INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab2

Group number:	**7**	**Name**	**IST Number**
Student 1:		Tiago Rosalino de Sousa Lopes Quinteiro	99336
Student 2:		Rafael José Porfírio Chuva	103164
Student 3:		Tiago António Esteves Firmino	103590

1 Acquired artifacts

Name	Type	SHA-256 Value
johnnymusk	SHA-256	5ecfbf9a5a2785414a461b91cf908ea24850664999d6fdd8cb716a79428ae5bd
backup.sh	SHA-256	98a727647725157f57a18ad3a43396c0ca9016d5fabb76fa86eab8d1661abba6
pass_gen.sh	SHA-256	83363303d40cbcef23466bb540d7a5bbe0f574d87db3655e01525a01dd4f2503
obfuscator	SHA-256	86a89e4c96282492bbabb364b5a601a9e187d8f9365c3c1c900c79c7db244560
seed.txt	SHA-256	0c4a848fe5e6225ad5b41f67af0d77040e2fad2bc713b7b4938569f9255e135e
Passwords.kdbx	SHA-256	40b6c756d4d1b4fb85cdc4c11c6e0b8f4ca5eb1019c05f51c356a4d669c7c38a
K5rb9cnL0Is.log	SHA-256	1fa61fc25578cd81146c31116327f4c7defa5282815265b8cbb5c2662b165aae
KFP7oy1K7O5.log	SHA-256	939b7ac1963a073f727683fd7a2ae66cf0b84b00f6157c628d324328b02c53e1
places.sqlite	SHA-256	d2713088801187b1bdbd115eb93eafb757640b4e72b3ee10aaca59f369c6e52e
.bash_history	SHA-256	9a656b05678b07ac0f4aa7a0fd167ea528bd395893290e09244fbe0888103a44
User_Manual.pdf	SHA-256	c8a2641e23014cb7fafc83f14e4e448500b141cb74fe09634f3db2f8b4ec6d20
global-messages-db.sqlite	SHA-256	ddbf65fbe6549326194c74a83bddeac7f0706b694a18a71a8ab03e69884573d0
#thebasement.09-26.log	SHA-256	b19ce5156507851d206f7559ed67cb308d2b8b774f096296fcfee754cb98df82
kern.log	SHA-256	e5de9e937bef1814ff988eba4c191a1768e8bb123f6f671a66cd4457e2eb7429

2 Report of all findings

johnnymusk, backup.sh, pass_gen.sh

By searching johnnyDisk with the **mmls** and **fls** commands (we immediately used fls with the -r flag and copied all of the files' names and inodes to a txt file, to facilitate parsing through them -> **fls -o 4096 johnnyDisk -r**) , the first interesting thing we found was a series of cron files, which we later found out to be a Linux scheduling service. By further investigating, we saw that in a file called **johnnymusk**, a crontab where there was a script scheduled to run every 10 minutes called backup.sh in folder backups. After finding that file, we found that student João Musk had been compressing some password protected backups (generated through a bash script called **pass_gen.sh),** called backup_{TS}, with TS being the timestamp and sending them to his file system in the sigma service. In turn, that script was calling another script called **obfuscator,** passing the timestamp as a variable.

obfuscator, seed.txt, Passwords.kdbx, K5rb9cnL0Is.log, KFP7oy1K7O5.log

After extracting the **obfuscator** file with the **icat** command, we found that it was a compiled python script and used the **uncompyle6** command to revert it back to a python script. It is in this script that the password for the zips is generated (by hashing a seed concatenated to a timestamp) and the next seed that will be used for the next password is generated and stored in the file **seed.txt,** along with its iteration number. By the time we got to the seed, it was already in its 78th iteration. meaning that we had no chance to reverse engineer the hash and find out what other seeds were used for the passwords, which we needed to crack the backup zips present in the backup image. We needed the first seed to generate all 78 seeds and try to crack the zips with each of them.

This led us to dig around more and more and find an interesting file called **Passwords.kdbx**, which we found out was a password manager where Mr. Musk saved his passwords. However, we had another setback - we opened this file with the **KeePass** program and it was also password protected. Like before, this lead us to to a deeper exploration of the johnnyDisk image and, in the tmp folder, we found two **.log** files (**K5rb9cnL0Is.log, KFP7oy1K7O5.log**) that captured keyboard input. Comparing both logs, we found a sentence that repeated itself (**ilovemydadthegoat**) and found it to be the master password for the password manager. This way, we had access to the initial backups password and some others that didn't interest us (netflix, etc). To prove that this password was the initial seed, we ran the py script obfuscator.py 78 times and found that it generated the exact same 78th seed as the one found in the disk image. This way, we saved those 78 seeds to a text file (**all_seeds.txt**) and implemented a script (**unzip_script**) that, for each of the backup files, combined those seeds with the respective backup timestamp in a single string, encrypted it with a sha256 hash (just as it was done in obfuscator.py), and attempted to crack each backup zip file with them (using the py library **zipfile**). All of these attempts were successful!

findings in the backup zip files

In the first five backup zip files (**backup_1727365201, backup_1727365801, backup_1727366402, backup_1727367001, backup_1727367601**) we found basically the same thing: in some of them only the previously mentioned **nmap** file and in another the nmap file plus a file named **ist90834@10.0.2** that, as far as we could gather, has the exact same content (both contain the fenix credentials).

In the sixth backup file (**backup_1727368201**), we have the exact same files that were retrieved from Sigma in the first stage of the investigation.

In the seventh backup file (**backup_1727368801**), we made a stranger discovery: a video that appears to be some sort of tiktok titled "**This Is MF DOOM**" and containing gameplay from a videogame.

places.sqlite

Another set of files we thought Mr. Musk could have left behind in his personal computer was browser information, which could be very damning. For this purpose, we conducted some online search on what names these files could have and found that firefox browser history was in a file called **places.sqlite**. In our text file that contained all file names, we searched for it and, voilá, found a file with that exact name. Then, we extracted and opened this file on a database manager and found two tables containing the browser history and the browser downloads, which we exported to JSON files called **browser_history.json** and **browser_downloads.json.** We will explore the content of these files in more detail further ahead, but it is safe to say they contained a large amount of evidence, ranging from hacking tools to mind control propaganda to searches about restaurants in Oeiras, all themes connected to our investigation.

.bash_history

We also thought that it would be interesting to have access to Musk's bash history, which was stored in a file called **.bash_history** that he also left behind in his home computer. We searched for it and quickly found its inode, extracted it using **icat** and analyzed the file. It also contained a great deal of information about hacking scripts, the documents we found in the sigma filesystem, about the Ariane6 satellite launch and design, etc. Again, we will go into further detail about these commands in the next section of the report.

User_Manual.pdf

While browsing the bash history of the johnnyDisk image, we noticed that a large amount of commands involved the Documents folder of Musk's home folder. Because of this, we investigated this folder carefully and discovered a lot of files we had already seen in the first stage of this investigation. However, we also found an interesting pdf called **User_Manual.pdf**. This file seems to be a user manual for the software present in the Ariane 6 satellite, made as a master's dissertation by student David Silva, a matter obviously of great relevance for João Musk.

global-messages-db.sqlite

Similarly to how we thought there might be some browser history left behind in the johnnyMusk disk image, we had the same thought process towards potential information that still might be present there regarding emails. After searching in our text file containing all files for some time, we found a mozilla thunderbird folder containing a file called **global-messages-db.sqlite**, which we immediately thought might contain some sort of record of emails sent or received. It ended up only having 2 received emails, one of lesser importance from google and another one from an account called **somebodysupercool**, this one very interesting, talking about a mind control program called MKUltra tied to the IST Satellite Ariane6, targeting the Oeiras population. This was probably the email that tipped off Musk about what was supposedly going on and led him down the conspiracy theorist black hole. This suspicious user then went on to say that he has proof of his accusations, in a USB drive present in a Locky near IST. He urges Musk to go there and pick up the USB and learn more about this matter.

#thebasement.09-26.log

Given that Mr. Musk was leaving everything behind, we also thought that we could obtain information about his online conversations, namely internet relay chats or instant messaging platforms. By searching for the most well-known platforms of this kind of service, we found a folder called **irssi**, a popular terminal-based internet relay chat. Inside this folder, we have a very interesting log called **thebasement.09-26.log**, in which a user named **RootKitty** maintains two conversations with João Musk, the first of which he says that he was able obtain a series of IST fenix credentials using techniques learnt on the STT nucleus. In the second chat, Musk tells RootKitty about the USB pen drive he obtained from the anonymous email and about the files that are included, namely the api of MKUltra, the blueprint of the ariane6 rocket, a bank statement from Virgolino Gonçalves, the logs indicating that this tech is being used to send people to Oeiras restaurants and a DECO report confirming that these restaurants' revenues have increased.

kern.log

Since we knew that Musk had inserted the USB drive found on Locky in his computer, we searched deeper to try and figure out when said drive was used. After looking for a while on the johnnyDisk image, we came across a file called **kern.log**, which we discovered that it was the file that the kernel records when, among other things, a USB device is inserted into the computer. By looking at the kernel logs in the file, we found the date and log of which the insertion happened ("2024-09-26T16:51:44.495782+01:00 mainframe kernel: usb-storage 1-3:1.0: **USB Mass Storage device detected**") and when it was removed ("2024-09-26T16:53:00.340175+01:00 mainframe kernel: usb 1-3: **USB disconnect, device number 3**"). Since these dates are in between when he received the email containing the location of the pen drive and when he messaged RootKitty about its contents, we can infer that it's indeed the same as the one he obtained from the anonymous email sender.

3 Analysis of relevant findings

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

Yes. We found the originally discovered files from João Musk's sigma account on his computer on the backup present in the home directory for the user johnnymusk's desktop. Specifically in the **backup_1727368201.zip** backup file of the backupDisk. The **poster.pdf** and **thrones.pdf** files were also found in johnnyDisk's Documents directory and the **best-intro.wav** was found as got.wav in the Music directory. The files **hd.jpg, wallpaper.png, got.jpg** hidden inside the myzip.zip artifact are located in the Pictures directory. The **cartwheel.tiff, andromeda.png, lactea.jpg, tagus.png** files are also found in the Pictures directory of johnnyDisk. The **nmap** file was discovered in the password protected backup zip files, and since it was where we discovered the stolen ist credentials, we can safely assume that this was highly important information for Musk, hence why he safeguarded it so dearly.

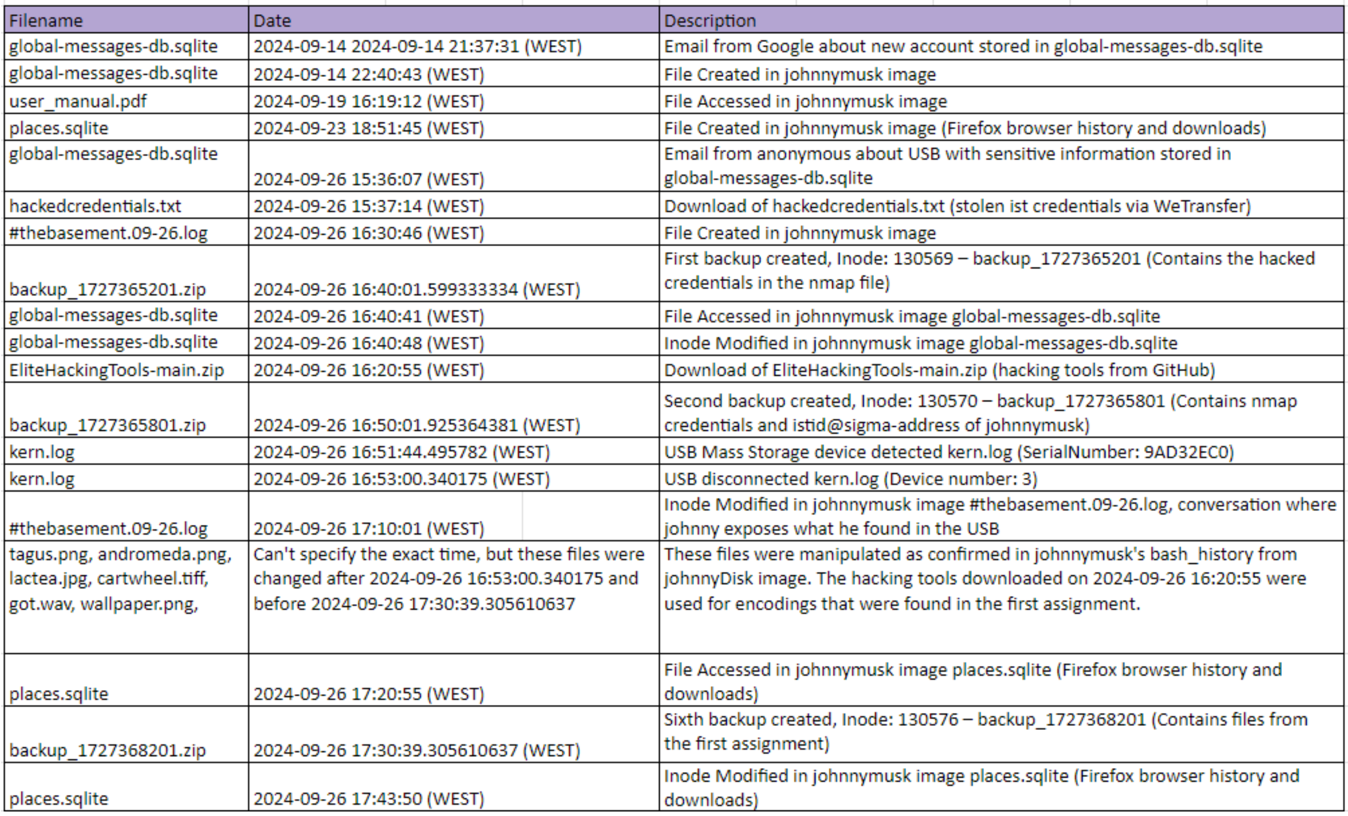
About the hidden artifacts, we know that João Musk got access to the hacked credentials by receiving them from an unknown user "RootKitty" whom he had conversations with in "Issra", we will talk more about that shortly. **The Bank Statement, the blueprint of the Ariane 6 rocket, MKUltra API Documentation, MKUltra related logs and the DECO report** were all found in a USB that Musk picked up in the LockerLocky from the CTT in IST Lisboa, after he was presented with an email form an anonymous entity.

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

Almost all of the hidden stage1 artifacts (bankstatement, ist_satellite, mkultra_logs, mkultra_api, deco_article) are known to come from the USB drive that Mr. Musk retrieved from the Locky locker on September 26th. The other hidden artifact, the fenix_credentials, were sent to him via his IST colleague RootKitty on a WeTransfer link on that same day. All these files suffered some kind of transformation, as our suspect did everything he could to hide them, just like we witnessed in the first stage of this investigation, and then deleted them. We will talk about these transformations in detail in section 3.3.

When reviewing the backupDisk image, we can find in most of the backups a **ist90834@10.0.2.166** file, which seems to be the session in which Musk's sigma cluster services were established, since those range between 10.0.2.160 and 10.0.2.180. He was in the same sigma session throughout all backups recorded, which happened on the 26th of September 2024.

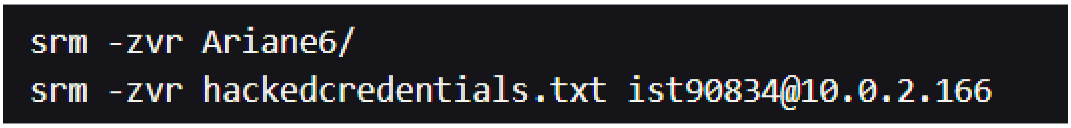
The following timeline allows us to understand the source and alterations to the file. This timeline is also located in the zip (**csf2425-timeline-lab2-G007.xlsx**), located in the sheet called "3.2 Timeline"



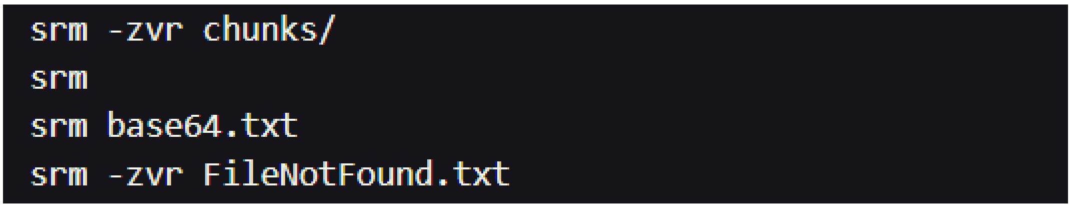
Filename	Date	Description
global-messages-db.sqlite	2024-09-14 2024-09-14 21:37:31 (WEST)	Email from Google about new account stored in global-messages-db.sqlite
global-messages-db.sqlite	2024-09-14 22:40:43 (WEST)	File Created in johnnymusk image
user_manual.pdf	2024-09-19 16:19:12 (WEST)	File Accessed in johnnymusk image
places.sqlite	2024-09-23 18:51:45 (WEST)	File Created in johnnymusk image (Firefox browser history and downloads)
global-messages-db.sqlite	2024-09-26 15:36:07 (WEST)	Email from anonymous about USB with sensitive information stored in global-messages-db.sqlite
hackedcredentials.txt	2024-09-26 15:37:14 (WEST)	Download of hackedcredentials.txt (stolen ist credentials via WeTransfer)
#thebasement.09-26.log	2024-09-26 16:30:46 (WEST)	File Created in johnnymusk image
backup_1727365201.zip	2024-09-26 16:40:01.599333334 (WEST)	First backup created, Inode: 130569 – backup_1727365201 (Contains the hacked credentials in the nmap file)
global-messages-db.sqlite	2024-09-26 16:40:41 (WEST)	File Accessed in johnnymusk image global-messages-db.sqlite
global-messages-db.sqlite	2024-09-26 16:40:48 (WEST)	Inode Modified in johnnymusk image global-messages-db.sqlite
EliteHackingTools-main.zip	2024-09-26 16:20:55 (WEST)	Download of EliteHackingTools-main.zip (hacking tools from GitHub)
backup_1727365801.zip	2024-09-26 16:50:01.925364381 (WEST)	Second backup created, Inode: 130570 – backup_1727365801 (Contains nmap credentials and istid@sigma-address of johnnymusk)
kern.log	2024-09-26 16:51:44.495782 (WEST)	USB Mass Storage device detected kern.log (SerialNumber: 9AD32EC0)
kern.log	2024-09-26 16:53:00.340175 (WEST)	USB disconnected kern.log (Device number: 3)
#thebasement.09-26.log	2024-09-26 17:10:01 (WEST)	Inode Modified in johnnymusk image #thebasement.09-26.log, conversation where johnny exposes what he found in the USB
tagus.png, andromeda.png, lactea.jpg, cartwheel.tiff, got.wav, wallpaper.png,	Can't specify the exact time, but these files were changed after 2024-09-26 16:53:00.340175 and before 2024-09-26 17:30:39.305610637	These files were manipulated as confirmed in johnnymusk's bash_history from johnnyDisk image. The hacking tools downloaded on 2024-09-26 16:20:55 were used for encodings that were found in the first assignment.
places.sqlite	2024-09-26 17:20:55 (WEST)	File Accessed in johnnymusk image places.sqlite (Firefox browser history and downloads)
backup_1727368201.zip	2024-09-26 17:30:39.305610637 (WEST)	Sixth backup created, Inode: 130576 – backup_1727368201 (Contains files from the first assignment)
places.sqlite	2024-09-26 17:43:50 (WEST)	Inode Modified in johnnymusk image places.sqlite (Firefox browser history and downloads)

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

Yes, we found several kinds of evidence of anti-forensic activity. One of them was the use of the **srm** command, where it was used to delete several files, as we discovered in the .bash_history file .The use of this command is noteworthy in this context because by using it to delete a file, the file becomes impossible to uncover with commands like **fls -Frd** and unrecoverable through file carving.



```
srm -zvr Ariane6/
srm -zvr hackedcredentials.txt ist90834@10.0.2.166
```



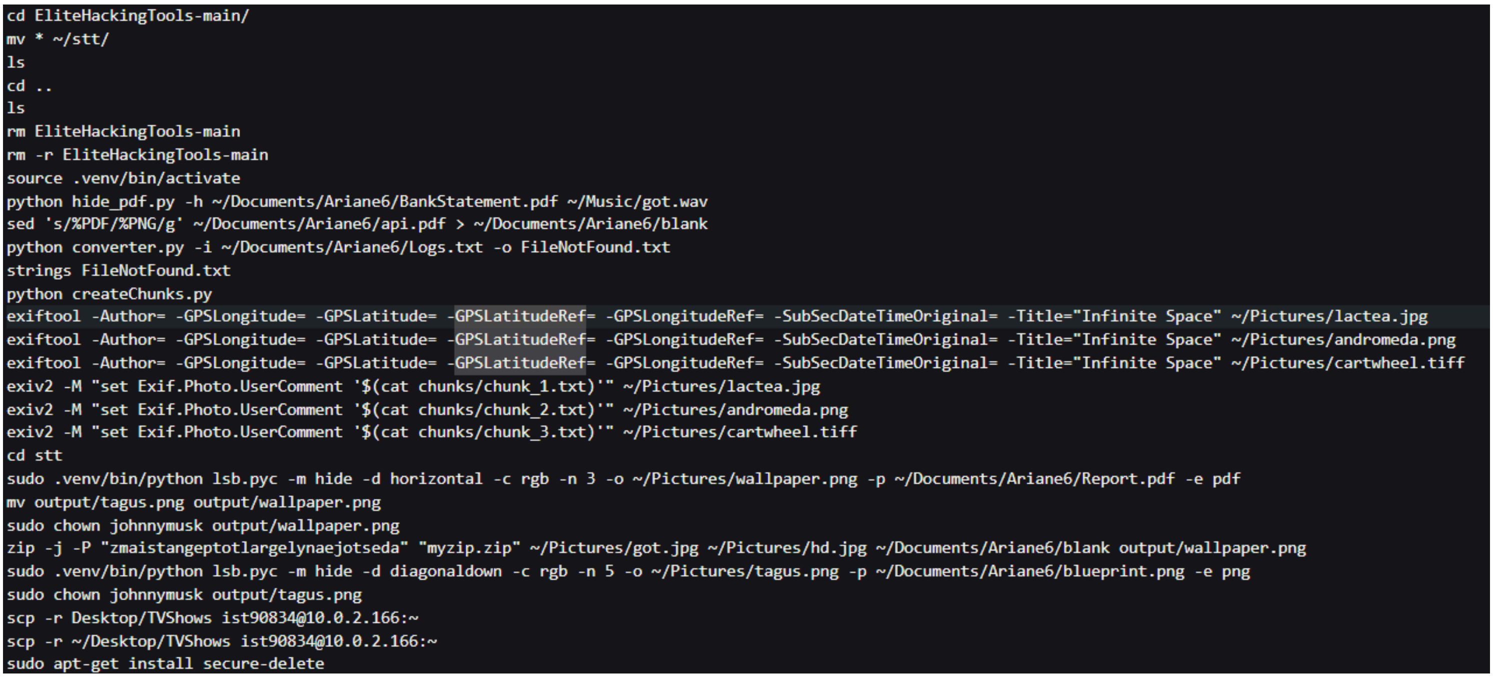
```
srm -zvr chunks/
srm
srm base64.txt
srm -zvr FileNotFound.txt
```

In this case, srm was used with the -z flag, which zeroes out the file's data before deletion and makes it much more difficult to recover any of them and with the -r flag which allows the user to recursively delete the contents of a folder.

We also found two browser entries related to secure file deletion:

- "Ways to Permanently and Securely Delete ‘Files and Directories’ in Linux - GeeksforGeeks"
- "how to secure delete in linux - Pesquisa Google"

Another piece of evidence of anti-forensic activities we discovered were the “Elite Hacking Tools”, Musk downloaded from the website “https://github.com/PirateMajima/EliteHackingTools”, as we can check on the file browser_downloads.json. Besides these tools, Musk also used a multitude of steganography tools when he was in the process of concealing the files given to him in the flash drive. We have evidence of the use of these tools through the .bash_history:

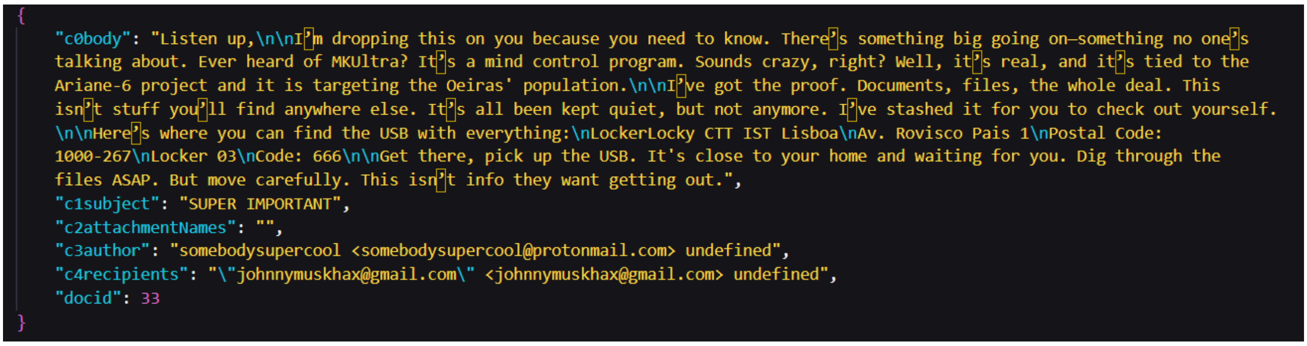


```
cd EliteHackingTools-main/
mv * ~/stt/
ls
cd ..
ls
rm EliteHackingTools-main
rm -r EliteHackingTools-main
source .venv/bin/activate
python hide_pdf.py -h ~/Documents/Ariane6/BankStatement.pdf ~/Music/got.wav
sed 's/%PDF/%PNG/g' ~/Documents/Ariane6/api.pdf > ~/Documents/Ariane6/blank
python converter.py -i ~/Documents/Ariane6/Logs.txt -o FileNotFound.txt
strings FileNotFound.txt
python createChunks.py
exiftool -Author= -GPSLongitude= -GPSLatitude= -GPSLatitudeRef= -GPSLongitudeRef= -SubSecDateTimeOriginal= -Title="Infinite Space" ~/Pictures/lactea.jpg
exiftool -Author= -GPSLongitude= -GPSLatitude= -GPSLatitudeRef= -GPSLongitudeRef= -SubSecDateTimeOriginal= -Title="Infinite Space" ~/Pictures/andromeda.png
exiftool -Author= -GPSLongitude= -GPSLatitude= -GPSLatitudeRef= -GPSLongitudeRef= -SubSecDateTimeOriginal= -Title="Infinite Space" ~/Pictures/cartwheel.tiff
exiv2 -M "set Exif.Photo.UserComment '$(cat chunks/chunk_1.txt)'" ~/Pictures/lactea.jpg
exiv2 -M "set Exif.Photo.UserComment '$(cat chunks/chunk_2.txt)'" ~/Pictures/andromeda.png
exiv2 -M "set Exif.Photo.UserComment '$(cat chunks/chunk_3.txt)'" ~/Pictures/cartwheel.tiff
cd stt
sudo .venv/bin/python lsb.pyc -m hide -d horizontal -c rgb -n 3 -o ~/Pictures/wallpaper.png -p ~/Documents/Ariane6/Report.pdf -e pdf
mv output/tagus.png output/wallpaper.png
sudo chown johnnymusk output/wallpaper.png
zip -j -P "zmaistangeptotlargelynaejotseda" "myzip.zip" ~/Pictures/got.jpg ~/Pictures/hd.jpg ~/Documents/Ariane6/blank output/wallpaper.png
sudo .venv/bin/python lsb.pyc -m hide -d diagonaldown -c rgb -n 5 -o ~/Pictures/tagus.png -p ~/Documents/Ariane6/blueprint.png -e png
sudo chown johnnymusk output/tagus.png
scp -r Desktop/TVShows ist90834@10.0.2.166:~
scp -r ~/Desktop/TVShows ist90834@10.0.2.166:~
sudo apt-get install secure-delete
```

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

After analyzing the contents of both Mr. Musk's workstation and his backup server, it's safe to say that we have a much better understanding of what happened in this complicated situation.

From our understanding, the first important event was the email that João Musk received from author somebodysupercool@protonmail.com, one of the new relevant actors in our investigation, telling him to retrieve a flash drive from a Locky and see for himself the evidence uncovered about a mind control program called MKUltra.



```
{
    "c0body": "Listen up,\n\nI’m dropping this on you because you need to know. There’s something big going on—something no one’s talking about. Ever heard of MKUltra? It’s a mind control program. Sounds crazy, right? Well, it’s real, and it’s tied to the Ariane-6 project and it is targeting the Oeiras' population.\n\nI’ve got the proof. Documents, files, the whole deal. This isn’t stuff you’ll find anywhere else. It’s all been kept quiet, but not anymore. I’ve stashed it for you to check out yourself. \n\nHere’s where you can find the USB with everything:\nLockerLocky CTT IST Lisboa\nAv. Rovisco Pais 1\nPostal Code: 1000-267\nLocker 03\nCode: 666\n\nGet there, pick up the USB. It's close to your home and waiting for you. Dig through the files ASAP. But move carefully. This isn’t info they want getting out.",
    "c1subject": "SUPER IMPORTANT",
    "c2attachmentNames": "",
    "c3author": "somebodysupercool <somebodysupercool@protonmail.com> undefined",
    "c4recipients": "\"johnnymuskhax@gmail.com\" <johnnymuskhax@gmail.com> undefined",
    "docid": 33
}
```

Because of this email, it seems that Musk had the urge to go grab the USB flash drive and go through all of its contents, which point to a conspiracy theory involving a mind control program that uses the satellite Ariane6 to control the minds of the population of Oeiras and make them eat at the restaurants in the area. After looking at these files, Musk felt the need to go on a deep browsing investigation about:

- **the launch of Ariane6**

- "ISTSat-1: Satélite totalmente desenvolvido no Técnico chegou ao Espaço – Técnico Lisboa"
- "ANACOM - Lançamento do ISTSAT-1 assinala mais um importante passo da presença de Portugal no espaço"
- "ISTSat-1: O primeiro nanosatélite do Técnico - YouTube"
- "ESA - Ariane 6 overview"

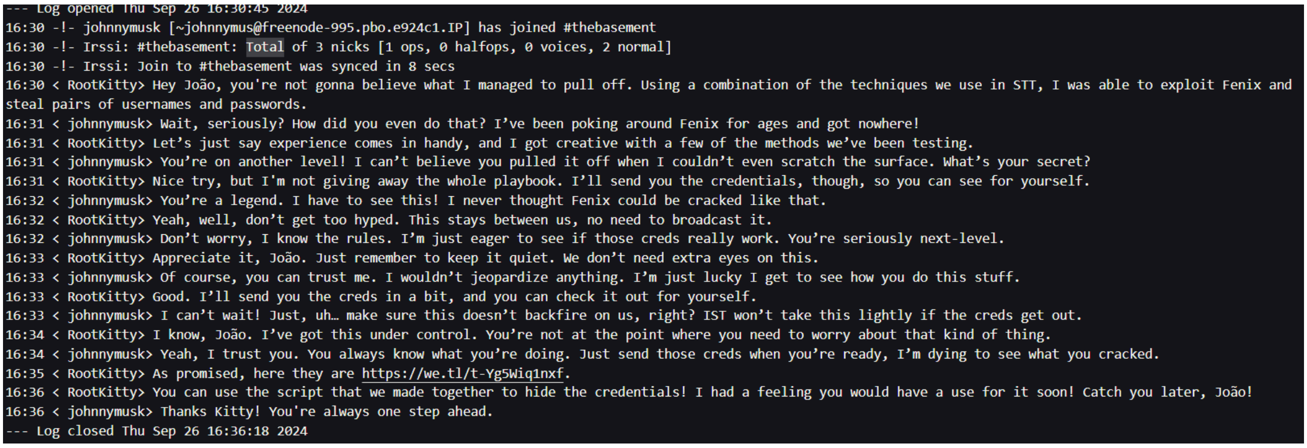
- **some Oeiras restaurants and their reviews**

- "A TENDINHA, Oeiras - Rua Rodrigues de Freitas 5 - Comentários de Restaurantes, Fotos & Número de Telefone (2024)"
- "O POMBALINO, Oeiras - Comentários de Restaurantes, Fotos & Número de Telefone"
- "A CACOILA, Oeiras - Comentários de Restaurantes, Fotos & Número de Telefone (2024)"
- "RESTAURANTE O TRANSMONTANO, Oeiras - Comentários de Restaurantes, Fotos & Número de Telefone"

- **the possibility of mind control**

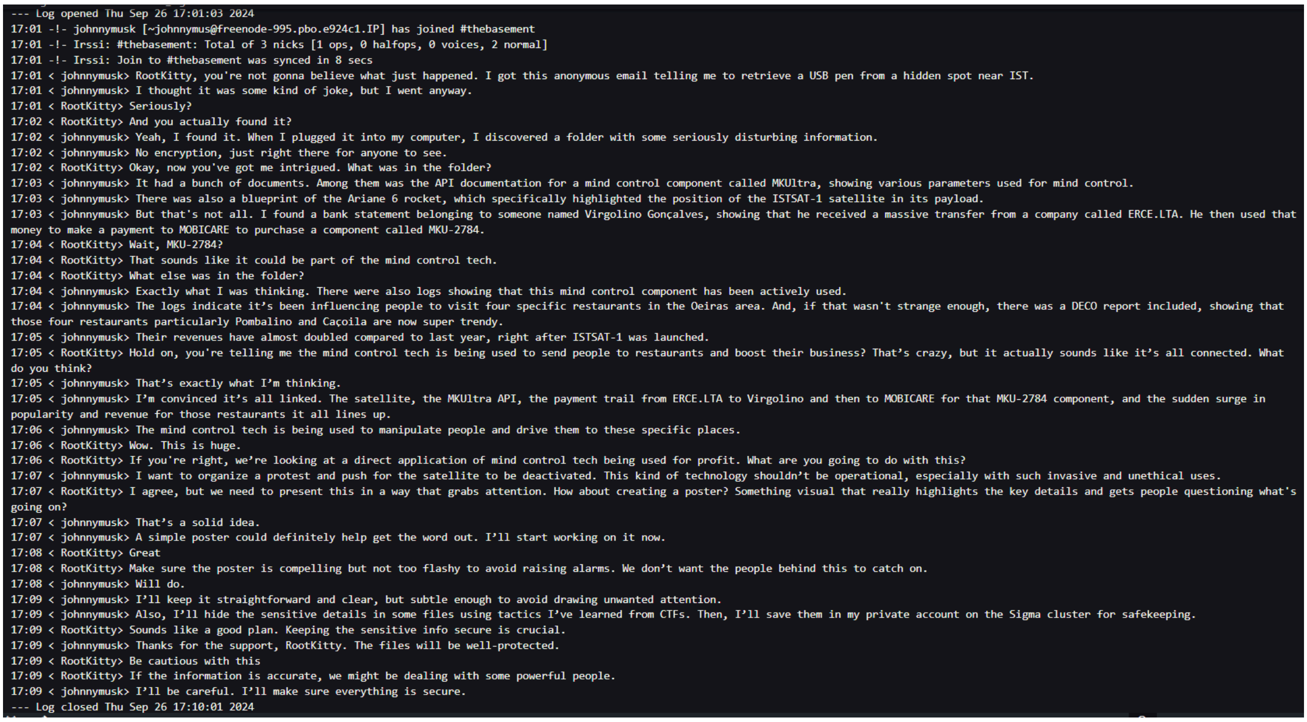
- "is mind control really possible - Pesquisa Google"
- "MIT School of Engineering | » Is it possible to control someone's thoughts?"
- "can i get a girlfriend via mind control - Pesquisa Google"
- "How To Get A Girl To Like You 💟 Using Mind Control 💟 - YouTube"

After all this research, Mr. Musk receives a message from an IST colleague, here named RootKitty (another relevant actor) saying that they have been able to steal pairs of usernames and passwords from Fenix, using techniques they learned at STT.



```
--- Log opened Thu Sep 26 16:30:45 2024
16:30 -!- johnnymusk [~johnnymus@freenode-995.pbo.e924c1.IP] has joined #thebasement
16:30 -!- Irssi: #thebasement: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2 normal]
16:30 -!- Irssi: Join to #thebasement was synced in 8 secs
16:30 < RootKitty> Hey João, you're not gonna believe what I managed to pull off. Using a combination of the techniques we use in STT, I was able to exploit Fenix and
steal pairs of usernames and passwords.
16:31 < johnnymusk> Wait, seriously? How did you even do that? I've been poking around Fenix for ages and got nowhere!
16:31 < RootKitty> Let's just say experience comes in handy, and I got creative with a few of the methods we've been testing.
16:31 < johnnymusk> You're on another level! I can't believe you pulled it off when I couldn't even scratch the surface. What's your secret?
16:31 < RootKitty> Nice try, but I'm not giving away the whole playbook. I'll send you the credentials, though, so you can see for yourself.
16:32 < johnnymusk> You're a legend. I have to see this! I never thought Fenix could be cracked like that.
16:32 < RootKitty> Yeah, well, don't get too hyped. This stays between us, no need to broadcast it.
16:32 < johnnymusk> Don't worry, I know the rules. I'm just eager to see if those creds really work. You're seriously next-level.
16:33 < RootKitty> Appreciate it, João. Just remember to keep it quiet. We don't need extra eyes on this.
16:33 < johnnymusk> Of course, you can trust me. I wouldn't jeopardize anything. I'm just lucky I get to see how you do this stuff.
16:33 < RootKitty> Good. I'll send you the creds in a bit, and you can check it out for yourself.
16:33 < johnnymusk> I can't wait! Just, uh… make sure this doesn't backfire on us, right? IST won't take this lightly if the creds get out.
16:34 < RootKitty> I know, João. I've got this under control. You're not at the point where you need to worry about that kind of thing.
16:34 < johnnymusk> Yeah, I trust you. You always know what you're doing. Just send those creds when you're ready, I'm dying to see what you cracked.
16:35 < RootKitty> As promised, here they are https://we.tl/t-Yg5Wiq1nxf.
16:36 < RootKitty> You can use the script that we made together to hide the credentials! I had a feeling you would have a use for it soon! Catch you later, João!
16:36 < johnnymusk> Thanks Kitty! You're always one step ahead.
--- Log closed Thu Sep 26 16:36:18 2024
```

Our suspect goes and downloads the hacked credentials from a WeTransfer link, given the information we were able to obtain in the file browser_downloads.json and then returns to the chat to tell RootKitty about the pen drive he obtained and its discoveries.

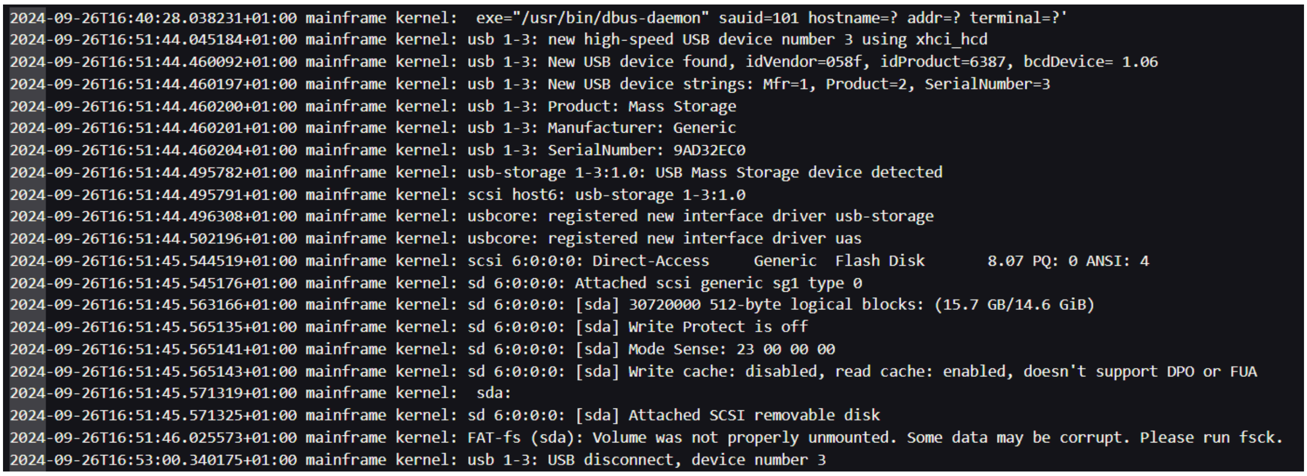


```
--- Log opened Thu Sep 26 17:01:03 2024
17:01 -!- johnnymusk [~johnnymus@freenode-995.pbo.e924c1.IP] has joined #thebasement
17:01 -!- Irssi: #thebasement: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2 normal]
17:01 -!- Irssi: Join to #thebasement was synced in 8 secs
17:01 < johnnymusk> RootKitty, you're not gonna believe what just happened. I got this anonymous email telling me to retrieve a USB pen from a hidden spot near IST.
17:01 < johnnymusk> I thought it was some kind of joke, but I went anyway.
17:01 < RootKitty> Seriously?
17:02 < RootKitty> And you actually found it?
17:02 < johnnymusk> Yeah, I found it. When I plugged it into my computer, I discovered a folder with some seriously disturbing information.
17:02 < johnnymusk> No encryption, just right there for anyone to see.
17:02 < RootKitty> Okay, now you've got me intrigued. What was in the folder?
17:03 < johnnymusk> It had a bunch of documents. Among them was the API documentation for a mind control component called MKUltra, showing various parameters used for mind control.
17:03 < johnnymusk> There was also a blueprint of the Ariane 6 rocket, which specifically highlighted the position of the ISTSAT-1 satellite in its payload.
17:03 < johnnymusk> But that's not all. I found a bank statement belonging to someone named Virgolino Gonçalves, showing that he received a massive transfer from a company called ERCE.LTA. He then used that
money to make a payment to MOBICARE to purchase a component called MKU-2784.
17:04 < RootKitty> Wait, MKU-2784?
17:04 < RootKitty> That sounds like it could be part of the mind control tech.
17:04 < RootKitty> What else was in the folder?
17:04 < johnnymusk> Exactly what I was thinking. There were also logs showing that this mind control component has been actively used.
17:04 < johnnymusk> The logs indicate it’s been influencing people to visit four specific restaurants in the Oeiras area. And, if that wasn't strange enough, there was a DECO report included, showing that
those four restaurants particularly Pombalino and Caçoila are now super trendy.
17:05 < johnnymusk> Their revenues have almost doubled compared to last year, right after ISTSAT-1 was launched.
17:05 < RootKitty> Hold on, you're telling me the mind control tech is being used to send people to restaurants and boost their business? That’s crazy, but it actually sounds like it’s all connected. What
do you think?
17:05 < johnnymusk> That’s exactly what I’m thinking.
17:05 < johnnymusk> I’m convinced it’s all linked. The satellite, the MKUltra API, the payment trail from ERCE.LTA to Virgolino and then to MOBICARE for that MKU-2784 component, and the sudden surge in
popularity and revenue for those restaurants it all lines up.
17:06 < johnnymusk> The mind control tech is being used to manipulate people and drive them to these specific places.
17:06 < RootKitty> Wow. This is huge.
17:06 < RootKitty> If you're right, we’re looking at a direct application of mind control tech being used for profit. What are you going to do with this?
17:07 < johnnymusk> I want to organize a protest and push for the satellite to be deactivated. This kind of technology shouldn’t be operational, especially with such invasive and unethical uses.
17:07 < RootKitty> I agree, but we need to present this in a way that grabs attention. How about creating a poster? Something visual that really highlights the key details and gets people questioning what's
going on?
17:07 < johnnymusk> That’s a solid idea.
17:07 < johnnymusk> A simple poster could definitely help get the word out. I’ll start working on it now.
17:08 < RootKitty> Great
17:08 < RootKitty> Make sure the poster is compelling but not too flashy to avoid raising alarms. We don’t want the people behind this to catch on.
17:08 < johnnymusk> Will do.
17:09 < johnnymusk> I’ll keep it straightforward and clear, but subtle enough to avoid drawing unwanted attention.
17:09 < johnnymusk> Also, I’ll hide the sensitive details in some files using tactics I’ve learned from CTFs. Then, I’ll save them in my private account on the Sigma cluster for safekeeping.
17:09 < RootKitty> Sounds like a good plan. Keeping the sensitive info secure is crucial.
17:09 < johnnymusk> Thanks for the support, RootKitty. The files will be well-protected.
17:09 < RootKitty> Be cautious with this
17:09 < RootKitty> If the information is accurate, we might be dealing with some powerful people.
17:09 < johnnymusk> I’ll be careful. I’ll make sure everything is secure.
--- Log closed Thu Sep 26 17:10:01 2024
```

After this chat, Musk goes on to encrypt every file on the flash drive + the hacked credentials into the files encountered in the first stage, just like we previously analyzed. He writes scripts to automatically backup his sensitive information to his Sigma server, using diverse steganography techniques. He also designs a poster to encourage people to rebel and protest against the Ariane6 launch, due to his recent discoveries.

4 Appendices

The section of kern.log in which we can see a USB device being connected and disconnected:



```
2024-09-26T16:40:28.038231+01:00 mainframe kernel:  exe="/usr/bin/dbus-daemon" sauid=101 hostname=? addr=? terminal=?'
2024-09-26T16:51:44.045184+01:00 mainframe kernel: usb 1-3: new high-speed USB device number 3 using xhci_hcd
2024-09-26T16:51:44.460092+01:00 mainframe kernel: usb 1-3: New USB device found, idVendor=058f, idProduct=6387, bcdDevice= 1.06
2024-09-26T16:51:44.460197+01:00 mainframe kernel: usb 1-3: New USB device strings: Mfr=1, Product=2, SerialNumber=3
2024-09-26T16:51:44.460200+01:00 mainframe kernel: usb 1-3: Product: Mass Storage
2024-09-26T16:51:44.460201+01:00 mainframe kernel: usb 1-3: Manufacturer: Generic
2024-09-26T16:51:44.460204+01:00 mainframe kernel: usb 1-3: SerialNumber: 9AD32EC0
2024-09-26T16:51:44.495782+01:00 mainframe kernel: usb-storage 1-3:1.0: USB Mass Storage device detected
2024-09-26T16:51:44.495791+01:00 mainframe kernel: scsi host6: usb-storage 1-3:1.0
2024-09-26T16:51:44.496308+01:00 mainframe kernel: usbcore: registered new interface driver usb-storage
2024-09-26T16:51:44.502196+01:00 mainframe kernel: usbcore: registered new interface driver uas
2024-09-26T16:51:45.544519+01:00 mainframe kernel: scsi 6:0:0:0: Direct-Access     Generic  Flash Disk       8.07 PQ: 0 ANSI: 4
2024-09-26T16:51:45.545176+01:00 mainframe kernel: sd 6:0:0:0: Attached scsi generic sg1 type 0
2024-09-26T16:51:45.563166+01:00 mainframe kernel: sd 6:0:0:0: [sda] 30720000 512-byte logical blocks: (15.7 GB/14.6 GiB)
2024-09-26T16:51:45.565135+01:00 mainframe kernel: sd 6:0:0:0: [sda] Write Protect is off
2024-09-26T16:51:45.565141+01:00 mainframe kernel: sd 6:0:0:0: [sda] Mode Sense: 23 00 00 00
2024-09-26T16:51:45.565143+01:00 mainframe kernel: sd 6:0:0:0: [sda] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
2024-09-26T16:51:45.571319+01:00 mainframe kernel:  sda:
2024-09-26T16:51:45.571325+01:00 mainframe kernel: sd 6:0:0:0: [sda] Attached SCSI removable disk
2024-09-26T16:51:46.025573+01:00 mainframe kernel: FAT-fs (sda): Volume was not properly unmounted. Some data may be corrupt. Please run fsck.
2024-09-26T16:53:00.340175+01:00 mainframe kernel: usb 1-3: USB disconnect, device number 3
```