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

In our investigation process, we primarily utilized two tools: **`mmls`** and **`Autopsy`**. We began with **`mmls`**, a command-line utility from The Sleuth Kit, 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.

```
└─$ mmls caesarDisk.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   0001054719   0001050624   EFI System Partition
006:  002       0001054720   0052426751   0051372032
007:  -------   0052426752   0052428799   0000002048   Unallocated
```

```
└─$ 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)
007:  -------   0041940992   0041943039   0000002048   Unallocated
```

Figure 1, 2 - command *mmls* on caesarDisk.img and backupDisk.img

Once we had this partition information, we transitioned to using **`Autopsy`** which is an advanced forensic analysis tool with a user-friendly interface. This software streamlines the process of exploring the data stored on the disk, making it practical for memory forensics analysis. By starting with **`mmls`** to identify and define the partitions on the disk, we laid the groundwork for our subsequent forensic investigation using Autopsy. This approach ensured that we could systematically and effectively analyze the disk and its memory, optimizing the entire investigative process.

1 Did you find any traces of the hidden artifacts and/or the files from the lost pen drive on César Silva Ferro's computers?

Yes. During our investigation we were able to find multiple traces of the hidden artifacts and files from the lost pen drive.

1.1 Backup Disk Image analysis (backupDisk.img)

In the **`backupDisk.img`**, we encountered several intriguing zip files within the **`backupDisk.img/vol2/home/ironcaesar/`** directory, each named in the format *"backup_<number>.zip"*. A detailed examination of these files will be presented later in this report. Specifically, within **`backup_1696076401.zip`**, we identified **artifacts identical to all of those from the lost pen drive**. This discovery was accompanied by the presence of a **`CSF.zip`** file, containing course materials for CSF, and a **`CSE102-CheatSheetCSSLong.pdf`** file, both common to all other backup zip files.

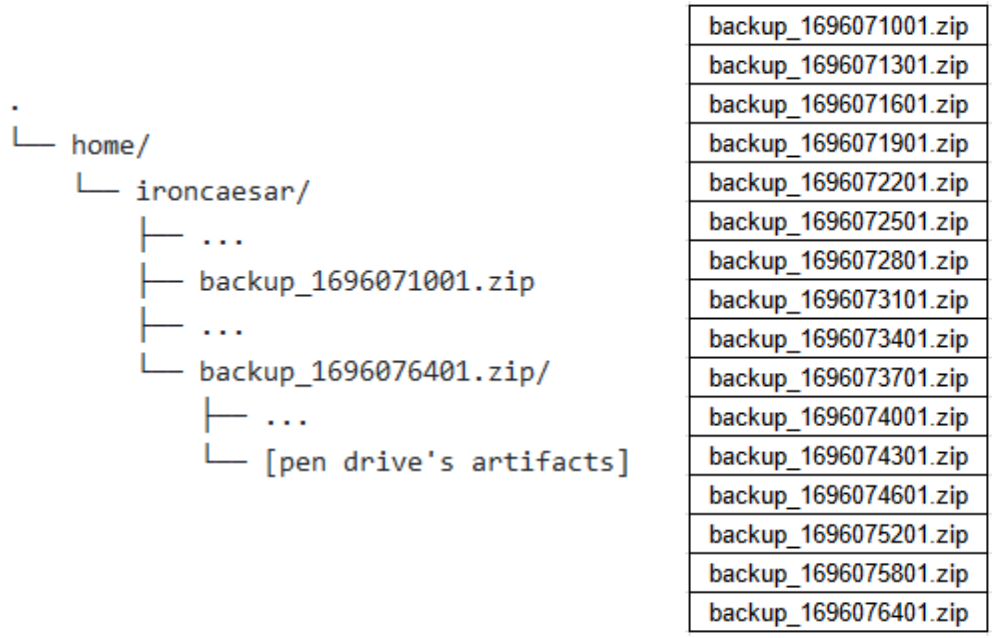

Figure 3 - File System reconstructions for all backup .zip files

We have substantiated the identity of these files as those recovered from the lost pen drive by cross-referencing their SHA-256 hashes. In cases where artifacts share identical names, their corresponding SHA-256 hashes validate their equivalence (as seen in the images below).

```
~/vault/tmp/csf/lab2/analysis/backup_pen_artifacts
❯ sha256sum *
d8028eb28c6aa2b94607df770515368e0d2c0488279328599ca51fe1bdbced6c  BdC_on_the_beat
1f196d05bbf3ac03620a8f1108630531bb65cfedf31e16321dedfd6e5c3d877b  CSE102-CheatSheetCSSLong.pdf
c4dc316983f9bc7a66dc97b3c4cac28f2c24725962ce1c7358b34621d463ea7a  CSF.zip
240cb4494b4a4e0e367f67afa80bd7287dda09755e3eaa66af1994a03ea3e316  Cool_stuff.mp4
8873a7055c9838ef8847424306f6997c3eb0d0aa6373acd65206ede85bfe8ec8  Rialva.png
50011896abe7f70e9e8b00b4d3ccc25acf6a2272f11b343b2758be01355d21f4  Social.png
ec54db5e6df2093573548d685ce72f3c4ffa548032e6a26ac2cc3f544bd3c283  Tagus.png
3bb7305396f84dff0ee88150438d32c0a366e7ab3e4fbf61d6a72080f7fe3eed  logo.png
30bb4ca7580bd331d3334bf4bba6b9e45165d1f51960eb7ee345a631aee90f70  report.docx
7d4e8b5d0d8d127fdf31f097a208a511847872884c2e11db662279292a0969cd  sporting_anthem
bb3a2ee5816ae1ff8b09bd1d5f0796a005a3db1af8d898392e8a915a7277149e  video.mp4
941b69160a7c4d6e3483c54c43a9a8fd52ff12b65af77b770d879cace846bce4  waste-of-time
```

```
~/vault/tmp/csf/lab1/artifacts
❯ sha256sum *
d8028eb28c6aa2b94607df770515368e0d2c0488279328599ca51fe1bdbced6c  BdC_on_the_beat
240cb4494b4a4e0e367f67afa80bd7287dda09755e3eaa66af1994a03ea3e316  Cool_stuff.mp4
8873a7055c9838ef8847424306f6997c3eb0d0aa6373acd65206ede85bfe8ec8  Rialva.png
50011896abe7f70e9e8b00b4d3ccc25acf6a2272f11b343b2758be01355d21f4  Social.png
ec54db5e6df2093573548d685ce72f3c4ffa548032e6a26ac2cc3f544bd3c283  Tagus.png
d25a8d99bccc3e176b2852acb72b92f3d40c8f7e4b6501d2145101929de637fb  logo.png
30bb4ca7580bd331d3334bf4bba6b9e45165d1f51960eb7ee345a631aee90f70  report.docx
7d4e8b5d0d8d127fdf31f097a208a511847872884c2e11db662279292a0969cd  sporting_anthem
941b69160a7c4d6e3483c54c43a9a8fd52ff12b65af77b770d879cace846bce4  waste-of-time
```

Figure 4, 5 - sha256 values comparison between the lost pen drive contents and the found backup pen artifacts

1.2 Caesar Disk Image analysis (caesarDisk.img)

Within the caesarDisk.img, further traces of the concealed files were discovered. Specifically, within the **`caesarDisk.img/vol6/home/ironcaesar/Documents/video/`** directory, we uncovered the mp3 audio file and all the images used to generate the **`coolStuff.mp4`** artifact from the lost pen drive. Furthermore, the **`./Documents`** directory revealed an intriguing subfolder labeled **`Steg_Tools_v5.7.0_By_Lapsus$`**, containing tools that appeared to be used in the creation of numerous pen drive artifacts (a thorough explanation of these tools and the way they were used will be made later into the report). The subfolder also contained the previously mentioned audio and images, along with other significant discoveries:

1.2.1 Images

The three *"food review"* image artifacts were located under **`./Documents/images`**.

1.2.2 Zip Decoy Files

Within **`./Documents/zipDecoyFiles`**, we encountered three files found inside one of the pen drive artifact's hidden zip files, further reinforcing the hypothesis that these files were merely decoys.

The discovery of matching artifacts in both the backupDisk.img and caesarDisk.img further strengthens the significance of our findings.

1.3 Bash History analysis (caesarDisk.img)

Apart from the files found still in the disk, some more interesting discoveries were made by investigating the **`.bash_history`** file under **`caesarDisk.img/vol6/home/ironcaesar/`**, where we got a look at César's last used bash commands.

With the information present in this file we can legitimize the claim that all the lost pen drive's artifacts, and the files hidden inside them, were at some point in the disk. Not only that, but we can explain how the files found inside some of the artifacts were hidden, and also be sure that the artifacts that couldn't be found in the disk image were in fact purposely deleted (more on this further into the report).
From commands like **`xdg-open Bank-Statement-11-09-2023-1.png`**, **`xdg-open tunnel.jpeg`**, and many more we can create a reconstruction of the disk image from when all the artifacts were still present in it:

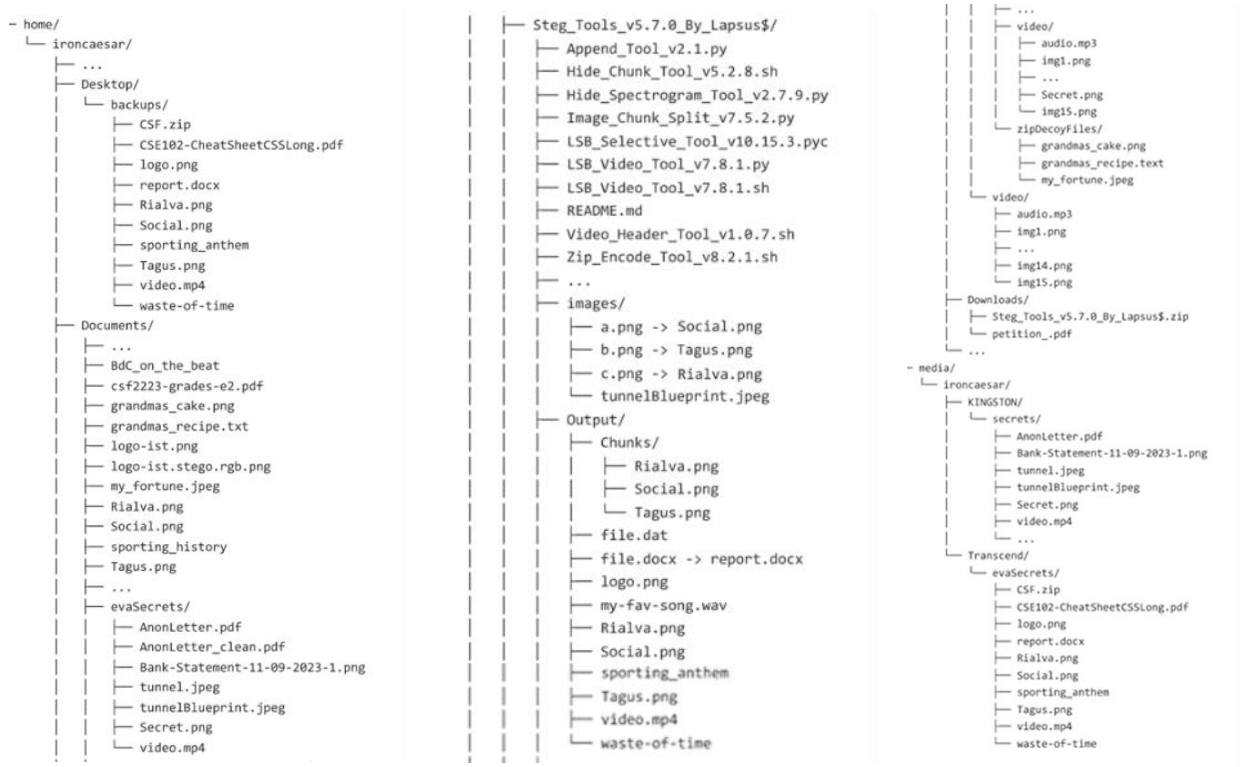

Figure 6 –bash_history File System reconstruction of caesarDisk.img

2 If so, can you trace the source of these files and how they have been manipulated over time? Establish a timeline of relevant events.

2.1 Backup Zip files' origin

A subsequent examination was conducted within the caesarDisk.img file. The investigation unearthed several suspicious files, including **`.bash_history`**, **`backup.sh`**, **`obfuscator`**, and **`pass_gen.sh`**, all located within **`caesarDisk.img/vol6/home/ironcaesar/backups/`**.

Upon a detailed analysis of these files, it was observed that two of them were bash scripts, one contained a bash history log, and another was named obfuscator. The obfuscator file warranted significant attention as the 'file' command indicated it was a **`python3.8 byte-compiled`** file, implying that it might be a **`.pyc`** file. Further scrutiny revealed that the content had undergone some form of obfuscation, rendering it unreadable to conventional methods, hence its name (further elaborated in later sections of this report).

File	Type	Created At	Modified At	Accessed At	SHA-256
.bash_history	text/plain	2023-09-30 13:40:26	2023-10-01 13:36:06	2023-10-01 13:36:06	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
backup.sh	application/x-sh	2023-09-28 9:04:02	2023-09-28 09:04:03	2023-10-01 13:30:01	68174cb8c46c01ef9755dca86ac067b40f23f86eecd60e67b08c9ce9fffd1a83
obfuscator	application/octet-stream	2023-09-30 11:45:08	2023-09-30 11:45:08	2023-10-01 13:30:01	86a89e4c96282492bbabb364b5a601a9e187d8f9365c3c1c900c79c7db244560
pass_gen.sh	application/x-sh	2023-09-30 11:45:08	2023-09-30 11:45:08	2023-10-01 13:30:01	c0a4c3cc51aaa45692e892e62ab71c679d043b4ad72f384f08a1a556c8e89785

2.1.1 backup.sh analysis

The **`backup.sh`** file is a Bash script designed for specific data manipulation and secure transfer tasks. It primarily serves to create password-protected zip files. It derives the zip file's name from a timestamp (TS), in the format *"backup_<TS>.zip"*, and secures it with a password created by calling **`pass_gen.sh`** with TS as its argument.

After this, the script employs SSH for secure, remote file transfer. It effectively copies the password-protected zip files to the home directory of **ironcaesar@10.0.2.16**, following which the original zip files are deleted from their source location.

2.1.2 pass_gen.sh analysis

pass_gen.sh serves as a connecting component within the operational sequence. It acts as an intermediary, initiating the **obfuscator** file with the argument it receives, which corresponds to the timestamp created in **backup.sh** (TS).

It's crucial to recognize the sequential execution of the scripts: **./backup.sh** > **./pass_gen.sh TS** > **obfuscator TS**.

2.1.3 obfuscator analysis

The obfuscator file presents intriguing characteristics. The **file** command initially identified it as a **python3.8 byte-compiled file**, suggestive of a **.pyc** file. With this information, a Python decompilation process was conducted by renaming the file to **obfuscator.pyc** and using the command **uncompyle6 obfuscator.pyc > obfuscator.py**, ultimately yielding a human-readable Python script.

The analysis of **obfuscator.py** unveiled its primary function. It operates using an initial seed, located under **/tmp/seed.txt**, and an argument, in this case the timestamp (TS) from **backup.sh**. These elements are used to generate a sha256 hash of a string in the format *"<seedTS>"*. The hash is then converted into hexadecimal format and serves as the password for the password-protected backup zip files. Notably, the script exhibits a mechanism where the initial seed evolves in subsequent iterations. Each seed iteration (seed_i+1) is derived from the sha256 hash of the previous seed (seed_i).

The script provides a notable clue with the phrase "For the first run, please just place your password in the SEED_PATH file." This alludes to the necessity of discovering an initial password to initiate the process.

2.1.4 .bash_history analysis

When opened, the **.bash_history** file appears to be empty. Perhaps César created a copy of the actual bash history and placed it in this directory. Either way, this version of **.bash_history** wasn't found to be useful for our investigation.

We saved the **backup.sh**, **pass_gen.sh**, and **obfuscator** in our **/findings** folder. However we did not save the **.bash_history** file as it was empty.

2.2 Bash History analysis (from caesarDisk.img's home directory)

In an effort to find some sort of password to use as an initial seed, the group moved to a deeper analysis of the **.bash_history** found under **caesarDisk.img/vol6/home/ironcaesar/**, which proved to be more useful than the aforementioned bash history file present in the **backups/** directory.

Apart from the evidence of the lost pen drive's artifacts, we also find an explanation to what happened to these files. Just like we did above in the report, we can reconstruct a timeline of events that provide an explanation to these files' disappearance.

Firstly, we can see that the **Steg_Tools_v5.7.0_By_Lapsus$** folder mentioned earlier played a big role in the creation of the lost pen drive's hidden artifacts, as it contains the tools used to hide some of the files. A quick search on this folder's name reveals that it is indeed a Steganography Tool Kit created by a hacker group by the name of Lapsus$.

César installed the required modules for the tool kit to work, and proceeded to make use of it. We will now analyze each one of the tools and how they were used (the descriptions present below all come from the **`README.md`** file found inside the tool kit's folder).

2.2.1 Append_Tool_v2.1.py

"Append_Tool is a Python script that allows for the seamless insertion of malicious payloads into various file formats. It can be used to compromise systems and exfiltrate sensitive data or simply to hide secrets."

The use of the command **`python3 Append_Tool_v2.1.py ../csf2223-grades-e2.pdf ../evaSecrets/Bank-Statement-11-09-2023-1.png csf2223-grades-e2.pdf`**, tells us that this script was used to hide the bank statement image found in our previous investigation inside the waste-of-time artifact (csf2223-grades-e2.pdf).

2.2.2 Hide_Chunk_Tool_v5.2.8.sh

"Hide_Chunk_Tool is a versatile shell script designed to hide images divided in chunks within different file formats. It can be used to evade detection and deliver malicious payloads or simply to hide secrets"

From the tool's description, the following series of commands:

```
Bash ./Hide_Chunk_Tool_v5.2.8.sh
cd Output/Chunks
mv a.png Social.png
mv b.png Tagus.png
mv c.png Rialva.png
```

And from our discoveries in these *"food review"* artifacts from our previous investigation, we can conclude that this tool was used to hide the treasure map image across these three files' web statement fields.

2.2.3 Hide_Spectrogram_Tool_v2.7.9.py

"Hide_Spectrogram_Tool is a Python script that specializes in hiding content within audio spectrograms. This tool can be used to distribute audio-based threats."

With the command **`python Hide_Spectrogram_Tool_v2.7.9.py ../evaSecrets/Secret.png -h`**, and the tool's description, we can deduce that this tool was used to hide the secret number image found inside the **sporting_anthem** artifact's spectrogram.

2.2.4 LSB_Video_Tool_v7.8.1.sh

"This shell script version of LSB_Video_Tool provides a script to create a video out of images and audio and for hiding data within video files."

The command **`bash LSB_Video_Tool_v7.8.1.sh ../evaSecrets/tunnel.jpeg`**, along with the tool's description and further analysis of the actual script, indicates that this tool was used to hide the tunnel image blueprint found inside of the **Cool_stuff.mp4** artifact.

2.2.5 Video_Header_Tool_v1.0.7.sh

"Video_Header_Tool is a shell script that manipulates video file headers, corrupting the video file metadata."

Using a similar approach to the one made above, from the tool's description, analysis of the script file and from the commands:

```
cp ../evaSecrets/video.mp4 ./video.mp4
bash Video_Header_Tool_v1.0.7.sh
mv ./Output/file.dat ./corrupted.pdf
```

We can conclude that this tool was used to corrupt the header of the mp4 file (renamed to **corrupted.pdf**) found hidden inside the **report.docx** artifact.

2.2.6 LSB_Selective_Tool_v10.15.3.pyc

"LSB_Selective_Tool is a compiled Python script that focuses on least significant bit (LSB) steganography."

Once again, from tool's description, analysis of the script file and the commands:

```
python3 ./LSB_Selective_Tool_v10.15.3.pyc -m hide -i 009FE3 -c rgb -n 5 -o
../logo-ist.png -p ../evaSecrets/AnonLetter_clean.pdf
mv ../logo-ist.stego.rgb.png ./Output/logo.png
```

We can infer that this tool was used to hide the **AnonLetter_clean.pdf** file (letter from the previous investigation) inside the 5 Least Significant Bits of the **logo.png** artifact's pixels with an rgb color of **#009FE3**. Which matches up with our previous findings, as the hidden letter was found in the LSB(5) of the logo's blue colored pixels (#009FE3).

2.2.7 Missing artifacts

The absence of some of the lost pen drive's artifacts can be explained by the multiple commands present in the .bash_history file, mainly the remove commands **`rm`**, **`srm`** and **`rmdir`**, which were employed by César to delete folders and files that contained the missing artifacts.

2.3 Communication Logs

2.3.1 Web browser history analysis

Upon analyzing the **caesarDisk.img**, we discovered 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: **/img_caesarDisk.img/vol_vol6/home/ironcaesar/snap/firefox/common/.mozilla/firefox/rktbn4nn.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 César's detailed browser history. We extracted this table and saved it as "**moz_places.csv**" in our findings folder.

Notably, the browser history revealed several interesting websites César had visited, shedding light on his online activities:

1. https://www.thunderbird.net/thunderbird/102.0/eoy/ - this link informs us that César uses Thunderbird as his preferred webmail service;
2. https://ytmp3.nu/Hcni/ - César visited this website, which allows users to convert YouTube .mp4 videos into .mp3 audio files, suggesting an interest in multimedia conversion tools;
3. https://www.reddit.com/r/Steganography/?rdt=45658 - César explored the Steganography subreddit;
    a. https://www.reddit.com/r/Steganography/comments/16suajy/lapsus_steg_bundle/ - within it, César accessed a post which contained a download link for a bundle of Steganography tools. This download, marked with an id number of 45 in the **moz_places.csv** table, can be found on his computer at the location **/img_caesarDisk.img/vol_vol6/home/ironcaesar/Documents/Steg_Tools_v5.7.0_By_Lapsus$**. (the folder is saved in our **findings** folder with the same name);
    b. a google search on who the author of the bundle (Lapsus$) really is
4. Several google searches for deleting files safely on Ubuntu, indicating an interest, or need, in data security practices;
5. https://shrtco.de/xq56SY - a password protected link (detailed examination of this link later on the report)
6. https://twitter.com/CsarSilvaF20952 - a login to his X (formerly Twitter) account, which provides insight into his social media activity.
7. https://drive.google.com/file/d/1FtLHkqwGdfZQHpdxF2Vq4daS9TK4LJrM/edit - César accessed a file named "**petition_.pdf**" with editing privileges. This file can also be located on his disk under **/img_caesarDisk.img/vol_vol6/home/ironcaesar/Downloads/petition_.pdf** (the file is saved in our **findings** folder with the same name).

File	Type	Created At	Modified At	Accessed At	SHA-256
places.sqlite	application/x-sqlite3	2023-09-19 21:49:43 WEST	2023-09-30 14:01:48 WEST	2023-09-30 14:01:48 WEST	e2cf6701619f62e8285e592fb71d38910c33648e20a91b04f7a92f6262ef67ce

2.3.2 Webmail and IRC server logs analysis

The group proceeded to delve into his Thunderbird email communications for any pertinent details related to the case. Our search led us to the following directory: **`/img_caesarDisk.img/vol_vol6/home/ironcaesar/.thunderbird/gjht15t3.default-release/Mail/pop.gmail.com/`** where we encountered two notable files: **`Inbox`** and **`Sent`** (saved in our **`findings`** folder with the same name).

The **`Inbox`** file had an email from Shady Friend (shadyman217@outlook.com) delivered to César (cesarsilvaferro0@gmail.com) with the subject "**Spicy Intel**" from the date Sat, 30 Sep 2023 11:06:23 +0000 with following body:

```
Listen up,
There's some serious dirt on Eva Rocha, and I've got the inside track.
It's the kind of stuff that could set off fireworks.
Word is you're the force behind that online petition targeting Eva, and
I've dug up some damning evidence that could send her on a wild ride. I
think you will find this interesting :)
Eva Rocha was part of the team in charge of building the Arco do Cego.
But here's the twist: She allegedly took under-the-table payments to  keep
a lid on the construction of a super-secret tunnel. And what's that tunnel
for, you ask? Well, it's all about sneaking into the Casa da  Moeda to
print some sneaky cash on the side.
Here's the lowdown: I've hidden a pendrive at:

LockerLocky CTT IST Lisboa
Address: Av. Rovisco Pais 1
Postal code: 1000-267,

in locker 06 with access code 155. Inside, you'll find all the ammunition
to expose Eva. Grab it when the stars align, and let the games begin.

Stay sharp,
YourShadyFriend
```

Meanwhile the file **`Sent`** had an email from César (cesarsilvaferro0@gmail.com) to catarina.f.silva@outlook.com with the Subject "**Urgent: Need Your Help ASAP**" from the date Sat, 30 Sep 2023 12:25:28 +0100 with following body:

Hey Cat,
I've got some crazy news about my arch-nemesis, Teacher Eva Rocha and I need your help to figure it out.
So, I got this email from some mystery sender (no idea who they are), claiming they've got a pendrive loaded with stuff to take down Eva. You know how much I can't stand her, right? Anyway, at first, I thought it might be some light ammo for my petition. But when I started digging into it, I was floored. It's got some seriously incriminating evidence against Eva Rocha.
But here's where it gets nutty. While watching a video, I spotted someone I recognize, someone close to you... I can't quite wrap my head around how they fit into all this craziness, but it's freaking me out.
I think we need to talk about this ASAP. I have a hunch this could be some CIA type of stuff, so its better we talk over IRC. Here are the details:

Server: irc.freenode.net
IRC Channel: #thebasement

Please, please join me ASAP. This is crucial, and I need your input on how to handle this situation. I'll explain more when we chat. It's like something out of a movie, and I can't believe what I've found.
Stay safe,Cesar S. Ferro

The **Sent** file revealed a connection to irc.freenode.net and specifically, the IRC Channel *#thebasement*. This discovery prompted us to intensify our efforts to uncover any relevant information regarding the conversation between César and Catarina Silva, a key figure in this case.

Our team successfully located the pertinent data within the directory: **/img_caesarDisk.img/vol_vol6/home/ironcaesar/snap/irssi/common/irclogs/2023/freenode/** . Inside this folder, we unearthed various logs from different IRC channels, including the sought-after *#thebasement* channel. The file was named as **#thebasement.09-30.log** (saved in our **findings** folder with the same name), dated Sat Sep 30 12:26:26 2023 and contained all contents of the conversation between César and Catarina Silva, transcribed below:

Ironcaesar: Hey Cat, is that you?
CatSil: Hey Cesar, yeah, I'm here. What's going on?
Ironcaesar: You won't believe what I found out about that pendrive.
CatSil: I got curious when you said there could be someone related to me in that pendrive.
Ironcaesar: So, as I was going through the files, I found evidence of plans and blueprints of a tunnel under Arco do Cego. That's where you are interning right?
CatSil: It is..
Ironcaesar: This is where it gets weird. There was this video of a guy named Fernando Silva also talking about the tunnel. That's when it hit me - It's your father.
CatSil: WTF it can't be...
Ironcaesar: it gets even weirder. Eva is involved too
CatSil: So, you're saying my dad is involved in a project of a secret tunnel beneath Arco do Cego with the IST teacher Eva Rocha?
Ironcaesar: Yeah

Ironcaesar: I also got evidence of some weird company transferring loads of money to her. This is some serious shit. She could be incriminated for this!
Ironcaesar: I always knew there was something shady about her
CatSil: I'm just processing this.. I haven't talked to my dad for long, and he does have a troubled history.. but going from that to some secret tunnel project? That's madness
CatSil: that could ruin my family's name
Ironcaesar: I know.. but he never liked you.. he never helped you pay for the Uni, remember? You had to work for yourself on that.. Maybe this could bring some justice.
Ironcaesar: I mean, I could get rid of Eva, you could get rid of your dad.
CatSil: How can you say that? I won't help you incriminate my own dad!!
Ironcaesar: He seems to have gotten himself into this mess.. As he always has. You have nothing to do with this.
Ironcaesar: I will make this go public. Eva needs to go. And I'm sorry that your dad is involved too. But I think it's for the best of both our sakes.
CatSil: Jesus.. so you will really put this on the big screens?
Ironcaesar: This is now more than my hate for Eva.. This is about a possible scheme using the tunnel to get into Casa da Moeda.. I think we must put this into the public!
CatSil: I mean, it's a hard choice for me..
CatSil: but if you really think it's the way to go, Cesar, I'll go along with it.
CatSil: I'm just not entirely sure about this because, you know, it's my dad we're talking about.
CatSil: But maybe it's time he faces the consequences. Let's hope this pans out right.
Ironcaesar: I hope so
Ironcaesar: I gtg now
Ironcaesar: Stay safe Cat
CatSil: You too, cya

File	Type	Created At	Modified At	Accessed At	SHA-256
Inbox	application/mbox	2023-09-27 10:04:23 WEST	2023-09-30 12:06:56 WEST	2023-09-30 12:06:56 WEST	e47dade67812950049f87ac5d53909c2b1b512a55efe69401b45c5d15bcc1679
Sent	application/mbox	2023-09-30 12:25:29 WEST	2023-09-30 12:25:29 WEST	2023-09-30 12:25:30 WEST	b8e45c1c272fe4f57ed1eaa898d290f03ea73d8f1f36b5bc569df59528a4294d
#thebasement.09-30.log	text/plain	2023-09-30 12:26:26 WEST	2023-09-30 12:40:29 WEST	2023-09-30 12:26:26 WEST	1769807e7868933f8c4479f68780792d4bf5f6edcdc1da5175e17a70bcc5f9e4

2.3.3 Related files analysis

The group proceeded to look at the discovered **petition_.pdf** file and upon examination, it was determined that this file is, in fact, a petition calling for the resignation of IST's Teacher Eva Rocha. What makes this document particularly noteworthy is the fact that César authored it, signaling his active involvement in instigating this petition. Moreover, the petition has garnered substantial support from a diverse group, including students, assistant professors, and parents. This demonstrates a collective effort to pressure Ms. Eva Rocha into resigning from her position.

File	Type	Created At	Modified At	Accessed At	SHA-256
petition_.pdf	application/pdf	2023-09-30 14:01:48 WEST	2023-09-30 14:01:48 WEST	2023-09-30 14:01:48 WEST	4aa4aef66f05c53792fbd04c6f4fe6507923fe2a4fea30cedd440796f465d111

In addition to the discovery of the petition, the group unearthed another significant piece of evidence, the **.bash_history** file (saved in our **findings** folder with the same name) in the **/img_caesarDisk.img/vol_vol6/home/ironcaesar/** folder. Its contents provide a detailed record of César's command-line interactions, and more notably, reveal his explicit manipulation of the contents of the pen drive that Shady Friend delivered to him.

1. César initiated the sequence of actions by navigating to a directory that no longer exists, named **/media/ironcaesar/KINGSTON/secrets**. Then, he conducted the following operations:
    - ***a.*** He listed all the contents contained within the directory.
    - ***b.*** He opted to open three specific files: **Bank-Statement-11-09-2023-1.png**, **tunnel.jpeg**, and **AnonLetter.pdf**.
2. Next, he created a folder within **/Documents** named **evaSecrets** and copied all files from **/media/ironcaesar/KINGSTON/secrets** (a folder that no longer exists) into it;
3. Afterwards, he unzipped the **Steg_Tools_v5.7.0_By_Lapsus.zip** he previously downloaded, moved it to the **/Documents** folder and accessed it. Then, he read the **README.md** of the tools and installed the python libraries as suggested, carelessly including a very concerning one: "*pynput*";
4. Then, he accessed the *Steg_Tools* folder and utilized them on the files Shady Friend's pen drive provided him:
    - ***a.*** used **Append_Tool_v2.1.py** to append the **../evaSecrets/Bank-Statement-11-09-2023-1.png** **(f2.png in lab1_secrets)** in **../csf2223-grades-e2.pdf**, naming the output as **waste-of-time**;
    - ***b.*** created the **./images** folder and moved three *.png* files (**Social.png**, **Tagus.png**, and **Rialva.png**) into it. Then he correspondingly renamed them as **a.png**, **b.png** and, **c.png**. Afterwards he moved the **tunnelBlueprint.jpeg** into **./images** as well. After this pre-processing he used **Hide_Chunk_Tool_v5.2.8.sh** to conceal the **../evaSecrets/tunnelBlueprint.jpeg** **(f4.jpeg in lab1_secrets)** in these pictures' *Web Statement* field;
    - ***c.*** used **Hide_Spectrogram_Tool_v2.7.9.py** on **../evaSecrets/Secret.png** to conceal it in **sporting_anthem**'s spectrogram **(f6.txt in lab1_secrets)**;

d. used **`LSB_Video_Tool_v7.8.1.sh`** on **`../evaSecrets/tunnel.jpeg`** **(f3.jpeg in lab1_secrets)** with the files from **`./video`** (that were copied from **`../video`**) and created the file **`video.mp4`**;

e. used **`Video_Header_Tool_v1.0.7.sh`** in **`../evaSecrets/video.mp4`** **(f5.mp4 in lab1_secrets)** and created **`file.dat`**, which he then renamed as **`corrupted.pdf`**. Afterwards, he created a folder named **`/zipDecoyFiles`** and copied **`../grandmas_cake.png`**, **`../grandmas_recipe.txt`**, and **`../my_fortune.jpeg`** into it. Then he used **`Zip_Encode_Tool_v8.2.1.sh`** on **`corrupted.pdf`** and the **`/zipDecoyFiles`** folder, creating the **`file.docx`** file that he renamed as **`report.docx`**;

f. used **`LSB_Selective_Tool_v10.15.3.pyc`** on **`../logo-ist.png`** to conceal the **`../evaSecrets/AnonLetter_clean.pdf`** **(f1.pdf in lab1_secrets)** in one of **`../logo-ist.png`**'s RGB channels and named it as **`logo.png`**.

5. He moved all **`./Output`** folder contents to **`~/Desktop/backups/`** and then safely removed all auxiliary files and folders he used with the tool "*srm*", a tool that he probably found out about when searching on how to safely remove files on Ubuntu. Afterwards he once again copied all files from **`~/Desktop/backups/`** to **`/media/ironcaesar/Transcend/`** (which also no longer exists) newly created folder: **`/evaSecrets/`**. After copying he safely removes those files and deletes the **`/media/ironcaesar/Transcend/evaSecrets/`** directory as well.

2.4 Key Logger

As mentioned before, César installed the python library **`pynput`** which allows you to control and monitor input devices.

After further investigation of the **`Steg_Tools_v5.7.0_By_Lapsus`** folder, we discovered a file with the extension .**`pyc`**. A **`.pyc`** file is a binary file generated by the Python programming language. Decompilation is the process of converting bytecode (as found in a **`.pyc`** file) back into human-readable Python code so, after decompiling the file, the code revealed that it was actually a keylogger application designed to record and log every keystroke made on a computer, using the **`pynput`** library.

In addition to the keylogging code, we stumbled upon another piece of code that seems to be related to manipulating image colors and bits. An insightful discovery came from analyzing the **`.bash_history`** file where we uncovered the following command: **`python3 ./LSB_Selective_Tool_v10.15.3.pyc -m hide -i 009FE3 -c rgb -n 5 -o ../logo-ist.png -p ../evaSecrets/AnonLetter_clean.pdf`**.

Upon revisiting the code, we've deciphered its purpose: it utilizes the Least Significant Bit (LSB) steganography technique to conceal the **`AnonLetter_clean.pdf`** file within the **`logo-ist.png`** image file.

Besides that, the keylogger saved the keystrokes in text files with a unique naming convention. Each text file generated was named in the following manner: "K" followed by a combination of N random ASCII letters or numbers, where N is an integer. This naming convention allows anonymity and discretion when storing the recorded data. Upon further examination of the code, we could tell that a file with $N = 10$ would be created and saved in the **`/tmp`** directory.

While looking for such file, we found a file that followed the naming convention we were expecting: **`tmp/KQRbv8Zj1Ba.log.log`**. Upon further examination of this file and as expected, we found the logs of the keys that had been pressed.

File	Type	Created At	Modified At	Accessed At	SHA-256
LSB_Selective_Tool_v10.15.3.pyc	application/octet-stream	2023-09-30 21:03:05	2023-09-30 20:59:09	2023-09-30 21:03:05	b52c903aed6a200293c2c709b04f1149f38df45f909c57096fe1654d4b2ede77
KQRbv8Zj1Ba.log.log	text/x-log	2023-09-30 13:06:49	2023-10-01 13:38:11	2023-09-30 13:06:49	122c7819ff8e168884ce36d495bce8bd934bab7b88b1c11cc9a1d4d48f27c98f

By examining the **`KQRbv8Zj1Ba.log.log`** file, we managed to extract what was typed from the keylogger logs. Amongst other less relevant information, we found the previous password-protected link César had visited, `https://shrtco.de/xq56SY`, along with what appeared to be the password to access the website (since he typed it exactly after visiting the website), **`viktor_yokeres_1906`**.

After accessing the link and entering the assumed-to-be password, we came across a google document with what appeared to be more passwords since the name of the file was “My Password Manager”. Between them, there was the password to the zip file we discovered while examining the contents of the pen drive: (Three-time-champion).

The google document can be found here and and in our **`/findings`** folder, saved as a *.txt* file under the same name.

2.5 Backup Zips' passwords

With the new information obtained from our Keylogger findings, we can now resume our investigation on the aforementioned password-protected zip files found under **backupDisk.img/vol2/home/ironcaesar/**.

We deduced that for the initial seed of the obfuscator script we had to use some sort of password that might be found somewhere in the disk. From the google document found, there were what appeared to be 15 passwords for us to choose from.
By trial and error, we eventually stumbled upon the correct one: **WolfgangPuckCulinary$**.

Using this password as the initial seed and the timestamp of the first zip file, we were able to obtain the right password for it, and with that done, all the remaining passwords were easily obtained by feeding the zips' timestamps to the obfuscator script.
The passwords for all the zip files are the following:

1696071001 - a26daa976257889f8df7d5f1c659d12947d03c9c2bda3b57edce2466e7faacbe
1696071301 - bc6d217c0394b3515c24c0b0ffdbfb2cfff0ee581b230909765ca9d7c1276496
1696071601 - 25e9ebd98dcc606953b51094d5111eab8d44dcf18a0791792aa195bce8163f57
1696071901 - eaeae474ed862ea32b5868c992c82cea9609422a0f04fcc40bdf23a746e43902
1696072201 - 39defc4ceda3ba14aa750f10a7dbfff1312a943bccafec35b0c28ad258d52ba3
1696072501 - 5ea4bd29b7e662d10122003152895ace9d5daa3cbc5eaabad25894bcbebd8fed
1696072801 - de1ef3ae259839c4e20f19f29d2cd368708b73ca2496e0fcfb9554861acf692d
1696073101 - e19f0a3d1498960876872627a13ed16452c951cf2e425d225d87719f293e4c46
1696073401 - 9c407bdb6fb6f8e29cba59fb2638eb02ca7cfbe4941c69f64d7c7b25d88ae1cc
1696073701 - 372b9260114a86daad1a4a9282c1626d00cf5070b1a85a6529c0b6fc09b715da
1696074001 - 037f8f265ff20484fa8a54ffe4beee051da201d918796491924e38b04fc093fc
1696074301 - 5e1aa1f630eaa153960e22548718f665fe8f5a272b2355601a53bc444d9214d5
1696074601 - f41c8e3b8cb72c37dd44209a1f2a30c46fde34519bb6c2b78540150527ae714f
1696075201 - a47cf17a9ee9a0c77afa421057b5b539248176c0301a49fab35a28ca6b14c943
1696075801 - f37a8544ceaceef0a63357db9d3608ad1d48e73177818634cafbf7398e934aba
1696076401 - ff5a43c16680b5103153bca1a81fcbc8920500e8b9ead93b7f1d1861281113d0

We can deduce that these backups were programmed to happen every 5 minutes, as evidenced by the 300 second difference between each timestamp, which can also explain why most of them are exactly the same. Some of the more recent zip files were created within 600 seconds (10 minutes) of each other, maybe because of some problem in the transferring of the files.
A copy of the last decompressed zip file – the most recent one - was stored in our findings folder (**backup_1696076401.zip)**.

3 Do you find any evidence of anti-forensic activity?

During our investigation, a significant discovery was made within the caesarDisk, specifically located in the directory **`caesarDisk.img/vol_vol6/home/ironcaesar/backups/`**. We encountered a file named **`obfuscator`** (mentioned above), which was obfuscated, rendering it unreadable through conventional means.

The deliberate obfuscation of the **`obfuscator`** file is an action that suggests an intent to conceal its contents and hinder investigative efforts. Obfuscation techniques are commonly employed by individuals seeking to subvert forensic examination. These techniques are designed to render files and data unintelligible, effectively obscuring their purpose or content, and so, we have legitimate reasons to use this file as proof of anti-forensic behaviors.

Throughout the investigation, our team also found a type of malware, specifically a spyware in the form of a keylogger on the **`caesarDisk.img`** disk. Keyloggers can be used for various purposes, both legitimate and malicious, however, during the investigation, it was determined that the keylogger had been installed accidentally. César Silva Ferro was trying to install and utilize steganography tools to hide and encrypt the data that Shady Friend gave to him and was **not** trying to engage in anti-forensic activity through it.

Remarkably, the presence of the keylogger inadvertently assisted our investigation, as it provided a record of keystrokes that included the password for a password protected link, that ultimately held a *.docx* file that César named as his Password Manager. As anti-forensic activities involve measures taken to hide or destroy digital evidence, in this example, the keylogger doesn't point to anti-forensic intentions by César, but could mean anti-forensic intentions by the group LAPSUS$, a well-known hacker group that in 2020 tried to penetrate the Defense Ministry of Brazil.x

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

The recent investigation has unveiled significant discoveries that shed new light on the unfolding plot of the construction of the Tunnel between Casa da Moeda and Arco do Cego's new building.

It has been determined that the pen drive in question does not belong to César Silva Ferro, opposed to what we initially believed. Rather, it was handed over to him clandestinely, stashed away within a locker, by an individual that disguises themself online under the alias Shady Friend. This revelation implies a clandestine exchange and a mysterious connection between César and this disguised figure, which prompts further investigation of Shady Friend and the relationship between them and César.

Shady Friend is the one who actively investigated the construction and has provided a compelling theory regarding it. According to them, this covert passageway is likely being built for the surreptitious production and collection of counterfeit currency within Casa da Moeda.

Additionally, the investigation has unveiled a personal connection between the construction worker featured in a video recorded by Shady Friend, as this worker is none other than the father of César's friend, Catarina Silva, a man with a troubled history. This revelation suggests that Catarina Silva's father may be involved in the questionable activities linked to the tunnel's construction.

Finally, the investigation has uncovered a growing controversy involving IST's Teacher Eva Rocha. As found earlier, a bank statement of Eva Rocha's account reveals "*under-the-table payments to keep a lid on the construction of a super-secret tunnel*" as Shady Friend writes. However, a petition was initiated by César aiming at pressuring Teacher Eva Rocha to resign from her position which has garnered support from various quarters, including students, assistant professors, and parents. As César describes Eva Rocha as his arch-nemesis and after a brief analysis of the names of the petition supporters it's easy to theorize that some suspicious names are actually fake supporters:

Parents

- Fernando Mendes - a well-known Portuguese TV host;
- Pedro Teixeira Mota - a well-known Portuguese comedian;
- Antonio Costa - the prime-minister of Portugal.

Assistant Professors

- Humberto Delgado - Portuguese marshal that protagonized the fight against "Estado Novo" in 1960's and was assassinated because of it (César might have added as an analogy that him defying Eva Rocha's authority is an act comparable to overthrowing a fascist government);
- Pedro Eva - a subtle variation of IST's teacher Pedro Adão;
- Ruben Amorim - the current coach of César's football team, Sporting Clube de Portugal.

Students

- João Corceiro and Margarida Félix - amalgamations of the names "João Félix" (Portuguese football player) and "Margarida Corceiro," (Portuguese model and actress) who were previously in a romantic relationship;
- Eduardo Tesoura - a reference to the movie "Edward Scissorhands";
- Raul Meireles Silva - incorporating elements from the name of former Portuguese football player Raul Meireles and César's last name.
- Jorge Palma - a renowned Portuguese singer;
- Kátia Aveiro - the sister of football sensation Cristiano Ronaldo;
- Sara Sampaio - a famous Portuguese supermodel;
- Sérgio Conceição - the present coach of FCP (Futebol Clube do Porto).

It is important to note that this theory remains speculative, and these individuals may indeed be genuine supporters of César's petition. However, this intriguing revelation invites further investigation into the authenticity of these supporters, as it holds the potential to unveil the true identity of Shady Friend among them.