INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2019-2020 – 1st Semester

Digital Forensics Report

Carolina Carreira, Nº 87641

Daniela Mendes, Nº 87646

Rafael Branco, Nº 87698

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

We were given four files, corresponding to Tim's hard disk image (tim.disk) and memory dump (tim.mem) and Matty's hard disk image (matty.disk) and memory dump (matty.mem).

In **matty.disk** we found a few traces of the files that contained the leaked secrets. The procedure was:

We used the *mmls* tool to display the partition layout of the volume system (partition tables).

After running the following command:

```
mmls matty.disk
```

```
     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
```

Fig. 1: output of the mmls command

We inspected each partition and found a hidden one with files using the command:

```
fls -o 6387712 matty.disk
```

This command uses the *fls* tool, which is used to list file and directory names in a disk image, and uses the offset `6387712` as seen in the output of the *mmls* command.

The files found in the hidden partition with *fls* were:

1. d/d 11: lost+found
2. r/r 12: autopsy.mp4
3. r/r 13: Dan Birlew - Naruto_ Ultimate Ninja (Prima Official Game Guide)-Prima Games (2006).pdf
4. r/r 14: decks.jpg
5. r/r 15: FOO-19.jpg

6. r/r 16: Las_Vegas_Nevada.jpg
7. r/r 17: moredecks.jpg
8. r/r 18: setup.jpeg
9. r/r 19: akamaru.bmp
10. r/r 20: masashi_kishimoto.txt
11. r/r 21: naruto_run.gif
12. r/r 22: naruto_wikipedia.txt
13. r/r 23: villains.zip
14. r/r 24: attack
15. r/r 25: naruto_opening.wav
16. r/r 26: naruto_scream.wav
17. V/V 62593: $OrphanFiles

To extract the files from the disk image we used *icat* to output the contents of each file based on its inode number. To extract the files we used the following command:

```
icat -o 6387712 matty.disk $inode > $filename
```

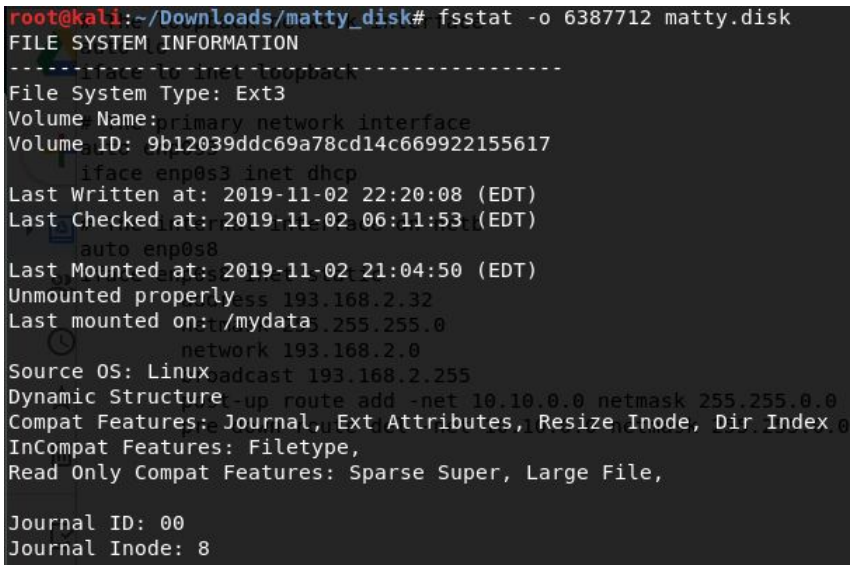
The inode corresponds to the output of the command described above (`fls -o 6387712 matty.disk`) and the filename to the name of the files.

The files 9 to 16 correspond to the files found in the pendrive. We checked all of their md5 values and concluded that they correspond to the same files. As such we can conclude that we found traces of the leaked files here (Matty's computer).

Nonetheless, we found other files (files 1 to 8) and tested them for hidden data using commands like *file*, *xxd* (with the same methods employed in the last report) but didn't find anything. So we didn't deem these files relevant.

We discovered that this partition was last mounted on /mydata and at 2019-11-02 21:04:50 (EDT) using the tool *fsstat.* This tool displays general details of the file system.

```
fsstat -o 6387712 matty.disk
```



In /root/.bash_history, we found evidence that pointed to a pen being mounted in this device. To recover this file we ran the command:

```
icat -o 2048 matty.disk 29467 > bash_history
```

There we found the command:

```
mount /dev/sdb1 usb_drive/
```

Then, inside /var/log/syslog, we also found a match for the pen drive's serial number. To recover the syslog we ran the command:

```
icat -o 2048 matty.disk 1495 > syslog
```

To discover the pen drive's serial number we ran the following command and found a match:

```
cat syslog | grep -a 052513000000046E
```

```
Nov  2 19:17:56 matty kernel: [ 4395.605936] usb 1-1: SerialNumber: 052513000000046E
```

This proves that the pen drive was used in this computer.

Afterwards we used the foremost tool to recover files from the disk image, based on specific file types.

The command used was:

```
foremost -i matty.disk -t png,bmp,zip,wav,gif
```

With the foremost tool, we discovered a .bmp file with that could be a part of the akamaru.bmp file and traces of the Naruto's wikipedia page (at the end of the .bmp) found on the pen drive (06477824.bmp). However none of these files had the corresponding hashes so we can't say they are relevant or even evidence.

In matty.disk we found emails matching the ones found in tim.disk this subject is going to be explored in section 2.

In **tim.disk** we found a few traces of the files that contained the leaked secrets. The procedure was:

We used the *mmls* tool to display the partition layout of the volume system.

```
mmls tim.disk
```

```
     Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0016777175   0016775128   Linux (0x83)
003:  -------   0016777176   0016777215   0000000040   Unallocated
```

We started by analysing the Linux partition.
With the foremost tool we discovered:

```
foremost -i tim.disk -t png,bmp,zip,wav,gif
```

- a zip file (17043872.zip) we suspected that could correspond to villains.zip: 17043872.zip had the same md5 hash as villains.zip found on the pendrive so we concluded that they were the same file.

- a png file (17046144.png) that we suspected that could correspond to the map of Area 51: 17046144.png has the same md5 hash as the map of Area 51 found inside naruto_opening.wav from the pendrive so we concluded that they were the same file.

As such we can conclude that we found traces of the leaked files in Tim's computer.

The following files, although we suspected that they could be the same files as the ones found on the pendrive, we came to the conclusion that they could not be considered traces, as their md5 values did not match:

- a wav file (17047128.wav) that we suspected that could correspond to the SOS morse code sent by the aliens;
- a wav file (17087824.wav) that we suspected that could correspond to the message in morse code about the captive aliens;
- a wav file (17055744.wav) that we suspected that could correspond to the naruto_opening.wav audio;
- a corrupted gif file (17041768.gif). We think this might be a corrupted version of the naruto_run.gif but we can't tell for sure;
- a bmp file (17039904.bmp) that we suspected that could correspond to akamaru.bmp found on the pendrive.

To obtain the md5 values mentioned above, we ran the command:

```
md5sum $filename
```

Where the filename corresponds to the name of the files.

We then decided to analyse the unallocated partition with the offset 16777176, as we thought that there could be some files hidden there:
We tried to access the partition with the *fls* tool, but that didn't work, because the tool could not determine the filesystem type.
Because of this, we opted to use the *gpart* tool, which tries to guess which partitions are on a hard disk by scanning the disk for several partition types. To restore (i.e. write) the partition table that corresponded to the mentioned unallocated partition, we ran the following command:

```
sudo gpart -W tim.disk tim.disk
```

This command allowed us to write the partition table that corresponded to the unallocated partition in tim.disk. Then, by executing the *mmls* tool, we were able to list the partition (now with the offset 16777216):

```
mmls tim.disk
```

```
      Slot    Start        End          Length       Description
000:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0016777175   0016775128   Linux (0x83)
003:  -------   0016777176   0016777215   0000000040   Unallocated
004:  000:001   0016777216   0018874367   0002097152   Linux (0x83)
```

We were then able to access the partition using the *fls* tool, but all the files listed were deleted. As such, we concluded that this partition did not have any traces of the rest of the files that contained the leaked secrets.

```
root@kali:~/Documents/storage1# fls -o 16777216 tim.disk
d/d * 11:       lost+found
r/r * 12:       commands.md
r/d * 13:       tools.zip
r/r * 14:       run_me.bin
d/d * 8193:     data
V/V 65537:      $OrphanFiles
```

We also found evidence that pointed to a pen being mounted on this device in /root/.bash_history. To recover the bash history, we ran the command:

```
icat -o 2048 tim.disk 78964 > bash_history_tim
```

Then we found the command:

```
mount /dev/sdb1 usb_drive/
```

Then, inside /var/log/syslog, we also found a match for the pen drive's serial number. To recover the syslog we ran the command:

```
icat -o 2048 tim.disk 1495 > syslog_tim
```

To discover the pen drive's serial number we ran the following command and found a match:

```
cat syslog_tim | grep -a 052513000000046E
```

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

This proves that the pendrive was used in this computer.

To analyze **tim.mem** and **matty.mem** we used the Volatility tool, this tool is a completely open collection of tools for the extraction of digital artifacts from volatile memory (RAM) samples.
To run this tool we used the Volatility profile available in: http://turbina.gsd.inesc-id.pt/csf1920/Ubuntu160406.zip (last accessed on 16/Nov/2019) that was given to us in the Lab Assignment II to help parse the memory dumps.

To see the active processes we ran the command:

```
volatility -f $memory --profile=LinuxUbuntu160406x64 linux_psaux
```

The memory corresponds to tim.mem and matty.mem respectively.
We didn't find anything that could be interesting in the context of this investigation. We also tried to run the command:

```
volatility -f $memory --profile=LinuxUbuntu160406x64 linux_bash
```

But it displayed incoerent results compared to the bash_history in the disks.
Besides this command, we tried several others like `linux_mount, linux_netstat, linux_threads.` But again found nothing that seemed relevant.

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

We ran the command:

```
icat -o 2048 tim.disk $inode > $mailname
icat -o 2048 matty.disk $inode > $mailname
```

With the inodes corresponding to the emails in matty.disk in */home/matty/Mail/Outlook* and in tim.disk in */home/tim/Mail/Gmail*.

We found mails in both Matty and Tim's disks that indicated that the people exchanging the mails were aware of some sort of secret files. These mails were between the addresses matty.roberts98@outlook.com and tim.frasik@gmail.com, which were provided to the school as Matty and Tim's primary contact points.

We can't conclude anything about the person/people responsible for leaking the secrets. The mails found in Matty and Tim's computers don't necessarily link them to their content. Someone could have hacked their email or their mails could be spoofed.

Nonetheless it is likely that the mails from these addresses originate from the suspects in question. Assuming that this is true and that the mails from Matty and Tim's addresses originate from them, we can say that the content of the mails hinted at secret information that both Matty and Tim wanted to obtain, and eventually Tim was able to get that information through a contact named "your friend". He copied it to a pen drive and gave it to Matty, who confirmed he had gotten it. We also know that the mails were read because of the folder in which they were found.

On Matty's hard drive we found a hidden partition and, there, the files found on the pendrive (as described in section 1). In the bash_history we also found that the files were copied to that partition, and then the partition was unmounted. This could suggest that the person using the computer actively tried to hide and mask these files.

Again we can't necessarily link Matty and Tim to their computers, because someone else could have had access to them, but we assume that they were the ones who used them. This assumption is also due to the logs found in /var/wtmp showing that the users authenticated themselves in the computers.

The command:

```
dd if=/dev/zero of=/dev/sda2 bs=512 count=1
```

Was found in the root/bash_history file in Tim's computer. This command not only deletes but also 'zeros' the content. This could indicate an intention to hide the evidence trail.

We found evidence in both disks that the pen drive found in Matty's room was used in them (See section 1, syslog) and, in their bash_history, we also found logs that could indicate that they copied the files to the pen drive.

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.

We synchronized the times by checking the timezone of the computers. To do this we found ran the commands:

```
icat -o 2048 tim.disk 776
icat -o 2048 matty.disk 776
```

In each disk and extracted their respective timezones (from etc/timezone).

We also know that the hidden partition in matty.disk was last mounted on /mydata and at 2019-11-03 01:04:50 (UTC) (See section 1).

In the following timeline there is a file "run_me" that contains a script and connects to the private IP 10.10.9.14. We suspect that the files were probably downloaded through this IP.

The emails from "your friend" were found to be spoofed using https://emkei.cz/. This information can be found in the headers of the mails from this sender.

An important note to keep in mind is that the following timeline results from evidence found in the disks and memories but there was some data that had to be speculated because we didn't have timestamps for it.

For the purpose of simplicity we assume that the person using the email and the computer (bash) is the owner of the computer in the timeline below.

Timeline:

Time	From	To	Message	Command
02/11/2019 at 14:16:23 UTC	matty.roberts98@outlook.com	tim.frasik@gmail.com	Sender asks receiver if he has news on the secret information (14-16-23.txt)	icat -o 2048 tim.disk 81136 > 14-16-23.txt
02/11/2019 at 14:20:06 UTC	tim.frasik@gmail.com	matty.roberts98@outlook.com	Sender answers to the previous question saying that he still doesn't have it (14-20-06.txt)	icat -o 2048 tim.disk 81135 > 14-20-06.txt
02/11/2019 at 14:21:50 UTC	matty.roberts98@outlook.com	tim.frasik@gmail.com	Sender tells the receiver that he can't wait to get the information and asks the receiver to keep him updated (14-21-50.txt)	icat -o 2048 tim.disk 78986 > 14-21-50.txt
03/11/2019 at 00:08:32 UTC	yourfriend@gmail.com	tim.frasik@gmail.com	Sender encodes four pieces of information in base64 (on sentence and three attachments) and sends it to the receiver (00-08-32.txt). The sentence in	entire email: icat -o 2048 tim.disk 2339 > 00-08-32.txt generate tools.zip:

	base64 informs the receiver of the following: *"I know you've been waiting for this message.* *I'm sending two attachments to you. Execute the file run_me.bin, follow the remaining instructions in file commands.md and use what's inside tools.zip"* We saved each attachment encoded with base64 in a .txt file: run_me: run_mebase64.txt commands: commandsbase64.txt tools: toolsbase64.txt	cat toolsbase64.txt | base64 -d > tools.zip generate run_me.bin: cat run_mebase64.txt | base64 -d > run_me.bin generate commands.md: cat commandsbase64.txt | base 64 -d > commands.md

By checking Tim's bash history (bash_history_tim), we formulated the following theory:

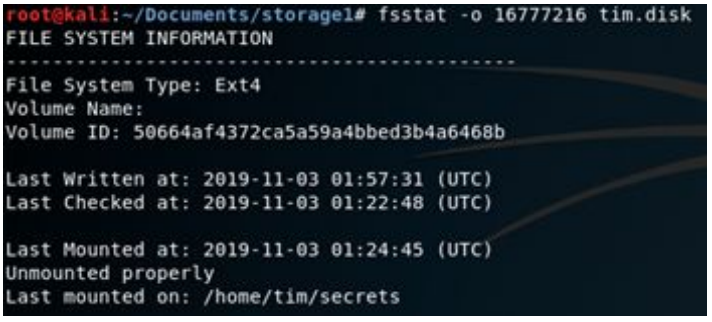
Tim starts by creating a filesystem:

```
mkfs -t ext4 /dev/sda2
```

and mounting it on the directory "secrets" in Tim's home directory:

```
mount dev/sda2 -t ext4 secrets
```

- We can corroborate this by executing the fsstat tool on the hidden partition we found in tim.disk:



Then, Tim moves commands.md, tools.zip and run_me.bin into "secrets" and executes run_me.bin. We believe that, by executing run_me.bin, a folder named "data" was created (inside "secrets") and this folder contains the artefacts/evidences over which Tim has to execute the commands in commands.d with what is inside tools.zip. Because of this, he moves tools.zip into "data" and unzips it. After that, he executes the commands (like "your friend" instructed), directing the output to the "out" folder he creates.

He then lists all usb devices (command *lsusb*) and creates a mount point, inside the "data" folder:

```
mkdir usb_device
```

And mounts the pendrive into the mount point:

```
mount /dev/sdb1 usb_device/
```

- We know that the pendrive (with Serial number 052513000000046E) was mounted in 03/11/2019 at 01:38:56 UTC from syslog (mentioned in section 1) and then the files in secrets were copied to the pendrive in Tim's computer.

Afterwards, he moves all the evidence into the "usb_device" folder (i.e. into /dev/sdb1).

Time	From	To	Message	Command
03/11/2019 at 01:45:10 UTC	tim.frasik@gmail.com	matty.roberts98@outlook.com	Sender informs the receiver that he has the secret information and asks him to store it. (01-45-10.txt)	icat -o 2048 tim.disk 2268 > 01-45-10.txt
03/11/2019 at 01:50:55 UTC	matty.roberts98@outlook.com	tim.frasik@gmail.com	Sender agrees to meet the receiver to obtain the drive. (01-50-55.txt)	icat -o 2048 tim.disk 2828 > 01-50-55.txt

After these mails, we think Tim unmounted the pen drive and the secrets directory and deleted everything inside "secrets".

We already showed that dev/sda2 was mounted into secrets and that that partition only had deleted files in them (see section 1), which were the files in secrets. By running

```
istat -0 16777216 tim.disk $inode
```

on the corresponding inodes, we concluded that these files were deleted between 01:53:24 (UTC) and 01:57:31 (UTC).

Tim then uses the "dd" command to delete and "zero" the /dev/sda2.

Then we know from syslog (in section 1) that Matty mounted the pendrive at 2019-11-03 at 02:17:56 UTC. Afterwards, the files are copied from the pendrive to /mydata (the hidden partition in matty.disk, that at this point wasn't "hidden" yet). After this, we know that /mydata was unmounted.

Time	From	To	Message	Command
03/11/2019 at 02:21:28 UTC	matty.roberts98@outlook.com	tim.frasik@gmail.com	Sender tells receiver that no one will find the files. Sender signs the mail with "They Can't Stop All of Us" (02-21-28.txt)	icat -o 2048 tim.disk 2626 > 02-21-28.txt

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

The identity of the person(s) responsible for leaking the secrets is unknown.

We can't conclude anything about the person(s) responsible for leaking the secrets. The email's found the Matty and Tim's computers don't necessarily link them to their content. Someone could have hacked their email or their mails could be spoofed.

Due to the fact that the mails found were their primary contact points from the university we assume that they were theirs.

What we know for sure is that the mails were read and were in the computer. The next step a forensic investigator could make is to try to legally gain access to the servers of the offlineimap to try and find useful logs. Another step that could be taken is to investigate the site https://emkei.cz/, because they may have saved logs that could help the investigation.

Our team found traces of the files that contain the leaked secrets in Matty's and Tim's hard drive. So the person(s) that used the computer was probably responsible for leaking the secrets.

We have to have in mind that although the computers belonged to the subjects we can't necessarily conclude that the evidence found was 'made' by them. This evidence could be planted there. However, because we also found the pen drive in their bedroom it likely that the evidence originated in them.

Another conclusion we can make is that someone tried to hide the files. We know that because the command "dd" not only deletes, but also "zeros" the content and that the hidden partition was unmounted, which could maybe mean someone tried to hide it.

The identity of the person responsible for leaking the secrets from Area 51 is unknown; we suspect that "your friend" was the one to do it, but we have no concrete evidence.

5 Annexed files

The files annexed to this report are the following:

Evidence Artifacts:

The MD5 value for the following artifact are in Auxiliary\ Items/tim_md5_hashes.txt

- Tim Artifacts
  - 17039904.bmp
  - 17041768.gif
  - 17043872.zip
  - 17046144.png
  - 17047128.wav
  - 17055744.wav
  - 17087824.wav
  - 14-16-23.txt
  - 14-20-06.txt
  - 14-21-50.txt
  - 00-08-32.txt
  - 01-45-10.txt

    - 01-50-55.txt
    - 02-21-28.txt
    - bash_history_tim
    - syslog_tim
    - commandsbase64.txt
    - toolsbase64.txt
    - run_mebase64.txt
    - commands.md
    - tools.zip
    - run_me.bin
    - var.log.wtmp

The MD5 value for the following artifacts are in Auxiliary\ Items/matty_md5_hashes.txt

- Matty Artifacts
    - akamaru.bmp
    - attack
    - masashi_kishimoto.txt
    - naruto_opening.wav
    - naruto_run.gif
    - naruto_scream.wav
    - naruto_wikipedia.txt
    - villains.zip
    - 06477824.bmp
    - bash_history
    - bash_history_root
    - deletedmail1
    - deletedmail2
    - deletedmail3
    - mail1
    - mail2
    - mail3
    - sent1
    - sent2
    - sent3
    - sent4
    - syslog
    - time_zone
    - var.log.wtmp