Digital Forensic Techniques

Namrata Choudhury,
Sr. Principal Information Security Analyst,
Symantec Corporation

Professional Techniques – T23

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

CRISC
CGEIT
CISM
CISA

2013 Fall Conference – "Sail to Success"

AGENDA

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

Computer Forensics vs. Digital Forensics

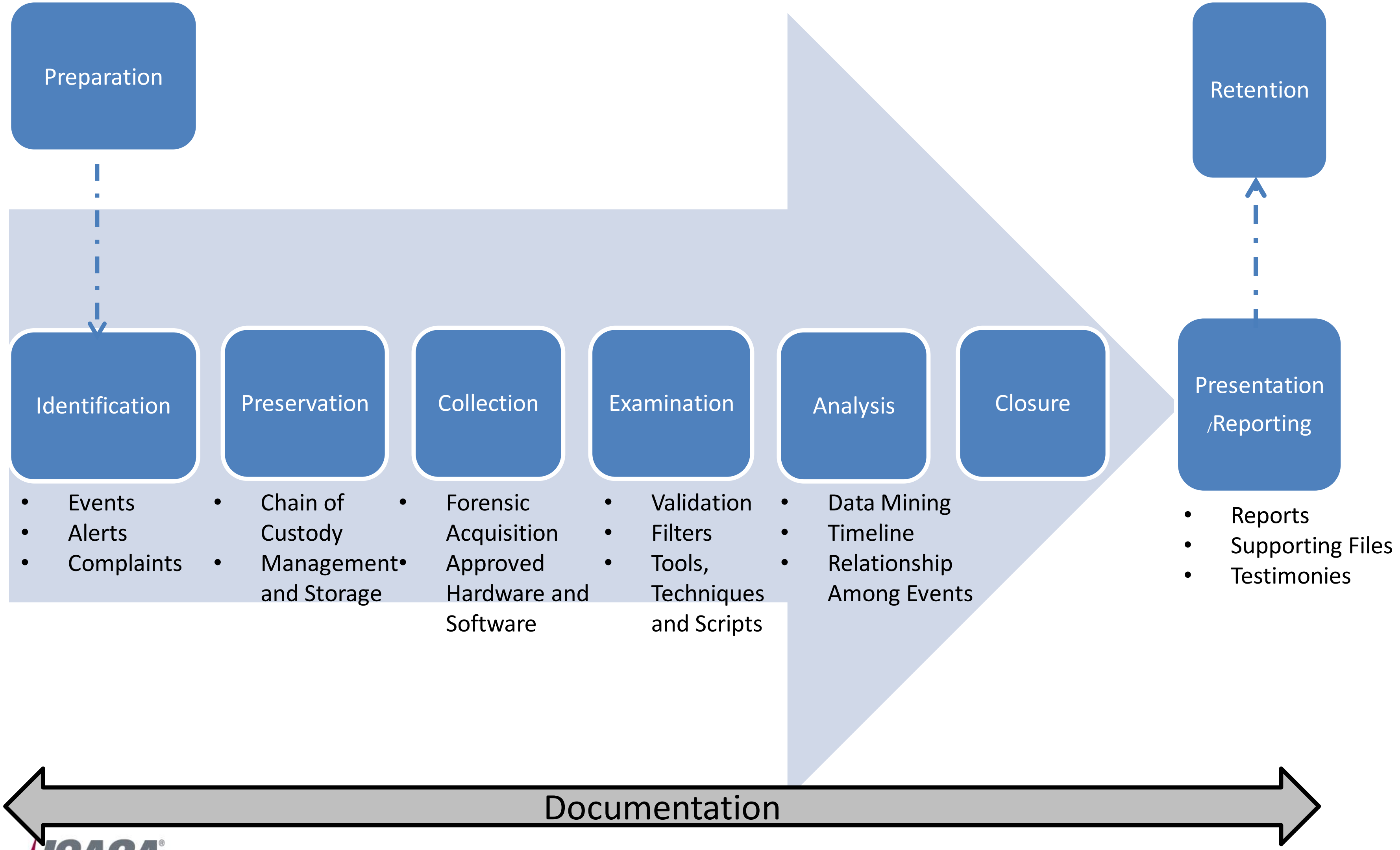
Computer Forensics vs Digital Forensics

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

Presentation /Reporting
- Reports
- Supporting Files
- Testimonies

Retention

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

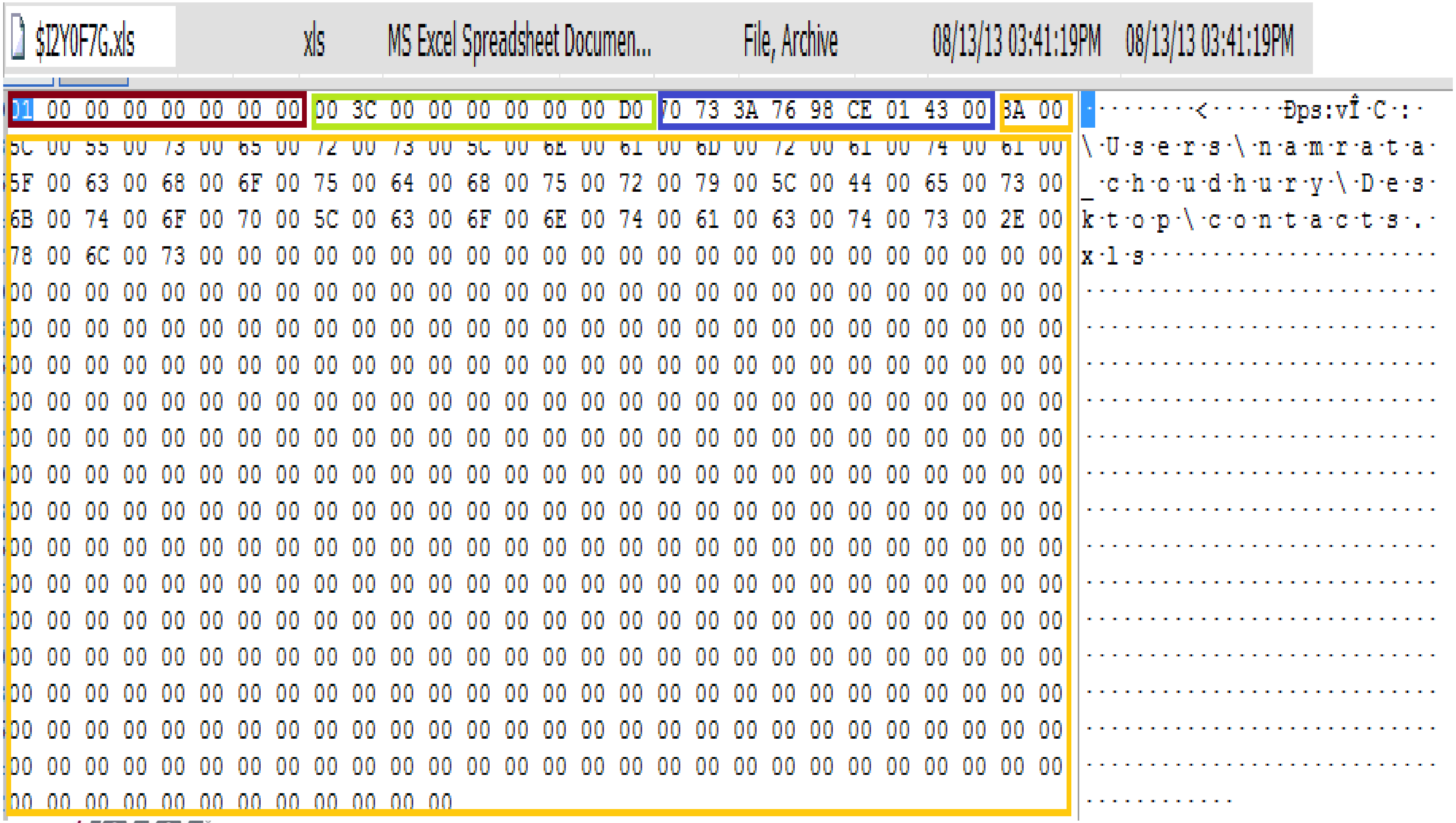
Why

- 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



```
$I2Y0F7G.xls    xls    MS Excel Spreadsheet Documen...    File, Archive    08/13/13 03:41:19PM    08/13/13 03:41:19PM

01 00 00 00 00 00 00 00 00 3C 00 00 00 00 00 00 D0 70 73 3A 76 98 CE 01 43 00 3A 00  ·········<······Ðps:vÎ·C·:·
5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6E 00 61 00 6D 00 72 00 61 00 74 00 61 00  \·U·s·e·r·s·\·n·a·m·r·a·t·a·
5F 00 63 00 68 00 6F 00 75 00 64 00 68 00 75 00 72 00 79 00 5C 00 44 00 65 00 73 00  _·c·h·o·u·d·h·u·r·y·\·D·e·s·
6B 00 74 00 6F 00 70 00 5C 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 73 00 2E 00  k·t·o·p·\·c·o·n·t·a·c·t·s·.·
78 00 6C 00 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  x·l·s·······················
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
00 00 00 00 00 00 00 00 00 00 00 00                                                  ············
```

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 de compress; 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

Name	File Ext	File Type	File Category	Signature	Description
letter.doc	doc	Word Document	Document	* JPEG Image Standard	File, Archive
EDRM-2-792.jpg	jpg	JPEG	Picture	Match	File, Archive
Vulnerability Report.pdf	pdf	Adobe PDF	Document	Match	File
DoNotIPs.xlsx	xlsx	MS Excel Spreadsheet	Document\Spreadsheet	Match	File, Archive
LogedLog.txt	txt	Text	Document	Match	File, Archive
Examples				Unknown	Folder

Analysis Phase - Internet History

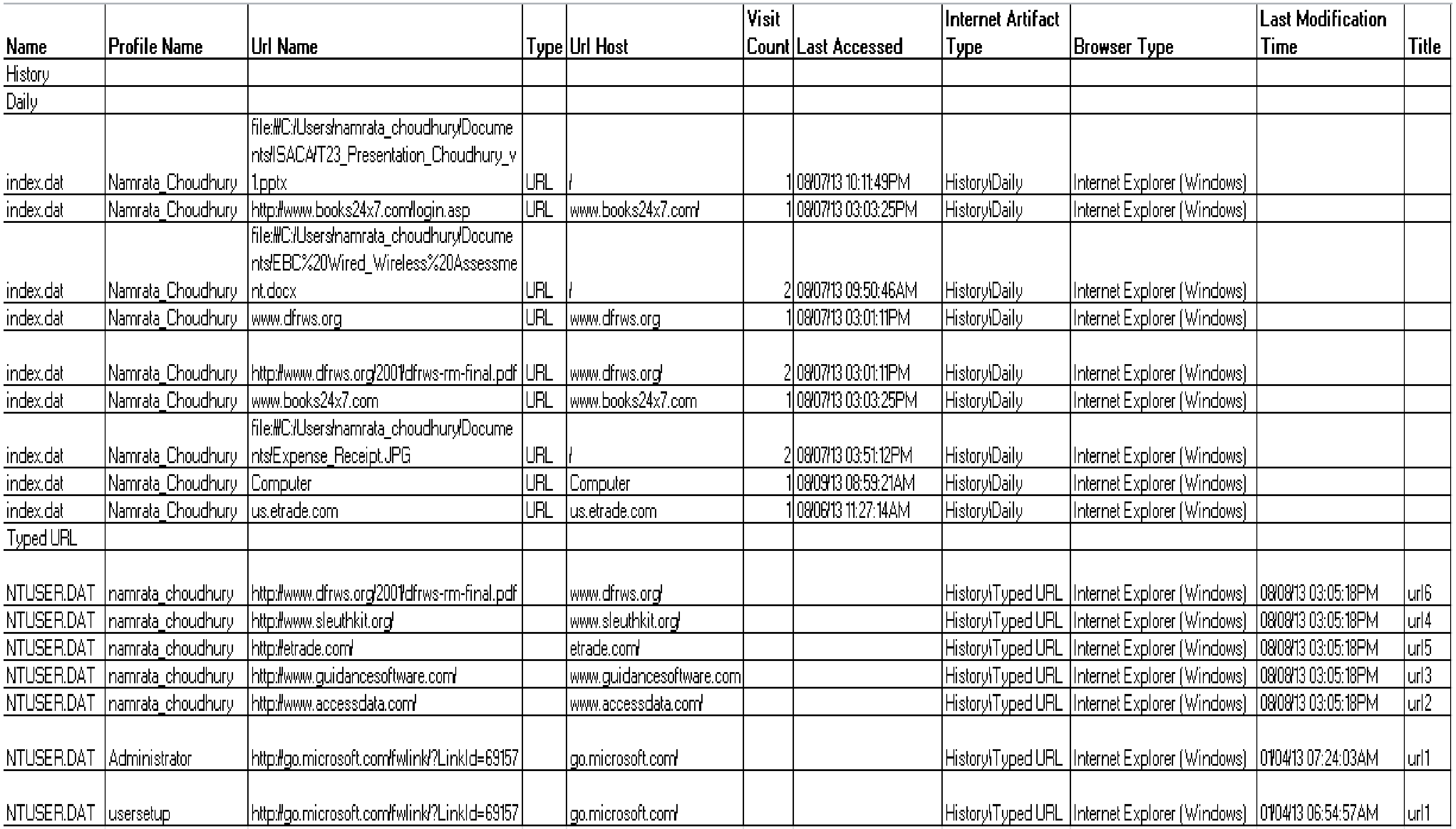
Why

- 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

Internet History - Example



Name	Profile Name	Url Name	Type	Url Host	Visit Count	Last Accessed	Internet Artifact Type	Browser Type	Last Modification Time	Title
History										
Daily										
index.dat	Namrata_Choudhury	file:///C:/Users/namrata_choudhury/Documents/ISACA/T23_Presentation_Choudhury_v1.pptx	URL	/	1	08/07/13 10:11:49PM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	http://www.books24x7.com/login.asp	URL	www.books24x7.com/	1	08/07/13 03:03:25PM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	file:///C:/Users/namrata_choudhury/Documents/EBC%20Wired_Wireless%20Assessment.docx	URL	/	2	08/07/13 09:50:46AM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	www.dfrws.org	URL	www.dfrws.org	1	08/07/13 03:01:11PM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	http://www.dfrws.org/2001/dfrws-rm-final.pdf	URL	www.dfrws.org/	2	08/07/13 03:01:11PM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	www.books24x7.com	URL	www.books24x7.com	1	08/07/13 03:03:25PM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	file:///C:/Users/namrata_choudhury/Documents/Expense_Receipt.JPG	URL	/	2	08/07/13 03:51:12PM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	Computer	URL	Computer	1	08/09/13 08:59:21AM	History\Daily	Internet Explorer (Windows)		
index.dat	Namrata_Choudhury	us.etrade.com	URL	us.etrade.com	1	08/06/13 11:27:14AM	History\Daily	Internet Explorer (Windows)		
Typed URL										
NTUSER.DAT	namrata_choudhury	http://www.dfrws.org/2001/dfrws-rm-final.pdf		www.dfrws.org/			History\Typed URL	Internet Explorer (Windows)	08/08/13 03:05:18PM	url6
NTUSER.DAT	namrata_choudhury	http://www.sleuthkit.org/		www.sleuthkit.org/			History\Typed URL	Internet Explorer (Windows)	08/08/13 03:05:18PM	url4
NTUSER.DAT	namrata_choudhury	http://etrade.com/		etrade.com/			History\Typed URL	Internet Explorer (Windows)	08/08/13 03:05:18PM	url5
NTUSER.DAT	namrata_choudhury	http://www.guidancesoftware.com/		www.guidancesoftware.com			History\Typed URL	Internet Explorer (Windows)	08/08/13 03:05:18PM	url3
NTUSER.DAT	namrata_choudhury	http://www.accessdata.com/		www.accessdata.com/			History\Typed URL	Internet Explorer (Windows)	08/08/13 03:05:18PM	url2
NTUSER.DAT	Administrator	http://go.microsoft.com/fwlink/?LinkId=69157		go.microsoft.com/			History\Typed URL	Internet Explorer (Windows)	01/04/13 07:24:03AM	url1
NTUSER.DAT	usersetup	http://go.microsoft.com/fwlink/?LinkId=69157		go.microsoft.com/			History\Typed URL	Internet Explorer (Windows)	01/04/13 06:54:57AM	url1

Analysis Phase - Registry Analysis

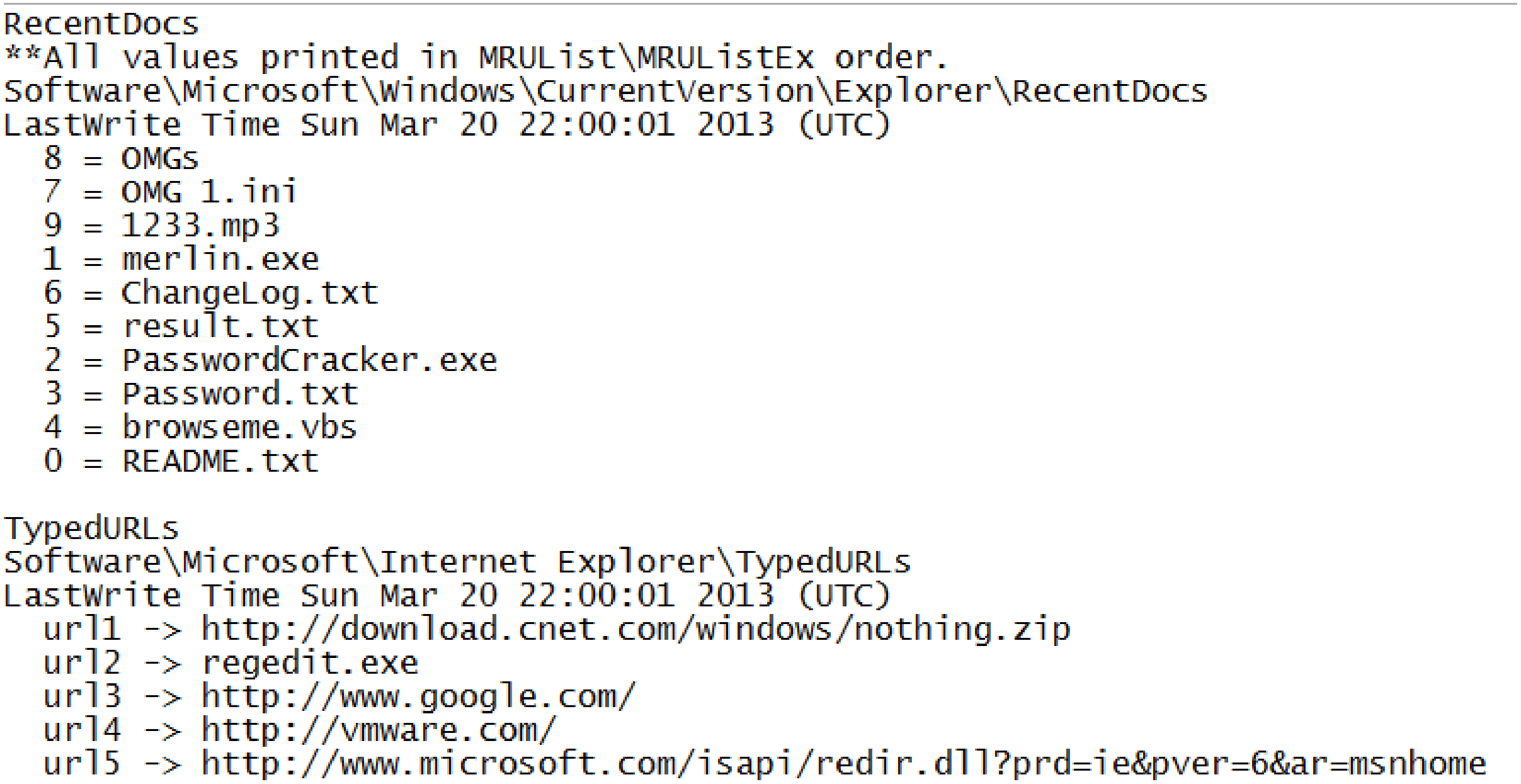
Why

- 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/
  url5 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
```

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 http://www.dfrws.org/2001/dfrws-rm-final.pdf
- Computer Forensics: An Overview by Frederick Gallegos, 2005, http://www.isaca.org/Journal/Past-Issues/2005/Volume-6/Documents/jpdf0506-Computer-Forensics-An.pdf
- Cyber Crime Investigations by Anthony Reyes et al. Syngress Publishing, 2007
- 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?