Special Thanks To

• Lt. Josh Moulin, Southern Oregon High Tech Crimes Task Force
• Lt. Joseph Rampolla, Park Ridge (NJ) Police Department
• Richard Kaplan, Computer Forensic Specialist, USDOJ CEOS
  • For their willingness to collaborate and share ideas in the digital world

Objectives

• Be able to identify sources of technical investigations
• Understand common terms related to computer hardware
• Understand how the Internet works and how IP addresses are assigned
• Understand how data is written, stored and deleted from storage devices

Objectives

• Understand commonly used computer forensics terms, hardware and software
• Understand the importance of computer forensics examinations, and how they are completed
• Be able to understand content of a computer forensics report
Sources of Investigations

- Walk-in complaints from citizens
- CyberTips from The National Center for Missing and Exploited Children - passed on from ICAC Task Force
- Referrals from other Law Enforcement Agencies
- Child Protection System undercover operations

Computer Forensics Defined

- “Pertaining to the Law”
- Coined in 1991 in the first training session held by the IACIS in Portland
- Described as the autopsy of a computer hard disk drive

Computer Forensics Defined:

Collection, Preservation, Examination, Documentation, and Presentation

...of computer related evidence.

Examimation and Documentation

Digital Evidence can be:
- The Fruits of the Crime
- The Instrumentality
- the Evidence

Your Electronic Crime Scene just changed...again!
Where is the Crime Scene?

What type of examination is needed?

- Tier 1 - On-scene preview of digital evidence
  - Seizure of evidence, documentation, interviews
  - Encryption, P2P evidence, wireless/storage,
    RAM capture, Forensic Scan, zSearch

- Tier 2 - Evidentiary Forensic Analysis
  - Acquisition, analysis for indictment and plea agreements
  - Case-specific forensic analysis
  - Evidence to corroborate statements, CVIP submission

- Tier 3 - Requests from DA/Defense
  - Analysis to answer concerns and requests of DA
  - Analysis offered to Defense to exculpate their client
  - Opportunity to close door on defenses, move plea forward

- Tier 4 - Trial Prep Forensics and Analysis
  - Includes all seized digital evidence for case
  - Defeating known/plausible defenses, complete analysis report,
    preparation of demonstrative evidence, meeting with DA,
    prep of expert witness questions/testimony

Basics to Understand

- Common types of digital storage media
- How data is stored
- Hashing, how it works, and why it is important
Identifying Digital Evidence

**Computer Forensics defined:**
- Collection,
- Preservation,
- Examination,
- Documentation, and
- Presentation

...of computer related evidence.

**Digital Evidence**

What does it look like?
- USB Drives
- Memory Cards
- External Hard Drives
- Computers
- Mobile Devices
- GPS Devices
- Cloud Storage
- RAM / CPU
Wireless Devices

- Be prepared to investigate wireless devices
- Understand how your own devices may interact wirelessly with suspect devices
- Wireless devices can contain evidence of crimes
- Evidence on wireless devices is generally volatile, and gone once power is lost
Evidence of Wireless Devices

Understanding Data

Data Sizes

• Bit (b) is a single zero or one
• Byte (B) is eight bits in sequence together
• Kilobytes (KB) is 1024 bytes, sometimes shown as 1000 bytes
• Megabytes (MB) is 1,048,576 bytes, sometimes shown as a million bytes
• Gigabytes (GB) is 1,073,741,824 bytes, sometimes shows as a billion bytes
• Terabytes (TB) is 1,099,511,627,776 bytes, sometimes shown as a trillion bytes

How Data is Written

• Data is written and read in 1’s and 0’s on the drive
• The hard drive is equipped with platters which spin at generally 7200 or 10000 rpm
• Mechanical arms move back and forth over the platters while they spin and write or retrieve data
• The data is written as the mechanical arm changes the magnetic coating on the platter’s surface as either + or – (a 1 or 0)
Hard Drive Terminology

- Data is stored on the surface of a platter in sectors and tracks. Tracks are concentric circles and sectors are pie-shaped wedges on the track:

Sectors and Clusters

- A sector contains a fixed number of bytes – typically 512 bytes. Sectors are grouped together to form clusters.
- Performing a high-level format prepares the hard drive for data by writing the file storage structure.

How Digital Data is Stored

- Data is written in binary code, or 1’s and 0’s.
- These 1’s and 0’s are grouped together in blocks of 8 and called bytes.
- For example, a sequence of “1010011” represents the letter “S”. The sequence “1001111” is the letter “O”.

Understanding Unallocated Space

- Allocated Space: Physical space on the hard drive that has been assigned and is being used by the file system at a specific moment in time. This includes:
  - Visible files
  - Hidden files
  - Slack space
Slack Space

- File slack can be an excellent source of evidence
- Computers write data one sector at a time but must allocate a minimum number of sectors for each file. These sectors are allocated even if you don’t use them
- It’s like a video tape... If you say that a video tape can only have one show on it at a time, you would allocate a 2 hour video tape per show. Now if you record a ½ hour program, you still have 1½ hours of tape left

Slack Space Recovery

- Often if data resides in slack space it can be forensically recovered
- Evidence from slack space will normally not have dates/times associated with it because that information may have been overwritten
- It is possible to get enough of a document or image to prosecute an individual

If there was a program on the tape before you recorded the new ½ hour show, you would see it at the end minus the first ½ hour. This is slack space.

Partial File Recovery - Slack Space
Understanding Unallocated Space

- Unallocated Space = Physical space on the hard drive that has not been assigned by the file system at a specific moment in time and is considered available for use. This includes:
  - Deleted files
  - Space that has not been assigned to a file

How Files are Deleted

- When a user deletes a file the computer does absolutely nothing with the file's data itself
- Depending on the file system that the hard drive is formatted to, some things are handled differently
- Regardless of the file system, the data still remains and the computer sees the space where that file resides as “available for use”
- Until something else is placed in its spot on the drive, the file will remain and can be recovered with forensic methods

Methods Impacting Deleted Files

- Running system utilities such as defrag can rearrange data and overwrite unallocated space and slack space
- Using secure erase features such as Norton secure erase or other third party applications that are designed to “shred” data
- Although this class is primarily about Windows computers, it should be noted that Mac computers have functionality built in to securely erase data

Hashing and Forensics
Terminology - Forensic Image

• It is no longer recommended to call forensic images a “mirrored image”
• Mirroring would imply that the duplicate looks exactly like the original. Although the content is the same it looks nothing like the original
• “Forensic Image” is the most appropriate and recommended.

Hashing

• Hashing is a very important tool for forensics
• Hashing is like a digital fingerprint for a file. It is mathematically derived from the contents of the item being hashed
• The odds of two files with different content sharing the same MD5 hash value is more than 1 in 340 undecillion (or 1 followed by 36 zeros)

Hashing

• Hashing is used in forensics for many things:
  • Known File Filters
  • Narrow search scope
  • Exclude items to be searched
  • Find known images of child pornography
  • Compare files to determine if they have been altered
  • Ensure the integrity of a forensic image process

Hashing

• There are several algorithms such as MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm), and others
• MD5 is a 128 bit 32 character algorithm and is the most commonly used hashing algorithm
• There are other hashing algorithms available for encryption, however forensics primarily focuses on MD5 and SHA1
• Hashing is used in many other areas such as download confirmation and encryption
What Affects a Hash Value

- Any change to the content of the file
  - One pixel in a picture
  - Add/remove one character in a document
- Changing the filename or file extension will have no affect on the hash value
- Sophisticated CP traders modify files to change hashes, and avoid detection

WARNING!!!

- Document all actions surrounding manipulation of system:
  - Seizure
  - Live Preview - Findings, exported files, reports
  - Live Acquisition
  - Automated Acquisition and Field Search

Tier 1 - On-scene Preview

How to collect:

- On-Site Preview
- On-Site Acquisition
- RAM Acquisition and Analysis
- Seizure of Computer and Associated Items

Tier 1 - On-scene Preview

On-Site Preview & Acquisition:

- Bootable CDs
  - ImageScan, Helix, Trinux, BartPE, ForwardDiscovery, Knoppix, WinEN, etc.
- USB/Other
  - e-fense “Live Response”, Forensic Dossier, Solo3, Logicube, Forensic Scan, FieldAgent, zSearch
- Acquisition and Analysis
  - MacLockPick
  - FTK Imager
  - EnCase Portable
MacLockPick

- USB Auto-performing system scan
- Retrieves “state of machine” information
  - Passwords, logs, registry entries, documents, pictures, etc.
- Forensically sound, X-platform
- First-responder deployable
- $399 for LE

EnCase Portable

- USB auto-performing data collection
- Integrates with EnCase Forensics
- Hash, search & copy
- Image entire drive
  - All attached drives
- $748.50 LE

zSearch

- Free product by SA Eric Zimmerman
  - FBI - Salt Lake City, UT
  - Distribution - eric[at]feeble-industries.com
- Plug-in live triage via USB
- Virtualization, encryption, mass storage, P2P, Gigatribe, picture & video preview, password gathering, and MORE!
- FREE!!!

Random Access Memory Analysis:

- DATA IS TRADITIONALLY LOST - NO MORE!
- CONTAINS COMPUTER’S RECENT ACTIVITY
  - IMAGES, DOCUMENTS, WEB PAGES, VIDEOS, ETC
  - PASSWORDS (BitLocker, KeyChain, Crypto)
- LARGE AMOUNT OF EVIDENTIARY DATA
  - RAM SIZES UP TO > 32GB OF INFORMATION
- CAPTURED FORENSICALLY, SAVED TO IMAGE FILE FOR ANALYSIS (DATA CARVING)
Tier 1 - Defeating Passwords

If password protected:
- On-scene analysis information
- RAM analysis
- Social engineering
- Known backdoors
- Internet
- Computer or BIOS manufacturer
- Passwords extracted from removable media
- Brute force attacks
- Specialized software
- Court order / immunity

Tier 1 - Collection and Preservation

How to seize digital evidence:
- If needed, call for assistance
- Determine legal authority
- Document and photograph area, screen, cables, etc
- If "off" -> leave "off"
- If "on" -> that changes things

Tier 1 - Collection and Preservation

If it is "on" then:
- Is there encryption in use?
  - Windows Vista & 7
  - Mac Leopard & Snow Leopard
  - Preview search using DOD-ICE CryptHunter
- Are there programs open?
  - TrueCrypt, BestCrypt, PGP
- Can it be shutdown properly?
- Don’t hesitate to call for help

Tier 1 - Collection and Preservation

Working around encryption:
- "Known" backdoors
- RAM analysis
- Written notes
- Corporate assistance
- Legal process/demand
- Co-defendant plea agreements
**Tier 1 - Collection and Preservation**

**What to collect:**

- **Hard Drive/Media Only**
  - Not best for running systems
  - Fine for loose digital media

- **Tower/Media Only**
  - Best option

- **Computer and All Peripherals**

**Computer and All Associated Items:**

- Monitor
- Keyboard
- Mouse
- Speakers
- Printer
- Scanner
- Web Camera
- Microphone
- External Drives
- Manuals
- Notes
- Other Media

**Tier 1 - Collection and Preservation**

**Marking The Computer and Associated Items:**

- Photographs are the BEST documentation
- Evidence Numbers
- Label all connections to re-assemble in court if required
- Tape over power, etc. if going to another agency...

**Transporting the System and Media:**

- Comfortable temperature
- Avoid car seats if possible (bouncy) — floorboards are more stable
- Avoid using police radio in transport vehicle if possible
Tier 1 - Collection and Preservation

Storing the System and Media:
- Clean, dry, secure area with reasonable temperature
- Avoid moving shelves
- Avoid areas with magnetic storage
- Avoid areas with police radio transmitters
- Consider anti-static bags, boxes, temp and static controlled storage room

Each case’s variables will dictate the path of the computer forensic examination
- No two exams will be the same
- No two reports will be the same

Forensic Examination:
- Know Your Scope
  - Search Warrant – Affidavit
  - Type of Crime Being Investigated
  - Articulate Authority
- Multi-Disciplinary Legal Auth.
  - Prosecutors should review/approve SW, Aff, Subpoenas, etc

Forensic Examination Equipment and Media:
- Secure, robust, dedicated
- Forensically sterile media
  - Wiped & verified
- Licensed software
- Tested write-block devices
Tier 2 - Evidentiary Forensic Analysis

Acquisition Authentication analysis

For indictment and plea agreements
Case-specific analysis and examination
Evidence to corroborate statements
CVIP submission

Tier 2 - Examination and Documentation

Forensic Documentation:
- Status of Computer
  - Operating system, users, ownership, media size, internet...
- Seized/Searched
  - Item by Item
  - Evidence? Contraband? 3rd Party?
- Methodology of examination
Examine the BIOS settings:

- **Date and Time settings**
  - Compare to known time — note findings
- **Boot Order (CD, HDD, Etc.)**
  - Important for Network other direct acquisitions

Tier 2 - Evidentiary Forensic Analysis
Image Acquisition:

- Do NOT allow the hard drive to enter the boot process
- Can Change THOUSANDS of Files and attributes
  - But - if it does happen, DOCUMENT IT.

Tier 2 - Evidentiary Forensic Analysis

Bit Image / Forensic Image:

- Physical or Logical acquisition
- Acquired & Verified by HASH
- Separate from other cases
  - Different Machine, Drive, Folder
- Must Include Slack, Erased, Unallocated, Pagefile, Etc.
- Archived – Reload if Required

Note digital media’s capacity and geometry and compare to later findings

- Obtain data from digital media using forensic methods
  - Write Blockers
  - Live / Network Acquisitions, Etc.
  - Smeared images*

* Smeared images

Select Source

Please Select the Source Evidence Type:
- Physical Drive
- Logical Drive
- Image File
- Contents of a Folder
(Logical file-level analysis only; excludes deleted, unallocated, etc.)
Physical vs. Logical

Pre-Acquisition Hash

Acquisition Hash & Verification

Tier 2 - Evidentiary Forensic Analysis

Bit Image:
- Physical or Logical acquisition
- Acquired & Verified by HASH
- Separate from other cases
  - Different Machine, Drive, Folder
- Must Include Slack, Erased, Unallocated, Pagefile, Etc.
- Archived – Reload if Required
The forensic image file for evidence item DB14, along with the other forensic image files related to this investigation, were all copied to the defense-provided external hard drive related to discovery for this case. I then returned the drive to Detective Beth Miller, for production to the defense council.

This report may not be inclusive of all potential evidence contained on the computer media referenced in this report. Any additional forensic analysis conducted on the referenced computer media will be documented in future reports.

**ACTION RECOMMENDED:**
- Investigation continuing.

---

**Tier 2 - Evidentiary Forensic Analysis**

**Forensic Image:**
- Physical or Logical acquisition
- Acquired & Verified by HASH
- Separate from other cases
  - Different Machine, Drive, Folder
- Must include Slack, Erased, Unallocated, Pagefile, etc.
- Archived – Reload if Required
**Tier 2 - Evidentiary Forensic Analysis**

**Bit Image:**
- **Physical or Logical acquisition**
- **Acquired & Verified by HASH**
- **Separate from other cases**
  - Different Machine, Drive, Folder
- **Must Include Slack, Erased, Unallocated, Pagefile, Etc.**
- **Archived – Reload if Required**

**Analogy**

- Slack Space: It’s like a video tape… If you say that a video tape can only have one show on it at a time, you would allocate a 2 hour video tape per show. Now if you record a ½ hour program, you still have 1½ hours of tape left.

```
               ------------------------  SLACK  ------------------------
               | 1/2 hour program      | 1 1/2 hour of old program |
               | 1 CLUSTER             | THIS IS THE SIZE OF THE FILE |
               | THIS IS UNUSED SPACE AND COULD CONTAIN DATA FROM A PREVIOUS FILE |
```

**Tier 2 - Evidentiary Forensic Analysis**

- **Forensic Write-block Devices**
  - Hardware vs. Software
  - Verified (and Validated?)
- **Tableau**
- **FastBloc**
- **Voom Technologies**
- **Logicube**
Tier 2 - Evidentiary Forensic Analysis

Forensic Examination:
- Index, Hash, Categorize files present
- Hash Set analysis
- Known files comparison
- Document Registry, LNK files.
  - As appropriate for your case
HASH Sets

- Collections of File Identification Information
- HASHes used during forensic investigations:
  - National Software Reference Library
  - www.nsrl.nist.gov
  - DHS-ICE HASH
  - Contact a Special Agent
  - HashKeeper
    - www.usdoj.gov/ndic/domex/hashkeeper.htm
  - AccessData Known Files Filter
  - Beyond FairPlay Tools (Forensic Scan, Media Library, etc)
  - Operation Round-Up hash sets
  - Case-specific hash values (from other seized evidence or UC Ops)

Traditional Hash Analysis

- Hashes of “known” files compared against hashes of files on suspect media
  - Hash analysis is based on binary content of file, rather than visual examination
  - Not effective against deleted files, Unallocated, slack space, unused disk area

File Block Hash Analysis

- Simon Key ~ Guidance Software (EnCase)
  - Block-based hash analysis works by calculating a hash for each block of the target file that would be allocated a sector or cluster to store its data.
  - A map of each block is generated, with the corresponding hash of each block. This is then fed to EnCase, and a search for the block-based hashes begins.
  - **Must have full version of target file sought**

Partial File Recovery

- **Only 8% of this file has been found**
Partial File Recovery

- We can rebuild partially recovered files (based on the hash map from good file)
- Render partial files as playable/viewable

New File System Features – Jump Lists

- Jump Lists - You can think of Jump Lists as miniature Start menus for program icons on the Taskbar. Each Jump List can contain tasks, links to recent and frequently used documents, and links to pinned documents.

Tier 2 - Evidentiary Forensic Analysis

Forensic Examination:

- Document Registry Artifacts
  - MRUs, WinRAR, Jump Lists

- Document LNK files.
  - Show path to other devices
  - Folder structure
  - Access

New File System Features – Jump Lists

- Jump Lists - You can think of Jump Lists as miniature Start menus for program icons on the Taskbar. Each Jump List can contain tasks, links to recent and frequently used documents, and links to pinned documents.
Forensic Examination:

- View Pictures, Movies, Docs
  - View in Native Format
  - View Forensically
  - EXIF Data for Pictures
  - Hidden Text, Updates/Changes
  - Notes, Properties, Etc.
Tier 2 - Evidentiary Forensic Analysis

EXIF/MetaData:

- Can be modified by programs
- Can be ‘cleaned’ or ‘stripped’ away during up/download
- Good corroborative evidence

“Case Specific” Data:

- Instant Messages
  - View in Native Format
  - LE or Commercial Decryption
  - View Forensically
  - Plain Text
  - Not Saved – Search UC for SN
Tier 2 - Evidentiary Forensic Analysis

“Case Specific” Data:

- **File Sharing Programs** (KaZaa, LimeWire, BearShare, Etc.)
  - View in Native Format
  - LE or Commercial Decoder
  - View Forensically
  - Database or Spreadsheet Formats
  - Additional Information in Slack Space
EXAMINATION AND DOCUMENTATION

“Case Specific” Data:

- Embedded Data
  - View in Native Format
  - Email attachments, Word, PPT
- View Forensically
  - Encoding format, link to other files, notable differences to like files,
Case Specific Data:

- E-Mail Messages
  - View in Native Application
  - Thunderbird, Outlook, Lotus Notes, Etc.
  - View Forensically
  - EnCase, FTK, ILook, Paraben, Etc.
  - Other Programs or Raw Data
  - Interim Changes/Embedded Data
**Tier 3 - Requests from DA & Defense**

**Acquisition Authentication Analysis**

Answer concerns & questions of DA
Analysis of artifacts at request of Defense
Exculpatory evidence specific search/analysis
Investigate suggested defenses (from D)

**Tier 4 - Trial Forensics Examination**

**Forensic Examination:**
- Run Searches &/or Scripts
  - Document search keywords & why
  - Careful of script pitfalls
  - Test/Authenticate Search String
  - Headers – Not Extensions
  - Case Names (Victim, Suspect, Etc.)
  - Case Terminology (R@ygold...)
Forensic Examination:

- Examine Erased/Recent Files
- Sort by status “Deleted”
- Sort by Dates/Times
- Most Recent
- Close Proximity to Crime, Etc.
- Info/Recycle Bin

Tier 4 - Trial Forensics Examination

Forensic Examination:

- Examine for Cloud/Network Storage
  - File sync software
  - File versions & comparisons
  - Online backup solutions
  - Push services to mobile/cloud
  - Stored shared user list
Forensic Examination:

- Examine Internet History
  - Registry for TypedURLs
  - Saved forms, pwds, cookies
  - Visited sites, first and last visit, count, info up/downloaded
- Comb through HTML files
  - EnCase, FTK, Net Analysis, etc
Forensic Examination:

- Check for Virus, Trojans, Etc.
- Emulated Disk for Scan
- Scripts for Virus Signatures
- If Found – Obtain More Info...
  - Virus Company Web Sites, Etc.
  - Research Capabilities, Etc.
  - Log files from computer
  - Statements of suspect RE: viruses
Mobile Devices

Gathering Data from Device:
- Hand-Jamming
- Examination & Analysis
- Extraction & Analysis
- Cloning, Examination & Analysis
- Flasher Box Extraction & Analysis

Some information in following slides taken from Purdue University's Purdue Phone Phorensics (P3) project at www.MobileForensicsWorld.com/p3

Seizure Documentation:
- Location where device found
- Condition when located (on/off)
- Chain of Custody
- Physical issues/description
- Photograph and document manipulation
Mobile Devices

Device Shielding/Isolation:
- Jamming/Spoofing signal
  - Vio of Comm. Act 1934 (FCC)
- Radio shielding bag/container
- Airplane Mode
- Turning off device
- Network Service Provider (NSP)
  - Court Orders & Assistance

Mobile Devices

Document w/o Modifying:
- Make, Model, Model #
- Vendor Logo
- Style (Flip/Slider/Clam Shell/Form Factor)
- External Memory Present (Type, Capacity)
- Digital Camera (Forward/Rear Facing)
- Compliance Label (ESN/MEID or IMEI & SIM)
- Battery present/not present
- Damage - Condition
Mobile Devices

Examination & Analysis:
- Subscriber Identity Module
  - Possibly clone SIM for analysis
- External Memory Cards
  - Same as Digital Media (Forensics)
  - Data carve deleted data
- Examination, extraction and analysis of data on physical handset

Gathering Data:
- Ideally through:
  - Cable connected - most secure
  - InfraRed (IrDA) - less secure
  - BlueTooth (BT) - least secure
- All may result in changed data or state of phone from original seizure

Evidence Analysis:
- Through Automated Tools or Raw Analysis:
  - Text (Short Msg Service)
  - MMS (Multimedia Msg Service)
  - Contacts / Address Book
  - Call Logs
  - Web History
  - Email
  - App Data
**Mobile Devices**

**CONSIDERATIONS:**
- Can we “forensically” analyze a phone or other mobile device?
- Can’t separate storage from device
- Often, access only provided areas of phone
- Do we need to perform “forensics” on mobile devices?
  - If we document our actions, is that sufficient?
  - **Most evolving area of forensics**

**Forensic Principle**

**Always Show Unbiased Methodology and Emphasize the Evidence that Relates to the Current Charges — Incriminating or Exculpatory**

---

**Forensic Principle**

**Consider Possible Defenses and Attempt to Prove or Disprove Them with Your Evidence**

---

**Instructor Information**

Detective Micah Smith
Linn County Sheriff’s Office
Computer Crimes and Computer Forensics

Voice: 541-812-9200
Email: msmith@le.linn.or.us