Forensic Analysis

The Treachery of Images

Alexandre Dulaunoy

a@foo.be

February 5, 2016

Disclaimer

Rene Magritte "La Trahison des Images" ("The Treachery of Images") (1928)

Gangster Story

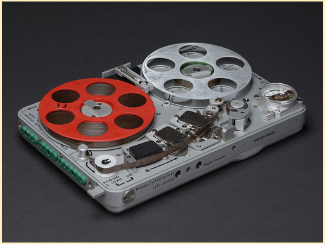
- The Italian gangster and forensic analysis...

Gangster Story

- Moral of the story : ”learning forensic analysis is useful even for gangster”.
- Forensic Analysis can help to discover any media sanitization defect.

A story from the other side...

Nagra SNST Recorder (gathered by Matt Blaze)



- An audio recorder (including a tape) purchased via eBay.
- But the tape contains an evidence recording of a confidential informant.
- `http://www.crypto.com/blog/watching_the_watchers_via_ebay/`.

Forensic Analysis - Theory

- Broad definition of (computer) forensic analysis : *"Forensic analysis involves the preservation, identification, extraction, documentation and interpretation of computer data"*
- *To reach those goals, the forensic specialists follow clear and well-defined methodologies. Flexibility is highly required when encountering the unusual.*

Forensic Analysis - Theory - Methodology

- Acquire the evidence without altering or modifying the original source.
- Authenticate that you gathered the evidence in a proper way.
- Analyze the non-original collected data without modifying it.

Forensic Analysis - Theory - Methodology

- Act always in ways that you can easily explaing to a court.
- Think twice before doing any action on the collected data.
- Take notes of everything not only the action taken but also any discoveries.

Forensic Analysis - Theory - The Order of Volatility (OOV)

The expected life of data :

Type of Data	Life Span
Registers or cache	Nanoseconds
Main Memory	Ten Nanoseconds
Network State	Milliseconds
Running Processes	Seconds
Disk	Minutes
Backup Medias	Years
CD-ROMS or printouts	Tens of years

Sometimes a small process trace can explain more than 50 gigabytes of a single backup...

Forensic Analysis - Theory - Layer(s)

- A computer system is a machine playing with the "treachury of images".
- An operation is often using one or more abstraction to be completed.
- The top-down approach of information from high-meaning to low-meaning is critical for forensic analysis.
- Computers become more and more mature but become less predictable at the row level.

Forensic Analysis - Theory - Layer(s) - The File System case

The file system is a great source of forensic information but :

- Forensic data must captured at the right layer. (e.g. using the tool of the file system is useful but not enough)
- Be prepare to collect partial information.
- File system analysis is often the next step after a detection. (e.g. from the network)
- File system analysis can be time consuming.

Forensic Analysis - General Practice

- First rule : Stay calm.
- Second rule : Limit risk but keep OOV in mind.
- Third rule : Never work on real data.

Forensic Analysis and Incident Response

- (Prevention)
- Detection
- Analysis
- Containment
- Investigation
- Eradication
- Postmortem

Forensic Analysis and Training

- The best way to be prepared for doing forensic analysis. It's to do it regularly.
- Participate to the reverse challenge of the honeynet project.
- Collect old filesystem and try to understand the last actions executed on the system.
- Prepare your legal staff to forensic analysis.

File System Analysis

File System Analysis can be used for

- Analysis the activities of an attacker on the honeypot file system.
- Analysis of a malware leaving traces on the file system.
- Analysis of a compromised system to recover legitimate and malicious activities.
- Recovering lost files or data on a file system.
- Correlating and validating memory or network analysis with the file system activities.

File System Analysis - Time is critical

Don't forget the following points:

- Timestamps stored on a system are not always in the same format (e.g. some might be in UTC, GMT or in system-local time).
- Timestamps can be also in different format (e.g. Epoch timestamp in 32-bit or 64-bit, NTFS 64-bit timestamp).
- Timezone and time are also important on your analysis workstation (e.g. don't mixup your timezone and the analysis timezone).
- Summer time and winter time are not the same in various timezones.
- GMT and UTC are not the same.
- Don't forget to take note of all the time, time zone or time references given during an acquisition.

File System Analysis - Format?

- ntfs (NTFS)
- fat (FAT (Auto Detection))
- ext (ExtX (Auto Detection))
- iso9660 (ISO9660 CD)
- hfs (HFS+)
- ufs (UFS (Auto Detection))
- raw (Raw Data)
- swap (Swap Space)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (Ext2)
- ext3 (Ext3)
- ufs1 (UFS1)

File System Analysis - Interface,Support and Acquisition

- SATA, IDE, USB 3.0/2.0/1.1, SAS, and FireWire (1394A/B).
- Acquisition in software or hardware?
- Support of the acquisition to another equivalent disk?
- Can we trust the acquisition process[1]?
- How long it will take?

[1] http://events.ccc.de/congress/2012/Fahrplan/events/5327.en.html Prototyping Active Disk Antiforensics

File System Analysis - Tools

Many proprietary and free software tools exist for file system analysis. In this lab, we will use sleuthkit[2] as a basis.

- Sleuthkit is including TCT (the coroner toolkit) but evolved overtime to support more file system and new tools.
- Sleuthkit got a GUI companion called Autopsy.
- Sleuthkit is able to analyze a lot of file system format from raw acquisition.
- Sleuthkit supports the extraction of metadata and timeline from supported file system in a non intrusive way.

[2] http://www.sleuthkit.org/

From raw to file systems

Extracting partition information:

```
mmls /home/adulau/dess/disk-image/raw.dd.raw
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000096   0000000097   Unallocated
02:  00:00   0000000097   0000250879   0000250783   DOS FAT16 (0x06)
```

Extracting the BOOT sector:

```
 dd if=/home/adulau/dess/disk-image/raw.dd.raw seek=0 count=97 bs=512 of=/tmp/boot
```

File System Analyses - SleuthKit - fls

fls lists file and directory names in a disk image.

```
fls -lr  -o 97 /home/adulau/dess/disk-image/raw.dd.raw
/usr/local/bin/fls -r -p fat-test.dd
```

As this is the representation of the file system, you can dump/recover files based on their inode reference

```
/usr/local/bin/icat fat-test.dd  965
```

```
fls -lr -m / -o 97 /home/adulau/dess/disk-image/raw.dd.raw | mactime -b -
Thu Jan 01 1970 01:00:00  3541836 ..c. r/rrwxrwxrwx 0        0        1029     /DCIM/111
                          2255115 ..c. r/rrwxrwxrwx 0        0        1030     /DCIM/111
                              884 ..c. r/rrwxrwxrwx 0        0        183301   /DCIM/CAN
                                0 ..cb r/rrwxrwxrwx 0        0        3        /CANON_DC
(Volume Label Entry)
                            16384 ..c. d/drwxrwxrwx 0        0        4        /DCIM
                            16384 ..c. d/drwxrwxrwx 0        0        517      /DCIM/111
                            16384 ..c. d/drwxrwxrwx 0        0        518      /DCIM/CAN
Sun Jun 02 2013 00:00:00  3541836 .a.. r/rrwxrwxrwx 0        0        1029     /DCIM/111
                          2255115 .a.. r/rrwxrwxrwx 0        0        1030     /DCIM/111
                              884 .a.. r/rrwxrwxrwx 0        0        183301   /DCIM/CAN
                                0 .a.. r/rrwxrwxrwx 0        0        3        /CANON_DC
(Volume Label Entry)
                            16384 .a.. d/drwxrwxrwx 0        0        4        /DCIM
                            16384 .a.. d/drwxrwxrwx 0        0        517      /DCIM/111
                            16384 .a.. d/drwxrwxrwx 0        0        518      /DCIM/CAN
Sun Jun 02 2013 15:42:32  3541836 m..b r/rrwxrwxrwx 0        0        1029     /DCIM/111
                            16384 m..b d/drwxrwxrwx 0        0        4        /DCIM
                            16384 m..b d/drwxrwxrwx 0        0        517      /DCIM/111
Sun Jun 02 2013 15:42:46  2255115 m..b r/rrwxrwxrwx 0        0        1030     /DCIM/111
Sun Jun 02 2013 15:44:08      884 m..b r/rrwxrwxrwx 0        0        183301   /DCIM/CAN
                            16384 m..b d/drwxrwxrwx 0        0        518      /DCIM/CAN
Sun Jun 02 2013 16:33:04        0 m... r/rrwxrwxrwx 0        0        3        /CANON_DC
(Volume Label Entry)
```

SleuthKit - fls - mactime

Usually in forensic analysis, you'll need to have a time line sorted for all the events on a file system. SleuthKit provides a tool called mactime allowing to use fls output to generate a time line.

```
/usr/local/bin/fls -mr fat-test.dd
   | /usr/local/bin/mactime -b -
```

SleuthKit - fls - mactime output

Mactime output and file system interpretation:

fs	m	a	c	b
EXT2/3	Modified	Accessed	Changed	N/A
FAT	Written	Accessed	N/A	Created
NTFS	File Modified	Accessed	MFT Modified	Created
UFS	Modified	Accessed	Changed	N/A

Mactime is doing an interpretation of the fls output. It might be missing some additional timestamp from some file system format (e.g. the deleted timestamp in Ext2/3). Extended time or values can usually be check with "istat".

SleuthKit - Autopsy Forensic Browser

Autopsy Forensic Browser[3] is a web interface to the SleuthKit toolsuite and provide an easy way to handle forensic analysis. Take the existing image and test it with Autopsy.

[3] http://www.sleuthkit.org/autopsy/index.php

Bibliography

- Forensic Discovery, Dan Farmer, Wietse Venema, Addison Wesley ω
- Incident Response, Kenneth R. Van Wyk, O'Reilly
- Computer Forensics, Incident Response Essentials, Warren G. Kruse, Addison Wesley
- File System Forensic Analysis, Brian Carrier, Addison Wesley
- Mechanisms, New Media and the Forensic Imagination, Matthew G. Kirschenbaum, The MIT press ω

Use case 1

- You have a public web server, hosted in a datacenter, that has been compromised (the main page has been defaced).
- The public web server also contains private information from the customer (mainly login and password).
- What should I do ?

Use case 2

- A laptop from a potential hostile employee has been given to you for analysis.
- What should I do ?

Use case 3

- You discovered a enterprise server with a proprietary software installed and doing unusual network connection to Internet.
- How forensic analysis could help me ?

Use case 4

- An employee gave you a flashcard where he would like to recover documents deleted ?
- How you would proceed ?

Q and A

- Thanks for listening.
- a@foo.be