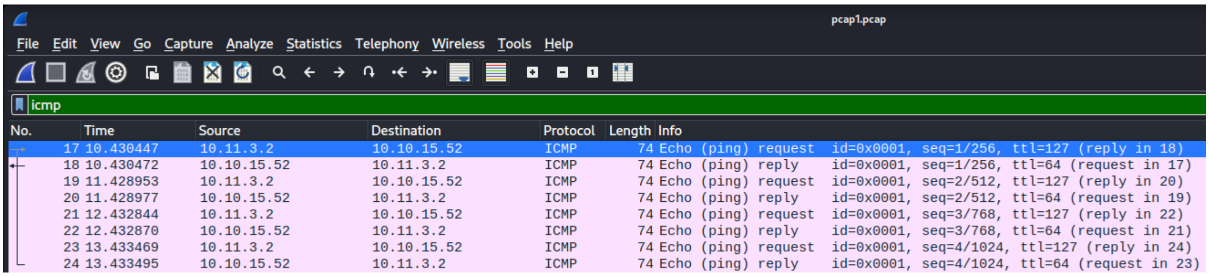
Day 7 - Networking The Grinch Really Did Steal Christmas

List of tools used: Wireshark

Question 1

Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Methodology: We open "pcap1.pcap" in Wireshark. Then, we use filter “icmp” to find package of ICMP protocol. We then find the source address of first ping request is 10.11.3.2.



icmp

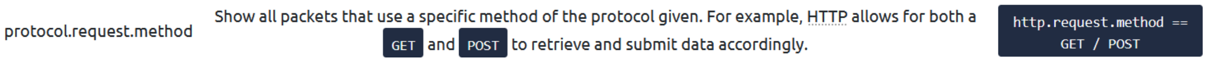
```
No.     Time        Source         Destination    Protocol Length Info
     17 10.430447   10.11.3.2      10.10.15.52    ICMP         74 Echo (ping) request  id=0x0001, seq=1/256, ttl=127 (reply in 18)
     18 10.430472   10.10.15.52    10.11.3.2      ICMP         74 Echo (ping) reply    id=0x0001, 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)
```

Answer: 10.11.3.2

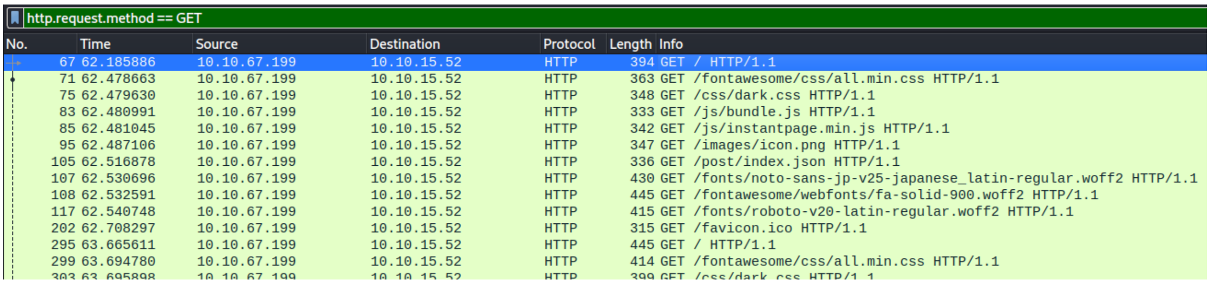
Question 2

If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

Methodology: We can see the guide on TryHackMe and use command “http.request.method == GET” to filter package. We try the filter in Wireshark and it only return package of http GET request with no error.



protocol.request.method	Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a `GET` and `POST` to retrieve and submit data accordingly.	`http.request.method == GET / POST`



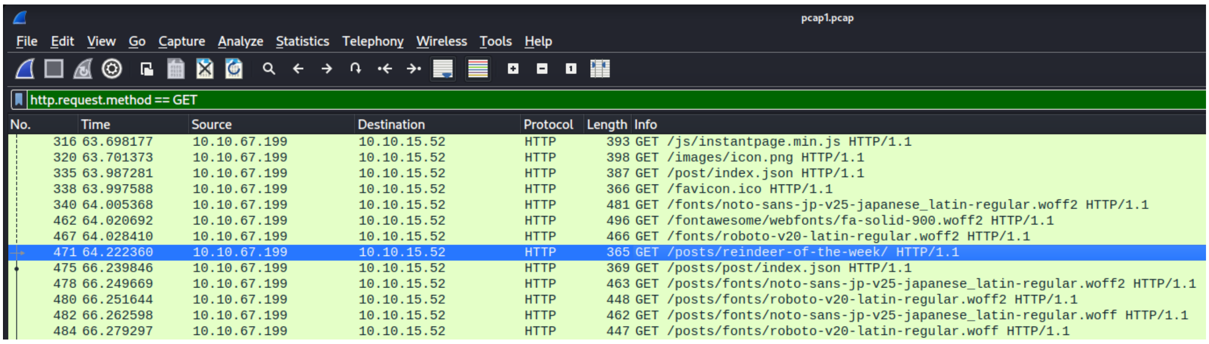
```
http.request.method == GET
No.   Time       Source        Destination   Protocol Length Info
   67 62.185886  10.10.67.199  10.10.15.52   HTTP     394 GET / HTTP/1.1
   71 62.478663  10.10.67.199  10.10.15.52   HTTP     363 GET /fontawesome/css/all.min.css HTTP/1.1
   75 62.479630  10.10.67.199  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 62.487106  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 62.708297  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
  299 63.694780  10.10.67.199  10.10.15.52   HTTP     414 GET /fontawesome/css/all.min.css HTTP/1.1
  303 63.695898  10.10.67.199  10.10.15.52   HTTP     399 GET /css/dark.css HTTP/1.1
```

Answer: http.request.method == GET

Question 3

Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

Methodology: We apply filter “http.request.method == GET” to only see package of http GET request. We then find an article named “reindeer-of-the-week”.


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

http.request.method == GET

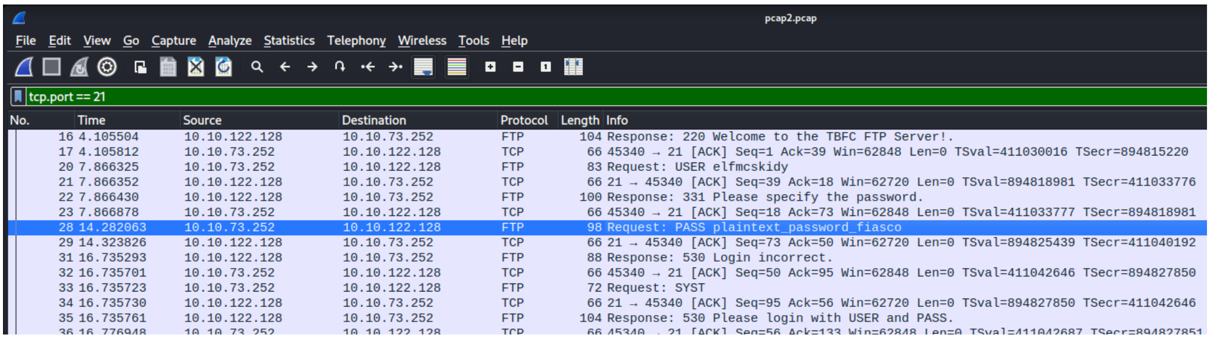
```
No.    Time        Source          Destination     Protocol  Length Info
   316 63.698177   10.10.67.199    10.10.15.52     HTTP       393 GET /js/instantpage.min.js HTTP/1.1
   320 63.701373   10.10.67.199    10.10.15.52     HTTP       398 GET /images/icon.png HTTP/1.1
   335 63.987281   10.10.67.199    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
```

Answer: reindeer-of-the-week

Question 4

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

Methodology: We know FTP is usually running on TCP port 21 so we use filter “tcp.port == 21” to find FTP traffic. We then find the login user is elfmcskidy and the password is plaintext_password_fiasco.


pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 21

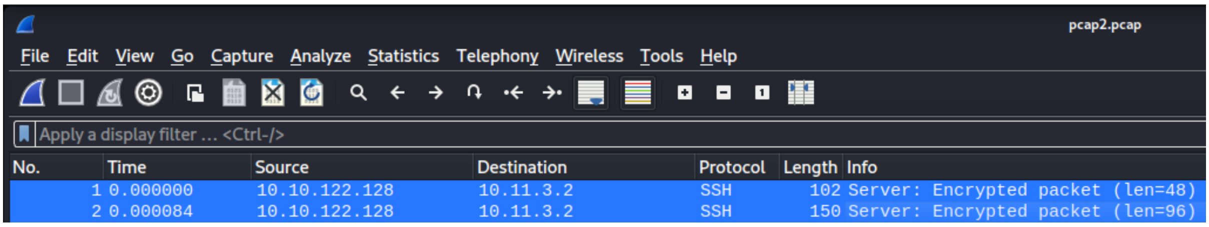
```
No.  Time       Source         Destination    Protocol Length Info
  16 4.105504   10.10.122.128  10.10.73.252   FTP      104 Response: 220 Welcome to the TBFC FTP Server!.
  17 4.105812   10.10.73.252   10.10.122.128  TCP       66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TSecr=894815220
  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.
  32 16.735701  10.10.73.252   10.10.122.128  TCP       66 45340 → 21 [ACK] Seq=50 Ack=95 Win=62848 Len=0 TSval=411042646 TSecr=894827850
  33 16.735723  10.10.73.252   10.10.122.128  FTP       72 Request: SYST
  34 16.735730  10.10.122.128  10.10.73.252   TCP       66 21 → 45340 [ACK] Seq=95 Ack=56 Win=62720 Len=0 TSval=894827850 TSecr=411042646
  35 16.735761  10.10.122.128  10.10.73.252   FTP      104 Response: 530 Please login with USER and PASS.
  36 16.776948  10.10.73.252   10.10.122.128  TCP       66 45340 → 21 [ACK] Seq=56 Ack=133 Win=62848 Len=0 TSval=411042687 TSecr=894827851
```

Answer: plaintext_password_fiasco

Question 5

Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

Methodology: We see Encrypted packet is sending in SSH protocol.


pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

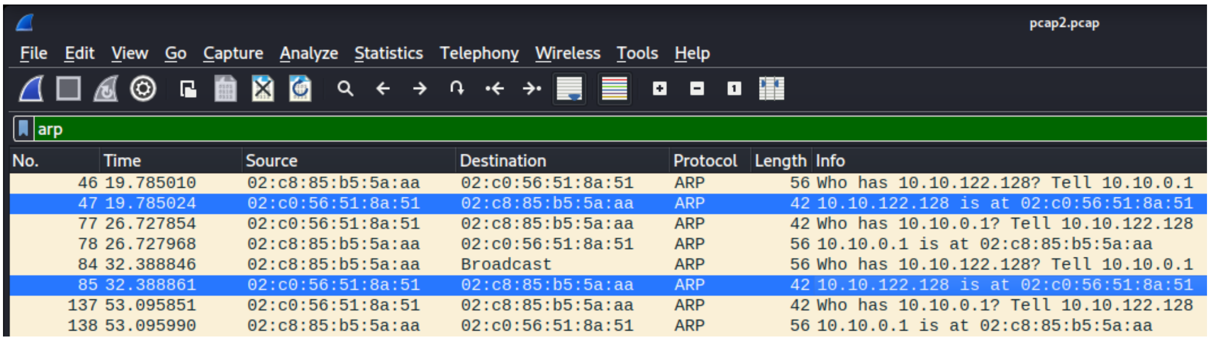
```
No.      Time        Source          Destination    Protocol Length Info
       1 0.000000    10.10.122.128   10.11.3.2      SSH         102 Server: Encrypted packet (len=48)
       2 0.000084    10.10.122.128   10.11.3.2      SSH         150 Server: Encrypted packet (len=96)
```

Answer: SSH

Question 6

Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

Methodology: We use filter “arp” to only see ARP package. Then, we see package with info of “Who has 10.10.122.128? Tell 10.10.10.1” following with “10.10.122.128 is at 02:c0:56:51:8a:51”.



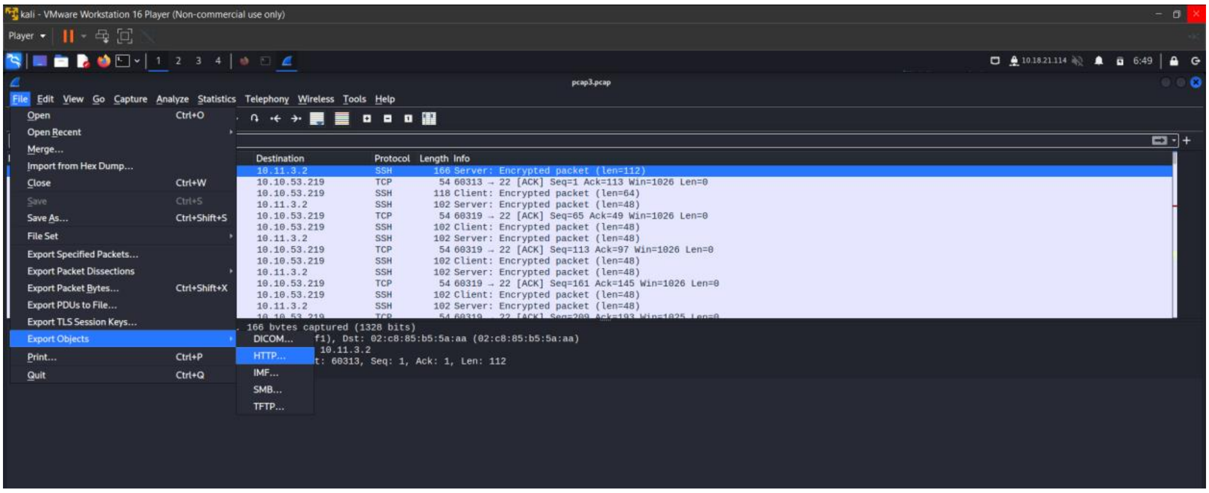
No.	Time	Source	Destination	Protocol	Length	Info
46	19.785010	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
47	19.785024	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
77	26.727854	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 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

Answer: 02:c0:56:51:8a:51

Question 7

Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

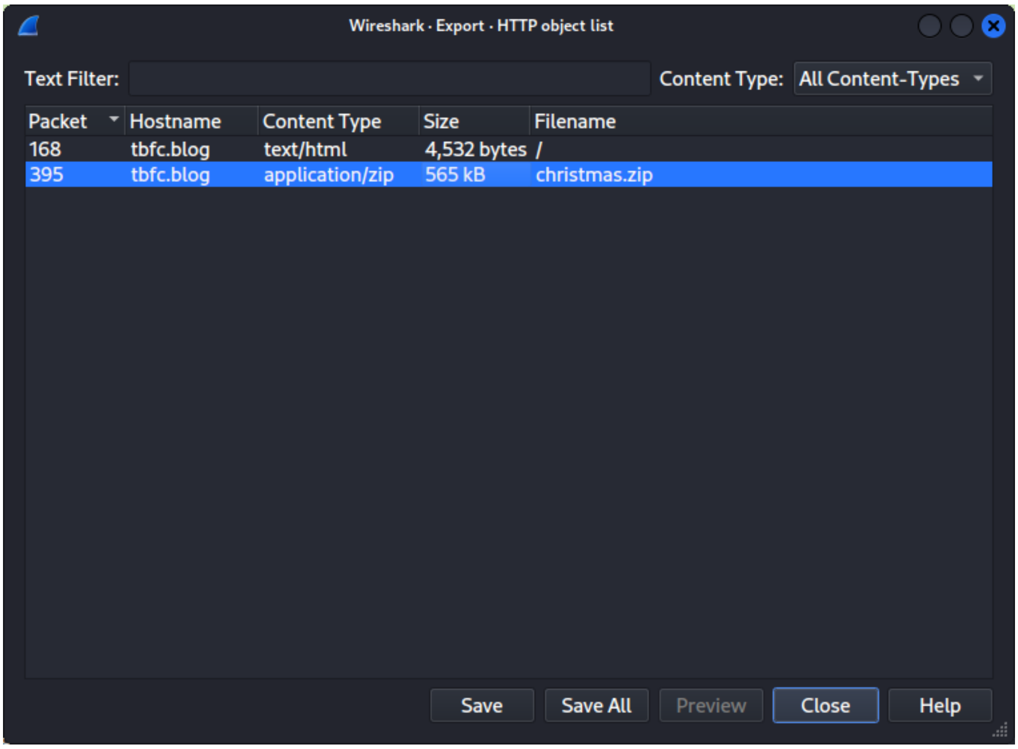
Methodology: We go to File>Export Objects>HTTP to see if there is any exportable package.


kali - VMware Workstation 16 Player (Non-commercial use only)
pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...

```
Destination      Protocol  Length Info
10.11.3.2        SSH          166 Server: Encrypted packet (len=112)
10.10.53.219     TCP           54 60313 → 22 [ACK] Seq=1 Ack=113 Win=1026 Len=0
10.10.53.219     SSH          118 Client: Encrypted packet (len=64)
10.11.3.2        SSH          102 Server: Encrypted packet (len=48)
10.10.53.219     TCP           54 60319 → 22 [ACK] Seq=65 Ack=49 Win=1026 Len=0
10.10.53.219     SSH          102 Client: Encrypted packet (len=48)
10.11.3.2        SSH          102 Server: Encrypted packet (len=48)
10.10.53.219     TCP           54 60319 → 22 [ACK] Seq=113 Ack=97 Win=1026 Len=0
10.10.53.219     SSH          102 Client: Encrypted packet (len=48)
10.11.3.2        SSH          102 Server: Encrypted packet (len=48)
10.10.53.219     TCP           54 60319 → 22 [ACK] Seq=161 Ack=145 Win=1026 Len=0
10.10.53.219     SSH          102 Client: Encrypted packet (len=48)
10.11.3.2        SSH          102 Server: Encrypted packet (len=48)
10.10.53.219     TCP           54 60319 → 22 [ACK] Seq=209 Ack=193 Win=1025 Len=0

166 bytes captured (1328 bits)
f1), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
10.11.3.2
t: 60313, Seq: 1, Ack: 1, Len: 112
```

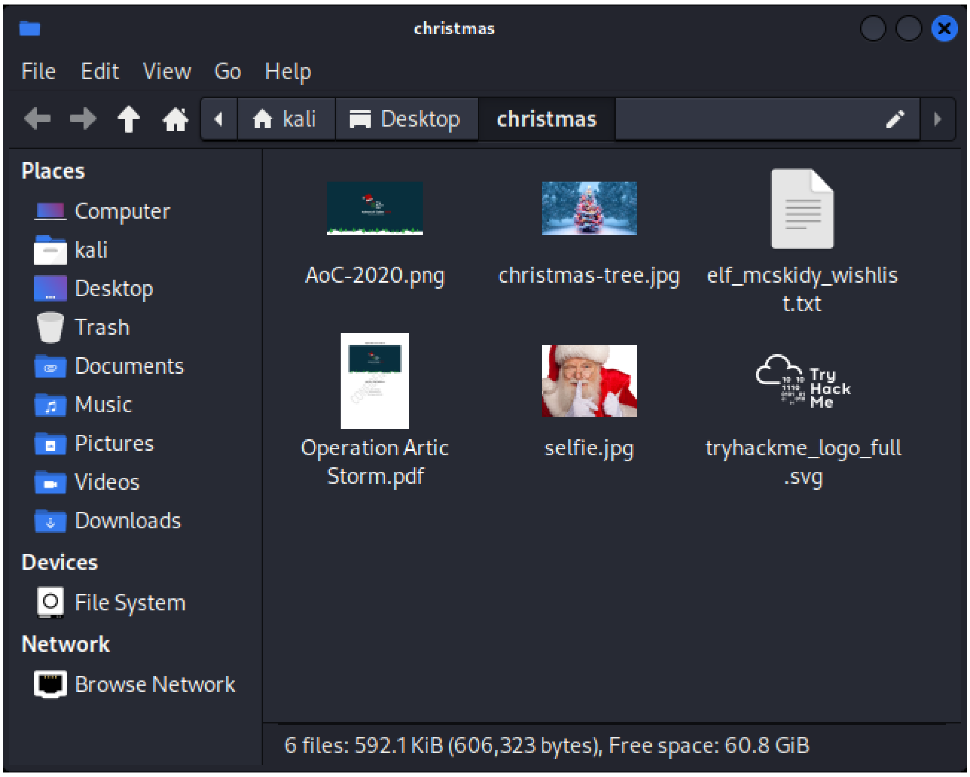
We see that there is a zip file and save it to Desktop.



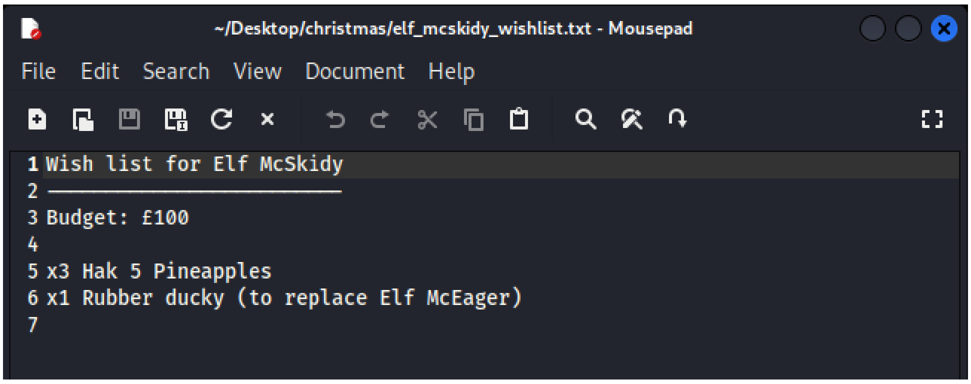
Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
168	tbfc.blog	text/html	4,532 bytes	/
395	tbfc.blog	application/zip	565 kB	christmas.zip

We open extract Christmas.zip and open it. There are several files, our target file is elf_msdkidy_wishlist.txt.



Inside elf_msdkidy_wishlist.txt, line 6, we can see rubber ducky will be used to replace Elf McEager.


~/Desktop/christmas/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help

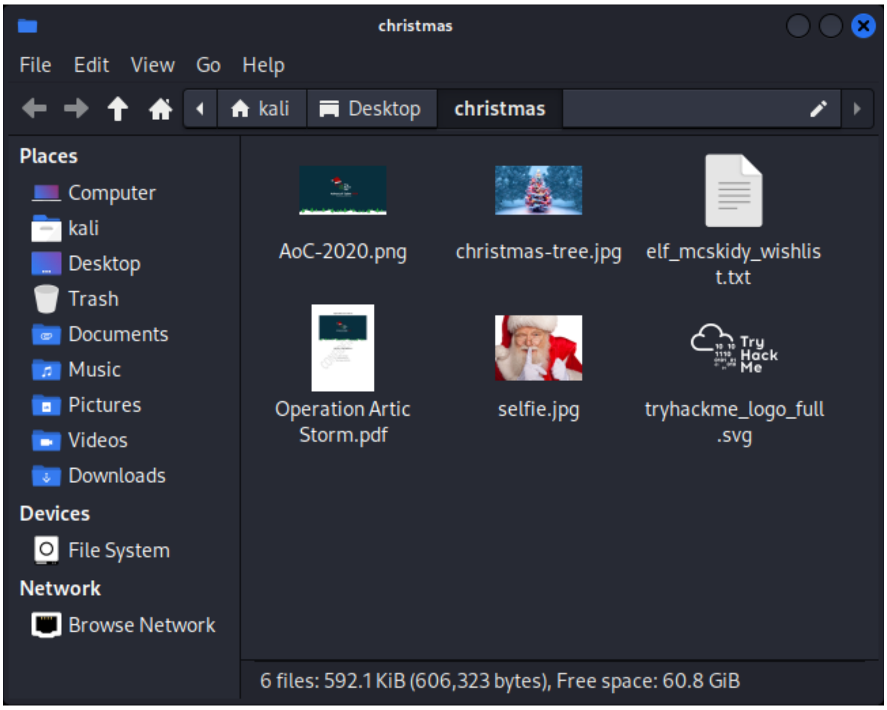
```
1 Wish list for Elf McSkidy
2 ─────────────────────────
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7
```

Answer: rubber ducky

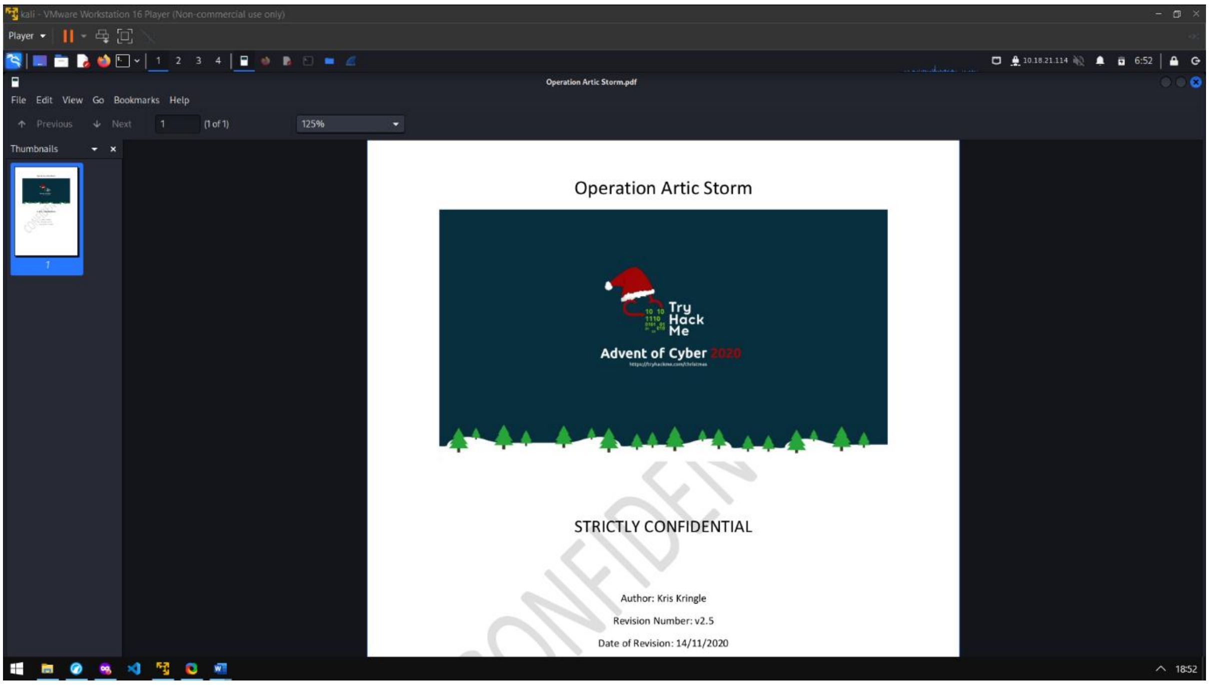
Question 8

Who is the author of Operation Artic Storm?

Methodology: In the same Christmas folder, there is a Operation Artic Storm.pdf file. We open it and see that the author is Kris Kringle.



6 files: 592.1 KiB (606,323 bytes), Free space: 60.8 GiB


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)
125%
Thumbnails
Try Hack Me
Advent of Cyber 2020
CONFIDENTIAL

Operation Artic Storm

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Answer: Kris Kringle