FORFUN

Week 3 Case Examination

Soraya Harding & Rahim Taheri

Session Content

- Examination types
- Examination categories

Dead & Live Examination

Dead Examination

- Dead examination involves checking the suspect machine in a non-booted fashion
- Case Management Software (e.g. FTK/Encase) mounts the suspect's file system – changes are cached by the tool – the analysis remains "dead"
- Benefits
  - The integrity of the suspect's data is ensured
  - No instant decision is required
  - Analysis can be repeated

Case Management Tools

- Tools that can manage the complete forensic process
  - Process a wide range of data types (e.g. emails); analyse the registry; decrypt files; crack passwords; and build a report
  - Reduces the time required to identify and document evidence
- Examples:
  - Guidance Encase, Access Data FTK ($3995), Internet Evidence Finder ($1700)
  - Autopsy, Digital Forensic Framework

Live Analysis

- Live analysis utilizes the suspects machine in a booted fashion for examination
  - Bespoke applications where its not possible to obtain a (licensed) version
  - Understanding how a piece of malware is behaving
  - Case dependent
- Order of volatility
  - Main physical memory, virtual memory, network state, running processes, hard drive, backup media, external storage (e.g. USB)
- Tools: Regshot, WinDirStat, net file, net session

Live Analysis

Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net session

Computer                User name            Client Type       Opens Idle time
-------------------------------------------------------------------------------
\\192.168.1.40          forensics                                 4 00:00:02

The command completed successfully.
```

Administrator: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>net file

ID          Path                                  User name            # Locks
-------------------------------------------------------------------------------
67108991    C:\Users\forensics                    forensics              0
67108994    C:\Users\forensics\Contacts\desktop.ini forensics            0
67108995    C:\Users\forensics\Desktop\desktop.ini  forensics            0
67108996    C:\Users\...\Documents\desktop.ini    forensics              0
67108997    C:\Users\...\Downloads\desktop.ini    forensics              0
67108998    C:\Users\...\Favorites\desktop.ini    forensics              0
67108999    C:\Users\forensics\Links\desktop.ini  forensics              0
67109015    C:\Users\desktop.ini                  forensics              0
67109018    C:\Users\                             forensics              0
67109021    C:\Users\forensics\Music\desktop.ini  forensics              0
67109022    C:\Users\forensics\Pictures\desktop.ini forensics            0
67109024    C:\Users\...\Saved Games\desktop.ini  forensics              0
67109025    C:\Users\forensics\Videos\desktop.ini forensics              0
67109026    C:\Users\forensics\Searches\desktop.ini forensics            0
67109054    C:\Users\forensics\Desktop            forensics              0
The command completed successfully.
```

Evidence in Volatile Memory

C:\Windows\system32\cmd.exe

```
pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for LL05710:

Name                 Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                   0   0   4    0      0    5:45:30.489     1:45:10.874
System                 4   8 202 6366    144    0:01:51.119     1:45:10.874
smss                 396  11   3   32    580    0:00:00.078     1:45:10.874
csrss                732  13   9 1140   2472    0:00:02.449     1:45:04.743
wininit              808  13   3   85   1652    0:00:00.218     1:45:01.124
csrss                932  13  13  739  11280    0:00:16.879     1:45:01.108
services             972   9  11  326   8784    0:01:11.588     1:45:01.030
lsass                988   9  10 1165   7924    0:00:54.381     1:45:00.905
OSPPSVC             6148   8   4  154   9632    0:00:23.930     1:36:20.664
WUDFHost            2736   8   9  204   1988    0:00:00.109     1:35:55.667
jucheck             7416   8   6  325   6956    0:00:01.123     1:35:28.104
POWERPNT            4920   8  12  541 106592    0:05:58.365     0:46:07.511
splwow64            6472   8   6   92   5048    0:00:00.156     0:46:06.497
mspaint             6156   8   6  124  86636    0:00:13.759     0:36:31.814
regedit             8148   8   1   71   5476    0:00:10.545     0:24:43.411
chrome              4004   4  15  339  71400    0:00:18.517     0:23:34.181
chrome              3612   8  13  240  47608    0:01:44.676     0:22:50.624
chrome              5912   8  11  294  53432    0:00:05.725     0:22:48.423
chrome               196   4  11  214  26532    0:00:01.310     0:22:44.755
AcroRd32            5508   8  13  272  10352    0:00:03.244     0:07:30.797
AcroRd32            6480   8  18  430 155064    0:00:46.269     0:07:30.126
TrustedInstaller    2100   8   5  126   4476    0:00:28.610     0:05:38.679
cmd                 5416   8   1   25   2364    0:00:00.015     0:00:29.720
conhost             5408   8   2   55   1884    0:00:00.078     0:00:29.541
pslist              2600  13   1  159   2828    0:00:00.421     0:00:00.531
```

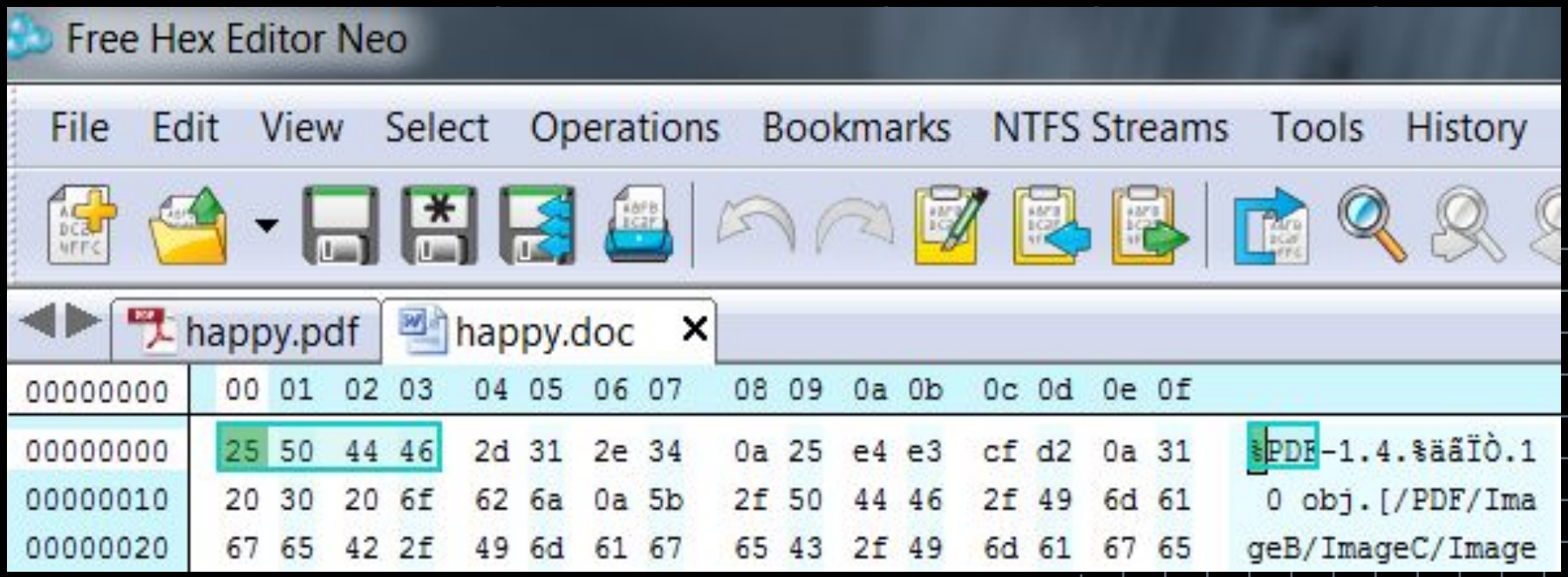
Examination Categories

File System (1)

- Data categories of a file system
  - File system: contains the general file system information – NTFS, FAT, EXT2
  - Content*:* contains the data that comprise the actual content of a file
  - File name: contains the data that assigns a name to each file – a.txt, b.docx
  - Metadata: contains the data that describes a file – MAC times

File System (2)

- Hashing for known and notable files
  - National Software Reference Library (NSRL)
  - National Child Victim Identification Program (NCVIP)
- File Signature Analysis



Data Carving Types

- Simple Data Carving:
  - The beginning of the file is not overwritten
  - The file is not fragmented
  - The file is not compressed (e.g. NTFS compressed) or encrypted
  - File signatures are not common contents (e.g. 0x6F66 – “of”, 0x6D79 – “my”)
- Advanced Data Carving:
  - The file is fragmented
  - Segments of file are out of order
  - Parts of the file are missing (e.g. header, footer and content)

Data Carving Techniques

- Header-Footer carving: using distinct byte patterns signifying the start and end of a file
- Header-Maximum file size carving carves a fixed number of bytes from the beginning of a file
- Header-Embedded File Length Carving: based on the size of the file embedded within the first few bytes of the file
- File structure based carving: using knowledge of the file internal structure

Application-Level Analysis (1)

ChromeHistoryView - C:\Users\lifudong\Desktop\History

File Edit View Options Help

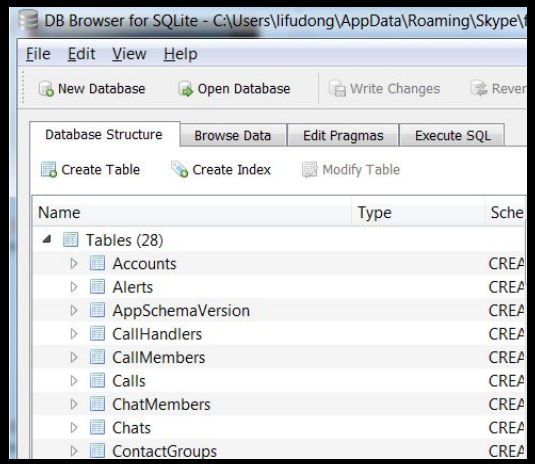
URL	Title	Visited On	Visit Count	Typed Count
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	18/08/2017 09:38:24	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	29/08/2017 11:49:12	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	29/08/2017 11:50:58	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	31/08/2017 14:17:15	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	01/09/2017 13:14:59	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	08/09/2017 16:27:18	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	12/09/2017 08:57:49	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	14/09/2017 14:52:40	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	17/09/2017 07:54:01	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	19/09/2017 16:22:08	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	20/09/2017 12:29:25	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	21/09/2017 15:57:11	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	22/09/2017 12:42:40	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	29/09/2017 08:02:09	28	23
http://www.bbc.co.uk/weather/2639996	BBC Weather - Portsmouth	29/09/2017 14:45:39	28	23

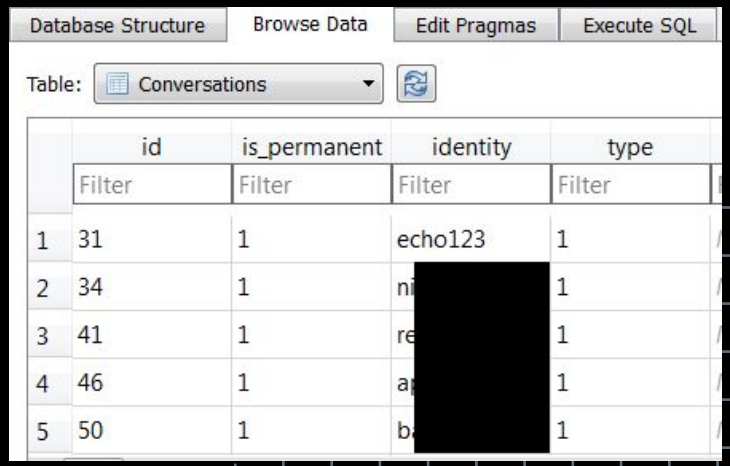
47167 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Application-Level Analysis (2)

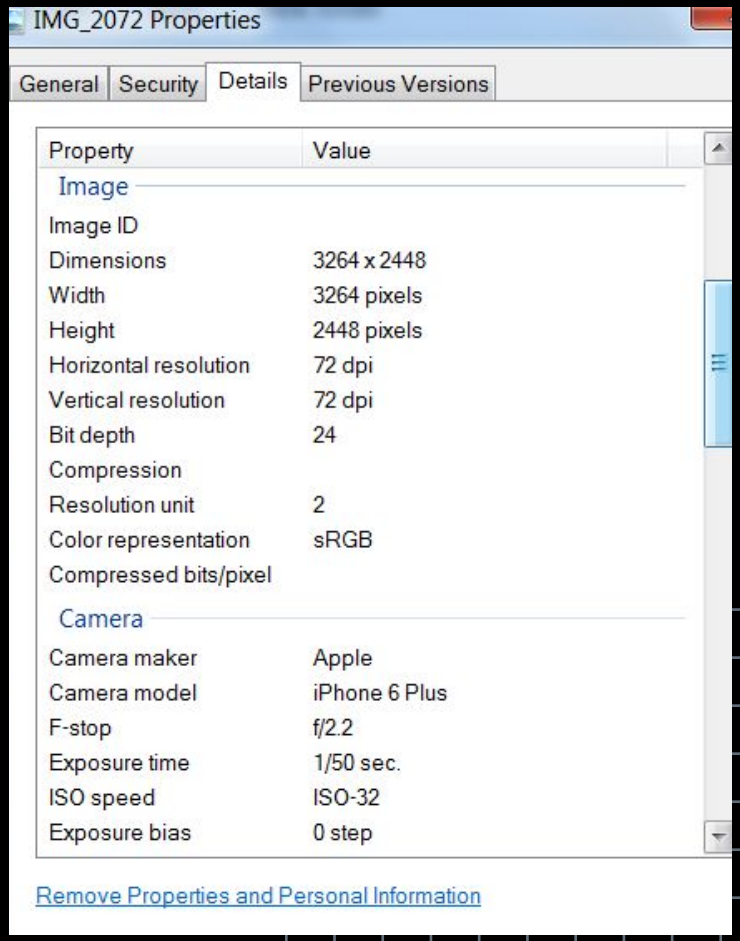
- For bespoke or less popular applications:
  - Install the client application on the forensic machine and use it to interpret the proprietary file
  - Develop a parser
  - View the proprietary file
  - Perform a live analysis on the host machine (more specifically, using an image of the host machine)





Multimedia Analysis

- Photos:
  - EXIF data: Dimensions, camera maker and model, flash mode, location info, MAC times, size…
  - Fuzzy hashing: identifies files that are similar but not exact equals
  - PhotoDNA: investigation on child abuse
- Videos:
  - Thumbnail creation from videos (x by min)
- Audios:
  - Could be used for data hiding



Search methods

- Regular Expression: Used to identify particular patterns within the image
  - Operates independently of the file system
  - \<[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\>

\<	The start of a word	[ ]	Set- match any one thing inside
\>	The end of a word	.	Match any one thing
-	Range delimiter	?	Match 1 or 0 preceding instances
\	Escape character	{ n }	Do the preceding thing n times
( )	Groups together a sub-expression, a sequence of characters that must be treated as a group and not as individual operands.		