Objectives

To be able to describe

- Evolving computer technology
- Increasing ubiquity of digital devices
- Types, sources, and volume of digital data
- Challenges in combating cyber crime
- The fundamentals of computer forensics
Crime Scene – Evidence?
Advancing Technology
Advancing Technology
Advancing Technology
Advancing Technology
Advancing Technology
Computer / Digital Technology

- Personal computers, at work and at home
- Digital cameras
- Web cams
- Camera and video cam cell phones
- Document and image scanners
- Digital recording and duplicating devices
- Large digital storage capacities
- Portable media
New crimes, New techniques

computer as *Target*

* unauthorized access, damage, theft
* spam, viruses, worms
* denial of service attacks

computer as *Tool*

* fraud
* threats, harassment
* child pornography

computer as *Container*

* from drug dealer records to how to commit murder
Murder!

- studied currents
- researched bodies of water
  - including San Fran Bay
- how to make cement anchors
- tide charts

had 5 home computers
“Cyber Crime”

“Computer crime”
“Network crime”
“Computer-related crime”
“Computer-facilitated crime”
“High tech crime”
“Internet crime” or “Online crime”
“Information age crime”

Any crime in which a computer or other digital device plays a role, and thus involves digital evidence
Digital Evidence

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

- 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
The Internet

- World Wide Web (the Web)
- E-mail
- Instant messaging (IM)
- Webcam/ Internet Telephone (VoIP)
- Peer-to-peer (P2P) networks

Legacy Systems
- Newsgroups
- Telnet and File transfer (FTP) sites
- Internet Relay Chat (IRC)
- Bulletin boards
Computer & Internet Uses

- Remote Computing
- Research
- Commerce
- Recreation
- Communication
Data Generated in 2006*

- 161 billion gigabytes (161 exabytes)
- 12 stacks of books each reaching from the Earth to the Sun
- 3 million times all the books ever written
- Would need more than 2 billion iPods to hold it

*According to report by technology research firm IDC
How Much Data?

- **1 Byte** (8 bits): A single character
- **1 Kilobyte** (1,000 bytes): A paragraph
- **1 Megabyte** (1,000 KB): A small book
- **1 Gigabyte** (1,000 MB): 10 yards of shelved books
- **1 Terabyte** (1,000 GB): 1,000 copies of Encyclopedia
- **1 Petabyte** (1,000 TB): 20 million four-door filing cabinets of text
- **1 Exabyte** (1,000 PB)
  - 5 EB: All words ever spoken by humans
Digital Evidence

User-created

- Text (documents, e-mail, chats, instant messages)
- Address books
- Bookmarks
- Databases
- Images (photos, drawings, diagrams)
- Video and sound (films, voice mail, .wav files)
- Web pages
- Hidden files
Digital Evidence

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
Forms of evidence

- **Files**
  - Present / Active
    - Documents, spreadsheets, images, email, etc.
  - Archive
    - Backups
  - Deleted
    - Files left in slack and unallocated space
  - Temporary
    - Cache, print records, Internet usage records, etc.
  - Encrypted or otherwise hidden
  - Compressed or corrupted
Forms of evidence

- Fragments of Files
  - Words
  - Sentences
  - Paragraphs
Digital Evidence Containers

- Home computers
- Office workstations
- Network servers
- Cell phones, PDAs, other portable devices
- Thumb drives and other external storage
- P2P network share folders
- Internet & Online Service Providers
- Vehicles
- New and evolving devices
Digital Devices / Sources of Digital Evidence
Hard Drives
Removable media
More
More
Digital devices / containers
Smart Phones

“... Are Moving Closer To Replacing PCs”

More
More
More
More

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

Infiniti G35
9.5 GB hard drive

Cadillac CTS
40 GB hard drive
More
More
Evidence Containers?
More Containers
Digital surveillance
Chicago’s 911 Network
Digital surveillance devices?
Digital surveillance device?
Digital device?
“From the attic to the cellar, we’re completely computerized.”
Challenges

- Increasing ubiquity and convergence of digital devices
- Increasing data storage capacity
- Shrinking devices and media
- Growing use of solid state devices
Effective Response Needs

- Training and equipment
- Knowledge of cyber crime, investigation techniques, legal constraints
- Personnel, training, & material support for computer forensics
Forensics

The application of scientific techniques of investigation to the problem of finding, preserving and exploiting evidence to establish an evidentiary basis for arguing about facts in court cases
Digital Forensics

Forensics applied to information stored or transmitted on computers

Three activities:

– Computer Forensics
– Network Forensics
– Software Forensics
Computer Forensics

“Involves preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis”

Usually pre-defined procedures are followed, but flexibility is expected and encouraged, because the unusual will be encountered

Essentially “post-mortem”
Computer Forensics

- **Seizing** computer evidence
  - bagging & tagging
- **Imaging** seized materials
- **Searching** the image for evidence
- **Presenting** digital evidence in court
Basic steps – 3 A’s

1. **Acquiring** the evidence without altering or damaging the original

2. **Authenticating** that the acquired evidence is the same as the data originally seized

3. **Analyzing** the evidence without modifying it
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 a third in a 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
Authenticating the Evidence

Proving that the evidence to be analyzed is exactly the same as what the 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

  - SHA (NIST Tool)
  - MD5 (CRCMD5)
Analyzing the evidence

- Always working on bit-stream images of the evidence; never the original
  - Prevents damage to the original evidence
  - Two backups of the evidence
    - One to work on
    - One to copy from if the working copy is altered

- Analyzing everything – clues may be found in areas or files seemingly unrelated
Analysis (cont.)

- Existing Files
  - Mislabeled
  - Hidden

- Deleted Files
  - Trash Bin
  - Show up in directory listing with $\sigma$ in place of first letter
    - “taxes.xls” appears as “$\sigma$axes.xls”

- Free Space
- Slack Space
- Swap Space
Free Space

- Currently unoccupied 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 that is not occupied by an active file, but is 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**

File A (In Memory) → File A saved to disk, on top of File B → File A overwrites File B, creating slack → Remains of File B (slack)

*Slack space*: the area between the end of the file and the end of the storage unit.
Swap Space

Virtual Memory

How much depends on the operating system and the user’s desires

Virtual memory is volatile memory.
  - When the computer is tuned off, virtual memory is still there, but now is free space.
  - When the computer is turned back on, virtual memory is erased.
Other sources mined for Transient Data

- Browser cache, history, cookies
- Residual chat data
- Activity logs
- Registry & registry backup files

Find the Golden Nuggets
“TOP 10” 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
Countermeasures that may be encountered

Ways of trying to hide data

- Encryption
- Password protection schemes
- Steganography
Summary

- Manner of seizing evidence
- Preservation of integrity of data
- Computers have readable & hidden data, both of which can be retrieved
Questions?

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