Digital Forensics

What, Why, and How

By: Ahmed M. Neil

OWASP Mansoura Egypt, Chapter leader
Ireland, 2013

Ahmed.Neil@owasp.org
Acknowledgment
• **Defined:** Pertains to legal evidence found in computers and digital storage mediums.

• **Goal:** To explain the current state of a “digital artifact.”

• A digital **artifact** is a computer system, storage media
Why Digital Forensics

• In legal cases.
• To recover data.
• To analyze a computer system after a break-in.
• To gather evidence against an employee.
• The purpose of debugging.
Who should be in

- the expert is called investigator.
- Who is should at least knowledgeable in computer science fields, Law, and programming.
- Misc.
- No Sex, drugs, Alcohol.. Single “like me” nosy
Who should be in “cont’d”

• A study by the Institute for Security Technology Studies at Dartmouth College:
  • 7% of computer crime investigators had no formal training.
  • 11% had completed a full course of academic study in a related field.
  • 90% of the survey respondents indicated an urgent need for additional training and education.
Digital evidence
What does it mean?

- “Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of crime.

- is any probative information stored or transmitted in digital form that a party to a court case may use at trial[1, 2].

Digital Evidence Collection Methodologies
Performing Digital Forensics
Analysis of Evidence

- Need to find "footprints", to establish
  - what
  - when (timeline of events)
  - how (point of entry, vulnerabilities exploited, ...)
  - who (?)
  - why (??)

- Initial analysis
  - check for hidden or unusual files
  - check for unusual processes and open sockets
  - check for unusual application requests
  - check for suspicious accounts
  - determine patch level of system
Be Careful!

- Digital evidence must be handled carefully to preserve the integrity.
- Some digital evidence requires special collection, packaging, and transportation techniques.
- Communication devices.
To be admissible in a court of law, evidence must be:

- Relevant
- Legally permissible
- Reliability
- Identification
- Preservation.
Digital forensic Tools
Digital forensic Tools

Preferred Software for Investigation

- Email Examiner
- Registry Viewer
- Password Cracker
- Data Lifter
- Cacheback
- Viewer
- Secret Explorer
- SCDDVD Inspector
- Beyond Compare
- Thumbs Plus
- Tableau TD1
- DT Search
- UTK Access Data
- Xways
- Ubuntu
- Sleuth Kit
- Autopsy
- Lib Forensics
- IDAPro
- Linen
- Intella
- Easy Recovery
- Prtek
- Access Data Registry
- Pearl Script
- Paraben
- Net Analysis
- Helix
- Encase FTK
- FTK Imager
- EnCase

frequency
Digital forensic Tools cont’d

• Encase
• Access Data Forensic Toolkit
• Helix
• dd
• The `dd` utility copies and converts files.
• `dd` is commonly used in forensics to copy an entire environment.
• This utility takes two basic arguments—`if` and `of`.

• The `if` argument specifies the **input** file.
• The `of` argument specifies the **output** file.
• When using *dd* to copy individual files, the utility abides by the operating system file size limit, normally 2GB.
• Larger files will simply be truncated or cut.
• For example, to copy a simple file from a source (such as /home/aaa/sn.txt) to a destination (such as /tmp/newfile), you would issue the following command:

```
dd if=/home/aaa/sn.txt of=/tmp/newfile
```
Digital forensic Tools cont’d

[root@sciserver root]#
[root@sciserver root]# dd if=/home/michael/sn.txt of=/tmp/newfile
2+1 records in
2+1 records out
[root@sciserver root]#
• Using similar syntax, you can copy the hard disk drive located at

```
dd if=/dev/hda1 of=/dev/hdb/case_img
```
Hardware
Digital Forensic Hardware
Final stage
Presenting your finding

• Your report is the one common tool.
• Being able to **write a clear, concise, and factual.**
• care in your **explanations...**
• No matter how convinced you are.
• Some forensic tools such as:
  • ASR Data’s SMART
  • Guidance Software’s EnCase,
  • Technology Pathways ProDiscover,
  • Paraben’s P2 suite,
  • and AccessData’s Forensic Tool Kit
• The reports generated by these tools are normally collections of **bookmarked** evidence that you have noted during your investigation.
Report References


• Or just google “Digital forensics report samples”
The Microsoft Computer Dictionary defines the registry as:

A central hierarchical database used in the Microsoft Windows family of Operating Systems to store information necessary to configure the system for one or more users, applications and hardware devices.
### Windows Registry cont’d

#### Hives
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
  - HARDWARE
  - SAM
  - SECURITY
  - SOFTWARE
  - SYSTEM
    - ControlSet001
    - ControlSet003
    - CurrentControlSet
    - LastKnownGoodRecovery
    - MountedDevices
    - Select

#### Keys

#### Values
- `ab` (Default
  - Type: REG_SZ
  - Data: (value not set)
- Current
  - Type: REG_DWORD
  - Data: 0x00000001 (1)
- Default
  - Type: REG_DWORD
  - Data: 0x00000001 (1)
- Failed
  - Type: REG_DWORD
  - Data: 0x00000000 (0)
- LastKnownGood
  - Type: REG_DWORD
  - Data: 0x00000003 (3)
Windows Registry cont’d

- List of applications and filenames of the most recent files opened in Windows
List of applications and filenames of the most recent files opened in Windows.
“LastWrite” time: last modification time of a file. The forensic analyst may have a copy of the file, and the last modification time, but may.
SOME SCENARIOS
Scenario 1: Malware Attacking

Used by a great many pieces of malware to remain persistent on the victim system.

Where to dig?!
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Scenario 1: Malware Attacking “Cont’d”

AppInit_DLLs Value
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\AppInit_DLLs
– Specifies a DLL to be loaded by a Windows GUI application
– Used by malware.

<table>
<thead>
<tr>
<th>(Default)</th>
<th>REG_SZ</th>
<th>(value not set)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppInit_DLLs</td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>DeviceNotSelectedTime...</td>
<td>REG_SZ</td>
<td>15</td>
</tr>
</tbody>
</table>
Scenario 3: Downloading and Viewing inappropriate photos

Most Recently Used (MRU)

• Determining what files, folders, or applications were most recently
• Showing that an individual opened a file, saved a file, or searched for a file can prove the suspect know the file.
• Mostly download the files in C:\Users\Zero\Documents

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
Scenario 3: Downloading and Viewing inappropriate photos “cont’d”
Some practice

Scenario 3: Downloading and Viewing Porn

photos "cont'd"
Scenario 3: Downloading and Viewing inappropriate photos “cont’d”

• To show all files recently executed or opened through Windows Explorer.
• files are organized according to file extension under respective subkeys and the Subkey Folder contains the folder of the recently open files.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Scenario 3: Downloading and Viewing inappropriate photos “cont’d”
Deleting important files scenario

- The following information is recovered:
- The created date of the file, from the MFT entry, is 10\textsuperscript{th} June 2009
- The last modified date, from the MFT, is 30\textsuperscript{th} July 2009
- The last accessed date was the 31\textsuperscript{st} July 2009
- The computer was shutdown on 9am 3\textsuperscript{rd} August 2009.
- The computer was power on 19\textsuperscript{th} August but no nobody appears to have logged on
- The computer was Imaged on 20\textsuperscript{th} August 2009
Deleting important files scenario

• Additional information:
• 1\textsuperscript{st} and 2\textsuperscript{nd} August 2009...
Online Fraud Crime Case study

• suspect called Mr A
• visited Amazon web site intending to tamper an online purchasing transaction.
Online Fraud Crime Case study Cont’d

- **Stage 1:** From the collected evidential devices; select the appropriate device which is relevant to the crime type.
- **Stage 2:** Take image from that device and keep it a safe place to extract all relevant data from it.
- **Stage 3:** If the image contain sufficient evidential data go to step 4, else close the case and write up your report.
- **Stage 4:** Examine all founded data “in our case it will be Windows Registry”.
- **Stage 5:** Go to HKEY_USERS key expand it and find Software\Microsoft\Internet Explorer\TypedURLs to extract all typed URLs.
- **Stage 6:** Go to HKLM key, expand it and find system sub key then move to ControlSet00x\Enum\USBSTOR and look for all plugged in USB sticks.
• **Stage 7**: Go to HKEY_LOCAL_MACHINE key, expand it and find system sub key then move to ControlSet001\Control\Print\Printers and look for all plugged in /installed Printers devices.

• **Stage 8**: If you find any of the desired potential data as shown in stages 5, 6, 7 then move to stage 9, else close the case and write up your report with the current status.

• **Stage 9**: Search in each relevant key value for the useful information such as installation date, Vendor name, etc.

• **Stage 10**: Write up your report describing all founded evidence in a readable form.

• **Stage 11**: Move to the court to testify with what you found accompanied with the report you wrote before.

• **Stage 12**: Case closed;
Start

Select the appropriate Device

Take an image from the device

Does it contain sufficient data for the crime?

Yes

Examine relevant data from the image

Go to HKEY_USERS to examine Internet activity

NO

Go to HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR and look for stored USB sticks

Go to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Printers and look for existing Printers

Did you find anything?

Yes

Search for the values for each relevant evidence

Write up your report

NO

Move to the court for testimony

End
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>url1</td>
<td>REG_SZ</td>
<td><a href="http://www.amazon.com/">http://www.amazon.com/</a></td>
</tr>
<tr>
<td>url11</td>
<td>REG_SZ</td>
<td><a href="http://www.facebook.com/">http://www.facebook.com/</a></td>
</tr>
<tr>
<td>url12</td>
<td>REG_SZ</td>
<td><a href="http://mrbool.com/course/csharp-4-0-course/269">http://mrbool.com/course/csharp-4-0-course/269</a></td>
</tr>
<tr>
<td>url15</td>
<td>REG_SZ</td>
<td><a href="http://localhost/ProfgaberSite">http://localhost/ProfgaberSite</a></td>
</tr>
<tr>
<td>url16</td>
<td>REG_SZ</td>
<td><a href="http://www.youm7.com/">http://www.youm7.com/</a></td>
</tr>
<tr>
<td>url17</td>
<td>REG_SZ</td>
<td><a href="http://youm7/">http://youm7/</a></td>
</tr>
<tr>
<td>url18</td>
<td>REG_SZ</td>
<td><a href="http://localhost/ProfgaberWebSite/Default.aspx">http://localhost/ProfgaberWebSite/Default.aspx</a></td>
</tr>
<tr>
<td>url19</td>
<td>REG_SZ</td>
<td><a href="http://www.google.com/">http://www.google.com/</a></td>
</tr>
<tr>
<td>url20</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/installation.php">http://www.abomarium.net/installation.php</a></td>
</tr>
<tr>
<td>url22</td>
<td>REG_SZ</td>
<td><a href="http://localhost/">http://localhost/</a></td>
</tr>
<tr>
<td>url23</td>
<td>REG_SZ</td>
<td><a href="http://tekpub.com/view/asnet4/6">http://tekpub.com/view/asnet4/6</a></td>
</tr>
<tr>
<td>url24</td>
<td>REG_SZ</td>
<td><a href="http://www.tansik.egypt.gov.eg/Results/">http://www.tansik.egypt.gov.eg/Results/</a></td>
</tr>
<tr>
<td>url25</td>
<td>REG_SZ</td>
<td><a href="http://www.youtube.com/watch?v=qw_8m40unXAI&amp;list=PL61AF4914C2862882&amp;index=1&amp;feature=plpp_video">http://www.youtube.com/watch?v=qw_8m40unXAI&amp;list=PL61AF4914C2862882&amp;index=1&amp;feature=plpp_video</a></td>
</tr>
<tr>
<td>url3</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/user/AdelSabo4?feature=CBwQwRS%3D">http://www.abomarium.net/user/AdelSabo4?feature=CBwQwRS%3D</a></td>
</tr>
<tr>
<td>url4</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/installation">http://www.abomarium.net/installation</a></td>
</tr>
<tr>
<td>url5</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/robots.txt">http://www.abomarium.net/robots.txt</a></td>
</tr>
<tr>
<td>url6</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/index.php">http://www.abomarium.net/index.php</a></td>
</tr>
<tr>
<td>url7</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/administrator">http://www.abomarium.net/administrator</a></td>
</tr>
<tr>
<td>url8</td>
<td>REG_SZ</td>
<td><a href="http://www.abomarium.net/administrators">http://www.abomarium.net/administrators</a></td>
</tr>
<tr>
<td>url9</td>
<td>REG_SZ</td>
<td><a href="http://www.mans.edu.eg/">http://www.mans.edu.eg/</a></td>
</tr>
</tbody>
</table>
WEB application server attack investigation

- On June 1, 2012, the client M/s xxx received a complaint from the ISP that the server is sending repeated mails to random ID’s.
- The Destination IP’s were blocked yet the problem was not resolved.
- This time it was again some executable that making the connections and generating the unknown traffic.
WEB application server attack investigation.
“Cont’d”

• The entire investigation was to be done on the live system as the same was being used in critical production environment. The access to the server being placed in US was provided through RDP “Remote Desktop Protocol”.
Following activities were performed by the investigation team:

- Identified the Key Indicators of compromise
- Identified and analyzed the network traffic.
- Log analysis to identify the critical events
- Analyzed the malware/ crafted tools for further back door and access maintenance
- Evaluated the entire methodology.
- Analyzed the Registry data and registry slack
• The Result:
• After entire investigation the entire process was found. The malware installation used a unique process with **Registry hives**:
• A Registry key was created in the auto run section
• \(\text{HKEY}\_\text{LOCAL}\_\text{MACHINE}\\text{\Software}\\text{\Microsoft}\\text{\Windows}\\text{\CurrentVersion}\\text{\Run}\\) as follows:
WEB application server attack investigation.

“Cont’d”

Clearly the Key did the following tasks
- Stopped the Windows firewall
- Opened a command that created the connection to the IP 111.67.192.11
- Entered the User name as “chajjan” and password as “123”
- Switched to binary mode
- Downloaded the file “seo.exe”
- Executed the executable

The executable performed the following tasks
- Deleted the key from the registry
- Started the reverse connection to the IP 111.67.192.11
- Provided the entire control to the remote user
- Download a second file with the same modus operandi
- Execute the same
WEB application server attack investigation. “Cont’d”

• The Second executable created a VB script to edit the group policy and run
  • The script entered values that will execute during shutdown
    • It creates the Key to download again the same file on the next boot.
  • As the Keys were repeatedly inserted and deleted the same could be traced in the registry slack.
• The analysis revealed that it was executed at least 23 times and the oldest of it was on Jan 21, 2010.
• The corroborative logs from the date (Jan 21, 2010) showed nothing and probably the server
  • was compromised far earlier than the date of last deleted entry available.
• The remains of “persistant script” for backdooring was found and the analysis suggested probably the use of “Metasploit framework” for initial compromise.
Further analysis revealed the remains of unscheduled backup of the database (MS SQL) in the second partition of the drive.

This provides the initial date of stealing the database to be Dec 19, 2009.

Probably the database was taken down and copied in offline mode to the local drive and

to be transported to remote location later on at a lower bandwidth.

The dates have already been shared with the ISP for further log analysis.

All credit for this case investigation goes to:

Boonlia Prince Komal
Director (Technology)

Sahil Modgil
Research Assistant
Conclusion

• When a crime takes place it becomes like a

• Because of the
Conclusion

• As a Digital Forensics experts we seek to
Finally.....
Any Questions?! I can only take 3 questions  
Or you can mail me and I will Respond ASAP  
Ahmed.neil@owasp.org