INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2023-2024 – 1st Period

Digital Forensics Report

Carolina Coelho 99189; Edson da Veiga 100731; Guilherme Leitão 99951

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.

We suspect that the owner of this pen drive is Cesar Silva Ferro since we found his name as Author on Tagus.png, Rialva.png, and Social.png metadata; and that he is a CSF student because his name is present on the waste-of-time that reveals a .pdf CSF exam scores (he was the only one who did the exam and didn't pass, probably because he was too busy doing the investigations).

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

Below is a list of the 6 concealed artifacts we discovered:

A. waste-of-time [Result: secret_bank.png]

First, we use the **file** command to discover the file extension:

```
file waste-of-time
waste-of-time: PDF document, version 1.4, 1 pages (zip deflate encoded)
```

So we realized it was a **PDF document**, and we added the PDF extension to the file to open it.

CSF 2022/23 - 2nd Exam

Nome	Total	I	I	I	I	I	I	I	I	II	
	0,1154	a.1	b.1	c.1	d.1	2.a	2.b	2.c	2.d	1	
	6.69	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	
Ana Sofia Oliveira Almeida	10,2	0,5	0	0	0	1	0,75	0,5	0	1	
André Luís Gonçalves Martins											
Beatriz Maria Santos Ferreira	12,7	1	1	0	0,5	1	0,5	1	1	1	
César Silva Ferro	3,1	3,1	0	0	0	0,5	1	1	0,75	0,5	
Hugo Manuel Silva Pereira											
Inês Carolina Alves Pinto	9,7	0	0	0	0	1	1	1	0,75	1	
João Pedro Silva Santos	10,2	0,5	0	0	0	1	0,75	0,5	0	1	
Pedro Miguel Costa Fernandes											
Rita Sofia Santos Fernandes											
Tiago José Rodrigues Oliveira	11,9	1	0,75	0	0	0,75	1	0,75	0	0	

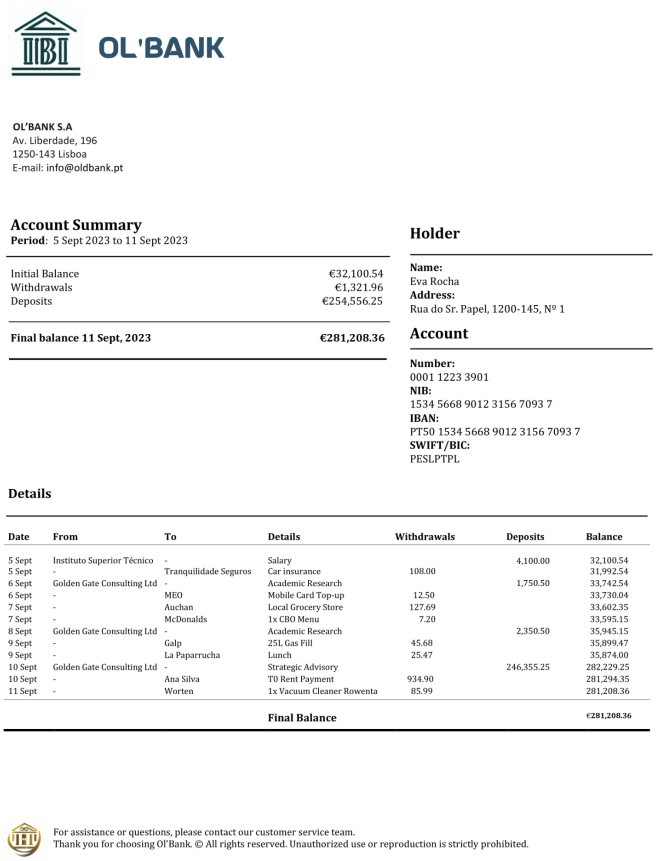
Image 01: full_process/secret_bank/waste-of-time

After discovering the PDF content we used hexdump to analyze the file's hexadecimal and ASCII content, and we realized that was a **PNG image** hidden after the PDF file end magic number.

```
00 n  0000231700 00000 n  0000231776 00000 n  0000231860 00000 n
  0000231956 00000 n  0000232052 00000 n  0000232126 00000 n  00
00232220 00000 n  0000232249 00000 n  0000232317 00000 n  000023
2559 00000 n  0000263666 00000 n  0000264202 00000 n  0000322013
 00000 n  0000325179 00000 n  0000325223 00000 n  trailer <</ID[
(D\325i\313`\002\221A\223\230\301\334\031\240Jd) (D\325i\313`\00
2\221A\223\230\301\334\031\240Jd)]/Info 16 0 R/Root 1 0 R/Size 2
274>> startxref 325246 %%EOF .PNG        IHDR   .   .     .*.,
  pHYs   .   . n.u>    PLTE...TTT      BBB......   ....Rj...   .
.............................222...   ......   JJJ      555   ..
.vvvccc&&&.................YYY...>>>...qqqmmm......OOO.........
.........   .........iii 87...   ................. <9...}}}9::R
RQ <>^^^......VVV =<...... CA***zzz...fffFFFsuu............ 88 <
;...\\\$$$.........```...DDD888 45<<<xxx 45 A< 24...... DC BB 97
......~..l..... e%...?`a...Uv{h]>+HH.n#...jV"d| .........l....D.
....'..8.......v%z.....Fh{.....:.........Rii0RR.sK..u9[r.....-..
```

Image 02: Hexdumb screenprint

So we copied the content from ".PNG" until the end to a new file, and we saved it as a PNG file. It was the first secret that we found, it was a bank account summary and we named **secret_bank.png**.



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.

Image 03: secrets/secret_bank.png

B. Social.png & Rialva.png [Result: secret_piso01.jpeg]

First, we looked for **metadata** information on Social.png:

```
$ exiftool Social.png
…
Web Statement:
/9j/4AAQSkZJRgABAQAAAQABAAD/2wEEEAAUABQAFAAUABUAFAAXABkAGQAXAB8AIgAeACIAHwAuACsAJwAnAC
sALgBGADIANgAyADYAMgBGAGoAQgBOAEIAQgBOAEIAagBeAHIAXQBWAF0AcgBeAKkAhQB2AHYAhQCpAMMApACb
AKQAwwDsANMA0wDsASoBGwEqAYUBhQILEQAUABQAFAAUABUAFAAXABkAGQAXAB8AIgAeACIAHwAuACsAJwA.....
…
```

We suspected this might be encoded with **base64** so we decided to attempt to decode it. First, we manually copied it to a file "web_content.out" and then used the following:

```
$ base64 -d web_content.out > web_content_decoded; hexdump -C web_content_decoded |
head
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 00 00 01  |......JFIF......|
00000010  00 01 00 00 ff db 01 04  10 00 14 00 14 00 14 00  |................|
00000020  14 00 15 00 14 00 17 00  19 00 19 00 17 00 1f 00  |................|
00000030  22 00 1e 00 22 00 1f 00  2e 00 2b 00 27 00 27 00  |"..."......+.'.'.|
…
```

We immediately noticed the "**JFIF**" so we knew we were dealing with a potential **.jpeg** image. However, since no "**ff d9**" magic number was present in the hexadecimal we knew it was incomplete and suspected we might find it in one of the other images on the **Web Content field**. And so we did find it in Rialva.png (after decoding it the same way as before). We copied the field and concatenated it at the end of the "web_content.out" file. Finally, we decoded it and added the .jpeg extension at the end of the filename and opened it:

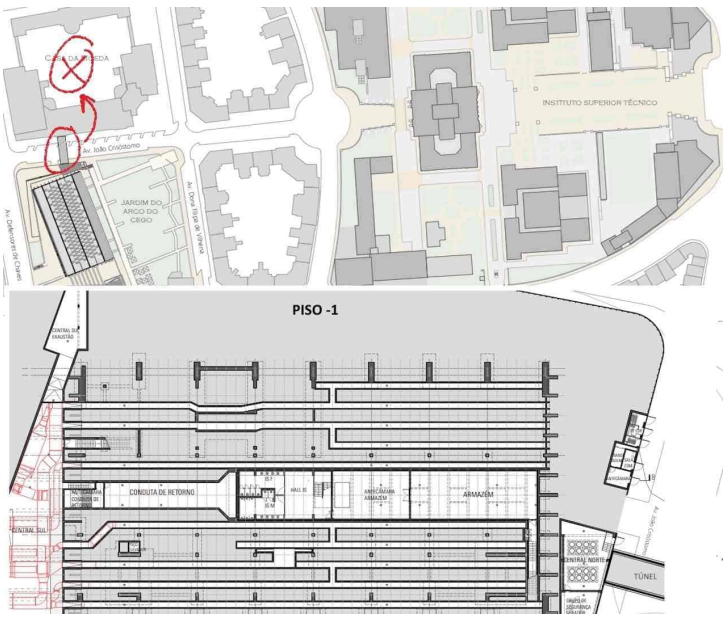


Image 04: secrets/secret_piso01.jpeg

C. report.docx & BdC_on_the_beat [Result: secret_constructionSite.mp4]

Analyzing the output of the "**hexdump**" command on the file "report.docx," we deduced that the content was in hexadecimal format.

```
hexdump -C report.docx | head -n 5
00000000  34 32 34 33 34 61 34 65  34 37 34 37 35 32 37 37  |42434a4e47475277|
00000010  37 35 35 31 34 31 34 31  35 31 34 39 34 32 35 31  |7551414151494251|
00000020  35 33 37 37 34 64 34 35  34 36 34 31 34 31 34 61  |53774d454641414a|
```

So, we used a hexadecimal to ASCII converter:

```
cp report.docx report.hex
xxd -r -p report.hex report_ascii.txt
```

Looking at the "**report_ascii.txt**" file, we recognized a pattern that led us to consider the file as base64 encoded. Therefore, we attempted to decode the file.

```
base64 -d report_ascii.txt > report_db64
```

Using, **binwalk** we found **lz4** compressed data, so we tried to convert it to a zip file and unzip it.

```
binwalk report_db64

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             LZ4 compressed data
11            0xB             Zip archive data, encrypted at least v2.0 to extract,
compressed size: 2064791, uncompressed size: 2064522, name: grandmas_cake.pnglz4 -d
report_db64 descompressed_data.zip
```

However, when we attempted to unzip it, we discovered that it was protected by a password.

```
unzip descompressed_data.zip
Archive:  descompressed_data.zip
[descompressed_data.zip] grandmas_cake.png password:
```

After using John with some popular web dictionaries, we didn't get any results. So, we concluded that we should attempt to find the password in another file. We remembered that the file "**BdC_on_the_beat**" contained a very long text, so we created a file with all the words that appeared in that document and provided it as input to John. We were correct; the password was indeed found in that file: (Three-time-champion)

```
zip2john descompressed_data.zip > zip_hash.txt
john --wordlist=word_list zip_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
(Three-time-champion) (descompressed_data.zip)
```

Then, we extracted the files from the zip file. The most interesting file was a "**corrupted.pdf.**" After analyzing the hexdump, we determined that it was actually an MP4 file, but there were some missing bytes.

```
hexdump -C corrupted.pdf | head -n 3
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....|
```

After adding the necessary bytes, we were able to play the video.

```
hexdump -C corrupted.mp4 | head -n 3
00000000  00 00 00 20 66 74 79 70  69 73 6f 6d 00 00 02 00  |... ftypisom....|
00000010  69 73 6f 6d 69 73 6f 32  61 76 63 31 6d 70 34 31  |isomiso2avc1mp41|
00000020  00 00 ba f9 6d 6f 6f 76  00 00 00 6c 6d 76 68 64  |....moov...lmvhd|
```

D. Cool_stuff.mp4 [Result: secret_tunnel.jpeg]

While watching the video, we easily spotted that something was off about the last picture. We extracted the **first frame** on the **59th second** for analysis:

```
$ ffmpeg -ss 59 -i Cool_stuff.mp4 -frames:v 1 last_frame.png
ffmpeg version 4.4.2-0ubuntu0.22.04.1 Copyright (c) 2000-2021 the FFmpeg developers
…
```

Afterward, we attempted to find **steganographic** content in the image using the *zsteg* tool:

```
$ zsteg last_frame.png -a
…
b6,g,lsb,xy         .. file: JPEG image data, JFIF standard 1.01, aspect ratio,
density 1x1, segment length 16, progressive, precision 8, 3584x1536, components 3
…
```

As you can see, it identified a **JPEG** file in the **6th-bit plane of the green channel, with an LSB method and left-to-right/top-to-bottom**. As such, we extracted that data using:

```
$ zsteg last_frame.png -e b6,g,lsb,xy > extracted_marcelo.jpeg
```

At the end, open the image and you get the following:

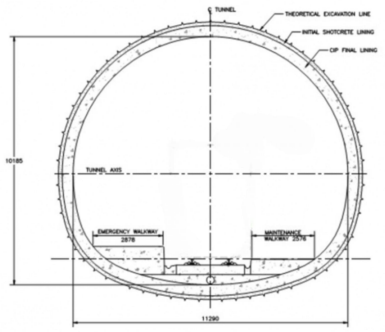


Image 05: secrets/secret_tunnel.jpeg

E. sporting_anthem [Result: secret_number.txt]

First, we use the file command to discover the file extension:

```
file sporting_anthem
sporting_anthem: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo
88200 Hz
```

So we realized it was a **WAVE audio,** and we added the extension **.wav**. The audio was 3:08, we played it and noticed that until 1:47 was the sporting anthem, and from 1:47 to the end was another song appended. But we also detected that the audio had a **noise**, so we suspected that maybe there was something hired on it. So we decided to verify the file metadata using the **exiftool**.

```
exiftool sporting_anthem
ExifTool Version Number         : 12.60
File Name                       : sporting_anthem
Directory                       : .
File Size                       : 67 MB
File Modification Date/Time     : 2023:09:16 16:53:04+01:00
File Access Date/Time           : 2023:09:17 09:41:59+01:00
File Inode Change Date/Time     : 2023:09:28 22:43:50+01:00
File Permissions                : -rw-r--r--
File Type                       : WAV
```

```
File Type Extension             : wav
....
Tempo                           : 130
Software                        : FL Studio 12
Duration                        : 0:03:09
```

From the metadata, we noticed that the **FL Studio 12** software was used on this file, so we installed the software e loaded the file on it, and started to explore the software to find a way to embed the hired content. After exploring many buttons, luckily we found out that on the "**Edit sample…**" window if we press the **Clean up (denoise)**, brush button, appears to an image:

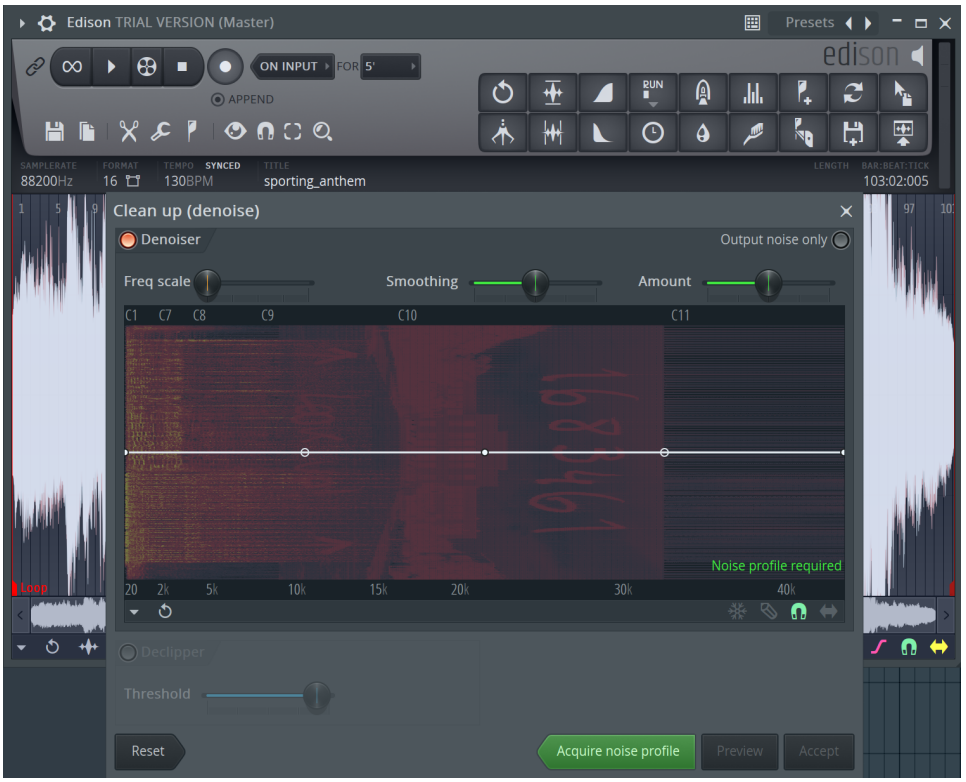


Image 06: sporting_anthem.wav spectrogram on FL Studio 21

That image wasn't so clear, so we searched for another software that allowed us to see the spectrum better and found the **Audacity**. On Audacity we load the sporting_anthem.wav, choose the spectrogram view, and then in the spectrogram settings we choose the max frequency at 34100 Hz and the grayscale scheme. As a result, we found this:

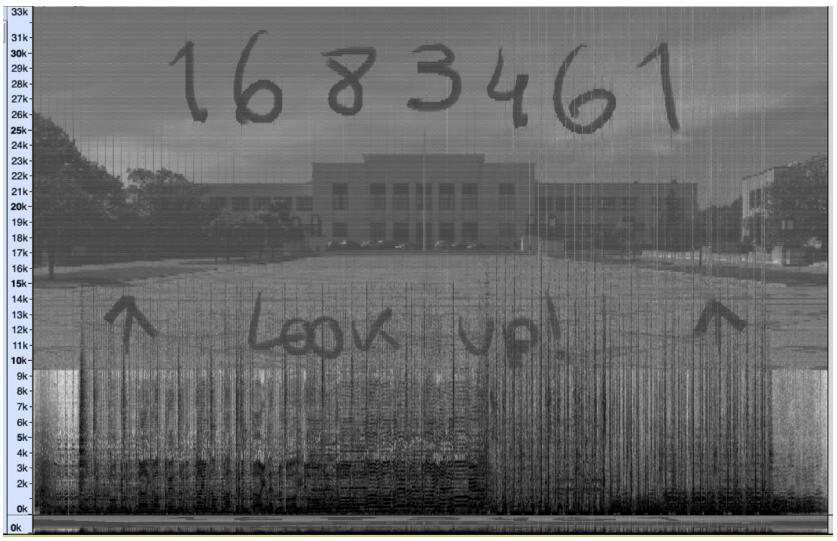


Image 07: Audacity sporting_anthem.wav spectrogram

We saved the number **1683461** on a .txt file named: **secret_number.txt**.

F. logo.png [Result: secret_letter.pdf]

When we opened the file "**logo.png**", we noticed that in a certain part of the image, the background appeared to contain potentially relevant information, as it was not the typical white background of the Instituto Superior Técnico logo.

However, we realized that to analyze this information, it would be necessary to remove the blue part of the image. To do that, we used the "**script.py**".

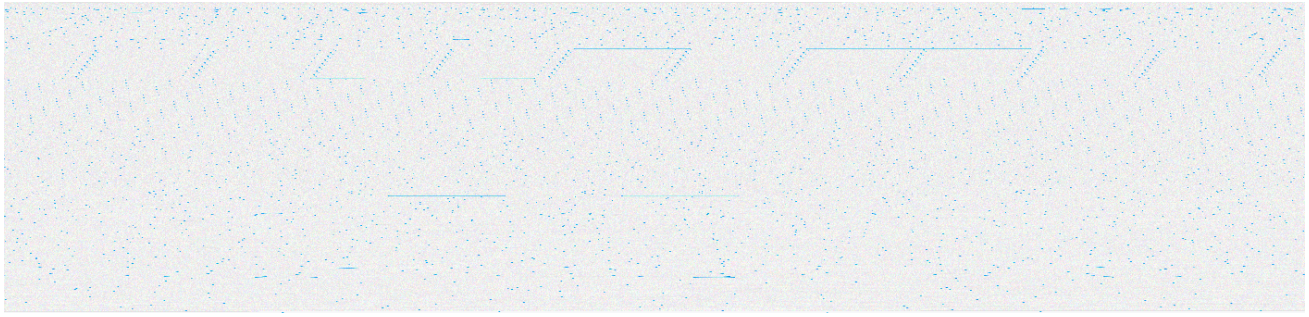


Image 08: logo.png without the IST logo

After removing the blue part of the image, we used the online steganography tool "**StegOnline**" (https://stegonline.georgeom.net/) to extract the hidden file from the image

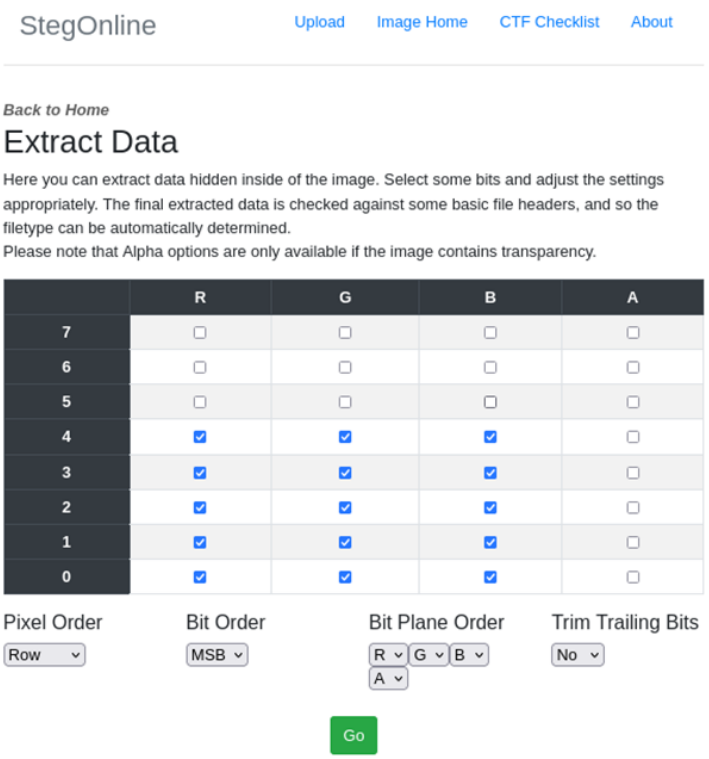
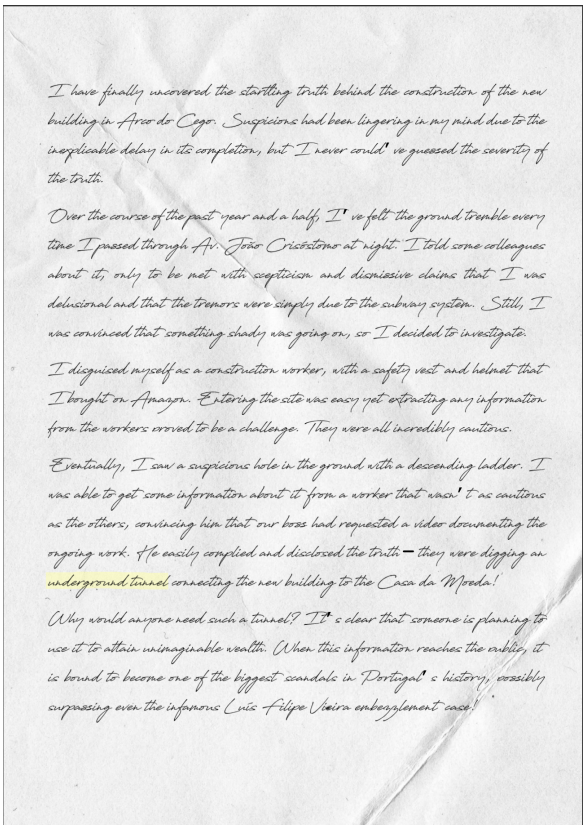


Image 09: Extract Data on StegOnline

The output obtained from "**StegOnline**" was a letter written by our suspect.



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 its 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 passed through Av. João Crisóstomo at night. I told some colleagues about it, only to be met with scepticism 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 would 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!

Image 10: secrets/secret_letter.pdf

However, since the image still contained some garbage data at the end of the file, it was also necessary to remove the data beyond the PDF's EOF (End of File).

```
hexdump -C output_image.pdf | grep EOF
000d7170  72 74 78 72 65 66 0a 32  31 36 0a 25 25 45 4f 46  |rtxref.216.%%EOF|
```

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.

Based on our investigation, we conclude that there is no evidence of an intention to spread malware or pose any other security threat. None of the files are executables (verified using the **'ldd'** tool), and the information we discovered suggests that our suspect may have been researching a potential future crime, specifically an assault on *Casa da Moeda*.

The secret files contained within the original files are evidence collected by the owner of the flash drive regarding the construction of a tunnel to the target point of the heist. The file that provides more information about our suspect's intentions is a letter (**secret_letter.pdf**). In this letter, the suspect reveals all the details about his investigation. He has also gathered what we suspect to be a secret code, a video where one of the construction site workers confirms the existence of the tunnel, a map depicting the connection between Arco do Cego and Casa da Moeda, a bank statement with suspicious transactions, and an image of the aforementioned tunnel.

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.

Based on the discoveries made during our cyber forensic analysis of the files extracted from the pen drive, here are some recommendations for the subsequent course of action and how Mr. Golias Matos should proceed with the investigation:

Legal Counsel: Consider seeking legal counsel to ensure that the institute is in compliance with all relevant laws and regulations regarding this investigation. Legal advice can help navigate any potential legal ramifications.

Contact Law Enforcement: Given the nature of the evidence, it's advisable to contact the local law enforcement authorities. Share all the relevant information, including the letter, video, map, and bank statement. Law enforcement can assess the situation, conduct their investigation, and take appropriate action to ensure public safety.

Preserve the Chain of Custody: Maintain the integrity of the chain of custody for all the evidence. This is crucial for any potential legal proceedings that may arise from the investigation. Ensure that all actions related to the evidence are documented and logged meticulously.

Secure the Evidence: Safeguard the original pen drive and all extracted files in a secure location. It's essential to prevent any unauthorized access or tampering with the evidence.

Maintain Confidentiality: Stress the importance of maintaining confidentiality among institute staff and anyone involved in the investigation. Loose lips can jeopardize the integrity of the case.

Review and Update Policies: Take this incident as an opportunity to review and update the institute's policies regarding lost and found items, data security, and the reporting of suspicious activities. Ensure that all staff and students are aware of these policies.

Attachment

	File	SHA-256 Value
1	secret_bank.png	1f70fc60e1c23b842e3278846e29c5fb66ed43c1d6ac3ccfe408f53acf005edb
2	secret_constructionSite.mp4	8f9a03d13221bf0477f8c7d178bcfbdd94c3ef22df05dcee05cc3962c82ff11c
3	secret_letter.pdf	a6a005c97a758f04220fe161c269a2ac229d7fe3b6fbfc88e40d6d8675be8fd6
4	secret_number.txt	d04cccf4ee29f190885641b1dbbf5e69375e9a3afb951c23ae97dd3016e5911b
5	secret_piso01.jpeg	131e54681ae4abca1d677384b3765bbc92c873eff252baec713196c2b696adeb
6	secret_tunnel.jpeg	dca0850ab895e45808235d32e9591d4ec08b09be89727760878cdd17963990bb