Digital Evidence and Computer Forensics

WAEI OBEID
8 December 2014

Resources
Donald R. Mason, Digital Evidence & Computer Forensics
https://blogs.sans.org/computer-forensics/
http://www.e-evidence.info/biblio.html
http://craigball.com/

Objectives

- Define and describe “digital evidence”
- Identify devices and locations where digital evidence may be found
- Identify and describe the basic principles, practices, and tools of digital forensics
- Describe selected trends and challenges in digital forensics
From the “old days” to

Evolving technology in ...
The “Digital age” with ...
Roles of Digital Devices

➢ Targets

➢ Tools

➢ Containers

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 pornography

➢ Computer as Container
  ✓ From drug dealer records to how to commit
  ✓ murder
Computers are Digital Devices

• A computer is like a light switch

<table>
<thead>
<tr>
<th>Switch</th>
<th>Computer</th>
<th>Binary Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>signal present</td>
<td>1</td>
</tr>
<tr>
<td>OFF</td>
<td>no signal present</td>
<td>0</td>
</tr>
</tbody>
</table>

• Each 0 or 1 is a BIT (for BINARY DIGIT)

• An 8-bit sequence = 1 byte = a keystroke

```
0 1 0 0 0 0 0 1
```

= A

Digital Data

- Data is written in binary code -- 1’s and 0’s
- These 1’s and 0’s are grouped together in blocks of 8, called “bytes.”
- For example, the sequence “10001111” represents the letter “O”.
Digital Evidence

- Information of probative value that is stored or transmitted in binary form and may be relied upon in court
- Information stored in binary code but convertible to, for example:
  - e-mail, chat logs, documents
  - photographs (including video)
  - user shortcuts, filenames
  - web activity logs
- Easily modified, corrupted, or erased
- But correctly made copies are indistinguishable from the original

Digital Evidence

- 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
Digital Evidence

- Computer-created
  - Dialing, routing, addressing, signaling info
  - Email headers
  - Metadata
  - Logs
  - Browser cache, history, cookies
  - Backup and registry files
  - Configuration files
  - Printer spool files
  - Swap files and other “transient” data
  - Surveillance tapes, recordings

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

Hand-held devices
- digital cameras
- PDAs
- tablets
- mobile phones
- GPS devices

Sources of Evidence

Servers
- ISP authentication user logs
- FTP and Web server access logs
- Email server user logs
- LAN server logs
- “Cloud” storage
- Web pages
- Social media
Sources of Evidence

- Online activity
  - Internet Protocol addresses
  - Router logs
  - Third party service providers

Computer Forensics
Computer Forensics

• *Forensics* is 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.

• *Computer Forensics* is the scientific study and use of processes involved in the identification, preservation, recovery, extraction, examination, interpretation, documentation, and presentation of the contents of computer media (digital evidence) for evidentiary and/or root cause analysis.

Features of Digital Evidence and Computer Forensics Methodology

- Digital evidence can be duplicated exactly.
- Computer forensics requires duplication of the original evidence so that a copy can be examined as if it were the original.
- Computer forensics involves both data recovery and analysis.
- Even if “deleted,” digital evidence can be recovered from computer media (at least until completely overwritten).
- Even when attempts have been made to destroy digital evidence, it can remain and be detected.
- Computer forensics is governed by valid laboratory principles.
Guiding Principles

- The rules of evidence apply to digital evidence
- Actions taken to secure, collect, and analyze digital evidence should not change the evidence in any way
- Persons accessing or conducting examinations of digital evidence should be trained for that purpose
- All activity must be fully documented

Computer Forensics

- Obtaining,
- Processing,
- Authenticating, and
- Producing
Computer Forensics

- Usually pre-defined procedures followed but flexibility is necessary as the unusual will be encountered
- Was largely “post-mortem”
  - “What’s on the hard drive?”
- Rapidly evolving
  - From “Pull the plug” to “Don’t power down before you know what’s on it”

Branches, Evolutionary trends

- Computer forensics
- Network forensics
- Live forensics
- Software forensics
- Image forensics
- Mobile device forensics
- “Browser” forensics
- “Triage” forensics
- “Distributed” forensics
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

Basic Steps

- **Acquiring (and preserving)**
  
  evidence without altering or damaging original data

- **Authenticating acquired evidence**
  
  by showing it’s identical to data originally seized

- **Analyzing (searching for) the**
  
  evidence without modifying it
Analysis (cont’d)

- **Existing Files**
  - Mislabeled
  - Hidden

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

- **Free Space**
- **Slack Space**
- **Hidden Data**

Forms of Evidence

- **Files**
  - Present / Active (doc’s, spreadsheets, images, email, etc.)
  - Archived (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**
  - Paragraphs
  - Sentences
  - Words
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
- How

Metadata

- Basic Examples
- Track Changes
- Comments
“Browser” Forensics

Web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox, Safari, Opera) maintain histories of recent activity, even if not web related

“Browser” Forensics
- Temporary Internet Files
- Internet History
- Typed URL’s
- Internet Navigation
- Search Strings
- History
- Cookies
“Triage” Forensics - Steps

- Attach/Install write-blocking equipment
- Turn on target device
- Scan for file extensions, such as:
  - doc
  - jpg (.jpeg)
  - mpg (.mpeg)
  - avi
  - wmv
  - bmp

Mobile Device Forensics

(or “Cell Phone Forensics”)
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”?  

➢ Others argue it’s still “forensics”  
➢ Follows the “computer forensics” process  
  ▪ Identification  
  ▪ Preservation  
  ▪ Collection  
  ▪ Examination  
  ▪ Analysis  
  ▪ Reporting

Cell phone data that *may* be recoverable

– 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
Cell phone data that *may* be recoverable

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

Questions?

Wael Obeid
obeidw@gmail.com