Lab 6

Forensic analysis

Contents

6.1 Objetives

Students will learn the basic procedures and methodologies that must be taken into account when performing a forensic analysis. It is also expected that after the lab you will increase your understanding of the forensic tools and applications needed to solve most of the security incidents where a digital evidence is involved.

6.2 Requisites

1. Download the class notes regarding Forensics.
2. Download the image Ubuntu64-18LTSv1 from the Software Repository available at the FIB (`softdocencia.fib.upc.edu/software`) or reuse the image already downloaded for the previous labs
3. Start Ubuntu OS.
4. **Autopsy is already installed in this image**. Following instructions are for reference in case you want to install it in another Ubuntu distribution

(in the second line, you're adding the universe packages to the repository /etc/apt/sources.list; write the whole command in one line):

```
sudo bash
sudo add-apt-repository "deb http://archive.ubuntu.com/ubuntu
          $(lsb_release -sc) universe"
apt-get update
apt-get install autopsy
```

5. Execute autopsy in background with **root privilege** and open the autopsy in the browser (http://localhost:9999/autopsy).

6. Download the image.zip file from Atenea (usually downloaded in /home/ubuntu/Downloads)

7. mount the image.zip file:

```
sudo bash
unzip image.zip
mkdir /mnt/disk
mount -o loop image /mnt/disk
```

More about loop device: A loop device is a file that acts as a block-based device. A loop device is therefore a pseudo-device that makes a file accessible as a block device. Loop devices are often used for CD ISO images and floppy disc images. Mounting a file containing a filesystem via such a loop mount makes the files within that filesystem accessible. They appear in the mount point directory using above commands.

Now you've mounted the disk image in /mnt/disk and in /home/ubuntu/Downloads you have the disk image to be analyzed in Autopsy.

6.3 Lab description

The following lab was taken from the honeynet project, a non profit organisation committed to "raise awareness of the threats and vulnerabilities that exist in the Internet today".

One of the most known actions of the honeynet project were the scan of the month challenges, the purpose of which was "to help the security community develop the forensic and analysis skills to decode real attacks".

In this lab we will go through scan of the month 24[1]. Here is the challenge description:

"Your mission is to analyse a recovered floppy and answer the questions below. What makes this challenge unique, you will need to read the police report before continuing your challenge (the police report is included at the end of this document). Just like an investigation in the real world, you will have some background

[1] http://www.honeynet.onofri.org/scans/scan24/

information and some evidence, but it's up to you and your technical skills to dig up the answers. In Atenea there is the disk image of the recovered floppy. This is the image that will provide you the answers, providing you can extract the data".

6.4 Goals

The prove you understand the different steps and solve the case, you are requested to answer the following questions. These questions will help you to answer correctly to the test in Atenea.

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

6.5 Autopsy

The Autopsy Forensic Browser is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyse Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

Autopsy is HTML-based, therefore you can connect to the Autopsy server from any platform using an HTML browser (`http://localhost:9999/autopsy`). Autopsy provides a "File Manager"-like interface and shows details about deleted data and file system structures.

6.5.1 Evidence Search Techniques

- **File Listing**: Analyse the files and directories, including the names of deleted files and files with Unicode-based names.
- **File Content**: The contents of files can be viewed in raw, hex, or the ASCII strings can be extracted. When data is interpreted, Autopsy sanitises it to prevent damage to the local analysis system. Autopsy does not use any client-side scripting languages.
- **Hash Databases**: Lookup unknown files in a hash database to quickly identify it as good or bad. Autopsy uses the NIST National Software Reference

Library (NSRL) and user created databases of known good and known bad files.

- **File Type Sorting**: Sort the files based on their internal signatures to identify files of a known type. Autopsy can also extract only graphic images (including thumbnails). The extension of the file will also be compared to the file type to identify files that may have had their extension changed to hide them.

- **Timeline of File Activity**: In some cases, having a timeline of file activity can help identify areas of a file system that may contain evidence. Autopsy can create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files.

- **Keyword Search**: Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions. Searches can be performed on either the full file system image or just the unallocated space. An index file can be created for faster searches. Strings that are frequently searched for can be easily configured into Autopsy for automated searching.

- **Meta Data Analysis**: Meta Data structures contain the details about files and directories. Autopsy allows you to view the details of any meta data structure in the file system. This is useful for recovering deleted content. Autopsy will search the directories to identify the full path of the file that has allocated the structure.

- **Data Unit Analysis**: Data Units are where the file content is stored. Autopsy allows you to view the contents of any data unit in a variety of formats including ASCII, hexdump, and strings. The file type is also given and Autopsy will search the meta data structures to identify which has allocated the data unit.

- **Image Details**: File system details can be viewed, including on-disk layout and times of activity. This mode provides information that is useful during data recovery.

6.5.2 Case Management

- **Case Management**: Investigations are organised by cases, which may contain one or more hosts. Each host is configured to have its own time zone setting and clock skew so that the times shown are the same as the original user would have seen. Each host may contain one or more file system images to analyse.

- **Event Sequencer**: Time-based events can be added from file activity or IDS and firewall logs. Autopsy sorts the events so that the sequence of incident events can be more easily determined.

- **Notes**: Notes can be saved on a per-host and per-investigator basis. These allow you to make quick notes about files and structures. The original location can be easily recalled with the click of a button when the notes are later reviewed. All notes are stored in an ASCII file.
- **Image Integrity**: It is crucial to ensure that files are not modified during analysis. Autopsy, by default, will generate an MD5 value for all files that are imported or created. The integrity of any file that Autopsy uses can be validated at any time.
- **Reports**: Autopsy can create ASCII reports for files and other file system structures. This enables you to quickly make consistent data sheets during the investigation.
- **Logging**: Audit logs are created on a case, host, and investigator level so that actions can be easily recalled. The exact Sleuth Kit commands that are executed are also logged.
- **Open Design**: The code of Autopsy is open source and all files that it uses are in a raw format. All configuration files are in ASCII text and cases are organised by directories. This makes it easy to export the data and archive it. It also does not restrict you from using other tools that may solve the specific problem more appropriately.
- **Client Server Model**: Autopsy is HTML-based and therefore you do not have to be on the same system as the file system images. This allows multiple investigators to use the same server and connect from their personal systems.

6.5.3 Case Creation in a Nutshell

Before starting using the autopsy browser, we have to set up some configurations:

1. Open a new case: it is necessary to provide a case and investigators names
2. Add a new host: it is necessary to provide a host name
3. Add an image: it is necessary to provide the complete location of the recovered floppy disk image[2]. The importation has to be done as “partition” and “Symlink”. You can ignore the MD5 checking.

6.5.4 Useful Autopsy Views

Here, we provide you some usefull information to make your life easier with autopsy:

1. Show the file content of the disk: to see the complete content of the diskette go to “analyze” -> “file analysis”. Here you can access to the complete file metadata information of each file.

[2]Note: you need to import the image not the mounted disk

2. Show the details of the image: to see the general file system details of the diskette go to "analyze" -> "image details". Here you can access to the information regarding the size of the cluster, the metadata and content information and, more important, which sectors contain data.

3. Show the file allocation disk: to see the allocated sectors of the image file you can go to "analyze" -> "data unit" -> "Allocation list"

4. Export some data sector into a new file: go to "analyze" -> "data unit" -> select the initial data sector and the number of sectors you want to export, then click "view" -> "export"

6.6 Some hints for the case

To help you in this case, we provide the following hints:

- The first file seems a jpg picture. Try to open it in the /mnt/disk directory. There is something wrong with this picture. Analyse with autopsy the metadata (column Meta) and check the consistency with the size and the sectors. Hints: i) each sector is 512 bytes long; ii) the image has a JPEG JFIF format; iii) you can select in "Data Unit" a starting sector and the number of sector and export the entire content to a file.

- The second file is highlighted in red: meaning it was deleted but autopsy recovered it. Hints: check the sectors in metadata (column Meta) and try to recover the entire file using the sector allocation capability in the "Data Unit".

- The third file seems an excel file. Hints: i) check the inconsistency between the sectors occupied by this last file and the image details (end at sector 105 vs end at sector 108); ii) the file is zipped and protected by a password; iii) you need to find the password in one of the previous files (check the hexdump)

6.7 References

- FAT, https://forensicswiki.xyz/wiki/index.php?title=FAT, http://www.c-jump.com/CIS24/Slides/FAT/lecture.html#F01_0020_fat

- Magic Numbers, http://en.wikipedia.org/wiki/File_format#Magic_number

- Autopsy, http://www.sleuthkit.org/autopsy/

6.8 Joe Jacobs police report

The scenario is: Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students. A local police officer posed as a high school student

was approached by Jacobs in the parking lot of Smith Hill High School. Jacobs asked the undercover cop if he would like to buy some marijuana. Before the undercover cop could answer, Jacobs pulled some out of his pocket and showed it to the officer. Jacobs said to the officer 'Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, he grows it himself.'

Jacobs has been seen on numerous occasions hanging out at various local high school parking lots around 2:30pm, the time school usually ends for the day. School officials from multiple high schools have called the police regarding Jacobs' presence at their school and noted an increase in drug use among students, since his arrival.

The police need your help. They want to try and determine if Joe Jacobs has been selling drugs to students at other schools besides Smith Hill. The problem is no students will come forward and help the police. Based on Joe's comment regarding the Colombians, the police are interested in finding Joe Jacob's supplier/producer of marijuana.

Jacobs has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer. Jacobs also refuses to validate the statement that he made to the undercover officer right before his arrest. Upon issuing a search warrant and searching of the suspect's house the police were able to obtain a small amount of marijuana. The police also seized a single floppy disk, but no computer and/or other media was present in the house.

The police have imaged the suspect's floppy disk and have provided you with a copy. They would like you to examine the floppy disk and provide answers to the following questions. The police would like you to pay special attention to any information that might prove that Joe Jacobs was in fact selling drugs at other high schools besides Smith Hill. They would also like you to try and determine if possible who Joe Jacob's supplier is.

Jacob's posted bail set at $10,000.00. Afraid he may skip town, the police would like to get him locked up as soon as possible. To do so, the police have asked that you have the results fully completed and submitted by December 16, 2020. Please provide the police with a strong case consisting of your specific findings related to the questions, where the findings are located on the disk, processes and techniques used, and any actions that the suspect may have taken to intentionally delete, hide and/or alter data on the floppy disk. Good Luck!

Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.