INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab2

Group number:	16	Name	IST Number
Student 1:		Inês Alves	99084
Student 2:		Afonso Pires	102803
Student 3:		António Dias da Silva	102879

1 Acquired artifacts

Name	Type	SHA-256 Value
Ariane6 secret	.png	
MKU secret	.png	16bd3a08718d706aab253e2ddbca5f2c553d38bb93b7a7c71cbef923082b589a
Deco secret	.png	956babc244fb9b4191ae7f35f823467b73e465bc9ea3b1f68d36dc8d94e3f81d
Bank Statements secret	.png	61a70aeed310a9e2772f694d5106408e8e65bba6e355a927e6dff900515591e3
Hacked Credentials	references	
#thebasement.09-26.log	.log	b19ce5156507851d206f7559ed67cb308d2b8b774f096296fcfee754cb98df82

2 Report of all findings

2.1 Overview

backupDisk.img

Artifact	Inode	Path	Actions to find it
andromeda.png best-intro.wav cartwheel.tiff	130576	/home/johnnymusk/backup_1727368201.zip	fls -o 2048 backupDisk.img fls -o 2048 backupDisk.img 130573 fls -o 2048 backupDisk.img 130561

lactea.jpg myzip.zip nmap poster.pdf tagus.png thrones.pdf			icat -o 2048 backupDisk.img 130576 > backup_1727368201.zip [the whole process of discovering the zip password is explained in the following section] unzip backup_1727368201.zip

johnnyDisk.img

Artifact	Inode	Path	Actions to find it
andromeda.png	533624	/home/johnnymusk/Pictures	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] fls -o 4096 johnnyDisk.img 525126 [/Pictures] icat -o 4096 johnnyDisk.img 525126 > andromeda.png
Ariane6.webp	533630	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533630 > Ariane6.webp
cartwheel.tiff	533629	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533629 > cartwheel.tiff
got.jpg	533622	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533622 > got.jpg
hd.jpg	533621	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533621 > hd.jpg
lactea.jpg	533618	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533618 > lactea.jpg
wallpaper.png	533627	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533627 > wallpaper.png
tagus.png	533632	/home/johnnymusk/Pictures	icat -o 4096 johnnyDisk.img 533632 > tagus.png
backup.sh	525469	/home/johnnymusk/backup	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] fls -o 4096 johnnyDisk.img 530482 [/backup] [visited this folder searching for backup zips' password] icat -o 4096 johnnyDisk.img 525469 > backup.sh
obfuscator	530485	/home/johnnymusk/backup	icat -o 4096 johnnyDisk.img 530485 > obfuscator
pass_gen.sh	533787	/home/johnnymusk/backup	icat -o 4096 johnnyDisk.img 533787 > pass_gen.sh

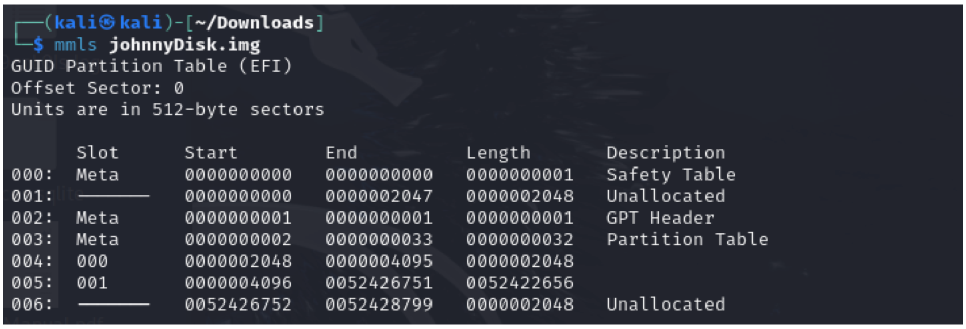
User_Manual.pdf	533519	/home/johnnymusk/Documents	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] fls -o 4096 johnnyDisk.img 525124 [/Documents] icat -o 4096 johnnyDisk.img 533519 > User_Manual.pdf
thrones.pdf	528140	/home/johnnymusk/Documents	icat -o 4096 johnnyDisk.img 528140 > thrones.pdf
poster.pdf	524881	/home/johnnymusk/Documents	icat -o 4096 johnnyDisk.img 524881 > poster.pdf
source.py	533782	/home/johnnymusk/stt	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] fls -o 4096 johnnyDisk.img 533761 [/stt] icat -o 4096 johnnyDisk.img 533782 > source.py
exploit.py	533755	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 533755 > exploit.py
source.zip	533790	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 533790 > source.zip
exploit.htpl	533791	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 533791 > exploit.htpl
cookieSteal.html	533786	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 533786 > cookieSteal.html
reflectedXSS.html	525860	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 525860 > reflectedXSS.html
doubleEncodingAndHidingInsideElf.py	574148	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 574148 > doubleEncodingAndHidingInsideElf.py
nmap_og	524896	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 524896 > nmap_og
converter.py	576586	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 576586 > converter.py
createChunks.py	576587	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 576587 > createChunks.py
hide_pdf.py	576588	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 576588 > hide_pdf.py
lsb.pyc	576589	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 576589 > lsb.pyc
README.md	576400	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 576400 > README.md

requirements.txt	576590	/home/johnnymusk/stt	icat -o 4096 johnnyDisk.img 576590 > requirements.txt
Passwords.kdbx	525007	/home/johnnymusk	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] icat -o 4096 johnnyDisk.img 525007 > Passwords.kdbx [had seed for backup zips' passwords]
.bash_history	525717	/home/johnnymusk	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] icat -o 4096 johnnyDisk.img 525717 > .bash_history
Inbox	530385	/home/johnnymusk/snap/thunderbird/common/.thunderbird/iw2y9jr6.default/Mail/pop.gmail.com	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/home] fls -o 4096 johnnyDisk.img 524925 [/johnnymusk] fls -o 4096 johnnyDisk.img 525178 [/snap] fls -o 4096 johnnyDisk.img 530176 [/thunderbird] fls -o 4096 johnnyDisk.img 530178 [/common] fls -o 4096 johnnyDisk.img 530232 [/.thunderbird] fls -o 4096 johnnyDisk.img 530242 [/iw2y9jr6.default] fls -o 4096 johnnyDisk.img 530382 [/Mail] fls -o 4096 johnnyDisk.img 530383 [/pop.gmail.com] icat -o 4096 johnnyDisk.img 530385 > Inbox CyberChef to decode from base64 [found suspicious emails]
#thebasement.09-26.log	574131	/home/johnnymusk/snap/irssi/common/irclogs/2024/freenode/	fls -o 4096 johnnyDisk.img 530362 [/irssi] [visited this folder because found irssi @ .bash_history] fls -o 4096 johnnyDisk.img 530476 [/common] fls -o 4096 johnnyDisk.img 531702 [/irclogs] fls -o 4096 johnnyDisk.img 533408 [/2024] fls -o 4096 johnnyDisk.img 574149 [/freenode] icat -o 4096 johnnyDisk.img 574131 > #thebasement.09-26.log [found conversation with confessions about activities]
syslog	274243	/var/log	fls -o 4096 johnnyDisk.img [/] fls -o 4096 johnnyDisk.img 131073 [/var] fls -o 4096 johnnyDisk.img 524925 [/log]

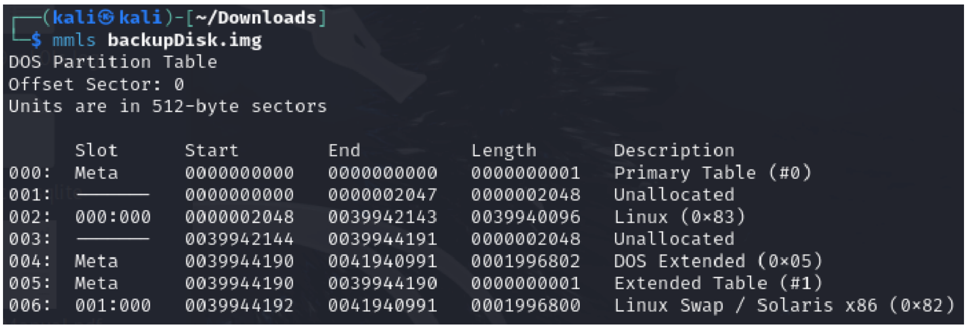
			icat -o 4096 johnnyDisk.img 274243 > syslog [found evidence of USB device]
places.sqlite	530334	/home/snap/firefox/common/.mozilla/firefox/t7pu9ru3.default/	fls -o 4096 johnnyDisk.img 533723 [/firefox] fls -o 4096 johnnyDisk.img 533785 [/common] fls -o 4096 johnnyDisk.img 533849 [/.mozilla] fls -o 4096 johnnyDisk.img 533850 [/firefox] fls -o 4096 johnnyDisk.img 533858 [/t7pu9ru3.default] icat -o 4096 johnnyDisk.img 530334 > places.sqlite [found browser history]
K5rb9cnL0Is.log	1310805	/tmp/	fls -o 4096 johnnyDisk.img 533858 [/tmp] icat -o 4096 johnnyDisk.img 1310805 > K5rb9cnL0Is.log [found Passwords.kdbx's password]
Ariane6 secret		output_foremost/png	foremost -i johnnyDisk.img -o output_foremost
MKU secret		output_foremost/png	foremost -i johnnyDisk.img -o output_foremost
Deco secret		output_foremost/png	foremost -i johnnyDisk.img -o output_foremost
Bank Statements secret		output_foremost/png	foremost -i johnnyDisk.img -o output_foremost

2.2 Detailed Process

In our investigation process, we primarily make use of mmls, which provided us with crucial information about the disks' partitions. This tool offers details about where each partition starts and ends on the disk in sector units. These partition offsets are fundamental for understanding the disk's layout.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ mmls johnnyDisk.img
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0000004095   0000002048
005:  001       0000004096   0052426751   0052422656
006:  -------   0052426752   0052428799   0000002048   Unallocated
```



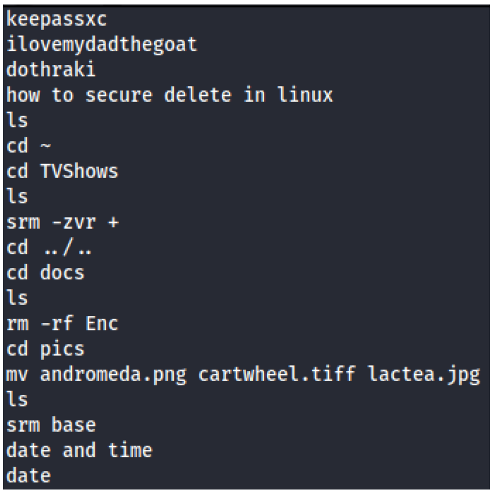
```
┌──(kali㉿kali)-[~/Downloads]
└─$ mmls backupDisk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0039942143   0039940096   Linux (0x83)
003:  -------   0039942144   0039944191   0000002048   Unallocated
004:  Meta      0039944190   0041940991   0001996802   DOS Extended (0x05)
005:  Meta      0039944190   0039944190   0000000001   Extended Table (#1)
006:  001:000   0039944192   0041940991   0001996800   Linux Swap / Solaris x86 (0x82)
```

Figure 1,2 – command mmls on johnnyDisk.img and backupDisk.img

Upon analyzing the disk images with the mmls command, two partitions from backupDisk.img and johnnyDisk.img were identified as significant for investigation. For backupDisk.img, the primary partition (starting at sector 2048) is formatted as a Linux filesystem (ID 0x83) and is crucial for uncovering user data and potential artifacts. In johnnyDisk.img, the partition beginning at sector 4096 is particularly interesting as it spans over 5 million sectors, indicating it likely holds the majority of the file system and user data. Investigating these partitions will be essential to identify any suspicious files or artifacts relevant.

In the backupDisk.img, we discover several zip files within the **/home/johnnymusk/** directory, each named in the format "backup_<number>.zip". Upon attempting to open these zip files, it became evident that they were password-protected, which meant they required the retrieval of the passwords to access their contents.

To assist in this endeavor, we examined the johnnyDisk.img and located a file named Passwords.kdbx within the **/home/johnnymusk/** directory, which also required a password to access. Further investigation revealed a log file called K5rb9cnL0Is.log located in /tmp/. The existence of this file was only possible, because one of the tools used by João to cover his files contained a keylogger. After decompiling the lsb.pyc script, the code revealed that it was a keylogger application designed to record and log every keystroke made on a computer. From this was created K5rb9cnL0Is.log , which then led us to conclude that the password for the Passwords.kdbx file is **ilovemydadthegoat**.



```
keepassxc
ilovemydadthegoat
dothraki
how to secure delete in linux
ls
cd ~
cd TVShows
ls
srm -zvr +
cd ../..
cd docs
ls
rm -rf Enc
cd pics
mv andromeda.png cartwheel.tiff lactea.jpg
ls
srm base
date and time
date
```

Figure 4 – content of the K5rb9cnL0Is.log

Additionally, we discovered a directory named backups, which contained three files: pass_gen.sh, obfuscator, and backup.sh. Analyzing these files indicated that the obfuscator was responsible for generating the passwords for the seven zip files. However, to execute this function, we needed the initial seed that we found on Passwords.kdbx, which was **TheBiteOf87**. Through this investigation, we successfully uncovered the passwords for the zip files contained in backupDisk.img:

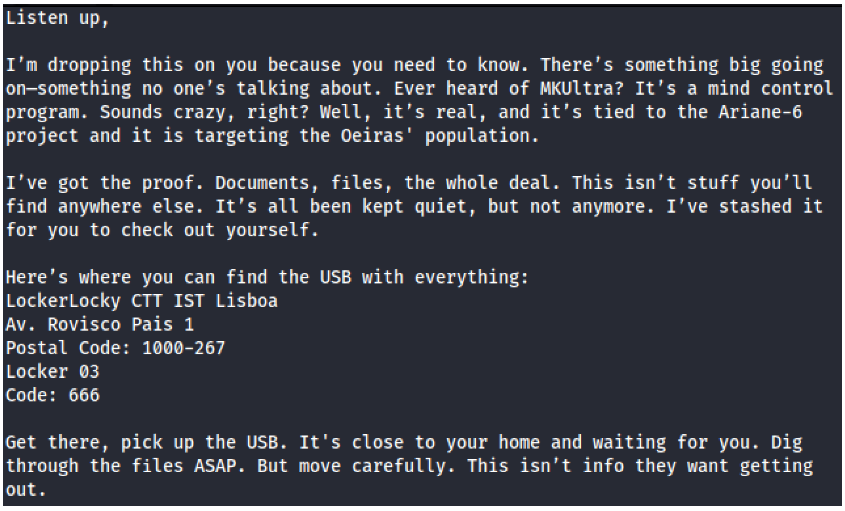
```
backup_1727365201: 06bef2e024c0633a8bde94fbd707c076754b7080f46ca7a9ed1ac645eab660f3
backup_1727365801: 88e1bbabfd59d10bd370b46f1dce954190d577abe06f2e3c38f3bdd7c71b57c9
backup_1727366402: b66ba2f6173988256ac09ac7aea93cd0d17fa8aa29fdec1dc4f66b14e65e13a2
backup_1727367001: 7a62bffa2a9f0ad4eb4e9efab5d9d8c6c1c7f584a830b73e13f6477fcfbd3614
backup_1727367601: f9f014590603d4f3d39484c2a5f5356718d9002756ac995508e7c508ccd0ef0e
backup_1727368201: ea930281417d02b2f3d2e26360ca869cd4f7b96f01fa0b2019b276e3dc49ce25
backup_1727368801: 9bb7fcdb745ab719b7a73c797c5a294760cb8b4d30a551b4fcc5ab71a3f8e3fb
```

A continuous analysis of the johnnyDisk.img allowed us to discover that his browser of choice is *Mozilla Firefox*. As a result, we focused our attention on investigating relevant data associated with this browser. We located a folder within at the following path **/home/snap/firefox/common/.mozilla/firefox/t7pu9ru3.default/** which held a file named "places.sqlite", which is a .sqlite file containing various tables of data, including the "moz_places" table, that contains João's detailed browser history. We extracted this table and saved it as "moz_places.csv" in our findings folder.

The browser history revealed several interesting websites João had visited, shedding light on his online activities:

1. https://www.geeksforgeeks.org/ways-to-permanently-and-securely-delete-files-and-directories-in-linux/ - Searched for a way to delete files and directories without leaving a trace, which means he would have something to hide;
2. https://github.com/PirateMajima/EliteHackingTools - Searched for hacking tools to hide evidences;
3. https://www.google.com/search?client=ubuntu-sn&channel=fs&q=o+pombalino+oeiras – There are evidences that João searched for four restaurants in Oeiras;
4. https://engineering.mit.edu/engage/ask-an-engineer/is-it-possible-to-control-someones-thoughts/ - searches about mind control and if it was possible;
5. https://pt.wikipedia.org/wiki/Ariane_6 - searches about the Ariane-6 satellite;
6. https://download.wetransfer.com/eugv/70d81c81dfb7332abc64867dc548718520240923102432/c26e6b480315e387c7beb45882dfe19bcc1b05dc/hackedcredentials.txt?cf=y&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImRlZmF1bHQifQ.eyJleHAiOjE3MjczNjU2MzMsImlhdCI6MTcyNzM2NTAzMywiZG93bmxvYWRfaWQiOiI3ZGJiYTFiOC0yNmM2LTRiZTYtODU1My05Nzk3M2E2MTNhMGIiLCJzdG9yYWdlX3NlcnZpY2UiOiJzdG9ybSJ9.iZWtbUzoeB8GTekQojpfnLnhDgtW6kdrKGjXFuyxB0o – download link for a file that contain the stolen credentials.

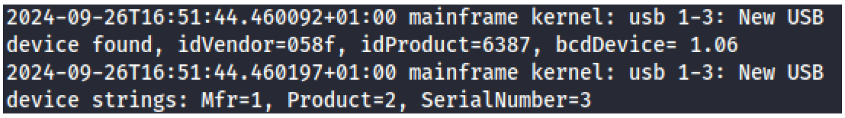
We proceeded to search into his Thunderbird email communications for any important information related to the case. Our search led us to the following directory: **/home/johnnymusk/snap/thunderbird/common/.thunderbird/iw2y9jr6.default/Mail/pop.gmail.com/** where we found a file Inbox. The Inbox file had an email from someone super cool (somebodysupercool@protonmail.com) delivered to João (johnnymuskhax@gmail.com) with the subject "**SUPER IMPORTANT**" from the date Thu, 26 Sep 2024 15:36:08 +0000.



```
Listen up,

I'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.

I'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.

Here's where you can find the USB with everything:
LockerLocky CTT IST Lisboa
Av. Rovisco Pais 1
Postal Code: 1000-267
Locker 03
Code: 666

Get 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.
```

Figure 4 – email received by João

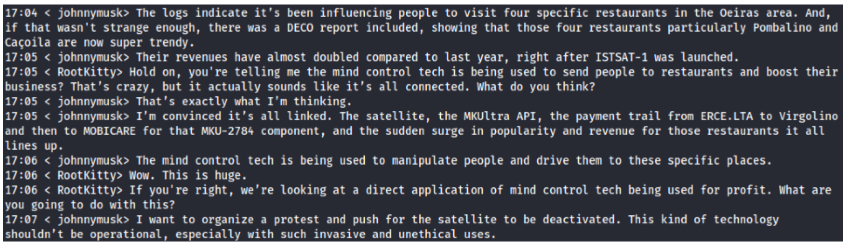
To confirm the existence of this USB drive, we searched the system logs to verify its insertion into João's computer. To find these logs, we executed the command "fls -o 4096 -r johnnyDisk.img > files.txt" and then "strings files.txt | grep -i 'log'". We were able to locate a sys.log file that recorded the insertion of a USB drive, thus confirming its existence.



```
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
```

Figure 5 – system log: insertion of USB

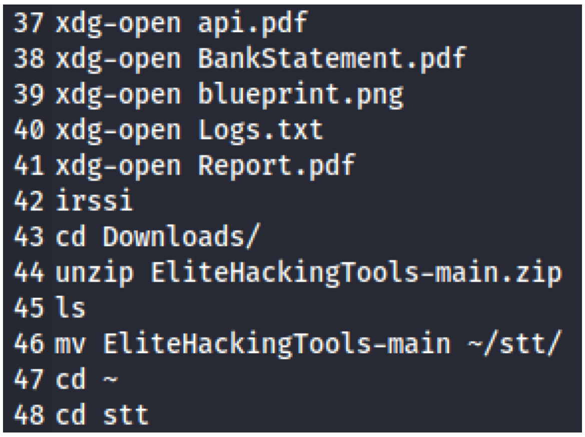
Our group also found a line in the .bash_history file under /home/johnnymusk/ where we got a look at João's last used bash commands. This file mentioned the Irssi command, after researching, we realized that it was used for one-on-one conversations, so there could be traces of João's conversations that are relevant to the case. We successfully located the pertinent data within the directory: **/home/johnnymusk/snap/irssi/common/irclogs/2024/freenode/**. Inside this folder, we unearthed various logs from different IRC channels. The file #thebasement.09-26.log was the only one that contains relevant evidence.



```
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.
```

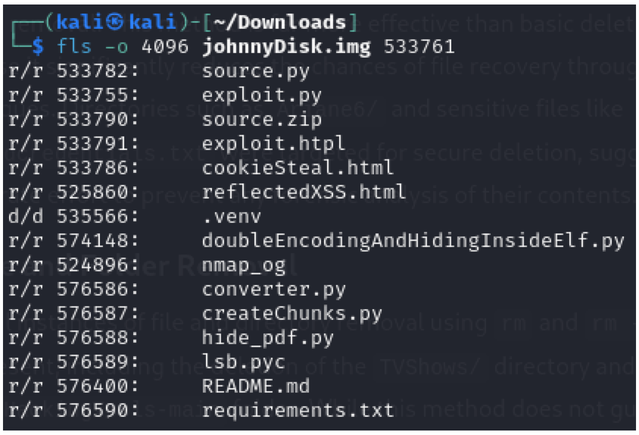
Figure 6 – part of the conversation between João and "RootKitty"

Apart from the files found still in the disk, some more interesting discoveries were made by investigating the .bash_history file. With the information present in this file, we found a suspicious folder labeled **EliteHackingTools-main**. This folder was in /home/johnntmusk/stt/ directory, containing tools (figure 8) that appeared to be used in the creation of the files found on João's sigma account.



```
37 xdg-open api.pdf
38 xdg-open BankStatement.pdf
39 xdg-open blueprint.png
40 xdg-open Logs.txt
41 xdg-open Report.pdf
42 irssi
43 cd Downloads/
44 unzip EliteHackingTools-main.zip
45 ls
46 mv EliteHackingTools-main ~/stt/
47 cd ~
48 cd stt
```

Figure 7 – part of the file .bash_history



```
┌──(kali㉿kali)-[~/Downloads]
└─$ fls -o 4096 johnnyDisk.img 533761
r/r 533782:	source.py
r/r 533755:	exploit.py
r/r 533790:	source.zip
r/r 533791:	exploit.htpl
r/r 533786:	cookieSteal.html
r/r 525860:	reflectedXSS.html
d/d 535566:	.venv
r/r 574148:	doubleEncodingAndHidingInsideElf.py
r/r 524896:	nmap_og
r/r 576586:	converter.py
r/r 576587:	createChunks.py
r/r 576588:	hide_pdf.py
r/r 576589:	lsb.pyc
r/r 576400:	README.md
r/r 576590:	requirements.txt
```

Figure 8 – files of EliteHackingTools-main

Within the johnnyDisk.img, further traces of concealed files were discovered. Specifically, within the /home/johnntmusk/Documents/ directory, we found a pdf file which was a manual of the Ariane6 software.

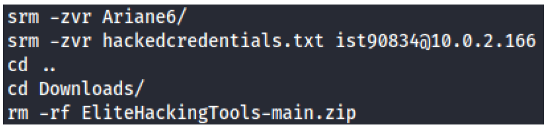
3 Analysis of relevant findings

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?

During our investigation we weren't able to discover the original files that João has on its sigma account. However, we found multiple evidences that those files exists on his computers.

From the .bash_history file, as previously mentioned, it was possible to verify some of the commands that João used in the terminal. This way, we can see that he used the command "srm -zvr Ariane6" to delete the Ariane6 directory and ensure that it could not be recovered in any way. Additionally, through the analysis of the bash file, it is evident that this directory contained the artifacts previously found (BankStatement.pdf, api.pdf, logs.txt, report.pdf, blueprint.png). By using the command "foremost -i johnnyDisk.img -o output_directory" to recover some of the deleted files, it was also possible to find some png files that prove João had possession of the secrets.

Finally, from the zip files presented in the backupDisk.img, we were able to recover all the original files that were provided to us at the start of our investigation. From these, it would be possible to uncover the hidden artifacts once again.



```
srm -zvr Ariane6/
srm -zvr hackedcredentials.txt ist90834@10.0.2.166
cd ..
cd Downloads/
rm -rf EliteHackingTools-main.zip
```

Figure 9 – Use of the command srm

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.

After exploring the files using istat commands and analyzing the logs files, we reached a alleged timeline of events, sustained in the csf2425-lab2-template-timeline.xlsx.

Primarly, João Musk created all scripts necessary for generating passwords for backup zips (found in /home/johnnymusk/backup) between September 14th 2024 and the 23rd, and then saved the seed on Passwords.kdbx on the 25th. He had also already created some hacking scripts on September 23rd at 18:50:43+01:00, probably by downloading EliteHackingTools.

On September 26th 2024, João received an email from Somebody Super Cool informing him to pick up a USB device available on a Locky lock. Meanwhile, João was chatting with Root Kitty, who confessed to stealing IST's credentials and sent them to him, which he encoded immediately. Right after, an USB device was inserted and ejected from João's machine. He proceeded to rejoin the chat to alert Root Kitty that he had been offered a pen drive containing secrets about Ariane6. Some minutes passed, and João created the backup_1727368201.zip using the previously created password generator, that contained all those secrets he found on the flash drive and the IST's credentials he received hidden into files he had on this computer. According to the .bash_history, we can conclude that he run the scripts to encode those files between 17:22:21+01:00 (when he ran hide_pdf.py to encode Bankstatement.pdf) and 17:26:11+01:00 (when he ran the lsb.pyc to encode blueprint.png), following by a secure remove of the rest of the evidences.

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

During our investigation, we uncovered an important finding in the johnnyDisk, specifically within the directory johnnyDisk.img/home/johnnymusk/backups/. We came across a file called obfuscator (previously mentioned), which had been obfuscated, making it unreadable by standard methods.

The intentional obfuscation of the obfuscator file indicates a clear attempt to hide its contents and interfere with the investigation. Such obfuscation methods are frequently used by those aiming to avoid forensic analysis. These techniques are meant to make files and data unreadable, thereby concealing their purpose or meaning. As a result, we have valid reasons to present this file as evidence of anti-forensic activities.

We were able to notice that in the .bash_history file the use of the srm command with options like -zvr indicates attempts to securely delete files by overwriting their contents multiple times before removal. This method is far more effective than basic deletion (rm) because it significantly reduces the chances of file recovery through forensic techniques. Directories such as Ariane6/ and sensitive files like hackedcredentials.txt were targeted for secure deletion, suggesting a deliberate effort to prevent any forensic analysis of their contents.

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

The recent investigation has unveiled significant discovers that shed new light on the unfolding plot of the mind control case that benefact four restaurants in Oeiras and the stolen IST credentials case.

It has been determined that the IST credentials were not stolen by João Musk, opposed to what we initially believed. Instead, they were sent to him by a friend named RootKitty, who was the one who acquired the IST credentials. This revelation calls for an investigation into João's friend as well as the reason behind this act.

Additionally, the investigation has unveiled an email received by João from someone whose identity is unknown (somebodysupercool). This email informed João that a USB drive with information about a mind control program affecting Oeiras had been left for him. From what we could ascertain, João did indeed connect a USB drive to his computer, according to system logs. Therefore, we believe João's relationship with this anonymous person should be investigated, as well as how this person is connected to the case, since they managed to acquire data proving the existence of the case.

4 Appendices

Feel free to attach appendices, e.g., displaying relevant evidence, etc.