INSTITUTO SUPERIOR TÉCNICO
Departamento de Engenharia Informática
Forensics Cyber Security
MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab2

Group number:	2	Name	IST Number
Student 1:		Simão Sanguinho	102082
Student 2:		Francisco Gouveia	102571
Student 3:		José Pereira	103252

1 Acquired artifacts

Name	Type	SHA-256 Value
bash_history	ASCII text	9a656b05678b07ac0f4aa7a0fd167ea528bd395893290e09244fbe0888103a44
andromeda.png	PNG	fcdd6ce7ae9a8f02c2ba3b2693d49848606b1ca5d332a076fe63013fcaa55ab2
best-intro.wav	RIFF	c3ea6b775dd7eaecebeef00e5523483d182602118ff6de0eb3d6a41b8f43c42f
cartwheel.tiff	TIFF	f6861a315acb49b9c8ac18e9d6e92ed366e78f43bd2850d0f2a8f30f695aad45
lactea.png	PNG	326f3601ab7ad66fff2c43b3c5d4465d820dbf7381be65ab20c6adac2d1c10bb
myzip.zip	ZIP	255a40424332be5b70c01c6301e05de6049b54ef2c7d2fb8551f0358866f5649
nmap	ELF	33da582bf8705b3a6818fa25d1f61ee339d46f58b8aedfdd951e1d4a915d582d
tagus.png	PNG	0b916d4d246372e07b1a6901585b632d8426a07b611fa4b1058341ef2a59f7b2
authlog.txt	TEXT	fde27cc876c3f28a0803827c337a6c32c61aa2de02cb6456ed3ecb1c26c8d6ed
syslog.txt	TEXT	21bd644a2359c064bbaae327e178930a9e83771916ab8f22cdf94ba4d4551baa
cronjob.txt	TEXT	5ecfbf9a5a2785414a461b91cf908ea24850664999d6fdd8cb716a79428ae5bd
KFP7oy1K7O5.log	UNICODE TEXT	939b7ac1963a073f727683fd7a2ae66cf0b84b00f6157c628d324328b02c53e1
K5rb9cnL0Is.log	UNICODE TEXT	1fa61fc25578cd81146c31116327f4c7defa5282815265b8cbb5c2662b165aae

2 Analysis of relevant findings

2.1 Did you find any traces of the hidden artifacts and/or the files originally discovered in João Musk's sigma account on his computers?

Looking at the Documents, Pictures and Music, we can find files used to hide the secrets and searching through the logs of the desktop (more specifically, going through /var/log/syslog.1), we can see the kernel logs of the USB pen drive with serial number 9AD32EC0 being connected to João Musk's desktop.

However these files found on Musk's primary disk did not completely match the ones from the first investigation, as they did not have any hidden messages. Nevertheless, on his backup disk there were some password protected zips that continued the same files, but now these files had the same SHA256 hashes from the ones included on the first investigation, from his sigma account. By looking through his bash_history we can verify that he sent these files from the machine to his sigma account via secure copy.

2.2 If so, can you trace the origin of these files and how they were processed over time? Construct a timeline of relevant events.

We've started our investigation by looking at João's primary disk. By running the command `mmls johnnyDisk.img` we can immediately see that there is a partition containing a *Linux* filesystem. For this purpose, we could also have used the command `fdisk -l johnnyDisk.img` which would also give us the information that there were two partitions (*"Bios Boot"* and *"Linux Filesystem"*). Knowing that the offset was 4096, we could now start looking into his files. Firstly we used the `fls` utility (in *The Sleuth kit*) passing the offset as parameter (`fls -o 4096 johnnyDisk.img`), but then we've reached the conclusion that, since we didn't find anything in the deleted files (with the command `fls -o 4069 johnnyDisk.img -Frd`), we could just mount the filesystem into a regular directory and navigate through it in the usual way. To do that we've ran two commands: `losetup -fP johnnyDisk.img` and `mount /dev/loop0p2 disk/`.

From this point on, we started to dig into his home directory, `/home/johnnymusk`. The first thing we found was the history of commands (`.bash_history` file), with a lot of commands used to hide files (artifacts from previous investigation) using mostly tools from the `home/johnny/stt` directory, showing that he really was the one that was responsible for developing the artifacts that were found in his sigma cluster. In this same file we also found that he launched a program named `irssi`, a client for *IRC* chats. With this in mind, we've turned our attention to find the logs regarding his conversations. To do that, we searched through the disk for files related to this *IRC* client with the command `fls -o 4096 johnnyDisk.img -Fr | grep -i "irssi"`, finding that under `home/johnnymusk/snap/irssi/common/irclogs/2024/freenode/` there were logs of his conversation. After exploring each one of them we found a log (`#thebasement.09-26.log` file), recovered with the command `icat -o 4096 johnnyDisk.img 574131` that contained critical information regarding a conversation between him and a username "*RootKitty*". After thoroughly reviewing this conversation we found out that it wasn't João who stole the IST credentials but instead "*RootKitty*". Moreover, in this conversation, João also told "*RootKitty"* about an anonymous email that he received regarding a USB pen and the contents that were in there. It's important to note that the description of the contents matched the files that he tried to hide in his sigma cluster, which were already found.

After checking his *IRC* chat, we continued to search through his `/home/johnnymusk/snap` folder and found that we had firefox and thunderbird installed on his machine, so our next step was to check if there was sensitive information in these files. To search for it, we ran the command `fls -o 4096 johnnyDisk.img -Fr | grep -i "thunderbird"`, and found that in the inode 530585 there was a sensitive email. Even though it didn't come in plain text, it didn't take long to use the command `base64 -d` to decode it and see the contents. This was the email that João was telling "*RootKitty"* about, the anonymous email to grab a pen drive in a locker near IST. Regarding *firefox* we did the same command aforementioned but with the change that now we want to look for files with "firefox"

instead of "thunderbird" and found his history was in a file named `home/johnnymusk/snap/firefox/common/.mozilla/firefox/t7pu9ru3.default/places.sqlite`. Since this was a SQLite database we used a SQLite viewer and discovered that he has visited many sites. What came to us as strange is that he searched for a repository of hacking tools, how to remove a file, the restaurants that were talked about in the Oeiras report, ISTSat-1 related information, a *WeTransfer* link given to him by "*RootKitty*" and a login into fénix.

It should be noted that we found other files (e.g. memes), but since they weren't relevant for this investigation we keep them out of this report. On another note, we've found on his documents folder (`/home/johnnymusk/Documents`) that he had a `User_Manual.pdf` file regarding a master thesis on the telemetry of the Ariane 6 which is consonant to the fear that he expressed in the conversation with "*RootKitty*".

After inspecting the logs in the primary disk (under 'var/log/syslog') we found a cron job was running with the purpose of doing backups. By opening the crontab file (under 'var/spool/cron/crontabs/johnnymusk')., we verified that there was a a script (/home/johnnymusk/backups/backup.sh) that was running every 10 minutes.

The above mention script creates a password protected zip file with all the contents on the home directory, where the password is generated by another script (/home/johnnymusk/backups/pass_gen.sh), and then sends the zips to the backup machine using the command `rsync`. The password is generated by creating an hash value from the timestamp passed as argument and the content of the file located at `/tmp/seed.txt`

In the Musk's backup disk's home directory 7 zips were found, all password protected (as expected). We knew that the passwords were generated by the `pass_gen.sh` file and upon inspecting this file we found out that it simply runs another file, this being `/home/johnnymusk/backups/obfuscator`. We then used uncompyle6 to decompile the obfuscator and see the code that generated such executable (obfuscator_reversed.py), which revealed that a password was meant to be used on the first run, by putting it into a file (`/tmp/seed.txt`). As we hadn't had any particular clue about this password, we turned into the `Passwords.kdbx` that we found in João's directory. This file corresponded to a *KeePass* special folder, and since "grepping" for the words "password" or "keepass" didn't allow us to advance, we decided to look in the `/tmp` folder, where we already found the seed. In this folder there were also two logs, related to key presses. In the file `/tmp/K5rb9cnL0Is.log` there was the following information:

"[ctrl][v][k][e][e][p][a][s][s][x][c][enter][i][l][o][v][e][m][y][d][a][d][t][h][e][g][o][a][t][enter]"

which tells us that the password for the keepass file that we had found earlier was "*ilovemydadthegoat*". With this we could open the *KeePass* folder and discover that the password that was meant to be used was "TheBiteOf87".

After taking a look at the `/tmp/seed.txt` file we can see that the script had already been run 78 times, as its content was ' 78 acacb6e8cdf5613a75320bbe4b00f88c9fbd706590984c122d59b73fe1a00f1d'. Since there were 7 zips we assumed that the passwords for the zips were generated on the iterations 72-78.Thus, we took the code from obfuscator_reversed.py and expanded it so that when it generates a password in an iteration it tries to open the zip file given as an argument. Then we created another script (`crack_script.sh`), that runs the first 71 times, and then tries to open the zips with the generated passwords on the iterations, which worked. To confirm that we were able to do everything correctly, we checked and after the final iteration the output of the `seed.txt` was the same as the file `tmp/seed.txt` we found on João's machine.

Finally, we looked at the logs and found that the pendrive, with serial number "9AD32EC0" found by João Musk has been connected to João Musk's desktop and the files generated by the steg tools have been copied to there.

Timeline:

Sep 26 16:30 - IRC log of RootKitty telling João Musk that he exploited Fenix and stole pairs of usernames and passwords

Sep 26 16:35 - IRC log of RootKitty sharing the credentials with João Musk through an url.

Sep 26 16:36 - Thunderbird email log of johnnymuskhax@gmail.com receiving an email from somebodysupercool@protonmail.com telling him about MKUltra and where to find the USB.

Sep 26 16:37 -Download of hackedcredentials.txt.

Sep 26 16:51:44 - Connected the USB pen drive with the serial number "9AD32EC0" to the desktop.

Sep 26 16:54 to 17:00 - Various google searched related to the data inside the USB

Sep 26 17:01 - IRC log of johnnymusk telling RootKitty about the email telling him to retrieve the USB

Sep 26 17:03 - IRC log of johnnymusk telling RootKitty about MKUltra and Ariane 6.

Sep 26 17:07 - IRC log of johnnymusk saying he wants to organize a protest and push for the satellite to be deactivated. João Musk and RootKitty decide to create a poster for this cause.

Sep 26 17:09 - IRC log of johnnymusk saying he's going to hide the sensitive details in some files using tactics learnt from CTFs, and then he is going to save them in his private account on the SIgma cluster.

Sep 26 17:20 - Download of the EliteHackingTools.

Sep 26 17:26:10 - Usage of ".venv/bin/python lsb.pyc -m hide -d horizontal -c rgb -n 3 -o /home/johnnymusk/Picutres/wallpaper.png -p /home/johnnymusk/Documents/Ariane6/Report.pdf -e pdf" to hide the report inside the wallpaper image. This execution also launched a keylogger that registers the pressed keys in /tmp/ K5rb9cnL0Is.log

Sep 26 17:26:52 - Usage of ".venv/bin/python lsb.pyc -m hide -d diagonaldown -c rgb -n 5 -o /home/johnnymusk/Picutres/tagus.png -p /home/johnnymusk/Documents/Ariane6/blueprint.png -e png" to hide the blueprint inside the tagus image.

Sep 26 17:30:01 - Backup of João Musk home directory with the files containing the hidden informations was performed

Sep 26 17:31 - Google searches about how to secure delete files and directories in linux

Sep 26 17:32:22 - Usage of "/usr/bin/apt-get install secure-delete" to remove files safely without the possibility to restore them.

2.3 Did you uncover any evidence of anti-forensic activities?

After examining João Musk's browser history, we discovered that he had been researching methods for securely and permanently deleting files in Linux. His searches included terms like "Ways to Permanently and Securely Delete Files and Directories in Linux" and "how to secure delete in linux." This suggests he was looking for ways to ensure that deleted data could not be recovered. Further investigation revealed that João Musk downloaded steganography tools from a GitHub repository (https://github.com/PirateMajima/EliteHackingTools), which he later renamed and stored in the directory /home/johnnymusk/stt.

By reviewing the .bash_history file on João Musk's desktop, we confirmed that he actively used these steganography tools to conceal sensitive information that we had previously uncovered. In addition, João Musk used the srm command, which, unlike the standard rm command, securely removes files by overwriting the data, making recovery impossible. This activity is also documented in his .bash_history file, showing his deliberate attempt to eliminate traces of his actions.

Besides this, the obfuscator file used to generate the password for the backups has its implementation hidden, indicating further attempts to obscure the process and protect his activities from scrutiny. These actions, taken together, strongly point to João Musk's involvement in both the use of steganography to hide critical data and his efforts to prevent any recovery of deleted files.

2.4 What new discoveries can you report that might clarify the plot or identify other relevant actors?

Our findings suggest a new hypothesis: João Musk was involved in attempting to hack the Fenix system and intending to use the stolen credentials of the IST users. Although he didn't steal the credentials himself, he knew who did and had access to them. João Musk was also the one who discovered the MKUltra mind control component, which was being misused. This discovery came through the USB João Musk found in a locker at the IST Alameda Campus, after receiving an email from 'somebodysupercool@protonmail.com' informing him of this. After finding this out, he later informed his friend RootKitty over IRC about the MKUltra exploitation. João Musk and RootKitty then conspired to stop the misuse, which led to the creation of the poster. They also discussed how MKUltra was being used to boost Oeiras Restaurants' business. Then, João Musk hid the secrets using steganography tools, as described in section 2.2.