Objectives

After this session, you will be able to:
- Define “digital evidence”
- Identify devices and locations where digital evidence may be found
- Recognize and utilize the basic practices, principles and tools of digital forensics
- Examine selected trends and challenges in computer forensics

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

The “Digital Age” with ...

“Computers”?
Computers = Digital Devices

- A computer is like a light switch
  - Switch  Computer       Binary Symbol
    ON        signal present    1
    OFF       no signal present 0

- Each 0 or 1 is a BIT (for BINARY DIGIT)
  - 00000001 = 1
  - 00000010 = 2 (2+0)
  - 00000011 = 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

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

Computer-created
- Email headers
- Metadata
- Activity logs
- Browser cache, history, cookies
- Backup and registry files
- Configuration files
- Printer spool files
- Swap files and other "transient" data
- Surveillance tapes, recordings
Internet Communications

- E-mail
- File transfer protocol (FTP)
- Bulletin and message board systems
- Newsgroups
- Chat rooms

Internet Communications

- Web sites
- Web cams
- E-groups
- Instant messaging
- Peer-to-Peer Networks

Internet Communities

- Interactive Internet communities
- Social networks
- Blogs
- Wikis
- Video or photo sharing sites
- Online role-playing games
- Virtual worlds
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

How Much in Real Cases?

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

Outside the Box
What is not stored in your computer
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

Variety of “Boxes”
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?
**Digital Knowledge & Intent Evidence (cont.)**

- 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?

**Digital Knowledge & Intent Evidence (cont.)**

- 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
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”

Captures
  - 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:**
3FDSJO90U43JJVJU904FRBEWH

**Verification Hash:**
3FDSJO90U43JJVJU904FRBEWH

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

“Hashing” an Image

<table>
<thead>
<tr>
<th>MD5</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ea8450e5e8cf1a1c17c6effccd95b484</td>
<td>01f57330f0b06c1d5872f5c1decefe8b8b9bcb</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MD5</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>021509c96bc7a6a47718950e78e7a371</td>
<td>77fe3b00c90063e5f35c266b19f5e449e5a97eb</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

- Tracks
- Sectors
- Clusters are groups of sectors

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 B (Draft in RAM) → File B saved to disk, on top of File A

File B (Saved to disk) → File B overwrites part of File A, creating slack

File B (Now on disk) → Remains of File A (Slack)

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

---

Selected Developments in Digital Forensics

---

The “Dead Box” Process

(1) Approach Computer
(2) Is it powered on?
(a) If no, continue process
(b) If yes, turn off computer

(3) Remove hard drive from target system
(4) Attach hard drive to forensic system
(5) Make imaged copy and analyze it

Digital Evidence and Computer Forensics
Copyright © 2013 National Center for Justice and the Rule of Law – All Rights Reserved 21
“Dead Box”Strengths

- Simple – clearly defined and straightforward stages of the acquisition, which can be verified at any time
- Reliable – no risk of altering / contaminating evidence as the data on the hard disk is not modified
- Thorough – analysis of every byte on the hard disk is acquired including unallocated, slack space and metadata

“Dead Box” Weaknesses

- Over-inclusive with data acquisition (can be invasive)
- Logistical problems with moving extensive amounts of computer equipment
- Encryption (an exact copy of an encrypted file is of no use)
- Increasing storage capacity of target devices
- Understanding that some evidence is lost by immediately powering down device
  - Decryption keys and network data may be stored as volatile data and lost when the computer is turned off

New Branches

- BROWSER FORENSICS
- NETWORK FORENSICS
- CLOUD FORENSICS
- TRIAGE FORENSICS
- COMPUTER FORENSICS
- LIVE FORENSICS
- IMAGE FORENSICS
- SOFTWARE FORENSICS
- REMOTE FORENSICS
"Live" Forensics

- a live analysis of programs on a suspect's computers to acquire RAM, unencrypted files, and other pertinent data
- Must stay within SW and minimize modified data
- Functions:
  - Determine if possible encryption;
  - Perform a live image of hard disks (limited guidelines though);
  - Assess the scope of the local network and identify other devices attached to the network
- Should be seen as an improvement to the process, not a total replacement of the traditional method

Live Forensics

- **Strengths:**
  - Avoids logistical problems: seizing a large number of devices for later analysis, which costs considerable resources
- **Weaknesses:**
  - Increasing target size
  - Difficulty in locating target (unidentified machines)
  - Analyzing drives of a large group of machines consumes considerable resources

"Triage" (or "Preview") Forensics
“Triage” Forensics

= a procedural model for the investigation of digital crime scenes including both traditional crime scenes and the more complex battlefield crime scenes

- AKA “rolling forensics” or “on-site preview forensics”
- Allows screening of multiple computers to determine which to seize or monitor

Triage Forensics

**Strengths:**
- Avoids the loss of valuable info that results from computer shutdown
- Saves time
- Increasingly important as the number and storage capabilities of devices grows
- Useful in consent situations

**Weaknesses:**
- Not all agencies are equipped or trained yet to do this
- Does not enable a comprehensive forensically sound examination

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”)*
Potentially recoverable data

- 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

Potentially recoverable data

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

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

- 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

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