INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

# Digital Forensics Report Lab1

| 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 |
|---|---|---|
| bankstatement.pdf | SHA-256 | 4b3d5084429cb211fdfe34c905074a43dbc221e40cc4eb51ff49ef4d11c7bc66 |
| ist_satellite.png | SHA-256 | 66b962895282f0d5b10014d507fc9566e3a4e34aab4871ac13c7c471cebc9da9 |
| deco_article.pdf | SHA-256 | 04c099abe319fe6dd90c420161b64523c0332905332640213eceea3f205500c8 |
| mkultra_doc.pdf | SHA-256 | 75a554633a3d0a98faed4b5b1cc2e52d166fd44ee2804deb808a8f889f6ca3a5 |
| mkultra_commands.txt | String | cf010061102c973fad845091448aa870ea9eb59af471667d4086b4d61982a1bb |
| fenix_credentials.txt | String | bfe6869955ed21e77bb510ea140b00ae2986cd6d08c7bf6f99c8aa2b8d20755a |

## 2 Report of all findings

We discovered 6 secrets, four of which are files, one is a json-like api command string and the other one is a string with IST Fénix user credentials. The methodology used to extract these secrets will be described below in 3.2.

From the initial artifacts found in the forensic copy of João Musk's private account on the IST sigma cluster, with the exception of poster.pdf (which we believe was more used to inform about the act he proposed to do), every single other one was used to uncover the secret artifacts.

Apart from the secrets, when the password for the zip was cracked, we also found the following got.jpg and hd.jpg files which after looking at their metadata we believe are just red herrings. These characters however, may be here to show his ambition in doing something for the greater good, even if that means having to break the law.

Figure 1 - Jon Snow from GOT HBO Show

Figure 2 - Rhaenyra Targaryen from HoD HBO Show

# 3 Analysis of relevant findings

## 3.1 Based on your analysis of the documents, did you find the stolen credentials? If so, describe how you identified them and provide details on the information you discovered.

As we were given to understand, the objects we analyzed were taken directly from the private files of student João Musk. Given that we found the missing credentials among these files, along with hidden artifacts related to a conspiracy theory, we can rightfully assume that Mr. Musk is the culprit of these cyber-crimes and a radicalized individual that clearly had bad intentions in mind regarding these credentials.

## 3.2 Did you uncover any additional concealed artifacts within the provided files? If so, explain how these artifacts were hidden and describe the methodology you used to extract them.

### mkultra_commands.txt

The first file we analyzed was andromeda.png - we started out by doing the basics and using the **strings** and **hexdump** commands on a linux terminal. The magic numbers and the tail of the file didn't reveal anything suspicious but the strings found revealed some metadata that could contain hidden information. Because of this, we used **exiftool** to extract the metadata of this picture and found some interesting headers, namely a description containing the website "http://www.pdf-tools.com" which we did not further utilize and a user comment of a series of dots and spaces that we thought could be some sort of code. By analyzing two other pictures - cartwheel.tiff and lactea.jpg - in the same manner, we found that they too had user comments containing dots and spaces.

One theory that we had, and proved out to be true, was that this apparent gibberish could be masking a binary string, with spaces being 0s and dots being 1s. By using a simple script (**convert_to_binary.py**) that performs this transformation and then using **CyberChef** to convert this binary information into **ASCII** characters, concatenated in the order lactea.jpg - andromeda.png - cartwheel.tiff, we discovered a series of commands given from a program called **MKUltra**, apparently used for geographic mind control.

An example of these commands is the following:

```
<2024-07-17T01:11:53Z>:{
    "endpoint": "/api/MKUltra/idea",
    "parameters": {
        "session_id": "session_lk21e31",
        "target_type": "region",
        "latitude": 38.6973,
        "longitude": -9.30836,
        "radius": 3,
        "idea": "I liked the restaurant 'O Pombalino' so much, I want to go there again this month"
    },
    "response": {
        "status": "started",
        "message": "Idea implanted in the region centered at (38.6973, -9.30836)."
    }
},
```

Figure 3 - Command of MKUltra to implant an idea in a specific location

## ist_satellite.png

Regarding the tagus.png picture, we didn't even need to run the usual commands (**strings** and **hexdump**) on the terminal, as we took one good look at the picture and immediately noticed patterns of banding on the top left corner. Then, we resorted to **StegOnline**'s bit planes feature and quickly discovered that there was information hidden in the 5 **LSBs** of the top left corner, in all RGB channels. Because of the triangle shape of the corner, we thought that maybe the bits were stored diagonally, as only this way would it be possible for them to be extracted continually. After implementing a simple script (**LSB_tagus.py**) for this matter and running it, we found that there was a picture hidden in the tagus.png file, containing the blueprint of the space rocket that transported **ISTSat-1**.

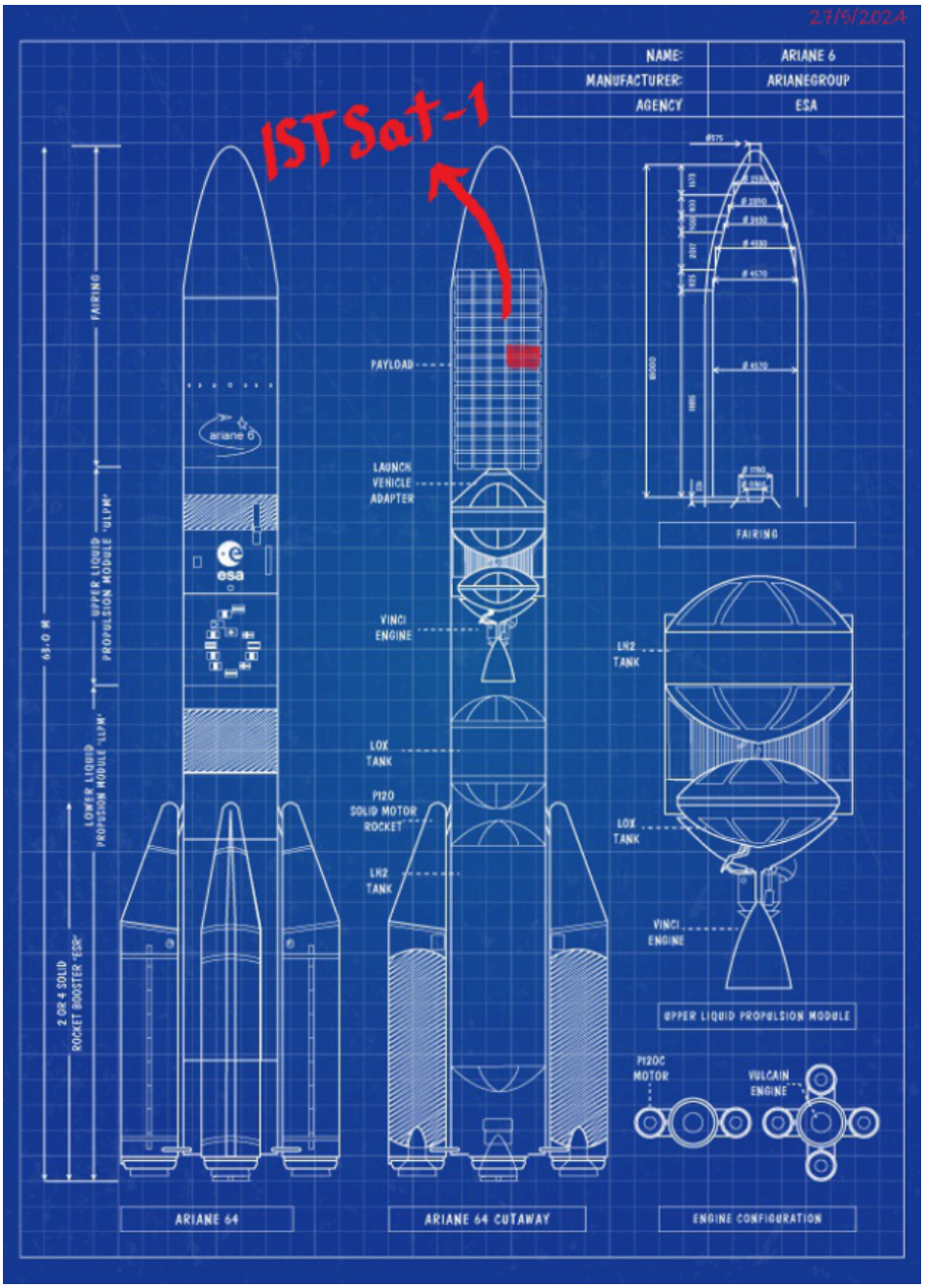


Figure 4 - Blueprint of the Ariane 6 esa Rocket that transported ISTSat-1

## fenix_credentials.txt

The next file we looked at was nmap. As we weren't sure what kind of file it was, we looked at its magic numbers and deduced it was an **ELF file**. We didn't know what to do with this information and had no idea if it was relevant so we still analyzed this file using the **strings** command, which indicated that there was a string of great length hidden in the file. After doing some investigation, we realized that this string was encoded with the **Base64** encoding scheme and quickly came up with a script **(nmap.py)** that decoded this information. The resulting string looked to be in **Hex**, so we resorted to an online tool that converts it to ASCII (https://www.binaryhexconverter.com/). To our surprise, it was there that Mr. Musk hid the Fenix credentials that he stole! For illustration purposes, we present to some of the credentials:

```
Username: ist572024, Password: 5@!k=)|Y>;Username: ist523045, Password: }
p]'a66W,U%t[N>;Username: ist537267, Password: >t{TZ05oHhr;Username:
ist532722, Password: 6}y^?njBa~;Username: ist573865, Password: Dv!
uL~]J8z;Username: ist593189, Password: q5Y4M<e*;Username: ist515624,
Password: .AoQK{1Ux2?;Username: ist592276, Password: Vck3S2.\;Username:
ist564447, Password: 53!m@!nWO;Username: ist599978, Password:
(^GA_sI3s2Dp0B;Username: ist523968, Password: v(6K{Fy[*<;Username: ist599702,
Password: 8~]rZEroK6}hh~H;Username: ist534031, Password: 4h"8"d^yM;Username:
ist560929, Password: Hk3`XzY!Ml;Username: ist569339, Password: >eJ$|4Ukcr,s
{;Username: ist557485, Password: y8f#C%k&kM0D5-;Username: ist537839,
Password: 9H{*/sZF%4N4"Wi;Username: ist517172, Password: 1&aPq28Q@;Username:
```

Figure 5 - Credentials of IST Fenix users that were stolen

## bankstatement.pdf

Regarding the file best_intro.wav, we started by using the same old commands (**strings** and **hexdump**), which showed some metadata that we assumed belonged to a pdf file called bankstatement.pdf. This way, we immediately thought that all the data pertaining to this pdf was hidden in this audio file (also with the help of command **binwalk**) and, through the use of the command **foremost**, we were able to retrieve that pdf in full. This bank statement is of someone called Virgolino Gonçalves, perhaps an alias used to support the anti-satellite cause while maintaining anonymity. An example of a section of the pdf follows:

FIRST CITIZENS BANK

Praça D. João I, 28
4000-295 Porto
firstcitizensbank.pt

**STATEMENT OF ACCOUNT**

Account Number: 198-719-871-987
Statement Date: 05/03/2024
Period Covered: 01/01/2024 to 31/01/2024

Page 1 of 1

Virgolino Gonçalves
R. Cidade de Guimarães
2870-457 Montijo

| | |
|---|---|
| Opening Balance: | 22.80 |
| Total Credit Amount: | 33,040.00 |
| Total Debit Amount: | 32,214.65 |
| Closing Balance: | 848.15 |
| Account Type: | Current Account |
| Number of Transactions: | 28 |

Transactions

| Date | Description | Credit | Debit | Balance |
|---|---|---|---|---|
| 01/01/2024 | Subscription - Netflix | | 11.99 | 10.81 |
| 01/01/2024 | Subscription - Spotify | | 8.99 | 1.82 |
| 01/01/2024 | Rent | | 500.00 | -498.18 |
| 01/01/2024 | Payment - Vodafone | | 12.99 | -511.17 |
| 05/01/2024 | WireTransfer from ERCE.LTA | 33,000.00 | | 32,488.83 |
| 06/01/2024 | MBWay Payment - Continente | | 95.67 | 32,393.16 |
| 06/01/2024 | Steam Purchase | | 59.99 | 32,333.17 |
| 06/01/2024 | Subscription - Tinder Gold | | 14.99 | 32,318.18 |
| 08/01/2024 | Payment - Restaurant "Fifty Seconds" | | 257.06 | 32,061.12 |
| 09/01/2024 | MBWay from Guilherme Cruz | 20.00 | | 32,081.12 |
| 10/01/2024 | Payment - MOBICARE (MKU-2784) | | 28,000.00 | 4,081.12 |
| 12/01/2024 | WireTransfer to Agência Abreu | | 2,500.00 | 1,581.12 |
| 12/01/2024 | taylorswift.com | | 19.99 | 1,561.13 |
| 12/01/2024 | MBWay to Magui Corceiro | | 150.00 | 1,411.13 |

Figure 6 - Statement of Account from Virgolino Gonçalves

## mkultra_doc.pdf

Concerning one particular file, thrones.pdf, in which there is a big text written in the fictional language High Valyrian from the Game of Thrones HBO Series, we weren't able to find anything suspicious. Because we also hadn't been able to crack the password for myzip.zip, we suspected that maybe the password could be one of the many Valyrian words present in this file. This way, we created a wordlist with all these words using a simple script to separate each word into a different line (**wordlist.py**) and attempted to crack the password using **john the ripper** on a linux terminal. Luckily, this attempt was successful and the right password was the word "zmaistangeptotlargelynaejotseda". Inside the zip folder, there were 4 files: two Game of Thrones related photos called got.jpg (with a Jon Snow picture) and hd.jpg (with a picture of Rhaenyra Targaryen), a picture called wallpaper.png and a file called blank, of apparently no format.

From a simple analysis of blank's magic numbers with **hexdump**, it was obvious that they closely resembled PDF's magic numbers and so we opened the file on an Hex editor and fixed those magic numbers to 25 50 44 46 2D (PDF).

After this, we were able to open the file with no problems, as it was in fact a pdf file documenting a mind control API of MKUltra, with the following table of contents:

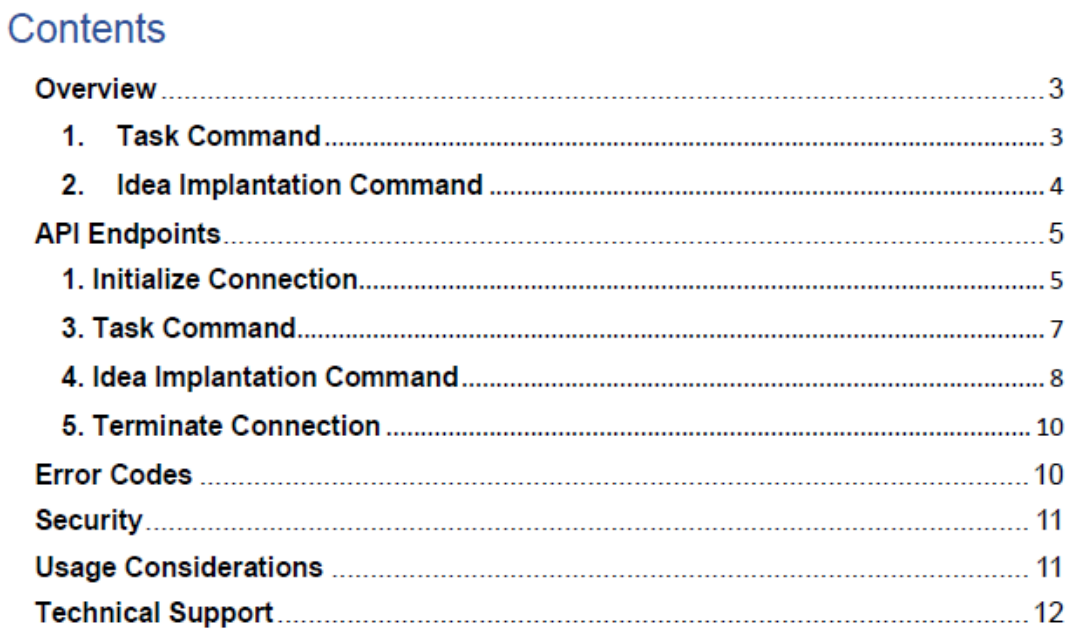


Figure 7 - MKUltra Mind Control Component API Documentation Contents

## deco_article.pdf

Besides the blank file, the image file called wallpaper.png also caught our attention, as it appeared to have very noticeable banding throughout the whole picture. This led us to upload it to **StegOnline** and realize that the banding wasn't actually indicative of something hidden. However, looking at the bit planes, there appeared to be some tampering with the picture on the top, specifically with the 3 LSBs. After running a script (**LSB_wallpaper.py**) that extracts those 3 LSBs from all RGB channels from left to right, we were able to discover a hidden pdf containing a DECO article titled "Oeiras restaurants stunning growth". The header of this article is displayed below:


Figure 8 - DECO article for Oeiras restaurants stunning growth

### 3.3 With a focus on the additional concealed secrets you recovered, analyze their content and relationships, and propose a possible interpretation of their meaning. Formulate a hypothesis regarding their significance and support it with the content of the recovered secrets. Additionally, prepare a timeline of the events as indicated by the recovered secrets.

Based on the additional secrets we recovered and after careful analysis of their content and relationships, we've reached a possible conclusion. Firstly, Musk bought the MKUltra mind control device on 10/01/2024 through a bank account under his possible alias Virgolino Gonçalves, according to the bank statement from January. Then, after it arrived in July (it probably took 6 months), he started using it on a small scale by making people visit restaurants in Oeiras. This was probably to test the device and/or to gain some revenue by collaborating with the owner(s) of those restaurants, this is supported by the logs and the news article indicating the growth in revenue of four restaurants. Now in September, the news article about the restaurants' growth is published and Musk stole the Fenix IST credentials from a large group of users, some of which could be teachers or even high-ranking professors with the authority to make critical decisions and override operations within Fenix. This is supported by the metadata of the nmap file. After collecting all this information and knowing the power of the MKUltra technology that he bought, he possibly aims for the control of the IST satellite that was deployed earlier this year, since the poster we found shows that he had interest in its uses.

We hypothesize that his main interest is to use the credentials of high-ranking professors so that he can gain control and overrule the Fenix DSI system, and by doing so gain access to the satellite to reach the end goal of fully utilizing the MKUltra's powers with a higher computational power and a greater area of effect.

### 3.4 Based on your findings, what recommendations would you make for the next steps in the investigation? Advise Mr. Ricardo Prado on the best course of action moving forward.

- Due to the evidence we collected throughout our findings, the next steps should be to analyze the MKUltra Mind Control Component API (**mkultra_doc.pdf**) and understand its power and usages, we would recommend contacting the provider as cited in the end of the **mkultra_doc.pdf** file and studying the logs discovered from the concatenation of the user comments in **lactea.jpg + andromeda.png + cartwheel.tiff** which are located on the file **mkultra_commands.txt**.
- By investigating the **poster.pdf** we can see that there were bad intentions regarding the uses of the IST satellite in Taguspark so we need to know if the people who attended were under the effect of the MKUltra or if they were Musk's accomplices.
- Regarding the Deco restaurant growth file (**deco_article.pdf**) the two listed individuals should be contacted and investigated, "Susana Santos" and "Ana Rita Costa" in order to better understand their sources regarding the contents of the news article. We also believe that contacting and arranging a meeting with the owners of the referred restaurants (A Tendinha, O Pombalino, A Caçoila, and O Transmontano) is necessary in order to investigate the connection between these, João Musk and the MKUltra.

- The **bankstatement.pdf** should be thoroughly analyzed, contacting the First Citizens Bank and accessing the firstcitizensbank.pt website, and examining the suspicious transactions made by Virgolino Gonçalves with other individuals, specially the 33,000€ he received. His connection to João Musk (perhaps Virgolino is just an alias of Musk to maintain anonymity, or vice-versa) should be confirmed.
- We also would advise Mr. Ricardo Prado to search if the IST credentials we found are from high-ranking professors with the authority to make critical decisions and override operations within Fenix and possibly to be able to take action in the process related to the control of the satellite through Fenix. All the teachers should be contacted as well as the upper management of the IST. The European Space Agency (ESA) should also be consulted regarding this situation.
- We believe that every person mentioned in this cybercriminal activity should be contacted and interrogated about their connections and affiliations with Musk, the restaurants, MKUltra and the satellite. We need to understand Musk's intentions with this whole plot, protect the satellite and prioritize IST and its members' security.

## 4 Appendices


This is the image present in the **poster.pdf** file that was with the rest of Musk's files. While it didn't have any secrets concealed inside, we speculate that it may be related to the entire plot.