PSP0201 Week 3 Writeup

Group Name: ikun no 1

Members

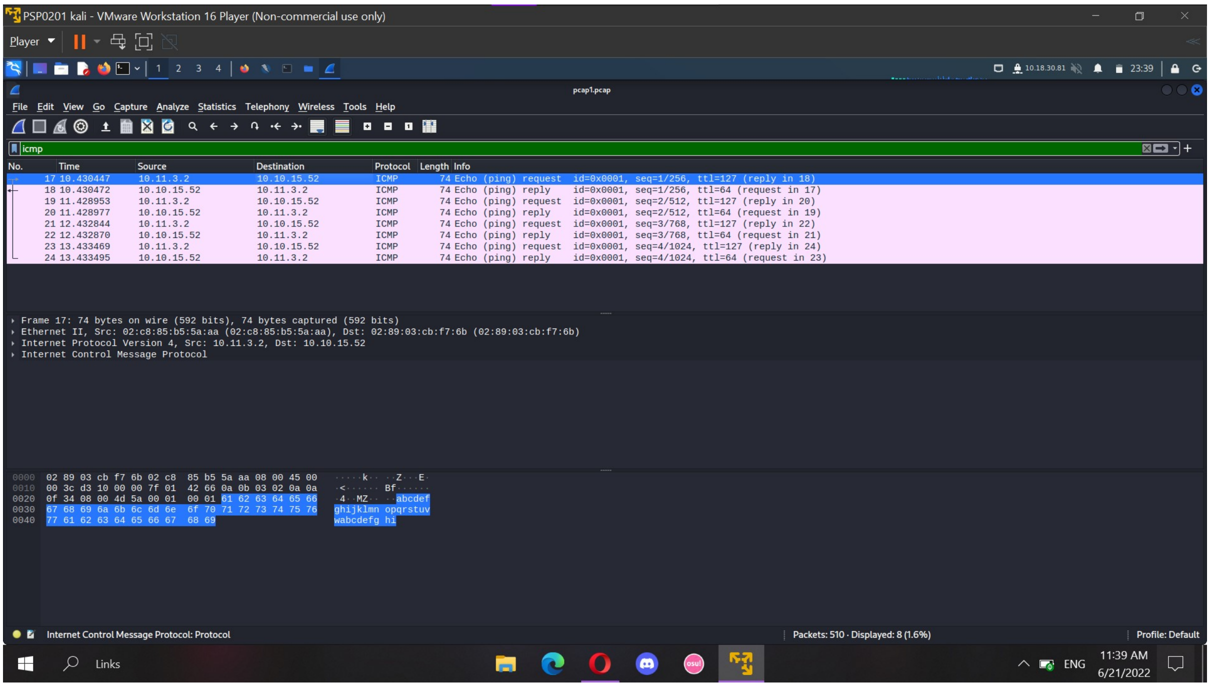
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 7 - [Networking] The Grinch Really Did Steal Christmas

Tool used: kali Linux, Firefox, Wireshark

Solution/Walkthrough:

Q1.



PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packets: 510 · Displayed: 8 (1.6%)
Profile: Default
Links
ENG
11:39 AM
6/21/2022

```
icmp
```

```
No.  Time       Source        Destination   Protocol Length Info
  17 10.430447  10.11.3.2     10.10.15.52   ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=127 (reply in 18)
  18 10.430472  10.10.15.52   10.11.3.2     ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (request in 17)
  19 11.428953  10.11.3.2     10.10.15.52   ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=127 (reply in 20)
  20 11.428977  10.10.15.52   10.11.3.2     ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (request in 19)
  21 12.432844  10.11.3.2     10.10.15.52   ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=127 (reply in 22)
  22 12.432870  10.10.15.52   10.11.3.2     ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (request in 21)
  23 13.433469  10.11.3.2     10.10.15.52   ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=127 (reply in 24)
  24 13.433495  10.10.15.52   10.11.3.2     ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=64 (request in 23)
```

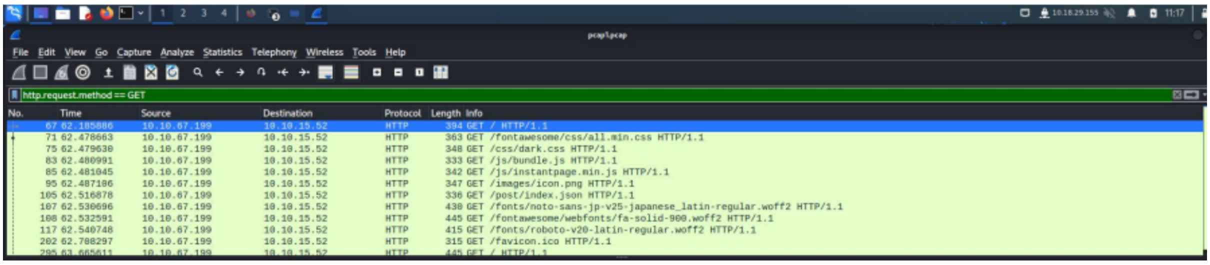
```
› Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
› Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)
› Internet Protocol Version 4, Src: 10.11.3.2, Dst: 10.10.15.52
› Internet Control Message Protocol
```

```
0000  02 89 03 cb f7 6b 02 c8  85 b5 5a aa 08 00 45 00   ·····k·· ··Z···E·
0010  00 3c d3 10 00 00 7f 01  42 66 0a 0b 03 02 0a 0a   ·<······ Bf······
0020  0f 34 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ·4··MZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol

Type in icmp in the search bar. The ip addresses that shown in the reply is the one that initiates an ICMP/ping towards the server.

Q2.



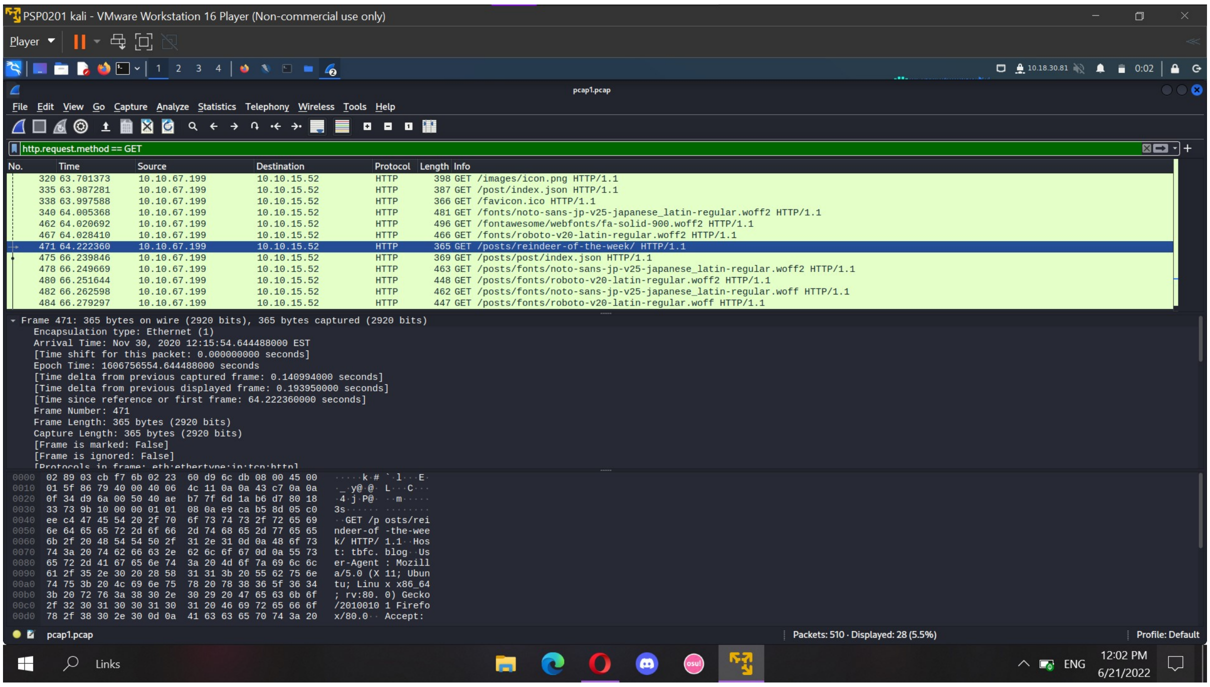
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
11:17

```
http.request.method == GET
```

```
No.  Time       Source         Destination   Protocol Length Info
  67 62.185886  10.10.67.199   10.10.15.52   HTTP     394 GET / HTTP/1.1
  71 62.478663  10.10.67.199   10.10.15.52   HTTP     363 GET /fontawesome/css/all.min.css HTTP/1.1
  75 62.479630  10.10.67.199   10.10.15.52   HTTP     348 GET /css/dark.css HTTP/1.1
  83 62.480991  10.10.67.199   10.10.15.52   HTTP     333 GET /js/bundle.js HTTP/1.1
  85 62.481045  10.10.67.199   10.10.15.52   HTTP     342 GET /js/instantpage.min.js HTTP/1.1
  95 62.487186  10.10.67.199   10.10.15.52   HTTP     347 GET /images/icon.png HTTP/1.1
 105 62.516878  10.10.67.199   10.10.15.52   HTTP     336 GET /post/index.json HTTP/1.1
 107 62.530696  10.10.67.199   10.10.15.52   HTTP     430 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
 108 62.532591  10.10.67.199   10.10.15.52   HTTP     445 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
 117 62.540748  10.10.67.199   10.10.15.52   HTTP     415 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
 202 62.788297  10.10.67.199   10.10.15.52   HTTP     315 GET /favicon.ico HTTP/1.1
 295 63.665611  10.10.67.199   10.10.15.52   HTTP     445 GET / HTTP/1.1
```

Try to type in [(protocool).request.method == (get/post)]. When the protocol used is HTTP and GET, we can see only HTTP GET requests.

Q3.


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packets: 510 · Displayed: 28 (5.5%)
Profile: Default
Links
ENG
12:02 PM
6/21/2022

http.request.method == GET

```
No.  Time       Source        Destination  Protocol Length Info
 320 63.701373  10.10.67.199  10.10.15.52  HTTP     398 GET /images/icon.png HTTP/1.1
 335 63.987281  10.10.67.199  10.10.15.52  HTTP     387 GET /post/index.json HTTP/1.1
 338 63.997588  10.10.67.199  10.10.15.52  HTTP     366 GET /favicon.ico HTTP/1.1
 340 64.005368  10.10.67.199  10.10.15.52  HTTP     481 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
 462 64.020692  10.10.67.199  10.10.15.52  HTTP     496 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
 467 64.028410  10.10.67.199  10.10.15.52  HTTP     466 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
 471 64.222360  10.10.67.199  10.10.15.52  HTTP     365 GET /posts/reindeer-of-the-week/ HTTP/1.1
 475 66.239846  10.10.67.199  10.10.15.52  HTTP     369 GET /posts/post/index.json HTTP/1.1
 478 66.249669  10.10.67.199  10.10.15.52  HTTP     463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
 480 66.251644  10.10.67.199  10.10.15.52  HTTP     448 GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
 482 66.262598  10.10.67.199  10.10.15.52  HTTP     462 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
 484 66.279297  10.10.67.199  10.10.15.52  HTTP     447 GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1
```

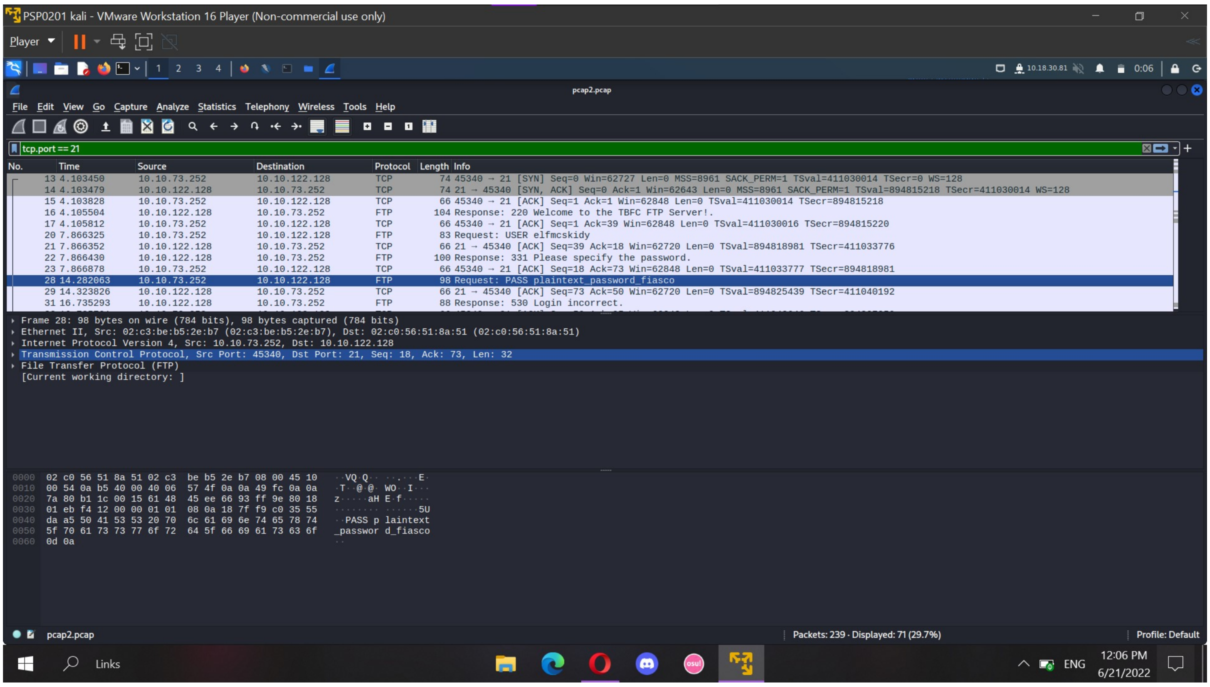
```
Frame 471: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 30, 2020 12:15:54.644488000 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1606756554.644488000 seconds
    [Time delta from previous captured frame: 0.140994000 seconds]
    [Time delta from previous displayed frame: 0.193950000 seconds]
    [Time since reference or first frame: 64.222360000 seconds]
    Frame Number: 471
    Frame Length: 365 bytes (2920 bits)
    Capture Length: 365 bytes (2920 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
```

```
0000  02 89 03 cb f7 6b 02 23  60 d9 6c db 08 00 45 00   ·····k·# `·l···E·
0010  01 5f 86 79 40 00 40 06  4c 11 0a 0a 43 c7 0a 0a   ·_·y@·@· L···C···
0020  0f 34 d9 6a 00 50 40 ae  b7 7f 6d 1a b6 d7 80 18   ·4·j·P@· ··m·····
0030  33 73 9b 10 00 00 01 01  08 0a e9 ca b5 8d 05 c0   3s······ ········
0040  ee c4 47 45 54 20 2f 70  6f 73 74 73 2f 72 65 69   ··GET /p osts/rei
0050  6e 64 65 65 72 2d 6f 66  2d 74 68 65 2d 77 65 65   ndeer-of -the-wee
0060  6b 2f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   k/ HTTP/ 1.1··Hos
0070  74 3a 20 74 62 66 63 2e  62 6c 6f 67 0d 0a 55 73   t: tbfc. blog··Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 35 2e 30 20 28 58  31 31 3b 20 55 62 75 6e   a/5.0 (X 11; Ubun
00a0  74 75 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   tu; Linu x x86_64
00b0  3b 20 72 76 3a 38 30 2e  30 29 20 47 65 63 6b 6f   ; rv:80. 0) Gecko
00c0  2f 32 30 31 30 30 31 30  31 20 46 69 72 65 66 6f   /2010010 1 Firefo
00d0  78 2f 38 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   x/80.0·· Accept:
```

pcap1.pcap

By using the same filter, we can find out the post and we get to know the name of the article.

Q4.


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packets: 239 · Displayed: 71 (29.7%)
Profile: Default
Links
ENG
12:06 PM
6/21/2022

tcp.port == 21

```
No. Time       Source         Destination    Protocol Length Info
 13 4.103450   10.10.73.252   10.10.122.128  TCP       74 45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSecr=0 WS=128
 14 4.103479   10.10.122.128  10.10.73.252   TCP       74 21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=894815218 TSecr=411030014 WS=128
 15 4.103828   10.10.73.252   10.10.122.128  TCP       66 45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSecr=894815218
 16 4.105504   10.10.122.128  10.10.73.252   FTP      104 Response: 220 Welcome to the TBFC FTP Server!.
 17 4.105812   10.10.73.252   10.10.122.128  TCP       66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TSecr=894815220
 20 7.866325   10.10.73.252   10.10.122.128  FTP       83 Request: USER elfmcskidy
 21 7.866352   10.10.122.128  10.10.73.252   TCP       66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=411033776
 22 7.866430   10.10.122.128  10.10.73.252   FTP      100 Response: 331 Please specify the password.
 23 7.866878   10.10.73.252   10.10.122.128  TCP       66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033777 TSecr=894818981
 28 14.282063  10.10.73.252   10.10.122.128  FTP       98 Request: PASS plaintext_password_fiasco
 29 14.323826  10.10.122.128  10.10.73.252   TCP       66 21 → 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 TSval=894825439 TSecr=411040192
 31 16.735293  10.10.122.128  10.10.73.252   FTP       88 Response: 530 Login incorrect.
```

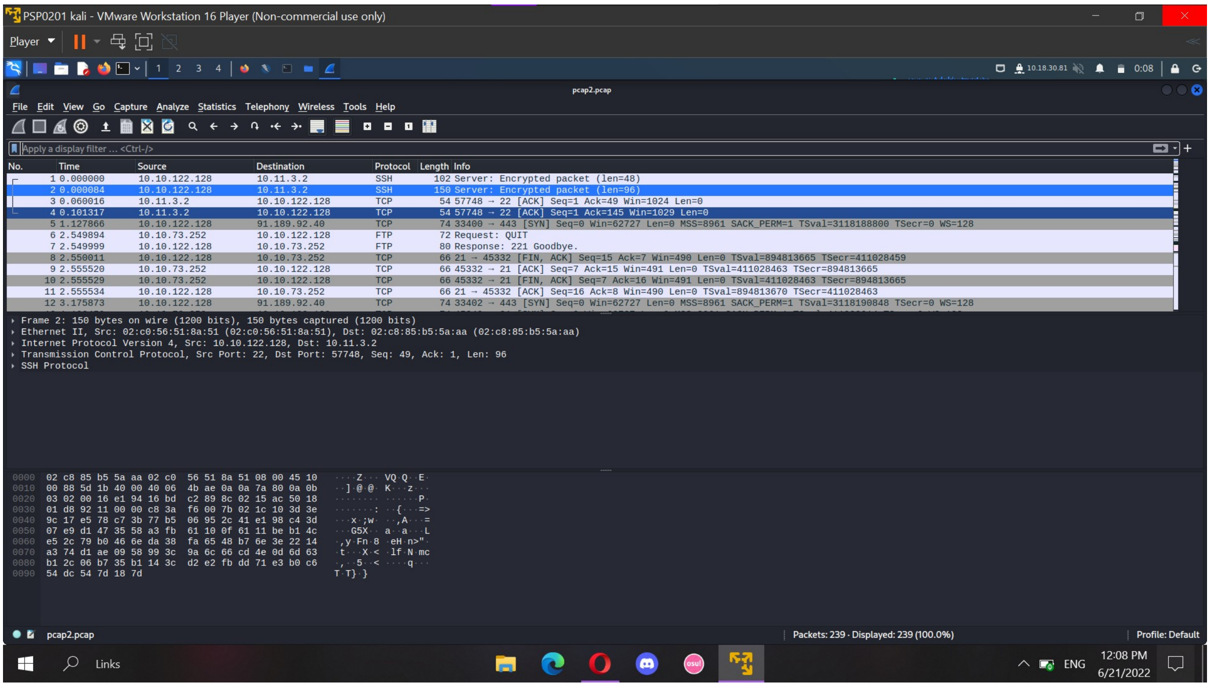
```
› Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
› Ethernet II, Src: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7), Dst: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
› Internet Protocol Version 4, Src: 10.10.73.252, Dst: 10.10.122.128
› Transmission Control Protocol, Src Port: 45340, Dst Port: 21, Seq: 18, Ack: 73, Len: 32
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  02 c0 56 51 8a 51 02 c3  be b5 2e b7 08 00 45 10   ··VQ·Q·· ··.···E·
0010  00 54 0a b5 40 00 40 06  57 4f 0a 0a 49 fc 0a 0a   ·T··@·@· WO··I···
0020  7a 80 b1 1c 00 15 61 48  45 ee 66 93 ff 9e 80 18   z·····aH E·f·····
0030  01 eb f4 12 00 00 01 01  08 0a 18 7f f9 c0 35 55   ········ ······5U
0040  da a5 50 41 53 53 20 70  6c 61 69 6e 74 65 78 74   ··PASS p laintext
0050  5f 70 61 73 73 77 6f 72  64 5f 66 69 61 73 63 6f   _passwor d_fiasco
0060  0d 0a                                              ··
```

pcap2.pcap

Have a look at FTP protocol content or using a filter to make it easier, the leaked password can be found.

Q5.

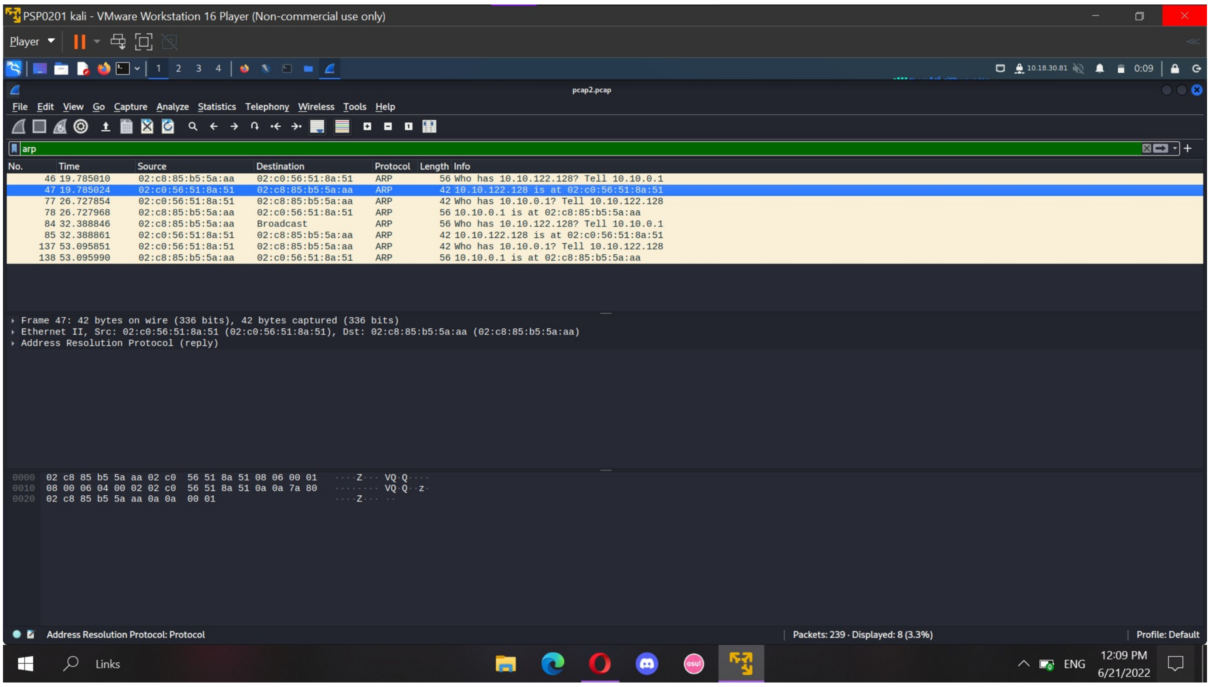


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
10.18.30.81
0:08
Links
ENG
12:08 PM
6/21/2022

```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  10.10.122.128   10.11.3.2       SSH      102 Server: Encrypted packet (len=48)
    2 0.000084  10.10.122.128   10.11.3.2       SSH      150 Server: Encrypted packet (len=96)
    3 0.060016  10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
    4 0.101317  10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
    5 1.127866  10.10.122.128   91.189.92.40    TCP       74 33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188800 TSecr=0 WS=128
    6 2.549894  10.10.73.252    10.10.122.128   FTP       72 Request: QUIT
    7 2.549999  10.10.122.128   10.10.73.252    FTP       80 Response: 221 Goodbye.
    8 2.550011  10.10.122.128   10.10.73.252    TCP       66 21 → 45332 [FIN, ACK] Seq=15 Ack=7 Win=490 Len=0 TSval=894813665 TSecr=411028459
    9 2.555520  10.10.73.252    10.10.122.128   TCP       66 45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
   10 2.555529  10.10.73.252    10.10.122.128   TCP       66 45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411028463 TSecr=894813665
   11 2.555534  10.10.122.128   10.10.73.252    TCP       66 21 → 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 TSecr=411028463
   12 3.175873  10.10.122.128   91.189.92.40    TCP       74 33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118190848 TSecr=0 WS=128

› Frame 2: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
› Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
› Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.11.3.2
› Transmission Control Protocol, Src Port: 22, Dst Port: 57748, Seq: 49, Ack: 1, Len: 96
› SSH Protocol

0000  02 c8 85 b5 5a aa 02 c0  56 51 8a 51 08 00 45 10   ····Z··· VQ·Q··E·
0010  00 88 5d 1b 40 00 40 06  4b ae 0a 0a 7a 80 0a 0b   ··]·@·@· K···z···
0020  03 02 00 16 e1 94 16 bd  c2 89 8c 02 15 ac 50 18   ········ ······P·
0030  01 d8 92 11 00 00 c8 3a  f6 00 7b 02 1c 10 3d 3e   ·······: ··{···=>
0040  9c 17 e5 78 c7 3b 77 b5  06 95 2c 41 e1 98 c4 3d   ···x·;w· ··,A···=
0050  07 e9 d1 47 35 58 a3 fb  61 10 0f 61 11 be b1 4c   ···G5X·· a··a···L
0060  e5 2c 79 b0 46 6e da 38  fa 65 48 b7 6e 3e 22 14   ·,y·Fn·8 ·eH·n>"·
0070  a3 74 d1 ae 09 58 99 3c  9a 6c 66 cd 4e 0d 6d 63   ·t···X·< ·lf·N·mc
0080  b1 2c 06 b7 35 b1 14 3c  d2 e2 fb dd 71 e3 b0 c6   ·,··5··< ····q···
0090  54 dc 54 7d 18 7d                                  T·T}·}

pcap2.pcap                     Packets: 239 · Displayed: 239 (100.0%)        Profile: Default
```

After several observations, SSH protocol is the only one encrypted.

Q6.

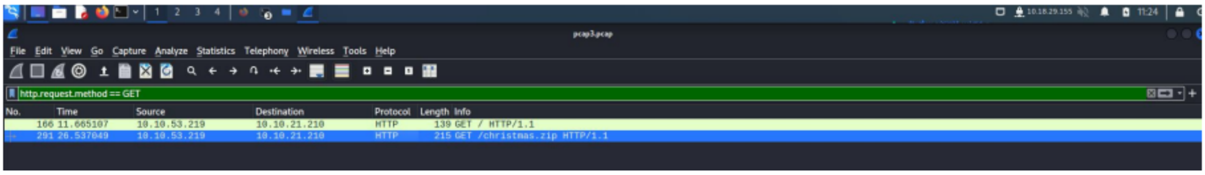


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
10.18.30.81
0:09
Links
ENG
12:09 PM
6/21/2022

```
arp

No.   Time       Source              Destination         Protocol Length Info
   46 19.785010  02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP      56 Who has 10.10.122.128? Tell 10.10.0.1
   47 19.785024  02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP      42 10.10.122.128 is at 02:c0:56:51:8a:51
   77 26.727854  02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP      42 Who has 10.10.0.1? Tell 10.10.122.128
   78 26.727968  02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP      56 10.10.0.1 is at 02:c8:85:b5:5a:aa
   84 32.388846  02:c8:85:b5:5a:aa   Broadcast           ARP      56 Who has 10.10.122.128? Tell 10.10.0.1
   85 32.388861  02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP      42 10.10.122.128 is at 02:c0:56:51:8a:51
  137 53.095851  02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP      42 Who has 10.10.0.1? Tell 10.10.122.128
  138 53.095990  02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP      56 10.10.0.1 is at 02:c8:85:b5:5a:aa

› Frame 47: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
› Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
› Address Resolution Protocol (reply)

0000  02 c8 85 b5 5a aa 02 c0  56 51 8a 51 08 06 00 01   ····Z··· VQ·Q····
0010  08 00 06 04 00 02 02 c0  56 51 8a 51 0a 0a 7a 80   ········ VQ·Q··z·
0020  02 c8 85 b5 5a aa 0a 0a  00 01                     ····Z··· ··

Address Resolution Protocol: Protocol      Packets: 239 · Displayed: 8 (3.3%)      Profile: Default
```

By using the filter, find out the answer. Copy the source and paste it.

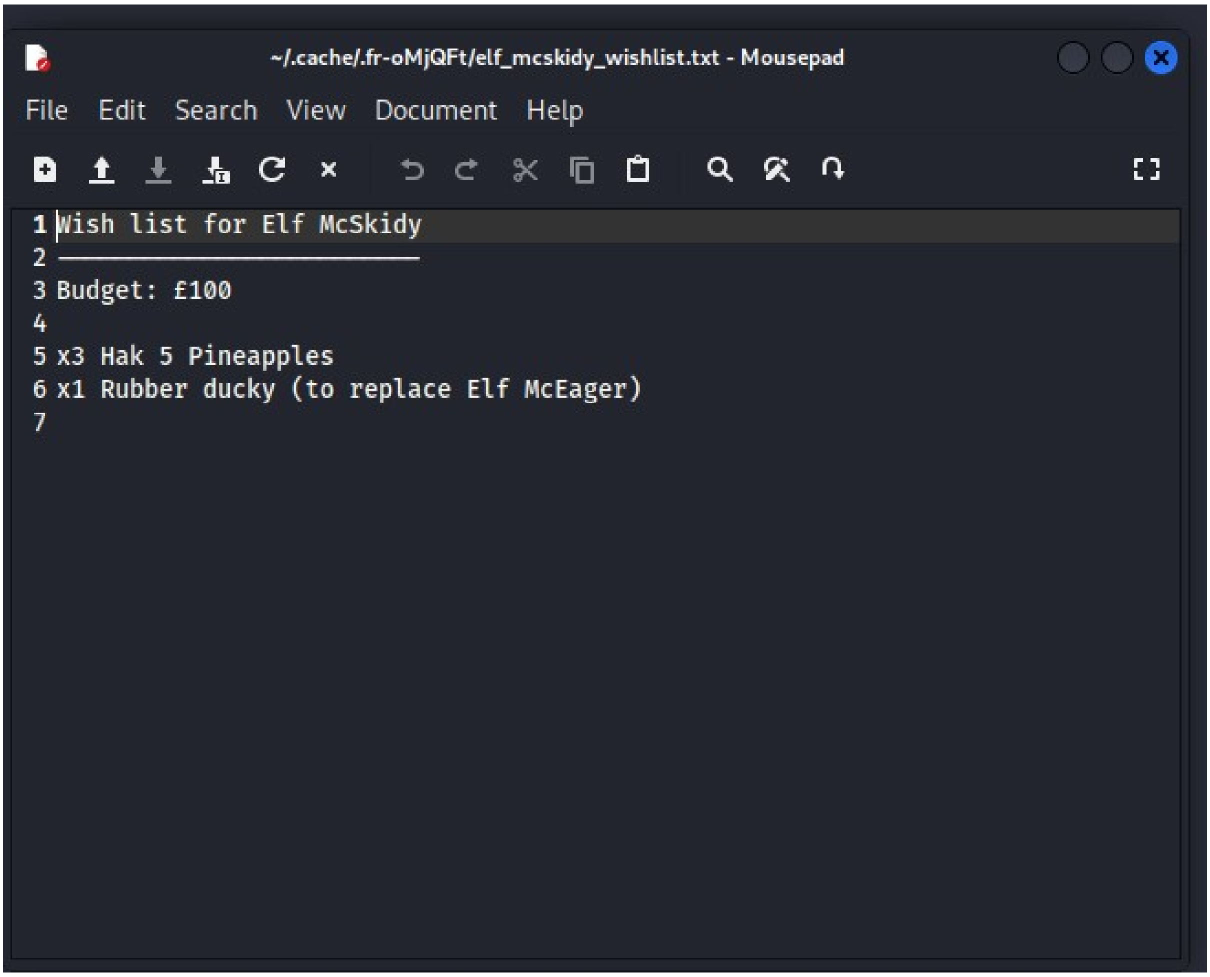
Q7.



pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
10.18.29.155
11:24

```
http.request.method == GET

No.   Time       Source         Destination    Protocol Length Info
  166 11.665107  10.10.53.219   10.10.21.210   HTTP     139 GET / HTTP/1.1
  291 26.537049  10.10.53.219   10.10.21.210   HTTP     215 GET /christmas.zip HTTP/1.1
```

Filter out the content with [get] to find the data. A zip file can be found. Extract and save it.

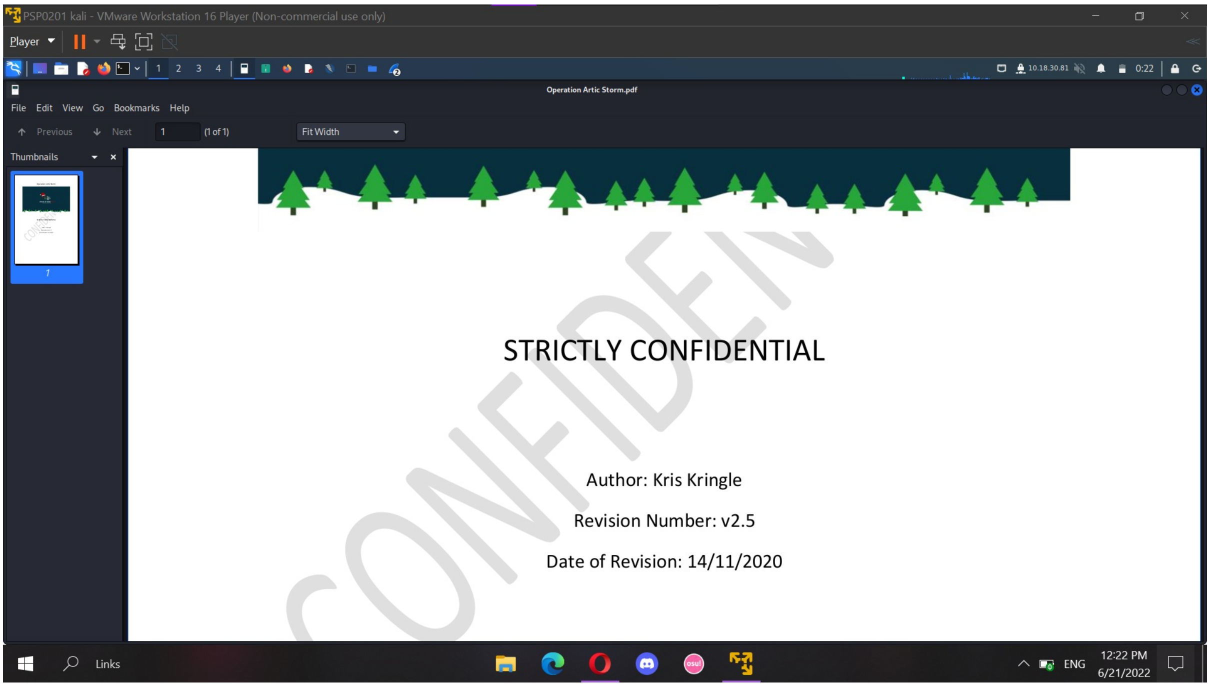


~/.cache/.fr-oMjQFt/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help

```
Wish list for Elf McSkidy
─────────────────────────
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)

```

Open the .txt file and the wishlist can be found.

Q8.



PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
Operation Artic Storm.pdf
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) Fit Width
Thumbnails
CONFIDEN
Links
ENG
12:22 PM
6/21/2022

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

The author can be found in the pdf extracted out from the zip file.