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)**

1 Objectives of the investigation

A 21-year-old college student, Matty Roberts, created an American Facebook event to raid Area 51 in a search for extraterrestrial life. It is still unknown whether he may have had access to classified information, and if so, how it leaked from Area 51. The investigation consists of searching for evidence about any leaked information and its source. The following sections present the analysis of files found on a pen drive in the suspect's dorm room.

2 Artifacts for analysis

The artifacts handed over appear to include two WAV files (*naruto_scream.wav* and *naruto_opening.wav*), one data file (attack), a ZIP compressed file (*villains.zip*), one BMP file (*akamaru.bmp*), two text files (*masashi_kishimoto.txt* and *naruto_wikipedia.txt*) and a GIF file (*naruto_run.gif*). We first verified the integrity of the artifacts by checking the MD5 fingerprint provided in the lab.

File	MD5 Value
masashi_kishimoto.txt	990eea6aae1cda8dba7f9e2b291b8163
naruto_run.gif	d28309dde3a82dddd524eb28d0ccd641
naruto_wikipedia.txt	d441c7d49cab2adf84d2c95302a04d36
villains.zip	12e20730ccdadfcfe72908be84ea27f1
akamaru.bmp	2954d9fc50198672430f053a455be783
attack	0fae36d3e066288d255df5a00fed1d13
naruto_scream.wav	3a50e65840707bd28f26219d6b7c9401
naruto_opening.wav	ddb4e1171739dfd0f1d8bdc5f2f705d4

3 Evidence to look for

Considering the objectives of the investigation and the artifacts we were handled, we are hoping to find evidence related to Matty and/or Area 51 (maybe confidential information that was leaked). We are also hoping to find relations with the other suspects: Joe Bartels, Justin Roberts and Tim Frasik.

We will start by exploring each file with the command *file* since it is a straightforward way to verify if the files are what they claim to be.

At first sight, we can see the files correspond to the given extension and the data file *attack* is in fact a byte-compiled Python program - which is something we will surely use to look for evidence. Reading the first text file, we can see it's Naruto's *Wikipedia* page, which, as of this moment, seems a perfectly normal and evidenceless text file. The other one is presumably encoded in *base64* (due to the usual ending '==' padding characters that appear at the end of the text).

We also have a password-protected zip file that we will try to crack either by using information from the other files or through brute force, using the proper tools for it.

As for the WAV, GIF and BMP files, if we open them, they look like regular files… We will surely look for hidden files or messages that might be covered with steganography techniques.

4 Examination details

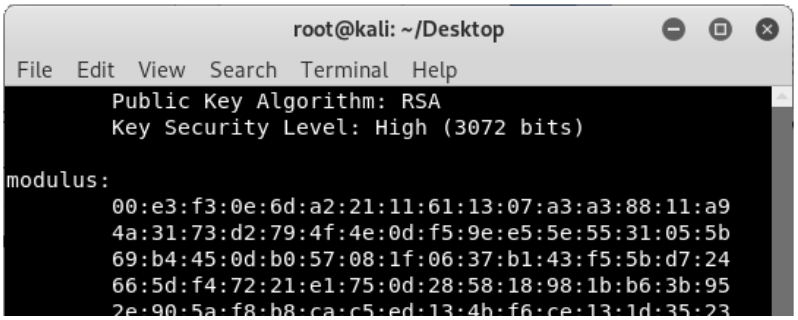
Before starting, we booted a trusted OS on a virtual machine (in this case, Kali Linux on *forensics mode*) so we wouldn't be running any malicious software on our own machines, and possibly compromise them and the artifacts.

As we mentioned in point 3, we suspected the masashi_kishimoto text file was encoded in *base64*. So, we successfully run the command *base64 -d masashi_kishimoto.txt* and we found the first secret.

```
root@kali:~/Desktop# base64 -d masashi_kishimoto.txt
Hello,

I'm sending you six pieces of evidence for that thing we talked about down in Nevada, including
credentials for acessing our server where there's more info.
Check them out and tell me what you think.

Mogul sure doesn't want this information to be exposed to the public, but I trust you'll do the
right thing.

-- They Can't Stop All of Us
```

Evidence #1

We then focused our attention on the *akamaru.bmp* file. By using the command *cat* on this file, we found someone had appended an *RSA Key* with a high level of security (key size of 3072 *bits*) at the end of the file.



Evidence #2

We then investigated the byte-compiled Python file. We figured it could be of use to have the original source code for the program in order to understand how or why it might have been used. We stumbled upon *uncompyle6*, a tool that receives a .pyc file and decompiles it to a *python* file, returning the original code. We successfully got the code (***attack.py***). We thoroughly analyzed it and understood how the program used audio steganography to encrypt files and conceal them inside a WAV file (a format present several times in our set of artifacts). This led us to believe that the ***attack.py*** program might have been used to conceal information into those files.

We reversed this program and we were able to extract a WAV file from the *naruto_scream.wav*. We heard it and our first thought was that we were dealing with a *morse code* message. We then searched for online *morse code* decoders that accepted audio input and obtained the following message:

> *SEND HELP. VISITING PLANET EARTH. CRASHED AT ROSWELL. CAPTURED AND TORTURED FOR OUR HIGH INTENSITY BLASTERS AND CONCENTRATED DARK MATTER CANNONS. DESPERATE FOR HELP. CHECK LOCATION IN MAP.*

Evidence #3

Then, we thought we could try to use our reverse function once again, so we used it on *naruto_opening.wav*. At first, it was not working - it was extracting corrupted illegible files. We were intrigued by this and tried to see what could be going on with this file. We were firmly convinced the least significant bits were hiding some, due to the background noise. Therefore, we changed the LSB number of bits on our python script to 1 and we were successfully able to extract the following image:

Evidence #4

Exploring the *villains.zip* file with the archive manager, we were able to see the list of files inside (*kaguya_otsutsuki.png*, *madara_uchiha.png* and *momoshiki_otsusuki*). As soon as we speculated that the password would be hidden somewhere in the other artifacts, we turned our attention to the apparently harmless *naruto_wikipedia.txt* text file. The tool fcrackzip's has a dictionary mode that uses a sorted file with a password per line and outputs the correct password, if it's present in the file. So, we processed the text file with a python script and provided that list of words to the tool as a dictionary for cracking the zip file's password. In less than a minute, we were able to recover the password - "Troublemaker".

After analyzing the files present in the villains folder, we suspected both images were decoys and the only interesting file was *momoshiki_otsusuki*. We actually searched on the web for similar files and didn't notice anything different in those files (using the *diff* command), so it means that these two files are irrelevant for this investigation (in the sense they don't hide any information in them). Then we used the *file* command on *momoshiki_otsusuki* and it said that it was a regular *data* file. Then, we used the *strings* command on this file, and we noticed something curious. The file had strings like "PLAME3.100" and "*LAME3.100". This suggested that this was a mp3 file. We listened to the audio with *vlc* and it was Donald Trump's voice saying:

> *"We can never let this happen. We're fighting to drain the swamp, and that's exactly what I'm doing. And you see why he have to do it. Because our country is at stake like never before."*

Evidence #5

Then we explored the *naruto_run.gif* file. By using *hexdump* on it, it was clear that this file was more than just a *gif*. We noticed the PK magic number that indicated we we're dealing with a *zip* file. By using *exiftool*, we saw that this file was on the metadata of the original *gif* so we extracted that *metadata* by running the command *exiftool naruto_run.gif -s -s -s -Comment -b -w zip*. We unzipped this file and were left with a WAV file *(a1.wav*). After hearing it, we suspected we were dealing with *morse code* once again and obtained the following message:

SOS SOS ROSWELL

Evidence #6

The files/evidences we gathered along with their MD5 fingerprint:

File	MD5 Value
(#1) masashi_kishimoto_decoded.txt	38558d9a74aa0cd516e5b1e3632984d0
(#2) rsa.txt	cd3000acd736503b927f678efe39d1c9
(#3) morse.wav	273c18fb603084928dbad3ae19f8d5e8
(#4) map.png	5e92a1fe4f675f7960f5d4f316f63356
(#5) momoshiki_otsusuki	273c18fb603084928dbad3ae19f8d5e8
(#6) a1.wav	1df1d41ca05096189bcd100acb35b1eb

5 Analysis results

After collecting our first piece of evidence (**evidence 1**) we got some relevant clues relative to the Area 51 raid. It seems someone is sharing confidential information about evidences of existing extraterrestrial life inside Area 51. First we noticed that there had already been a meeting between at least two entities (one of them being presumably Matty) in Nevada. This message also says that this evidence includes credentials for accessing a server with more info. We did not find any URL or IP to access this server, but maybe we found the credentials: the *RSA key* we found (**evidence 2**). Although this clue is not conclusive, we suggest that future investigations should take this into account. Finally, we found two plausible explanations for the last sentence "Mogul sure doesn't want this information to be exposed to the public, but I trust you'll do the right thing":

1) Mogul is the Secret Service codename for USA President Trump.

2) Project Mogul was a US military listening project using high altitude balloons. In the summer of 1947, one of those balloons crashed in the desert near Roswell (New Mexico) and conspiracy theories from *UFO* enthusiasts led to a celebrated *UFO* incident.

There is evidence to support both these explanations:

We have that audio file on **evidence 5** of Trump speaking, and this was inside a directory named "villians", which suggests that they are indeed saying that President Trump wouldn't like this information to be leaked.

On the other hand, the messages on **evidence 3** and **evidence 6** seem like a *morse* encoded message of aliens that crashed in Roswell and that were captured and are now being held in a determined location that we should "check in a map". On **evidence 4** we get an image that points to a facility in Area 51 saying "We are here", which is probably the map that was referenced on **evidence 3**.

6 Conclusions

The evidence obtained and analysed, by itself, cannot prove Matty's guilt or innocence. Even though these files were discovered on a pen drive found in Matty's dorm room, what is suspicious, someone might be trying to frame him. It also seems that the person behind these artifacts had access to confidential information, but the evidences gathered are not enough to prove it. We also didn't find any evidence related to the involvement of Joe Bartels, Justin Roberts or Tim Frasik.

Lastly, we wanted to reference the *morse code* decoder we used twice in the investigation:

https://morsecode.scphillips.com/labs/decoder/

This report was finished on the 25th of October 2019 and was written by Afonso Oliveira, João Tavares and Miguel Grilo.