Digital Forensic Techniques

Namrata Choudhury,
Sr. Principal Information Security Analyst,
Symantec Corporation
Professional Techniques – T23
AGENDA

• Computer Forensics vs. Digital Forensics
• Digital Forensics Process
• Digital Forensic Approaches
• Digital Forensic Techniques
• Case Studies
• Questions
Computer Forensics vs. Digital Forensics
Computer Forensics vs Digital Forensics

Digital forensics is the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law.

Computer forensics is the science of locating, extracting, and analyzing types of data from difference devices, which specialists then interpret to serve as legal evidence.
Digital Forensic Process
Digital Forensic Process

Preparation

Identification

• Events
• Alerts
• Complaints

Preservation

• Chain of Custody Management and Storage

Collection

• Forensic Acquisition Approved Hardware and Software

Examination

• Validation Filters
• Tools, Techniques and Scripts

Analysis

• Data Mining
• Timeline
• Relationship Among Events

Closure

Retention

Presentation / Reporting

• Reports
• Supporting Files
• Testimonies

Documentation
Digital Forensic Approaches
Digital Forensic Approaches

• Three main approaches
  – Media Analysis
    • OS, USBs, PDAs, Cell Phones, GPAs, Imaging, Time Line, Slack Space
  – Code Analysis
    • Malicious Code Review, Reverse Engineering
  – Network Analysis
    • Communication – Traffic Patterns, Log, Path Tracing
Digital Forensics Techniques
Digital Forensic Techniques

• Acquisition Phase
  – Chain of Custody
  – Forensic Duplication

• Analysis Phase
  – Recover Deleted Items
  – Compressed files
  – Signature Analysis
  – Internet History
  – Registry Analysis
  – Hash Analysis
  – Keyword Searching
Acquisition Phase – Chain of Custody

Why

• Layer of protection on a piece of evidence
• To proof in the court of law that evidence has not been tampered

How

• Physical document that goes with the evidence
• 5 “W” (What, When, Why, Where, and Who) and an “H” (How)
Acquisition Phase – Forensic Duplication

**Why**
- Avoid Spoliation; Guarantee the integrity of the evidence
- Plain copies of files and folders or ghost copy does not provide the data stored in Windows swap file, unallocated space and file slack.

**How**
- Use of write blockers
- SANS Investigative Forensics Toolkit – SIFT, Encase, FTK, Sleuth Kit, X-Way Forensics
Analysis Phase - Recover Deleted Items

Why

• Users often attempt to cover their tracks by deleting folders/files that are of interest

How

• Using tools such as Encase, FTK to recover deleted files
  • Open source tools such as Sleuth Kit or Autopsy(GUI); run on Unix platforms
Recover Deleted Items - Example
Analysis Phase - Compressed Files

Why

• Archive of information for easier transport
• Contents often ignored during scanning

How

• Use of forensic tools to mount the compressed files
• Export compressed files to physical drive and decompress; tedious; risky, sandbox environment, not on network
Analysis Phase - Signature Analysis

Why

• Tactic to hide data by changing the file extensions

How

• Sleuth Kit and Perl scripts to compare the contents of a file to a standard file containing headers and footers
• Forensic Tools such as Encase, loaded with predefined signatures. Report matching, mismatch and bad signatures
• http://www.garykessler.net/library/file_sigs.html
## File Signature - Example

<table>
<thead>
<tr>
<th>Name</th>
<th>File Ext</th>
<th>File Type</th>
<th>File Category</th>
<th>Signature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDRM-2-792.jpg</td>
<td>jpg</td>
<td>JPEG</td>
<td>Picture</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Vulnerability Report.pdf</td>
<td>pdf</td>
<td>Adobe PDF</td>
<td>Document</td>
<td>Match</td>
<td>File</td>
</tr>
<tr>
<td>DoNotIPs.xlsx</td>
<td>xlsx</td>
<td>MS Excel Spreadsheet</td>
<td>Document\Spreadsheet</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>LogedLog.txt</td>
<td>txt</td>
<td>Text</td>
<td>Document</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Examples</td>
<td></td>
<td></td>
<td>Unknown</td>
<td>Folder</td>
<td></td>
</tr>
</tbody>
</table>
Analysis Phase - Internet History

Why

- Web browsing history, cookies and temporary internet files

How

- Location: Windows 7 - 
  C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files
- Index.dat – database for web URLs, search queries and recently opened files; 
  index.dat analyzer to open
- Encase, FTK, Browser History
<table>
<thead>
<tr>
<th>Name</th>
<th>Profile Name</th>
<th>Url Name</th>
<th>Type</th>
<th>Url Host</th>
<th>Visit Count</th>
<th>Last Accessed</th>
<th>Internet Type</th>
<th>Browser Type</th>
<th>Last Modification Time</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td>file://C:/Users/Namrata Choudhury/Documents/Internet%23%20Wired%20Wireless%20Assessment.docx</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td><a href="http://www.cdfws.org">www.cdfws.org</a></td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td>index.dat</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td><a href="http://www.dhws.org/2013dfws-m.list.pdf">http://www.dhws.org/2013dfws-m.list.pdf</a></td>
<td>URL</td>
<td>dhws.org</td>
<td>2</td>
<td>10/09/2013 03:01:10PM</td>
<td>History/Daily</td>
<td>Internet Explorer (Windows)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td>file://C:/Users/Namrata Choudhury/Documents/Expenditure_Receipt.png</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td>Computer</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index.dat</td>
<td>Namrata Choudhury</td>
<td>usatrade.com</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TypedList</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>Namrata Choudhury</td>
<td><a href="http://www.electriclife.org">http://www.electriclife.org</a></td>
<td>URL</td>
<td>electriclife.org</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>Namrata Choudhury</td>
<td><a href="http://etrade.com">http://etrade.com</a></td>
<td>URL</td>
<td>etrade.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>Namrata Choudhury</td>
<td><a href="http://www.guidancesoftware.com">http://www.guidancesoftware.com</a></td>
<td>URL</td>
<td>guidancesoftware.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>Namrata Choudhury</td>
<td><a href="http://www.accessdata.com">http://www.accessdata.com</a></td>
<td>URL</td>
<td>accessdata.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>Administrator</td>
<td><a href="http://go.microsoft.com/fwlink/?LinkId=63157">http://go.microsoft.com/fwlink/?LinkId=63157</a></td>
<td>URL</td>
<td>go.microsoft.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>usersetup</td>
<td><a href="http://go.microsoft.com/fwlink/?LinkId=63157">http://go.microsoft.com/fwlink/?LinkId=63157</a></td>
<td>URL</td>
<td>go.microsoft.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2013 Fall Conference – “Sail to Success”  
September 30 – October 2, 2013
Analysis Phase - Registry Analysis

**Why**
- References from windows event logs, application logs
- User behavior, most recent visited websites, most recent documents, installed software and much more
- Malware behavior

**How**
- FTK Registry Viewer, Encase EnScripts
- Open source tools such as RegRipper
Registry Analysis - Example

RecentDocs
**All values printed in MRUList\MRUListEx order.**
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Sun Mar 20 22:00:01 2013 (UTC)
  8 = OMGs
  7 = OMG 1.ini
  9 = 1233.mp3
  1 = merlin.exe
  6 = ChangeLog.txt
  5 = result.txt
  2 = PasswordCracker.exe
  3 = Password.txt
  4 = browseme.vbs
  0 = README.txt

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Sun Mar 20 22:00:01 2013 (UTC)
  url1 -> http://download.cnet.com/windows/nothing.zip
  url2 -> regedit.exe
  url3 -> http://www.google.com/
  url4 -> http://vmware.com/
Analysis Phase - Hash Analysis

Why

• Increases efficiency. Where to stop? Exclude files such as operating system files, program files not relevant to the case
• Facilitates de-duplication
• Identify potential malicious files

How

• Scripts
• The Sleuth Kit
• Hash set using Encase
Analysis Phase - Keyword Searching

Why

• To review particular data of interest within file, deleted files and slack space
• Dangerous; False positives

How

• Encase and FTK’s Search Feature
• DtSearch Desktop
• PTK Forensics
Other Forensic Techniques

• Timeline Analysis – Chronological system events
• Email and Instant Messaging Artifacts
• Memory Analysis – Live forensics, open connections, running programs, temporal information
• Handheld Devices Acquisition and Analysis – iOS, Blackberry, Androids
• Malware Analysis – Static and Dynamic Analysis
• Data Mining and Behavior Analysis – Analyze from different perspectives
• Social Media Engineering – use of trusted pretext to obtain information
Summary

• Digital Forensic Model – Identify, Preserve, Collect, Examine, Analyze, Report
• Different Approaches – Media, Code and Network
• Techniques – File signatures, Hashing, Keyword Searching, Registry Analysis, Web Browsing activities

GOAL – High Integrity and Streamline Process
Case Studies
Case Study 1

- Case Type – Intellectual Property Theft
- Description – AMD accused four of its former employees for taking IP with them to NVIDIA.
- Which approach/techniques can be used in the investigation?
  - Registry Files
  - Email Artifacts
  - Keyword Search
  - Recover Deleted Files
Case Study 2

• Case Type – Misuse of Company’s Resources
• Description – IT team notices employee visiting illicit websites
• Which approach/techniques can be used in the investigation?
  – Internet History for Visited Websites
  – Keyword Searching
  – File Signature Analysis
Case Study 3

• Case Type – Hacked System
• Description – Stanford University Computer System Hacked
• Which approach/techniques can be used in the investigation?
  – Internet History for Temporary Internet Files
  – Timeline Analysis for Chronology of Events
  – Registry Analysis to Analyze Events
  – Keyword Search for Possible Data Breach
  – Hashing and Malware Analysis for APT
References

• A Road Map for Digital Forensic Research. 2001

• Computer Forensics: An Overview by Frederick Gallegos, 2005,


• Access Data

• Guidance Software

• The Sleuth Kit

• http://regripper.wordpress.com/

• http://www.dfresponse.com/computer-forensic-software.html

• http://en.wikipedia.org/wiki/List_of_digital_forensics_tools
QUESTIONS?