Digital Forensics 2.0

SBA Research &
Vienna University of Technology
Edgar R. Weippl

Overview

• Definition
• Digital Evidence
• How is a forensic investigation done today?
• What are future challenges?
Definition

• Forensic science is generally defined as the application of science to the law.
• “Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data”
• Source: NIST SP 800-86

Digital Evidence

• Growing importance since life becomes digital.
• Movies, series: CSI, ...
• Research papers: iPhone & Android Forensics, Cloud Forensics, Social Network Forensics, ...
• Becomes important for companies, budget increases
Digital Evidence

• Corporate Governance creates new responsibilities
  – Some person / department has to address information security.
  – Incident response is part of information security management
  – Management want explanations about what happened

• ISMS requires traceability of incidents

Digital Evidence

• White-collar crime often uses computers / networks
• Companies realize the potential losses such as
  – Media companies (music, movies, ...)
  – Software license
  – Employees using company equipment used privately
Increased Perception

- Sabu / Lulzsec, Anonymous, ...
- „Cyber Warriors“, such as United States Cyber Command in .us, ...
- „Cyber Defense“
  - 1600 in Austria, LKA / BKA
  - CCC in Germany
  - Cooperative Cyber Defense Centre of Excellence (CCDCoE) by NATO in Tallinn ...

Guide to Integration Forensic Techniques into Incident Response (NIST 800-86)
Data Collection

• Identifying possible sources of data
• Acquiring the data
  – Develop a plan to acquire the data
    • Likely Value
    • Volatility
    • Amount of Effort Required
  – Acquire the data
  – Verify the integrity of the data

Reporting

• Alternative Explanations
• Audience Consideration
• Actionable Information
Recommendations

- Organizations should perform forensics using a consistent process
- Analysts should be aware of the range of possible data sources
- Organizations should be proactive in collecting useful data
- Analysts should perform data collection using a standard process
- Analysts should use a methodical approach to studying the data
- Analysts should review their processes and practices

Different Methods

Methods depend on the task at hand

- What needs to be examined?
  – Which question should be answered?
  – Which artifacts are (still) available?
- Which tools?
  – Depends on data
- Which methods?
  – Is this a court case or do you (only) need to know where to focus your attention?
Example

Brandstiftung: WU- Gebäude muss schließen
Der Standard, 15.12.2005, Seite 1

Methods

Timeline Analysis

• Reconstruct series of events
• Data sources
  – Meta data on file system
  – Can sometime be recovered for deleted data
  – MAC time stamp
Time Stamps

• Last access to a file
  – Modified (last write)
  – Accessed (write/read also modified for read-only)
  – Created/changed (modification of attributes)

• Copy / Move may behave differently
• Unix / Windows behave differently
• Users, malware, programs can modify time stamp (e.g. touch, Total Commander)

Time Stamps

• Strange behavior when copying/moving files in NTFS
• Copy: M-time is before C-time
• Identification of source and target possible

• However: A-Time is not updated on Vista and NTFS by default (NtfsDisableLastAccessUpdate = 1)
• Linux mount flag noatime
FAT and NTFS

<table>
<thead>
<tr>
<th>ACTION</th>
<th>LAST MODIFIED DATE-TIME</th>
<th>LAST ACCESSED DATE-TIME</th>
<th>CREATED DATE-TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>File moved within a volume</td>
<td>Unchanged</td>
<td>Unchanged</td>
<td>Unchanged</td>
</tr>
<tr>
<td>File moved across volumes</td>
<td>Unchanged</td>
<td>Updated</td>
<td>Updated</td>
</tr>
<tr>
<td>File copied (destination file)</td>
<td>Unchanged</td>
<td>Updated</td>
<td>Updated</td>
</tr>
</tbody>
</table>
Timeline Analysis

• For each file it is possible to reconstruct what happened
  – Dropbox pack rat feature
  – When was file written, modified, change history
  – Was the file modified after accessing a Web site

Volume Snapshot Service

Volume Snapshot Service

Are you sure you want to restore the previous version of "e-books" from Today, February 20, 2010. 2 minutes ago?

This will replace the current version of this folder on your computer and cannot be undone.

Dropbox

Events

Events gives you a timeline of everything that’s happened in your Dropbox since the beginning of time.

My devices

All computers, phones, and tablets that have access to your Dropbox appear here.

<table>
<thead>
<tr>
<th>Name</th>
<th>Country</th>
<th>Most recent activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>NBA1W00002</td>
<td>Austria</td>
<td>In the last hour</td>
</tr>
<tr>
<td>Edgar.Wilkins-MacBook-Pro-SSD SBA</td>
<td>Austria</td>
<td>In the last hour</td>
</tr>
<tr>
<td>Katrin Lavoie WINP</td>
<td>Austria</td>
<td></td>
</tr>
<tr>
<td>Edgar’s Air</td>
<td>Austria</td>
<td></td>
</tr>
<tr>
<td>Edgar’s Mac Book white home</td>
<td>Austria</td>
<td></td>
</tr>
<tr>
<td>iPhone</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>iPad</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Versions</td>
<td>1.6.16</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>89.144.192.70</td>
<td></td>
</tr>
</tbody>
</table>
Internet Explorer History

- **Http-Auth:** %APPDATA\%\Microsoft\Credentials, in encrypted files
- **Form-based:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2, encrypted with the url http://securityxploded.com/iepassworddecryptor.php

Network Traffic

- Rootkits can hide processes, files
- Do not trust the operating system
- Data traffic is difficult to hide
- SSL – man in the middle
- TCPDump (IP address, ports, content)
Example

• For our example:
  – No network traffic available
  – Only two laptop recovered

Keyword Search

• Search in
  – Files
  – Empty space
  – Swap files, swap partitions
  – RAM

For key words; use word lists...

• E.g. strings RAMDump.bin | grep DVDRip
Search for „Kanister“ (fuel can)
Example

- Arson?
  - Bid to buy a fuel can

- No proof but indicates that further investigation makes sense

- Investigation is usually time-bounded.

Reconstruction of Data

Deleted files
- Trivial
  - Only reference to file is deleted
  - Files are marked as deleted
  - Files can be recovered with high probability
  - Also applies to cameras, smartphones, ...

- Advanced
  - You create a document, other processes in the background do other stuff, you add data to your document.
  - What happens if you use a secure delete on the file?
Copy-On-Write File System (e.g. BTRFS) or some SSDs

- Document can be recovered

File Carving

- Search for characteristic signatures of files
  - JPEG files start with 0xffd8 and end with 0xffd9
- Tools such as Foremost look for these signatures
Example

• Let’s get back to our example:
  – A file could be found (as deleted)
  – No new additional evidence could be found

Internet Browser History

• Tool Pasco
  – Cached Files are stored in index.dat (Internet Explorer)
  – Pasco can extract these and display results
• Details: Keith J. Jones, 2003, „Forensic Analysis of Internet Explorer Activity Files”
More Sources

• Look at other commonly used programs
  – E-Mail (Outlook, mbox) with tools such as scanpst

• Google Desktop Search
Windows Desktop Search

- Installed by default since Vista
- File Windows.edb
- Tools: esedbtools, EseDbViewer
- File location: %Profiles%/All Users/Application Data/Microsoft/Search/Data/Applications/Windows/
- May contain entire files or parts such as emails, documents,
- Paper by Joachim Metz, „Forensic analysis of the Windows Search database”

Last Commands and Applications Started

- Last commands and applications executed by a user (eg. Windows User Assist Key)
- “HKEY_USER\<sid>\Software\Microsoft \Windows\CurrentVersion\Explorer\UserAssist \{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count”
  - set “NoEncrypt=1” to stop encrypting and “NoLog=1” to stop logging altogether
Windows User Assist Key Analysis (Windows 7)


• “Weak ROT13 crypto has been replaced with “stronger” Vigenère crypto!”
• “The Vigenère key I found through some basic cryptanalysis is WHQNKTEZYFSLMRGXADUJOPIVC.”
• “To the Microsoft developer who designed this: great joke! You really made me laugh. Seriously.”

Registry Ripper (RegRipper)

• Files played in media player
  – “HKEY_USERS\<sid>\Software\Microsoft \MediaPlayer\Player\RecentURLList”
• ZIP Files opened/saved with “common dialog”
  – “HKEY_USER\<sid>\Software\Microsoft\Windows \CurrentVersion\Explore\ComDlg32\OpenSaveMRU \zip”
• “<sid>” = Security Identifier of user
• RegRipper: http://regripper.wordpress.com
More traces...

- Prefetch files (Win XP)
- Deleted images (with foremost)
- IE password / account / autocomplete recovery
  - IE Passview
  - OWADE
- Spooler files
  - Contains pages printed
    www.prnwatch.com
More traces...

• Prefetch files (Win XP)
• Deleted images (with foremost)
• IE password / account / autocomplete recovery – IE Passview – OWADE

Source: http://www.slideshare.net/jmichel.p/owade

Getting Facebook credentials require to bypass 4 layers of encryption
OWADE

Source: http://www.slideshare.net/jmichel.p/owade

Geolocation / WLAN

- Info stored for each access point
- Mac address (BSSID)
- Key (encrypted)
- Last time of access
- Wifi data are stored in
  - Registry (XP)
  - XML file and Registry (Vista/7)

Source: http://www.slideshare.net/jmichel.p/owade
Let’s get back to our example

• Analyze hard drive
  IE history (Pasco, index.dat)

• We could show that suspect had access to
  Web mail account of sender.

• Username/PW Kombination for Web mail
  account were found and still valid.

---

Sechs Jahre Haft für WU-Brandstifter
Für die Richterin stand fest: Den "großen Unbekannten
Angeklagte hat den verheerenden Brand gelegt

Wien - Natürlich muss sich der Prozessbeobachter die
niemand für Rudolf.S. ein psychiatrisches Gutachten ge-
der Mann, der am Mittwoch wegen der Brandstiftung in
Wirtschaftsuniversität (nicht rechtsträchtig) zu sechs Jahr-
worden ist, hat während der vier Prozesstage mitunter

Anonyme Mails

Dass auf seinem Laptop Texte gefunden worden sind, die große
ähnlichkeiten mit zwei anonymen Bekanntermails an die Kriminalpolizei
haben, wiegt schon schwerer. Vor allem, weil darin Details standen, die
öffentlich nicht bekannt waren. Und dass der Sachverständige auch noch
die Zugangsdaten für die E-Mail-Adresse, von der die beiden Botschaften
verschickt worden sind, auf dem Laptop entdeckt hat, machte die
Verurteilung praktisch fix.

http://derstandard.at/druck/?id=2972033
Friend-in-the-middle (FITM) attacks

- Hijack social networking sessions
- Attack surface: unencrypted WLAN traffic, LAN, router etc.
- User impersonation


Attack scenario
Fast Access to Data:
Collection of digital evidence through our social snapshot application

Access to Data

<table>
<thead>
<tr>
<th>Element</th>
<th>Download</th>
<th>social snapshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact details</td>
<td>–</td>
<td>✔ Crawler</td>
</tr>
<tr>
<td>News feed</td>
<td>–</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Checkins</td>
<td>–</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Photo Tags</td>
<td>–</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Video Tags</td>
<td>–</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Friends</td>
<td>name only&lt;sup&gt;a&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Likes</td>
<td>name only&lt;sup&gt;a&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Movies</td>
<td>name only&lt;sup&gt;a&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Music</td>
<td>name only&lt;sup&gt;a&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Books</td>
<td>name only&lt;sup&gt;a&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Groups</td>
<td>name only&lt;sup&gt;a&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Profile feed (Wall)</td>
<td>limited&lt;sup&gt;b&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Photo Albums</td>
<td>limited&lt;sup&gt;b&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Video Uploads</td>
<td>limited&lt;sup&gt;b&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
<tr>
<td>Messages</td>
<td>limited&lt;sup&gt;b&lt;/sup&gt;</td>
<td>✔ Graph API</td>
</tr>
</tbody>
</table>

<sup>a</sup> No additional information available.
<sup>b</sup> Missing meta-information such as UIDs.
Anonymized Social Interconnection Graph

Anonymized Social Interaction Graph using Picture Tags
Social interaction graph using direct messages

Example timeline
Order of Volatility

- "Order of Volatility" – RFC 3227:
  - registers, cache
  - routing table, arp cache, process table, kernel statistics,
  - memory
  - temporary file systems
  - disk
  - remote logging and monitoring data that is relevant to the system in question
  - physical configuration, network topology
  - archival media

Order of Volatility

- "Order of Volatility" - NIST 800-86
  - Network connections
  - Login sessions
  - Contents of memory
  - Running processes
  - Open files
  - Network configuration
  - Operating system time
Challenges with Acquisition

• dead man's control: shutdown, reboot
• Running rootkit
• OS logging – modify settings or not?
• Computer runs but locked
• Shutdown or pull the plug?
• Key remapping
• Superuser or user-level access?
• Pre-incident installation
• ...

Challenges with Acquisition

• Documentation!
  – In which state was the computer encountered?
  – What did you do?
  – Which software did you use? (exact versions!)
  – Which data did you copy to which location?
  – Hash values
Challenges with Acquisition

• Acquisition – Hardware vs. Software:
  – Software cheap but modifies state
  – Software can be tricked (kernel level Rootkit)
  – Hardware access requires additional hardware (DMA), such as Firewire, PCI, or PCMCIA
  – Hardware OS independent
  – Hardware can also be tricked (Rutkowska, BH 2007)

• There is no perfect answer!

Challenges with Acquisition

• Acquisition of virtual machines:
  – Suspend VMWare, copy .vmem file

• Windows Hibernation files
  – hiberfil.sys: switch to Hibernation Mode, copy file from hard disk
  – Not possible with Windows XP > 4 GB RAM
RAM Acquisition

- Image File Formats:
  - Raw – mit `dd` 1:1 image
  - Dumpfiles `.dmp` – CPU States information, required for Microsoft Tools

- Tools for Acquisition:
  - Kntdd – physical memory evidence from Microsoft Windows (XP, Win7, Win8)
  - Windd – disk dump
  - (Almost) all vendors (Encase, FTK, ...) have free utilities or Live CDs such as *FTK Imager*

---

RAM Acquisition

- Example for Windows – **NOT** good:
  - `psexec \target` –u Administrator –p password
    `dd.exe if=\PhysicalDrive0 of=\mymachine\share \
    $\target.drive0.dd bs=8k conv=noerroe`
  - `\PhysicalDriveX` are hard disks
  - `\PhysicalMemory` is RAM

  Better use FTK Imager

RAM Acquisition

- Bilby’s DDefy, Blackhat JP 2006
  - Protects against acquisition software
  - Modifies Page Fault Handler
  - Marks pages as “not present”

- Rutkowska DMA Redirection, Blackhat 2007
  - Protects against acquisition hardware
  - Reconfigures Northbridge
  - CPU & DMA see different content at same address
Cold Boot Attack

• *Lest We Remember: Cold Boot Attacks on Encryption Keys*, USENIX Security Symposium 2008

• Access RAM
  – Originally designed to capture crypto keys
  – Also useful for forensics (Screen locked, no USB, CD drive, investigator cannot start any external application)
  – Requires physical access
Windows RAM

- List of processes:
  - In Windows: all processes are in double chained list
  - Processes are objects
  - PsActiveProcessHead points to first element
  - Iterate shows all processes
  - Problem: root kits can modify the chain and make themselves invisible
  - What to do: scan entire memory; slow, specific of OS, difficult to do

Windows RAM

Enumeration of processes
Windows RAM

• Antiforensics: DKOM manipulation (Direct Kernel Object Manipulation)

Windows RAM

• Timeline can be generated after RAM has been saved
  – Threads & processes: created, terminated
  – Registry: last modification
  – Sockets: time of creation
  – Objects: almost everything (in Windows)!
    • File objects, Symlink Objects, Mutex, ...
Windows RAM

• Tools you can use:
  – FTK 3
  – EnCase
  – ...

• Open Source:
  – Volatility!

Windows RAM

• Volatility:
  – For Windows XP, Vista, 7, Server 2003 & 2008
  – Available for EnCase

• pfinder:
  – Original by Andreas Schuster
  – Development was continued for 2008 Server & Windows 7
Windows RAM

- Volatility – selected commands:
  - `strt`: "python vol.py commands" or "python volatility commands"
  - Convert images: `imagecopy`
  - Threads: `thrdscan`
  - Processes: `pslist`, `psscan`, `psthree`, `procexecdump`, `procmemdump`
  - Drivers: `driverscan`
  - Files: `filescan`
  - Sockets: `sockets`, `sockscan`
  - Connections: `connections`, `connscan`, `netscan`

RESEARCH IDEAS
Data Provenance Challenges

- **Confidentiality**
  - Cloud storage (e.g. Dropbox)
  - Authentication (e.g. WhatsApp)
  - Open data vs. unintended data leaks

- **Availability**
  - Dependability on infrastructure
  - Complex and hidden

- **Integrity**
  - Incomplete data,
  - Entry errors,
  - Processing,
  - Sensors,
  - Social media,
  - Latency of information,
  - Deception,
  - Modeling approximations
And even more challenges

Data Provenance Challenges

• Privacy
  – Combining different data sources (e.g. reading habits, diets)
  – Ambiguity of data and incorrect conclusions

• Security
  – Data and provenance do not share the same access policy
  – Detecting fake or fabricated records

• Object removal
  – How to preserve ancestral relation?

• Minimization
  – Provenance can get much bigger than actual data
  – Storing provenance costs
  – Even when minimized, has to be updated, queried, used

Questions?

eweippl@sba-research.org