Forensic Analysis - 2nd Lab Session

File System Forensic and Analysis

Alexandre Dulaunoy

adulau@foo.be

December 12, 2014

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)
- ufs2 (UFS2)

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/`

File System Analysis - SleuthKit - fls

fls lists file and directory names in a disk image.

```
/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
```

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 Foresinc Analysis, Brian Carrier, Addison Wesley
- Mechanisms, New Media and the Forensic Imagination, Matthew G. Kirschenbaum, The MIT press ω

Q and A

- Thanks for listening.
- a@foo.be