory)
  - Transportation
  - Storage
- Making at least two images of each container
- Documenting all steps

Preserving Digital Evidence

The “Forensic Image” or “Duplicate”

A virtual “clone” of the entire drive

- Every bit & byte
- “Erased” & reformatted data
- Data in “slack” & unallocated space
- Virtual memory data
Authenticating the Evidence

- Proving evidence to be analyzed / offered is exactly same as what was seized
  - 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)

MD5 Hash

- 128-bit (16-byte) message digest – a sequence of 32 characters
- Analogous to a file’s “fingerprint” or DNA
- Like a unique file name

Basic illustration:

“The quick brown fox jumps over the lazy dog”
9e107d9d372bb6826bd81d3542a419d6

“The quick brown fox jumps over the lazy dog.”
e4d909c290d0fb1ca068ffaddf22cbd0
“Hashing” Data Sets

MD5 Hash values:

Acquisition Hash: 3FDSJO90U43JIVJU904FRBEWH
Verification Hash: 3FDSJO90U43JIVJU904FRBEWH

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

“Hashing” an Image

<table>
<thead>
<tr>
<th>MD5</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>021509c96bc7a6a477f18950e78e7a371</td>
<td>77fe03b07c0063cf55dc268b19f5a449e5a97386</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MD5</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ea8450e58cf1a1c17c6effccdd95b484</td>
<td>01f57f330f9b06c16d5872f5c1decdf6eb88b69c8c</td>
</tr>
</tbody>
</table>
Hashing Tools – Examples

- [http://www.fileformat.info/tool/md5sum.htm](http://www.fileformat.info/tool/md5sum.htm)

- Also, AccessData’s **FTK Imager** is downloadable free at [http://www.accessdata.com/downloads.html](http://www.accessdata.com/downloads.html)

Other Ways of Authenticating

- Witness with knowledge
- Process
- Chain of custody, etc.

- Prima facie showing, per Rule 901, that evidence is what it is purported to be

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
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

Analysis (cont’d)

- Present / Active Files
  - Mislabeled
  - Hidden

- Deleted Files
  - Trash Bin
  - Free (unallocated) and Slack 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
- *Logical* file vs. *Physical* space

How Data Is Stored
- Every file in a computer fills a minimum amount of space
  - In some old computers, one kilobyte (1,024 bytes). In newer computers, 32 KB (32,768 bytes).
  - If file is 2,000 bytes long, everything after the 2000th byte is slack space.
How Data Is Stored

Files are written to Clusters

- Each file may occupy more or less than full clusters
- May write to non-contiguous clusters

How “Slack” Is Generated

- File A (“Erased,” on disk)
- File B overwrites part of File A, creating slack
- Remains of File A (Slack)
- File B (Now on disk)
- File B saved to disk, on top of File A
- File B (Saved to disk)
- File B (Draft in RAM)

Slack space: The area between the end of the file and the end of the storage unit

Selected Developments in Digital Forensics

- “Triage” Forensics
- Mobile Device Forensics
“Triage” (or “Preview”) Forensics

“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?”
Tool Example: osTriage

- “Live response tool”
- Developed by F.B.I. SA
- Free to U.S. law enforcement
- Validated by F.B.I. November 2011
- 43 MB software package
- Run from USB storage (e.g., thumb drive or external hard drive)

osTriage – Reasons to Use

- Increasing use and ease of “virtualization”
  - May be multiple additional “computers”
- Increasing use of free & low cost encryption
- Loss of valuable info when computer is rebooted
- Loss of visibility of network storage
- Saves time

osTriage – Capabilities

- Display comprehensive details
  - User accounts
  - Physical and logical hard drives
  - Mapped networked drives
  - NIC information
  - Every USB device ever inserted into machine
  - Browser history
  - “Flash cookies”
  - Applications running (e.g., P2P or encryption)
**osTriage – Capabilities**

- Searches drives, finds images/videos, displays thumbnails
- Allows easy copying of contraband images, videos to USB storage device
- Compares images/videos to SHAs
- Checks files names against keyword list
- Has built-in image viewer
- Supports viewing EXIF data and thumbs.db

**osTriage – Capabilities**

- Extracts saved passwords
- Extracts list of recently opened files
- Writes nothing to computer being scanned
- Allows for custom searches
- Looks inside archives for key word filenames
- Gathers and saves volatile data before shutdown

**osTriage - Limitations**

- Cannot find and display data no longer there (e.g., cleared browser history)
- Doesn’t look for deleted files
- Doesn’t look at file headers to identify images or videos
- Does not substitute for full, forensically sound examination of device, if needed
Mobile Device Forensics
(or “Cell Phone Forensics”)

Mobile Device Forensics

- A whole different story
- Special challenges
  - Preventing loss of data
    - Stopping overwriting or wiping
    - Removing from network
    - Finding passwords and working around locks
  - Diversity of makers, models, hardware
    - Phones
    - SIM cards
    - Removable media

Mobile Device Forensics, cont’d

- Special challenges, cont’d
  - Diversity of platforms and operating systems
    - CDMA, GSM, et al.
    - iOS, Android, et al.
  - Array of diverse tools that don’t work the same with all devices
  - Data recovery may be via
    - Physical acquisition (write protection; “chip-off”)
    - Logical analysis (capturing active files, etc.)
    - Manual extraction (e.g., screen shots with camera)
Mobile Device Forensics

- Debate as to whether it’s “forensics” at all
- “Hashing” may not be possible
  - iPads or other tablet computers, thumb drives, or similar devices can be imaged, hashed, and analyzed with digital forensic tools
  - Many (or most) phones cannot
- Deleted data may not be recoverable

Mobile Device “Forensics”?

- Some advocate “cell phone data recovery”
- Not same as “computer forensics”
  - Working on original evidence
  - Writing to phone
  - Documenting steps and reasons perhaps even more important for authentication

Mobile Device “Forensics”?

- Others argue it’s still “forensics”
- Follows the “computer forensics” process
  - Identification
  - Preservation
  - Collection
  - Examination
  - Analysis
  - Reporting
Cell phone data that may be recoverable

- Contacts
- Recent call history
- Ringtones
- Apps
- Custom wallpapers
- Voice mail
- Text messages (SMS)
- Calendar
- Memos
- GPS info
- Multimedia (MMS) files
  - Audio
  - Images
  - Videos
- E-mail
- Browser history
- Chats
- Documents

Cell phone data that may be recoverable

- Depends on
  - Phone model
  - Service provider plans and capabilities
  - Acquisition tools
  - Analysis software

Mobile Device Forensics

- Final observations
  - Mobile devices increasingly important
  - Mobile devices contain wealth of probative information
  - Multiple tools must be used as needed
  - Results must often be verified manually
Questions?

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