Digital Forensics for Attorneys

An Overview of Digital Forensics

About Your Presenter

- EnCase Certified Examiner (EnCE)
- Digital Forensics Certified Practitioner (DFCP)
- Blackthorn 2 Certified Examiner (BCE)
- Co-author of “Digital Forensics For Legal Professionals” (2011 Syngress Publishing)
- Over 190 hours of digital forensics training.
- Testified as expert witness 14 times.
  - Cell Phone Forensics
  - Computer Forensics
  - Cellular Technology Forensics (Cell Towers)
- Consulted on over 600 cases

Digital Forensics For Attorneys

- Overview of Digital Forensics
  - Types of Digital Evidence
  - Acquisition (Collection) and Preservation
- Experts, Evidence and Analysis
  - Understand Forensic Experts vs. Computer Experts
  - Digital evidence: discovery and usage
  - Analysis
  - Challenging Digital Evidence
In The Beginning...

INTERNET

Al Gore is so AWESUM for making the Internet!
By 2013 there will be over 1 trillion devices connected to the Internet

Digital Footprints
Digital evidence in 80% of cases
5+ billion cell phone subscriptions

Overview
• Digital Forensics – Four Primary Areas of Focus
  • Acquisition (Collection)
    • Obtaining the original evidence items
    • Making forensic copies of original evidence
  • Preservation
    • Protecting the original evidence items
  • Analysis
    • Finding evidence
  • Presentation
    • Reporting findings and testimony
Digital Forensics – The Sub-Disciplines

• Computer Forensics
  • Computers and Data Storage Devices
    • Hard drives, USB thumb drives, Backup Tapes, Media cards
  • Social Media Forensics
    • Facebook, Twitter, Chat, MySpace, Internet Presence on Blogs, Message Boards
• Email Forensics
  • Back tracking emails
  • Email recovery
  • Email authentication

Digital Forensics – The Sub-Disciplines

• Peer to Peer Forensics
  • File sharing via LimeWire, BitTorrent, Gigatribe, iTunes, others
• Cell Phone Forensics
  • Call logs, contacts, text messages, pictures, movies, geo-location
• Cellular Evidence Forensics
  • Cell phone record analysis, Cell phone ping analysis, Cell tower mapping
    • Typical Case Types: Murder, Kidnapping, Drugs

Digital Forensics – The Sub-Disciplines

• Digital Video and Image Forensics
  • Security Video, Camera Video, Pictures
• Audio Forensics
  • Police Interviews, Police Radio Recordings, Wiretaps
• GPS (Global Positioning Systems)
  • Data from GPS units, Logs from GPS tracking, House Arrest
Acquiring (Collecting) and Handling Digital Evidence

Digital forensics requires forensically sound acquisitions.

- Defensible Practices
  - Proper Chain of Custody
  - Verification of evidence
  - Proper documentation

Acquisition (Collection)

First contact with the original evidence.

- Most critical time for protecting the originals.
- Most likely time for police or others to damage or change evidence.
- General rules MUST be followed to preserve and protect evidence during this critical first response period.
- First point in establishing chain of custody.

_Policies for Law Enforcement are published by the National Institute for Justice_

What Is Forensically Sound?
This is Forensically Sound

Verification Must Be Done

MD5 Hash
9e107d9d372bb6826b88d1c10d49a187

1 in 340 billion billion billion billion
How Verification Works

**UNIQUE HASH VALUE FOR EACH FILE.**

**HASH VALUE MUST MATCH**

**ORIGINAL EVIDENCE**

**FORENSIC COPY**

---

Organization of Logical Data on a Hard Drive

**PARTITION**

**FOLDERS**

**FILES**

---
Logical Acquisition (Norton Ghost, computer backups, simply copying)

- Does not get deleted files
- Is NOT a complete forensic copy
- Is NOT collected in a verifiable forensic format
- Does not use forensic collection tools
- Subject to contamination
- Not Repeatable, Not Verifiable

Physical Acquisition

- A complete "mirror image" of the physical storage media, also referred to as a bit-stream copy.
- Gets everything, including deleted data and unallocated space
- Collected in forensic format that is easily verifiable
- Meets the standards for original evidence
- Supports full chain of custody
- Cannot be contaminated.
Two Types of Deleted Data
Preservation

• Once digital evidence is seized it must be handled carefully to preserve and protect the evidence.
  -- Everything should be tagged.
  -- No one should operate or preview any evidence on writable media without proper tools and training.
  -- Forensically sound copies of all original evidence must be made before analysis.
  -- Records must be kept.

Fragile Nature of Digital Evidence

• The next 3 slides demonstrate what happens when you operate a computer.
  -- Evidence is modified.
  -- Evidence is destroyed.
### Files In Original Condition

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Created</th>
<th>Last Written</th>
<th>Last Accessed</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>file1.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>file2.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>file3.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

All of the dates and times are the same for these file time stamps.

### Files After Opening and Viewing

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Created</th>
<th>Last Written</th>
<th>Last Accessed</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>file1.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>file2.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>file3.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

The last access date and time changes any time a file is opened and viewed while the computer is in operation.

This is true only for MS Windows prior to Vista and 7. The Last Accessed Time is no longer updated in those versions.

### Files After Saving

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Created</th>
<th>Last Written</th>
<th>Last Accessed</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>file1.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>file2.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>file3.jpg</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
<td>2023-01-01</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

The last write date and time changes any time a file is saved, copied while the computer is in operation.
Other Digital Evidence

- Global Position Systems (GPS)
- Vehicle Black Boxes
- iPods
- Digital Cameras
- Security Cameras
- Audio Recordings
- Game Consoles
- Security Systems
- Back up Tapes
- Databases

Why a Forensics Expert?

Computer Forensics Expert
- Should have comparable or better training and experience than the other expert.
- Should have specific training and experience as a digital forensics expert.
- Should have access to the same tools as the opposing expert.
- Must be able to qualify as a forensic expert in court.
Selecting a Digital Forensics Expert

Certifications

- EnCase Certified Examiner (EnCE)
  - This is probably the most widely known and recognized certification. This is a vendor-specific certification that is provided through Guidance Software, the publishers of the EnCase Forensic Software. EnCase is widely used in law enforcement and in the private sector. (www.ences.com)
- Access Certified Examiner (ACE)
  - This is the vendor-specific certification for the Forensic Tool Kit (FTK) software by Access Data Corporation. FTK is widely used in law enforcement and in the private sector. (www.accessdata.com)
- Certified Computer Examiner (CCE)
  - This is a vendor-neutral certification administered by The International Society of Forensic Computer Examiners. The CCE is one of the oldest certification programs. (www.isfci.com)
- GIAC Certified Forensic Examiner (GCFE) and GIAC Certified Forensic Analyst (GCFTA)
  - These are vendor-neutral certifications administered by SANS Institute and are supported by extensive training programs. (www.giac.org)
- Certified Forensic Computer Examiner (CFCE)
  - These certifications are offered by the International Association of Computer Investigative Specialists (IACIS). Until recently the certification has been open only to active or retired law enforcement officers. As of July 2011, the certification is open to the general public. (www.iacis.com)
Forensic Tools

Do they have appropriate forensic tools?

- Required to perform many digital forensic functions
- Computer Forensics (EnCase, FTK)
- Cell Phone Forensics (CelleBrite, Paraben, Susteen)
- GPS Device Forensics (Blackthorn, Paraben)
- Almost always needed to perform forensically sound acquisitions and examinations.

Analysis

Analyzing the Case

- Approaching the case holistically
  - Digital evidence can reach into all corners of a case:
    » Cell records
    » Email
    » Pictures
    » Timelines
    » Internet Activity
Analyzing the Case
Establish a framework for analysis by:
Reading the computer forensics reports
– What claims are being made?
– What statements were made?
– What facts support the claims and which do not?

What clues can lead to a more thorough digital analysis?
What clues can lead to a more thorough digital analysis?
• Defendant's statements
• Witness statements
• Police statements and interviews
• Call center records
• Search warrants and subpoenas
• Other supporting documents
• Law Enforcement's computer forensics report

Analyzing the Case
Check all the points in the case where mistakes are normally made:
Chain of custody.
Examination standard procedures.
RTC verified for all evidence containing clocks.
Evidence handling at the scene.
Was everything examined.
Claims made in the forensics report.
Pay particular attention to keyword search results, internet history results, link files, etc.
Placing the defendant at the computer.
Performing the Analysis

– Duplicate the other side’s work.
  
  • Verify the accuracy of their findings
    – Did they represent their findings correctly?
    – How thorough was the examination?
  • Verify the completeness of their report
    – Is everything they found in the report?
    – Why or why not?
    – Was exculpatory evidence ignored or missed?

Case Analysis

Examples

Document Metadata Example
Challenging the evidence

• Common mistakes that open digital evidence to challenges
  - Failing to verify clock times
    • Computer Clocks (Real Time Clock Setting)
      - Affects everything related to time lines:
        » Internet history
        » Emails
        » Computer activity
    • Digital Cameras
      - Affects the metadata inside the digital images.

Challenging the evidence

• Is there an attempt to place a person at a computer without adequate proof?
  • How can you tell?
    - Did the analyst check for unique user accounts with passwords?
    - Is there evidence anyone else used the computer under that person’s account or profile?
    - Was the computer in a common area?
    - Did others know the passwords to the user’s account?
    - Was access to the computer restricted by physical boundaries or location?
Challenging the evidence

• Games people play
  – Stating facts out of context
    • Keywords
      – Keyword hits are not always relevant
        » Murder case example
        » Hits were found for the keywords murder (156), kidnapping (34), disposal (76), and death (273) on the subject's computer.

Challenging the evidence

• Games people play
  – Stating facts out of context
    • A Keyword hit is not always based on a User Search.
      – Context based ad services create searches automatically.
      – There must be evidence that the user created the search, not an automated process.

Challenging the evidence

• Games people play
  – Stating facts out of context
    • Keywords
      » Hits were found for the keywords murder, homicide, insanity...
      » Where can these hits come from?
        – Lexicons, thesaurus, and spell check dictionaries
        – News focused web pages (MSN, Newspaper sites, Television sites, CNN, etc.)
      » When is a hit a hit?
        » Is 156 hits for murder meaningful?
### Challenging the evidence

“Listed below are the notable keyword searches and number of "hits" that FTK noted.”

- "Homicide" 230 hits
- "Homicidal" 540 hits
- "Insanity" 178 hits
- "Defense" 2429 hits
- "Defense and Insanity" 871 hits
- "Wikipedia" 6034 hits
- "Murder" 2497 hits
- "Pheedo" 155903 hits
- "Kill" 9010 hits
- "Police" 5788 hits
- "Killer666vampire" 4863 hits
- "Killer" 3872 hits
- "Insane" 4308 hits
- "Death" 7745 hits
- "Deathblow" 16 hits
- "BTK" 1174 hits
- "Attorney General" 546 hits
- "Preterm birth" 122 hits
- "Jeff Dunham" 1110 hits

### User Inputted Search Terms?

“Detective noted that the user inputted a search term or key word of “homicide”. In addition the user inputted key words of “Attorney General” and also “Preterm Birth”. The date on this particular example is dated August 5, 2010.”

- "http://www.msnbc.msn.com/id/38694786/ns/us_news/"
Challenging the evidence

• Games people play
  – Playing the techie game
    • Technical words no one understands
      – Unallocated space
      – Slack space
      – Browser cache
      – Typed URLs
      – Gnutella and Limewire
    • What does that mean?

• What does that mean?
  – If it is in the browser cache, does that mean the user did it on purpose?
    » How browser caching works.
    » Federal courts have ruled that files recovered:
      » in the internet cache do not constitute possession unless the prosecution can prove the user knew about the files in the cache.
      » In unallocated space do not constitute possession.
    » Same ruling in Georgia in 2007.
Challenging the evidence

- What the heck is unallocated space?
  - Unallocated space is areas on the hard drive that are available to store data.
  - When a file is deleted, it is only marked as deleted, so the old data remains on the hard drive in the unallocated space.
  - Forensic tools can recover files from this unallocated area of the hard drive.
  - Files recovered from unallocated space do not contain:
    - Dates or times.
    - Original file names
    - Original location on the hard drive.

Challenging the evidence

- Call Detail Records and Cell Phone Locations
  - Help to establish the whereabouts of the defendant?
    - You cannot locate a cell phone using call detail records.
    - 90% of the cases I have reviewed contain serious flaws in the reports by law enforcement.
    - Be very careful of claims overstating the accuracy of this type of location information.
    - No such thing as triangulation of a cell phone from call detail records.