

PSP0201

Week 2

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha Binti Muhd Firdaus	Member

Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

Find “ICMP” under protocol to obtain the IP address and copy it.

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The interface shows a list of packets with columns for No., Time, Source, Destination, Protocol, and Length. Packet 17 is highlighted, showing an ICMP Echo (ping) request from 10.10.15.52 to 10.11.3.2. The packet details pane shows the ICMP Echo (ping) request with ID 0x0001, sequence 1, and TTL 127. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.15.52	10.11.3.2	TCP	182	2222 → 57454 [PSH, ACK] Seq=1 Ack=1 Win=474 Len=48
2	0.000002	10.10.15.52	10.11.3.2	TCP	150	2222 → 57454 [PSH, ACK] Seq=49 Ack=1 Win=474 Len=96
3	0.000155	10.10.15.52	10.11.3.2	TCP	182	2222 → 57454 [PSH, ACK] Seq=145 Ack=1 Win=474 Len=48
4	0.033155	10.11.3.2	10.10.15.52	TCP	54	57454 → 2222 [ACK] Seq=1 Ack=49 Win=1027 Len=0
5	0.033157	10.11.3.2	10.10.15.52	TCP	54	57454 → 2222 [ACK] Seq=1 Ack=193 Win=1026 Len=0
6	2.507709	10.10.15.52	91.189.88.184	TCP	74	39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776387896 TSecr=0 WS=1
7	2.507792	10.10.15.52	91.189.88.185	TCP	74	34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522891897 TSecr=0 WS=1
8	3.537289	10.10.15.52	91.189.88.185	ICMP	72	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=5
9	3.537499	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1
10	3.697100	10.10.15.52	91.189.88.185	ICMP	72	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522891897 TSecr=0 WS=1
11	5.553381	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1
12	5.553594	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=5
13	9.005543	10.11.3.2	10.10.15.52	TCP	55	57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
14	9.005564	10.10.15.52	10.11.3.2	TCP	66	80 → 57463 [ACK] Seq=1 Ack=2 Win=491 Len=0 SFE=1 SRE=2
15	9.585388	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=5
16	9.585482	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1
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)
25	13.837385	10.10.15.52	91.189.88.184	TCP	74	58112 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522891897 TSecr=0 WS=1
26	15.601506	10.10.15.52	10.11.3.2	TCP	54	80 → 57463 [FIN, ACK] Seq=1 Ack=2 Win=491 Len=0
27	15.616777	10.11.3.2	10.10.15.52	TCP	54	57463 → 80 [ACK] Seq=2 Ack=2 Win=1029 Len=0
28	17.602711	10.10.15.52	10.11.3.2	TCP	54	80 → 57463 [RST, ACK] Seq=2 Ack=2 Win=491 Len=0

Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 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 00 00 45 00k...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 wabcedfg hi

Question 2

Read through and use the correct filter based on the description with the operator given.

Networks are, however, rather noisy...Wireshark captured 2,648 packets after a single minute on my machine. This makes analysing very hard. Thankfully, we can use filters to narrow down the results. We can filter by many things, but we'll only cover a couple of important ones in the table below. Note that all the examples below use the `==` operator to see if the filter exactly matches the value we give it.

Filter	Description	Example
ip.src	Show all packets that originate from the specified IP address	<code>ip.src == 192.168.1.1</code>
ip.dst	Show all packets that are destined to the specified IP address	<code>ip.dst == 192.168.1.1</code>
tcp.udp.port	Show all packets that are sent via the protocol and port specified	<code>tcp.port == 22 / udp.port == 67</code>
protocol.request.method	Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a <code>GET</code> and <code>POST</code> to retrieve and submit data accordingly.	<code>http.request.get / http.request.post</code>

Question 3

Remain using the filter in the search bar and find the name of the article that the given IP address had visited. Then, copy it.

The screenshot shows the Wireshark interface with the filter `http.request.method == GET` applied. The packet list pane displays a series of HTTP GET requests. The selected packet (No. 471) is a GET request for `/posts/post/index.json` from source IP `10.10.67.199` to destination IP `10.10.15.52`. The packet details pane shows the following information:

- Frame 471: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)
- Ethernet II, Src: MS-NLB-PhysServer-32, Dst: 02:89:03:cb:7f:6b (02:89:03:cb:7f:6b)
- Internet Protocol Version 4, Src: 10.10.67.199, Dst: 10.10.15.52
- Transmission Control Protocol, Src Port: 55658, Dst Port: 80, Seq: 1192, Ack: 1742344, Len: 299
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the HTTP request, including the status line `200 200 OK (application/json)` and the response body.

Question 4

Use the correct filter based on the given important ones, to search and find the right clue to the login info.

Wireshark packet capture showing an FTP session. The filter is `tcp.prt == 21`. The selected packet is packet 66, a TCP segment from 10.10.73.252 to 10.10.122.128, Seq=45332, Ack=15, Win=491, Len=0. The packet details show it's a FIN, ACK segment. The packet bytes show the raw data.

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	0.000916	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=1024 Len=0
5	1.127866	10.10.122.128	91.189.92.40	TCP	74	33400 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188900 TSecr=0 WS=...
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	2.550911	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=...
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 TS...
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	4.105584	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
18	6.247931	10.10.122.128	91.189.92.40	TCP	74	33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118193920 TSecr=0 WS=...
19	7.291840	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3...
20	7.866325	10.10.73.252	10.10.122.128	FTP	63	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
24	9.863853	10.10.122.128	91.189.92.40	TCP	74	33398 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196736 TSecr=0 WS=...
25	9.287952	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3...
26	11.367850	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] 33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3...
27	13.415851	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3...
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
29	14.292026	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=73 Ack=60 Win=62720 Len=0 TSval=1004025420 TSecr=411040103

Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 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: 45332, Dst Port: 21, Seq: 1, Ack: 1, Len: 6
 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 3a e4 7f 40 00 40 06 7d 9e 0a 0e 49 fc 0a 0a .:..@.}...I...
 0020 7a 80 b1 14 00 15 e0 fa 88 77 65 64 f6 db 80 18 Z.....wed....
 0030 01 eb 00 e2 00 00 01 01 08 0a 18 7f cb eb 35 54-.....ST
 0040 63 03 51 55 49 54 0d 0a c QUIT..

Then, right click on the mouse and choose the “follow” option. Proceed by clicking the TCP stream.

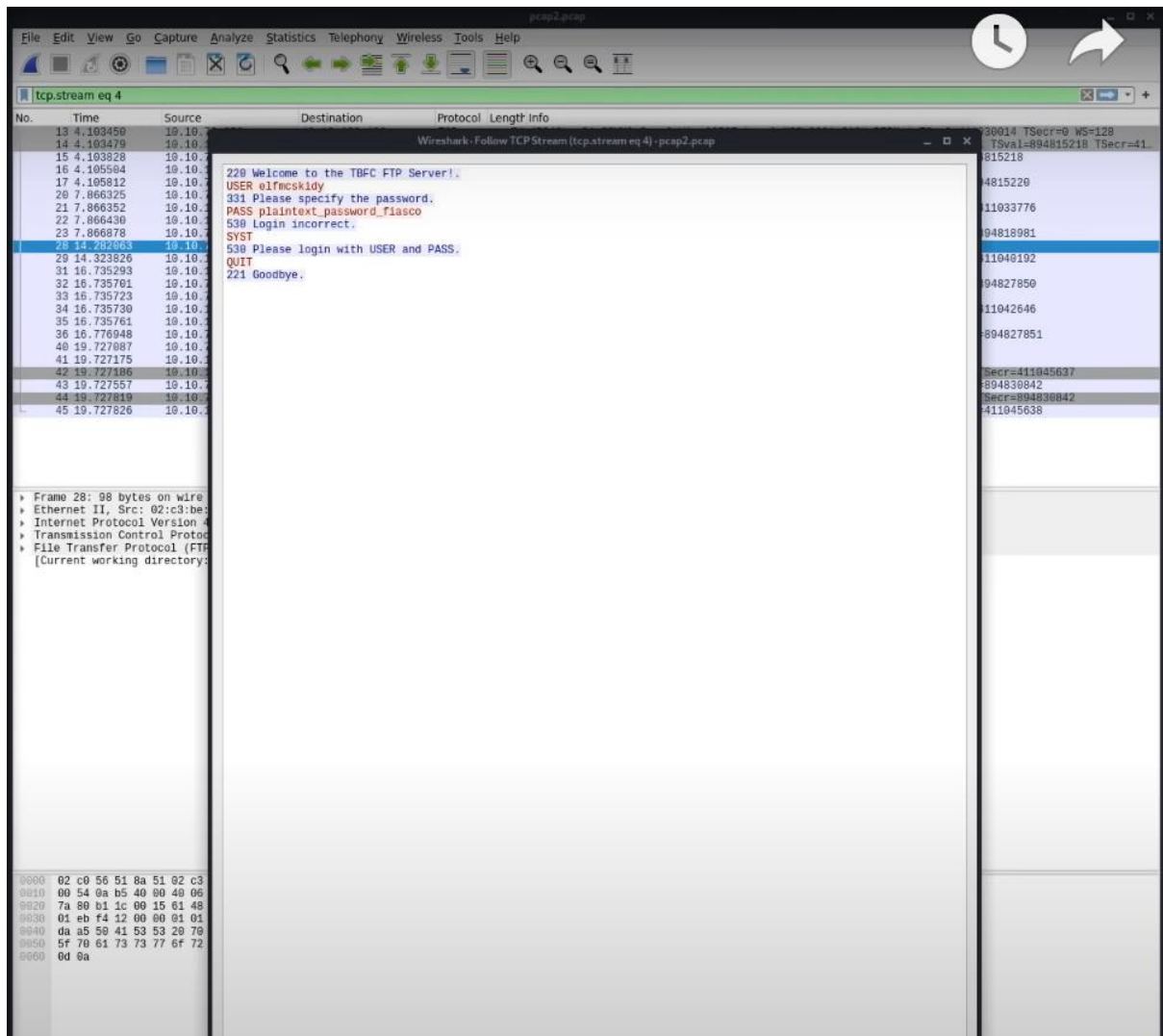
tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	162	Server: Encrypted packet (len=48)
2	0.000000	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)
3	0.060916	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	1.142166	10.10.122.128	91.189.92.48	TCP	74	33490 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188880 TSecr=0 WS=128
6	2.549854	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	2.550911	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=411928459
9	2.555529	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411928463 TSecr=894813665
10	2.555529	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [FIN, ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411928463 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=411928463
12	3.175873	10.10.122.128	91.189.92.48	TCP	74	33492 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=3118199848 TSecr=0 WS=128
13	4.103456	10.10.73.252	10.10.122.128	TCP	74	45340 → 21 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=411936014 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=0 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=411936014 TSecr=894815218
16	4.105812	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=39 Win=0 Len=0 TSval=411936014 TSecr=894815218
17	4.105812	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=39 Win=0 Len=0 TSval=411936014 TSecr=894815218
18	6.247931	10.10.122.128	91.189.92.48	TCP	74	33492 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=3118199848 TSecr=0 WS=128
19	7.272840	10.10.122.128	91.189.92.48	TCP	74	33492 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=3118199848 TSecr=0 WS=128
20	7.866352	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfes@sidy
21	7.866352	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=39 Ack=18 Win=0 Len=0 TSval=411936014 TSecr=894815218
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the filename
23	7.866878	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=18 Ack=73 Win=0 Len=0 TSval=411936014 TSecr=894815218
24	9.963853	10.10.122.128	91.189.92.48	TCP	74	33398 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=8961 SACK_PERM=1 TSval=3118199848 TSecr=0 WS=128
25	9.287852	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33492 → 443
26	11.367850	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33492 → 443
27	13.415851	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33492 → 443
28	14.282863	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password
29	14.293296	10.10.73.252	10.10.122.128	FTP	66	21 → 45340 [ACK] Seq=73 Ack=72 Len=0 TSval=411936014 TSecr=894815218

Frame 16: 164 bytes on wire (832 bits), 164 bytes captured (832 bits) on interface 0
 Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7)
 Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
 Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
 File Transfer Protocol (FTP)
 [Current working directory:]

0000 02 c3 be b5 2e b7 02 c0 56 51 8a 51 08 00 45 00 VQ Q E
 0010 00 5a cc 85 40 80 40 06 95 88 0a 0a 7a 80 0a 0a Z . @ . . . Z . .
 0020 49 fc 98 15 b1 1c 06 93 ff 56 61 48 45 0d 00 18 I T . VaHE . .
 0030 01 ea d8 dc 00 00 01 01 08 0a 35 55 cb f4 10 7f SU . . .
 0040 d1 fe 32 32 30 20 57 65 6c 63 6f 6d 65 20 74 6f . 220 We lcome to
 0050 20 74 68 65 20 54 42 46 43 20 46 54 50 20 53 65 the TB C FTP Se
 0060 72 76 65 72 21 2e 0d 0a rver! . . .

Results would be shown, find the password and copy it.



Question 5

Cancel "tcp.stream eq 4" and find the name of the protocol that is encrypted. Then, copy it.

pcap2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

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	0.060816	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	91.189.92.48	TCP	74	33400 → 443 [SYN] Seq=0 Win=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	2.550811	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	91.189.92.48	TCP	74	33402 → 443 [SYN] Seq=0 Win=0 MSS=8961 SACK_PERM=1 TSval=3118190848 TSecr=0 WS=128
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
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	4.105584	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
18	6.247931	10.10.122.128	91.189.92.48	TCP	74	33404 → 443 [SYN] Seq=0 Win=0 MSS=8961 SACK_PERM=1 TSval=3118193920 TSecr=0 WS=128
19	7.271846	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfrskidy
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
24	9.060853	10.10.122.128	91.189.92.48	TCP	74	33398 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118190736 TSecr=0 WS=128
25	9.287852	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
26	11.367850	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
27	13.415851	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
29	14.292094	10.10.73.252	10.10.122.128	FTP	88	31 → 45340 [ACK] Seq=73 Ack=60 Win=62720 Len=0 TSval=8948196420 TSecr=411040103

Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: 02:c3:b5:2e:b7 (02:c3: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 b5 2e b7 08 00 45 10 ..VQ Q E
0010 00 54 0a b5 40 00 48 06 57 4f 0a 0a 49 fc 0a 0a T I . . .
0020 7a 90 01 1c 00 15 61 48 45 0e 66 93 ff 9a 80 18 Z a H E f
0030 01 eb f4 12 00 00 01 01 08 0a 18 7f f9 c0 35 55 5U
0040 da 50 41 53 53 29 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

Question 6

From the same place we stopped at question 5, find who has 10.10.122.128. Then copy it.

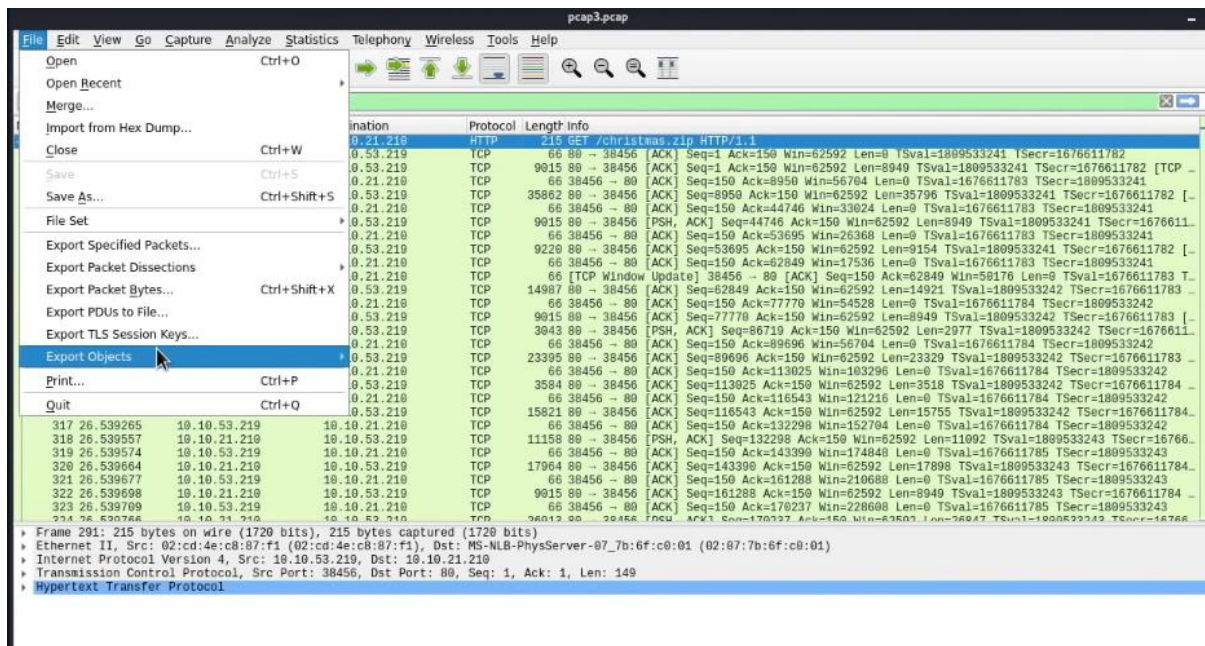
Apply a display filter ... <Ctrl-F>

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	0.060816	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	91.189.92.48	TCP	74	33400 → 443 [SYN] Seq=0 Win=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	2.550811	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	91.189.92.48	TCP	74	33402 → 443 [SYN] Seq=0 Win=0 MSS=8961 SACK_PERM=1 TSval=3118190848 TSecr=0 WS=128
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
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	4.105584	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
18	6.247931	10.10.122.128	91.189.92.48	TCP	74	33404 → 443 [SYN] Seq=0 Win=0 MSS=8961 SACK_PERM=1 TSval=3118193920 TSecr=0 WS=128
19	7.271846	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfrskidy
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
24	9.060853	10.10.122.128	91.189.92.48	TCP	74	33398 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118190736 TSecr=0 WS=128
25	9.287852	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
26	11.367850	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
27	13.415851	10.10.122.128	91.189.92.48	TCP	74	[TCP Retransmission] 33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
29	14.292094	10.10.73.252	10.10.122.128	FTP	88	31 → 45340 [ACK] Seq=73 Ack=60 Win=62720 Len=0 TSval=8948196420 TSecr=411040103

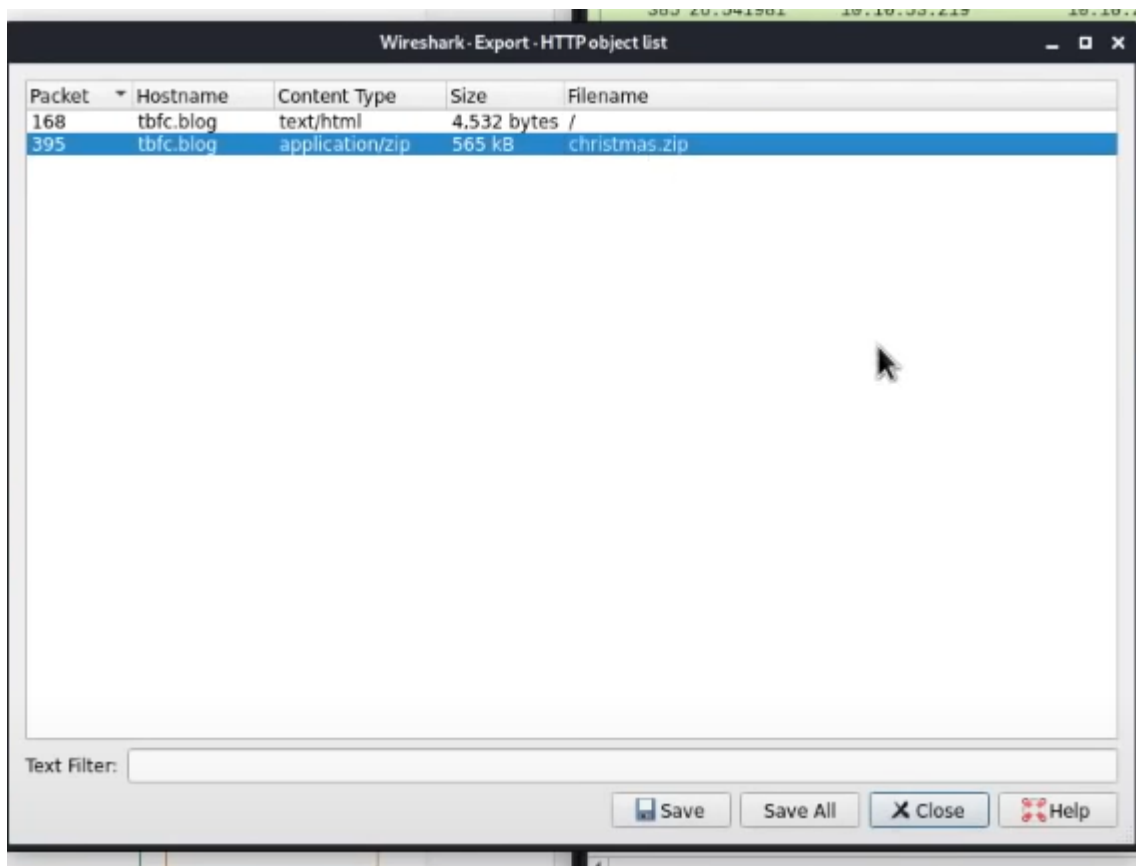
Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: 02:c3:b5:2e:b7 (02:c3:b5:2e:b7), Dst: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
Internet Protocol Version 4, Src: 10.10.73.252, Dst: 10.10.122.128
Transmission Control Protocol, Src Port: 45340, Dst Port: 21, Seq: 18, Ack: 73, Len: 32
File Transfer Protocol (FTP)
[Current working directory:]

Question 7

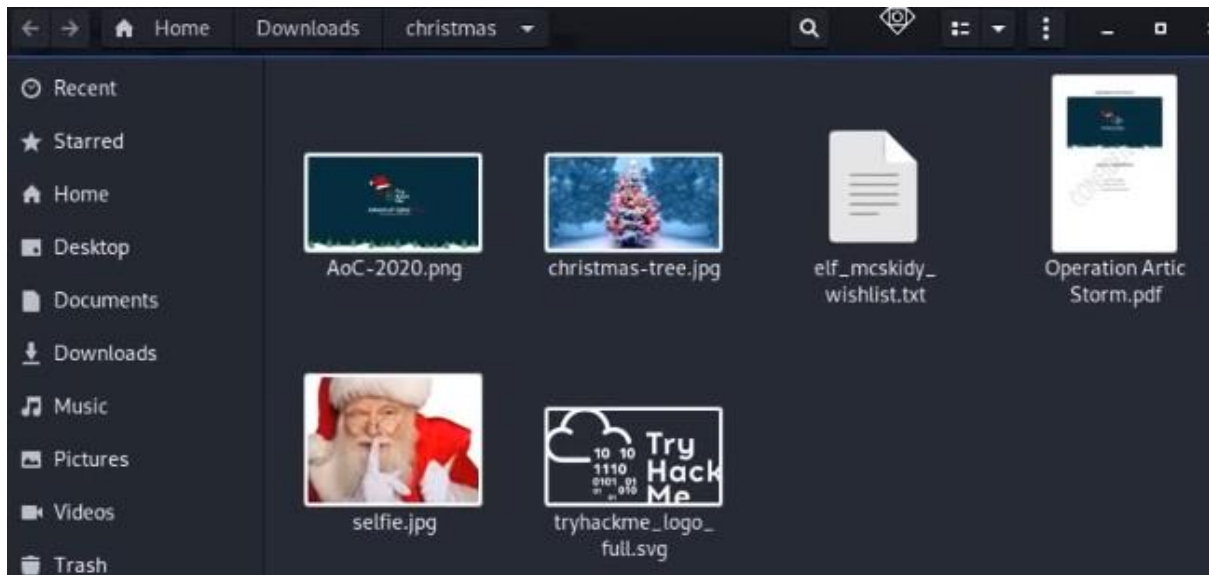
Find “GET /christmas.zip HTTP/” under the pcap3.pcap file and click on the export objects for the HTTP option.



The export object list would be shown and choose the christmas.zip to save it in the directory.



Open the directory and double click on the “elf_mcskidy_wishlist.txt”.



Then, find and choose the correct wish list that will be used to replace Elf McEager. Copy it.

```
File Edit Search View Document Help
Wish list for Elf McSkidy
Budget: £100
x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

Question 8

From the same directory of the zip files, click on the Operation Artic to open it. This will give us the author's name.

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Thought Process/Methodology:

Firstly, we downloaded the ZIP file "aocpcaps.zip" under the Challenge section to have access to the task files. We proceeded on opening the "pcap1.pcap" file and managed to find the IP address that initiated "ICMP" under protocol. We then went through the few important filters given together with its description to find the correct filter by using the operator (==). We also typed in the filter in the search section to double check our answer. We continued using the same filter in the search bar to find the name of the article that the given IP address (10.10.67.199) had visited. Next, we opened the "pcap2.pcap" file. As there were many irrelevant information that would confuse us, we started by using the correct filter from the table of important filters to find the right clue of the login information. We then right clicked on the correct clue that we found to access the TCP stream. This stream showed us the results of the login credentials and thus we managed to find the right password that was leaked during the login process from the captured FTP traffic. Next, we needed to cancel "tcp.stream eq 4" from the search bar in order to find the right protocol from the source given. We then find the information of who has 10.10.122.128 from the same place we found the protocol that was encrypted. Once done, we opened "pcap3.pcap" file for the next question. We proceeded on finding "GET /christmas.zip HTTP/", then we clicked and chose the HTTP under export objects. This action made us export the HTTP object list from Wireshark. Thus, we managed to save the christmas.zip file into the directory. Once saved, we opened the zip file, and we were given images such as christmas tree etc. The "elf_mcskidy_wishlist.txt" file was also included in the zip file. So, we opened it and were given Elf McSkidy's wishlist that was used to replace Elf McEager. Lastly,

from the same directory of the zip file, we have to open Operation Artic in order to find for the author's name.