Cisco And Evasion

Challenge by Théo ‘feloeht’ LEFEVRE

Step 1: Download and analyse the image.
The statement tells us about a technician who has taken an image of a suspect piece of equipment.
One can either expect a disk image or a memory image.

After downloading the latter, we realise that it is a gzip-compressed archive, we unzip it.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ file device.img.gz
device.img.gz: gzip compressed data, was "device.img", last modified: Tue May 10 22:52:10 2022, max compression, from Un
ix, original size modulo 2^32 3166699520
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ gzip -dk device.img.gz
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ file device.img
device.img: Linux rev 1.0 ext4 filesystem data, UUID=99f9cf68-e6fa-4b90-aeee-7fa3e9ed5c2d, volume name "rootfs" (extents
) (large files)
```

We mount the filesystem:

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ mkdir cisco && sudo mount -o loop device.img cisco
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ ls -la cisco/
total 84
drwxr-xr-x 19 root    root     4096 May 11 00:23 .
drwxrwxrwx  1 feloeht feloeht  4096 May 11 15:44 ..
lrwxrwxrwx  1 root    root        7 Apr  4 13:45 bin -> usr/bin
drwxr-xr-x  2 root    root     4096 Apr  4 14:05 boot
drwxr-xr-x  4 root    root     4096 Apr  4 13:45 dev
drwxr-xr-x 87 root    root     4096 May  8 18:38 etc
drwxr-xr-x  3 root    root     4096 Apr  4 14:07 home
lrwxrwxrwx  1 root    root        7 Apr  4 13:45 lib -> usr/lib
drwx------  2 root    root    16384 Apr  4 14:05 lost+found
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 media
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 mnt
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 opt
drwxr-xr-x  2 root    root     4096 Mar 27 05:33 proc
drwx------  3 root    root     4096 May  8 18:09 root
drwxr-xr-x  5 root    root     4096 Apr  4 13:50 run
lrwxrwxrwx  1 root    root        8 Apr  4 13:45 sbin -> usr/sbin
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 srv
drwxr-xr-x  2 root    root     4096 Mar 27 05:33 sys
drwxrwxrwx  2 nobody  nogroup  4096 May 11 00:23 tftpboot
drwxrwxrwt  9 root    root     4096 May 10 01:00 tmp
drwxr-xr-x 11 root    root     4096 Apr  4 13:45 usr
drwxr-xr-x 11 root    root     4096 Apr  4 14:06 var
```

We are basically trying to get an idea of what may have happened on this system:

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ ls -la home/
total 12
drwxr-xr-x  3 root    root    4096 Apr  4 14:07 .
drwxr-xr-x 19 root    root    4096 May 11 00:23 ..
drwxr-xr-x  3 feloeht feloeht 4096 May 10 12:55 h4x0r
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ ls -la home/h4x0r/
total 142188
drwxr-xr-x 3 feloeht feloeht      4096 May 10 12:55 .
drwxr-xr-x 3 root    root         4096 Apr  4 14:07 ..
-rw------- 1 feloeht feloeht       647 May 10 12:19 .bash_history
-rw-r--r-- 1 feloeht feloeht       220 Apr  4 13:48 .bash_logout
-rw-r--r-- 1 feloeht feloeht      3523 Apr  4 13:48 .bashrc
drwxr-xr-x 3 feloeht feloeht      4096 May  8 18:05 .local
-rw-r--r-- 1 feloeht feloeht       807 Apr  4 13:48 .profile
-rw-r--r-- 1 feloeht feloeht       215 May  8 17:49 .wget-hsts
-rw-r--r-- 1 feloeht feloeht   5636152 May 10 12:53 capture.pcapng
-rw-r--r-- 1 feloeht feloeht 139921525 May  8 17:49 rockyou.txt
```

We notice some activity in the h4x0r home directory, so we decide to find out more:

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat home/h4x0r/.bash_history
sudo apt install hydra-gtk
wget https://raw.githubusercontent.com/praetorian-inc/Hob0Rules/master/wordlists/rockyou.txt.gz
gzip -d rockyou.txt.gz
sudo hydra -p rockyou.txt 10.0.10.1 cisco
sudo apt install telnet
telnet 10.0.10.1
sudo apt install xinetd tftpd tftp
sudo nano /etc/xinetd.d/tftp
sudo mkdir /tftpboot
sudo chmod -R 777 /tftpboot
sudo chown -R nobody /tftpboot
sudo /etc/init.d/xinetd start
telnet 10.0.10.1
sudo cp /tftpboot/sw-office-paris-confg /tftpboot/sw-office-paris-new
sudo nano /tftpboot/sw-office-paris-new
telnet 10.0.10.1
sudo apt-get install vlan tcpdump
sudo tcpdump -B 16096 -i eth1 -w capture.pcapng &feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$
```

At this point, we can either go straight to the endpoint, and explore the pcapng capture, or we can choose to learn a little more, and explore different referenced files.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat etc/xinetd.d/tftp
service tftp
{
protocol        = udp
port            = 69
socket_type     = dgram
wait            = yes
user            = nobody
server          = /usr/sbin/in.tftpd
server_args     = /tftpboot
disable         = no
}
```

This file is just a tftp configuration, which points to the /tftpboot directory.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ ls -la tftpboot/
total 28
drwxrwxrwx  2 nobody nogroup 4096 May 11 00:23 
drwxr-xr-x 19 root   root    4096 May 11 00:23 ..
-rw-r--r--  1 root   root    8195 May  9 00:37 sw-office-paris-confg
-rw-r--r--  1 root   root    8186 May 10 12:55 sw-office-paris-new
```

In this directory we find two files, we choose to study them by date.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat tftpboot/sw-office-paris-confg
Current configuration : 8173 bytes
!
! Last configuration change at 00:55:46 UTC Mon Mar 1 1993 by cisco
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW-Office-Paris
!
boot-start-marker
boot-end-marker
!
!
```

This is a configuration file for a Cisco switch, which could obviously be recovered following a bruteforce attack on the telnet administration interface using hydra and rockyou in the history. We can therefore deduce that the second file contains this modified configuration, so we are trying to understand what was modified.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ diff tftpboot/sw-office-paris-confg tftpboot/sw-office-paris-new
1,4d0
< Current configuration : 8173 bytes
< !
< ! Last configuration change at 00:55:46 UTC Mon Mar 1 1993 by cisco
< !
359a356,357
> monitor session 1 source vlan 10 both
> monitor session 1 destination interface GigabitEthernet0/47
```

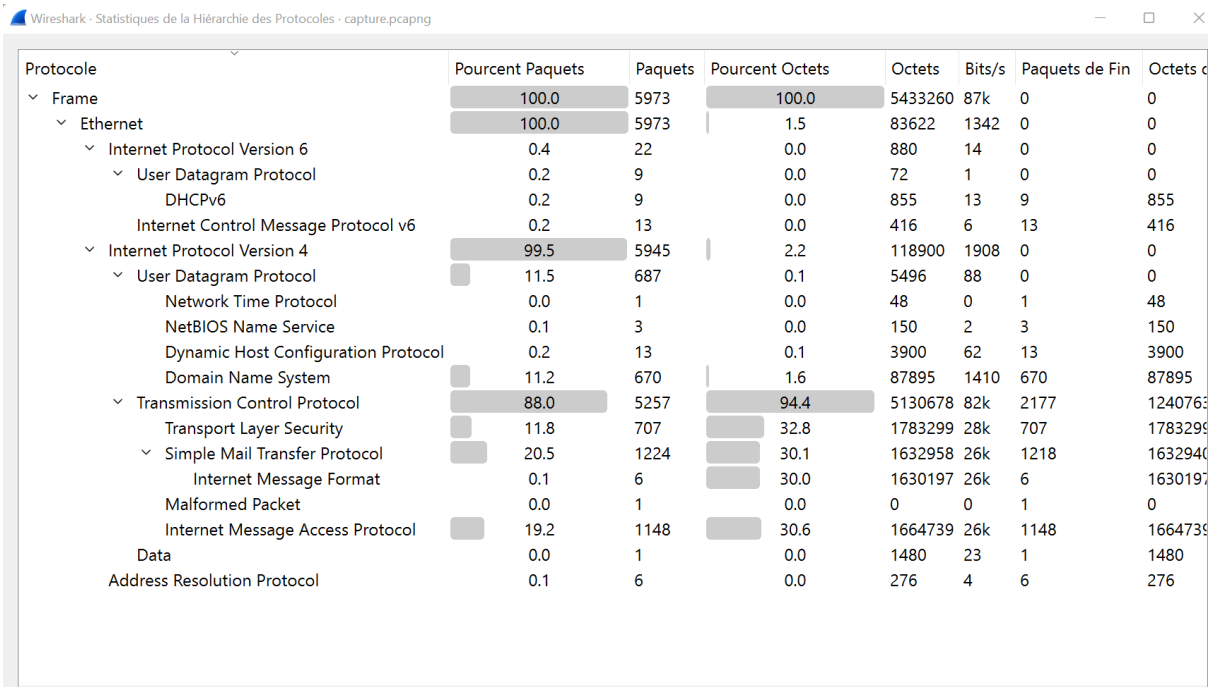
Apart from the deletion of the dating comments, we note the addition of cisco port-monitoring instructions, copying all traffic from vlan 10 to interface 47.
We can therefore deduce that a sniffer device has been connected to this same port in order to retrieve the traffic from vlan 10.

```
interface Vlan10
 description SERVERS
 ip address 10.0.10.1 255.255.255.0
!
interface Vlan20
 description DIRECTION
 ip address 10.0.20.1 255.255.255.0
!
interface Vlan30
 description COLLABORATORS
 ip address 10.0.30.1 255.255.255.0
!
interface Vlan100
 description INTERCO-WAN
 ip address 172.16.100.100 255.255.255.0
!
ip default-gateway 172.16.100.254
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.100.254
!
```

According to the previous configuration, we discover that VLAN 10 is named VLAN SERVERS, it is thus a question of spying on the traffic to and from the servers (both).

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat home/h4x0r/.bash_history
sudo apt install hydra-gtk
wget https://raw.githubusercontent.com/praetorian-inc/Hob0Rules/master/wordlists/rockyou.txt.gz
gzip -d rockyou.txt.gz
sudo hydra -p rockyou.txt 10.0.10.1 cisco
sudo apt install telnet
telnet 10.0.10.1
sudo apt install xinetd tftpd tftp
sudo nano /etc/xinetd.d/tftp
sudo mkdir /tftpboot
sudo chmod -R 777 /tftpboot
sudo chown -R nobody /tftpboot
sudo /etc/init.d/xinetd start
telnet 10.0.10.1
sudo cp /tftpboot/sw-office-paris-confg /tftpboot/sw-office-paris-new
sudo nano /tftpboot/sw-office-paris-new
telnet 10.0.10.1
sudo apt-get install vlan tcpdump
sudo tcpdump -B 16096 -i eth1 -w capture.pcapng &feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$
```

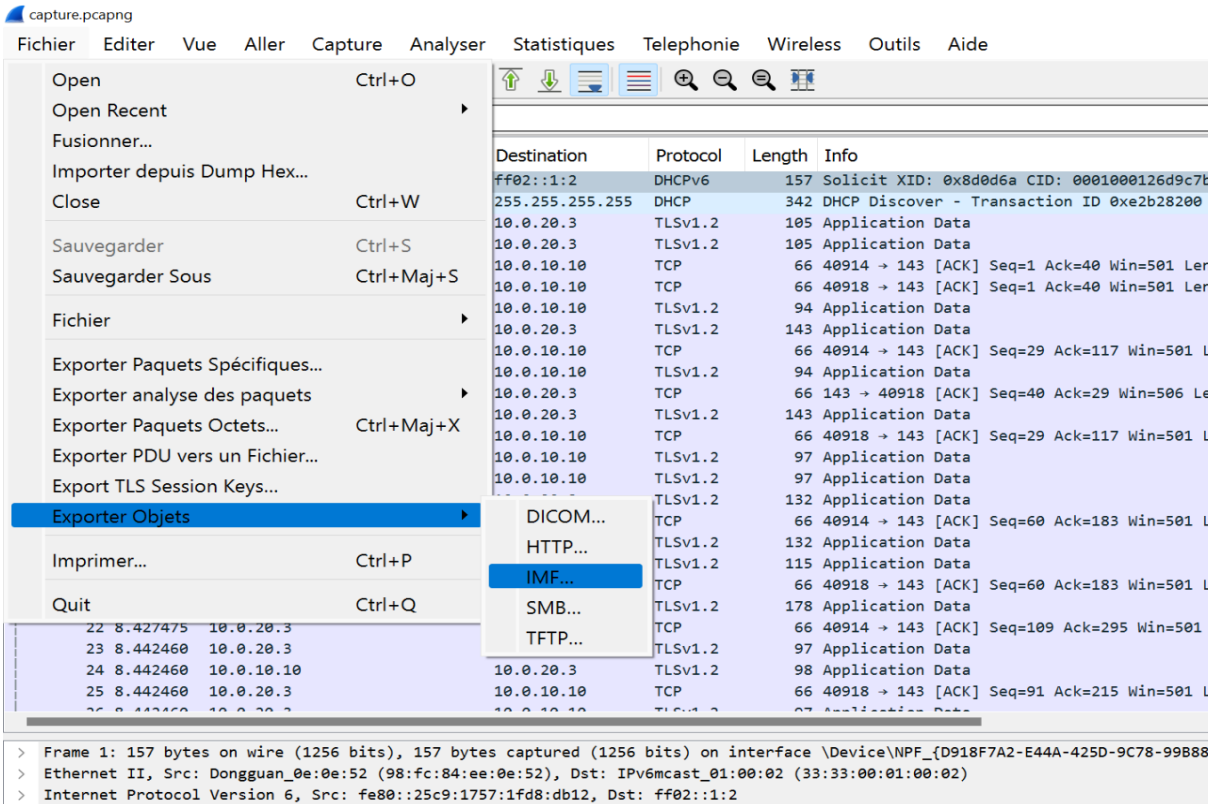
If we look at the config again, we can see that a network capture is being executed, saved in the file capture.pcapng. It therefore seems sensible to look at this file.

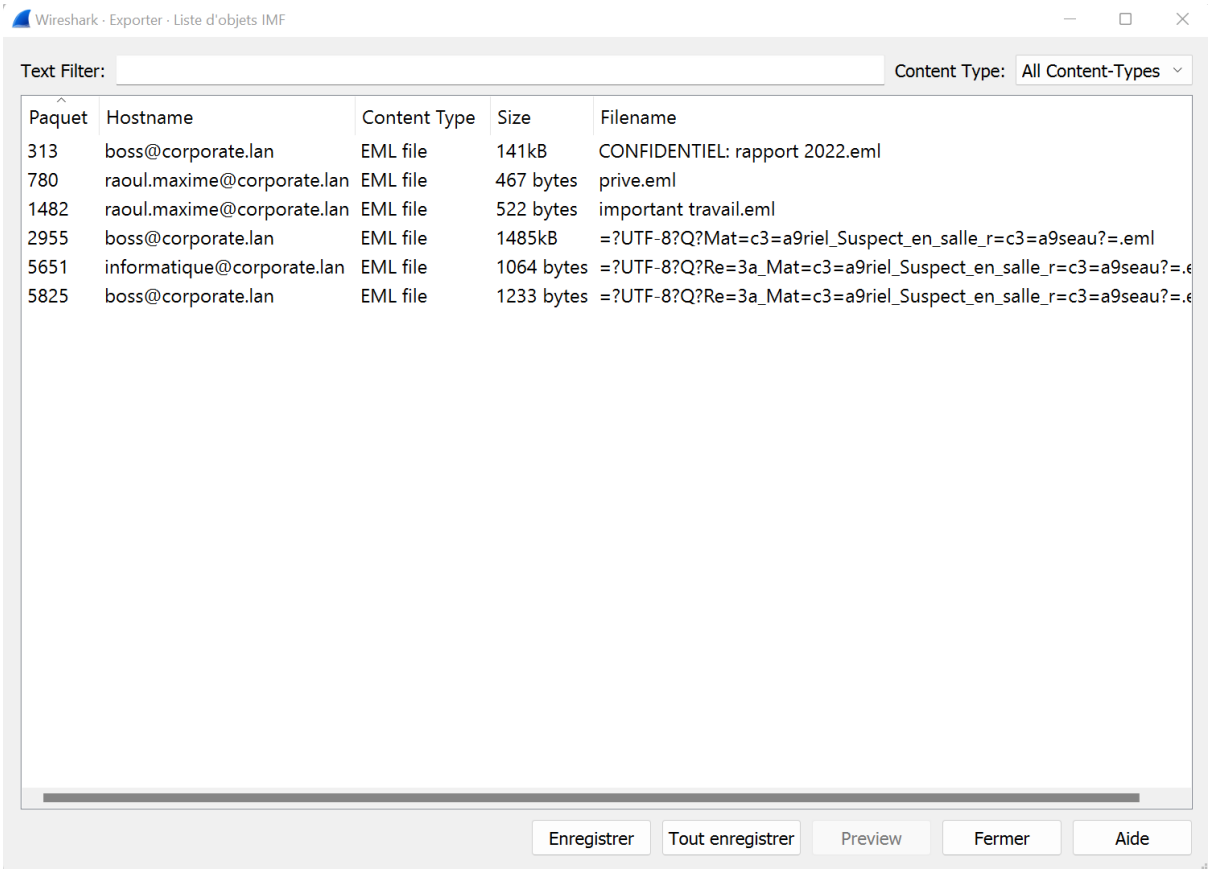


Protocole	Pourcent Paquets	Paquets	Pourcent Octets	Octets	Bits/s	Paquets de Fin	Octets d
Frame	100.0	5973	100.0	5433260	87k	0	0
Ethernet	100.0	5973	1.5	83622	1342	0	0
Internet Protocol Version 6	0.4	22	0.0	880	14	0	0
User Datagram Protocol	0.2	9	0.0	72	1	0	0
DHCPv6	0.2	9	0.0	855	13	9	855
Internet Control Message Protocol v6	0.2	13	0.0	416	6	13	416
Internet Protocol Version 4	99.5	5945	2.2	118900	1908	0	0
User Datagram Protocol	11.5	687	0.1	5496	88	0	0
Network Time Protocol	0.0	1	0.0	48	0	1	48
NetBIOS Name Service	0.1	3	0.0	150	2	3	150
Dynamic Host Configuration Protocol	0.2	13	0.1	3900	62	13	3900
Domain Name System	11.2	670	1.6	87895	1410	670	87895
Transmission Control Protocol	88.0	5257	94.4	5130678	82k	2177	124076
Transport Layer Security	11.8	707	32.8	1783299	28k	707	178329
Simple Mail Transfer Protocol	20.5	1224	30.1	1632958	26k	1218	163294
Internet Message Format	0.1	6	30.0	1630197	26k	6	163019
Malformed Packet	0.0	1	0.0	0	0	1	0
Internet Message Access Protocol	19.2	1148	30.6	1664739	26k	1148	166473
Data	0.0	1	0.0	1480	23	1	1480
Address Resolution Protocol	0.1	6	0.0	276	4	6	276

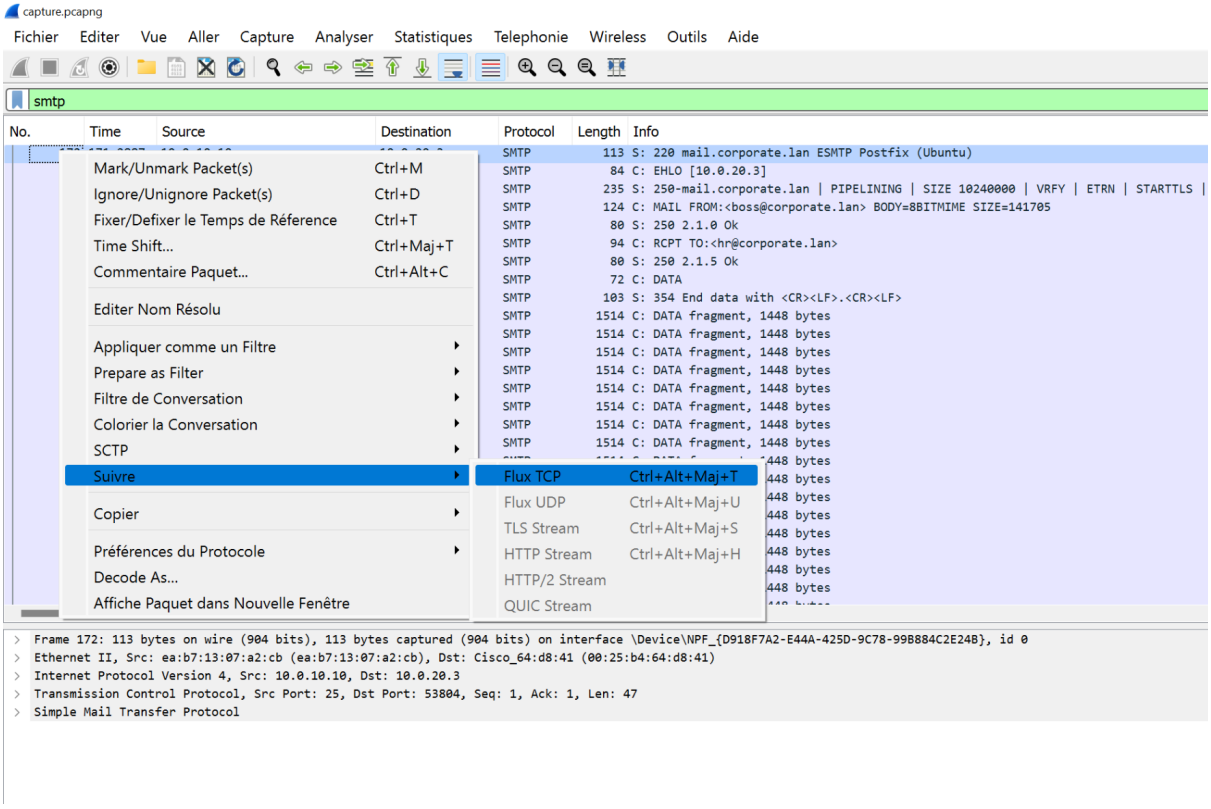
A quick statistical analysis of the protocols shows an important use of TCP, UDP, DNS... but nothing exciting, however, we notice the significant presence of SMTP!

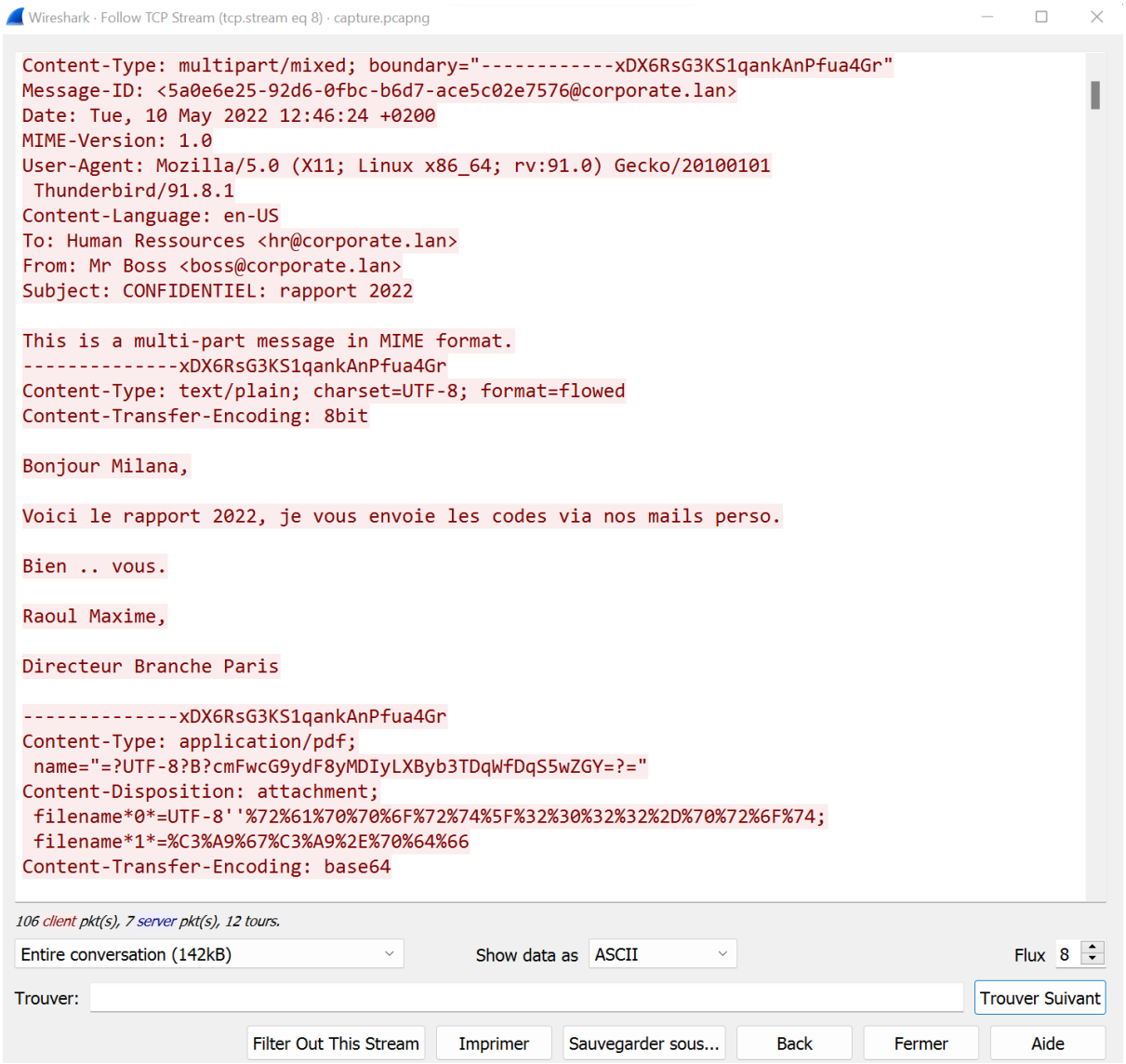
At this stage, there are two solutions, either we know the tricks and we export objects, or we trace the SMTP frames in order to automatically reconstitute the exchanges or not.



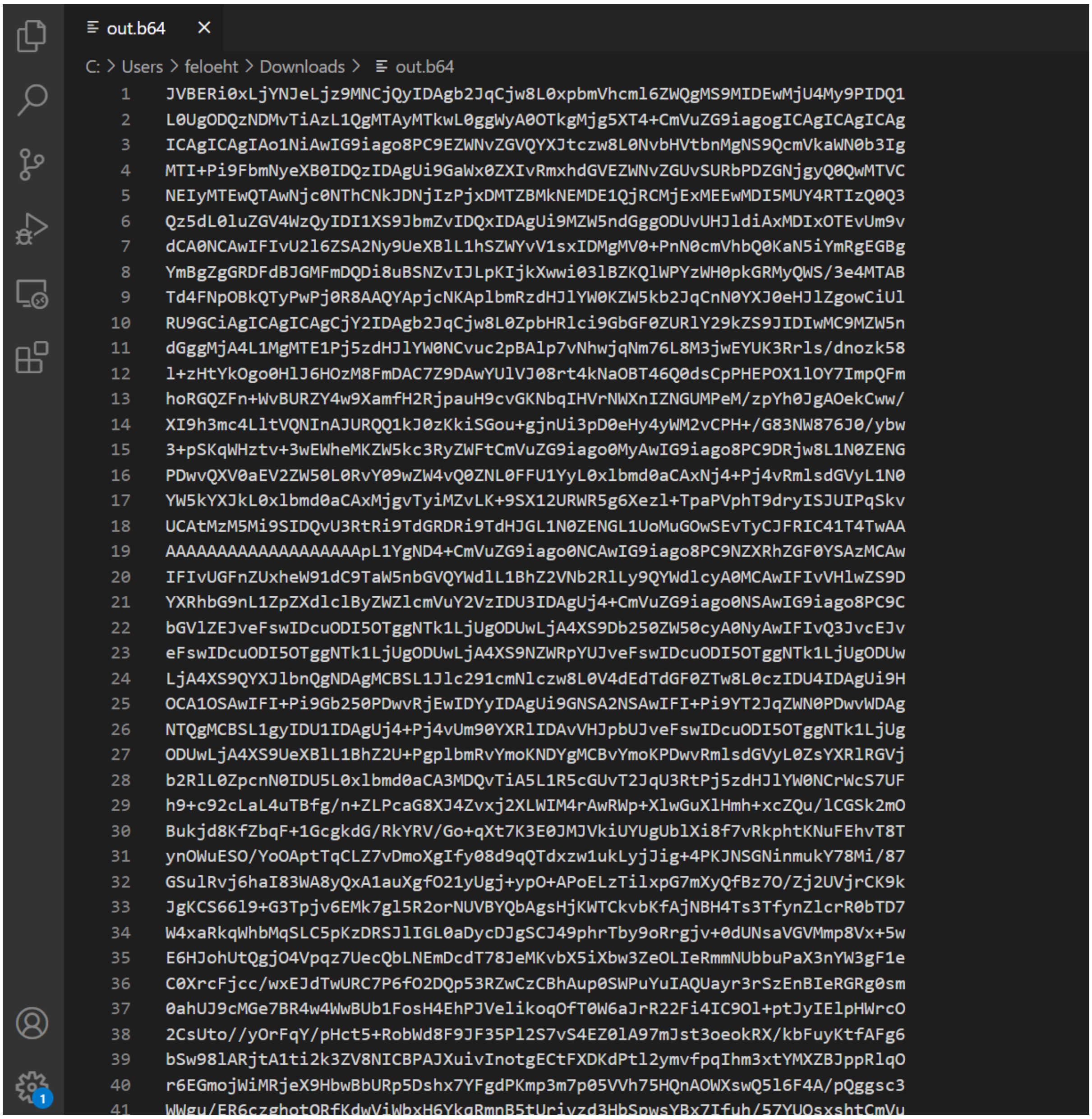


With this solution you can directly export the mails and continue the challenge.
Here is the second solution.

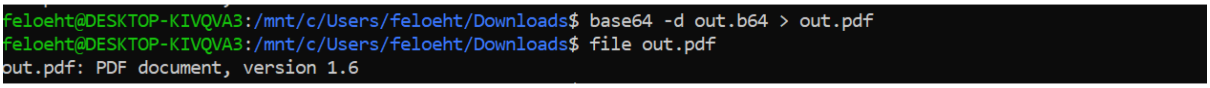




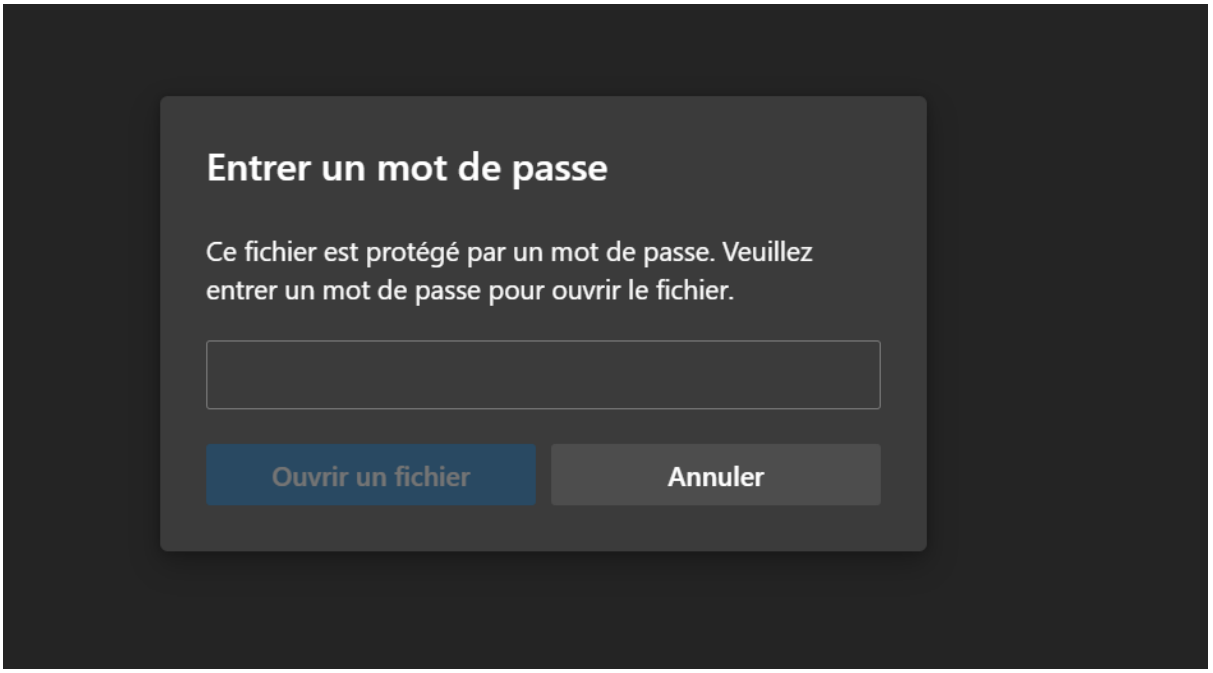
We can now discover the contents of the first message, which seems to contain a password file. It is therefore a question of extracting this file, in a way that suits us.
One way to do this is to export the conversation in ASCII, or RAW, and keep only the part containing the file, encoded in base64.



After deleting the rest of the message, only the base64 code remains.



We get a PDF, let's open it!



Unfortunately it is password protected. We remember reading that the password is sent in another email. Let's look for this email.

We find in another exchange the password in clear text, which allows us to open the PDF containing the flag.

The aim of this challenge is to show both the problems linked to the physical security of a network, as well as the importance of using encrypted protocols, which is currently not sufficiently the case.