INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab1

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
bankstatement.pdf	SHA-256	6ac9c4d35d790a3a2d3f3b3b1866a2f5d0e40c08a839799c39643c238e705829
deco.pdf	SHA-256	04c099abe319fe6dd90c420161b64523c0332905332640213eceea3f205500c8
mku-documentation.pdf	SHA-256	55bd8016769dc421ba0c87e1c657477b00893e1194fc447cd20147b5438a39f5
IST credentials	String	1e3ae9f210ec59d69c9ff467488cdc5605bd54ce3bd8dea87a61f2799fe56c6c
MKU	String	9e34f9c2fa40ac0be0a8cb773ac4bb3711fc792994fe7a0a5f5d6c8c886e2736
ariane6.png	SHA-256	e675e7cc9bb52fdb8eb43834395371e7dee57ab3726ff0a03099cd279c81dcaf

2 Report of all findings

2.1 Overview

Bankstatement.pdf

- binwalk best-intro.wav
- foremost -t pdf best-intro.wav

Deco.pdf

- zsteg -a wallpaper.png
- zsteg wallpaper.png -E b3,rgb,lsb,xy > deco.pdf

MKU-2784.pdf

- hexdump -C blank | head

add .pdf to the end of the file

IST credentials

- strings nmap

CyberChef "from Base64" + "from Hex"

MKU-restaurants

- exiftool andromeda.png
- exiftool cartwheel.tiff
- exiftool lactea.jpg

copied each User Comment section and run the script decoder_pontos.py

Ariane6.png

- stegsolve tagus.png

saw there was information on the top left side encoded diagonally

ran script lsb_decoder.py

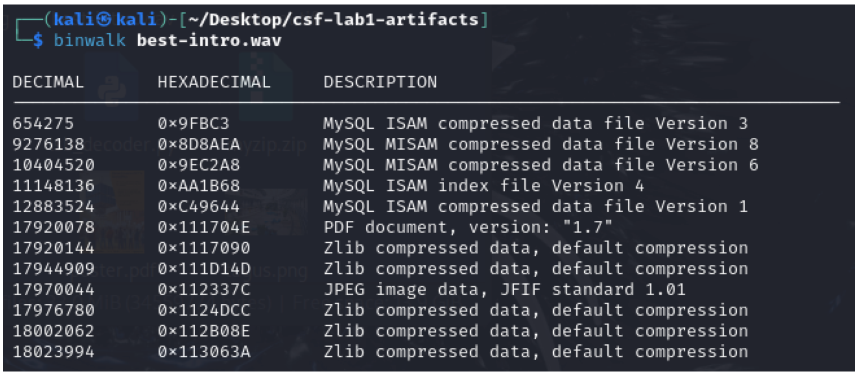
2.2 Detailed process

We have discovered six artifacts, three of these are files, one is an IST credentials and the other two are commands.

The first artifact we found was a PDF file of a bank statement of a person called Virgolino Gonçalves, which we discovered by analyzing the file called "best-intro.wav". We started of by verifying the file type with the command "file" and metadata with the command "exiftool", all of these commands seemed normal. Then we used the command "xxd best-audio.wav | head" to verify the magic numbers of the file and these matched with the one of a wav extension, according to "List of file signatures" Wikipedia page. We then investigated potential hidden content:

- binwalk best-intro.wav

The output of this command revealed that there was a PDF embedded within the WAV file (fig.1). Using the "foremost" tool we were able to extract the PDF from the file.



```
┌──(kali㉿kali)-[~/Desktop/csf-lab1-artifacts]
└─$ binwalk best-intro.wav

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
654275        0x9FBC3         MySQL ISAM compressed data file Version 3
9276138       0x8D8AEA        MySQL MISAM compressed data file Version 8
10404520      0x9EC2A8        MySQL MISAM compressed data file Version 6
11148136      0xAA1B68        MySQL ISAM index file Version 4
12883524      0xC49644        MySQL ISAM compressed data file Version 1
17920078      0x111704E       PDF document, version: "1.7"
17920144      0x1117090       Zlib compressed data, default compression
17944909      0x111D14D       Zlib compressed data, default compression
17970044      0x112337C       JPEG image data, JFIF standard 1.01
17976780      0x1124DCC       Zlib compressed data, default compression
18002062      0x112B08E       Zlib compressed data, default compression
18023994      0x113063A       Zlib compressed data, default compression
```

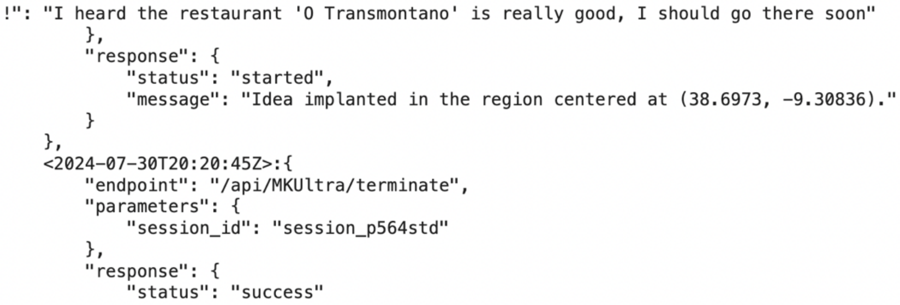
Figure 1 – binwalk tool employed on finding out best-intro.wav's hidden files

The second artifact we found were some IST credentials, which were hidden within the contents of the nmap file. We followed the same strategy mention before, however none of those tools showed anything out of normal. We decided to search for any relevant strings that might have been hidden within the contents of the file. To do this we executed the following command:

- strings nmap

The resulting output was a string ending with the character "=", that lead us to think about the fact of this output being encoded in base64. To verify our theory, we decided to search for an online decoder of base64, this produced a hexadecimal result that when converted to text made it possible to identify a list of several IST credentials.

The third artifact we discovered were some commands, these were found on the metadata of the files andromeda.png, lacteal.png and cartwheel.tiff. After checking the metadata of these files, we found a suspicious content in the "User Comment" field. This was a set of blank spaces and dots, which we thought could be Morse Code. After decoding the string, it didn't result in anything useful so we considered replacing the spaces with zeros and the dots with ones. We used a script that did this and then converted each byte into an ASCII character, as well as testing all possible combinations of the three messages (fig. 2).



```
!": "I heard the restaurant 'O Transmontano' is really good, I should go there soon"
        },
        "response": {
            "status": "started",
            "message": "Idea implanted in the region centered at (38.6973, -9.30836)."
        }
    },
    <2024-07-30T20:20:45Z>:{
        "endpoint": "/api/MKUltra/terminate",
        "parameters": {
            "session_id": "session_p564std"
        },
        "response": {
            "status": "success"
```

Figure 2 – part of the result of applying the script

To identify the fourth artifact, an image of Ariane6's blueprint, we analyzed the information hidden in the image tagus.png. We proceeded to look at this file with some steganography analyzing tools, which allowed us to find something peculiar. While looking through the different bit planes of the image, we came across a noise section that seemed to cover the pixels of the png on a diagonal on the left side, meaning that some information could be hidden in the image's LSBs (Least Significant Bits).

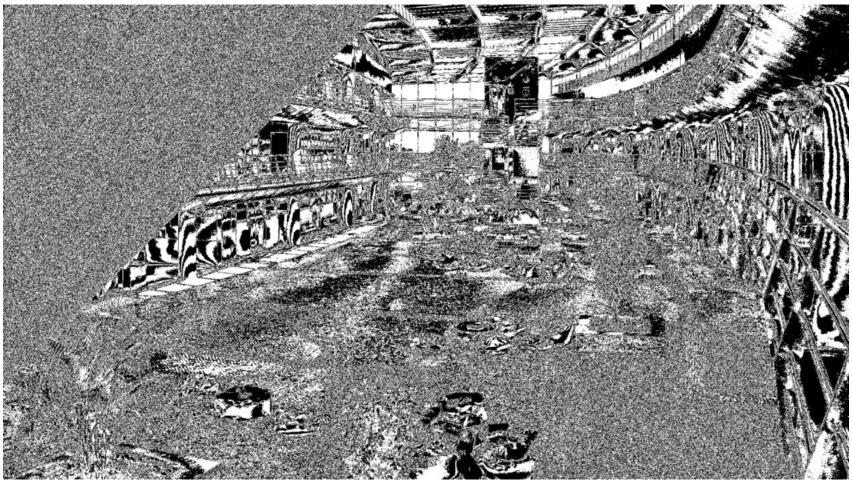


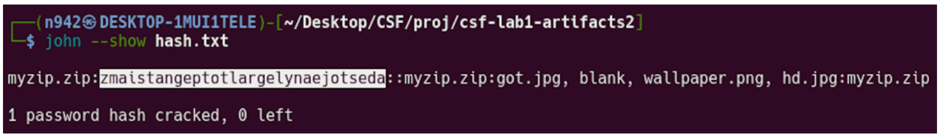
Figure 3 – tagus.png altered to showcase the noise section

To extract the LSBs from this noise section, we proceeded to develop a custom python script (lsb_decoder.py). After running it, we got the png file with the blueprint of Ariane6.

For the last two artifacts, we suspected they would be on the ZIP file. As expected, we started the analysis of the myzip.zip file by attempting to open it and extract its contents, however, while trying to do so, we immediately discovered that it was protected with a password. On our first effort to find the password of the zip file we though about launching a bruteforce attack. With that goal in mind, we proceeded to extract the hash of the file and then launch the first attack with rockyou dictionary:

- zip2john myzip.zip > hash.txt
- john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Since none of the words in the rockyou dictionary worked, we decided to create our own dictionary based on the thrones.pdf that was given to us. This pdf had a lot of different words that could possibly be the password for the ZIP file. To prepare the text file to use as a password dictionary, we extracted every word within it by splitting the text based on whitespace characters. With the password dictionary ready, a new attack was conducted on the ZIP archive. The tool john was employed to automate the attack on the ZIP archive, and the correct password was successfully identified as **zmaistangeptotlargelynaejotseda**.



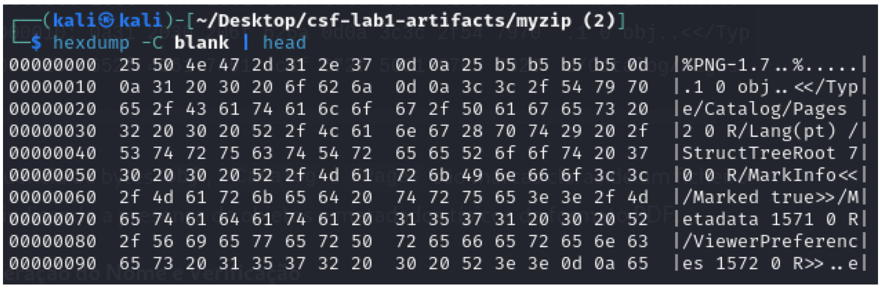
```
┌──(n942㉿DESKTOP-1MUI1TELE)-[~/Desktop/CSF/proj/csf-lab1-artifacts2]
└─$ john --show hash.txt

myzip.zip:zmaistangeptotlargelynaejotseda::myzip.zip:got.jpg, blank, wallpaper.png, hd.jpg:myzip.zip

1 password hash cracked, 0 left
```

Figure 4 – output of the dictionary attack on myzip

Following the successful extraction of the ZIP's contents, a file named blank was found. However, we continuously failed to open this file, as it appeared to be corrupted and inaccessible. To investigate the nature of this corruption within the file, a hexdump analysis was performed using the command:

- hexdump -C blank | head

During the hexdump analysis, an unexpected discovery was made. The hexdump output revealed that the file began with a non-standard PNG header (%PNG-1.7), which is not a valid PNG format. Further inspections of the hexdump showed structures commonly associated with PDF files, such as /Catalog, /Pages, and obj, indicating that the file was actually a PDF disguised as a PNG through header manipulation. Finally, we simply added the ".pdf" extension to the file and attempted to open it.



```
┌──(kali㉿kali)-[~/Desktop/csf-lab1-artifacts/myzip (2)]
└─$ hexdump -C blank | head
00000000  25 50 4e 47 2d 31 2e 37  0d 0a 25 b5 b5 b5 b5 0d  |%PNG-1.7..%.....|
00000010  0a 31 20 30 20 6f 62 6a  0d 0a 3c 3c 2f 54 79 70  |.1 0 obj..<</Typ|
00000020  65 2f 43 61 74 61 6c 6f  67 2f 50 61 67 65 73 20  |e/Catalog/Pages |
00000030  32 20 30 20 52 2f 4c 61  6e 67 28 70 74 29 20 2f  |2 0 R/Lang(pt) /|
00000040  53 74 72 75 63 74 54 72  65 65 52 6f 6f 74 20 37  |StructTreeRoot 7|
00000050  30 20 30 20 52 2f 4d 61  72 6b 49 6e 66 6f 3c 3c  |0 0 R/MarkInfo<<|
00000060  2f 4d 61 72 6b 65 64 20  74 72 75 65 3e 3e 2f 4d  |/Marked true>>/M|
00000070  65 74 61 64 61 74 61 20  31 35 37 31 20 30 20 52  |etadata 1571 0 R|
00000080  2f 56 69 65 77 65 72 50  72 65 66 65 72 65 6e 63  |/ViewerPreferenc|
00000090  65 73 20 31 35 37 32 20  30 20 52 3e 3e 0d 0a 65  |es 1572 0 R>>..e|
```

Figure 5 – blank head hexdump containing its magic numbers

The last artifact we discovered was a PDF file of a DECO report about the economic growth of four restaurants in Oeiras. Inside the ZIP file we had previously opened, was a PNG file named wallpaper.png. By using a steganography tool, we uncovered a hidden PDF file that we were able to extract using the following command:

```
zsteg wallpaper.png -E b3,rgb,lsb,xy > deco.pdf
```

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.

Based on the documents given, we were able to analyse and discover the IST credentials that were stolen. We identified them because the string has an IST username and a password. The credentials were hidden on the nmap file and they were encoded in base64.

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.

Within the provided files, we were not only able to find the IST credentials but also 5 other artifacts. To extract them, we started by trying to unzip the files from myzip.zip, and discovered the password by the methods described in the previous section. After gathering all of these files, we started by checking their file types with the file command, which did not raise any suspicion. Then, we compared magic numbers (hexdump command) to their extension: that is how we found out the file blank was the Deco.pdf artifact. We explored the metadata of the remaining files using the exiftool command, and our attention was drawn to a strange sequence of dots and blank spaces in the User Comment field of andromeda.png, lacteal.png, and cartwheel.tiff. This sequences turned out to be a list of MKU-restaurants, after replacing the spaces with zeros and the dots with ones and then converting each byte into an ASCII character, through a script. Another command we used on every file was strings -n 8 <filename>. We chose the size 8 because we considered it to be enough to reduce the appearance of random strings. For files other than nmap (where we found the IST credentials), there were no artifacts. Lastly, we used the command binwalk to search for files embedded into the given ones. We found a pdf in best-intro.wav, that was retrieved with command foremost -t pdf, this pdf was the bankstatements.pdf. We ended up opening the images to search for clues. Two files caught our eyes: the wallpaper.png due to blurred edges and indistinct lines and the colors on the top left side of the tagus.png. We used the zsteg command to extract the embedded pdf on wallpaper.png, latter named Deco.pdf. Due to the complexity of the embedding on tagus.png, we created a script to extract the last significant bits of that image's noise, that found a png file with the blueprint of Ariane6.

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 remaining uncovered artifacts it was possible to discover a bank statement belonging to Mr. Virgolino Gonçalves, documentation for a component that allows mind control (MKU-2784), a set of instructions for this same component, a rocket blueprint, and a report on the financial growth of four restaurants in Oeiras.

We believe that all these artifacts we discovered are connected, starting with the bank statement, where it is possible to notice a payment of €28,000. This payment includes a description referencing the mind control component. Additionally, it is clear that the instructions found refer to the four restaurants whose economic growth has been remarkable in recent months, according to the report found. The rocket blueprint references the satellite from Instituto Superior Técnico, which was recently launched and is also mentioned in one of the provided files, indicating some concern around it.

From our point of view, this could be a case where someone or some institution is using a tool that allows them to control how people act and think for their own benefit. In this specific case, it seems to be aimed at boosting the profits of the four restaurants mentioned in the report ("O Pombalino," "A Tendinha," "A Caçoila," and "O Transmontano").

Our hypothesis is supported by a series of connections between these artifacts and their dates:

- Payment for the mind control component (MKU-2784) – 10/01/2024.
- Payment made to an influencer who later visited the restaurants in Oeiras – 12/01/2024.
- The Ariane 6 rocket plan, which carries Técnico's satellite and would allow easier access to people's minds. It would also be easier for someone within Técnico to include this component in the satellite – 27/05/2024.
- Arian 6 launch – 09/07/2024.
- The start of the instructions found, suggesting that people visit and recommend the four restaurants in Oeiras – 16/07/2024.
- Increased revenue from two restaurants, to which the initial instructions were dedicated – 16/07/2024.
- After the recommendation instructions were spread, a report is released confirming the financial growth of the same restaurants – 05/09/2024.
- Concerns arise regarding Técnico's new satellite, and a protest is scheduled demanding its deactivation, since controlling people's minds can easily spread wrong ideas – 14/09/2024.

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.

Based on our findings, we recommend the following steps to continue the investigation:

- Investigate individuals that might be associated with the data, specially Virgolino Gonçalves, for possible involvement in illicit activities.

- Reset the passwords that were stolen immediately.
- Upon obtaining further confirmation of Virgolino's or another person's involvement, it is advisable to request a warrant to search their residence for additional evidence.
- Coordinate with the authorities to initiate legal proceedings if criminal activity is confirmed.
- Identify the individuals behind the use of the MKUltra Mind Control API.
- Request access to pertinent network traffic and system logs within the MKUltra Mind Control API's servers.
- Investigate the eventual illegitimate financial activities of the mentioned restaurants.
- Ensure all recovered evidence, including the original files and extracted artifacts, are documented and stored securely following proper chain of custody procedures.
- Inform the university administration about the findings, including the compromised credentials.
- Request access to security footage and seek witness accounts to corroborate suspicions of unauthorized access or theft.

4 Appendices

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