PSP0201 Week 3 Writeup

Group Name: ikun no 1

Members

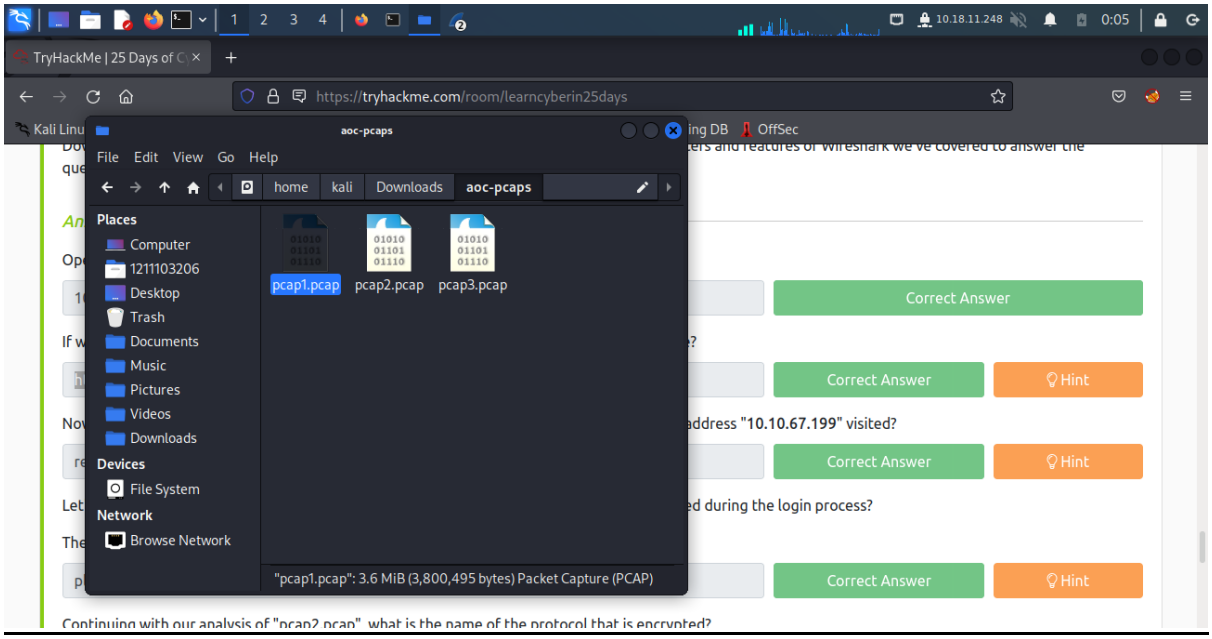
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

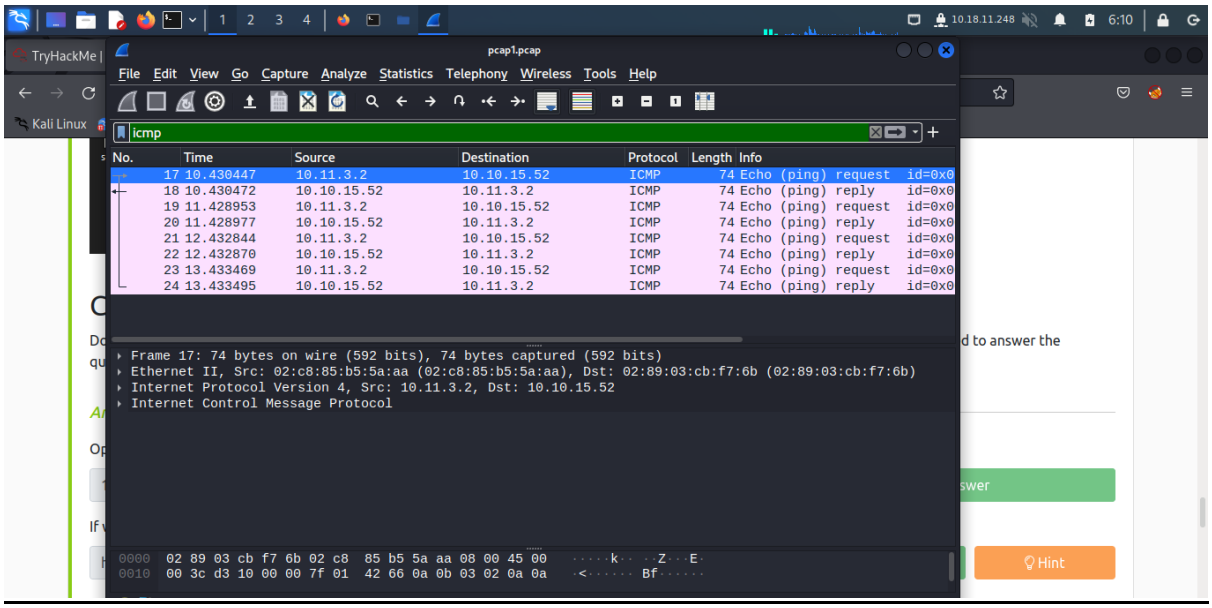
Day 7: Networking The Grinch Really Did Steal Christmas

Tool used: Kali-Linux, WireShark

Solution/walkthrough:

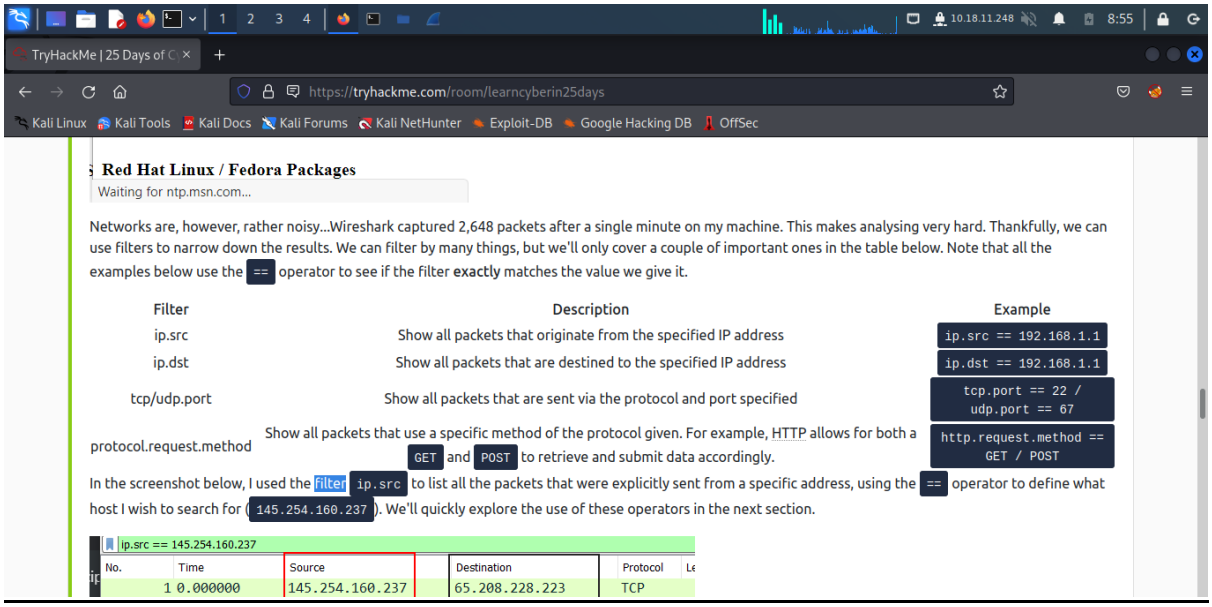
Question 1





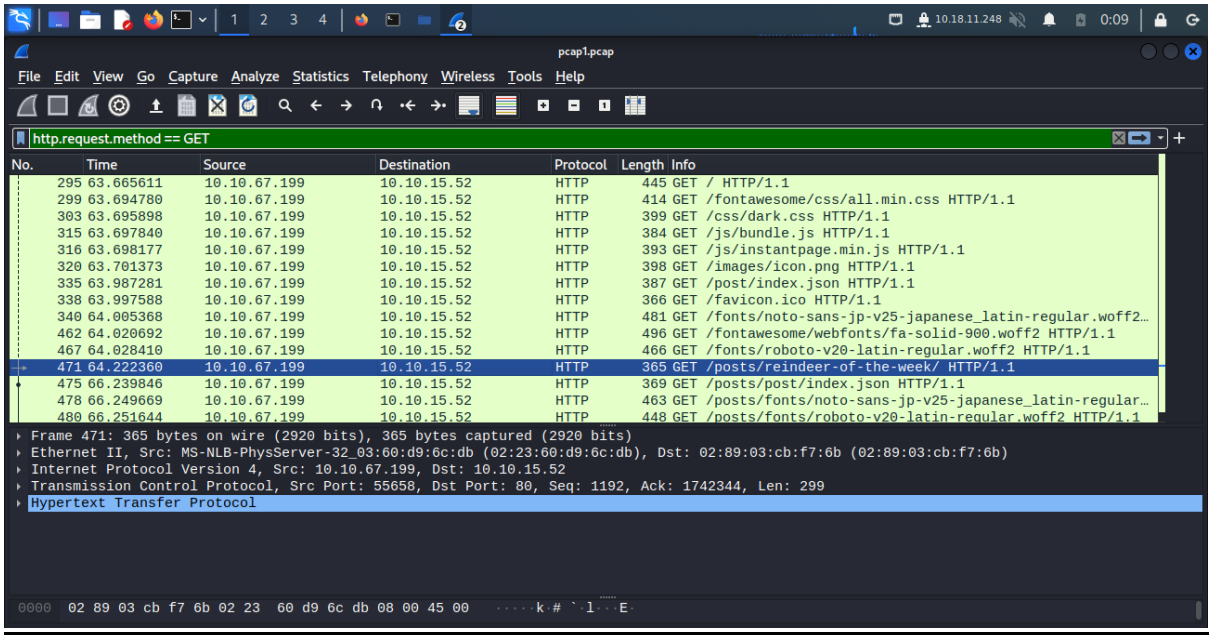
Download the zip file that has given and unzip it. Open pcap1 and type icmp and the ip address shown.

Question 2



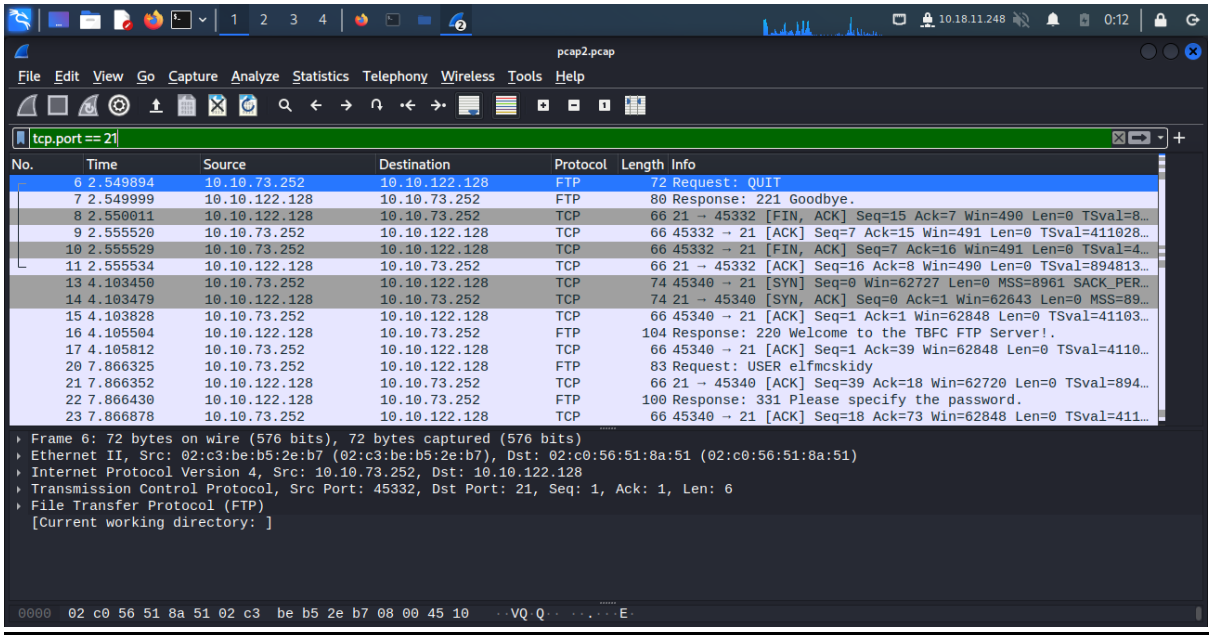
Learn from the THM.

Question 3

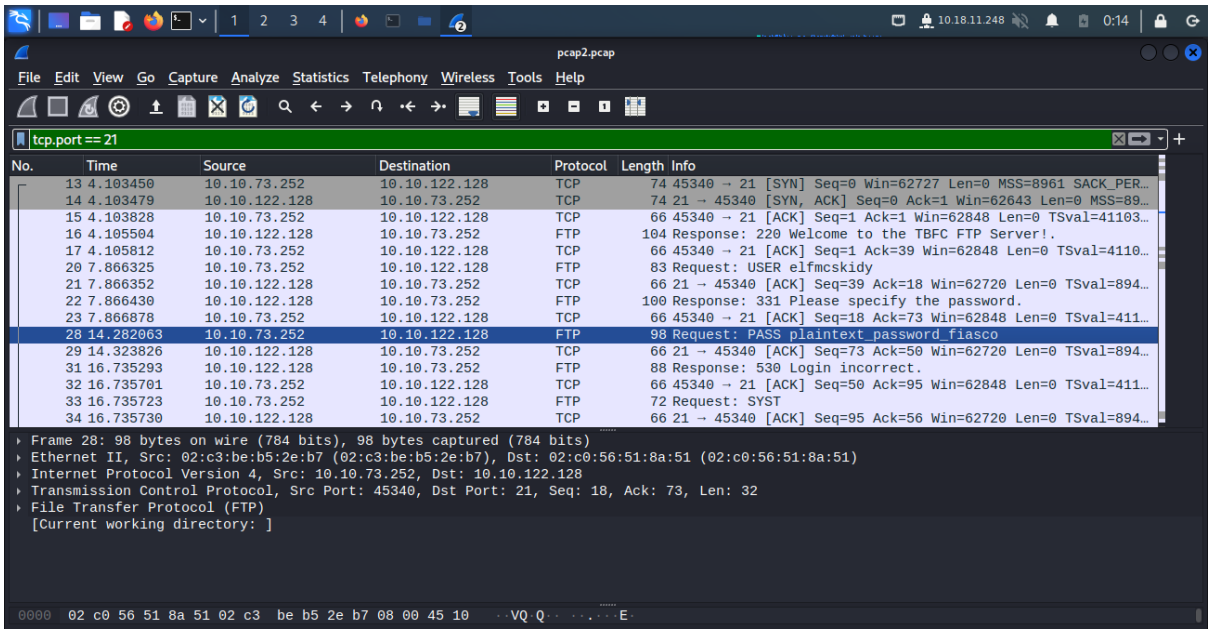


Copy the HTTP GET filter and paste on the search bar and find the answer of article with /posts/.

Question 4

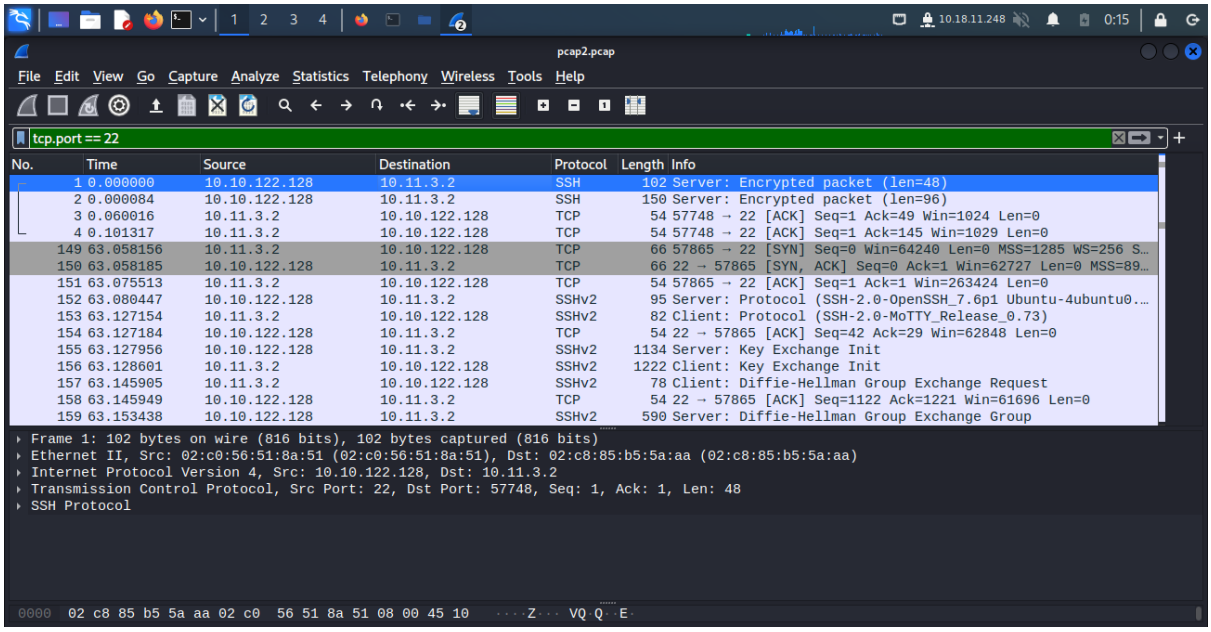


Open pcap2 and use tcp.port == 21 to filter it.



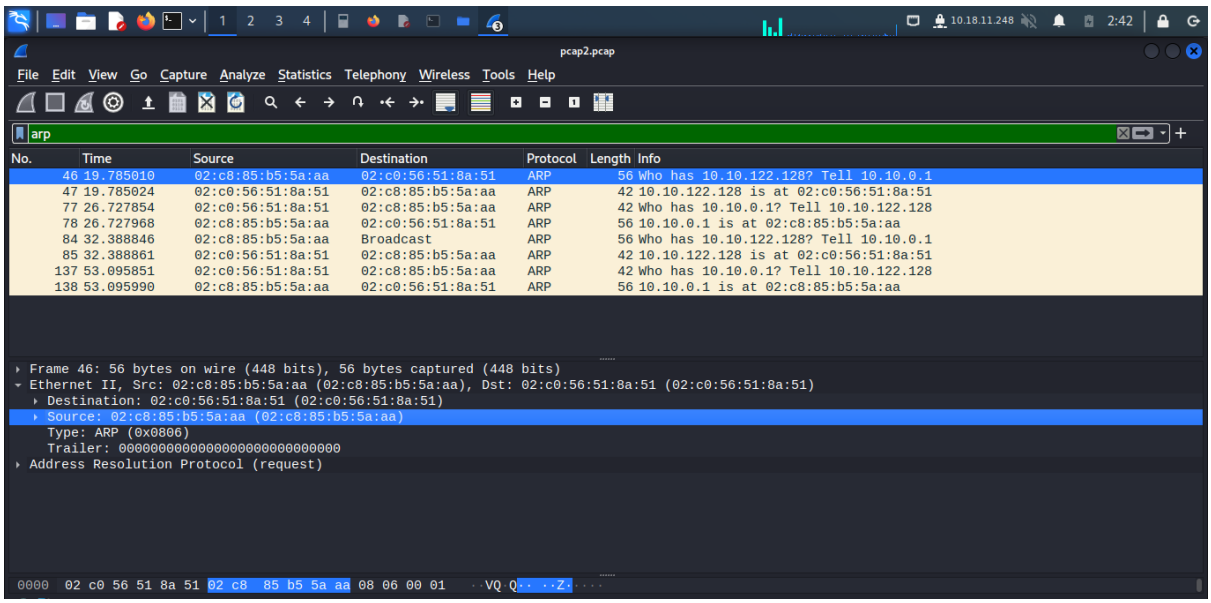
Next, look for the answer. The password shown.

Question 5



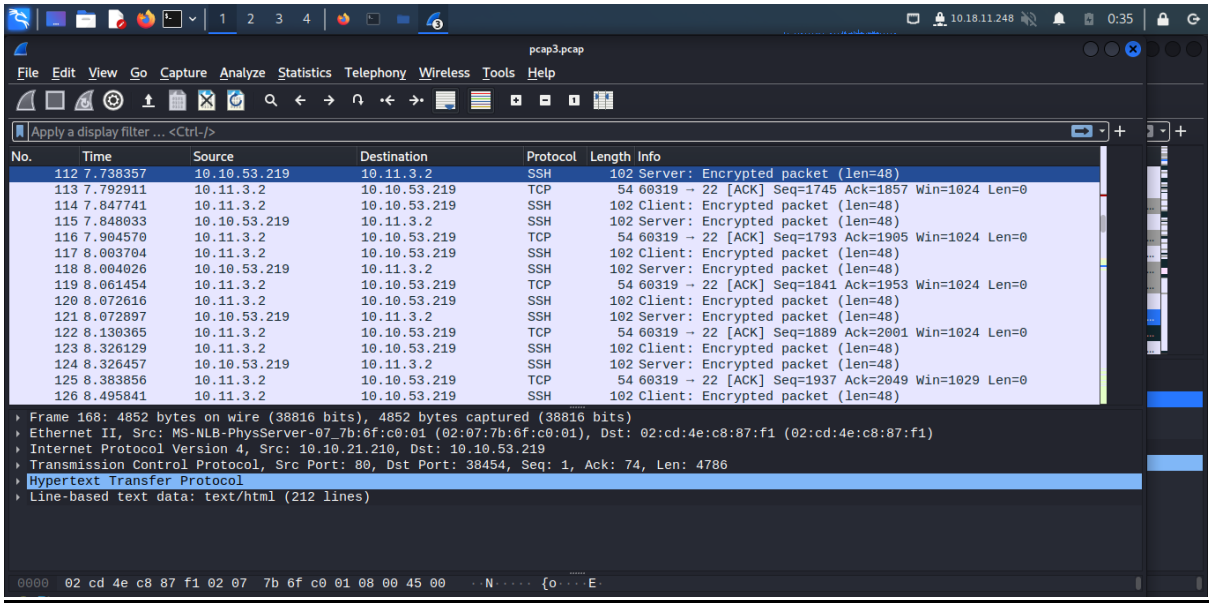
Continue using tcp.port == 22 this filter, change the number of 22 into other number to find the protocol that has been encrypted. Lastly, SSH shown in number 21.

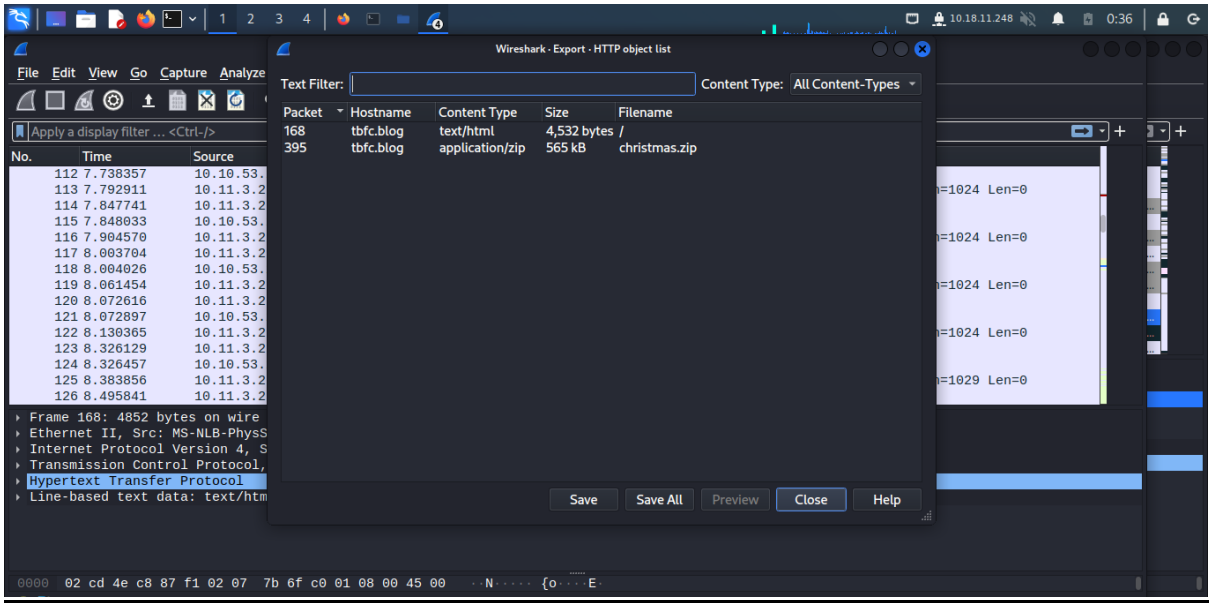
Question 6



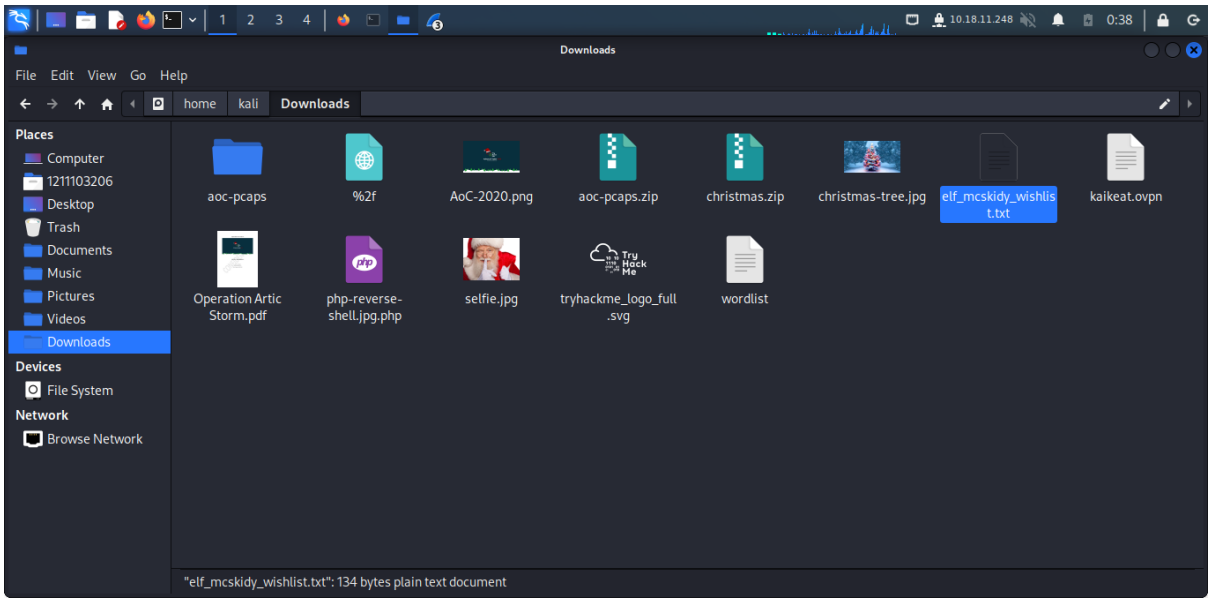
Type arp on the bar and the answer shown.

Question 7

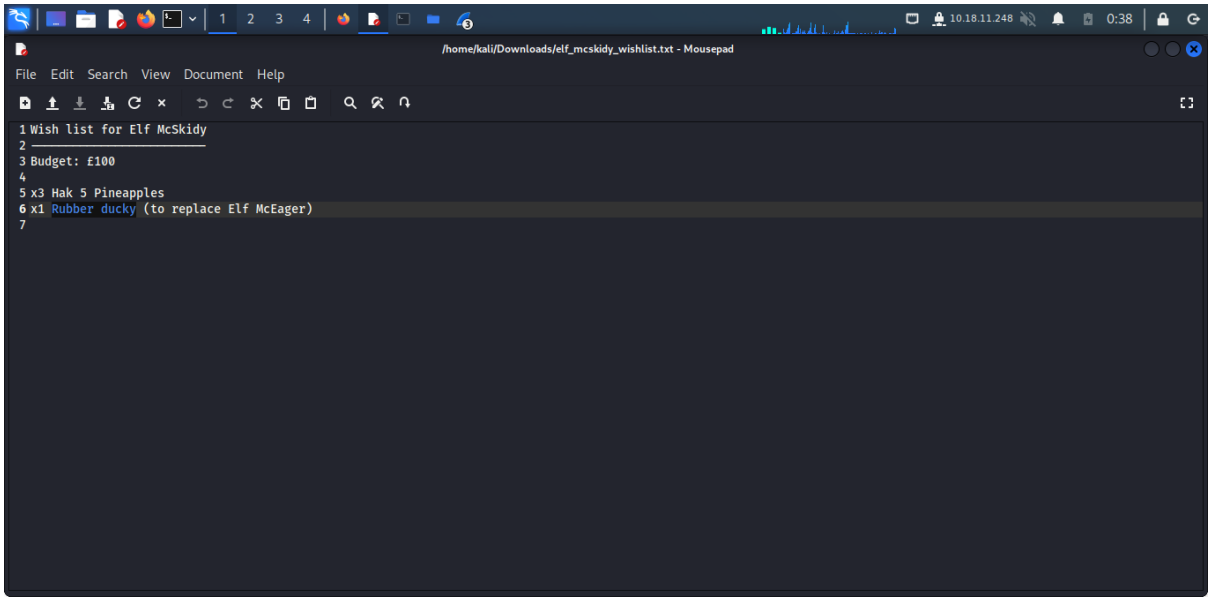

pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
112 7.738357 10.10.53.219 10.11.3.2 SSH 102 Server: Encrypted packet (len=48)
113 7.792911 10.11.3.2 10.10.53.219 TCP 54 60319 → 22 [ACK] Seq=1745 Ack=1857 Win=1024 Len=0
114 7.847741 10.11.3.2 10.10.53.219 SSH 102 Client: Encrypted packet (len=48)
115 7.848033 10.10.53.219 10.11.3.2 SSH 102 Server: Encrypted packet (len=48)
116 7.904570 10.11.3.2 10.10.53.219 TCP 54 60319 → 22 [ACK] Seq=1793 Ack=1905 Win=1024 Len=0
117 8.003704 10.11.3.2 10.10.53.219 SSH 102 Client: Encrypted packet (len=48)
118 8.004026 10.10.53.219 10.11.3.2 SSH 102 Server: Encrypted packet (len=48)
119 8.061454 10.11.3.2 10.10.53.219 TCP 54 60319 → 22 [ACK] Seq=1841 Ack=1953 Win=1024 Len=0
120 8.072616 10.11.3.2 10.10.53.219 SSH 102 Client: Encrypted packet (len=48)
121 8.072897 10.10.53.219 10.11.3.2 SSH 102 Server: Encrypted packet (len=48)
122 8.130365 10.11.3.2 10.10.53.219 TCP 54 60319 → 22 [ACK] Seq=1889 Ack=2001 Win=1024 Len=0
123 8.326129 10.11.3.2 10.10.53.219 SSH 102 Client: Encrypted packet (len=48)
124 8.326457 10.10.53.219 10.11.3.2 SSH 102 Server: Encrypted packet (len=48)
125 8.383856 10.11.3.2 10.10.53.219 TCP 54 60319 → 22 [ACK] Seq=1937 Ack=2049 Win=1029 Len=0
126 8.495841 10.11.3.2 10.10.53.219 SSH 102 Client: Encrypted packet (len=48)
Frame 168: 4852 bytes on wire (38816 bits), 4852 bytes captured (38816 bits)
Ethernet II, Src: MS-NLB-PhysServer-07_7b:6f:c0:01 (02:07:7b:6f:c0:01), Dst: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1)
Internet Protocol Version 4, Src: 10.10.21.210, Dst: 10.10.53.219
Transmission Control Protocol, Src Port: 80, Dst Port: 38454, Seq: 1, Ack: 74, Len: 4786
Hypertext Transfer Protocol
Line-based text data: text/html (212 lines)
0000 02 cd 4e c8 87 f1 02 07 7b 6f c0 01 08 00 45 00


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
168 tbfc.blog text/html 4,532 bytes /
395 tbfc.blog application/zip 565 kB christmas.zip
Save Save All Preview Close Help

Open pcap3 and click export object of this file, there was 2 file shown and save it. After saving the file, unzip the file.

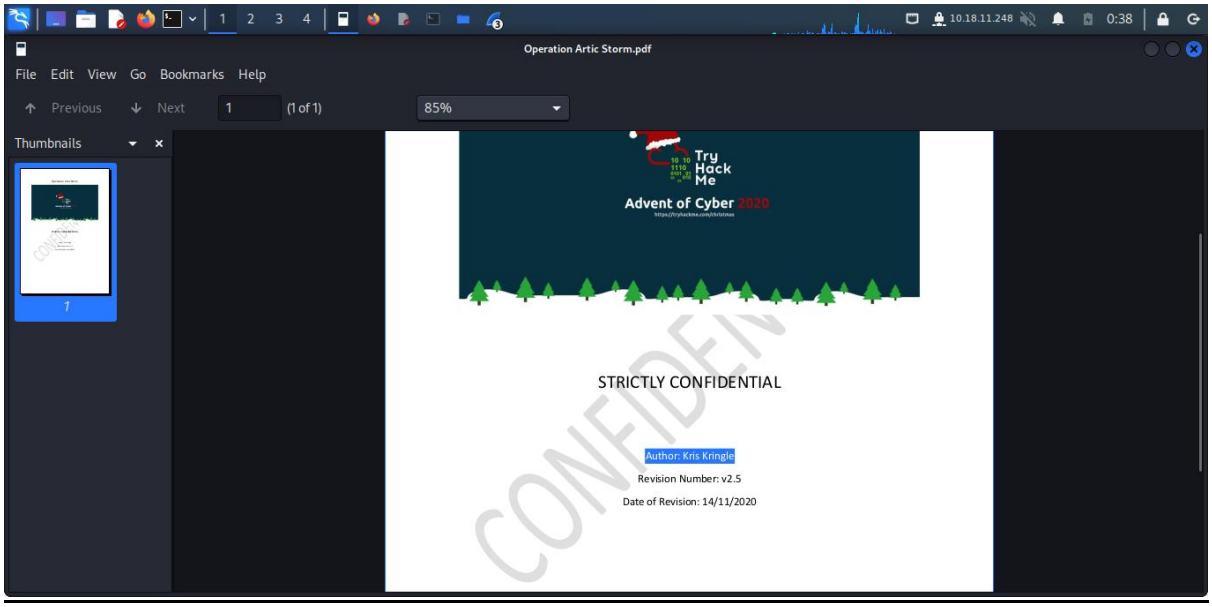


Next, open the txt file.



The answer shown.

Question 8



Open the pdf file that has been unzip, the name of the author shown.