Day 7 - The Grinch Really Did Steal Christmas

Scenario

Story

It's 6 AM and Elf McSkidy is clocking-in to The Best Festival Company's SOC headquarters to begin his watch over TBFC's infrastructure. After logging in, Elf McEager proceeds to read through emails left by Elf McSkidy during the nightshift.

More automatic scanning alerts, oh look, another APT group. It feels like it's going to be a long, but easy start to the week for Elf McEager.

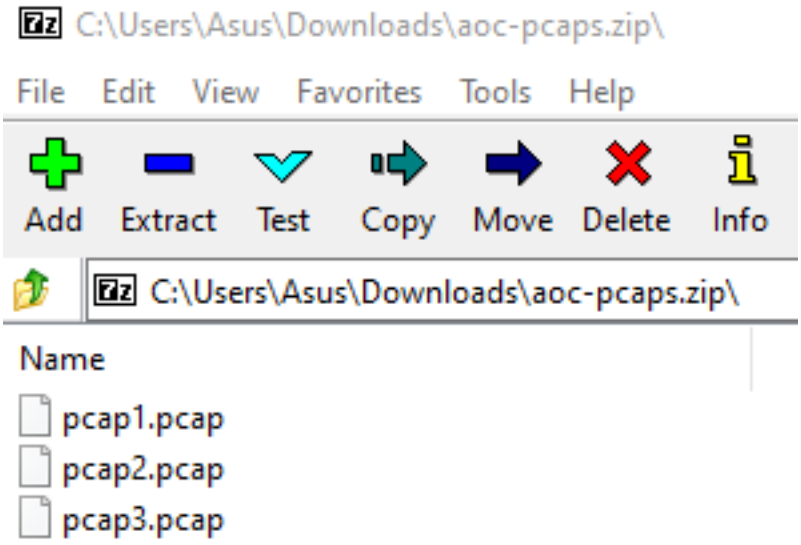
Whilst clearing the backlog of emails, Elf McEager reads the following: "**URGENT:** Data exfiltration detected on TBFC-WEB-01". "*Uh oh*" goes Elf McEager. "*TBFC-WEB-01? That's Santa's webserver! Who has the motive to steal data from there?!*". It's time for the ever-vigilant Elf McEager to prove his salt and find out exactly what happened.

Unknowingly to Elf McEager, Elf McSkidy made this all up! Fortunately, this isn't a real attack - but a training exercise created ahead of Elf McEager's performance review.

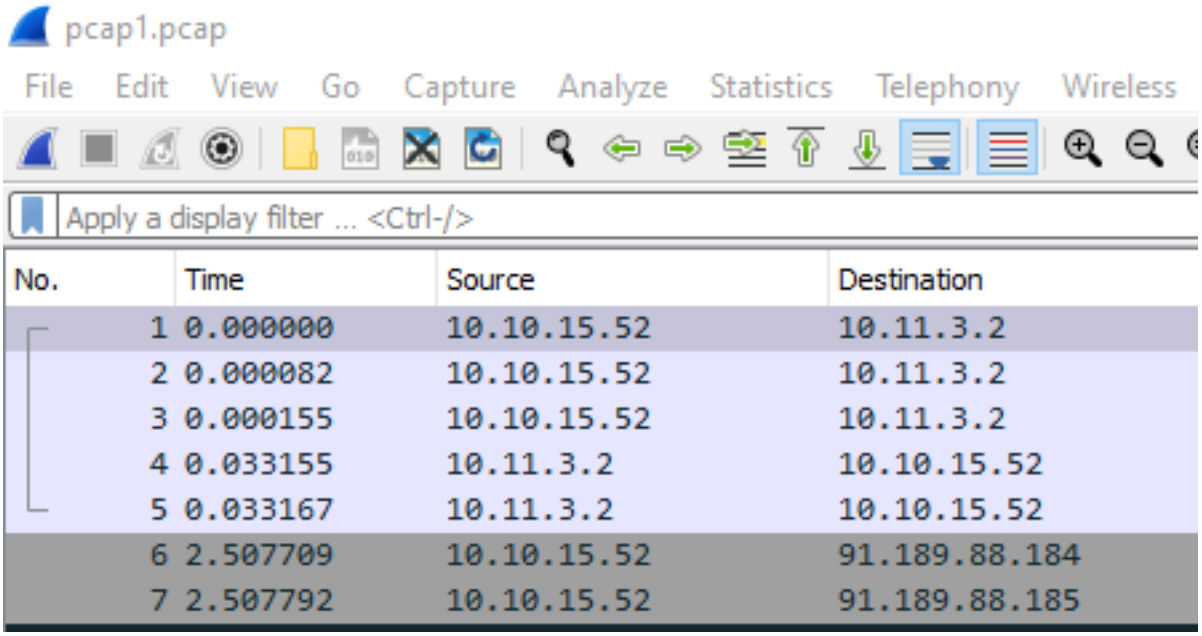
Challenge

Download the ZIP file "aocpcaps.zip" that is attached to this task, use a combination of the filters and features of Wireshark we've covered to answer the questions below:

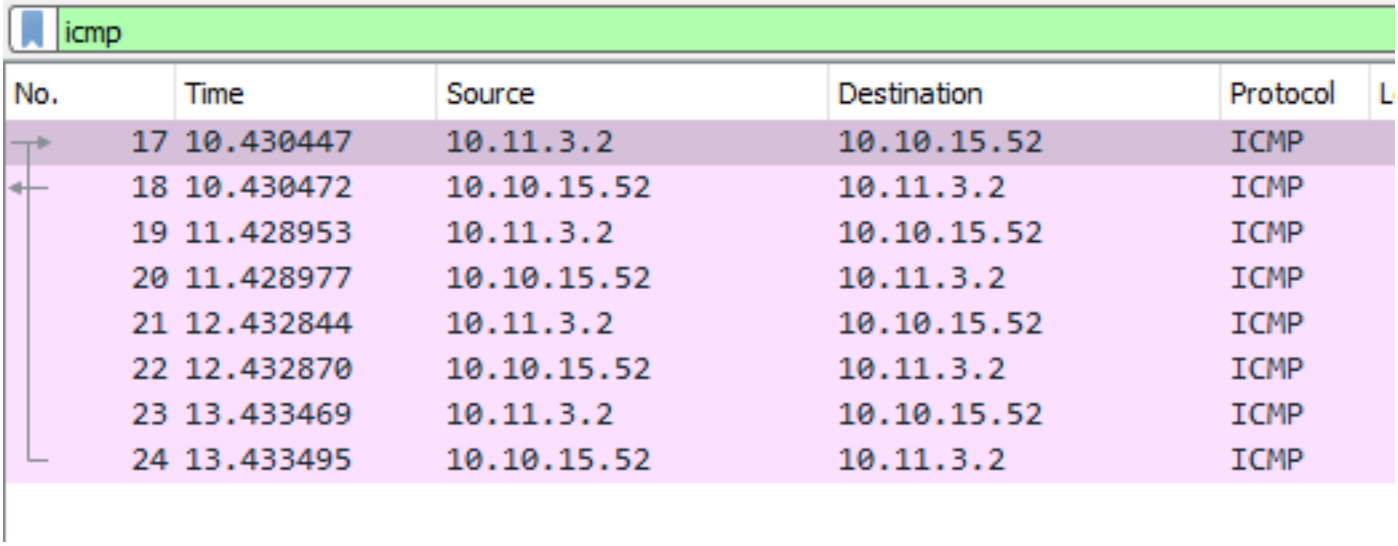
download the pcap zip file, there's 3 pcap files in it



now let's open pcap1 file using wireshark

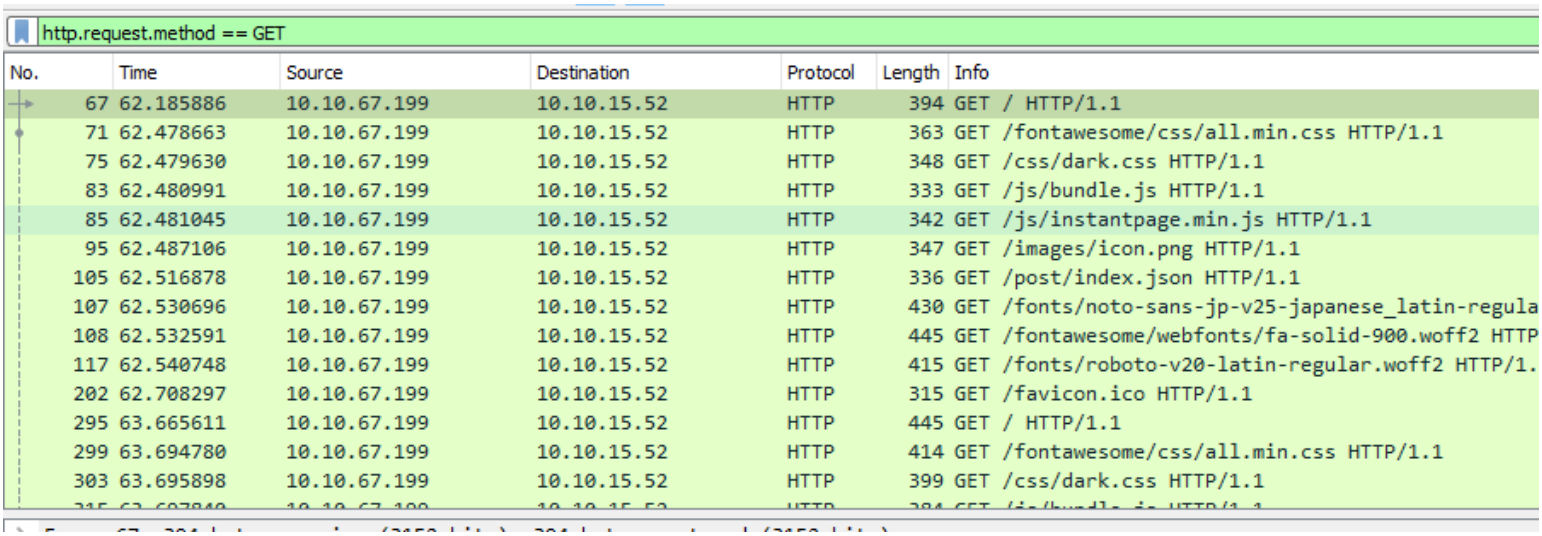


let's search for the IP that initiate ICMP/ping
//here we can see that 10.11.3.2 are the IP that intiate ICMP/ping to the destination 10.10.15.52



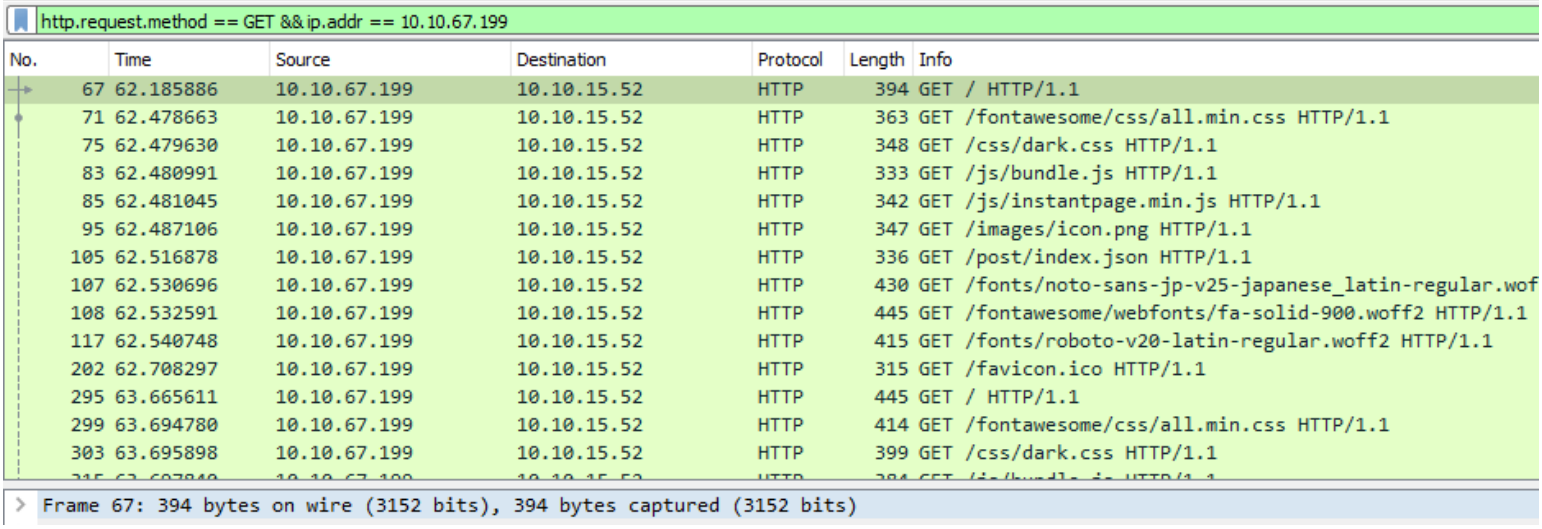
Question: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?
-10.11.3.2

now let's check for any GET request made in http protocol

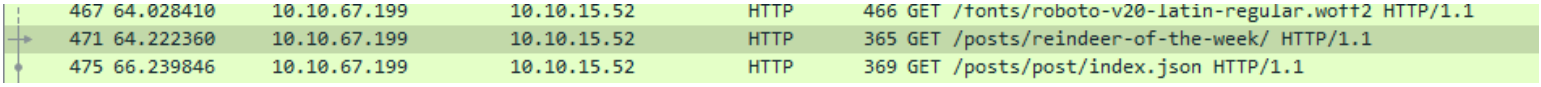


Question: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?
-http.request.method == GET

now we need to find the article that IP '10.10.67.199' visited, we can append this command into it

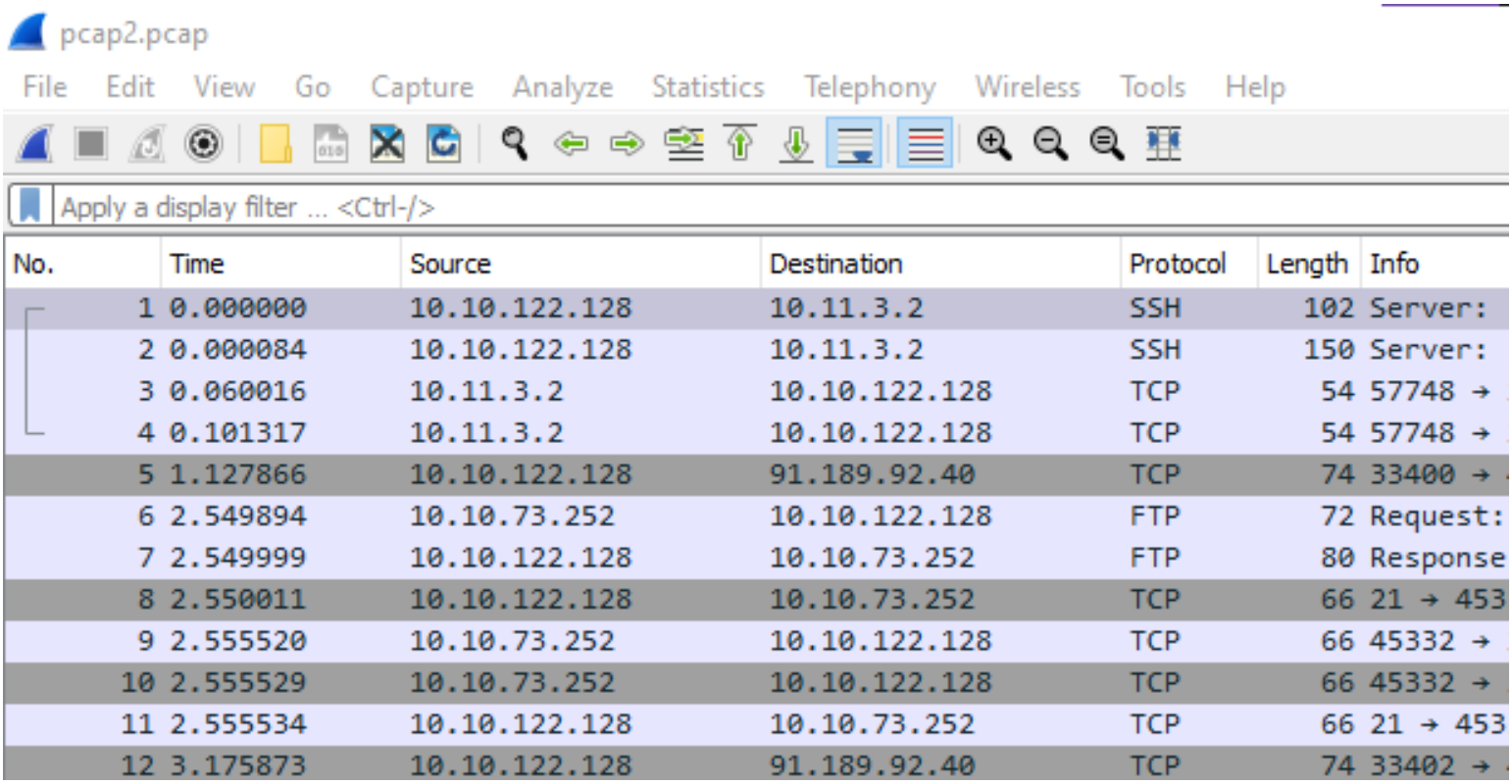


so this is the article that the IP 10.10.67.199 visited

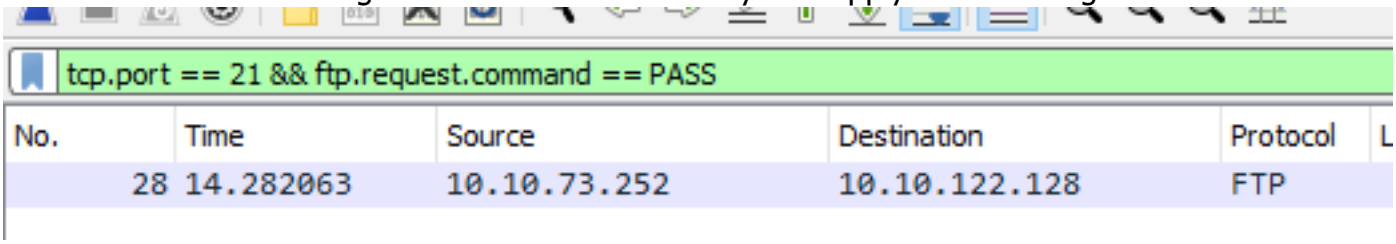


Question: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?
-reindeer-of-the-week

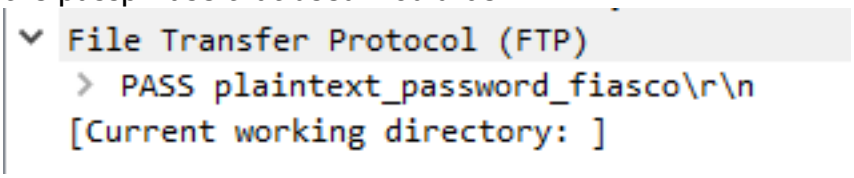
now let's analyze the pcap2 file using wireshark, we need to look for the FTP traffic & find the plaintext passphrase



to filter the FTP traffic & get the PASS command only let's apply the following filter

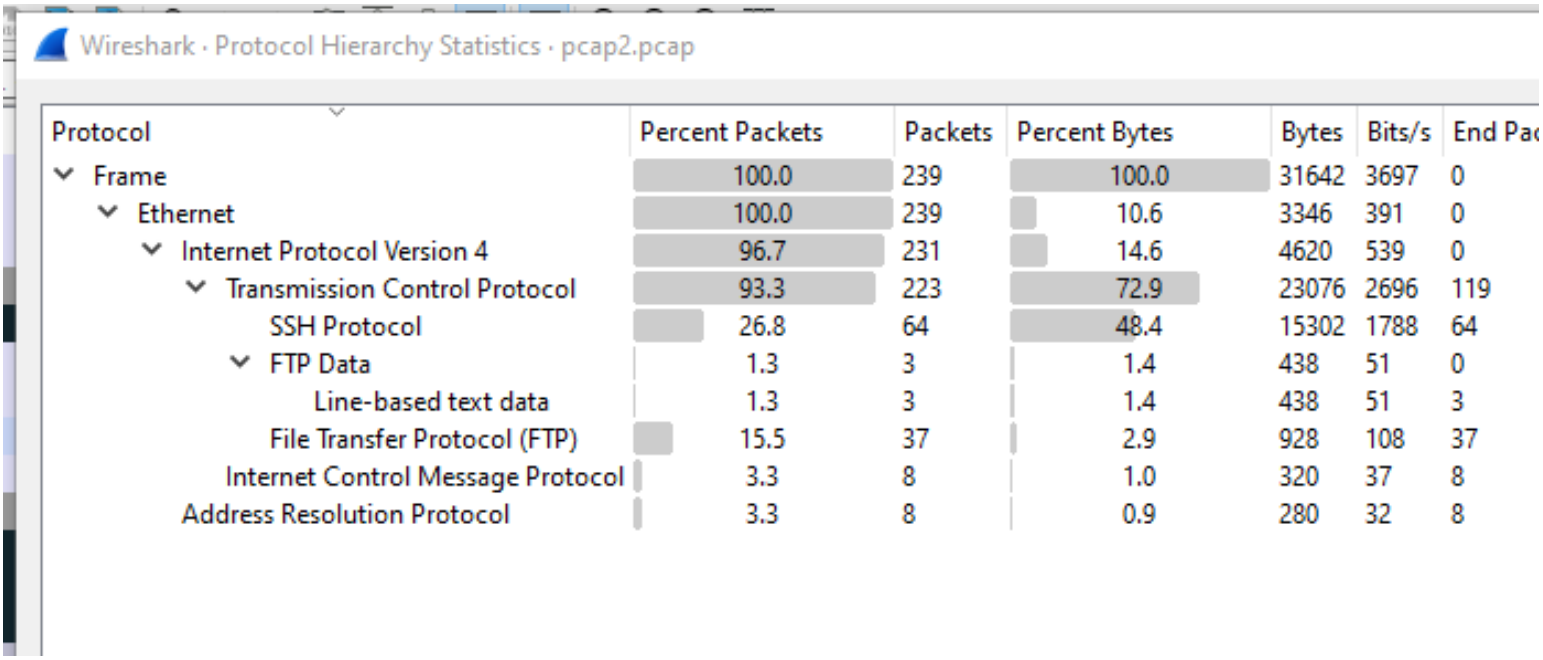


the passphrase that used would be



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

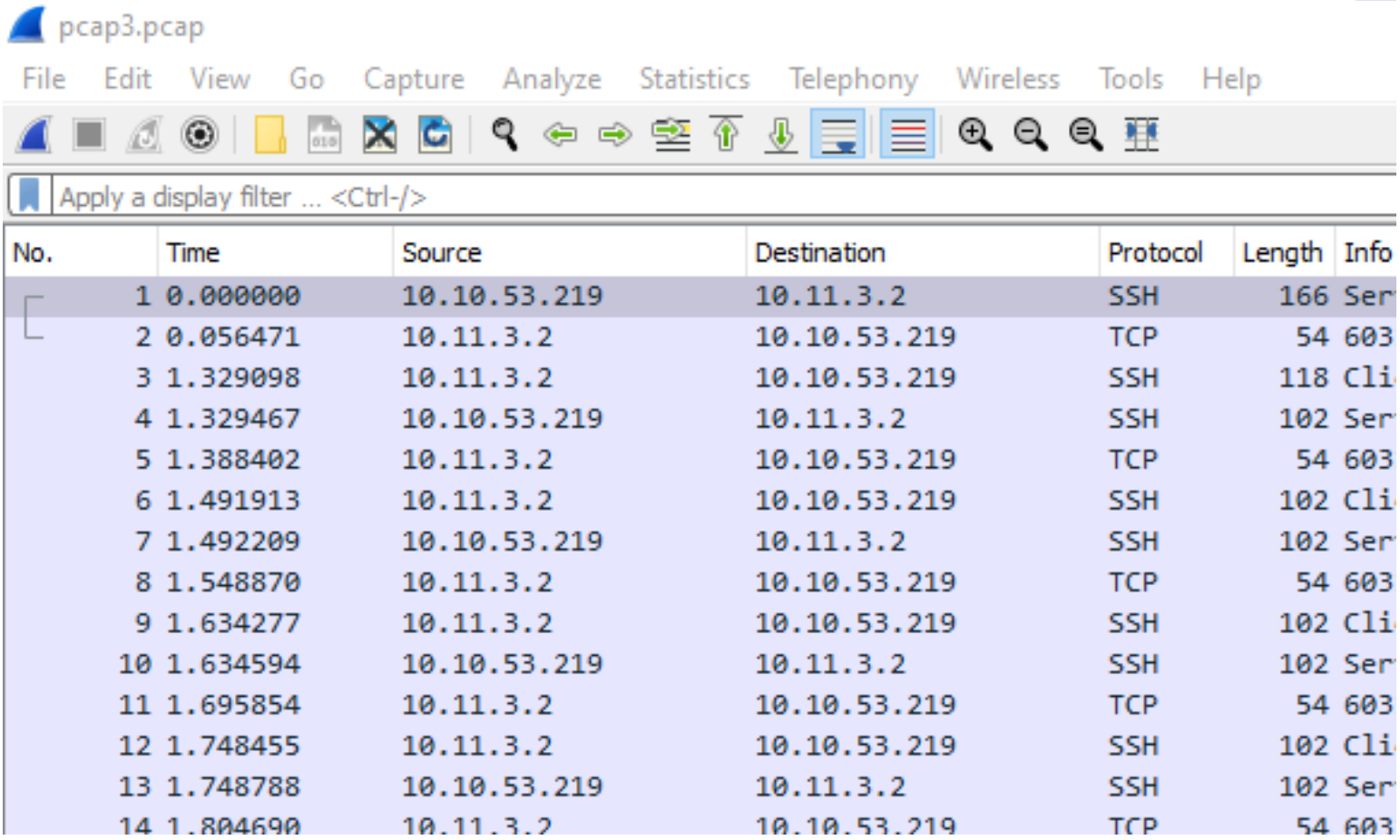
now let's find all the services that have in this pcap file, we can list it by using 'statistic > protocol hierarchy
//so the encryted protocol would be the SSH protocol in this case



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Pac
Frame	100.0	239	100.0	31642	3697	0
Ethernet	100.0	239	10.6	3346	391	0
Internet Protocol Version 4	96.7	231	14.6	4620	539	0
Transmission Control Protocol	93.3	223	72.9	23076	2696	119
SSH Protocol	26.8	64	48.4	15302	1788	64
FTP Data	1.3	3	1.4	438	51	0
Line-based text data	1.3	3	1.4	438	51	3
File Transfer Protocol (FTP)	15.5	37	2.9	928	108	37
Internet Control Message Protocol	3.3	8	1.0	320	37	8
Address Resolution Protocol	3.3	8	0.9	280	32	8

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

now let's analyze the pcap3 using wireshark again

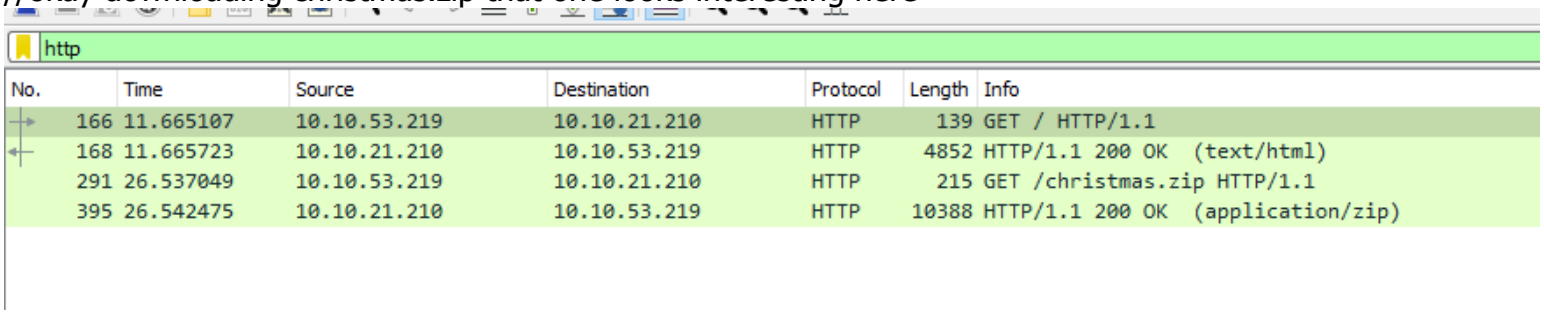


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.53.219	10.11.3.2	SSH	166	Ser
2	0.056471	10.11.3.2	10.10.53.219	TCP	54	603
3	1.329098	10.11.3.2	10.10.53.219	SSH	118	Cli
4	1.329467	10.10.53.219	10.11.3.2	SSH	102	Ser
5	1.388402	10.11.3.2	10.10.53.219	TCP	54	603
6	1.491913	10.11.3.2	10.10.53.219	SSH	102	Cli
7	1.492209	10.10.53.219	10.11.3.2	SSH	102	Ser
8	1.548870	10.11.3.2	10.10.53.219	TCP	54	603
9	1.634277	10.11.3.2	10.10.53.219	SSH	102	Cli
10	1.634594	10.10.53.219	10.11.3.2	SSH	102	Ser
11	1.695854	10.11.3.2	10.10.53.219	TCP	54	603
12	1.748455	10.11.3.2	10.10.53.219	SSH	102	Cli
13	1.748788	10.10.53.219	10.11.3.2	SSH	102	Ser
14	1.804690	10.11.3.2	10.10.53.219	TCP	54	603

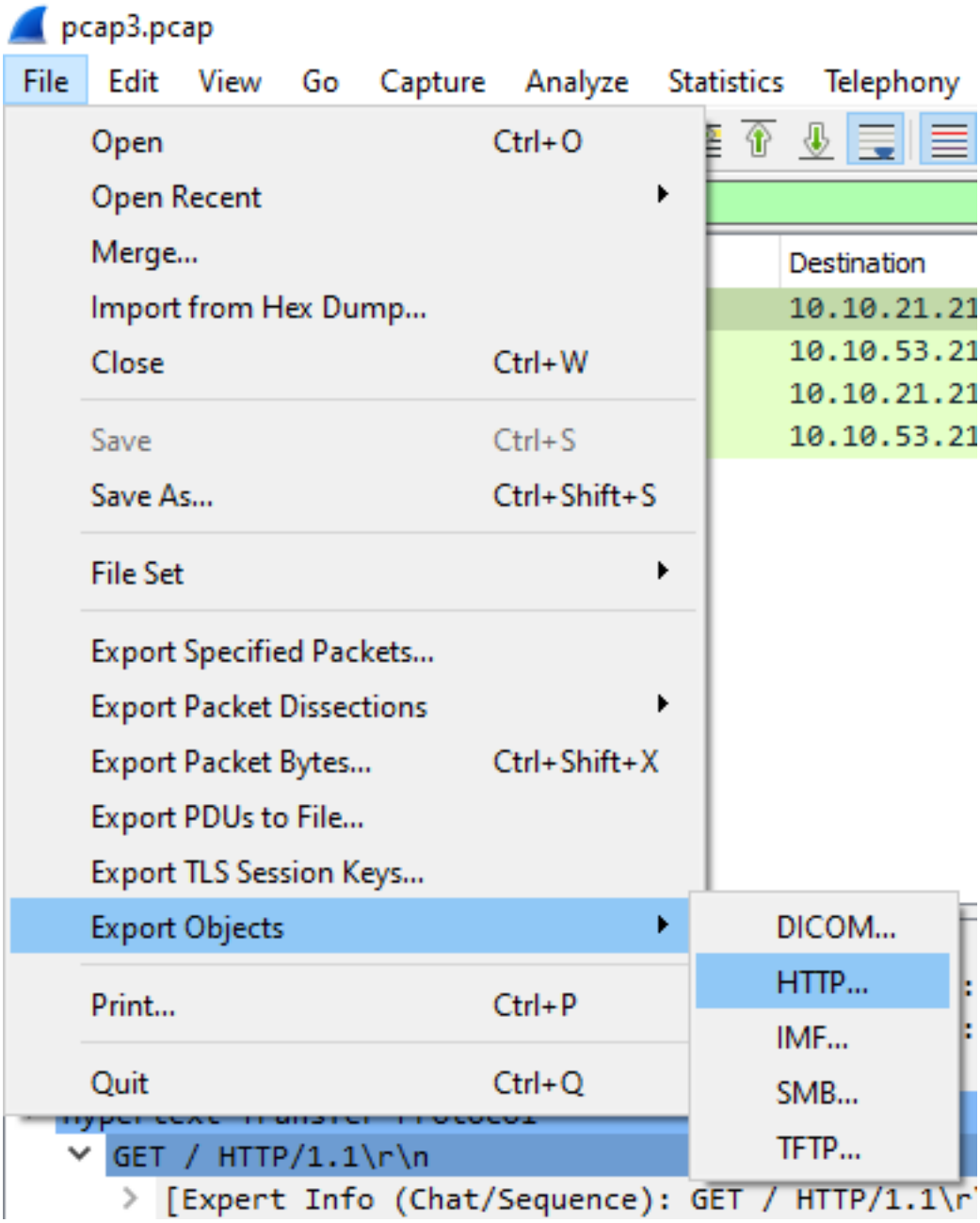
let's check the services that's available in this pcap file first, to find the interesting protocol that might shows Elf McSkidy's whishlist

Protocol	Percent Packets	P
Frame	100.0	4(
Ethernet	100.0	4(
Internet Protocol Version 4	99.5	4(
Transmission Control Protocol	99.5	4(
SSH Protocol	46.8	1(
Hypertext Transfer Protocol	1.0	4
Media Type	0.2	1
Line-based text data	0.2	1
Address Resolution Protocol	0.5	2

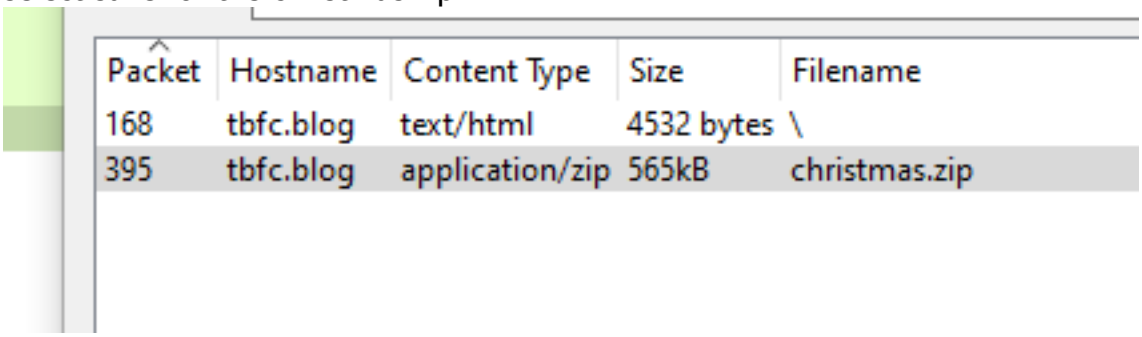
the HTTP protocol are not encrypted, so let's check out the HTTP protocol
//okay downloading christmas.zip that one looks interesting here



let's export the christmas.zip file out from this pcap file

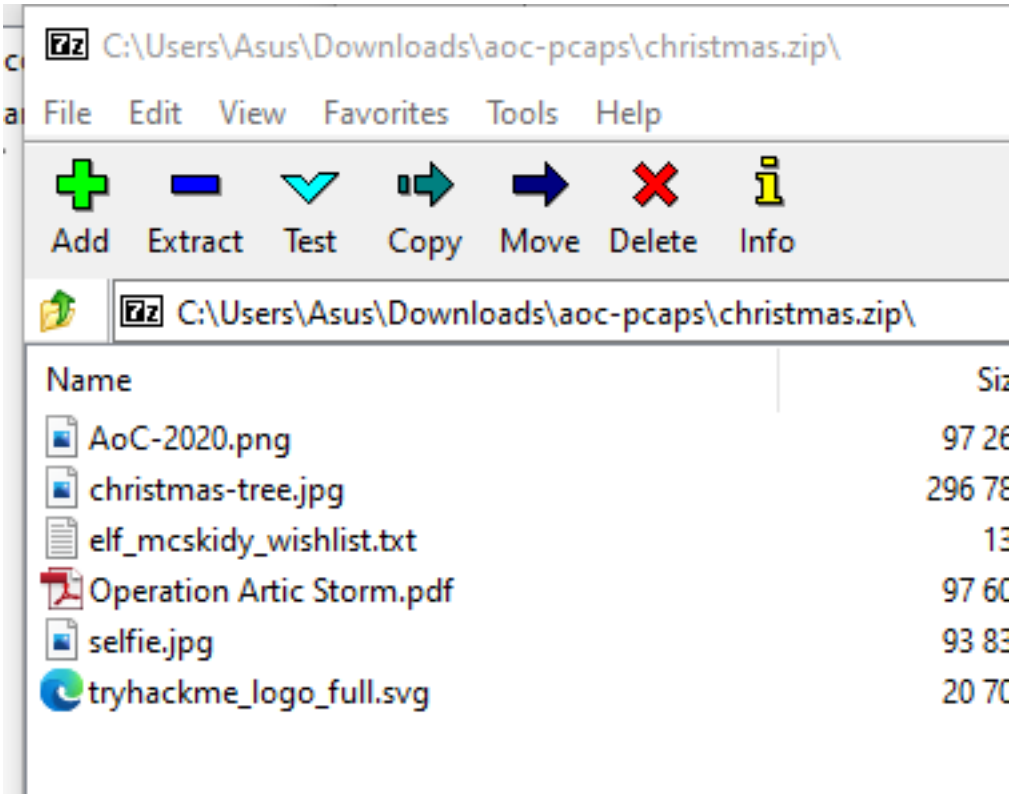


select save for the christmas.zip



Packet	Hostname	Content Type	Size	Filename
168	tbfc.blog	text/html	4532 bytes	\
395	tbfc.blog	application/zip	565kB	christmas.zip

opening the christmas.zip file & we found elf mcskidy wishlist text file



interesting stuff we found in there, seems like elf mcskidy wanna use rubber ducky to replace elf mceager

```
x1 Rubber ducky (to replace Elf McEager)
```

Question: What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?
-rubber ducky