INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

File System Analysis

2017/2018

{danielporto, nuno.m.santos}@tecnico.ulisboa.pt

Introduction

The goal of this assignment is to exercise your skills in file system forensics. It comprises two exercises which require the examination of two independent file systems, Ext3 and FAT32, respectively. For this assignment we recommend you to use The Sleuth Kit (TSK)[1], file carving tools such as foremost or scalpel, and other helper tools such as strings, grep, file, and dd. We suggest you to look for documentation and usage examples of these tools on the Internet. You will need to download two archives from the website containing the artifacts to be analyzed in each exercise: `compromized.zip`, and `usb-drive.zip`. Both files are available at `http://web.tecnico.ulisboa.pt/~danielporto/csf1718/lab2/`. To analyze these artifacts, we recommend you to use the Kali Linux distribution.

Exercise 1: Infected server

Consider a server which we suspect might be infected by malware. Your task is to perform a forensic analysis of the server's file system. You have access to the server's HDD, which we emulate with a virtual disk named `linux.vmdk`. The virtual disk was formatted to Ext3 file system and it was compressed into a 99MB-sized tarball file (`compromized.zip`). The MD5 of the virtual disk file is:

MD5: `261d5f0f2ccfcfe5d0b80da4cb4d65fc`

This time is your turn to properly collect all evidences. The virtual disk file we provide is not a collected HDD image in this case. It is simply a way to emulate the actual hard drive detached from the server under analysis. You have to attach the virtual disk to your virtual forensic station using Virtualbox. Next, create a forensically sound image of the virtual disk and each one of its partitions. You must use a storage created according to the instructions of Tutorial 1 to properly save all artifacts you may find. You can check the disk partition information with fdisk -l, mmstat and fsstat tools. Then, perform a forensic analysis of the collected image by executing the following tasks:

1. Try to recover all deleted files from folder `/var/log`. Some useful tools for performing this task are available in the Sleuthkit package [2]. Write a small report in which you describe the contents of each file. Would you be able to tell why some of the recovered files do not look like ordinary log files?

2. In addition to the log files successfully obtained in the previous task, it is possible to collect further relevant data from the disk. In particular, there are fragments of file server and web server logs that can be retrieved from unallocated disk regions. These logs correspond, respectively, to the log files of samba (smbd) and apache (httpd) which were installed on the server. Search on the Internet for additional information about the format of samba and apache logs. Then, use this information to locate existing fragments of such logs. For this, we suggest you to use fls, grep, strings e blkcat. Extend the report of task 1 by describing your new findings and by providing a possible explanation for them.

Exercise 2: USB thumb-drive

In this exercise, you have to examine an image that was created from a USB thumb-drive. All we know is that this image is a "raw" partition image of a FAT32 file system. The file system is 62MB and is compressed to a 11MB zip file (`usb-drive.zip`). The MD5 of the image is:

MD5: `0069813c892a462f88dc6d376624f7d9`

[1] `https://www.sleuthkit.org`
[2] `http://wiki.sleuthkit.org/index.php?title=FS_Analysis`

Your task is to extract as many files you can from this image. Look for allocated as well as deleted files. If certain files are fragmented and cannot be entirely extracted, do the best you can to extract the largest fragments of such files. Write a report in which you provide the following information:

- **Description of obtained artifacts**: For each collected file or file fragment, indicate its size, their respective MD5 values, file type, and indication whether the artifact corresponds to a complete or to an incomplete file. Present this information in a table and assign an ID (a number) to each recovered file (this will help the explanation below).
- **Explanation:** Explain succinctly how you obtained each of the files or file fragments from the provided image. Refer to each of those artifacts by the assigned ID.

TIP: There are in total 15 files inside the file system. These files consist of documents, compressed files, images, audio, and movies. Their file formats are popular. Some files cannot be entirely extracted.

Deliverables

Your task is to analyze these artifacts and search for any evidence of industrial secrets that might be present in them. Write a forensic report that describes your findings. The deadline for this work is November 10^{th}. Until then, you must upload to Fenix a compressed zip file containing independent deliverables for exercises 1 and 2. For each exercise, provide four deliverables:

- **Digital Forensic Report**: A document in which you present your main findings according to what was requested in each exercise. You must identify all recovered evidence artifacts, if any, and explain how you obtained them. We suggest that you use the basic template that can be downloaded from the course website for this specific assignment.
- **Evidence Artifacts:** All evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.
- **Examination Log:** Consists of a document in which you must note down all steps that were performed during the investigation. A template of a sample examination log can be retrieved from the course website.
- **Auxiliary Items:** Programs, scripts, and additional documents that you have produced during the investigation which are important to justify your results must also be included.

Good luck!