INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2023-2024 – 1st Period

Digital Forensics Report

Authors - G037

ist199230 - Guilherme Almeida Patrão

ist199314 - Raquel Filipa Marques Cardoso

ist199343 - Valentim Costa Santos

1 Based on your analysis of the documents, can you deduce the likely identity of the owner of this pen drive? Justify your answer with relevant findings.

The initial step of this investigation entailed creating forensic images of all files within the pen drive, using the `dd if=./example_file of=./dd/example_file bs=4M status=progress` command for all files, and afterwards calculating their fingerprints with the **`sha256sum`** command. By doing this, we confirmed our files had not been manipulated and were the same as the ones Mr. Matos' had.

```
┌──(raquel㉿NEPTUNO)-[~/Documents/csf2324-lab1-artifacts]
└─$ ls dd
BdC_on_the_beat  logo.png     Rialva.png  sporting_anthem  waste-of-time
Cool_stuff.mp4   report.docx  Social.png  Tagus.png
```

Figure 1 - Directory with the forensic images of every file

```
┌──(raquel㉿NEPTUNO)-[~/Documents/csf2324-lab1-artifacts/dd]
└─$ sha256sum *
d8028eb28c6aa2b94607df770515368e0d2c0488279328599ca51fe1bdbced6c  BdC_on_the_beat
240cb4494b4a4e0e367f67afa80bd7287dda09755e3eaa66af1994a03ea3e316  Cool_stuff.mp4
d25a8d99bccc3e176b2852acb72b92f3d40c8f7e4b6501d2145101929de637fb  logo.png
30bb4ca7580bd331d3334bf4bba6b9e45165d1f51960eb7ee345a631aee90f70  report.docx
8873a7055c9838ef8847424306f6997c3eb0d0aa6373acd65206ede85bfe8ec8  Rialva.png
50011896abe7f70e9e8b00b4d3ccc25acf6a2272f11b343b2758be01355d21f4  Social.png
7d4e8b5d0d8d127fdf31f097a208a511847872884c2e11db662279292a0969cd  sporting_anthem
ec54db5e6df2093573548d685ce72f3c4ffa548032e6a26ac2cc3f544bd3c283  Tagus.png
941b69160a7c4d6e3483c54c43a9a8fd52ff12b65af77b770d879cace846bce4  waste-of-time
```

Figure 2 – SHA-256 fingerprint values for every file

Subsequently, upon inspecting all the files, it became apparent that three of them - **`Rialva.png`**, **`Social.png`**, and **`Tagus.png`** - had undergone manipulation using a photo editing program, evidenced by the presence of handwritten content on them for what seemed like "food review" content. Prompted by this discovery, we proceeded to employ the **`exiftool`** tool in order to determine the owner of the pen drive:

```
└─$ exiftool *.png | grep "Author"
Author                          : Cesar Silva Ferro
Author                          : Cesar Silva Ferro
Author                          : Cesar Silva Ferro
```

Figure 3 - Finding out the pen drive owner

Every **`.png`** file that had the "Author" field indicated "Cesar Silva Ferro" as the value, leading us to deduce that César Silva Ferro is the probable owner of the pen drive.

This assertion is corroborated by the contents of the file **`waste-of-time`**, which was also found in the pen drive and encompasses the grades for the 2nd exam of the curricular unit Forensics Cyber Security in its 2022/2023 execution. This file prominently displays César's name along with a grade of 3.1/20, indicating that he failed the exam and therefore why the grading details was named a waste of time by him.

CSF 2022/23 - 2nd Exam

Nome	Total
	0,1154
	6.69
Ana Sofia Oliveira Almeida	10,2
André Luís Gonçalves Martins	
Beatriz Maria Santos Ferreira	12,7
César Silva Ferro	3,1
Hugo Manuel Silva Pereira	
Inês Carolina Alves Pinto	9,7
João Pedro Silva Santos	10,2
Pedro Miguel Costa Fernandes	
Rita Sofia Santos Fernandes	
Tiago José Rodrigues Oliveira	11,9

Figure 4 - CSF 2022/23 2nd exam grading details

In the context of this lab assignment César Silva Ferro can be abbreviated as CSF, which is also known as Ciber-Segurança Forense - the portuguese nomenclature for this curricular unit. However, it's of extreme importance to note that this correspondence in initials should be regarded merely as coincidental and it's not intended to be held as legitimate evidence in this investigation.

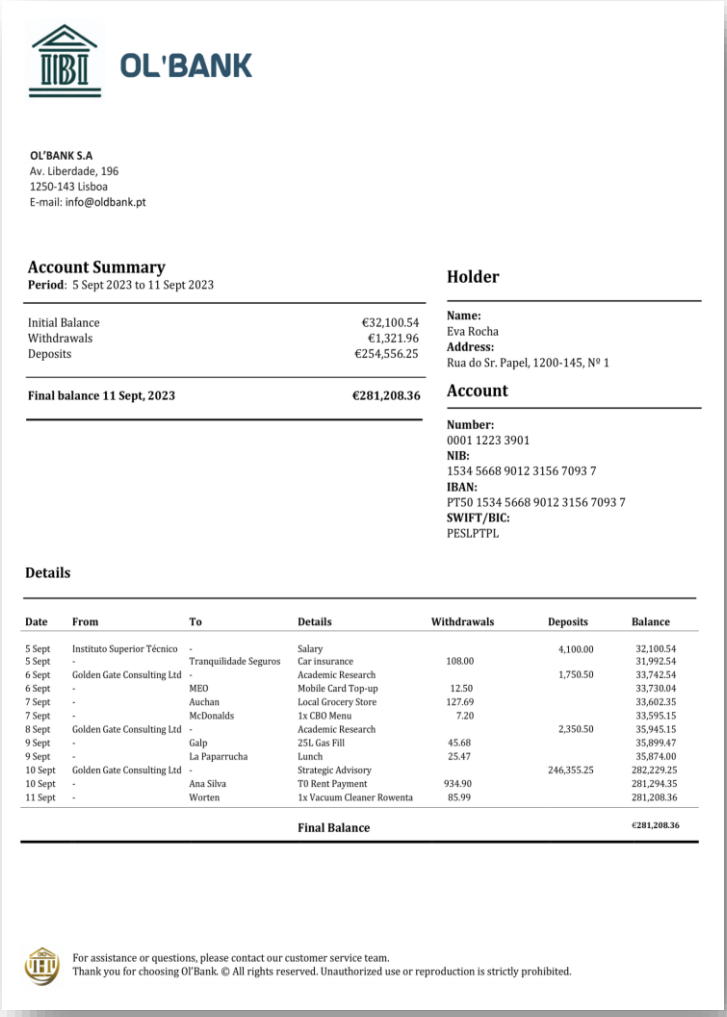
2 Were there any concealed artifacts within the provided files? If so, detail how these artifacts were embedded and your methodology to extract them.

Following the identification of the pen drive owner, our investigation transitioned to detecting the six concealed artifacts within the provided files.

Secret 1: Bank Statement

Our investigation commenced with a comprehensive examination of the **`waste-of-time`** file. Subsequently, we utilized the file carving tool **`foremost`** to analyze its contents, successfully extracting a concealed **`.png`** file, and storing it in our findings folder **`(bank_statement.png - sha256: 86ff52a0cf5731064a4c071c8c8a49c2f19b62bf4d2a5a471d68afe61547778d)`**

The extracted **`.png`** file revealed itself as a bank statement from *"OL'BANK"* covering the period from 5th September 2023 to 11th September 2023, linked to a portuguese account registered under the name of "Eva Rocha'' and the corresponding IBAN PT50 1534 5668 9012 3156 7093 7. Noteworthy transactions included a salary deposit from Instituto Superior Técnico and payments from Golden Gate Consulting, including a deposit of 246,355.25€ designated for "Strategic Advisory", significantly surpassing the average remuneration for similar roles in the Portuguese economy.



OL'BANK

OL'BANK S.A
Av. Liberdade, 196
1250-143 Lisboa
E-mail: info@oldbank.pt

Account Summary
Period: 5 Sept 2023 to 11 Sept 2023

Initial Balance	€32,100.54
Withdrawals	€1,321.96
Deposits	€254,556.25
Final balance 11 Sept, 2023	**€281,208.36**

Holder

Name:
Eva Rocha
Address:
Rua do Sr. Papel, 1200-145, Nº 1

Account

Number:
0001 1223 3901
NIB:
1534 5668 9012 3156 7093 7
IBAN:
PT50 1534 5668 9012 3156 7093 7
SWIFT/BIC:
PESLPTPL

Details

Date	From	To	Details	Withdrawals	Deposits	Balance
5 Sept	Instituto Superior Técnico	-	Salary		4,100.00	32,100.54
5 Sept	-	Tranquilidade Seguros	Car insurance	108.00		31,992.54
6 Sept	Golden Gate Consulting Ltd	-	Academic Research		1,750.50	33,742.54
6 Sept	-	MEO	Mobile Card Top-up	12.50		33,730.04
7 Sept	-	Auchan	Local Grocery Store	127.69		33,602.35
7 Sept	-	McDonalds	1x CBO Menu	7.20		33,595.15
8 Sept	Golden Gate Consulting Ltd	-	Academic Research		2,350.50	35,945.15
9 Sept	-	Galp	25L Gas Fill	45.68		35,899.47
9 Sept	-	La Paparrucha	Lunch	25.47		35,874.00
10 Sept	Golden Gate Consulting Ltd	-	Strategic Advisory		246,355.25	282,229.25
10 Sept	-	Ana Silva	T0 Rent Payment	934.90		281,294.35
11 Sept	-	Worten	1x Vacuum Cleaner Rowenta	85.99		281,208.36
			Final Balance			€281,208.36

For assistance or questions, please contact our customer service team.
Thank you for choosing Ol'Bank. © All rights reserved. Unauthorized use or reproduction is strictly prohibited.

Figure 5 - The bank statement that was found

Secret 2: Seven Number Sequence

The investigation then progressed to the analysis of the **sporting_anthem** file. The group started by using the **file** command to correctly determine its datatype.

```
┌──(raquel㉿NEPTUNO)-[~/Documents/csf2324-lab1-artifacts/dd]
└─$ file sporting_anthem
sporting_anthem: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 88200 Hz
```

Figure 6 - file tool employed on finding out sporting_anthem's datatype

Despite initial attempts to extract concealed data with file carving tools such as **binwalk** and **foremost**, no results were obtained, so the group opted to conduct a more in-depth analysis of the file using the program Audacity.

Upon meticulous exploration of this file using **Audacity**, a significant breakthrough was made: when converting the audio waves into a spectrogram, a concealed message was uncovered - **"LOOK UP!"**, discernible within the frequency range of 9000 Hz to 19000 Hz.

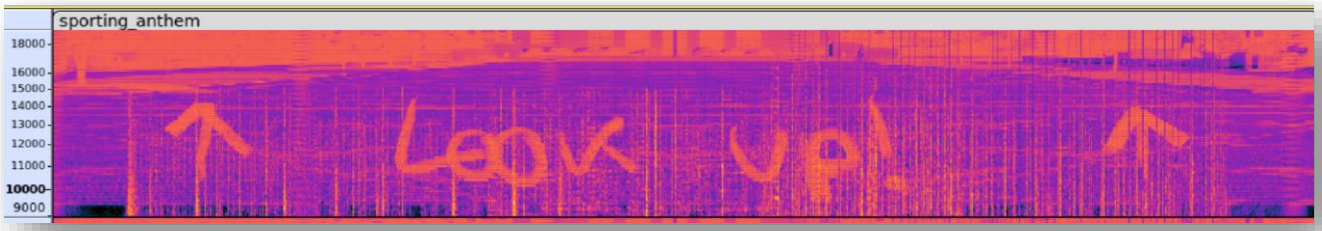


Figure 7 - "LOOK UP" message found on the file's spectrogram

Additionally, when following the message and upping the frequency scale between 14000Hz to 25000Hz, an image portraying *Instituto Superior Técnico*'s central pavilion emerged. However, we decided to keep "looking up" and when defining the frequency scale from 15000Hz to 35000Hz we discovered a hidden seven number sequence: **1683461**.

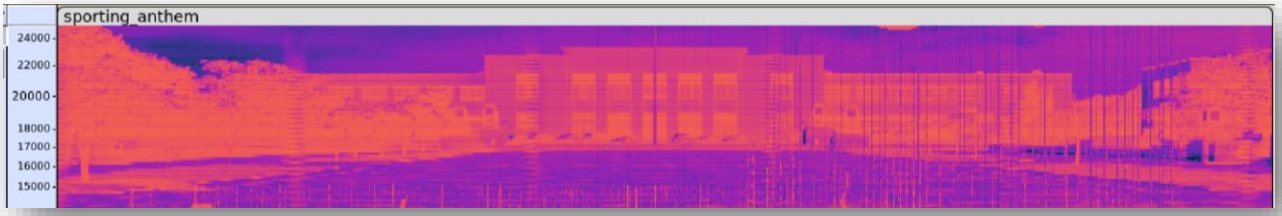


Figure 8 - Instituto Superior Técnico's central pavilion found on the file's spectrogram

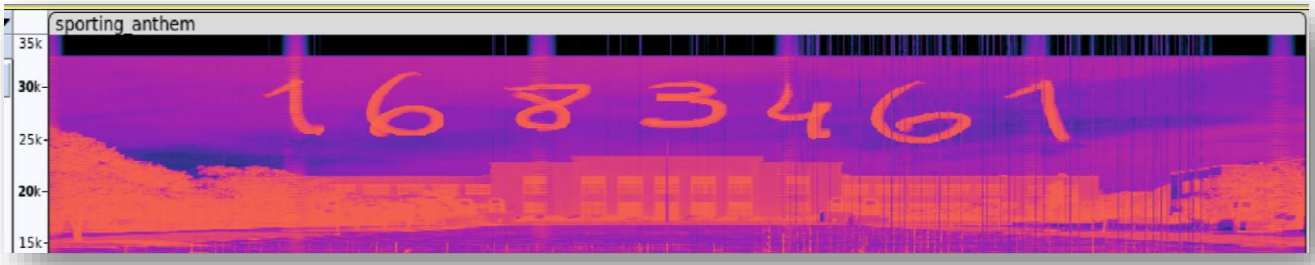


Figure 9 - The 1683461 number sequence found on the file's spectrogram

Regrettably, throughout the remainder of our investigation, the meaning and purpose of this sequence of numbers remained a mystery.

Secret 3: Map

Afterwards, our investigation turned to the analysis of the **.png** files within the pen drive: **logo.png, Social.png, Rialva.png,** and **Tagus.png.** Employing the same method used to determine the owner of the pen drive, we opted to utilize the command **exiftool *.png** to extensively analyze their metadata. Several intriguing details emerged. However, the **logo.png** file didn't yield any unusual information:

```
~/vault/tmp/csf/lab1/artifacts
> exiftool logo.png
ExifTool Version Number         : 12.40
File Name                       : logo.png
Directory                       : .
File Size                       : 1038 KiB
File Modification Date/Time     : 2023:09:28 10:43:54+01:00
File Access Date/Time           : 2023:09:28 10:49:52+01:00
File Inode Change Date/Time     : 2023:09:28 10:44:46+01:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1406
Image Height                    : 1693
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Image Size                      : 1406x1693
Megapixels                      : 2.4
```

Figure 10 - logo.png file metadata details

In contrast, the **Rialva.png, Social.png** and **Tagus.png** files exhibited some suspicious fields in their metadata, specifically the "Web Statement" field, which contained an unusually lengthy string. We decided to employ the **exiftool -b -WebStatement [name].png > [name]_webstatement** command to extract this field's data for further analysis.

Upon closer examination, it became apparent that the text was encoded, as it was unreadable in its current state. Our first course of action was to decode it using the command **cat [name]_webstatement | base64 -d > [name]_base64**. We then examined the decoded files using **base64**. Executing the **file *_base64** command immediately led us to a significant discovery.

```
~/vault/tmp/csf/lab1/analysis/exiftool
> file *_base64
rialva_base64: OpenPGP Secret Key
social_base64: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1268x1070, components 3
tagus_base64:  ASCII text, with very long lines (37000), with no line terminators
```

Figure 11 - file command being employed

Through this, we were able to identify that the *"Web Statement"* fields were actually an **OpenPGP Secret Key** (pertaining to **`Rialva.png`**) and a **`.jpeg`** file (related to the **`Social.png`**). Since the key presented limited utility, and it is most likely just a file that coincidently matched the magic numbers of an OpenPGP Secret Key, we moved on to the **`.jpeg`** image. After properly renaming the file (**`social_statement.jpeg - sha256: 8d5117114353f5399dbad61534902c1eee97505da767167ed85a8c14d67d1656`**) and storing it in our findings folder, we examined it.

The image depicts the new Arco do Cego building that has been under construction for the past year and half, and next to it, a path that leads to the Casa da Moeda building across the street.

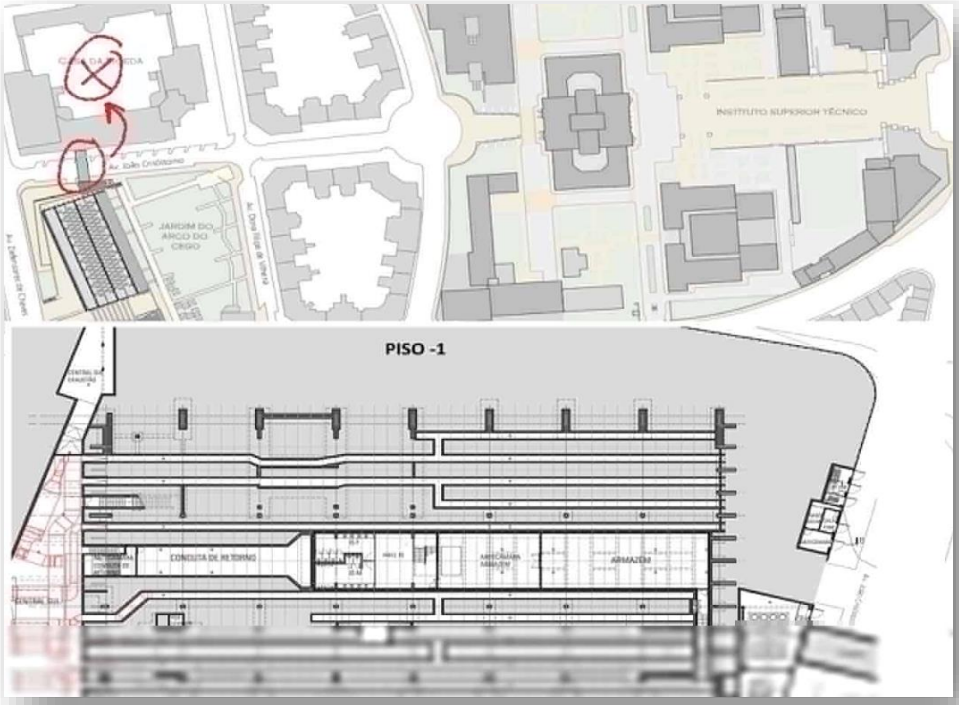


Figure 12 - the image that was found using Social.png's "Web Statement" field

By taking a quick look at the image, it was evident that its bottom part was blurred and it is possible that some information was missing, as the appearance of the bottom pixels suggest. To fix this issue, we postulated that this missing portion could come from the **"Web Statements"** found earlier in the examination.

After trying several combinations of the **"Web Statements"**, we eventually reached the right one. Combining all the **"Web Statements"** into a single file with the command **`cat social_webstatement rialva_webstatement tagus_webstatement > joined_statements`** - which turns out to be the images ordered in descending order of their review -, and once again decoding this data with **`base64`** we obtained the following image:

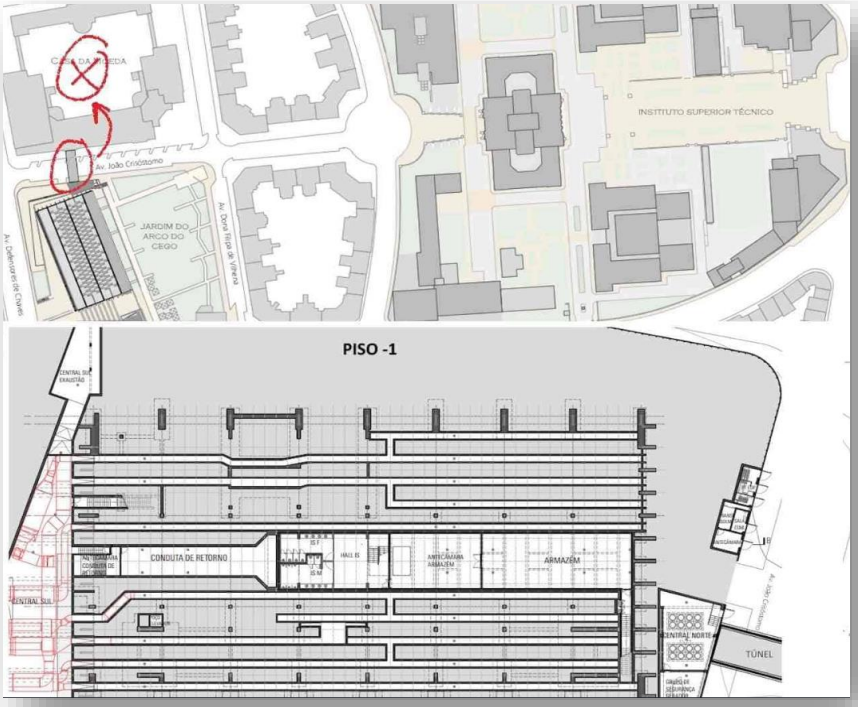


Figure 13 - Image found using the three files "Web Statement" fields

The image looks much clearer now. We renamed it appropriately (**`joined_base64.jpeg - sha256: ad962cbd8f1d558d6e3cb8a46e88793500c078a029682b3ead703d1baf9ffa84`**) and stored it in our *`findings`* folder.

Secret 4: Tunnel Video

Upon an initial analysis of the **report.docx** file we could immediately tell that we were unable to open it. A **.docx** file is a Microsoft Word document commonly used for word processing. In cases where such files become corrupted and refuse to open, it is imperative to explore unconventional methods to recover their content.

The initial examination of the corrupted **.docx** file revealed a series of plain text that resembled a hexdump. This observation indicated that the file might be recoverable through some decoding techniques.

The presence of hex-like text suggested that the data might have originally been in binary form. To begin the recovery process, the hexdump-like text was converted into binary format, using the command **xxd ‘r ‘p report.docx > report-tobin.bin**. By converting the text to binary, the data could be interpreted as a series of bits, making it more amenable to further analysis.

After this, we decided to decode this binary data using **base64**. In this case, the base64-encoded data was decoded to retrieve its original binary form with the command **base64 -d -i report-tobin.bin > report-base64decoded.**

Upon further investigation of the decoded file, using the **file -i** command, it was identified that it contained data in the **LZ4** format. To proceed with the recovery, the LZ4-compressed data needed to be decompressed. To do that, we employed the **lz4 -d report-base64decoded decoded_file** command.

```
┌──(guilherme㉿kali)-[~/Documents/report/csf2324-lab1-artifacts]
└─$ file -i report-base64decoded.txt
report-base64decoded.txt: application/x-lz4; charset=binary
```

Figure 14 - output of the file command when used on report-base64decoded.txt

Following the **LZ4** decompression, it was discovered that the data was actually a **ZIP archive**. Upon successfully identifying the ZIP archive, it was discovered that the ZIP file was password protected. This security measure prevented immediate access to the contents of the archive which we could tell were 2 **.png** files, 1 **.txt** file and 1 **.pdf** file.

```
┌──(guilherme㉿kali)-[~/Documents/report/csf2324-lab1-artifacts]
└─$ unzip decoded_file
Archive:  decoded_file
[decoded_file] grandmas_cake.png password:
   skipping: grandmas_cake.png       incorrect password
   skipping: grandmas_recipe.txt     incorrect password
   skipping: my_fortune.jpeg         incorrect password
   skipping: corrupted.pdf           incorrect password
```

Figure 15 - decoded_file contents

To discover the ZIP archive's password, an investigation was conducted to gather potential clues. During this process, it was decided to leverage the **BdC_on_the_beat** text file as a potential source for a password dictionary. This decision was based on the assumption that the password might be a word or phrase present in the file. To prepare the text file for use as a password dictionary, we extracted every word within it by splitting the text based on whitespace characters. The resulting list of words was then sorted alphabetically.

The process of creating this password dictionary was done through the use two commands: **`sed 's/ /\n/g' BdC_on_the_beat > words.txt`**, followed by **`sort words.txt | uniq > zip_passwords.txt`**.

With the password dictionary ready, a *password dictionary attack* was conducted on the ZIP archive. This method involves trying each word or phrase from the dictionary as a potential password until the correct one is found. The tool **frackzip** was employed to automate the attack on the ZIP archive, and the correct password was successfully identified as ***(Three-time-champion)***.

```
┌──(guilherme㉿kali)-[~/Documents/report/csf2324-lab1-artifacts]
└─$ fcrackzip -v -D -p zip_passwords.txt decoded_file
found file 'grandmas_cake.png', (size cp/uc 2064791/2064522, flags 9, chk 9838)
found file 'grandmas_recipe.txt', (size cp/uc   1072/  2033, flags 9, chk 9838)
found file 'my_fortune.jpeg', (size cp/uc  13982/ 13984, flags 9, chk 8d9b)
found file 'corrupted.pdf', (size cp/uc 38839816/38860767, flags 9, chk 90e2)
possible pw found: (Three-time-champion) ()
```

Figure 16 - output of the dictionary attack on decoded_file

Following the successful extraction of the ZIP's contents, it was found that the recovered data included a file named **corrupted.pdf**. However, attempts to open this PDF file were met with failure, as it appeared to be corrupted and inaccessible. To investigate the nature of the corruption within the file, a hexdump analysis was performed using the command **`hexdump -C corrupted.pdf | head`**. This command allowed us to examine the initial bytes of the file and gain insights into its structure.

During the hexdump analysis, an unexpected discovery was made. The hexdump output revealed a portion of data within the file that resembled an incomplete MP4 file header: the portion "**isomisozavc1mp41**". A comparison was then made between the incomplete MP4 file header found in the **corrupted.pdf** file and the header of a complete and valid MP4 file, **Cool_stuff.mp4**. This comparison aimed to identify discrepancies and determine the necessary adjustments required for data recovery.

```
┌──(guilherme㉿kali)-[~/Documents/report/csf2324-lab1-artifacts]
└─$ hexdump -C corrupted.pdf | head
00000000  00 00 00 20 69 73 6f 6d  00 00 02 00 69 73 6f 6d  |... isom....isom|
00000010  69 73 6f 32 61 76 63 31  6d 70 34 31 00 00 ba f9  |iso2avc1mp41....|
00000020  6d 6f 6f 76 00 00 00 6c  6d 76 68 64 00 00 00 00  |moov...lmvhd....|
00000030  00 00 00 00 00 00 00 00  00 00 03 e8 00 00 ac 27  |...............'|
00000040  00 01 00 00 01 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  00 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000070  40 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |@...............|
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 03  |................|
00000090  00 00 6a 6d 74 72 61 6b  00 00 00 5c 74 6b 68 64  |..jmtrak...\tkhd|
```

Figure 17 - corrupted.pdf head hexdump containing its magic numbers

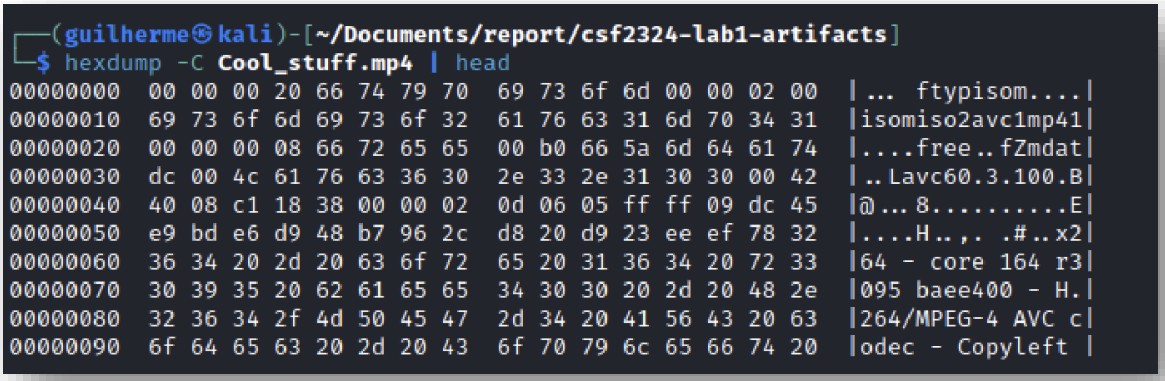


Figure 18 – Cool_stuff.mp4 head hexdump containing its magic numbers

It was observed that the incomplete MP4 file header lacked the proper "magic numbers'' that characterize a valid MP4 file. To facilitate data recovery, hexcode editing was employed to modify the corrupted PDF. Specifically, the hexcode was adjusted to include the correct magic numbers associated with an MP4 file.

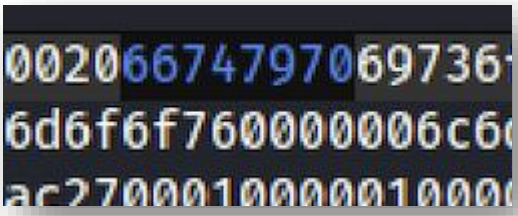


Figure 19 - The missing bits in corrupted.pdf hexdump

After the necessary hexcode modifications were made, it became possible to open the previously corrupted file. However, it was now apparent that this file was not a PDF document, but rather an MP4 video file. The corrections to the hexcode allowed the system to recognize and interpret the file as a valid MP4 file, revealing the valuable multimedia content within. We stored this file in our findings folder **(nolongercorrupted.mp4 - sha256: 8f9a03d13221bf0477f8c7d178bcfbdd94c3ef22df05dcee05cc3962c82ff11c).**

Upon further examination of the other three files that were in the ZIP, it was determined that they were indeed as they initially appeared, without any additional complexities or issues. These files were:

- **(grandmas_cake.png sha256: 8112eada7a480d85ef8b4c43010bda2192dd37dbaca91abafde25006d7397d7c);**
- **(grandmas_recipe.txt - sha256: a4b09747a56a8a3b2670f205541498699fe4157b807e8327bd91182a6bfaf649);**
- **(my_fortune.jpeg - sha256: 96e434b503d68822a03ad2886e243dbbd6d6723b661e29d4025a54b681d5ec2e).**

Secret 5: Tunnel Architecture Plans

The investigation then extended to the `Cool_stuff.mp4` file, presenting as a whimsical and lighthearted minute-long video montage. After meticulous observation, an anomaly was discerned in the concluding image - an edited picture of His Excellency, President Marcelo Rebelo de Sousa partially submerged in water, exhibiting distinct green static, blur and desaturation.

Figure 20 - The suspicious frame

We employed the `ffmpeg` tool as `ffmpeg -i Cool_stuff.mp4 cool_stuff_frames/frame%04d.png` to extract each frame from the video, organizing them into a localized folder: *`cool_stuff_frames`*. Afterwards, we generated a forensic image of the frame corresponding to the **above-mentioned** image and generated its fingerprint.

```
┌──(raquel㉿NEPTUNO)-[~/Documents/csf2324-lab1-artifacts]
└─$ sudo dd if=./cool_stuff_frames/frame0060.png of=marcelo.png bs=4M status=progress
0+1 records in
0+1 records out
1293098 bytes (1.3 MB, 1.2 MiB) copied, 0.000805785 s, 1.6 GB/s
```

Figure 21 - Creation of the forensic image for the frame

```
┌──(raquel㉿NEPTUNO)-[~/Documents/csf2324-lab1-artifacts]
└─$ sha256sum marcelo.png
1a29f70064544029b01ccde7b5988a16994ff5cc85cf0aad4208317cee7b6e70  marcelo.png
```

Figure 22 - Generation of the sha-256 fingerprint value for the frame

To proceed with our investigation, we utilized the website stegonline, to scrutinize the bit planes of the image, aiming at identifying those afflicted by noise. Our examination revealed that the Green Bit Planes from 0 to 5 exhibited discernible noise and, therefore, we used the functionality "Extract Files/Data" to successfully unveil the concealed image within these planes - a **.jpg** file portraying a tunnel to "Casa da Moeda" along with its architectural blueprints. We named it appropriately **(tunnel.jpeg- sha256: 2830c60333ca6bd736df58731822ebd24ea477f9cdb8feb2e72c92b87c4580cb)** and stored it in our findings folder.

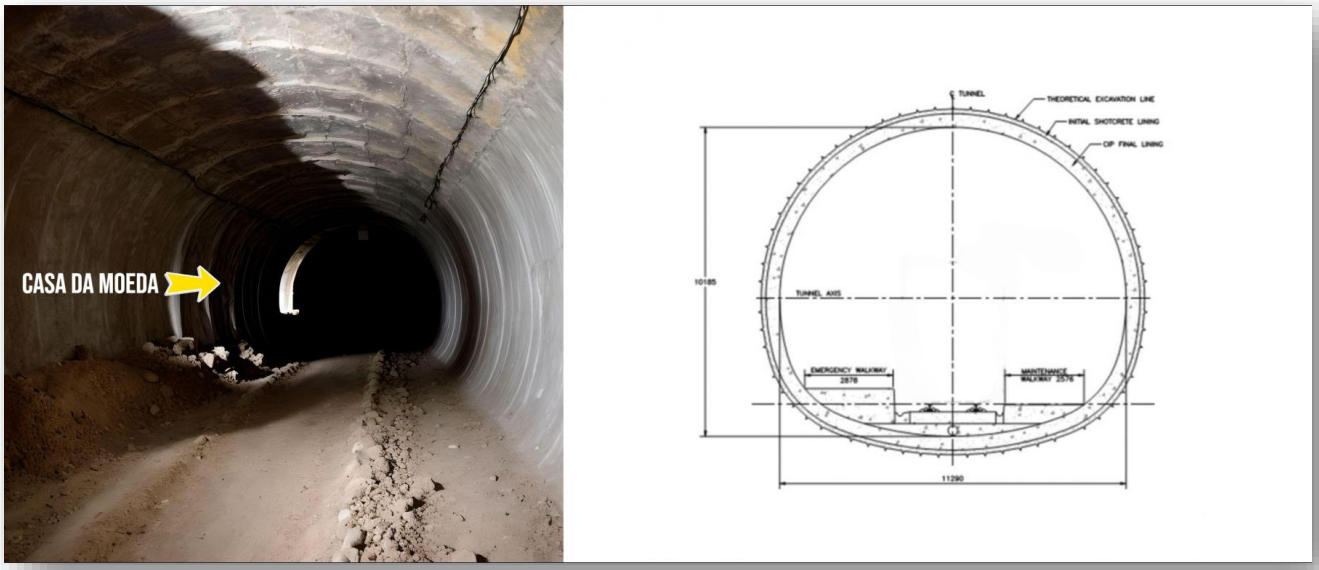


Figure 23 - The found image containing a photograph of the tunnel and its architectural plans

Secret 6: IST Logo Steganography

We then proceeded to take another look at the **logo.png** file with some steganography analysis 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 all the upper pixels of the **.png** except for the blue colored ones, from the actual logo, meaning that some information might be hidden in the image's LSBs (Least Significant Bits).

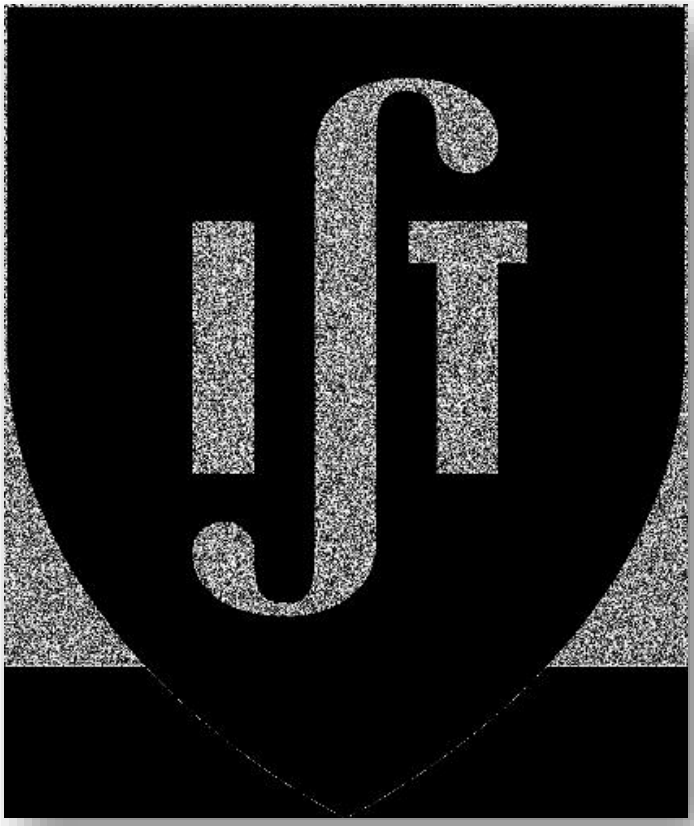


Figure 24 - IST logo altered to showcase the noise section

To extract the LSBs from this noise section, we proceeded to develop a custom python script (**lsb_decoder.py**). After running it and analyzing the extracted files with **file ***, we got the following results:

```
~/vault/tmp/csf/lab1/analysis/lsb/logo
❯ file *
logo_lsb1: data
logo_lsb2: data
logo_lsb3: OpenPGP Secret Key
logo_lsb4: data
logo_lsb5: PDF document, version 1.7, 1 pages
```

Figure 25 - file command output of the extracted bits

Just as we suspected, there was in fact a hidden file inside the logo image. We copied this file to our *findings* folder **(logo_lsb5.pdf - sha256: 2007318984389f207361fe5d4095977865a3aa08ee729243970b275f6ac3e711)**, and afterwards it was possible to open and read it. Another thing worth mentioning is that **file *** also returned a possible **OpenPGP Secret Key**, in the **logo_lsb3** file, which is most likely another coincidence. Nonetheless, we stored it in our *findings* folder (**logo_lsb3_OpenPGP - sha256: 32bfc1590da552e68ed2b63c0542df79ff15a67095e91ce463c5a4cb4d94b855).**

When opened, the PDF contained the following text:

> *"I have finally uncovered the startling truth behind the construction of the new building in Arco do Cego. Suspicions had been lingering in my mind due to the inexplicable delay in the completion, but I never could've guessed the severity of the truth.*
>
> *Over the course of the past year and a half, I've felt the ground tremble every time I pass through Av. João Crisóstomo at night. I told some colleagues about it, only to be met with skepticism and dismissive claims that I was delusional and that the tremors were simply due to the subway system. Still I was convinced that something shady was going on, so I decided to investigate.*
>
> *I disguised myself as a construction worker, with a safety vest and helmet that I bought on Amazon. Entering the site was easy yet extracting any information from the workers proved to be a challenge. They were all incredibly cautious.*
>
> *Eventually, I saw a suspicious hole in the ground with a descending ladder. I was able to get some information about it from a worker that wasn't as cautious as the others, convincing him that our boss had requested a video documenting the ongoing work. He easily complied and disclosed the truth - they were digging an underground tunnel connecting the new building to the Casa da Moeda!*
> *Why should anyone need such a tunnel? It's clear that someone is planning to use it to attain unimaginable wealth. When this information reaches the public, it is bound to become one of the biggest scandals in Portugal's history, possibly surpassing even the infamous Luís Filipe Vieira embezzlement case!"*

With this new development in the case, we discovered that the owner of the pen drive - César Silva Ferro – was uninvolved in the construction of the tunnel connecting Arco do Cego's new building to the Casa da Moeda and was only a bystander who uncovered and documented the details around it.

Other Concealed Artifacts (not considered important to the case)

---

report.docx

Besides the **corrupted.pdf** found in the **decode.zip** file, there were another three files:

- **grandmas_cake.png;**
- **grandmas_recipe.txt;**
- **my_fortune.png;**

Rialva.png

An Open PGP secret key was found in **Rialva.png's** *"Web Statement"*.

Logo.png

An Open PGP secret key was found in **logo.png's** LSB(3).

sporting_anthem

A VMWare was found in the **sporting_anthem**, however the group was unable to open it.

Finally, in the end of our investigation, our *findings* folder ended up with the following files (and their respective sha256s):

```
~/vault/tmp/csf/lab1/findings
❯ sha256sum *
86ff52a0cf5731064a4c071c8c8a49c2f19b62bf4d2a5a471d68afe61547778d  bank_statement.png
8112eada7a480d85ef8b4c43010bda2192dd37dbaca91abafde25006d7397d7c  grandmas_cake.png
a4b09747a56a8a3b2670f205541498699fe4157b807e8327bd91182a6bfaf649  grandmas_recipe.txt
ad962cbd8f1d558d6e3cb8a46e88793500c078a029682b3ead703d1baf9ffa84  joined_base64.jpeg
32bfc1590da552e68ed2b63c0542df79ff15a67095e91ce463c5a4cb4d94b855  logo_lsb3_OpenPGP
2007318984389f207361fe5d4095977865a3aa08ee729243970b275f6ac3e711  logo_lsb5.pdf
96e434b503d68822a03ad2886e243dbbd6d6723b661e29d4025a54b681d5ec2e  my_fortune.jpeg
8f9a03d13221bf0477f8c7d178bcfbdd94c3ef22df05dcee05cc3962c82ff11c  nolongercorrupted.mp4
d5887449d28ead98181ea4e76fe466bbd76423d284c3a85e097d41747efe285d  rialva_OpenPGP
8d5117114353f5399dbad61534902c1eee97505da767167ed85a8c14d67d1656  social_statement.jpeg
2830c60333ca6bd736df58731822ebd24ea477f9cdb8feb2e72c92b87c4580cb  tunnel.jpeg
```

Figure 26 - All files found in the investigation and their corresponding sha-256 fingerprint value

3 Based on the secrets you recovered, is there any indication that the pen drive was intended to spread malware or present a specific security threat? If there's no direct evidence of malicious intent, how would you interpret the data? Formulate a hypothesis regarding their purpose and justify it using the content of the recovered secrets.

Our investigation has revealed that the concealed contents of the pen drive were an integral part of a meticulously conducted investigation led by César Silva Ferro, aimed at unearthing details concerning the undisclosed construction occurring in Arco do Cego. While there's no evidence of malware within the pen drive's contents, their examination strongly suggests an ongoing security threat, with the possibility of an imminent heist targeting Casa da Moeda.

Furthermore, it's plausible to theorize that César deliberately left his pen drive in the Lab 5 because he was aware of DEI's rigorous internal regulations, which claim that any unclaimed or misplaced storage device found on the premises must be subjected to an in-depth forensic analysis. Given that none of César's colleagues believed his suspicions regarding the shady activities undergoing at the construction site, he took it upon himself to disguise as a construction worker and misleading the workers for further information.

As a result, if he reported his findings to the competent authorities and his involvement became public, he could be in considerable danger. Hence, it's conceivable that César hoped that DEI would independently report the findings, safeguarding his identity and also ensuring that his findings would be appropriately addressed.

4 Given your discoveries, what would be your recommendations for the subsequent course of action? Advise Mr. Golias Matos on how best to proceed with this investigation.

Given our confirmation that César is the owner of the pen drive, and the dangerous implications that its contents hold, it is imperative that we promptly apprise Mr. Golias Matos of its concealed contents. Additionally, we should take the necessary steps to notify the relevant authorities. This will enable them to conduct a thorough investigation, including a potential inspection of the construction site.