“FakeBank”

Forensic Case

By Omri Braja

Answers Sheet

Part I

Network Forensics

1> Tools:

1. #> **tshark -r <filename.pcap> -T fields -e ip.src | grep -E '^(10.10)' | sort -u**

```
10.10.0.1
10.10.0.19
10.10.0.20
10.10.0.20,10.10.0.39
10.10.0.20,213.57.22.5
10.10.0.20,213.57.2.5
10.10.0.32
10.10.0.32,213.57.22.5
10.10.0.37
10.10.0.38
10.10.0.38,213.57.2.5
10.10.0.39
10.10.0.39,10.10.0.1
10.10.0.40
gakusei@gakusei-VirtualBox:~/Desktop/Pcaps$
```

2. #> **tshark -r <filename.pcap> -Y 'nbss'**

```
37584 1352.390627   10.10.0.39 139 10.10.0.38   51468 SMB 97 LogOff AndX Response
38226 1492.720217   10.10.0.20 50959 10.10.0.38   139 NBSS 126 Session request, to ALICE-PC<20> from DAVID-PC<00>
38227 1492.720409   10.10.0.38 139 10.10.0.20   50959 NBSS 60 Positive session response
38228 1492.722069   10.10.0.20 50959 10.10.0.38   139 SMB 127 Negotiate Protocol Request
38229 1492.722698   10.10.0.38 139 10.10.0.20   50959 SMB2 228 Negotiate Protocol Response
38230 1492.722783   10.10.0.20 50959 10.10.0.38   139 SMB2 232 Negotiate Protocol Request
38231 1492.723124   10.10.0.38 139 10.10.0.20   50959 SMB2 228 Negotiate Protocol Response
38322 1495.208966   10.10.0.20 50963 10.10.0.39   139 NBSS 126 Session request, to BOB-PC<20> from DAVID-PC<00>
38323 1495.209630   10.10.0.39 139 10.10.0.20   50963 NBSS 60 Positive session response
38324 1495.209815   10.10.0.20 50963 10.10.0.39   139 SMB 127 Negotiate Protocol Request
38325 1495.211014   10.10.0.39 139 10.10.0.20   50963 SMB2 228 Negotiate Protocol Response
38326 1495.211118   10.10.0.20 50963 10.10.0.39   139 SMB2 232 Negotiate Protocol Request
38327 1495.212026   10.10.0.39 139 10.10.0.20   50963 SMB2 228 Negotiate Protocol Response
60584 1638.274853   10.10.0.40 53436 10.10.0.39   139 NBSS 126 Session request, to BOB-PC<20> from CAROL-PC<00>
60585 1638.274972   10.10.0.39 139 10.10.0.40   53436 NBSS 60 Positive session response
```

Answer:

Command #1 will dump all IP addresses in the specified range;

- **10.10.0.1**
- **10.10.0.19**
- **10.10.0.20**
- **10.10.0.32**
- **10.10.0.37**
- **10.10.0.38**
- **10.10.0.39**
- **10.10.0.40**

Applying an "**nbss" display filter (Command #2)** will output netBIOS data including **host names** and their **designated IP** addresses.

NBSS (netBIOS session service) is a method of connecting between two computers for large data transmission purposses.

Mainly used for printer and file services and runs on TCP port no. 139.

There seem to be Four active hosts in this network;

- **ALICE-PC – 10.10.0.38**
- **BOB-PC – 10.10.0.39**
- **CAROL-PC – 10.10.0.40**
- **DAVID-PC – 10.10.0.20** .

The **10.10.0.1** IP is likely to be a **gateway**.

2> Tools:

#> sudo tcpdump -r <filename.pcap> -nA | grep -i task

```
type=dir;modify=20201001121906; tasks
16:55:21.098148 IP 10.10.0.20.51103 > 192.168.1.112.21: Flags [P.], seq 186:210, ack 1384, win 251, length 24: FTP: CWD /FTP/ezm0n3y/tas
ks
.....p.......{G.GMP....h..CWD /FTP/ezm0n3y/tasks
16:55:21.099951 IP 192.168.1.112.21 > 10.10.0.20.51103: Flags [P.], seq 1384:1448, ack 210, win 2052, length 64: FTP: 250 CWD successful
. "/FTP/ezm0n3y/tasks" is current directory.
......G.GM....P.......250 CWD successful. "/FTP/ezm0n3y/tasks" is current directory.
16:55:21.104278 IP 192.168.1.112.21 > 10.10.0.20.51103: Flags [P.], seq 1448:1496, ack 215, win 2052, length 48: FTP: 257 "/FTP/ezm0n3y/
tasks" is current directory.
......G.G.....P....G..257 "/FTP/ezm0n3y/tasks" is current directory.
16:55:21.116293 IP 192.168.1.112.21 > 10.10.0.20.51103: Flags [P.], seq 1543:1615, ack 227, win 2052, length 72: FTP: 150 Opening data c
hannel for directory listing of "/FTP/ezm0n3y/tasks"
......G.G.....P.......150 Opening data channel for directory listing of "/FTP/ezm0n3y/tasks"
16:55:21.117495 IP 192.168.1.112.21 > 10.10.0.20.51103: Flags [P.], seq 1615:1666, ack 227, win 2052, length 51: FTP: 226 Successfully t
ransferred "/FTP/ezm0n3y/tasks"
......G.H4....P...p:..226 Successfully transferred "/FTP/ezm0n3y/tasks"
This is your tasks folder,
you will get one task at a time
for each task completed,
and the next task will
```

```
.(.......e.].?P....l..257 "/ezm0n3y/tasks" is current directory.
17:00:42.595393 IP 192.168.1.112.21 > 10.10.0.40.53467: Flags [P.], seq 1287:1355, ack 164, win 256, length 68: FTP: 150 Opening data ch
annel for directory listing of "/ezm0n3y/tasks"
.(.........].KP.......150 Opening data channel for directory listing of "/ezm0n3y/tasks"
.(.     ..NS<.L...P...*[..type=file;modify=20201005135636;size=272; TASK01
17:00:42.595731 IP 192.168.1.112.21 > 10.10.0.40.53467: Flags [P.], seq 1355:1402, ack 164, win 256, length 47: FTP: 226 Successfully tr
ansferred "/ezm0n3y/tasks"
.(.........].KP...[z..226 Successfully transferred "/ezm0n3y/tasks"
17:00:57.497026 IP 10.10.0.40.53477 > 192.168.1.112.21: Flags [P.], seq 45:65, ack 282, win 255, length 20: FTP: CWD /ezm0n3y/tasks
.(...p....6.>...q.P...~...CWD /ezm0n3y/tasks
17:00:57.499388 IP 192.168.1.112.21 > 10.10.0.40.53477: Flags [P.], seq 282:342, ack 65, win 2052, length 60: FTP: 250 CWD successful. "
/ezm0n3y/tasks" is current directory.
.(......q.6.>.P.../...250 CWD successful. "/ezm0n3y/tasks" is current directory.
17:00:57.500365 IP 192.168.1.112.21 > 10.10.0.40.53477: Flags [P.], seq 342:386, ack 70, win 2052, length 44: FTP: 257 "/ezm0n3y/tasks"
is current directory.
.(......q.6.>.P.......257 "/ezm0n3y/tasks" is current directory.
17:00:57.503303 IP 10.10.0.40.53477 > 192.168.1.112.21: Flags [P.], seq 84:97, ack 452, win 254, length 13: FTP: RETR TASK01
.(...p....6.>+..r8P....9..RETR TASK01
17:00:57.534296 IP 192.168.1.112.21 > 10.10.0.40.53477: Flags [P.], seq 452:535, ack 97, win 2052, length 83: FTP: 150 Opening data chan
nel for file download from server of "/ezm0n3y/tasks/TASK01"
.(......r86.>8P.......150 Opening data channel for file download from server of "/ezm0n3y/tasks/TASK01"
  TASK1
17:00:57.534296 IP 192.168.1.112.21 > 10.10.0.40.53477: Flags [P.], seq 535:589, ack 97, win 2052, length 54: FTP: 226 Successfully tran
sferred "/ezm0n3y/tasks/TASK01"
.(......r.6.>8P....{..226 Successfully transferred "/ezm0n3y/tasks/TASK01"
17:10:40.215060 IP 10.10.0.20.51150 > 192.168.1.112.21: Flags [P.], seq 1:25, ack 101, ack 493, win 254, length 24: FTP: CWD /FTP/ezm0n3y/tasks
.....p....>>...^..P....h..CWD /FTP/ezm0n3y/tasks
17:10:40.219227 IP 192.168.1.112.21 > 10.10.0.20.51150: Flags [P.], seq 493:557, ack 101, win 256, length 64: FTP: 250 CWD successful. "
/FTP/ezm0n3y/tasks" is current directory.
```

Answer:

The command above will **output all headers and payloads containing the expression** "task" that exists in the capture. You can see that the **"task" files are transferred using the FTP protocol.**

This command also shows the user's **current working directory (CWD)** which is **/ezm0n3y/tasks,** and we can see **downloads of the files "TASK01", "TASK02", "task1comp.txt",** and **"task2comp.txt" from /FTP/ezm0n3y** and **/FTP/ezm0n3y/tasks, made by the user in 10.10.0.40 .**

Downloads are indicated by the **"RETR" flag** and the **"successfully transferred"** messages.

3> Tools:

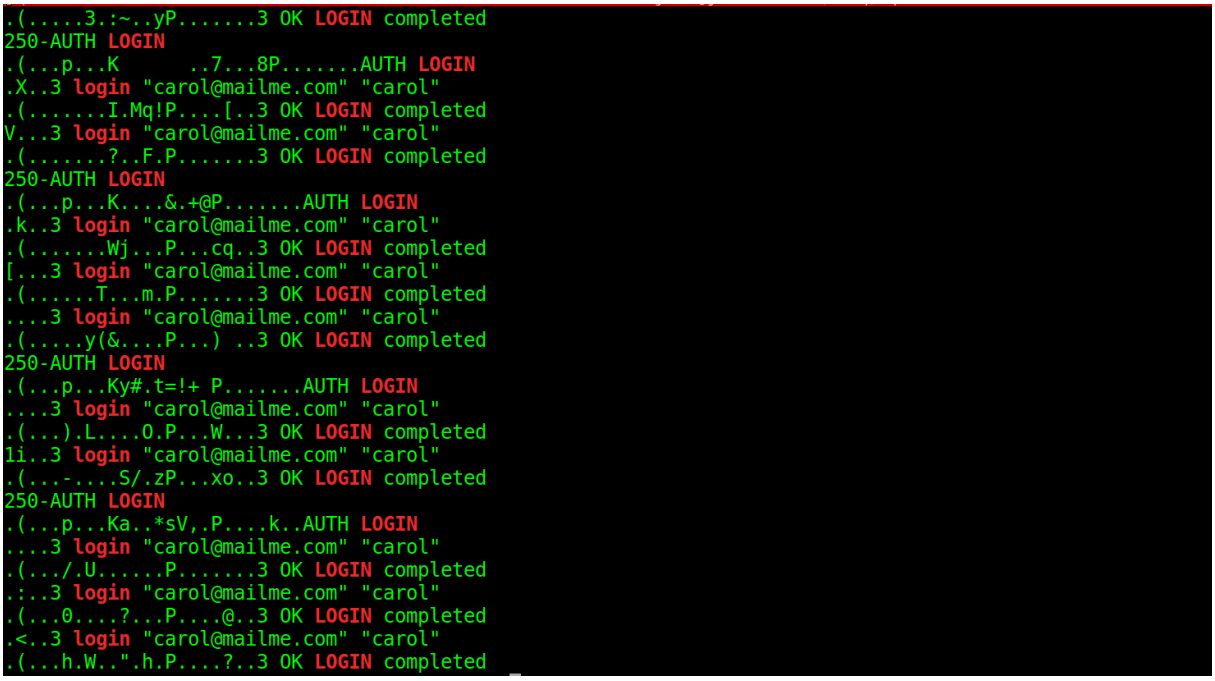
1. #> **tshark -r <filename> -Y ftp -T fields -e ip.src -e ip.dst**

```
10.10.0.20      192.168.1.112
10.10.0.40      192.168.1.112
192.168.1.112   10.10.0.20
192.168.1.112   10.10.0.40
gakusei@gakusei-VirtualBox:~/Desktop/Pcaps$
```

2. #> **sudo tcpdump -r <filename.pcap> -nA | grep -E '<IP_address>' -A 7 > <newfile>**

3. #> **cat <newfile> | grep -i login**

```
.....p...K!].`.M27P....\..AUTH LOGIN
.....p.....=.\`.Q.P....r..3 login "anon@mailme.com" "anon"
......`.Q..=.~P.......3 OK LOGIN completed
.....p......#.%...P....r..3 login "anon@mailme.com" "anon"
......%.....#$P....]..3 OK LOGIN completed
.....p.......$..8P....t..3 login "david@mailme.com" "david"
......$..8....P...Z...3 OK LOGIN completed
17:08:39.974840 IP 10.10.0.20.62965 > 213.57.2.5.53: 2300+ A? login.live.com. (32)
...9.....5.(..............login.live.com.....
17:08:40.016939 IP 10.10.0.20.62965 > 213.57.22.5.53: 2300+ A? login.live.com. (32)
...9.....5.(..............login.live.com.....
17:08:40.121422 IP 213.57.2.5.53 > 10.10.0.20.62965: 2300 10/10/2 CNAME login.msa.msidentity.com., CNAME www.tm.lg.prod.aadmsa.akadns.net., A 40.90.137.120, A 40.90.137.126, A 40.90.137.125, A 40.90.137.127, A 40.90.23.208, A 40.90.23.247, A 40.90.23.154, A 40.90.137.124 (498)
...login.live.com.................login.msa
17:08:40.123772 IP 213.57.22.5.53 > 10.10.0.20.62965: 2300 11/4/4 CNAME login.msa.msidentity.com., CNAME www.tm.lg.prod.aadmsa.trafficmanager.net., CNAME blu-main-ips.b.lg.prod.aadmsa.trafficmanager.net., A 40.90.23.154, A 40.90.137.125, A 40.90.137.120, A 40.90.23.153, A 40.90.23.206, A 40.90.137.126, A 40.90.137.124, A 40.90.23.208 (436)
...5.... ..............login.live.com.................login.msa
...i.........login.live.com..........
..Microsoft Corporation1.0...U....login.live.com0.."0.. *.H.............0..
.....p.......L.y.SP....r..3 login "anon@mailme.com" "anon"
.......y.S...nP....y..3 OK LOGIN completed
.....p.....H..V0.IP....r..3 login "anon@mailme.com" "anon"
......V0.I.H..P...=...3 OK LOGIN completed
.....p.....ys..."3P....t..3 login "david@mailme.com" "david"
........"3.ys:P.......3 OK LOGIN completed
.....p.....~@.fa]OP....r..3 login "anon@mailme.com" "anon"
......fa]O.~@.P.......3 OK LOGIN completed
```



Answer:

Running command #1 we form a list of all **source and destination IP** addresses that **connected in FTP**.

We can see the **server's IP (192.168.1.112)** and that the only two connections to it were from **10.10.0.20 and 10.10.0.40** .

Running command #2 dumps **ASCII data that contains the desired IP** to a new file and then, using command #3 we **filter out the users login information**.

Running commands #2 and #3 on both IP addresses shows that the user in **10.10.0.20** logged into **two email accounts**; **david@mailme.com with password "david"** and **anon@mailme.com with password "anon" ,** And the user in **10.10.0.40** logged into one email account; **carol@mailme.com with password "carol"**.

So the two **suspects are david and carol**.

4> Tools:

#> **tshark -r <filname.pcap> -Y ftp | grep -i pass**

```
95172 6645.943022 192.168.1.112 21 10.10.0.20   51256 FTP 87 Response: 331 Password required for admin
95173 6645.943123   10.10.0.20 51256 192.168.1.112 21 FTP 68 Request: PASS fzadmin
95180 6645.952854 192.168.1.112 21 10.10.0.20   51256 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95196 6645.985375 192.168.1.112 21 10.10.0.20   51256 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95744 6791.724992 192.168.1.112 21 10.10.0.20   51267 FTP 87 Response: 331 Password required for admin
95745 6791.725173   10.10.0.20 51267 192.168.1.112 21 FTP 68 Request: PASS fzadmin
95752 6791.729746 192.168.1.112 21 10.10.0.20   51267 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95778 6798.287958 192.168.1.112 21 10.10.0.20   51269 FTP 87 Response: 331 Password required for admin
95779 6798.288108   10.10.0.20 51269 192.168.1.112 21 FTP 68 Request: PASS fzadmin
95786 6798.301156 192.168.1.112 21 10.10.0.20   51269 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95802 6798.353244 192.168.1.112 21 10.10.0.20   51269 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95840 6808.482179 192.168.1.112 21 10.10.0.40   53602 FTP 87 Response: 331 Password required for guest
95841 6808.482316   10.10.0.40 53602 192.168.1.112 21 FTP 66 Request: PASS guest
95848 6808.486687 192.168.1.112 21 10.10.0.40   53602 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95864 6811.498056 192.168.1.112 21 10.10.0.40   53602 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95888 6814.225205 192.168.1.112 21 10.10.0.40   53605 FTP 87 Response: 331 Password required for guest
95889 6814.225446   10.10.0.40 53605 192.168.1.112 21 FTP 66 Request: PASS guest
95896 6814.233577 192.168.1.112 21 10.10.0.40   53605 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
95910 6816.021003 192.168.1.112 21 10.10.0.40   53605 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
```

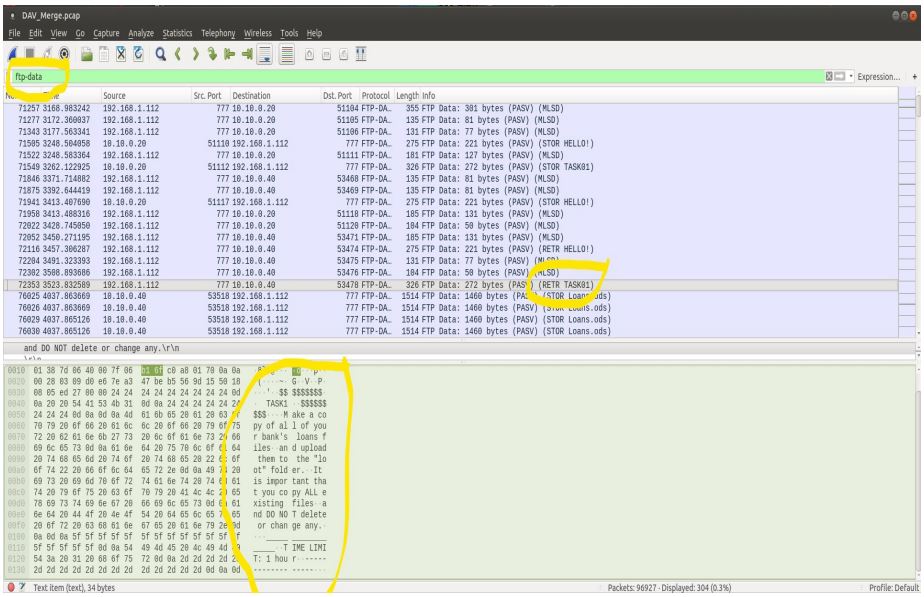
Answer:

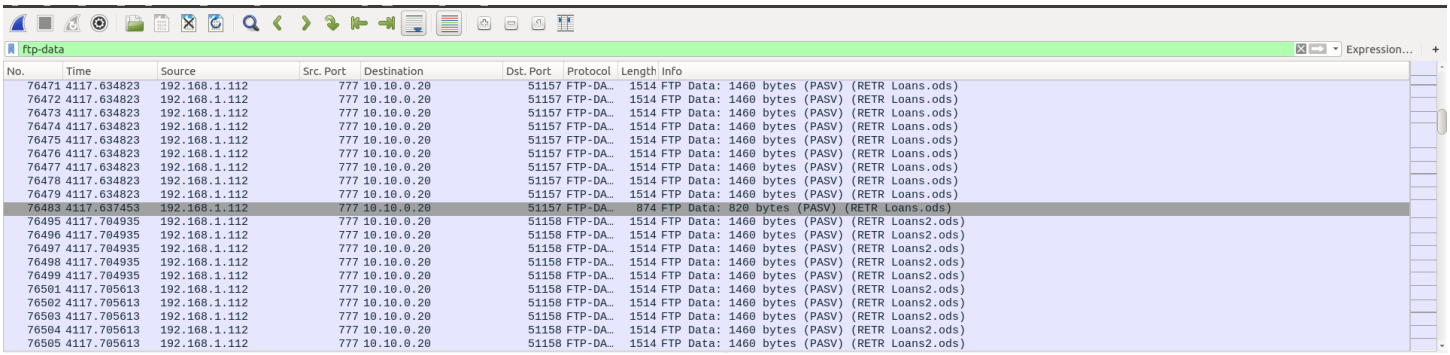
Using the command above we can see **two users logging in** to the FTP server;

- **User: admin** **Password: fzadmin**
- **User: guest** **Password: guest**

5> Tools:

WIRESHARK – File extraction, **GOOGLE**





Answer:

Using wireshark with the '**ftp-data**' **display filter** we can view the content of all the instructive "TASK"

files in clear text at the bottom of the screen. We can see in TASK01 the **objective files are loan**

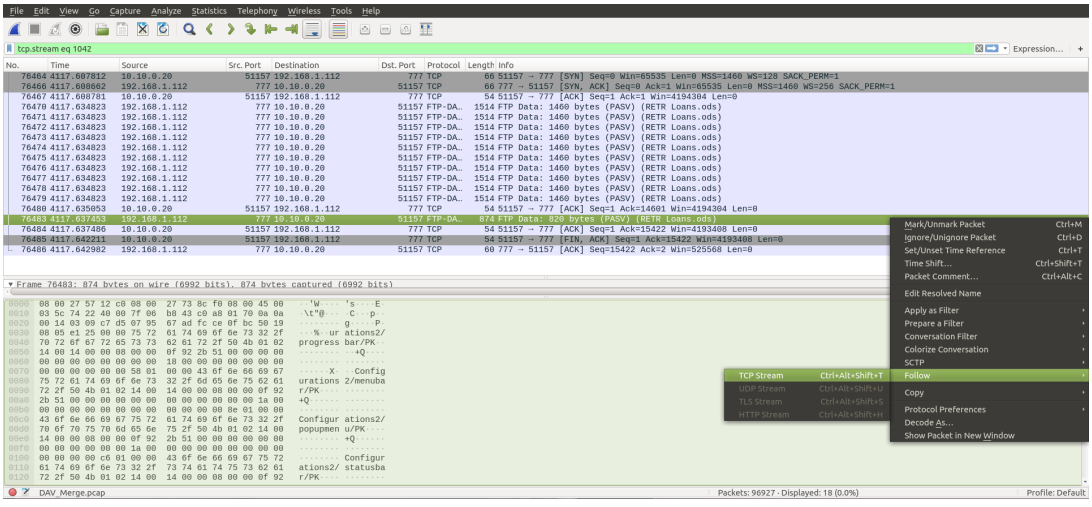
files and that the suspect is asked to upload them to the "loot" folder on that same server.

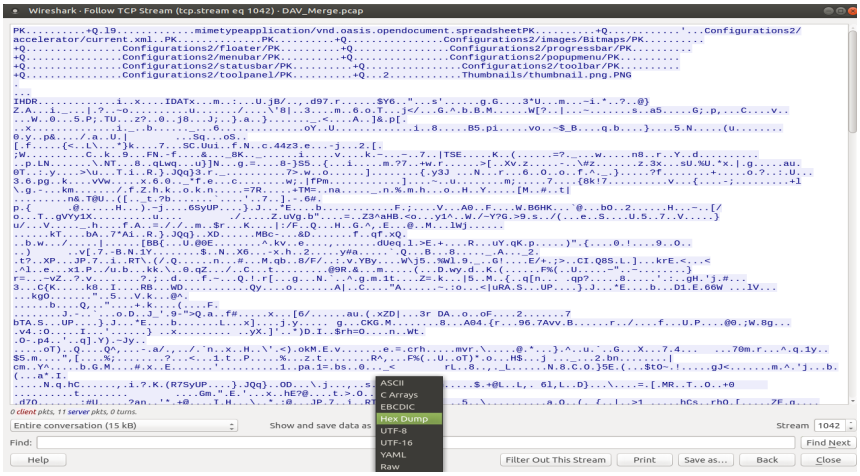
So we know it will be transferred in FTP.

two possible files are presented in this view; loans.ods and **loans2.ods**
Sure enough, this is the right answer but if we want to be absolutely sure of that

we can extract specific files from pcap as follows:

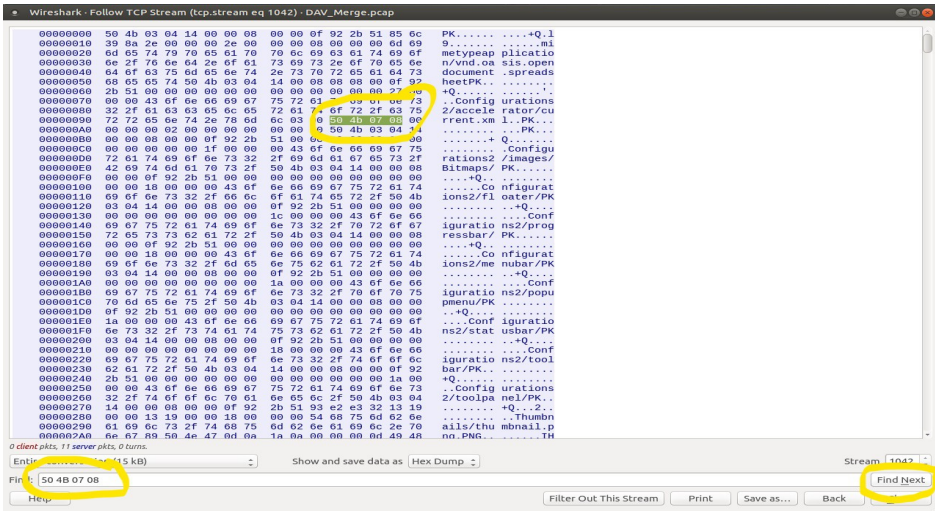
- after screening for ftp-data packets, we select a packet indicating a file transfer with the name of the file we want to extract (loans.ods, loans2.ods). Right click the packet and s**elect FOLLOW >> TCP stream , and change the display format to "Hex Dump".**



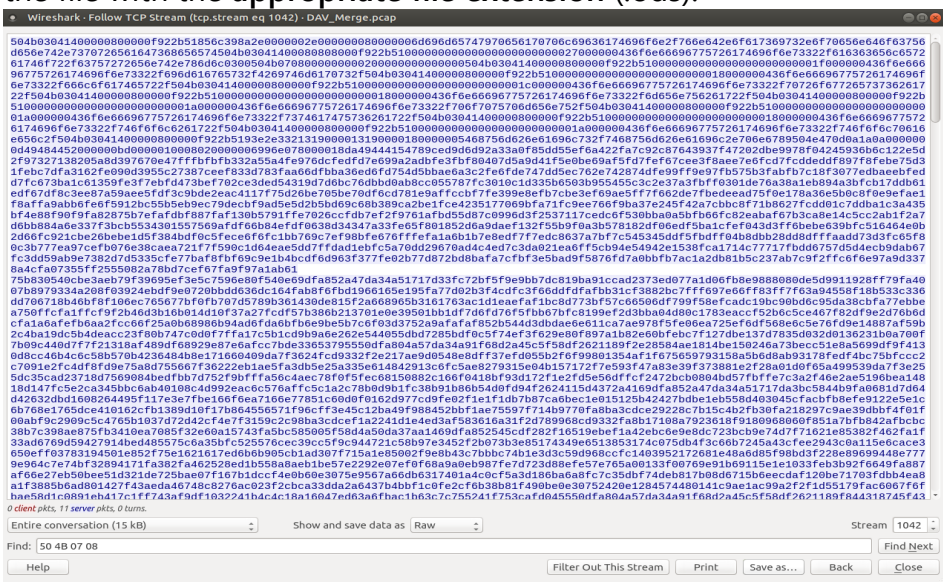


- Google search the file signature for the sfecific file type you would like to extract, in this case - a ".ods" type. The signature for open documents (ods,odt,odd etc.) is 50 4B 03 04 ***OR*** 50 4B 05 06 ***OR*** 50 4B 07 08.

- copy paste the signature into the search line and **search for it in the current stream**. If the signature is found, that is indication that it is in fact a ".ods" file.



- Next step is to **extract** the file; change the **display format to** “**Raw**”, **click** ”**Save as…**” and name the file with the **appropriate file extension** (.ods).



- After doing so, open the files and see if the data fits the description of what you were searching for. We can see that the files contain sheets of customer data that seems pretty genuine, which makes it more likely that these are in fact the stolen loan files.

6> Tools:

WIRESHARK – File extraction

Answer:

To answer this question we have to start looking for clues as we haven't seen any information in this matter.

If we look at the payload of **TASK02 we can see a request for the retrieval and deletion of HR reports**, and then we start seeing multiple file transfers, And among these files is a file named **"accounts HR reports 2019.ods"**.

Extracting this file as explained previously would retrieve a sheet of HR information for the accounts department employees, in which we can see there are actually **two** most senior employees; **Maisie Swanson** and **Mercy Farrington**. Who have been employed for **22 years** each.

7> Tools:

1. #> **tshark -r <filename.pcap> -Y ftp | grep -i transfer**

```
71556 3262.166852 192.168.1.112 → 10.10.0.20   FTP 112 Response: 226 Successfully transferred "/FTP/ezm0n3y/tasks/TASK01"
71849 3371.715136 192.168.1.112 → 10.10.0.40   FTP 88 Response: 226 Successfully transferred "/"
71878 3392.644617 192.168.1.112 → 10.10.0.40   FTP 88 Response: 226 Successfully transferred "/"
71947 3413.442149 192.168.1.112 → 10.10.0.20   FTP 98 Response: 226 Successfully transferred "/FTP/HELLO!"
71962 3413.488867 192.168.1.112 → 10.10.0.20   FTP 91 Response: 226 Successfully transferred "/FTP"
72025 3428.745176 192.168.1.112 → 10.10.0.20   FTP 105 Response: 226 Successfully transferred "/FTP/ezm0n3y/tasks"
72055 3450.271425 192.168.1.112 → 10.10.0.40   FTP 88 Response: 226 Successfully transferred "/"
72119 3457.306743 192.168.1.112 → 10.10.0.40   FTP 94 Response: 226 Successfully transferred "/HELLO!"
72208 3491.326759 192.168.1.112 → 10.10.0.40   FTP 95 Response: 226 Successfully transferred "/ezm0n3y"
72305 3508.894024 192.168.1.112 → 10.10.0.40   FTP 101 Response: 226 Successfully transferred "/ezm0n3y/tasks"
72355 3523.832589 192.168.1.112 → 10.10.0.40   FTP 108 Response: 226 Successfully transferred "/ezm0n3y/tasks/TASK01"
75084 3947.680659 192.168.1.112 → 10.10.0.40   FTP 100 Response: 226 Successfully transferred "/ezm0n3y/loot"
75990 4031.357738 192.168.1.112 → 10.10.0.40   FTP 100 Response: 226 Successfully transferred "/ezm0n3y/loot"
76055 4038.370246 192.168.1.112 → 10.10.0.40   FTP 110 Response: 226 Successfully transferred "/ezm0n3y/loot/Loans.ods"
76067 4038.384472 192.168.1.112 → 10.10.0.40   FTP 100 Response: 226 Successfully transferred "/ezm0n3y/loot"
76095 4040.812569 192.168.1.112 → 10.10.0.40   FTP 111 Response: 226 Successfully transferred "/ezm0n3y/loot/Loans2.ods"
76107 4040.871012 192.168.1.112 → 10.10.0.40   FTP 100 Response: 226 Successfully transferred "/ezm0n3y/loot"
76354 4102.730572 192.168.1.112 → 10.10.0.20   FTP 91 Response: 226 Successfully transferred "/FTP"
76373 4106.535167 192.168.1.112 → 10.10.0.20   FTP 105 Response: 226 Successfully transferred "/FTP/ezm0n3y/tasks"
76390 4108.073641 192.168.1.112 → 10.10.0.20   FTP 104 Response: 226 Successfully transferred "/FTP/ezm0n3y/loot"
76481 4117.636285 192.168.1.112 → 10.10.0.20   FTP 114 Response: 226 Successfully transferred "/FTP/ezm0n3y/loot/Loans.ods"
76507 4117.705952 192.168.1.112 → 10.10.0.20   FTP 115 Response: 226 Successfully transferred "/FTP/ezm0n3y/loot/Loans2.ods"
77090 4290.602747 192.168.1.112 → 10.10.0.20   FTP 99 Response: 226 Successfully transferred "/FTP/ezm0n3y"
77109 4300.010435 192.168.1.112 → 10.10.0.20   FTP 91 Response: 226 Successfully transferred "/FTP"
77128 4302.523095 192.168.1.112 → 10.10.0.20   FTP 99 Response: 226 Successfully transferred "/FTP/ezm0n3y"
77201 4322.541860 192.168.1.112 → 10.10.0.20   FTP 113 Response: 226 Successfully transferred "/FTP/ezm0n3y/task1comp.txt"
77214 4322.589689 192.168.1.112 → 10.10.0.20   FTP 99 Response: 226 Successfully transferred "/FTP/ezm0n3y"
77240 4336.263584 192.168.1.112 → 10.10.0.20   FTP 112 Response: 226 Successfully transferred "/FTP/ezm0n3y/tasks/TASK02"
77255 4336.300527 192.168.1.112 → 10.10.0.20   FTP 105 Response: 226 Successfully transferred "/FTP/ezm0n3y/tasks"
79401 4385.778858 192.168.1.112 → 10.10.0.40   FTP 100 Response: 226 Successfully transferred "/ezm0n3y/loot"
```

2. #> **tshark -r <filename.pcap> -Y 'frame.number eq 76107' -T fields -e frame.time**

```
Oct  5, 2020 17:09:34.572719000 IDT
```

Answer:

Using command #1 we carve for **ftp-data** that was **successfully transferred**, obviously, **non-successful transfers could not indicate** for task accomplishment.

The output shows that the transfer of “loans2.ods” took happened in packets 76095 and 76107.

Running command #2 we simply carve for the **last packets frame time**.

Task01 was completed at Oct 5, 2020 17:09:34.572719000 IDT, Frame #76107.

8> Tools:

#> tshark -r <filename.pcap> -Y ftp | grep -E 'RETR'

```
72111 3457.303015   10.10.0.40 → 192.168.1.112 FTP 67 Request: RETR HELLO!
72345 3523.801596   10.10.0.40 → 192.168.1.112 FTP 67 Request: RETR TASK01
76462 4117.606943   10.10.0.20 → 192.168.1.112 FTP 70 Request: RETR Loans.ods
76490 4117.683052   10.10.0.20 → 192.168.1.112 FTP 71 Request: RETR Loans2.ods
79445 4395.328043   10.10.0.40 → 192.168.1.112 FTP 74 Request: RETR task1comp.txt
79509 4426.396679   10.10.0.40 → 192.168.1.112 FTP 67 Request: RETR TASK02
94188 6487.457605   10.10.0.20 → 192.168.1.112 FTP 88 Request: RETR Accounts HR report 2019.ods
94235 6487.512019   10.10.0.20 → 192.168.1.112 FTP 96 Request: RETR .~lock.Accounts HR report 2019.ods#
94274 6487.547827   10.10.0.20 → 192.168.1.112 FTP 88 Request: RETR Counters HR report 2019.ods
94286 6487.571128   10.10.0.20 → 192.168.1.112 FTP 82 Request: RETR IT HR report 2019.ods
94358 6487.654405   10.10.0.20 → 192.168.1.112 FTP 89 Request: RETR Managment HR report 2019.ods
94369 6487.674004   10.10.0.20 → 192.168.1.112 FTP 85 Request: RETR Misc. HR report 2019.ods
94554 6547.829103   10.10.0.20 → 192.168.1.112 FTP 88 Request: RETR Accounts HR report 2019.ods
94576 6547.832264   10.10.0.20 → 192.168.1.112 FTP 96 Request: RETR .~lock.Accounts HR report 2019.ods#
94596 6547.842353   10.10.0.20 → 192.168.1.112 FTP 88 Request: RETR Counters HR report 2019.ods
94627 6547.857097   10.10.0.20 → 192.168.1.112 FTP 82 Request: RETR IT HR report 2019.ods
94657 6547.878107   10.10.0.20 → 192.168.1.112 FTP 89 Request: RETR Managment HR report 2019.ods
94686 6547.901294   10.10.0.20 → 192.168.1.112 FTP 85 Request: RETR Misc. HR report 2019.ods
95897 6814.233886   10.10.0.40 → 192.168.1.112 FTP 74 Request: RETR task2comp.txt
95911 6816.021710   10.10.0.40 → 192.168.1.112 FTP 72 Request: RETR goodjob.txt
```

#> tshark -r <filename.pcap> -Y 'frame.number eq 72345' -T fields -e frame.time

Answer:

As we already know, TASK01 was **completed at 17:09:34**.

So all we need to find next is when did it begin.

To do that we'll carve for FTP again, but this time we'll **search for the "RETR" flag**,

which indicates the beginning of a download process, and more specifically, **the**

initial download request made by the recipient (command#1).

The **frame number is 72345**. Carve for the frame time **(command #2)** and we get

the time **17:00:57**. Completing TASK01 took **8:37 minutes**.

9> **Tools:**

WIRESHARK – File extraction

Answer:

The only way to know that is to extract the “management HR report 2019. ods”

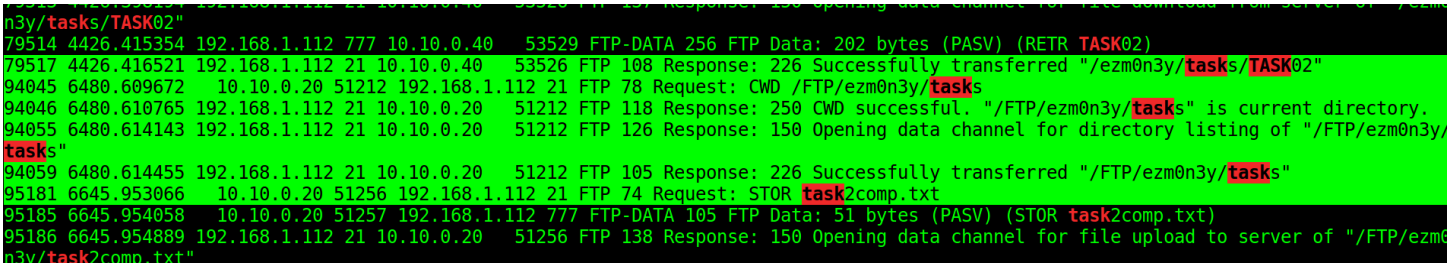
spreadsheet. Doing so we see that **David King has been employed at the bank for**

8 years.

10> Tools:

- **WIRESHARK**

1.#> **tshark -r <filename.pcap> | grep -i task**



2. #> **tshark -r <filename.pcap> -Y 'ip.src eq 10.10.0.40 && frame.number > 79517 && frame.number < 95181' -T fields -e tcp.dstport | sort -u / uniq -c**

```
139
143
21
2869
3389
443
51038
51039
51045
51048
51053
51055
51189
51192
51242
51246
51251
51586
51587
51607
51611
51667
51674
51678
51680
51683
5357
587
777
```

3. #> **sudo tcpdump -r <filename.pcap> -nA | grep -E 'document' -A 5**

```
--
.(...p.R.       ....e..bP.......p://openoffice.org/2004/office" xmlns:grddl="http://www.w3.org/2003/g/data-view#" office:version="1.2"><
office:meta><meta:initial-creator>alice alice</meta:initial-creator><meta:creation-date>2020-09-16T19:33:33.99</meta:creation-date><dc:d
ate>2020-09-16T23:06:47.73</dc:date><dc:creator>alice alice</dc:creator><meta:editing-duration>PT3M38S</meta:editing-duration><meta:edit
ing-cycles>3</meta:editing-cycles><meta:generator>OpenOffice/4.1.6$Win32 OpenOffice.org_project/416m1$Build-9790</meta:generator><meta:d
ocument-statistic meta:table-count="3" meta:cell-count="105" meta:object-count="0"/></office:meta></office:document-meta>PK.........0Q.
.............META-INF/manifest.xml...n. ...}.....z.P..&.      ..`.I.. 0U..#..f[;-Uo.....A.6.g.=.d<6..?.
P..`....{..6...)4.$...*}..a.rD.U2I.r.$i..`.uv.$......M.,.zQ]x..P..x.T;h.....a*.k...-.....>%..".6.........uP.k.`b...*o.;..x...Bi..J...9..
a..L...S.A.g....?O3....D....v..'*c......y....a3W!eJ.ou..& *o?=^......^ul....1.K.C.; 5._ ...PK..IH,.&...E...PK...........0Q.l9.......
.................mimetypePK...........0Q.........................T...Configurations2/floater/PK...........0Q...........'.........
.......Configurations2/accelerator/current.xmlPK...........0Q.............................Configurations2/images/Bitmaps/PK.........
.0Q.............................Configurations2/progressbar/PK...........0Q.........................X...Configurations2/menubar/PK...
.........0Q..................
17:48:34.731505 IP 10.10.0.40.53586 > 192.168.1.112.777: Flags [FP.], seq 16061:16753, ack 1, win 32768, length 692
E...yC@.....
```

4. #> tshark -r <filename.pcap> -Y 'tcp.port eq 3389' -T fields -e frame.time

```
Oct  5, 2020 17:49:57.878986000 IDT
Oct  5, 2020 17:49:57.919767000 IDT
Oct  5, 2020 17:49:57.919767000 IDT
Oct  5, 2020 17:49:57.919767000 IDT
Oct  5, 2020 17:49:57.919979000 IDT
Oct  5, 2020 17:49:57.919979000 IDT
Oct  5, 2020 17:49:57.919979000 IDT
Oct  5, 2020 17:49:57.920770000 IDT
Oct  5, 2020 17:49:57.921192000 IDT
Oct  5, 2020 17:49:58.079860000 IDT
Oct  5, 2020 17:49:58.079967000 IDT
Oct  5, 2020 17:49:58.090546000 IDT
Oct  5, 2020 17:49:58.264795000 IDT
Oct  5, 2020 17:49:58.265524000 IDT
Oct  5, 2020 17:49:58.265524000 IDT
Oct  5, 2020 17:49:58.444404000 IDT
Oct  5, 2020 17:49:58.642237000 IDT
Oct  5, 2020 17:49:59.750595000 IDT
Oct  5, 2020 17:49:59.755578000 IDT
Oct  5, 2020 17:49:59.961185000 IDT
Oct  5, 2020 17:50:03.476520000 IDT
Oct  5, 2020 17:50:03.671341000 IDT
Oct  5, 2020 17:50:03.810153000 IDT
Oct  5, 2020 17:50:03.810153000 IDT
Oct  5, 2020 17:50:03.810308000 IDT
Oct  5, 2020 17:50:03.810375000 IDT
```

5.#> tshark -r <filename.pcap> -Y 'ftp && frame.time > "Oct 5, 2020 17:50:03.810375000"'

```
94229 6487.503303 192.168.1.112 21 10.10.0.20   51217 FTP 154 Response: 226 Successfully transferred "/FTP/ezm0n3y/loot/HR_Documents/Acc
ounts/Accounts HR report 2019.ods"
94233 6487.510457   10.10.0.20 51218 192.168.1.112 21 FTP 60 Request: PASV
94234 6487.511749 192.168.1.112 21 10.10.0.20   51218 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
94235 6487.512019   10.10.0.20 51218 192.168.1.112 21 FTP 96 Request: RETR .~lock.Accounts HR report 2019.ods#
94239 6487.513754 192.168.1.112 21 10.10.0.20   51218 FTP 191 Response: 150 Opening data channel for file download from server of "/FTP/
ezm0n3y/loot/HR_Documents/Accounts/.~lock.Accounts HR report 2019.ods#"
94240 6487.515500   10.10.0.20 51212 192.168.1.112 21 FTP 90 Request: CWD /FTP/ezm0n3y/loot/HR_Documents
94246 6487.528307 192.168.1.112 21 10.10.0.20   51212 FTP 130 Response: 250 CWD successful. "/FTP/ezm0n3y/loot/HR_Documents" is current
directory.
94247 6487.528480   10.10.0.20 51212 192.168.1.112 21 FTP 69 Request: CWD Managment
94248 6487.528765 192.168.1.112 21 10.10.0.20   51218 FTP 162 Response: 226 Successfully transferred "/FTP/ezm0n3y/loot/HR_Documents/Acc
ounts/.~lock.Accounts HR report 2019.ods#"
94250 6487.530515 192.168.1.112 21 10.10.0.20   51212 FTP 140 Response: 250 CWD successful. "/FTP/ezm0n3y/loot/HR_Documents/Managment" i
s current directory.
94251 6487.530623   10.10.0.20 51212 192.168.1.112 21 FTP 59 Request: PWD
94252 6487.531419 192.168.1.112 21 10.10.0.20   51212 FTP 124 Response: 257 "/FTP/ezm0n3y/loot/HR_Documents/Managment" is current direct
ory.
94253 6487.531546   10.10.0.20 51212 192.168.1.112 21 FTP 60 Request: PASV
94254 6487.532457 192.168.1.112 21 10.10.0.20   51212 FTP 101 Response: 227 Entering Passive Mode (192,168,1,112,3,9)
94256 6487.532758   10.10.0.20 51212 192.168.1.112 21 FTP 60 Request: MLSD
94259 6487.534561 192.168.1.112 21 10.10.0.20   51212 FTP 148 Response: 150 Opening data channel for directory listing of "/FTP/ezm0n3y/
loot/HR_Documents/Managment"
94263 6487.534728 192.168.1.112 21 10.10.0.20   51212 FTP 127 Response: 226 Successfully transferred "/FTP/ezm0n3y/loot/HR_Documents/Man
agment"
```

Answer:

TASK02 was to **copy, upload and delete** the HR report files.
To know how the files were retrieved we will use **command #1** to start looking for a chain of events starting at **packet #79517**, the time the "TASK02" file was successfully downloaded by the recipient - **Carol 10.10.0.40,** and ending at **packet #95181** where the file **"task2comp.txt"** was uploaded by **David (10.10.0.20)**.
Command #2 will output which services were used by carol in this time frame.

The well known ports that carol used are:

777 – Multiling-http
2869 – Icslap
53 - DNS
143 – Imap
443 – Https
1900 - SSDP
587 – Message Submission Agent (MSA)
3389 – MS WBT server
21 – FTP
139 – NetBIOS session service (NBSS)
5357 – Web services for devices (WSDAPI)

Most of these ports host services used exclusively by computers and do not engage in any interaction with the user.
If we **pipe command #2 through "uniq -c"** we see that port 3389 is highly active in this time frame and this should raise some strong suspicions;

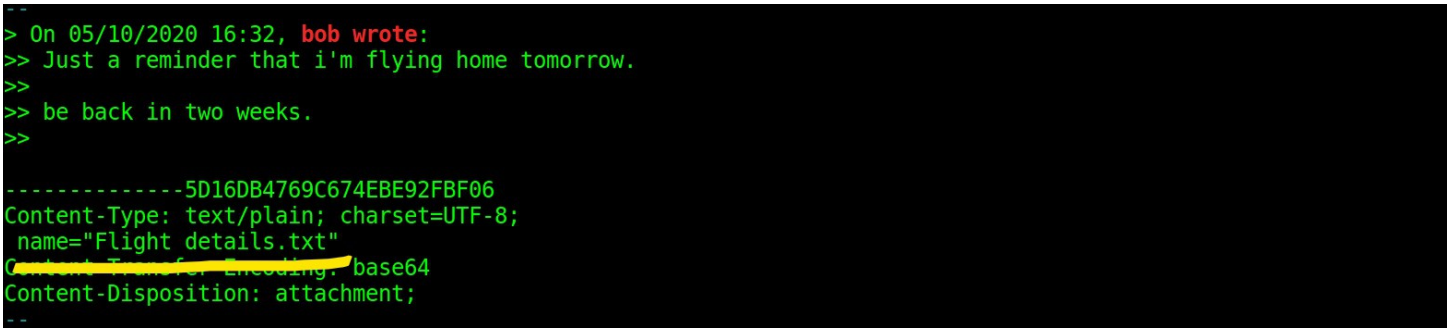
Port #3389 is commonly known as the port for **Remote Desktop** service.
Although it could be **dissected as TLS, WBT, or TCP**, just seeing this port number used by someone other than a sys admin should be worth investigating.
And in fact, using **WIRESHARK**, we can see massive sets of 'application data' packets sent to port #3389 concluded by 'reassembled PDU'.
These packets contain an **msthash cookie** with the invaded hostname (**alice-pc)** and and **RDP indicator**.
So now we have **evidence of a remote session** taking place on alice-pc.

Next clue is the previous email correspondences in which alice is asked to go over the HR reports and pass them over to david. This should let us presume that the files may have very well been on Alice's computer. We see an email from Carol talking Alice into taking a break and leaving her desk to go eat.

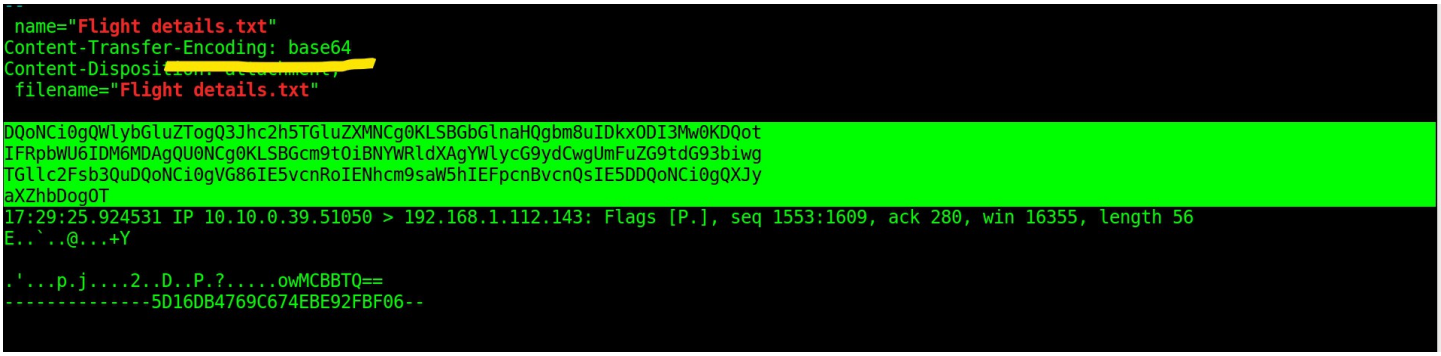
Finally the last step is to mine information about any transferred documents **(command #3)**, and discover multiple uploads of open office **documents created by Alice**, to the FTP server, executed by Carol.
If we have a look at the FTP data from the end of the RDP session **(commands #4, #5)**, we can indeed see all the different HR reports uploaded by Carol.
Method used: Remote Desktop, Protocol: RDP (TLSv1), Port no. 3389.

11> Tools:

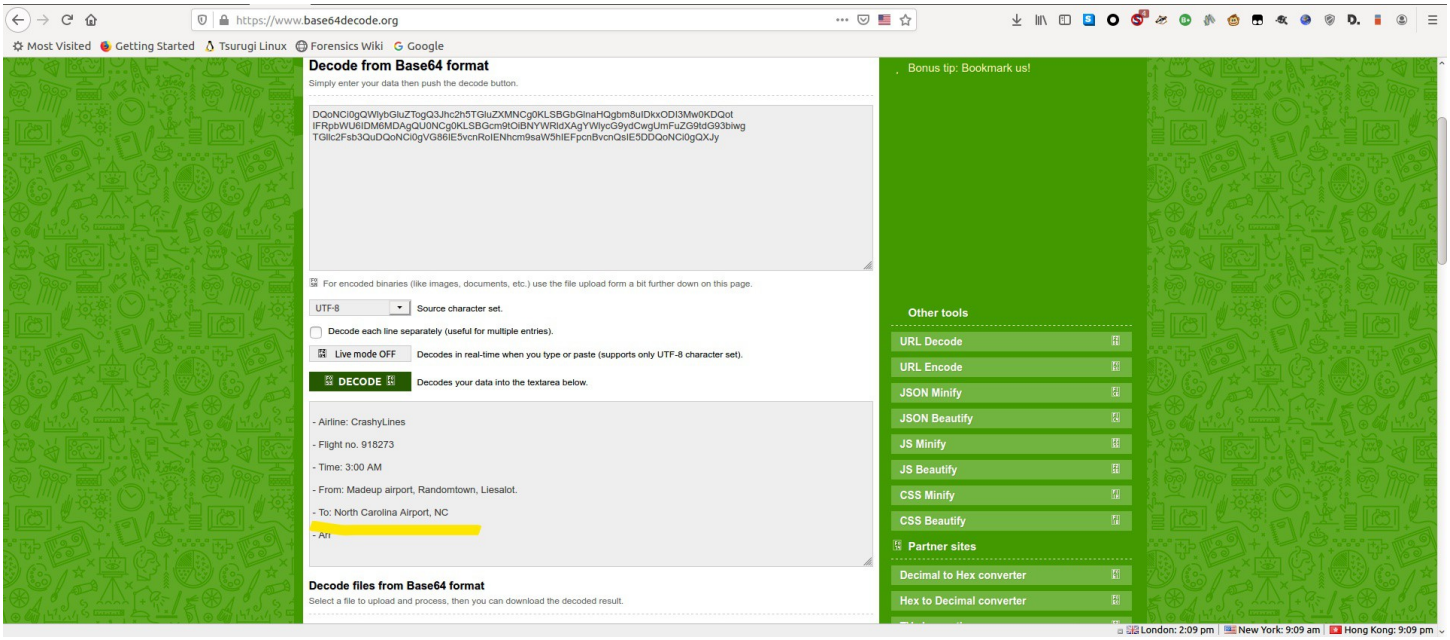
1. #> **sudo tcpdump -r <filename.pcap> -nA | grep -E 'bob wrote' -A 10**



2. #> **sudo tcpdump -r <filename> -nA | grep -E "Flight details.txt" -A 15**



3. **Base64decode.org** - Online Base64 decoder/encoder



Answer:

Appearently, the fastest way to browse through someone's emails sent with Mozzila Thunderbird is to curve for an expression including the person's name and the word "wrote", as described in command #1.

Doing that we learn about bob's upcoming flight home. We see that in one of the emails he is sending a file named **Flight details.txt** to david and we're able to view the file's content encoded in Base64 (command #2).

Notice that the file is devided to multiple segments, but you only relly need one of them to answer the question.

Decoding the Base64 hash online shows the following details:

- Airline: CrashyLines
- Flight no. 918273
- Time: 3:00 AM
- From: Madeup airport, Randomtown, Liesalot.
- **To: North Carolina Airport, NC**
- Arrival: 9:00 AM

12> Tool:

#> **sudo tcpdump -r <filename.pcap> -nA | grep -i login | grep -E 'anon@mailme'**

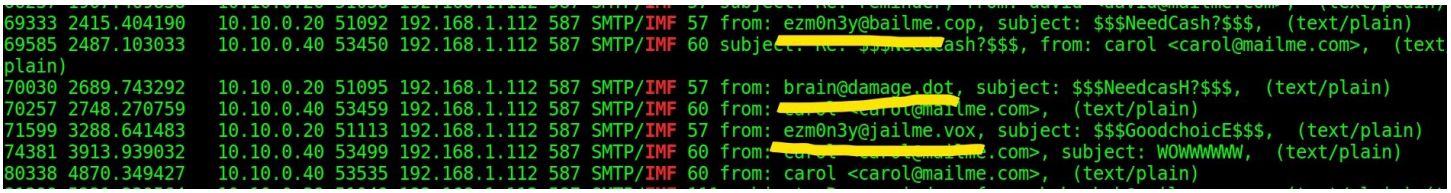
```
reading from file DAV_Merge.pcap, link-type EN10MB (Ethernet)
.....p......Lg...HP....r..3 login "anon@mailme.com" "anon"
.....p.....[....pdP....r..3 login "anon@mailme.com" "anon"
.....p. .....0,.'.P....r..3 login "anon@mailme.com" "anon"
.....p.u....(*.K..P....r..3 login "anon@mailme.com" "anon"
.....p....y?...x..P....r..3 login "anon@mailme.com" "anon"
.....p....'Y.}....P....r..3 login "anon@mailme.com" "anon"
.....p......SX.|..P....r..3 login "anon@mailme.com" "anon"
```

Answer:

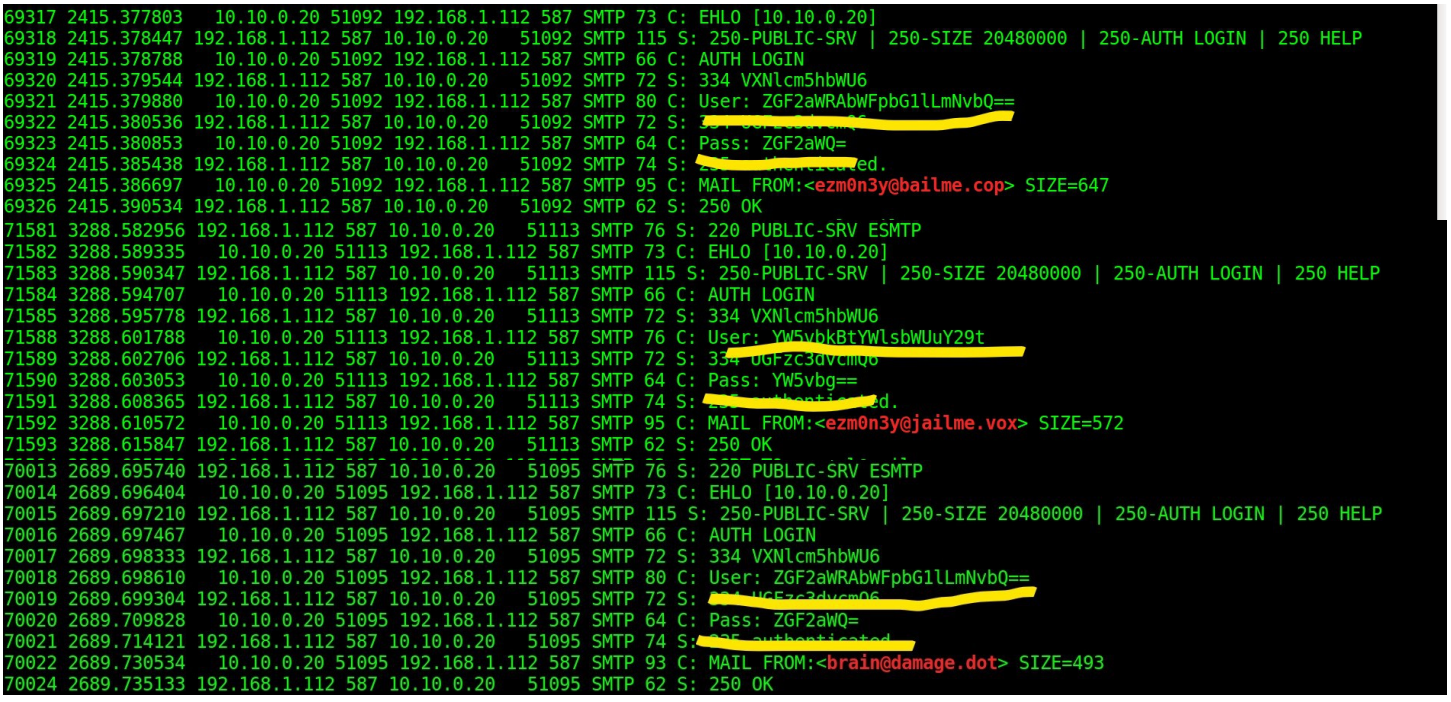
The command above outputs **all login attempts by the username** specified. **password is anon**

13> Tool:

1. #> **tshark -r <filename.pcap> -Y smtp | grep -i imf**



2. #> **tshark -r <filename.pcap> -Y smtp | grep -E <suspicious_mail_address>**



Answer:

Using command #1 tshark **lists all IMF message headers** including all sender's addresses and passwords in Base64 encryption.
IMF is the syntax used for the textual part of messages.
Next, running command #2 we **filter out the SMTP** activities of a specific email address and **decode the email addresses with a base64 decoder** as shown previously. This shows the true email address from which messages were sent rather than the spoofed one.

The spoofed addresses and the sender behind them are:

- **spoofed: ezm0n3y@bailme.cop -> sender: david@mailme.com**
- **spoofed: ezmoney@jailme.vox -> sender: anon@mailme.com**
- **spoofed: brain@damage.dot -> sender: david@mailme.com**

As we can recall **David is behind both addresses** so the answer is David.