INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

STORM AREA 51 – Stage II

2019/2020

nuno.m.santos@tecnico.ulisboa.pt

Introduction

In this assignment, you will continue the investigation of the case "Storm Area 51". In the first stage (see Lab Assignment I), you were given the task to obtain evidence about the leakage of secrets from Area 51 by analyzing the files contained in a pen drive. This second assignment will be focused on trying to explain how those secrets have been obtained by analyzing hard disk images and memory dumps. These artifacts can be downloaded from the course web site. To solve this exercise, you need to develop your skills in file and memory forensic techniques. As in the first assignment, we suggest you to use the Kali Linux distribution on a forensically sound virtual machine as a platform for performing this analysis.

Scenario presentation

As part of the USAF team that was responsible for the investigation of potential leakage of classified information from Area 51, your first task has been proven to be fruitful. Remember that your goal was to search for the existence of secrets enclosed in a set of digital artifacts (files) that where obtained from a pen drive located in Matty Robert's room; Matty was the responsible for creating an American Facebook event on September 20, 2019, to raid the Area 51 site in a search for extraterrestrial life. Interestingly, by analyzing the pen drive's files, the following relevant documents have been retrieved (can be downloaded from `http://turbina.gsd.inesc-id.pt/csf1920/secrets.tar.gz`):

File	MD5 Value	Description
f1.txt	`cd3000acd736503b927f678efe39d1c9`	Public and private key pair
f2.txt	`38558d9a74aa0cd516e5b1e3632984d0`	Short message listing the pieces of evidence to be found
f3.png	`348188142eec398b3621315a86afc54e`	Map of Area 51, pointing to the aliens' location
f4.wav	`5225d093f1c293407db195fa57bdf414`	Short message in morse code about the captive aliens
f5.wav	`1df1d41ca05096189bcd100acb35b1eb`	SOS morse code sent by the aliens
f6.mp3	`e915e7d07ee94d42fd178f2579c8dc49`	Recording about the leakage of classified information

Now that secrets have indeed been confirmed to have leaked, the next step is to investigate how they were stolen and who was responsible for this action. At the moment, we know that the pen drive was found inside Matty's dorm room. We also know that Matty shares his room with Tim Frasik, his long-time close friend. When confronted with these findings, Matty acknowledged the fact that the pen drive was his, but he blatantly refused to provide any further explanations about how the files have gotten into his pen drive. Tim was also interviewed, but he said he knew nothing about this business.

In light of these developments, you were called to investigate Matty's and Tim's computers in search for evidence about the provenance of said secrets. Their computers are Linux workstations, located in the dorm room, and connected to the local network, which in turn is connected to the Internet. Next, we have a compilation of the new material that we can analyze in our investigation:

- We have access to the hard disk images and to the memory dumps extracted by USAF's first responder team at the time the dorm room was searched and when the pen drive was retrieved. Below is the list of files containing the hard disk images and memory dumps:

File	MD5	Description
matty_disk	`d13c8103dc88de4e8b1a53002976aae5`	A forensic image of Matty's hard drive.
matty_mem	`fdc5796104c9b4f04d6cb1328a730812`	A memory dump of Matty's computer.
tim_disk	`b3143a90154f643e1826ff3432b2fdb7`	A forensic image of Tim's hard drive.
tim_mem	`7725be2d9cd98f618780b241f56c84d1`	A memory dump of Tim's computer.

- The IP addresses of Matty's and Tim's computers have been statically assigned, and are, respectively: `193.168.2.32`, and `193.168.2.27`.

- We found that Matty and Tim use the email addresses, `matty.roberts98@outlook.com` and `tim.frasik@gmail.com`, by checking that these email addresses were provided to the school as their primary contact points.
- We learned additional details about the pen drive, namely the serial number (`052513000000046E`) and the model (`General USB Flash Disk`).

The files containing the digital artifacts listed above can be downloaded from the course's website or directly from the following links:

- `http://turbina.gsd.inesc-id.pt/csf1920/matty_disk.tar.gz`
- `http://turbina.gsd.inesc-id.pt/csf1920/matty_mem.tar.gz`
- `http://turbina.gsd.inesc-id.pt/csf1920/tim_disk.tar.gz`
- `http://turbina.gsd.inesc-id.pt/csf1920/tim_mem.tar.gz`

In this exercise, your job is to analyze these digital artifacts and answer the following four questions. Justify your answers by providing all the relevant evidence you can find. Make sure to explain your hypotheses and how you have proceeded to validate them.

1. Are there any traces of the files that contain the leaked secrets in Matty's or Tim's computers?
2. Do you find any evidence suggesting that Matty or Tim were aware of the existence of these files?
3. Can you determine how the files containing the leaked secrets have been stolen from Area 51 and gotten into the pen drive? Establish a timeline of relevant events.
4. What can you tell about the identity of the person(s) responsible for leaking the secrets?

Deliverables

Write a forensic report that describes your findings. The deadline for this work is November 22^{nd}. Until then, you must upload to Fenix a compressed zip file containing three deliverables:

- **Digital Forensic Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend you to use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All relevant evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.
- **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.

TIPS: Use the Volatility profile available in `http://turbina.gsd.inesc-id.pt/csf1920/Ubuntu160406.zip` to help parse both memory dump.

Good luck!