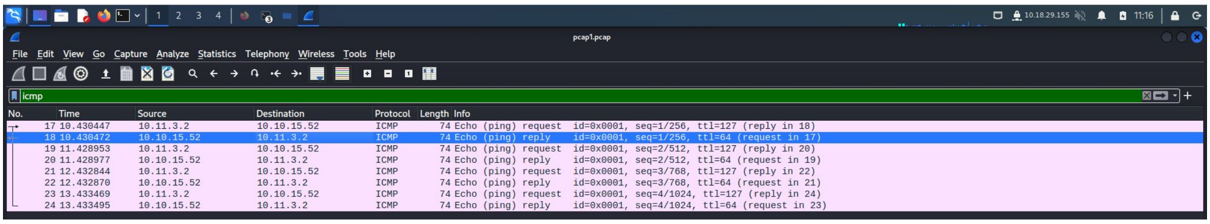
Day 7 - [Networking] The Grinch Really Did Steal Christmas

Tool used: kali Linux, Firefox, Wireshark

Solution/Walkthrough:

Q1

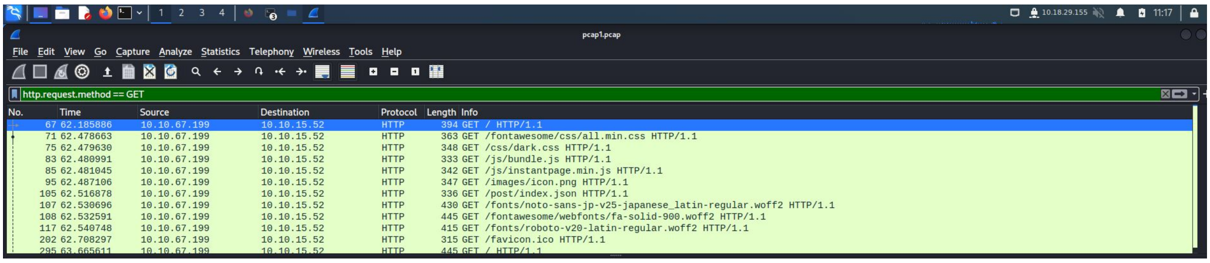


1 2 3 4
10.18.29.155
11:16
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
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)
```

To have a look at all ICMP, search icmp in the search bar. In reply, destination is the IP address that initiates an ICMP/ping toward the server at the source.

Q2

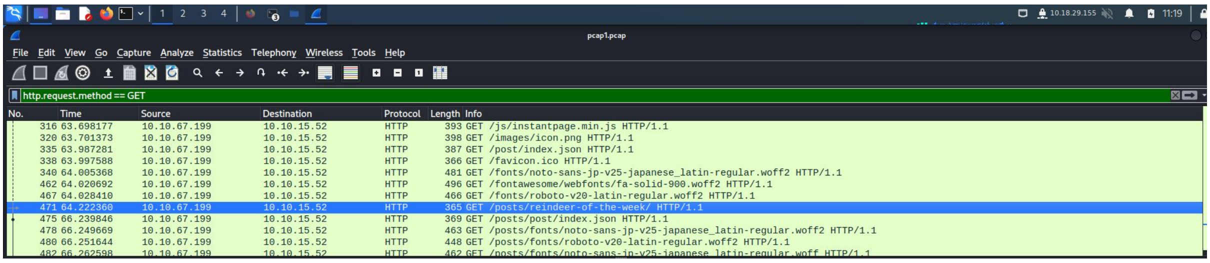


1 2 3 4
10.18.29.155
11:17
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
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
```

To see ‘http get requests’, use[<protocol>.request.method == (get/post)]to filter out, where protocol is [http],[get] to see the get requests.

Q3

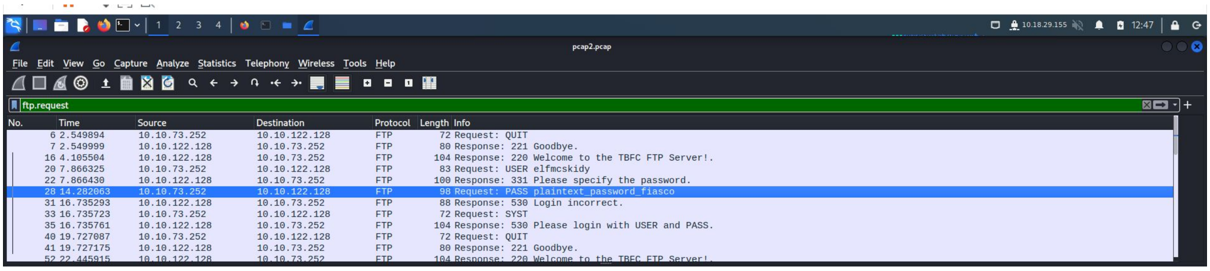


1 2 3 4
10.18.29.155
11:19
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
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
```

Apply the filter, examine the filtered data, and a post is found.

Q4

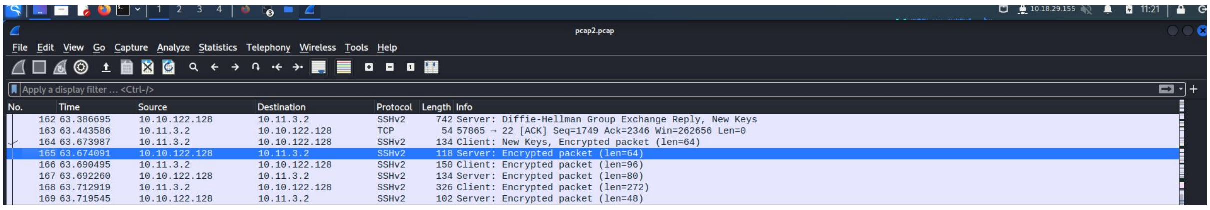

pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp.request

```
No.   Time       Source          Destination     Protocol Length Info
    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.
   16 4.105504   10.10.122.128   10.10.73.252    FTP       104 Response: 220 Welcome to the TBFC FTP Server!.
   20 7.866325   10.10.73.252    10.10.122.128   FTP        83 Request: USER elfmcskidy
   22 7.866430   10.10.122.128   10.10.73.252    FTP       100 Response: 331 Please specify the password.
   28 14.282063  10.10.73.252    10.10.122.128   FTP        98 Request: PASS plaintext_password_fiasco
   31 16.735293  10.10.122.128   10.10.73.252    FTP        88 Response: 530 Login incorrect.
   33 16.735723  10.10.73.252    10.10.122.128   FTP        72 Request: SYST
   35 16.735761  10.10.122.128   10.10.73.252    FTP       104 Response: 530 Please login with USER and PASS.
   40 19.727087  10.10.73.252    10.10.122.128   FTP        72 Request: QUIT
   41 19.727175  10.10.122.128   10.10.73.252    FTP        80 Response: 221 Goodbye.
   52 22.445915  10.10.122.128   10.10.73.252    FTP       104 Response: 220 Welcome to the TBFC FTP Server!.
```

Filter out the requests, a request of password is found.

Q5

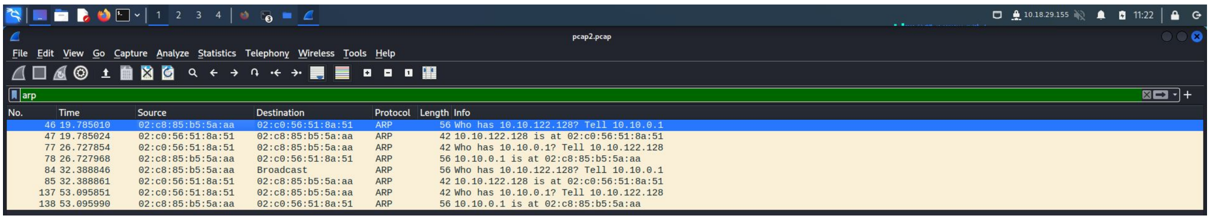

pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

```
No.   Time       Source          Destination     Protocol Length Info
  162 63.386695  10.10.122.128   10.11.3.2       SSHv2     742 Server: Diffie-Hellman Group Exchange Reply, New Keys
  163 63.443586  10.11.3.2       10.10.122.128   TCP        54 57865 → 22 [ACK] Seq=1749 Ack=2346 Win=262656 Len=0
  164 63.673987  10.11.3.2       10.10.122.128   SSHv2     134 Client: New Keys, Encrypted packet (len=64)
  165 63.674091  10.10.122.128   10.11.3.2       SSHv2     118 Server: Encrypted packet (len=64)
  166 63.690495  10.11.3.2       10.10.122.128   SSHv2     150 Client: Encrypted packet (len=96)
  167 63.692260  10.10.122.128   10.11.3.2       SSHv2     134 Server: Encrypted packet (len=80)
  168 63.712919  10.11.3.2       10.10.122.128   SSHv2     326 Client: Encrypted packet (len=272)
  169 63.719545  10.10.122.128   10.11.3.2       SSHv2     102 Server: Encrypted packet (len=48)
```

After examining and analysing, only SSH protocol has shown to be encrypted.

Q6

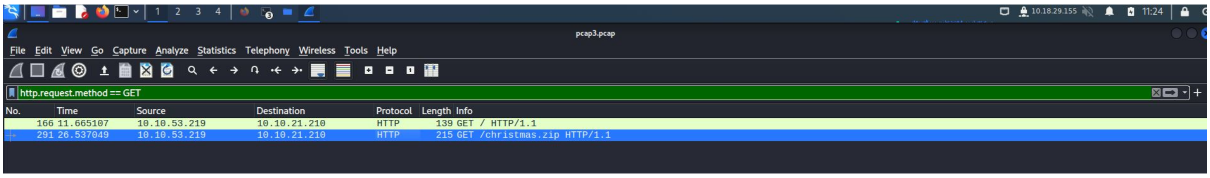

pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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
```

Filter out ARP communications. Copy and paste the source.

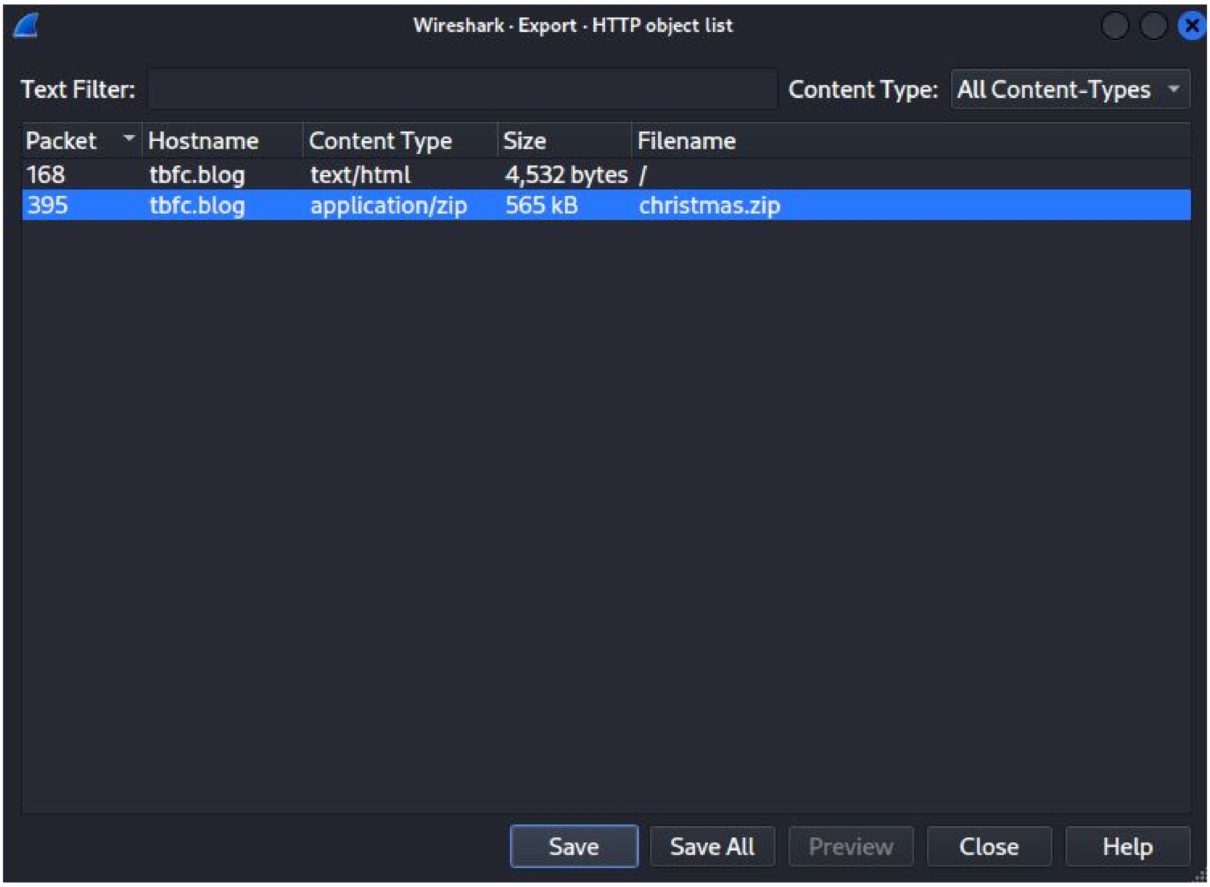
Q7


pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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 using [get] to find the data retrieved. A file named christmas.zip is found.

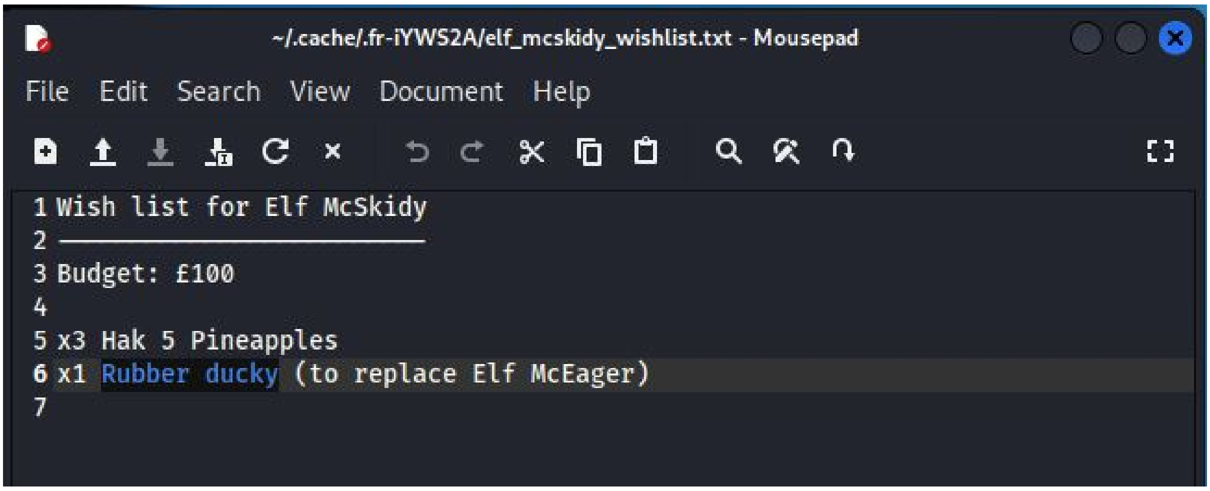


Text Filter:

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

Extract the file and save it.



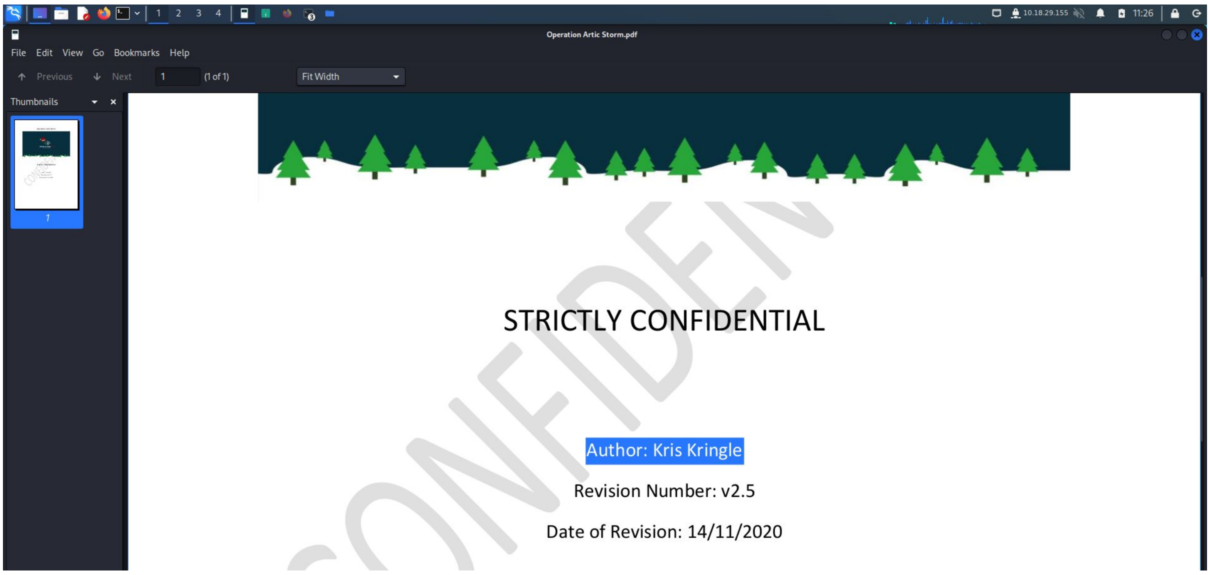
```
Wish list for Elf McSkidy
─────────────────────────
Budget: £100

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

```

In the file extracted, examine the content. The answer is found in elf_mcskidy_wishlist.txt.

Q8



Operation Artic Storm.pdf
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) Fit Width
Thumbnails

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

In the extracted file, the author name is found in a pdf.