



Digital Forensics

What, Why, and How

By: Ahmed M. Neil

OWASP Mansoura Egypt, Chapter leader
Ireland, 2013

Ahmed.Neil@owasp.org

Acknowledgment

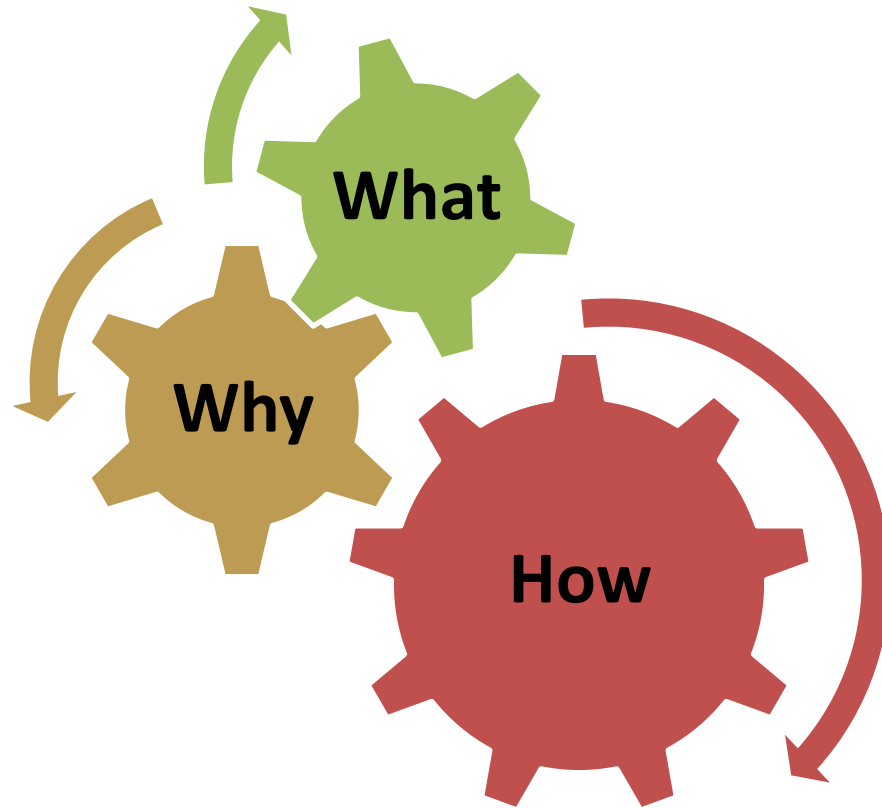


My Objective





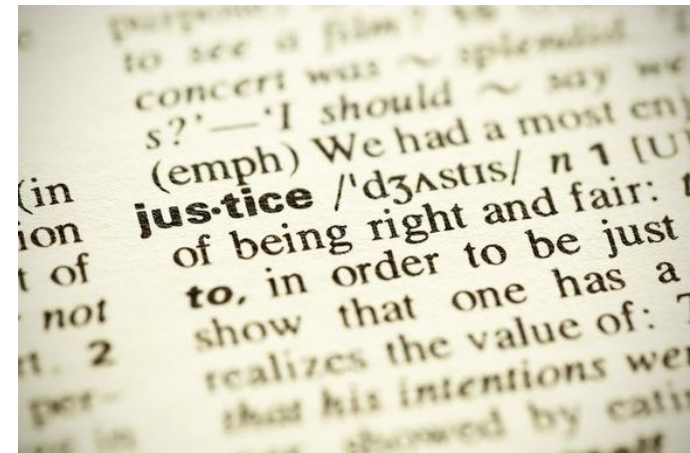
Agenda





Introduction

- **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].



[1] Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier.

[2] http://en.wikipedia.org/wiki/Digital_evidence#cite_note-casey-1

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.

BE CAREFUL

**THIS MACHINE
HAS NO BRAIN
USE YOUR OWN**



Evidence Admissibility

- To be admissible in a court of law evidence must be :
 - **Relevant**
 - **Legally permissible**
 - **Reliability**
 - **Identification.**
 - **Preservation.**

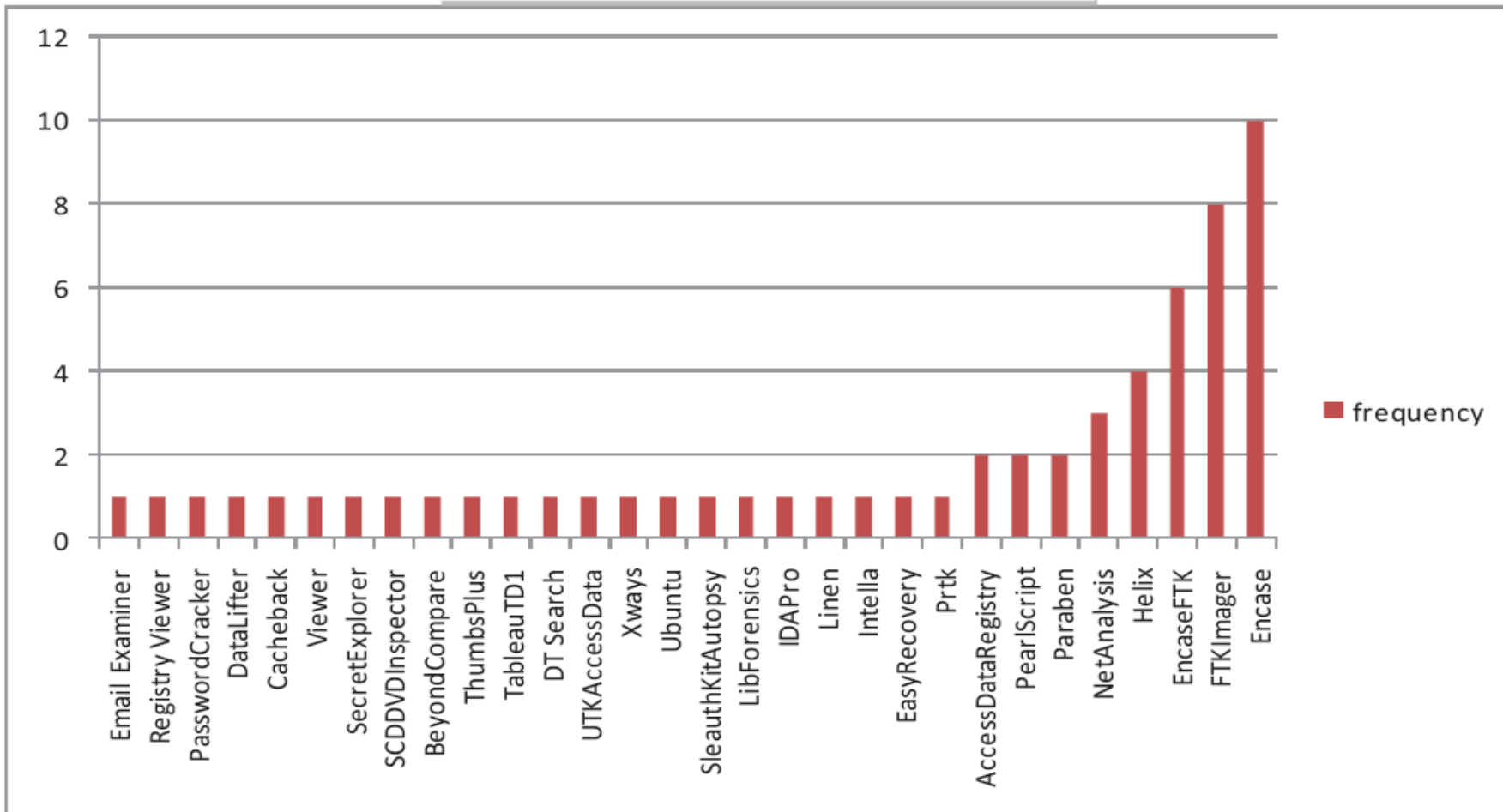


Digital forensic Tools



Digital forensic Tools

Preferred Software for Investigation





Digital forensic Tools cont'd

- Encase
- Access Data Forensic Toolkit
- Helix
- **dd**



Digital forensic Tools cont'd

- 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



Digital forensic Tools cont'd

- 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]#
```



Digital forensic Tools cont'd

- 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.**





Report generating tools

- 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

- <http://computer-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics>
- Or just google “ Digital forensics report samples”



Windows Registry

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

The screenshot shows the Windows Registry Editor. On the left is the tree view, and on the right is a list of registry values. Arrows point from labels at the bottom to specific parts of the interface:

- Hives**: Points to the root of the tree view (My Computer).
- Keys**: Points to the SYSTEM\CurrentControlSet\LastKnownGoodRecovery key.
- Values**: Points to the (Default) value in the list.
- Data**: Points to the data field for the LastKnownGood value.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000003 (3)





Windows Registry cont'd

- List of applications and filenames of the most recent files opened in windows

The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure, with the path `My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32>LastVisitedMRU` selected. The right pane shows a list of registry values, with the 'h' value selected. An 'Edit Binary Value' dialog box is open, showing the value name 'h' and its binary data. The binary data is displayed in hexadecimal and ASCII format.

Hex	ASCII
0000 41 00 63 00 72 00 6F 00	A.c.r.o.
0008 52 00 64 00 33 00 32 00	R.d.3.2.
0010 2E 00 65 00 78 00 65 00	.e.x.e.
0018 00 00 43 00 3A 00 5C 00	.C.:.\
0020 44 00 6F 00 63 00 75 00	D.o.c.u.
0028 6D 00 65 00 6E 00 74 00	m.e.n.t.
0030 73 00 20 00 61 00 6E 00	s.a.n.
0038 64 00 20 00 53 00 65 00	d.S.e.
0040 74 00 74 00 69 00 6E 00	t.t.i.n.
0048 67 00 73 00 5C 00 74 00	g.s.\.t.
0050 73 00 63 00 68 00 77 00	s.c.h.w.
0058 61 00 72 00 7A 00 5C 00	a.r.z.\.
0060 4D 00 79 00 20 00 44 00	M.y.D.



Windows Registry cont'd

- List of applications and filenames of the most recent files opened in windows

The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure, with the path `My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32>LastVisitedMRU` selected. The right pane shows a list of registry values, with the 'h' value selected. An 'Edit Binary Value' dialog box is open, showing the value name 'h' and its binary data. The binary data is displayed in hexadecimal and ASCII format.

Hex	ASCII
0000 41 00 63 00 72 00 6F 00	A.c.r.o.
0008 52 00 64 00 33 00 32 00	R.d.3.2.
0010 2E 00 65 00 78 00 65 00	.e.x.e.
0018 00 00 43 00 3A 00 5C 00	.C.:.\
0020 44 00 6F 00 63 00 75 00	D.o.c.u.
0028 6D 00 65 00 6E 00 74 00	m.e.n.t.
0030 73 00 20 00 61 00 6E 00	s..a.n.
0038 64 00 20 00 53 00 65 00	d..S.e.
0040 74 00 74 00 69 00 6E 00	t.t.i.n.
0048 67 00 73 00 5C 00 74 00	g.s.\.t.
0050 73 00 63 00 68 00 77 00	s.c.h.w.
0058 61 00 72 00 7A 00 5C 00	a.r.z.\.
0060 4D 00 79 00 20 00 44 00	M.y..D.



The Registry as a log file

“**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.

 (Default)	REG_SZ	(value not set)
 AppInit_DLLs	REG_SZ	
 DeviceNotSelectedTim...	REG_SZ	15





Scenario3 : 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





Scenario3 : Downloading and Viewing inappropriate photos “cont’d”

ActiveDownloads
Explorer
Advanced
ApplicationDestinations
AutoplayHandlers
BitBucket
CabinetState
CD Burning
CIDSave
CLSID
ComDlg32
 CIDSizeMRU
 FirstFolder
 LastVisitedPidIMRU
 LastVisitedPidIMRULe
 OpenSavePidIMRU
 *
 jpg
 pdf
Discardable
FileExts
HideDesktopIcons
LowRegistry
MenuOrder
Modules
MountPoints2
NewShortcutHandlers
RecentDocs
RunMRU
SearchPlatform
SessionInfo
Shell Folders
StartData

(Default)
REG_SZ (value not set)
REG_BINARY 0 14 00 1f 42 25 48 1e 03 94 7b c3 4d b1 31 e9 46 b4 4c 8d d5 74 00 00 00 1a 00 ee
REG_BINARY 1 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
REG_BINARY 2 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
REG_BINARY 3 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
REG_BINARY 4 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
REG_BINARY 5 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
REG_BINARY 6 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
REG_BINARY 7 14 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 20 00 00 00 1a 00 ee bl
MRUListEx REG_BINARY 07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 02 00 00 00 03 00 00 00 01 00 00 00

Edit Binary Value

Value name:
0

Value data:

0298	6D	00	65	00	6E	00	74	00	m.e.n.t.
02A0	73	00	00	00	40	00	73	00	s...@.s.
02A8	68	00	65	00	6C	00	6C	00	h.e.l.l.
02B0	33	00	32	00	2E	00	64	00	3.2...d.
02B8	6C	00	6C	00	2C	00	2D	00	l.l.,.-.
02C0	32	00	31	00	37	00	37	00	2.1.7.7.
02C8	30	00	00	00	18	00	74	00	0.....t.
02D0	32	00	00	00	00	00	00	00	2.....
02D8	00	00	80	00	77	61	72	6E	...warn
02E0	65	72	32	30	31	31	69	6A	er2011ij
02E8	63	63	2E	70	64	66	00	00	cc.pdf..

OK Cancel



Evidence Tree

G:\

- NONAME [FAT32]
 - [root]
 - AUTORUN.INF
 - CISSP course
 - Mahezain
 - RR
 - samples
 - HOT girls**
 - abd elghafar thesis
 - Fuzzy Logic Controller C#
 - New WinRAR ZIP archive.zip
 - Users
 - New Folder
 - !488156_
 - A7med_Nile
 - English_in_Use
 - 02.Pre-Intermediate
 - [unallocated space]

Name	Size	Type	Date Modified
------	------	------	---------------

Custom Content Sources

Evidence:File System Path File	Options
--------------------------------	---------



Scenario3 : Downloading and Viewing inappropriate photos “cont’d”

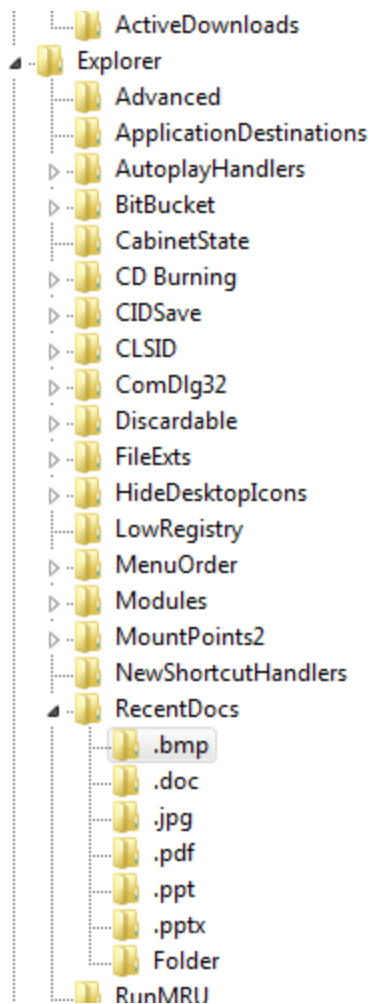
- To show all files recently executed or opened through Windows Explorer.
- files are organized according to file extension under respective subkeys and the Subkey Folder contains the folder of the recently open files.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs





Scenario3 : Downloading and Viewing inappropriate photos “cont’d”



Registry Editor view of MRUListEx:

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	48 00 6f 00 74 00 5f 00 67 00 69 00 72 00 6c 00 73 00
MRUListEx	REG_BINARY	00 00 00 00 ff ff ff ff

Edit Binary Value dialog box:

Value name: 0

Value data:

Offset	Hex	ASCII
0000	48 00 6F 00 74 00 5F 00	H.o.t._.
0008	67 00 69 00 72 00 6C 00	g.i.r.l.
0010	73 00 2E 00 62 00 6D 00	s...b.m.
0018	70 00 00 00 64 00 32 00	p...d.2.
0020	00 00 00 00 00 00 00 00
0028	00 00 48 6F 74 5F 67 69	..Hot_gi
0030	72 6C 73 2E 6C 6E 6B 00	rls.lnk.
0038	48 00 08 00 04 00 EF BE	H.....i%
0040	00 00 00 00 00 00 00 00
0048	2A 00 00 00 00 00 00 00	*.....
0050	00 00 00 00 00 00 00 00



Deleting important files scenario

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





Deleting important files scenario

- **Additional information:**
- 1st and 2nd 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.

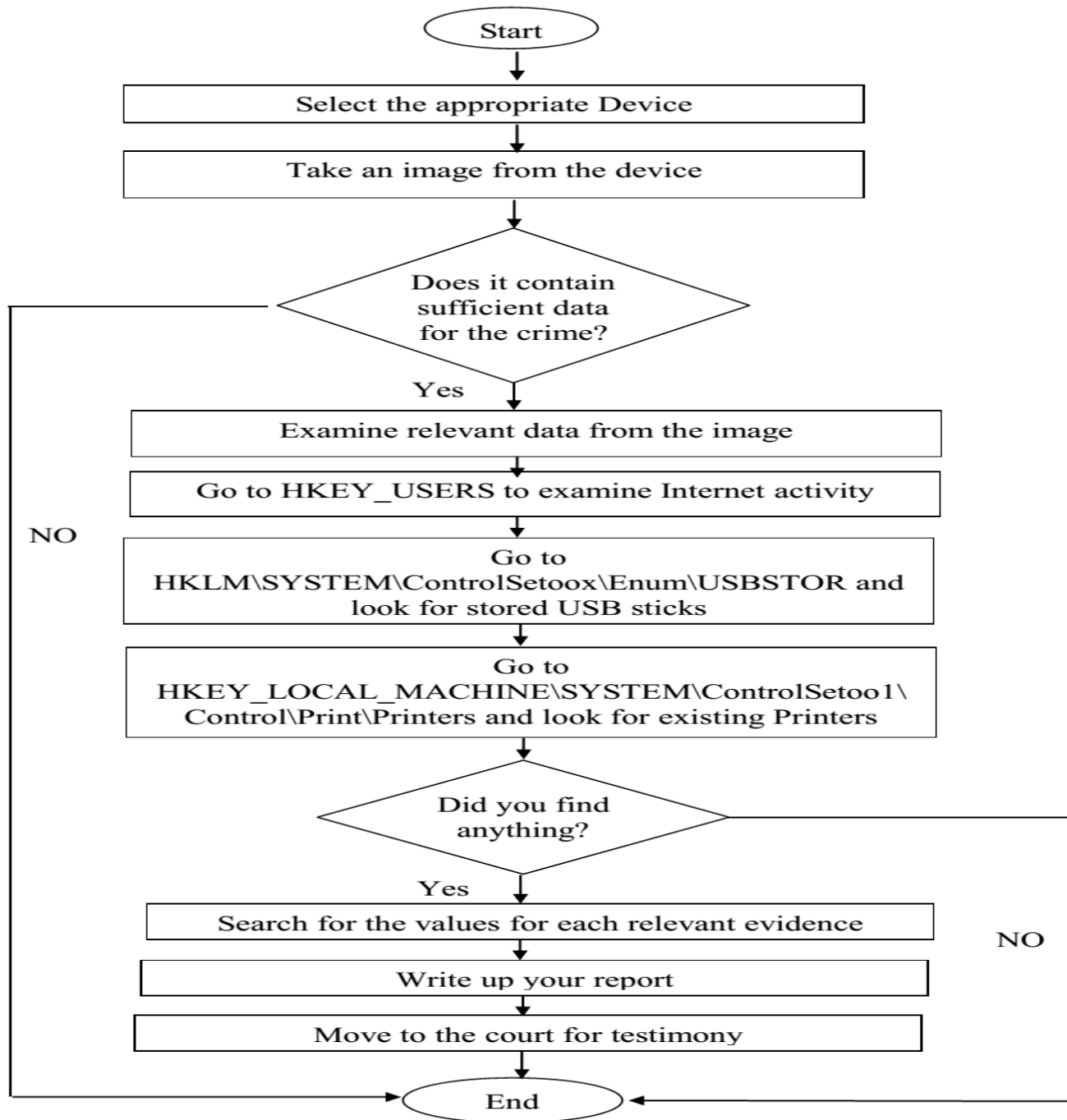




Online Fraud Crime Case study Cont'd

- **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;





Search

- GPActivities
- Help_Menu_URLs
- IEDevTools
- IESetting
- IEtId
- IntelliForms
- International
- InternetRegistry
- LinksBar
- LinksExplorer
- Low Rights
- LowRegistry
- Main
- MAO Settings
- MenuExt
- MINIE
- New Windows
- PageSetup
- PhishingFilter
- Privacy
- ProtocolExecute
- Recovery
- Safety
- SearchScopes
- SearchUrl
- Security
- Services
- Settings
- Setup
- SQM
- Styles
- Suggested Sites
- TabbedBrowsing
- TaskbarPreview
- Toolbar
- TypedURLs
- New Key #1
- URLSearchHooks

Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://www.amazon.com/
url10	REG_SZ	http://199.91.153.158/0hq8fb54052g/gyezhymmj0y/Anashed.Nasr.El.Deen.Toobar.Othersway.Com-By.Lely.zip
url11	REG_SZ	http://www.facebook.com/
url12	REG_SZ	http://mrbool.com/course/csharp-4-0-course/269
url13	REG_SZ	http://roque-patrick.com/windows/final/bbl0193.html
url14	REG_SZ	http://rapidgator.net/file/12824833/Tekpub.Mastering.Linq.part4.rar.html
url15	REG_SZ	http://localhost/ProfGaberSite
url16	REG_SZ	http://www.youm7.com/
url17	REG_SZ	http://youm7/
url18	REG_SZ	http://localhost/ProfGaberWebSite/Default.aspx
url19	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.abomariam.net/installation.php
url20	REG_SZ	http://localhost/ProfGaberWebApp/Default.aspx
url21	REG_SZ	http://localhost/
url22	REG_SZ	http://tekpub.com/view/aspnet4/6
url23	REG_SZ	http://www.tansik.egypt.gov.eg/Results/
url24	REG_SZ	http://www.youtube.com/watch?v=w_8m40unXAI&list=PL61AF4914C2862882&index=1&feature=plpp_video
url25	REG_SZ	http://www.youtube.com/user/AdelSabour?feature=CBwQwRs%3D
url3	REG_SZ	http://www.abomariam.net/installation
url4	REG_SZ	http://www.abomariam.net/robots.txt
url5	REG_SZ	http://www.abomariam.net/index.php
url6	REG_SZ	http://www.abomariam.net/administrator
url7	REG_SZ	http://www.abomariam.net/administrators
url8	REG_SZ	http://www.abomariam.net/
url9	REG_SZ	http://www.mans.edu.eg/



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*”.





WEB application server attack investigation. “Cont’d”

- 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





WEB application server attack investigation.

“Cont’d”

- 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
- (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\) as follows:





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.



WEB application server attack investigation.

“Cont’d”

- 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 take place it become like a

- Because of the





Conclusion

- **As a Digital Forensics experts we seek to**





Finally.....





Thanks!!



Any Questions?!

**I can only
take**

3 questions

**Or you can mail me
and I will Respond ASAP**

Ahmed.neil@owasp.org