INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2021-2022 – 1st Period

Digital Forensics Report

Authors

Group 12

89415 - António Lopes

90074 - Francisco Romão

92513 - Mafalda Ferreira

1 Do you find any traces of the Football Leaks files on Mr. Daniels' computers?

Firstly, an analysis of the first disk image "backup_disk.img" was performed by displaying the partition layouts of the volume system and listing the directories corresponding to the partition Linux system was installed. This sector corresponds to table ID = 02 and entry = 000:000, starting at sector 2048.

Three different zip backup files were found during the listing of all the files in "backup_disk.img" at "/home/charlied". These three zip files were extracted from the disk using the following commands:

```
$ icat -o 2048 backup_disk.img -r
$ icat -o 2048 backup_disk.img 168635 > backup_1634405485.zip
$ icat -o 2048 backup_disk.img 168646 > backup_1634412601.zip
$ icat -o 2048 backup_disk.img 168650 > backup_1634414401.zip
```

Secondly, an analysis of the second disk "charlied_disk.img" was performed using the same method as before:

```
$ mmls charlied_disk.img
$ fls -o 1052672 charlied_disk.img -D
```

A script named 'backup.sh' was found under the path "/home/charlied/cron_manager" when listing, recursively, all files and directory names in the disk image. An extraction of the content was performed after obtaining the script inode number using the following commands:

```
$ fls -o 1052672 charlied_disk.img 434942 -r
$ icat -o 1052672 charlied_disk.img 423847 > backup.sh
```

Following the inspection of the extracted script, a conclusion was made that "backup.sh" used two different files named "obfuscator" and "seeds.txt" located in "charlied_disk.img" at "/home/charlied/password_gen". The content of these files was also extracted and "obfuscator" file decompiled to a Python code.

```
$ icat -o 1052672 charlied_disk.img 557134 > obfuscator
$ icat -o 1052672 charlied_disk.img 557188 > seeds.txt
$ mv obfuscator obfuscator.pyc
$ uncompyle6 obfuscator.pyc > obfuscator
```

It was discovered that "backup.sh" was used to create the previous backup zip files named as "backup_$(timestamp).zip", where timestamp corresponds to the unix timestamp when the backup was executed. These backup zip files were encrypted with a $BACKUP_PASS using the sha256 hash function to perform an encryption of the concatenation of the first line of "seeds.txt" and the assigned timestamp. A new python program named "obfuscator_reverse.py" was created to obtain the previously generated passwords to extract concerning the backup zip files.

```
$ python3 obfuscator_reverse.py

$ mkdir backup_1634405485
$ unzip -P 8c34a71b8ae5c67a2ee309622f4ae28bdcc838f76cf924c994b8b9d719d684ae
backup_1634405485.zip -d backup_1634405485

$ mkdir backup_1634412601
$ unzip -P 0b70142bc4d6bb1a78a0466c4986d18b5e2383f69d0a017f280a5d16c1177a9b
backup_1634412601.zip -d backup_1634412601
$ mkdir backup_1634414401
$ unzip -P e64b1b6ba974f1b1097d767175ff7adaad0cb17caff3f71683cfa7362764ebe4
backup_1634414401.zip -d backup_1634414401
```

File	MD5 Value
obfuscator_reverse.py	a0110191c8098d1c51da253ee1c66b62

Figure 1 - MD5 Values of "obfuscator_reverse.py".

A hidden file named ".bash_history" was found in "charlied_disk.img" at "/home/charlied/". This file stored a list of commands used in the command line by the user in question. This file contained evidence about the commands used, mainly, the download of a zip file named "wetransfer_obfuscator_2021-10-06_2110.zip", the procedure of hiding leaks files using the script "chapman_extract.sh", the execution of the script "backup.sh" which was found earlier and the secure removal of all files used in "/home/charlied/rhfc". It was also acknowledged that the user added a new line to "crontab" file which is known as a job scheduler for Linux. The content of this file was extracted from "/var/spool/cron/crontabs/charlied". This new line regards a new job execution of "bash.sh" every 30 minutes of any given date: "***/30 * * * * /home/charlied/cron_manager/backup.sh**". Later, when inspecting the content of "syslog" at "var/log/" three logs were found regarding backups performed at three different times (**18:31:25, 20:30:01 and 21:00:01**) of the day of 16th October. The first backup was done manually as seen in the bash history and the last two were previously scheduled.

The following commands were performed to find and extract ".bash_history" content:

```
$ fls -o 1052672 charlied_disk.img 434942 -F
$ icat -o 1052672 charlied_disk.img 395585 > bash_history
$ fls -o 1052672 charlied_disk.img 434942 -r | grep “crontabs”
$ fls -o 1052672 charlied_disk.img 566590 -r
$ icat -o 1052672 charlied_disk.img 567365 > crontabs
$ icat -o 1052672 charlied_disk.img 262544 > syslog
```

Inside the second backup file “backup_1634412601.zip”, all five documents related to the football leaks and all files containing the hidden leaked documents were found under the path /home/charlied/rhfc”. This confirms the presence of the leaked files on Mr. Daniels’ computer.

All md5 values of each document found correspond to the same values as the ones computed in the pen drive. These values are presented in the following table:

Document	MD5 Value
bank_statement.pdf	33bd1f8ed5f5692c5bf1e5a87d6110b2
club_memo.pdf	f0882eedb95122f39e692a9397c1f5c5
club_statement.pdf	e02839232a2283ac0843de8ecfc980a0
James_Santos_profile.pdf	44d015d11ecd0ec4ecaa6cb350032d17
supporters_statement.pdf	2be65457105ca324381952538fc94de7

Figure 2 - MD5 Values of leaked documents found in the second backup file.

File	MD5 Value
daft_punk.gif	5305480b1832ad42698bdf91f8c2c8e1
discovery.jpg	8331798d0e376a5336fe6838174e74e8
homework.jpg	8963c92d2f964492ed1c7e9138849ad9
ram.jpg	5c766ce1155a907627355633a9f61340
SNA_Football_Lyrics.mp4	7083c363444daa3b0eb391443320ecd8
ticket.jpg	d8bdf6c05594548670f5cceda02fded2
hbfs.wav	ab7ad5f3427854429ac3a4574197ae0b

Figure 3 - MD5 Values of files containing the hidden leaked documents.

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

From the first backup file “backup_1634405485”, it was observed that Mr. Daniels had previously accessed two forensics tools “seeds.txt” and “obfuscator“, both extracted from a zip file named “wetransfer_obfuscator_2021-10-06_2110.zip”, as seen in “.bash_history”. Both tools were extracted on the 7th of October at 00:08:17 WEST which corresponds to the 6th of October at 23:08:17 UTC. This information was acquired using the following commands and obtaining the corresponding output:

```
$ istat -o 1052672 charlied_disk.img 557188
$ istat -o 1052672 charlied_disk.img 557134
```

```
└─$ istat -o 1052672 charlied_disk.img 557134
inode: 557134
Allocated
Group: 68
Generation Id: 1856252442
uid / gid: 1000 / 1000
mode: rrw-r--r--
Flags: Extents,
size: 452
num of links: 1

Inode Times:
Accessed:       2021-10-16 18:31:53.510266700 (WEST)
File Modified:  2021-10-06 22:11:05.000000000 (WEST)
Inode Modified: 2021-10-16 14:55:34.134601174 (WEST)
File Created:   2021-10-07 00:08:17.278941884 (WEST)
```

```
└─$ istat -o 1052672 charlied_disk.img 557188
inode: 557188
Allocated
Group: 68
Generation Id: 2659279981
uid / gid: 1000 / 1000
mode: rrw-r--r--
Flags: Extents,
size: 2100000
num of links: 1

Inode Times:
Accessed:       2021-10-16 21:00:01.651002556 (WEST)
File Modified:  2021-10-16 21:00:01.495003642 (WEST)
Inode Modified: 2021-10-16 21:00:01.495003642 (WEST)
File Created:   2021-10-07 00:08:17.282941838 (WEST)
```

Figure 4 - Details of “seeds.txt” and “obfuscator” metadata, respectively.

Note that the timestamp corresponding to the modification data of “obfuscator” file was altered to “2021-10-06 22:11:05.000000000” which isn’t in agreement with the creation date of the file.

Later, when analyzing “recently-used.xbel” in “/home/charlied/.local/share/”, two downloads were uncovered regarding new files “backup.sh” and “obfuscator”, on the 16th of October at 13:45:26 UTC and 14:07:38 UTC, respectively. Furthermore, it will be concluded that “obfuscator” was obtained through the link “https://we.tl/t-F1WCkIL3WA”. The previously obtained “obfuscator” file was replaced with this most recent file, which could be confirmed through “obfuscator.trashinfo” file in “/home/charlied/.local/share/Trash/info”.

All the previous files “seeds.txt”, “obfuscator” and “backup.sh” were used in combination to perform the three backups found in the system with an encrypted password.

```
<bookmark href="file:///home/charlied/cron_manager/backup.sh" added="2021-10-16T13:45:26Z" modified="2021-10-16T17:24:29Z" visited="1969-12-31T23:59:59Z">
  <info>
    <metadata owner="http://freedesktop.org">
      <mime:mime-type type="application/x-shellscript"/>
      <bookmark:groups>
        <bookmark:group>gedit</bookmark:group>
      </bookmark:groups>
      <bookmark:applications>
        <bookmark:application name="org.gnome.Nautilus" exec="&apos;gedit %U&apos;" modified="2021-10-16T17:24:26Z" count="9"/>
        <bookmark:application name="gedit" exec="&apos;gedit %u&apos;" modified="2021-10-16T17:24:29Z" count="1"/>
      </bookmark:applications>
    </metadata>
  </info>
</bookmark>
```

```
<bookmark href="file:///home/charlied/Downloads/obfuscator" added="2021-10-16T14:07:38Z" modified="2021-10-16T14:07:38Z" visited="1969-12-31T23:59:59Z">
  <info>
    <metadata owner="http://freedesktop.org">
      <mime:mime-type type="application/octet-stream"/>
      <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;" modified="2021-10-16T14:07:38Z" count="1"/>
      </bookmark:applications>
    </metadata>
  </info>
</bookmark>
```

Figure 5 - Bookmarks with reference to the new downloaded file “backup.sh” and “obfuscator”, recorded in “/home/charlied/.local/share/recently-used.xbel”.

The following commands were used to extract “recently-used.xbel”:

```
$ icat -o 1052672 charlied_disk.img 420010 > recently-used.xbel
```

Following this investigation, it was then proceeded with the analysis of the second backup file “backup_1634414401”. Regarding this, all the subsequent inspected files were found within the second backup file since it corresponds to the backup done immediately before the removal of all manipulated files. Then, the same files were extracted from “charlied_disk.img” to make sure to have the latest modifications.

As known from the previous lab assignment, Mr. Daniel had on his possession a pen drive containing some of the files found on his computer at “/home/charlied/rhfc”. After analyzing the conversation logs in “chapman13.10-16.log” located at “/home/charlied/irclogs/2021/EFNet” it was concluded that this pen-drive was acquired from “chapman13” during a meeting at Jake’s cybercafé between 18:32:08 and 18:54:02 on the 16th of October, which corresponds to the period after the closure of the conversation and between the closure of the session and a new session login for user “charlied”, registered in “auth.log” at “var/log/”.

After acquiring some relevant logs from the disk “charlied_disk.img”, such as “auth.log” and “kern.log”, both at “var/log/”, some information was extracted from “kern.log” regarding a recorded computer login on Oct 16 18:54:02, following the meeting. As observed in “syslog” events, it was introduced a pen drive (SerialNumber: 43F34AADd, Vendor=058f, idProduct=6387) into Mr. Daniel’s computer on Oct 16 19:07:30 and then mounted at “/media/charlied/CHAPMAN1337” on Oct 16 19:07:35, where a zip file named “hawks_fc.zip” containing the suspicious files was copied into “/home/charlied/rhfc” and then extracted, as shown in the bash history.

The extraction of the content of all three log files was performed using the following commands:

```
$ icat -o 1052672 charlied_disk.img 404770 > chapman13.10-16.log
$ icat -o 1052672 charlied_disk.img 262845 > auth.log
$ icat -o 1052672 charlied_disk..img 262544 > syslog
```

Furthermore, it was suspected that a zip file named “1337_tools.zip” was obtained through the link “https://we.tl/t-UA0iKwkxTa” provided by the user “chapman13”. To confirm this suspicion, it was required to access the user’s browser history database, “places.sqlite”. The first SQL table “moz_places” contained multiple entries confirming the access to the website “WeTransfer” with the title of “obfuscator” and “1337_tools.zip”. The second table “moz_annos” contained entries confirming the download of the tool looked for. Although there was no evidence regarding a command-line extraction of the zip file in “.bash_history”, “recently-used.xbel” contained a bookmark concerning the addition of the zip file on the 16th October 2021 at 17:19:45 UTC. This file was also found in the second disk backup under the path “/home/charlied/rhfc” along with the extracted tools “extract_tool.py” and “chapman_extract.sh” meaning that it was moved from “/home/charlied/Downloads”.

The content of the SQL file was accessed with a tool named “DB Browser” and extracted using the following command:

```
$ icat -o 1052672 charlied_disk.img 552464 > places.sqlite
$ sqlitebrowser places.sqlite
```

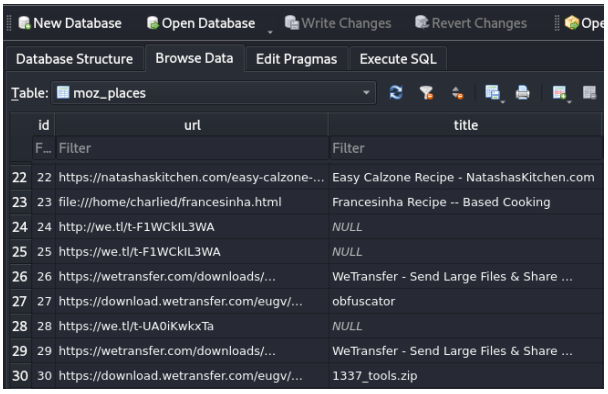


Figure 6 - SQL tables "moz_places" and "moz_annos" presented in "/home/charlied/.mozilla/firefox/zmpu4nds.default-release/places.sql" firefox visited pages and download history.

Figure 7 - Bookmark with reference to the new downloaded file "1337_tools.zip" recorded in "/home/charlied/.local/share/recently-used.xbel".

After obtaining all required tools and files, Mr. Daniel extracted all files in "hawks_fc.zip" and "chants.zip" and then ran the provided tool "chapman_extract.sh" in order to extract all five leaked files mentioned in the first question. Then, he proceeded with the visualization of the obtained files with his predefined application "Document Viewer" to view PDF's documents, using "$ xdg-open ${file}" command, where file corresponds to the current file to be opened. This can be confirmed by looking at the thumbnail's pictures present in "/home/charlied/.cache/thumbnails/large".

On the 16th of October at 20:04, Mr. Daniels notified "chapman13" through IRC chat about his new blog post online regarding the exposure of Levy Fran Velucci's fraudulent actions. The creation of this file was done with the support of the leaked files obtained from "chapman13". It is entitled "Truth in Football" and can be found at "https://truthinfootball.wordpress.com/".

President of the Red Hawks FC Involved in Fraudulent Transfer o Star Player James Santos

At the end of 30th of August, the football community was surprised by the news confirming the transfer of James Santos, the 23-year-old star midfielder of the Red Hawks FC. Most recently relevant documents related to this transfer reached the **Truth in Football** team proving that the president of the Red Hawks FC, Levy Fran Velucci, received 3 million euros in his personal bank account from James Santos' agent, George Sednem, who, in turn, collected an unusually high fee of 8 million euros for the player transfer.

James Santos at the Cyber Football Awards award ceremony.

Figure 8 - Preview of the new Mr. Daniel's blog post at WordPress, "https://truthinfootball.wordpress.com/".

Finally, before meeting up for a celebration for the special occasion, "chapman13" suggested Mr. Daniels to remove all traces of the presence of leaked files. He looked up online an article in "TecMint.com" on "3 Ways to Permanently and SecurelyDelete 'Files and Directories' in Linux". He then proceeded with the safe removal of the leaked files using a Linux tool "`$ srm -vz ~/rhfc/*`" which also overwrites the data with zeros instead of writing random data.

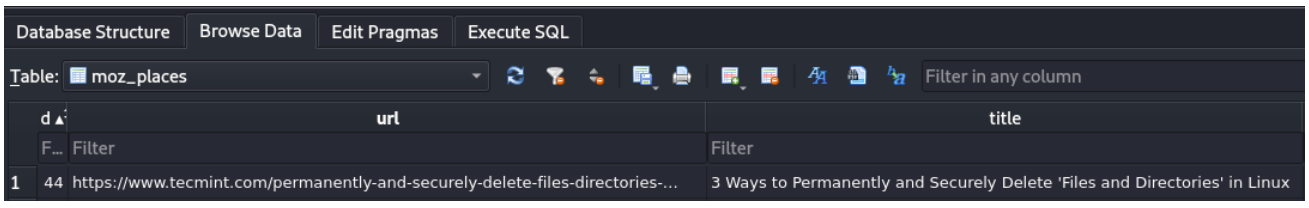


Figure 9 - SQL table "moz_places" regarding a search in the "TecMint.com" website, presented in "places.sql" firefox history at "/home/charlied/.mozilla/firefox/zmpu4nds.default-release".

```
cat extract_instructions.txt
unzip hawks_fc.zip
chmod 777 chapman_extract.sh
./chapman_extract.sh
unzip chants.zip
./chapman_extract.sh
ls -lah
xdg-open James_Santos_profile.pdf
xdg-open supporters_statement.pdf
xdg-open club_statement.pdf
xdg-open bank_statement.pdf
ghex chant2
mv chant2 club_memo.pdf
xdg-open club_memo.pdf
irssi
ls -lah
cd rhfc/
vim secure_delete_commands.txt
ls -lah
cat ~/rhfc/secure_delete_commands.txt
srm -vz ~/rhfc/*
sudo apt install secure-delete
srm -vz ~/rhfc/*
ls -lah
```

Figure 10 - Extraction, visualization and secure removal of leaked files in "/home/charlied/", recorded in ".bash_history" at "/home/charlied/".

The following image represents the timeline regarding the period from when Mr. Daniels obtained the forensic tools and leaked documents until their secure removal. This timeline was established with the support of all logfiles and "recently-used", previously obtained. Linux command "istat" was also used to display the details of a given inode meta-data structure. This timeline considers the differents timezones regarding all the documents extracted since its timezone was set to Europe/London in "/etc/timezone" (WEST/GMT+1). This meant all events covered in log files were also set according to this timezone, including conversation logs. In order to maintain a consistent timeline, the following events are recorded with the WEST timezone.

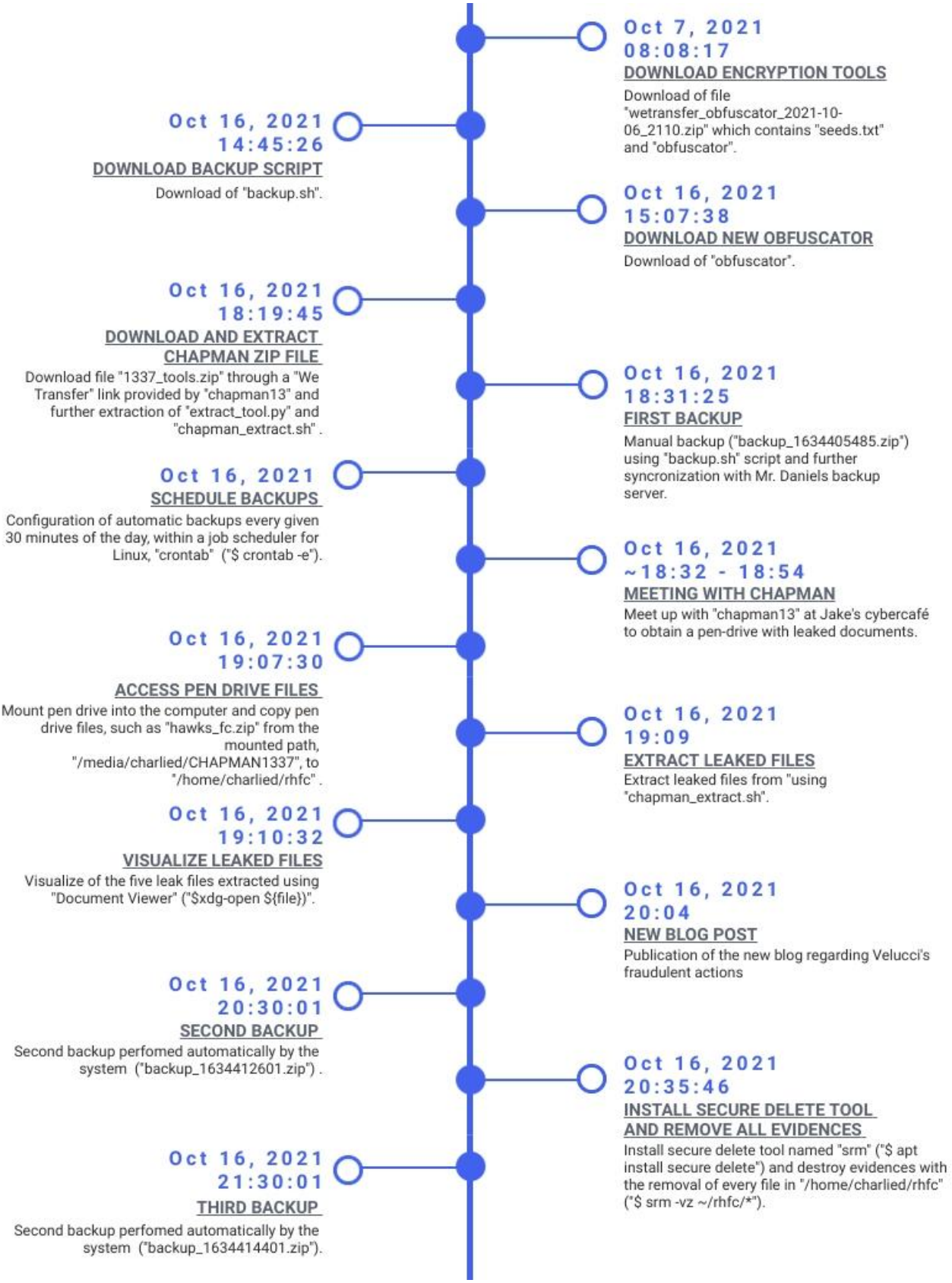


Figure 11 - Timeline regarding all relevant events regarding Mr. Daniel's suspicious activity.

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

Yes, multiple examples of anti-forensic activity were found.

A tool named “obfuscator” that was used to generate encrypted passwords, based on a given timestamp was also found inside “/home/charlied/password_gen/”. The passwords were used to protect the backup zip files generated with the “backup.sh” script so that only Mr. Daniels could extract them later on. Later, this tool “obfuscator” was deleted by the “charlied” user. To recover the passwords of the zip files a reverse script “obfuscator_reverse.py”, created during the investigation, was used, resulting in the passwords shown below:

```
8c34a71b8ae5c67a2ee309622f4ae28bdcc838f76cf924c994b8b9d719d684ae
0b70142bc4d6bb1a78a0466c4986d18b5e2383f69d0a017f280a5d16c1177a9b
e64b1b6ba974f1b1097d767175ff7adaad0cb17caff3f71683cfa7362764ebe4
```

Figure 12 - Encrypted passwords obtained using “obfuscator_reverse.py”.

From the IRC chat log it is known that the user chapman sent a link to Charlie with a zip file named “1337_tools.zip” containing a script named “chapman_extract.sh” and a python program “extract_tool.py” to extract hidden files.

```
18:19 <chapman13> By the way, download this tool so you can get access to this files without anyone suspecting of you.
18:19 <chapman13> https://we.tl/t-UA0iKwkxTa
18:19 <charlied> done
18:20 <chapman13> Amazing!
18:20 <chapman13> You just unzip the tool on the ir-ssame directory as the red hawks files.
18:20 <chapman13> And then you run the script chapman_extract.sh
```

Figure 13 - Conversation log with “chapman13” regarding a shared link.

These tools were able to recover hidden files from unsuspected files. This way, no one would notice the presence of the leaked files with a superficial analysis.

After the publication of the new blog, “chapman13” recommended Mr. Daniels to delete the extracted files since they wouldn’t be no longer needed and anyone could suspect the activity. Mr. Daniels saved the procedure of the removal of the command within a text file named “secure_delete_commands.txt” that was discovered inside the second backup “backup_1634412601.zip”. This file contains a tutorial on how to completely delete the contents of the directory “ ~/rhfc”, and overwrite it with zeros. This method was used as an anti-forensic tool in order to delete any traces of the presence of the leaked files in the computer. The tool used is presented in the following image:

```
20:04 <chapman13> Please, delete the files that were hidden within the Daft Punk album covers.
20:05 <charlied> you mean all the pdfs i extracted?
20:05 <chapman13> Yes
20:06 <chapman13> I mean, hidden within all files I sent you...
```

Figure 14 - Conversation log with “chapman13” regarding the removal of the leaked files.

```
srm -vz ~/rhfc/*
```

Figure 15 - Linux tool to remove leaked files as evidence.

Adding to the deletion of the files within "/home/charlied/rhfc/", an assumption was made three files were previously renamed. It is suspected that these files correspond to the anti-forensic tools used by Mr. Daniels since there were present in the same directory of the second backup "backup_1634412601.zip".

The three anti-forensic tools present in the backup file that were suspected to have been renamed are "chapman_extract.sh", "extract_tool.py" and "1337_tools.zip".

The three files listed in "charlied_disk.img" in the same folder are presented as the following:

- "drqoid.xsd"
- "mydxwzfivvvaloc.zv"
- "ozgivkdthslzms.nbv"

This was observed using the following tool to list all files in "charlied_disk.img" at "/home/charlied/rhfc/":

```
$ fls -o 1052672 charlied_disk.img -F 434898
```

```
└─$ fls -o 1052672 charlied_disk.img -F 434898
r/r * 404856:   drqoid.xsd
r/r * 397778:   extract_instructions.txt
r/r * 397780:   extract_tool.py
r/r * 398254:   hawks_fc.zip
r/r * 398255:   chants.zip
r/r * 399244:   daft_punk.gif
r/r * 404851:   discovery.jpg
r/r * 404852:   hbfs.wav
r/r * 404853:   homework.jpg
r/r * 404854:   ram.jpg
r/r * 404855:   SNA_Football_Lyrics.mp4
r/r * 404856:   ticket.jpg
r/r * 397777:   mydxwzfivvvaloc.zv
r/r * 404860:   club_statement.pdf
r/r * 404861:   data.zip
r/r * 404862:   James_Santos_profile.pdf
r/r * 419418:   chant2
r/r * 419448:   chant1.wav
r/r * 419456:   supporters_statement.pdf
r/r * 419418:   club_memo.pdf
r/r * 404857:   ozgivkdthslzms.nbv
r/r * 422938:   secure_delete_commands.txt
```

Figure 16 - List of all deleted files inside "/home/charlied/rhfc/" in "charlied_disk.img"

Furthermore, it was found, using the "istat" tool of the inode corresponding to "obfuscator" in "charlied_disk.img" at "/home/charlied/password_gen", that the date of modification of this tool was altered to "2021-10-06 22:11:05.000000000" which isn't in agreement with the creation date of the file, as we can see in the 3rd Figure. No concrete evidence regarding the reason for this action was found but it was suspected that this was done to cover the traces about when the tool was used.

4 What can you tell about the identity of the person(s) involved in the leakage of the files?

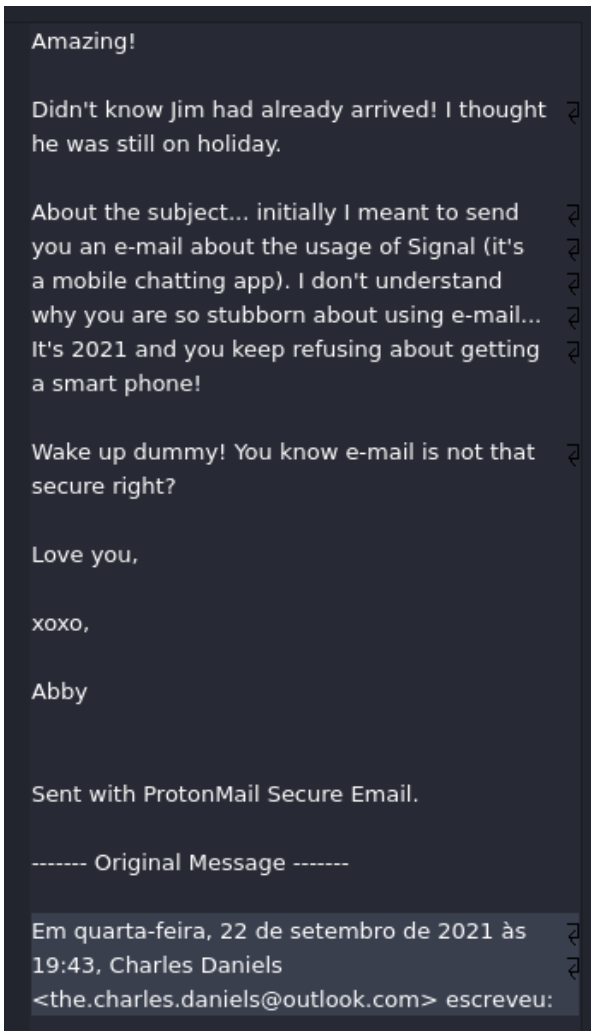
There are three relevant log files inside the third backup file, at "/home/charlied/irclogs/2021/EFNet". After digging deeper into "chapman13.10-16.log" it is found a conversation between "charlied" and a user named "chapman13". who apparently may be partners in a romantic relationship.

Later, inside the backup zip files, it was found a SQL file "global-messages-db.sqlite" containing the history of Mr. Daniels email INBOX history. This file reveals a plethora of old emails, from September of 2021, exchanged between Charlie and other people. Within those emails, a couple of emails were exchanged with the "chapman" user which is sometimes referred to as Abby, which might be her real name.

The content of the SQL file was accessed with a tool named "DB Browser" and extracted using the following command:

```
$ icat -o 1052672 charlied_disk.img 419525 > global-messages-db.sqlite
$ sqlitebrowser global-messages-db.sqlite
```

The content of the emails exchanged between both users are in SQL Table "messagesText_content" in "/home/charlied/.thunderbird/largus1u.default-release", as presented in the following images:



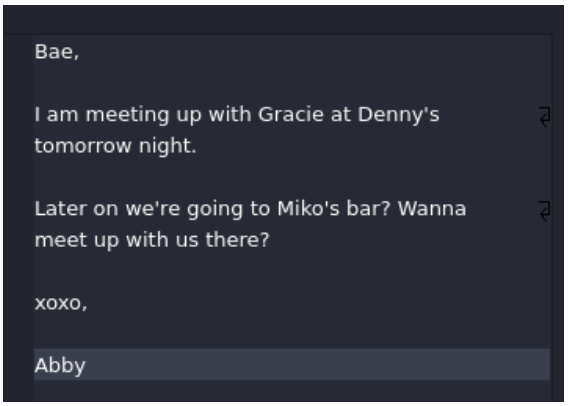


Figure 17 - Emails exchanged between 'charlied' (Mr. Daniels) and 'chapman13' (Abby).

From these emails, it is possible to extract Mr. Daniel's emails and more importantly the email from the chapman user.

The following emails addresses were obtained through the emails exchanged between:

- Mr. Daniels, known as "charlied": the.charles.daniels@outlook.com
- Abby, known as "chapman13": chapmanabby1337@protonmail.com

On the 16th of October, Mr. Daniel's met up with Abby at Jake's cybercafé, where she gave him a pen drive containing the hidden leaked files, as seen in the conversation log between both of them. During the investigation, there were obtained several pieces of information about the pen-drive given to Mr. Daniels when analyzing "kern.log" at "/var/log/".

- "SerialNumber: 43F34AADd"
- "Vendor=058f"
- "idProduct=6387"

This sensitive information can be further used to pursue an investigation regarding Abby's possessions.

To conclude, Abby, "chapman13" was the identity responsible for leaking and providing the leaked files to Mr. Daniels, "charlied". It is known that Abby doesn't live too far from Jake's cybercafé and Miko's bar.

5. Extracted files and auxiliary tools

The following table contains the Disk Name, Partition Sector and Inode origin as well as the MD5 value computed using the Linux command "md5sum" for all remaining relevant files extracted during the analysis of this case:

File	Source | Disk	Partition Sector	Inode	MD5 Value
backup_1634405485.zip	backup_disk.img	2048	168635	916d0381116ab59948e62c32d6fa6ad9
backup_1634412601.zip	backup_disk.img	2048	168646	fd91a7a26cf58b99ab5488227542858b
backup_1634414401.zip	backup_disk.img	2048	168650	9b11a2fdd0c636e443b9bd59a7828f2e
backup.sh	charlied_disk.img	1052672	423847	00c4155996496ed94488d7f37feb5ce3
obfuscator1 (trash)	charlied_disk.img	1052672	557134	d52c5ac8132e93ab77f534b98a610e97
obfuscator2 (most recent)	charlied_disk.img	1052672	264702	8c682b97daf72a9a555758d6a8c85f8e
seeds.txt	charlied_disk.img	1052672	557188	1192989e7df0e4701d9d97beba5338bf
bash_history	charlied_disk.img	1052672	395585	0f50cc7b81f81344840c09e008ec894a

crontabs_charlied	charlied_disk.img	1052672	434942	b2379e6f640fac7ea08cca654d5fd8b7
chapman13.10-16.log	charlied_disk.img	1052672	404770	6de001cd9a5042649e4d075673ba9afa
config	charlied_disk.img	1052672	397765	a50f1667bc48a8cc89fcb8a3a9f729ce
auth.log	charlied_disk.img	1052672	262845	61d0ecf0811327d96a211e775144ba38
syslog	charlied_disk.img	1052672	262544	97936704ef7290537e39c139aaa1fe69
history.log	charlied_disk.img	1052672	566563	8f26943569e78088ea18fd692cc6368b
kern.log	charlied_disk.img	1052672	262662	8d8d52b6039299106aeaad4bcb41cfb6
global-messages-db.sqlite	charlied_disk.img	1052672	419525	2a92e0a94f088db09fa1c76610cf0ed5
places.sqlite	charlied_disk.img	1052672	552464	1d97509db85b02f2a03b41ab0ff417f1
passwd-	charlied_disk.img	1052672	263661	aa14dea2367e7debe6558163b57e25d0
shadow-	charlied_disk.img	1052672	263698	aefe37d707981ca578623442f9d676ed
timezone	charlied_disk.img	1052672	262384	27fb759573780869d660f67032dc7
recently-used	charlied_disk.img	1052672	420010	bf0fee6fe5dc0ab6293e2b2f85240228
thunderbird_logins.json	charlied_disk.img	1052672	419611	df3367149813223c26539b6b8f06626a
obfuscator.trashinfo	charlied_disk.img	1052672	420229	6e14a868038303976dc43de1c07e6fe4

Figure 18 - Table regarding Disk Name, Partition Sector, Inode from where each file was obtained and their respective MD5 Value.

All analyzed files during this investigation are attached inside “extracted”, as well as two auxiliary tools “obfuscator_reverse.py” and “extract.sh” inside “tools”. The last script performs the extraction of all accessed files in “charlied_disk.img” and “backup_disk.img” as well as the leaked files involved in this case, shared by “chapman13” and computes all corresponding md5 values presented in the previous tables.