# 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 |

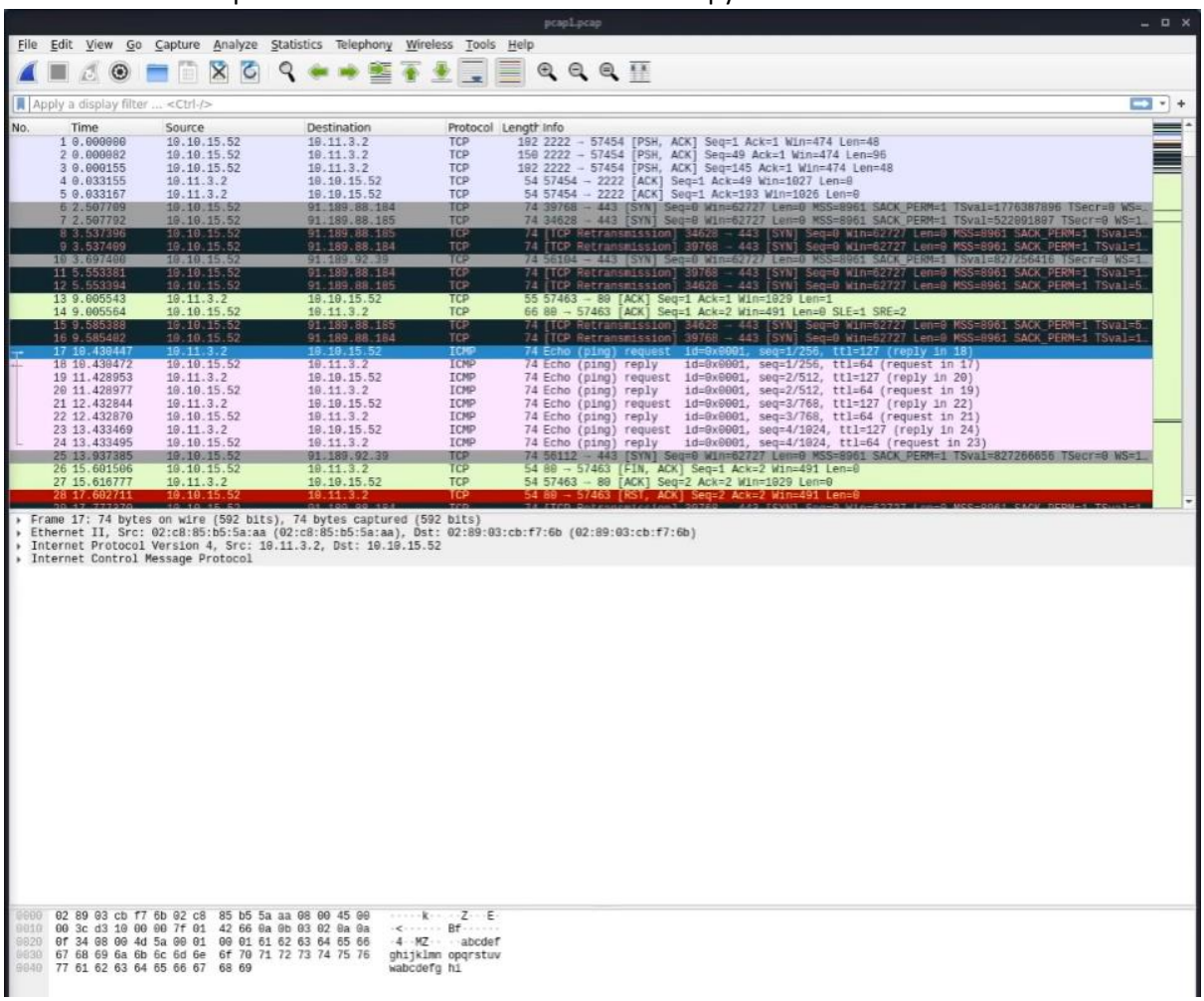
**Day 7: Networking – The Grinch Really Did Steal Christmas**

**Tools used**: Kali Linux, Firefox

**Solution/walkthrough**:

Question 1

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




Question 2

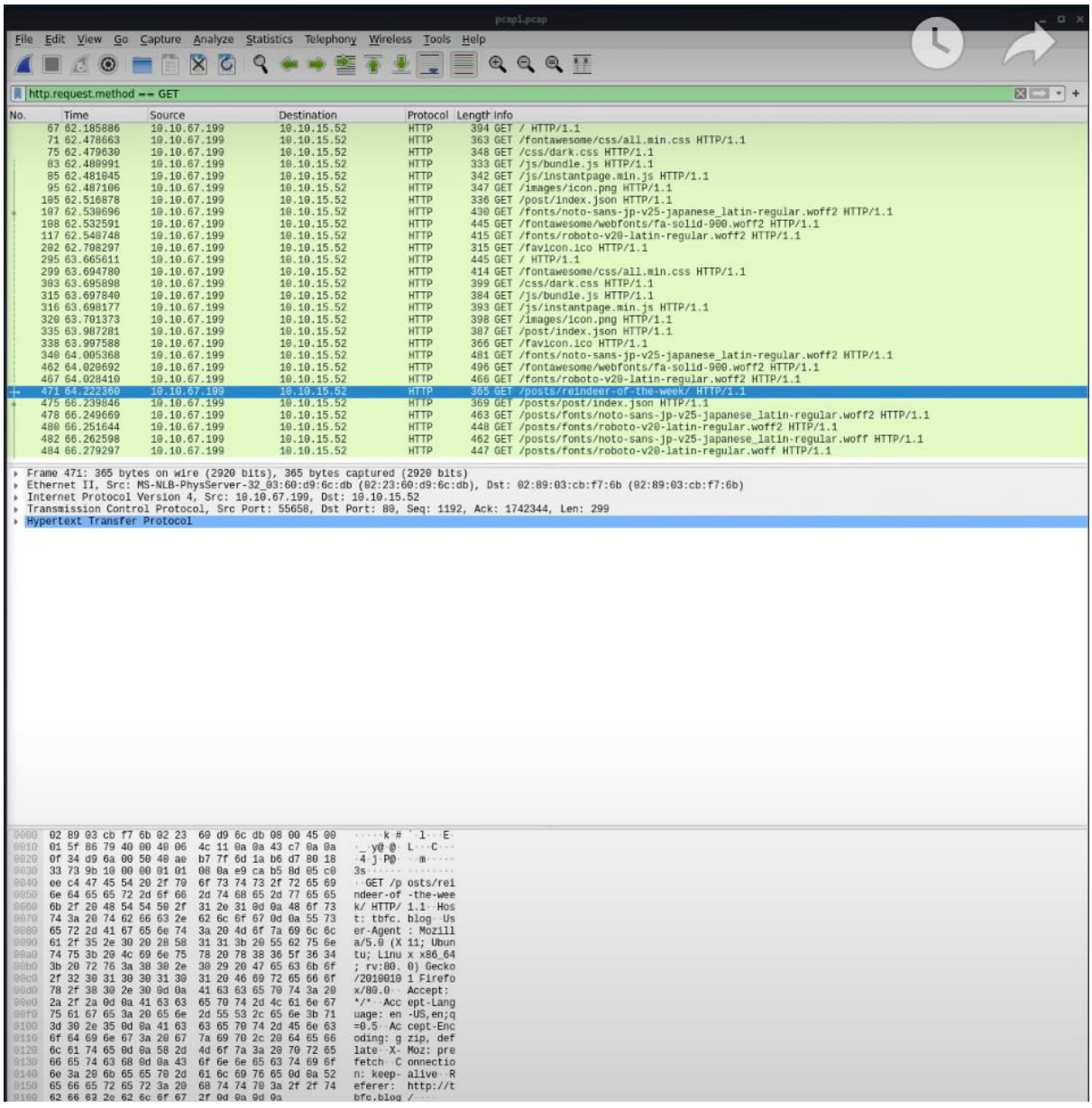
Read through and use the correct filter based on the description with the operator given.

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 | `ip.src == 192.168.1.1` |
| ip.dst | Show all packets that are destined to the specified IP address | `ip src == 192.168.1.1` |
| tcp/udp.port | Show all packets that are sent via the protocol and port specifiyed | `tcp.port == 22 / udp.port == 67` |
| 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.get` / `http.request.post` |

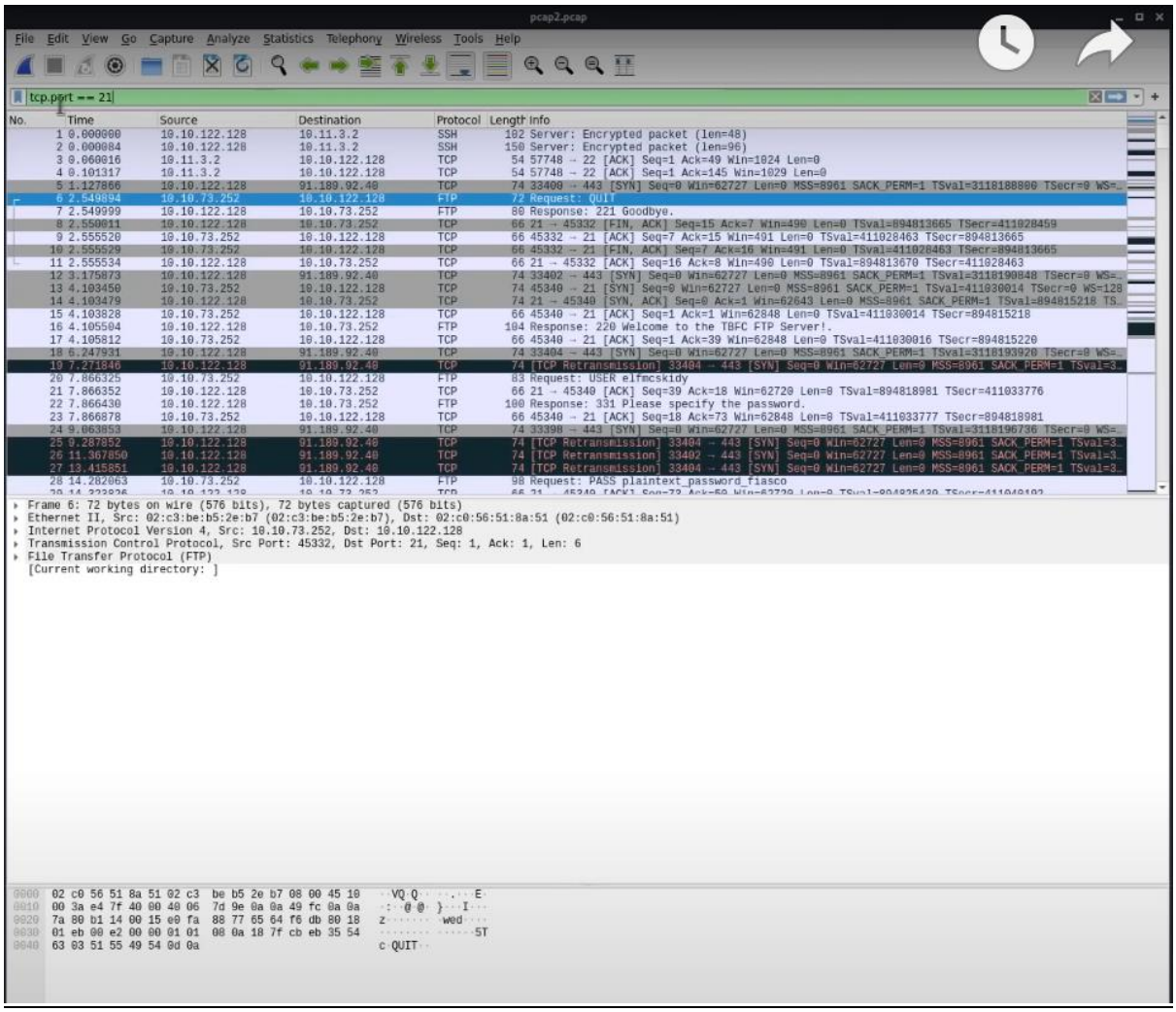
## Question 3

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.

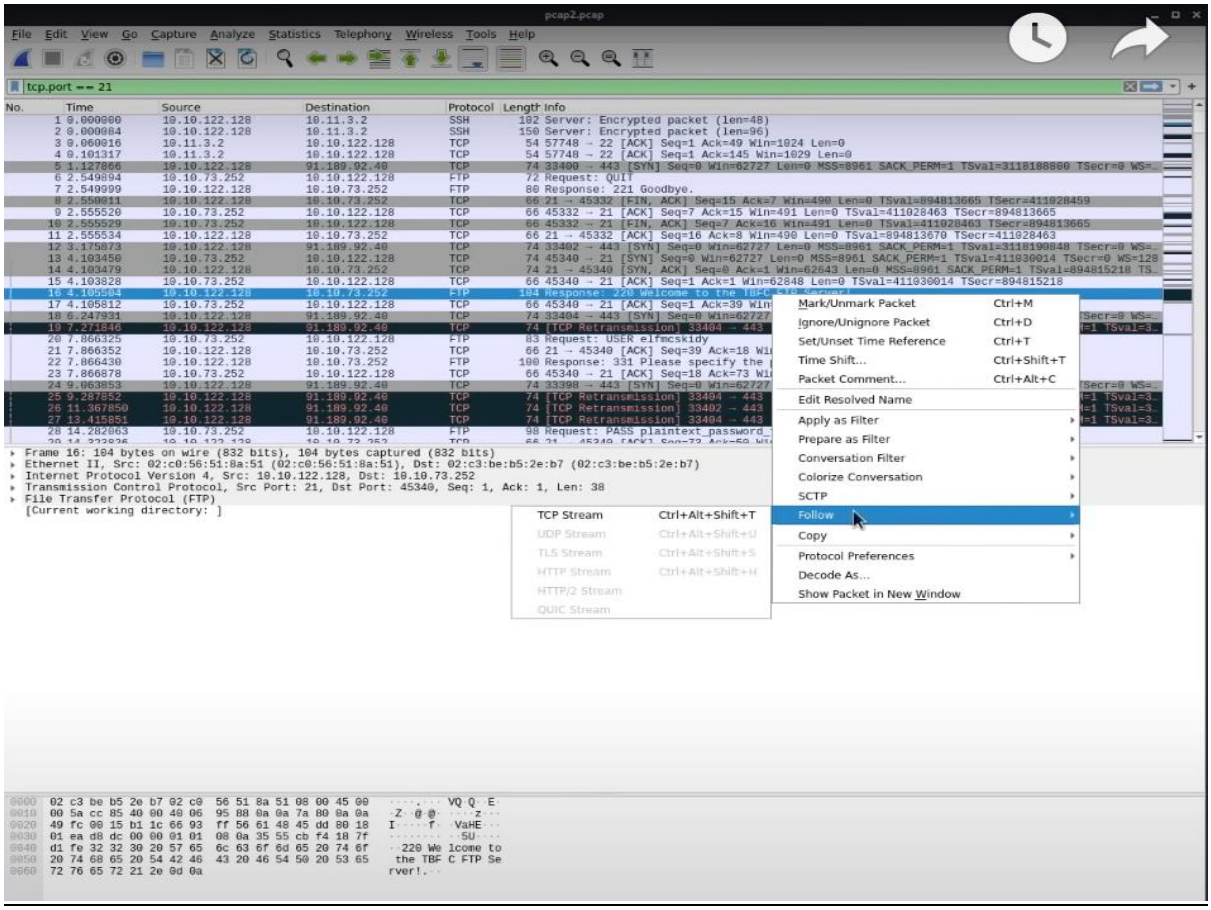



## Question 4

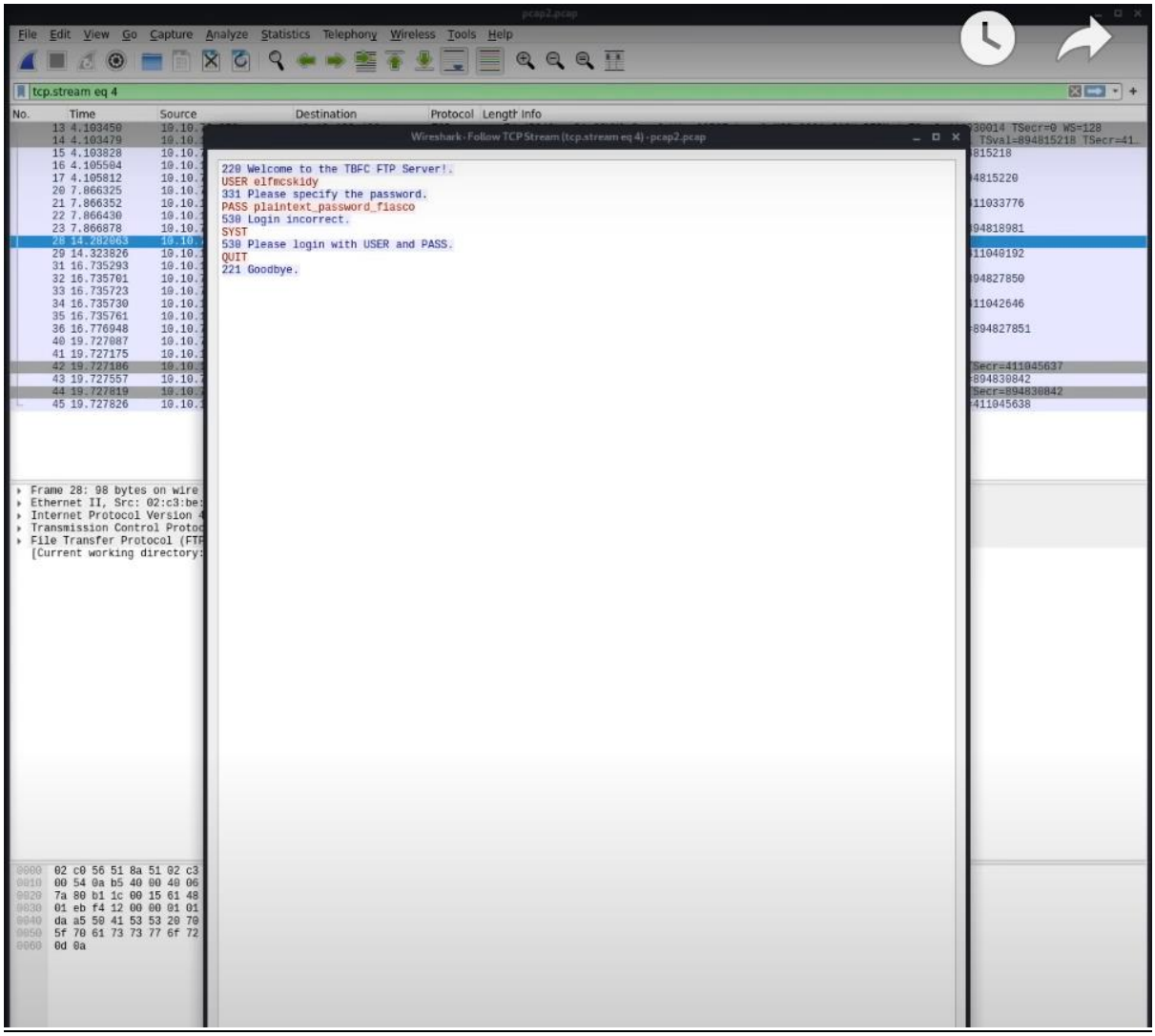
Use the correct filter based on the given important ones, to search and find the right clue to the login info.




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

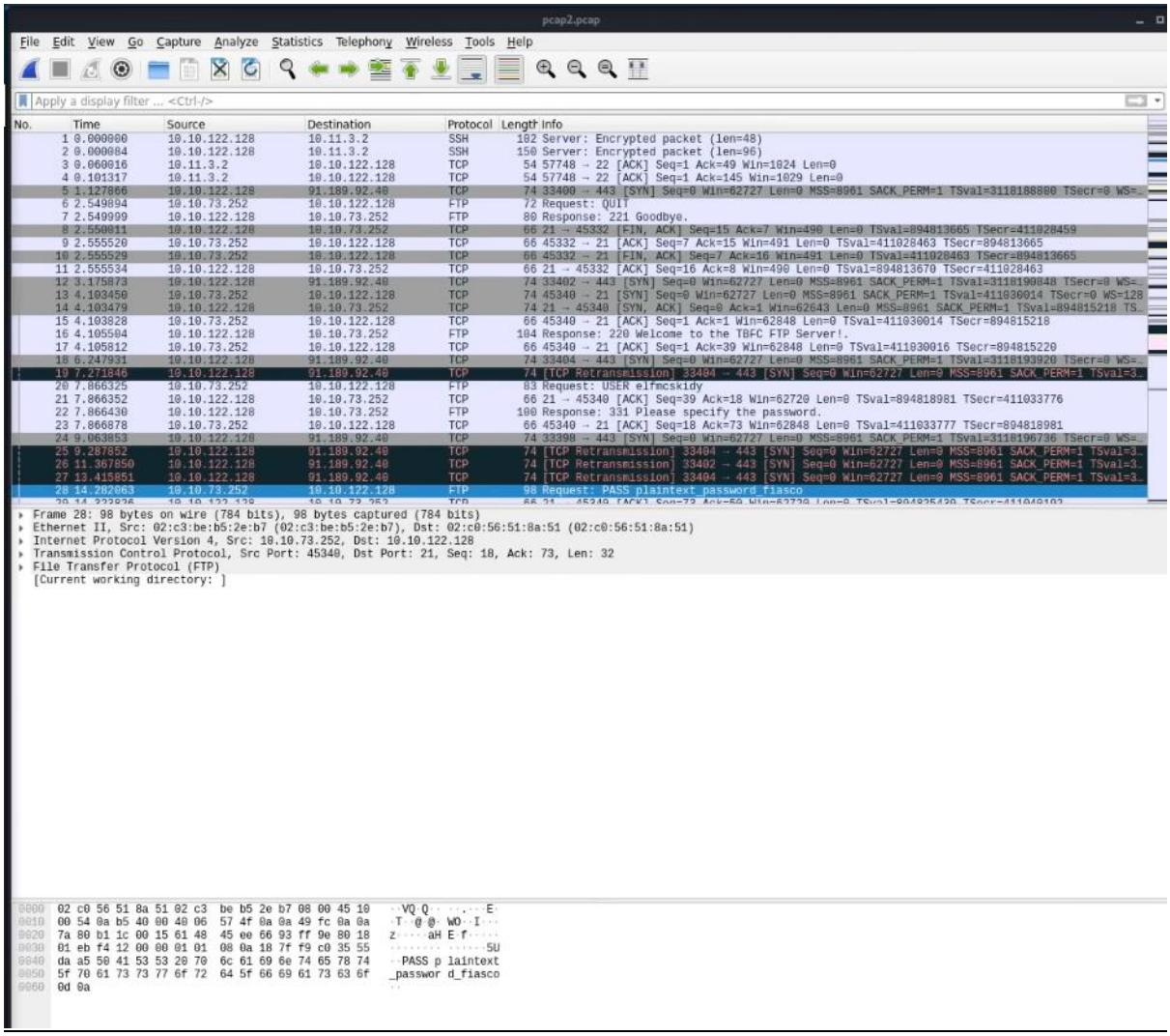



Results would be shown, find the password and copy it.



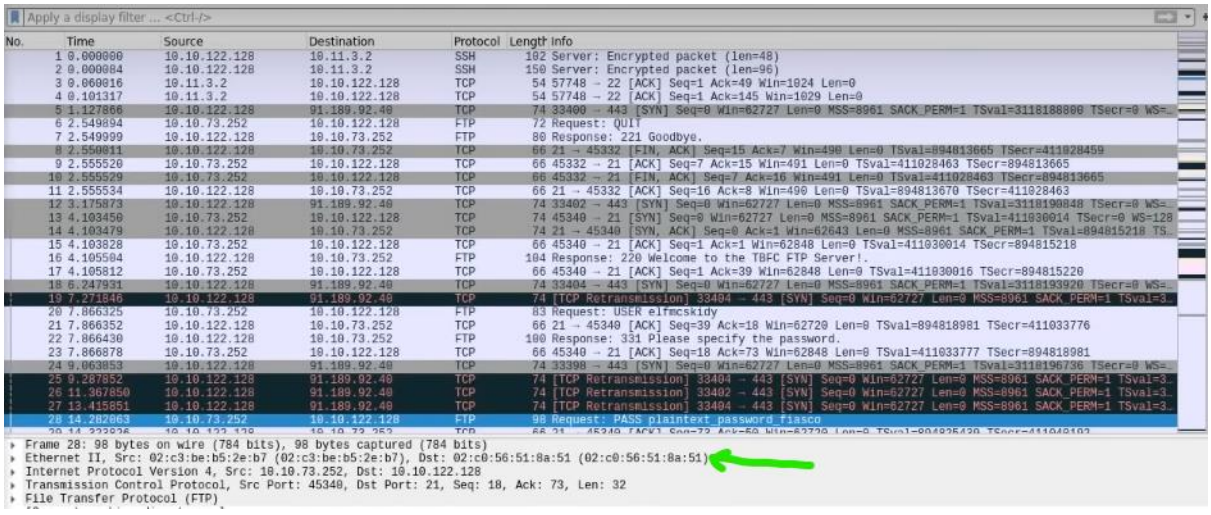

Question 5

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



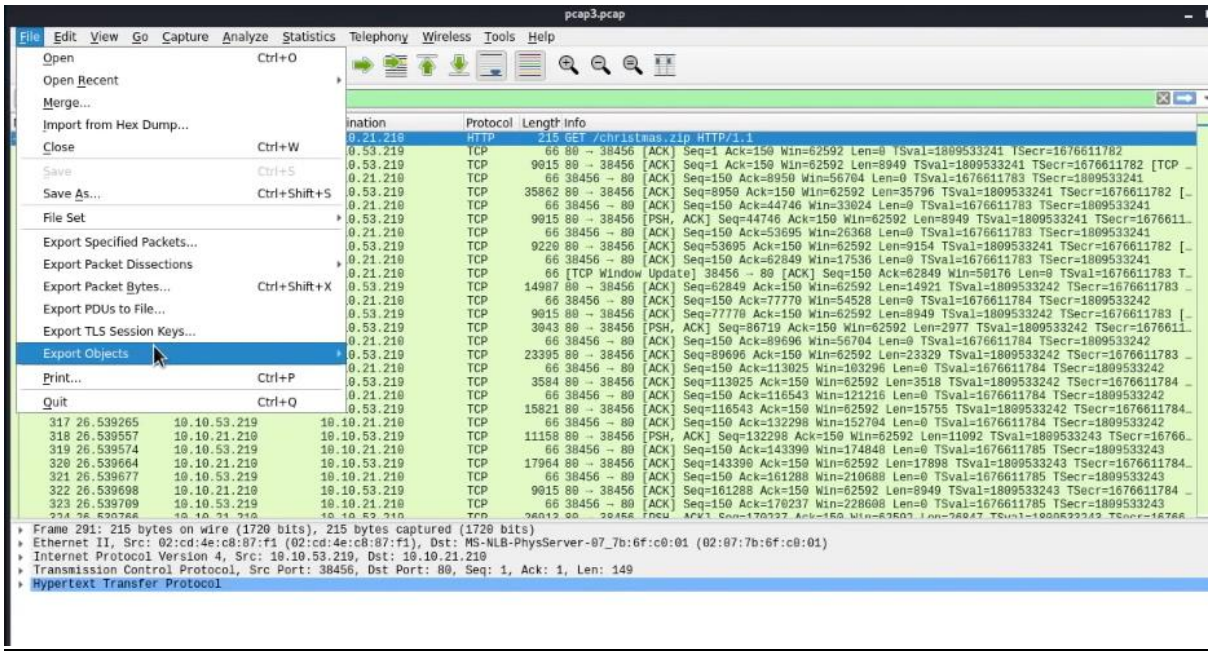

Question 6

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

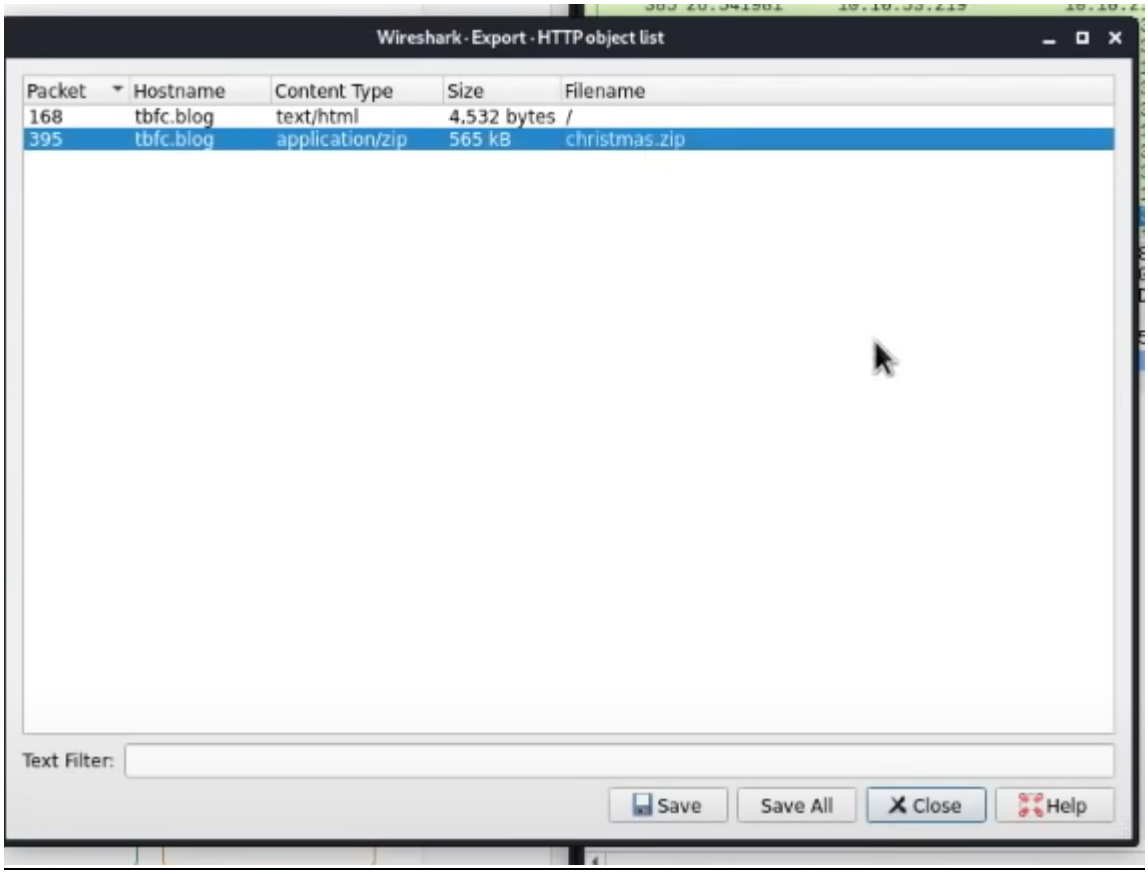



Question 7

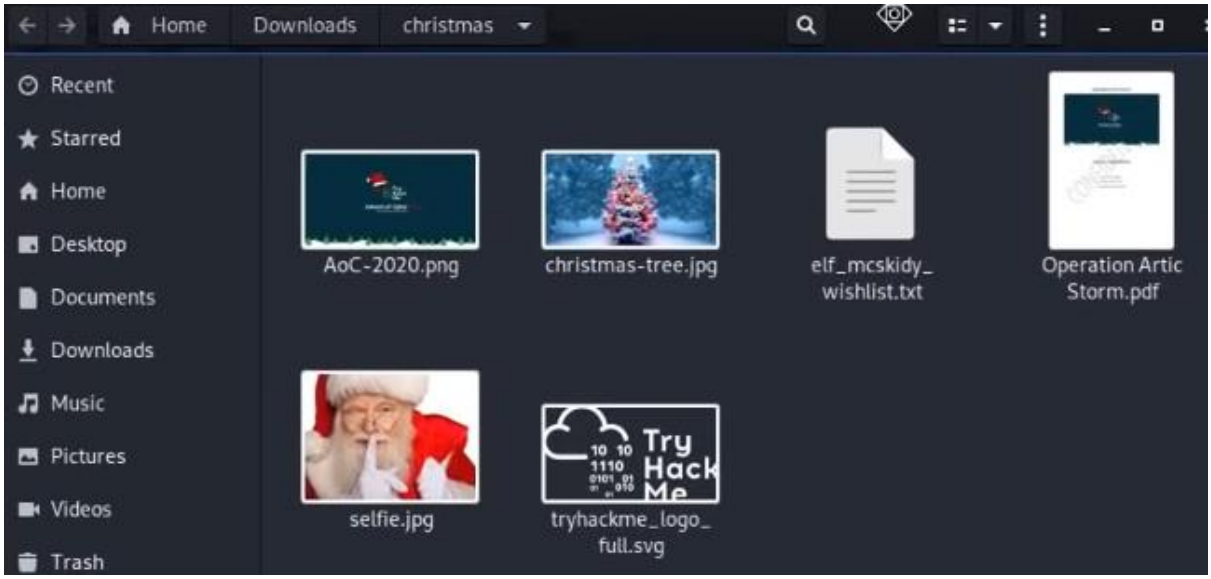
Find “GET /christmas.zip HTTP/” under the pcap3.pcap file and click on the export objects for the HTTP option.



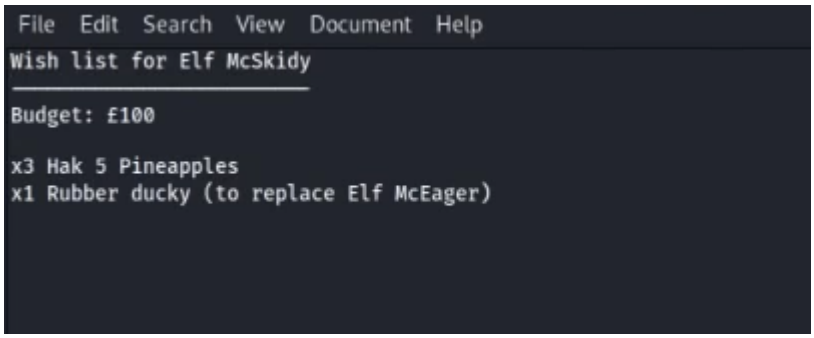

The export object list would be shown and choose the christmas.zip to save it in the directory.




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.




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.