INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

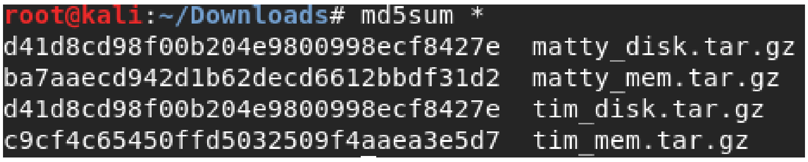
MEIC / METI 2019-2020 – 1st Semester

Digital Forensics Report

Afonso Oliveira (86367) **João Tavares (86443)** **Miguel Grilo (86489)**

General Overview

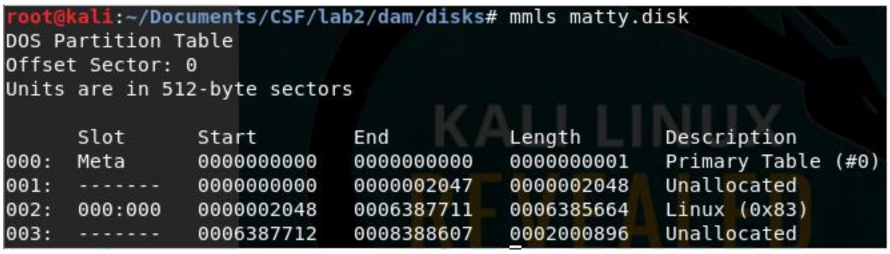
For our investigation, we used an install of *Kali Linux* so we could explore the files on a forensically sound machine. Using the command *md5sum*, we verified the *MD5 fingerprint* of the artifacts in order to ensure their integrity. We include all artifacts collected in Section 5 of this report with their respective *MD5 fingerprints* and content description.



```
root@kali:~/Downloads# md5sum *
d41d8cd98f00b204e9800998ecf8427e  matty_disk.tar.gz
ba7aaecd942d1b62decd6612bbdf31d2  matty_mem.tar.gz
d41d8cd98f00b204e9800998ecf8427e  tim_disk.tar.gz
c9cf4c65450ffd5032509f4aaea3e5d7  tim_mem.tar.gz
```

Figure 1 - MD5 fingerprint of the artifacts

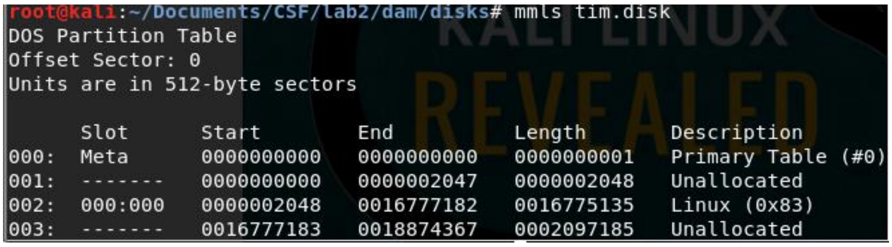
Our first step was analysing the disks, listing the partition tables with command *mmls*. In both disk images we were able to extract a regular Linux Ext4 File System partition, both presented in the output of *mmls*. In Matty's disk we were able to extract another partition that was supposedly "Unallocated" [Slot 003 - Ext3 File System] which turned out to contain relevant in regards to the purpose of our investigation.



```
root@kali:~/Documents/CSF/lab2/dam/disks# mmls matty.disk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0006387711   0006385664   Linux (0x83)
003:  -------   0006387712   0008388607   0002000896   Unallocated
```

Figure 2 - Matty's disk partition table



```
root@kali:~/Documents/CSF/lab2/dam/disks# mmls tim.disk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0016777182   0016775135   Linux (0x83)
003:  -------   0016777183   0018874367   0002097185   Unallocated
```

Figure 3 - Tim's disk partition table

Afterwards we extracted the partitions with the following commands:

```
dd if=matty_disk of=matty_part.dd skip=2048 count=6385664

dd if=tim_disk of=tim.dd skip=2048 count=16775135

dd if=matty.disk of=hidden_matty_part.dd skip=6387712 count=2000896
```

[Artifacts: *matty_part.dd*, *tim_part.dd*, *hidden_matty.dd*, respectively]

We analysed each one of those partitions navigating through the *inodes* structure using command *fls*. By doing so, we found some interesting information that can help us answer the main questions presented on this report.

***matty_part.dd* analysis:**

The home directory of *matty_part.dd* revealed a folder with a large number of emails exchanged between Matty and Tim [Artifact: *matty-emails.zip*]. We also found traces of a deleted PDF file named "*Dan Birlew - Naruto_ Ultimate Ninja (Prima Official Game Guide)-Prima Games (2006).pdf*", we tried to recover missing/corrupted files using *foremost* but we did not find anything interesting.

***hidden_matty.dd* analysis:**

In this partition of Matty's disk we found a series of interesting files including all the secrets from the previous report, with matching *MD5 signatures*, as well as images of an UFO, a video of an alien autopsy and some other less relevant files [Artifact: *matty-hidden.zip*].

***tim_part.dd* analysis:**

Analysing *tim_part.dd* we discovered not only those same emails but also another one he had received from the address yourfriend@gmail.com containing various files encoded in *base64* which we later decrypted. The names of the files attached to the email matched three deleted file names we had found in the partition (*run_me.bin*, *secrets* and *commands*) so we assumed Tim downloaded the files that were sent to him. There was also an unusual directory named *h4ks* which contained John the Ripper (both compressed and decompressed) as well an installer for the Metasploit Framework, two very popular hacking tools.

We searched in both partitions */var/log/syslog* for evidence related to the USB drive with the respective serial number, but we could only find such evidence on Tim's partition. Using the command *"icat tim_part.dd 1495 | grep 052513000000046E"* we obtained the following output (which indicates the drive had been plugged in to Tim's laptop):

```
Nov  2 18:38:56 tim kernel: [ 927.874379] usb 1-1: SerialNumber: 052513000000046E
```

Finally we ran *foremost* on this partition and recovered multiple audio files of an unidentified individual talking about running exploits and obtaining a shell [Artifact: *tim_wavs.zip*].

***matty.mem* analysis:**

We used the tool *Volatility* to analyse Matty's memory image. The most relevant information was his bash history [Artifact: *matty-linux-bash.dump*]. The command history indicates that he copied the secret files to a directory named */mydata*.

***tim.mem* analysis:**

In Tim's memory image we also used the *Volatility* tool for analysis. With the command *linux_bash* of *Volatility* we were able to confirm that Tim executed some relevant commands [Artifact: *tim-linux-bash.dump*], in particular the ones instructed to him by an email from "yourfriend@gmail.com".

1 Are there any traces of the files that contain the leaked secrets in Matty's or Tim's computers?

As previously referred, in Matty's "Unallocated" partition we found the same leaked files that were on the USB drive - *akamaru.bmp*, *masashi_kishimoto.txt*, *naruto_opening.wav*, *naruto_run.gif*, *naruto_scream.wav*, *naruto_wikipedia.txt* and *villains.zip*.

In Tim's disk, we were able to extract an email from yourfriend@gmail.com which contains instructions on how to download the encrypted secrets (the 6 artifacts found on the USB drive) from a server at https://10.10.9.14:8080 and instructions on how to decrypt them.

2 Do you find any evidence suggesting that Matty or Tim were aware of the existence of these files?

We recovered multiple emails between matty.roberts98@outlook.com (Matty Roberts) and tim.frasik@gmail.com (Tim Frasik) where they discuss the files in question, all the correspondence between the two is available at [Artifact: matty-emails.zip]. There is also a single email between tim.frasik@gmail.com (Tim Frasik) and yourfriend@gmail.com (Anonymous) [Artifact: yourfriend-email.txt] containing direct references to these files.

A detailed analysis of the emails can be found below:

On the 2nd of November 2019 between 06:57 and 07:21, Matty and Tim exchanged three emails. Matty initiated the conversation by sending "Hey, Tim! What's up? Got some news about that super-secret thing we've been talking about for a while now?" to which Tim replied "Not yet... But stay tuned, because we're about to wreak havoc on the ENEMY!!", finally Matty ended the conversation with "I can't wait to get my hands on that info. People need to know what's going on."

Later on that day, an email was sent to Tim from yourfriend@gmail.com (Anonymous) at 17:08 with the subject "The Truth". With that email, there was a list of commands (*commands.md*), a script (*run_me.py*) and some tools (*tools.zip*) that when put together would "recover each of the six secrets hidden" (the ones we had found on the previous report).

At 18:50, presumably after reading this message, Tim sent an email to Matty saying "I got the info. You won't believe it!! I have to show this to you and I need you to store it for me. Tim" to which Matty replied at 19:21 "Done! No one will ever find these files. They Can't Stop All of Us Matty".

These emails suggest that both Matty and Tim were aware of the existence of the secrets. Firstly they send emails about expecting some kind of "super-secret news". Afterwards Tim receives instructions on how to obtain the secret files from yourfriend@gmail.com (Anonymous) and then Tim sends Matty a message saying that he is in possession of the secrets and Matty answers by quoting the text of one of the secret files "They Can't Stop All of Us".

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.

On the 2nd of November at 17:08 yourfriend@gmail.com (Anonymous) sent an email to tim.frasik@gmail.com (Tim Frasik) containing resources to download and extract the leaked secrets from Area 51.

On the 3rd of November at 01:58 the following commands were run on Tim's computer (in this order):

```
mv commands.md tools.zip run_me.bin secrets/
```

python2.7 run_me.bin (Here is when Tim tries to use the python script we received on his email to download the secrets from a server located at https://10.10.9.14:8080. We assume the download failed because afterwards, he uses *pip* to install several dependencies required by the script)

Tim extracts the artifacts from the leaked secrets by following the instructions specified on the *commands.md* (also using the tools on *tools.zip*)

mount /dev/sdb1 usb_device/ (Tim mounts the USB drive)

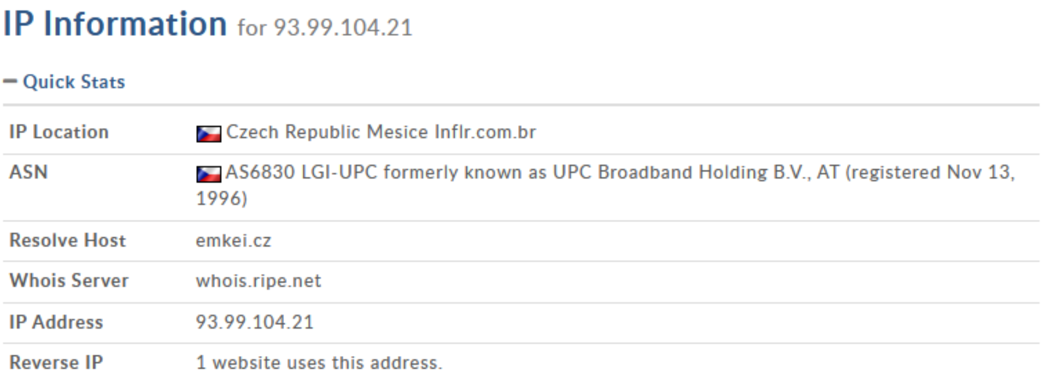
cp akamaru.bmp naruto_opening.wav attack naruto_run.gif villains.zip naruto_scream.wav masashi_kishimoto.txt naruto_wikipedia.txt usb_device/ (Tim copies the leaked secrets to the mounted USB)

umount /dev/sdb1 (Tim unmounts the USB)

Note: Since the IP address for the server from were Tim downloaded the files is private, we cannot determine the location of it by simply running *whois*. This indicates that Tim was connected to the same private network as the server when he downloaded the files.

4 What can you tell about the identity of the person(s) responsible for leaking the secrets?

During our initial investigation we were able to determine that the leaked secrets were downloaded by Tim, from a server located at https://10.10.9.14:8080, after being guided on how to do so by an email received at 17:08 of November 2nd 2019 [Artifact: *yourfriend-email.txt*]. We did some more research on the email address of the sender and were able to confirm our suspicions about it being a spoofed address. The leaker of the files used a email spoofing service (more info below) in order to conceal its identity making it impossible for us to accurately pinpoint the bad actor. It is relevant to notice that some audio files recovered from Tim's disk [Artifact: *tim_wavs.zip*] contained recordings of someone talking about successfully running an exploit what given the context leads us to believe the person in this recordings might be the same one who leaked the files to Tim.



IP Information for 93.99.104.21

− Quick Stats

IP Location	Czech Republic Mesice Inflr.com.br
ASN	AS6830 LGI-UPC formerly known as UPC Broadband Holding B.V., AT (registered Nov 13, 1996)
Resolve Host	emkei.cz
Whois Server	whois.ripe.net
IP Address	93.99.104.21
Reverse IP	1 website uses this address.

Figure 4 - whois report for the email spoofing service

Afterwards, as indicated by Tim's bash history, extracted from *tim.mem*, he copied the leaked secrets to an usb drive at 01:58:27 of November 3rd 2019. The */var/sys/syslog* file recovered from Tim's disk contains a log entry for an usb (serial number: 052513000000046E), the same serial number for the drive containing the previous report's secrets which indicates the secrets were copied into it by Tim.

5 Artifacts

We present below the list of the most relevant files found and produced during the investigation, a short description of their contents and their respective MD5 fingerprints.

artifacts/your-friend-files/original/		
File name	**MD5**	**File contents**
commands.md.b64	7407adc65328f3055fcbb4f685395b7e	Commands to recover each of the six hidden secrets encoded in base64.
run_me.bin.b64	40685f64943cc2ba5982f968e78f56aa	Python program for collecting the six hidden secrets from a server located at 10.10.9.14:8080 encoded in base64.
tools.zip.b64	c887d2d6edc894da0ff5700f29c855cc	Folder containing auxiliar tools for decrypting the six hidden secrets encoded in base64.

artifacts/your-friend-files/decoded/		
File name	**MD5**	**File contents**
commands.md	c259bafd4d274bc9f555930153a101da	Commands to decrypt each of the six hidden secrets.
run_me.py	de4eeeea10870ae7067621fcb907b392	Python program for collecting the six hidden secrets from a server located at 10.10.9.14:8080.
run_me.pyc	66e3edb97f890a672d43c6aa658f8b1b	The previous program compiled.
tools.zip	d68a2460d32d12159eb373aacaf9e711	Folder containing auxiliar tools for decrypting the six hidden secrets.

artifacts/		
File name	**MD5**	**File contents**
matty_part.dd	bb4fdeb5331c59c0dbdbbcb14b8f3fc2	Matty's Linux partition dump.
tim_part.dd	0d553ed3c675298d471822646bb928fe	Tim's Linux partition dump.
hidden_matty.dd	7e85bf0c13222e0114261540723af463	Matty's hidden partition dump.
matty-artifacts.zip	5faeefac2ff49a2bea77e81cea531856	Folder containing the artifacts found on Matty's hidden partition.
matty-emails.zip	79490ec248663e3cdff6e6ebe5db6c63	Folder containing Matty's communication through email (with Tim).
wav.zip	9f72af12f23a74c3246b9de38df68249	Folder containing five audio files found on Tim's disk.
yourfriend-email.txt	8ce73f63cc21723c2f9351be772dd9f4	Email sent to Tim from yourfriend@gmail.com address.
matty-linux-bash.dump	a851773d9b7716d66263e806385b9170	Matty's recovered bash history from bash process memory.
tim-linux-bash.dump	11e8ef28c1b87c3b2ba306a2307ce15a	Tim's recovered bash history from bash process memory.