Evidence Bytes

Digital Evidence, Authentication, and Metadata

Presented to
2016 Nevada Judicial Leadership Summit
Edward Hunter, Hunter Forensics
What is Digital Evidence?

• Digital evidence is “information and data of value to an investigation that is stored on, received, or transmitted by an electronic device” (National Institute of Justice [NIJ], 2008)

• Digital evidence has a wider scope, can be more personally sensitive, is mobile, and requires different training and tools compared with physical evidence.
Where To Find Digital Evidence

- Internet
- Hard Disk Drives
- Flash drives (thumb drives)
- CD-ROM/DVD-R
- Smart Phones/Tablets
- PEDs
- Automobiles
- Internet of Things
Where To Find Digital Evidence

• Digital evidence can come from both suspects and victims, as all involved parties may have their own personal devices that are relevant to the investigation
Digital Forensics

• Digital forensics -- science or art. "Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science." United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005)
Investigation Plan

1. Preservation
2. Collection
3. Validation
4. Identification
5. Analysis
6. Interpretation
7. Documentation
8. Presentation
Evidence must be acquired only by permission from competent authority or by informed consent. The provenance, credibility and admissibility of evidence must be verified and approved.
Preparation & Initiation

- Clearly define and understand what you are being asked to find out.
- Ask yourself where would the relevant/pertinent data reside on the system.
- Determine what applications may have been used in creating the relevant data.
- Determine the appropriate tools required and test them for accuracy.
- Agree in advance what action you should take.
- Stay in touch with those requesting/directing the investigation.
Evidence Collection

- Plan and execute collection of evidence based on the objectives of the investigation and the digital forensic tools to be used.

- If performing ‘Live Forensic’ collection of evidence, minimize the impact on the system and document all your actions thoroughly.

- Use the Locard Exchange Principle of Forensic Science
  - When an investigator attaches a removable storage device to a computer, evidence of the attachment will remain on the computer.
Sealing, labeling and tagging – seal the evidence item in a waterproof Faraday bag.

(A Faraday bag prevents radio waves from accessing the contents. This is particularly necessary when the computer/smart phone/tablet has WiFi or cellular/mobile transmission and reception capability).

Document who collected it, date/time of collection, assign an evidence number to it.
Live vs Postmortem

• Primum non nocere – first, do no harm
• Stop pulling the plug
• Critical information in live memory
• When to do “live forensics”
• When to do “cold disk forensics”
Tools

• Validate your tools

• Choose tools for the task

• Know the system and its application
  – Ref Casey Anthony case (Florida, 2011)

• Use two tools for each task

• Bit-wise and byte-wise analysis, if necessary
Forensic Analysis and Examination

Incident Response & Evidence Collection

- Plan of Action
- Authority to Proceed
- Verification of Incident
- System Description
- Collection & Preservation of Evidence

Investigation & Analysis

- Network Analysis
- Data Analysis
- Memory Analysis
- String/Byte Search
- Timeline Analysis
- File System Analysis

Results, Reports, Lessons Learned
Documentation

• What is the basis of authority to investigate?
• What were the initial goals of the investigation?
• What you collected and reviewed?
• What results did your investigation produce?
• What is the context of your findings, conclusions and opinions?
Acquisition Process
Memory Acquisition

- Drivers required
- 3rd Party application often used
- Documentation must be thorough
- Know what changes are caused by act of acquiring memory image
- How to analyze
  - Volatility Framework
  - Rekall
Order of Volatility

• Order in which changes occur within a system.
• Collect items which change most rapidly first / or those which have the least effect on other items
• Example: Capture System RAM before capturing a logical disk image
• Stop Pulling The Plug!!
• Document everything!
Order of Volatility

• Live Memory (RAM)
• Network Connections/Communications
• Open Files
• Logged On Users
• Running Processes and Services
Order of Volatility

• Be cognizant of your investigative goals and where evidence can exist. Don’t destroy it.
Authentication

• Version control
  – Firefox v15.0 vs v18.0

• True nature of the evidence

• File extension vs file identification number
  – .exe vs MZ (4D 5A)

• Data Structure Authentication
Data Acquisition from Devices

• Hardware vs Software Write Blockers
  – Hardware:
    • Pros – Faster, less prone to errors, more reliable
    • Cons – Requires special interface connectors, cost, training
  – Software:
    • Pros – Less expensive, not tied to physical interface
    • Cons – If not used properly, can corrupt data
Environment

• Version/Type of Operating System
  – Windows XP, Vista, 7, 8, 8.1, 10
  – Mac OS X (Mountain Lion, Mavericks, Yosemite, El Capitan)
  – iOS (iPhone 4, 5, 6 or iPad Air or iPad Mini)
  – Android (Multiple)
  – Linux
  – Unix
  – Proprietary
Cryptographic Hashing

• A cryptographic hash function is a type of security mechanism that produces a hash value, message digest or checksum value for a specific data object.

• Cryptographic hash functions must exhibit pre-image resistance, second pre-image resistance and collision resistance properties to ensure resilience against any cryptoclastic attack. Common examples of cryptographic hash functions are MD5 and SHA-1.
Cryptographic Hashing - Collisions

• MD5 shown to be vulnerable to collisions
• SHA-1 to be deprecated
• SHA-256 and SHA-512 preferred
• MD5 – 64-bit \((2^{64}) (1.38 \times 10^{38})\)
• SHA-1 – 128-bit \((2^{128}) (1.0 \times 10^{77})\)
• SHA-256 – 256-bit \((2^{256}) (4.3 \times 10^{156})\)
• SHA-512 – 512-bit \((2^{512}) (1.0 \times 10^{324})\)
Classes of Digital Evidence

• Original
  – Avoid analysis on original disks, if at all possible

• Best copy
  – Retain to make additional working copies

• Working copies (min 2)

• Only examine working copies
Authentication

• Windows
  – BIOS
  – Registry
• Mac/iOS
  – BIOS
  – System Files
  – Binary Property Lists
• Applications
  – Vendor documentation
  – Examiner testing, documented research, peer review
MetaData – Data about Data
MetaData

• Qualitative data – descriptive information
• Quantitative data – numerical information
• Discrete data – can only take certain values (application-specific)
• Continuous data – any value within a range
MetaData

• When data was created or last accessed or modified
• Created or modified by whom
• Time each action is performed
MetaData

- Time Stamps
- Track changes
- Downloaded files
- Application-Specific
- Hidden data/artifacts
Analysis
Determine if...

- Alibi holds weight
- USB drive was connected
- File existed/copied/deleted/moved
- User sent email
- User accessed a remote system
- User visited a specific website
- User wiped files or drive artifacts
- A particular file was printed
- User possessed or transmitted indecent images
- User uses a specific alias on a website
- Data was compromised during an intrusion
- User was in a specific location
- Something happened on/from this system...
Hash Analysis

• Too Much Data / Big Data (TB $\rightarrow$ PB)
• Known Good Files vs. Known Bad Files
  – www.nsrl.nist.gov
• Updated March 2011 - 63,634,656 Known Files - 19,255,196 unique
• Enterprise Gold Disk Images
• Forensic Triage
  – Great options for reducing data sets to analyze
File Signature Analysis

- Valid File Extension (PDF/DOCX)
- Windows File / Software Association
Timeline Analysis

- Provides context to activity
- Focuses on activity, not just artifacts
- Reduces amount of data to analyze
- System Clock Time Skew??
Time Stamps

• Each Operating System/File System records time differently:
  • **Modification** – Time data attribute was last modified
  • **Access** – Time file data was last accessed
  • **Changed** – Time metadata layer (MFT) was changed (Deleted time for Linux/Unix ext#)
  • **Born-on/Created** – Time file was created
Time Stamps

• M A C B times change when
  – Copying to same volume
  – Moving (cut & paste) to same volume
  – Copying to different volume
  – Moving (cut & paste) to different volume
Types of Digital Artifacts

- Office Documents
- Windows Registry Keys
- Browser cache
- e-Mail (Outlook, pop3, and Web-based)
- Prefetch files
- Volume Shadow Copies
- Logs
- Digital Photographs/images
Types of Digital Artifacts

• On-line Gaming
• USB traces
• Unallocated Space
• Slack space
• Network traffic capture (Beware: ECPA)
MetaData on Photo Artifact

![Photo Properties](image)

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression</td>
<td></td>
</tr>
<tr>
<td>Resolution unit</td>
<td>2</td>
</tr>
<tr>
<td>Color representation</td>
<td>sRGB</td>
</tr>
<tr>
<td>Compressed bits/pixel</td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td></td>
</tr>
<tr>
<td>Camera maker</td>
<td>Apple</td>
</tr>
<tr>
<td>Camera model</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>F-stop</td>
<td>f/2.2</td>
</tr>
<tr>
<td>Exposure time</td>
<td>1/30 sec.</td>
</tr>
<tr>
<td>ISO speed</td>
<td>ISO-200</td>
</tr>
<tr>
<td>Exposure bias</td>
<td></td>
</tr>
<tr>
<td>Focal length</td>
<td>4 mm</td>
</tr>
<tr>
<td>Max aperture</td>
<td></td>
</tr>
<tr>
<td>Metering mode</td>
<td>Pattern</td>
</tr>
<tr>
<td>Subject distance</td>
<td></td>
</tr>
<tr>
<td>Flash mode</td>
<td>No flash</td>
</tr>
<tr>
<td>Flash energy</td>
<td></td>
</tr>
<tr>
<td>35mm focal length</td>
<td>30</td>
</tr>
</tbody>
</table>

Remove Properties and Personal Information
Example – EXIF from Digital Images

• Camera has exif data capture enabled
• GPS/Geo-tagging is enabled
• Google Image Search
<table>
<thead>
<tr>
<th>Tag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Research In Motion</td>
</tr>
<tr>
<td>Model</td>
<td>BlackBerry 9800</td>
</tr>
<tr>
<td>Orientation</td>
<td>top - left</td>
</tr>
<tr>
<td>x-Resolution</td>
<td>72.00</td>
</tr>
<tr>
<td>y-Resolution</td>
<td>72.00</td>
</tr>
<tr>
<td>Resolution Unit</td>
<td>Inch</td>
</tr>
<tr>
<td>Software</td>
<td>Rim Exif Version1.00a</td>
</tr>
<tr>
<td>Date and Time</td>
<td>2011:12:28 07:41:37</td>
</tr>
<tr>
<td>YCbCr Positioning</td>
<td>co-sited</td>
</tr>
<tr>
<td>Exposure Time</td>
<td>1/-2147483648 sec.</td>
</tr>
<tr>
<td>Exif Version</td>
<td>Exif Version 2.2</td>
</tr>
<tr>
<td>Date and Time (original)</td>
<td>2011:12:28 07:41:37</td>
</tr>
<tr>
<td>Color Space</td>
<td>sRGB</td>
</tr>
<tr>
<td>PixelXDimension</td>
<td>1568</td>
</tr>
<tr>
<td>PixelYDimension</td>
<td>1168</td>
</tr>
<tr>
<td>GPS tag version</td>
<td>4 bytes undefined data</td>
</tr>
<tr>
<td>North or South Latitude</td>
<td>N</td>
</tr>
<tr>
<td>Latitude</td>
<td>32.00, 46.78, 0.00</td>
</tr>
<tr>
<td>East or West Longitude</td>
<td>W</td>
</tr>
<tr>
<td>Longitude</td>
<td>117.00, 9.67, 0.00</td>
</tr>
<tr>
<td>Altitude reference</td>
<td>1 bytes undefined data</td>
</tr>
<tr>
<td>Altitude</td>
<td>19.00</td>
</tr>
</tbody>
</table>
Look Familiar?
Challenges Ahead

- Internet of Things (IoT)
- Cloud Computing
- Encryption (Apple v. FBI)
- CSI effect
- 1 Billion more users in next decade
- International Crime
- State-sponsored hacking/cyber attacks
References

- **US DOJ:** [http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx](http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx)
- **Ball In Your Court:** [https://ballinyourcourt.wordpress.com/](https://ballinyourcourt.wordpress.com/)
- **Consortium of Digital Forensics Specialists:** [www.cdfs.org](http://www.cdfs.org)
Questions

• “Here is my lens. You know my methods.”
  – Sherlock Holmes
Contact Information

Edward Hunter
Forensic Consultant | CISSP | GCFA

Phone: 858.218.4754
E-mail: hunter4n6@gmail.com
Twitter: @hunterforensics