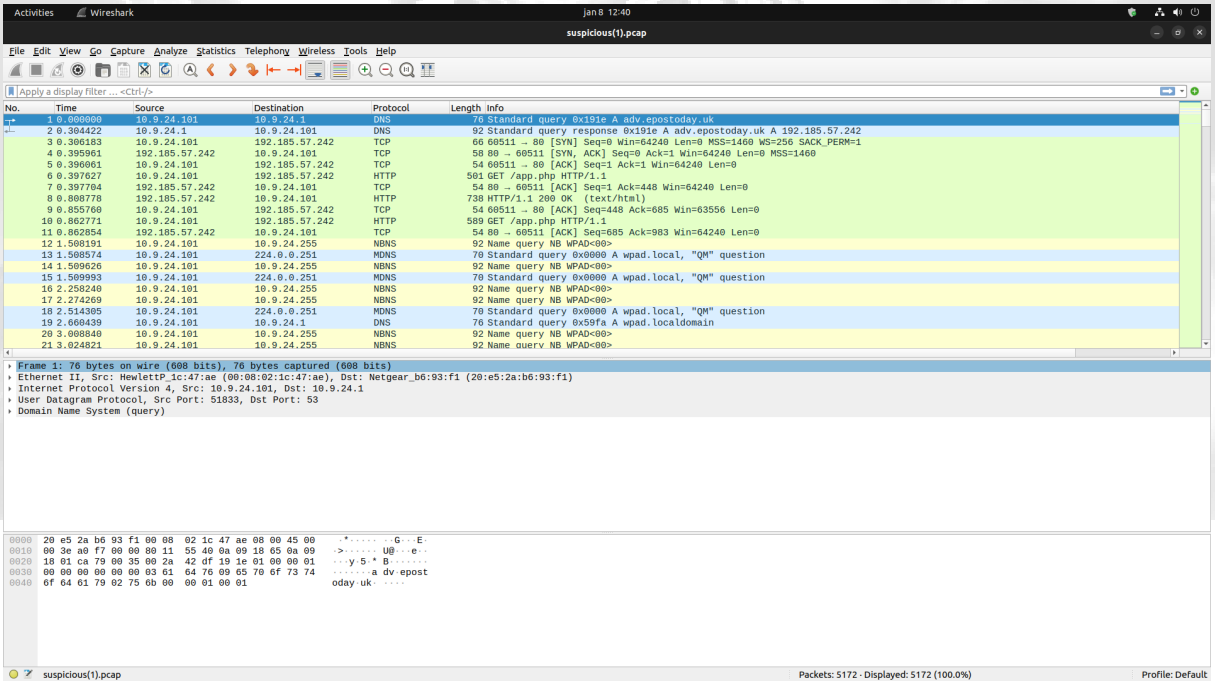
Write-up CTF
SANS - Holiday Hack Challenge 2022
Challenge: Wireshark-Practice
Difficulty: Very Easy
https://github.com/brunopelegrini

First of all, open the Objectives session in the left menu.

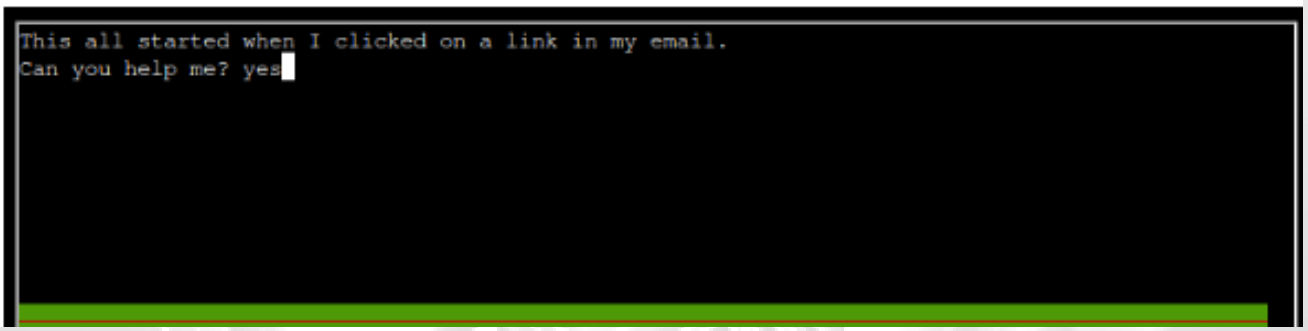
For this challenge, we have the suspicious PCAP file to analyze. Download this file, then open it in the Wireshark.



@badposeidon1
https://github.com/brunopelegrini

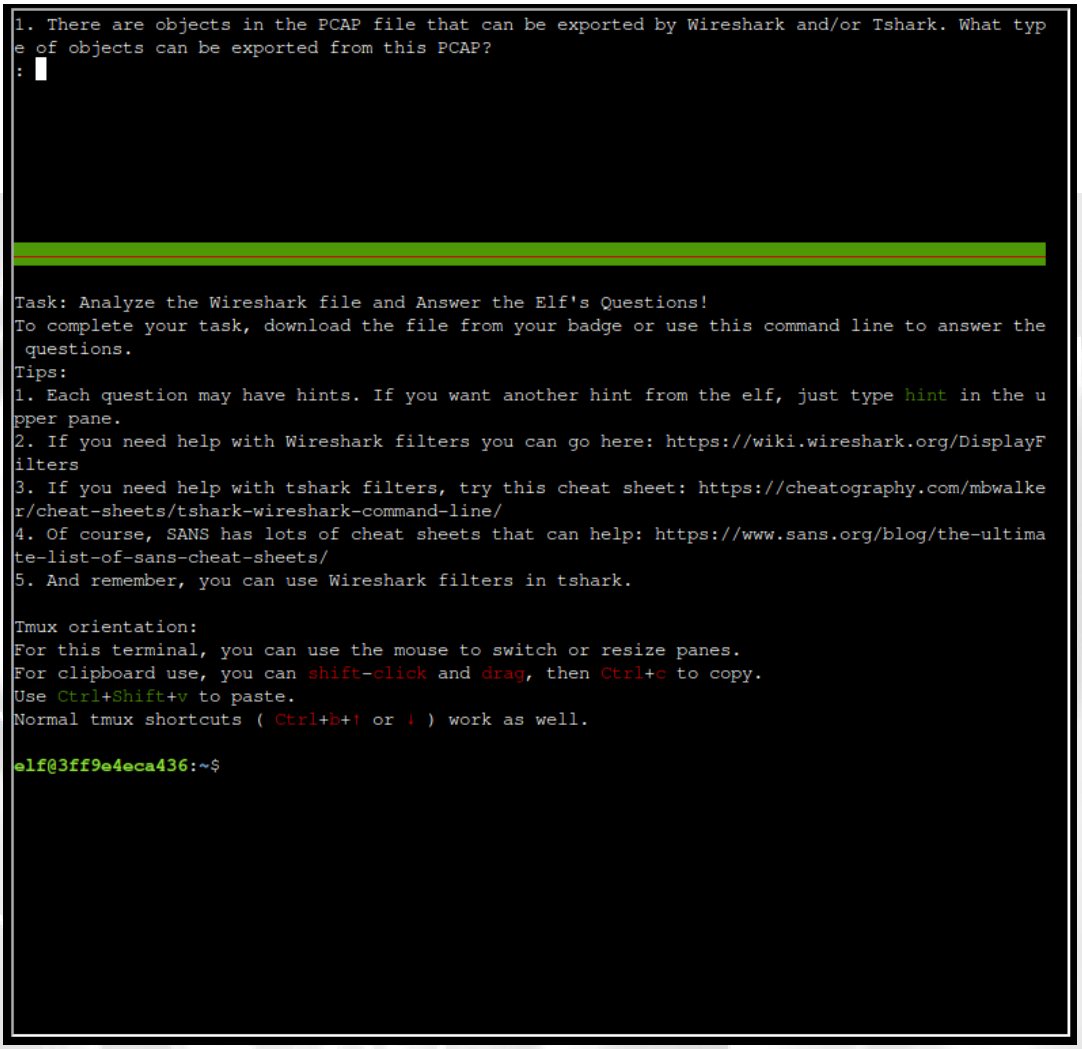
In the Kringlecon game, go to Tokien Ring tunnels and search for Wireshark Phishing Terminal, then connect.

The Terminal will show two sessions. In the above session is where you'll insert your answers.
Then type **“Yes”** to continue.

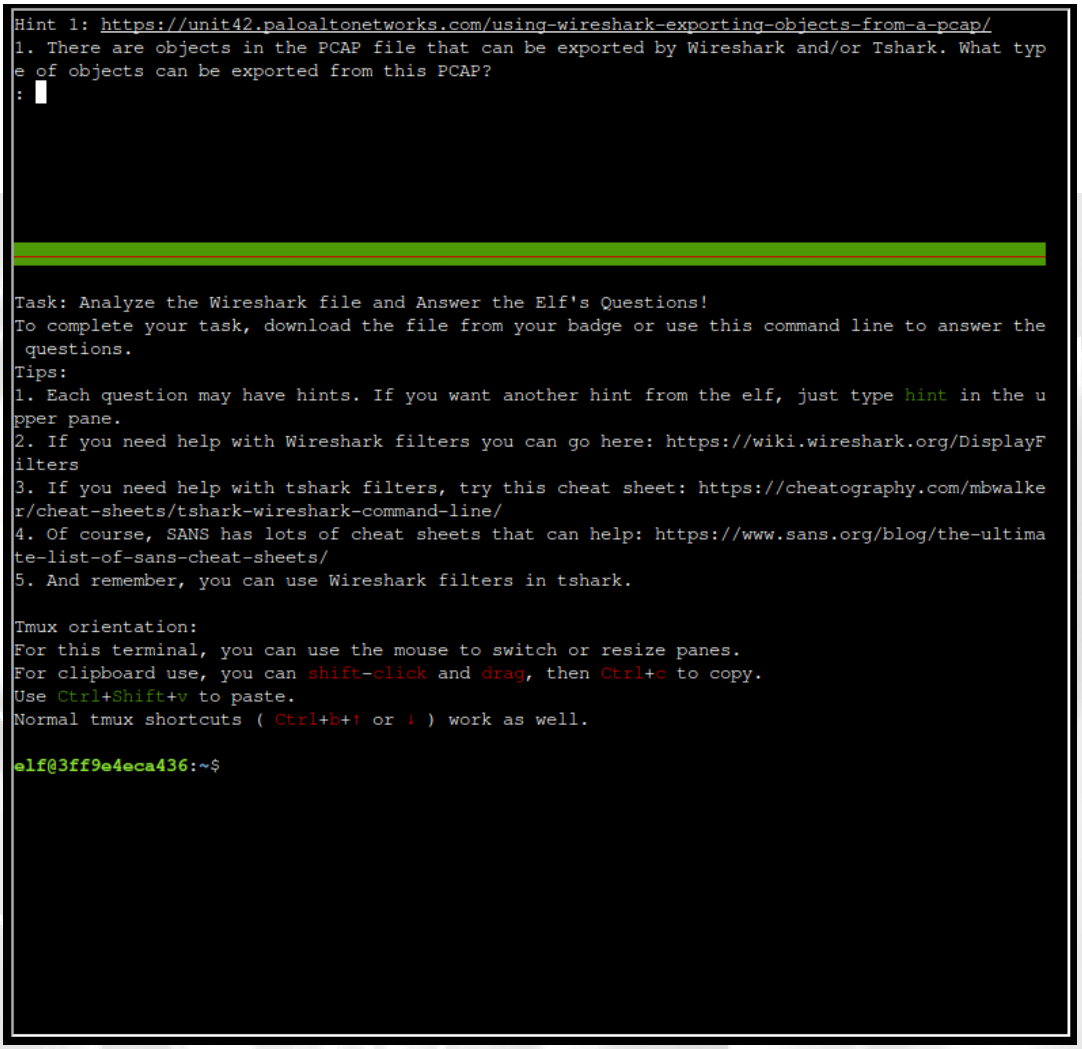


@badposeidon1
https://github.com/brunopelegrini

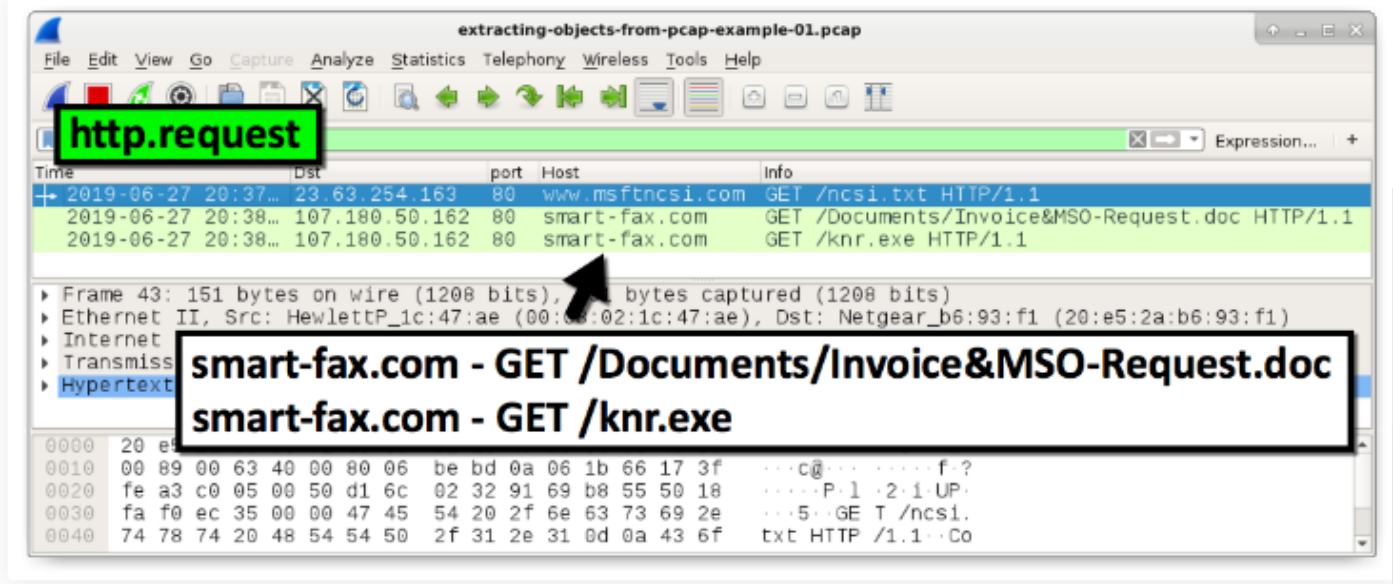
Now the first question about challenge is shown, it refers to what type of object could be exported by Wireshark PCAP.



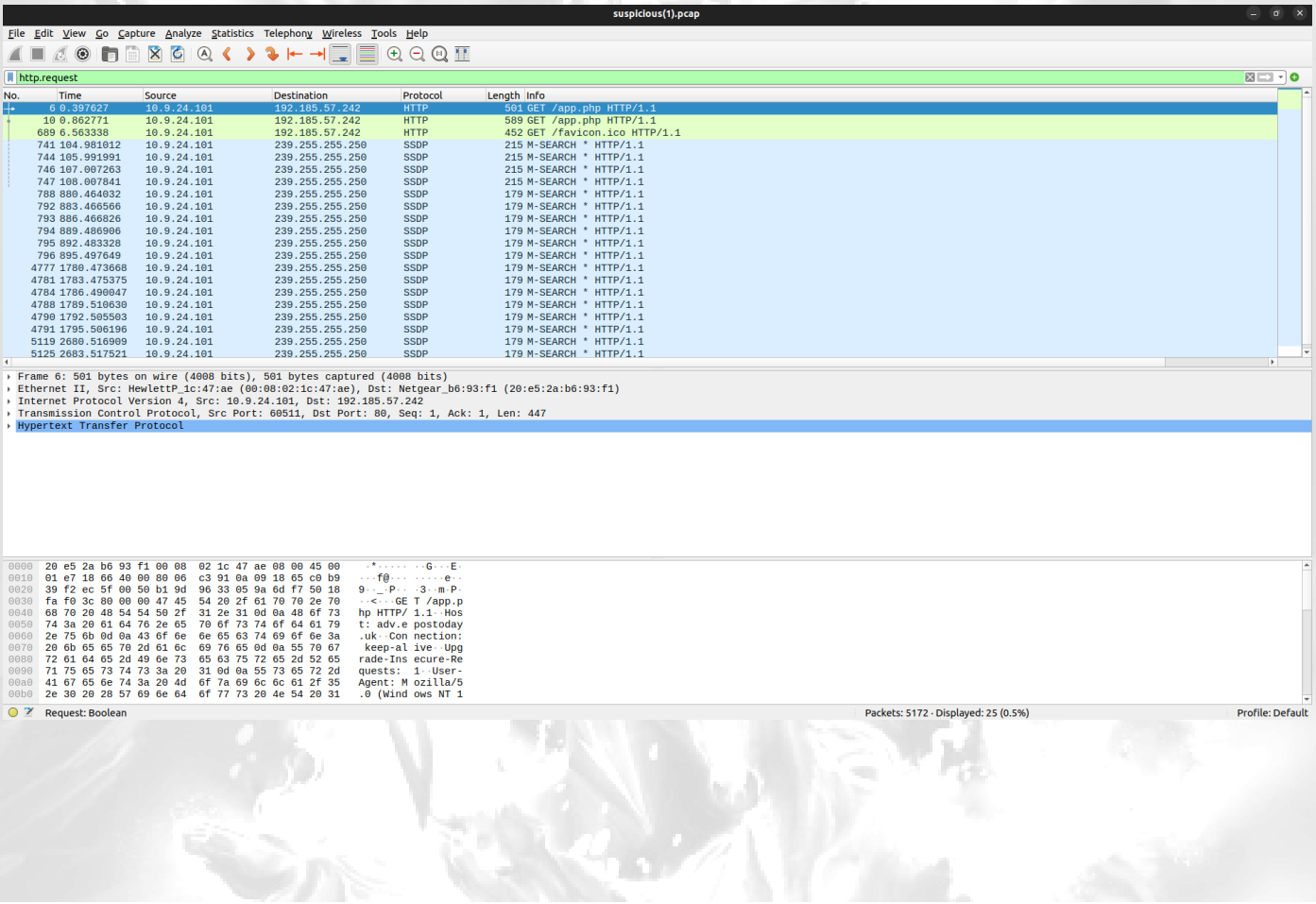
In this step, I searched in Google about “Extraction files in Wireshark”, how I can’t find it, so I decided to ask for a hint for the terminal.



It shows a link for reference. In this reference we have a specific session about HTTP requests, then I decided to try it!

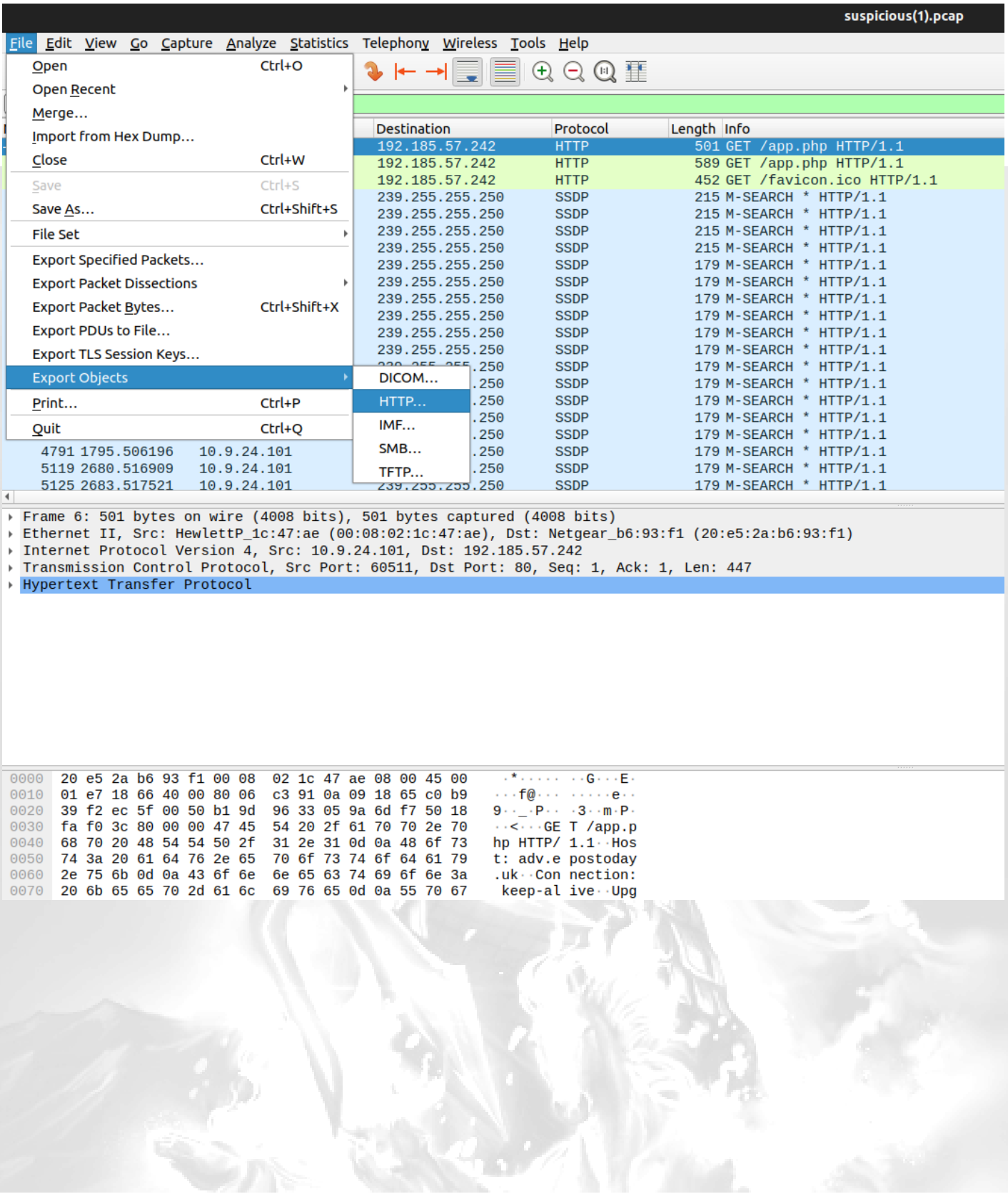


Now, I filtered by HTTP requests, and now I have only 3 lines about HTTP requests.



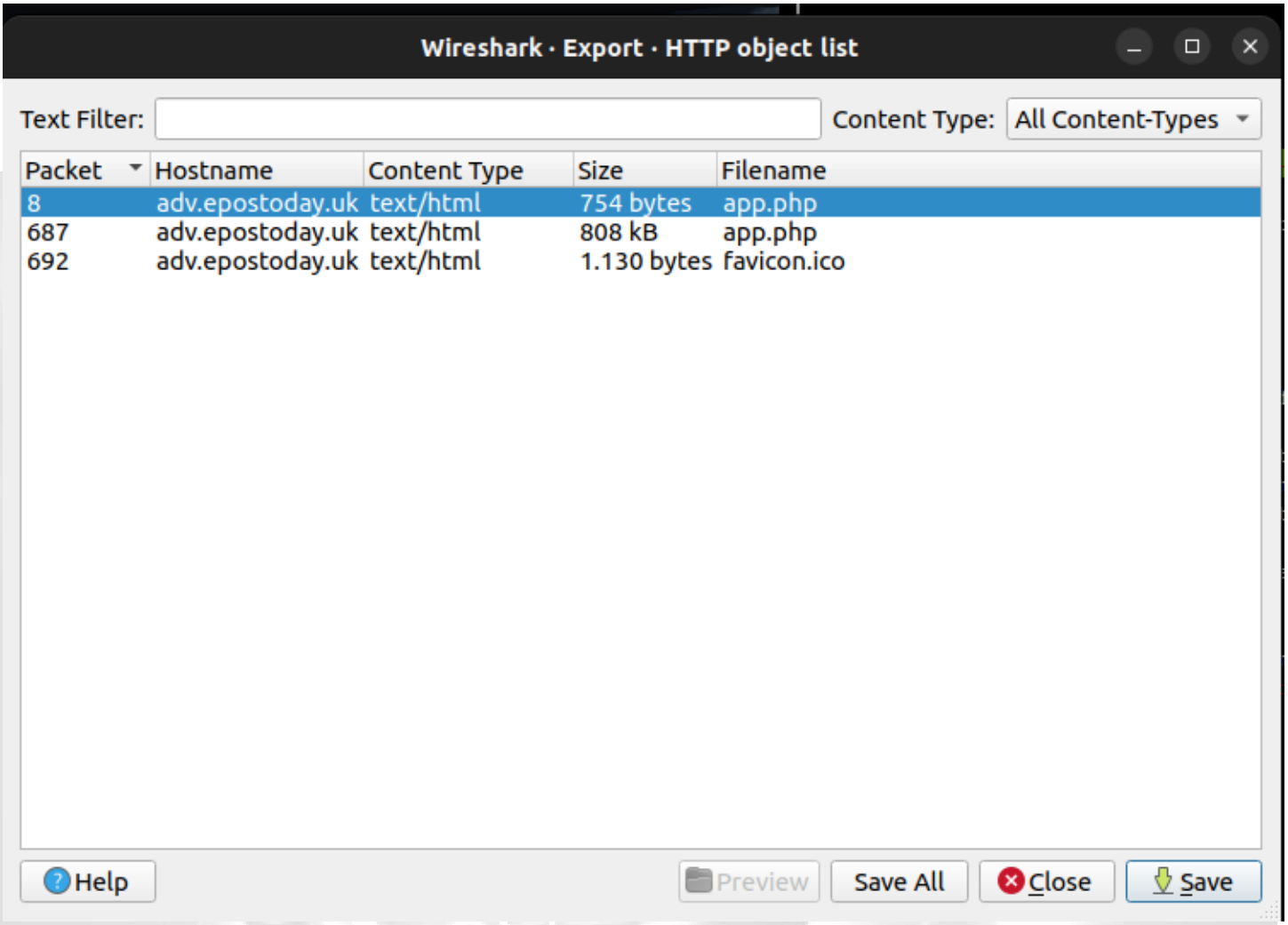
@badposeidon1
https://github.com/brunopelegrini

Following the reference available, I tried exporting the HTTP request.

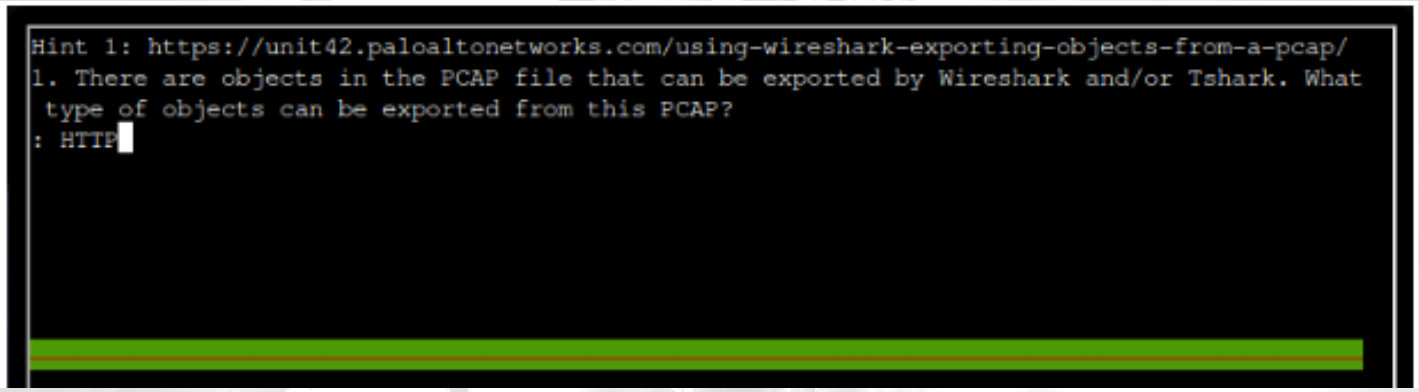


@badposeidon1
https://github.com/brunopelegrini

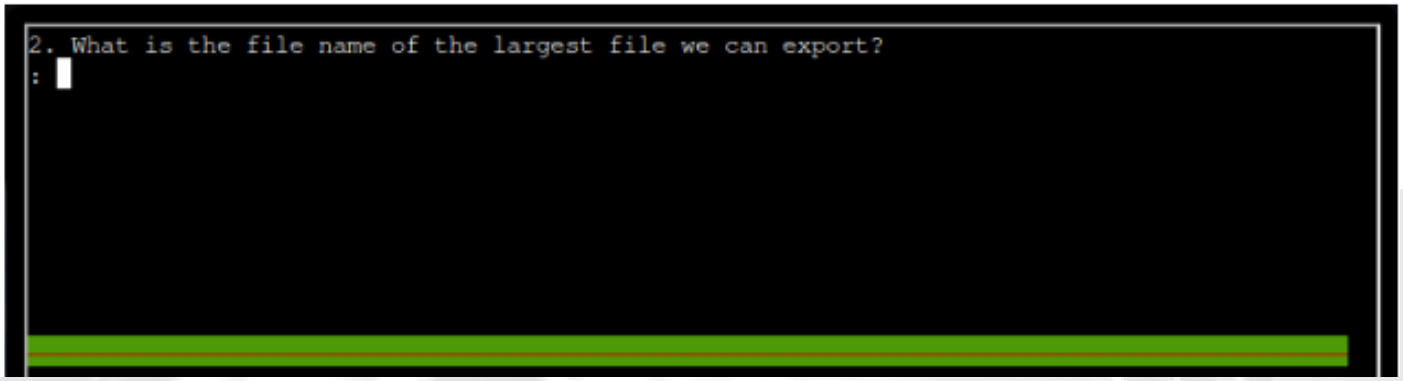
Notice, in the window opened we have two files, the app.php and favicon.ico, but the object showing in the bar is HTTP object list. I saved the first file in my PC to after analyzing.



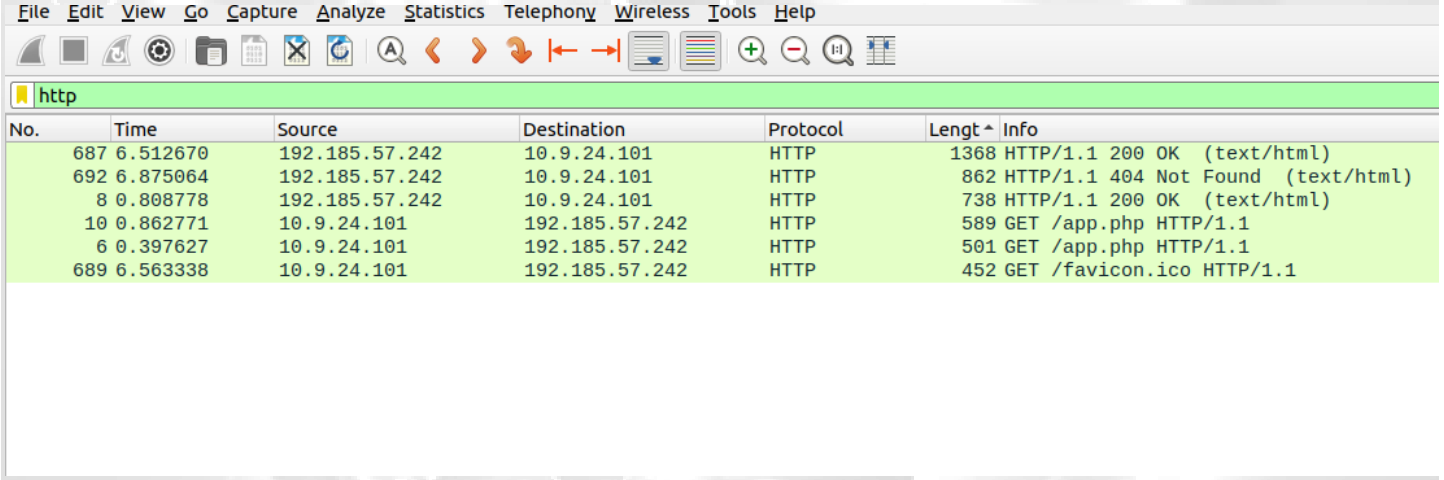
In Terminal, I tried to type “HTTP”, because the object exported for me it’s of type HTTP.



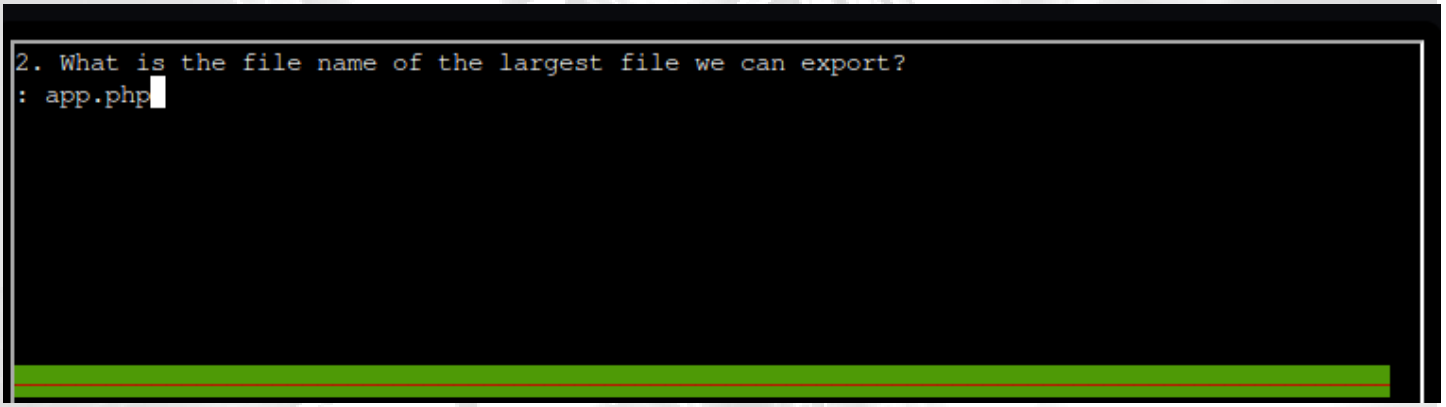
Now the terminal is asking for the largest file we can export.



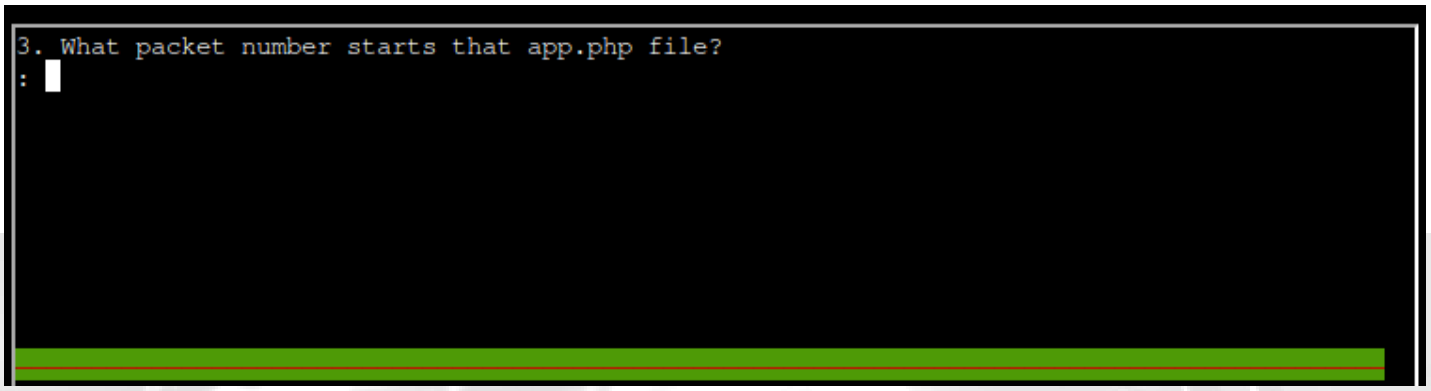
For this step I changed the filter by “http” and I ordered the largest file in the Length column.



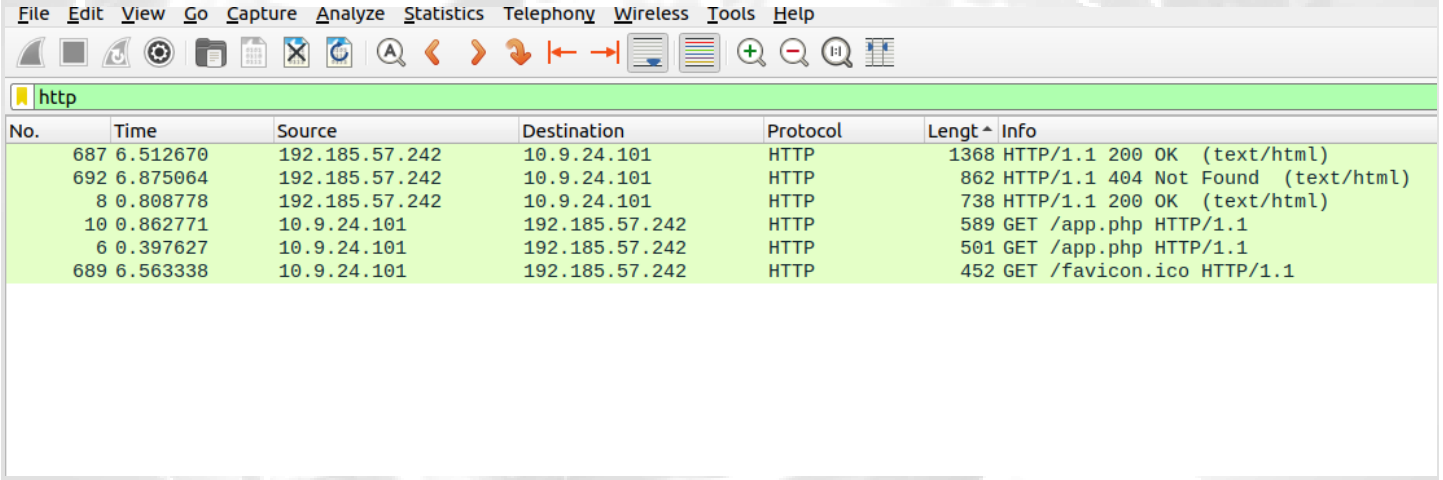
In the terminal I type app.php, which references the largest package.



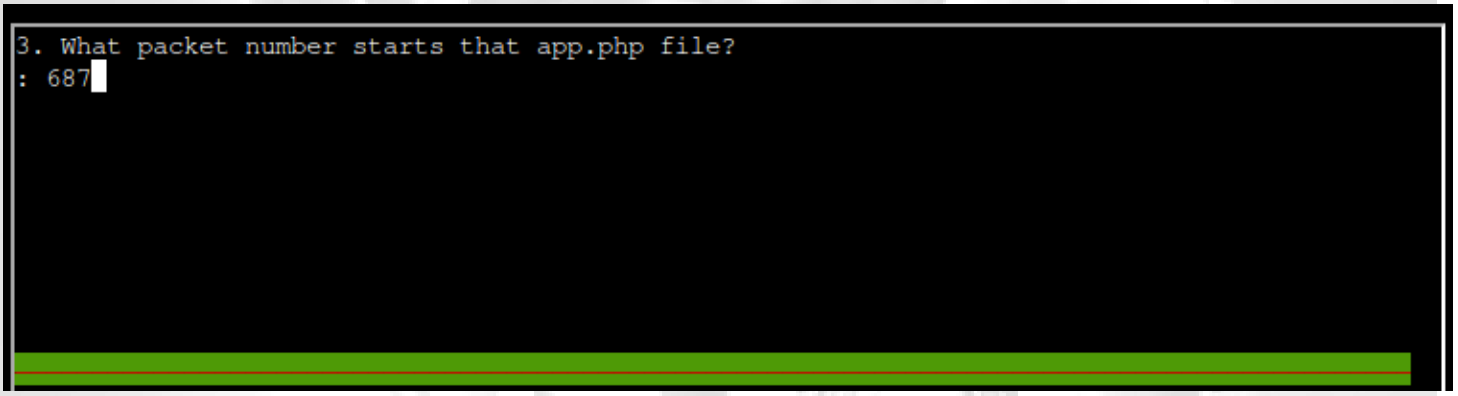
Now, we have question number 3, what number packet it refers to.



Look for the first packet ordained.

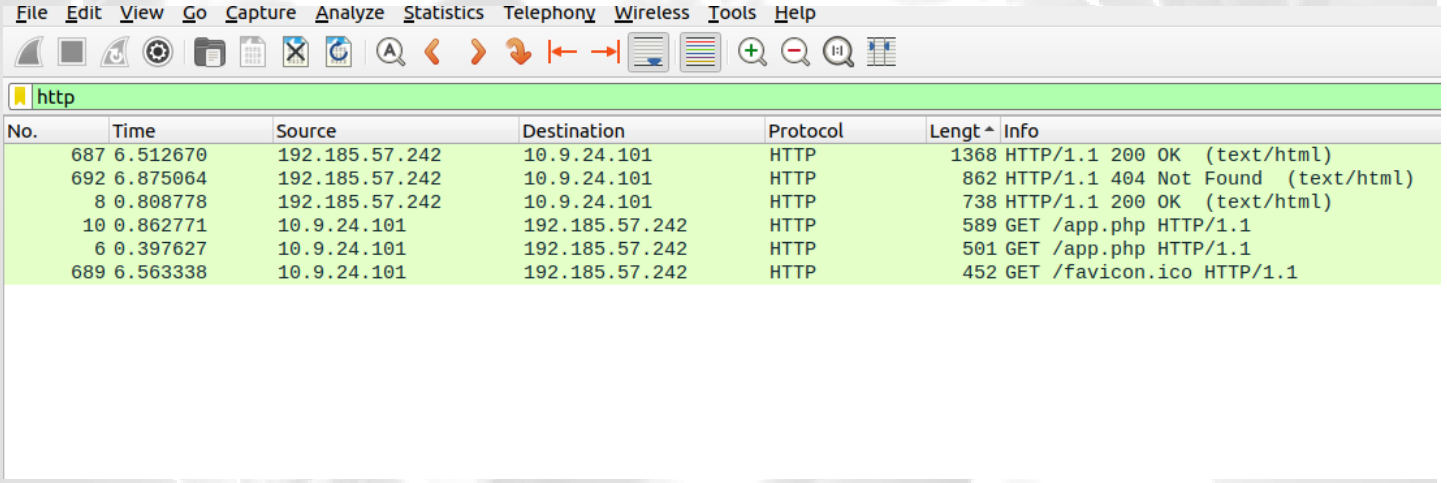


In the terminal type 687 and press enter.



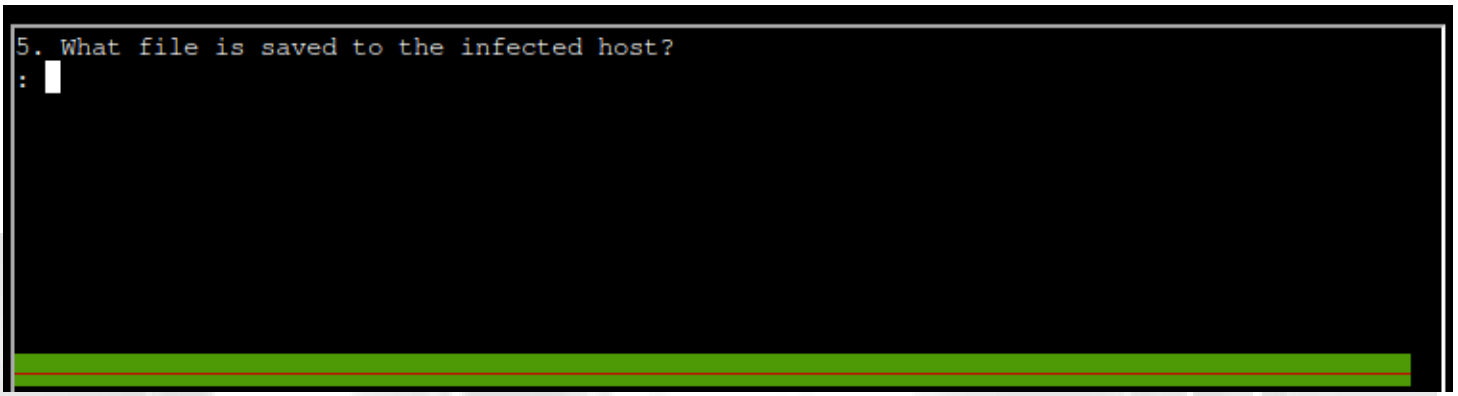
Now, we have question number 4.

Look for the same line, the IP Source to find the required IP.

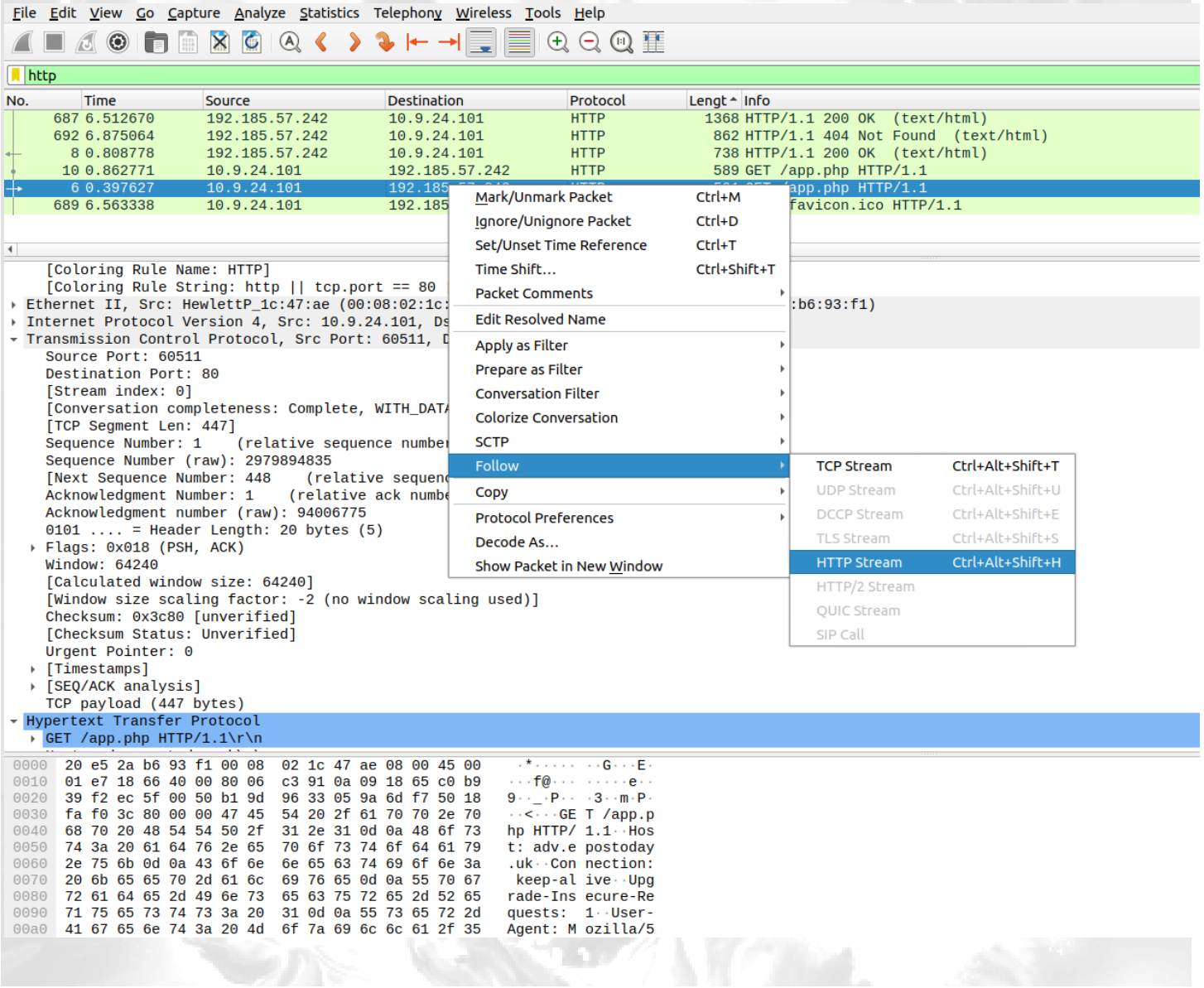


So, type 192.185.57.242 and press Enter.

We have question number 5.

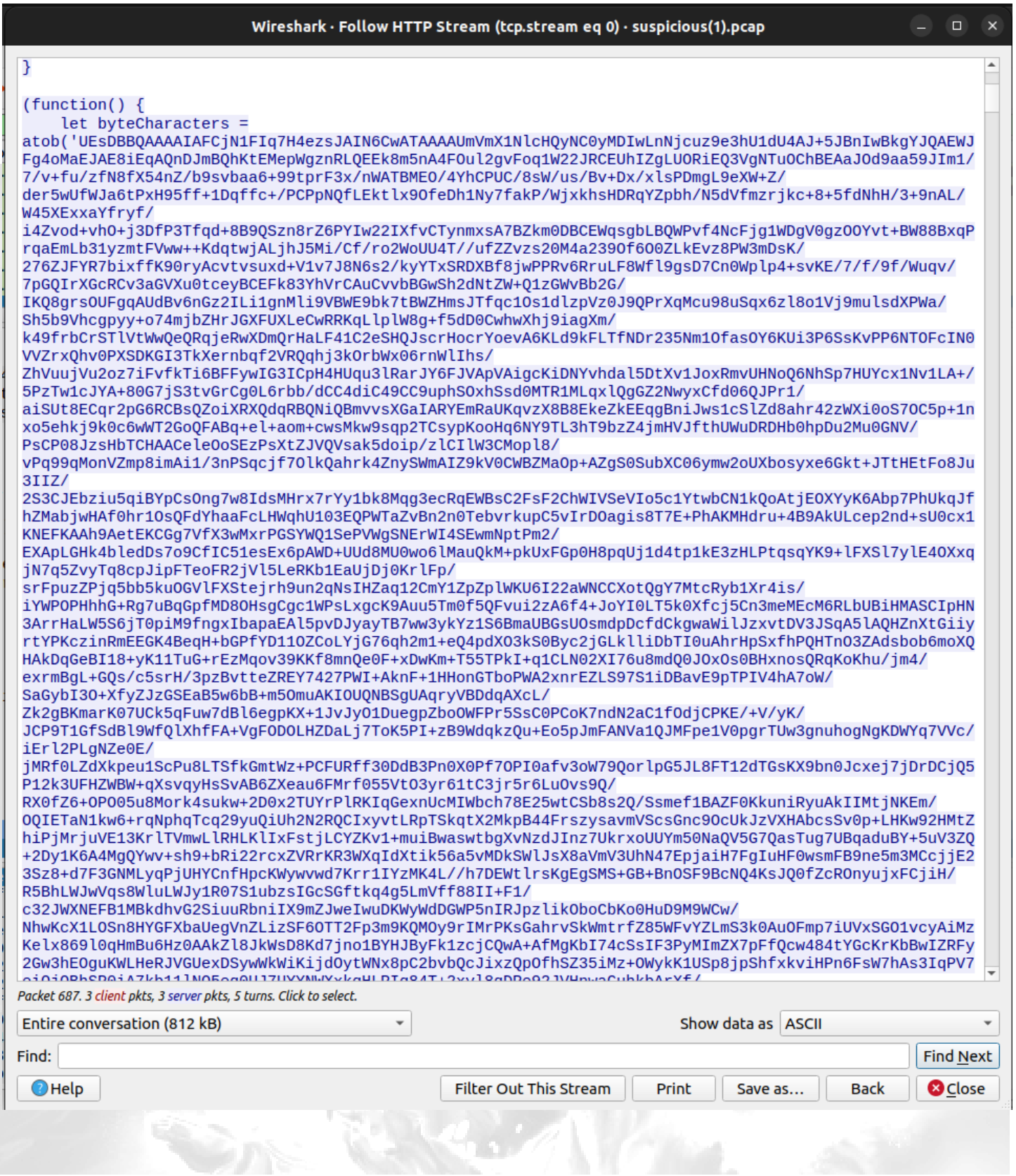


Select the line refer to app.php request, then right click, click Follow and HTTP Stream.



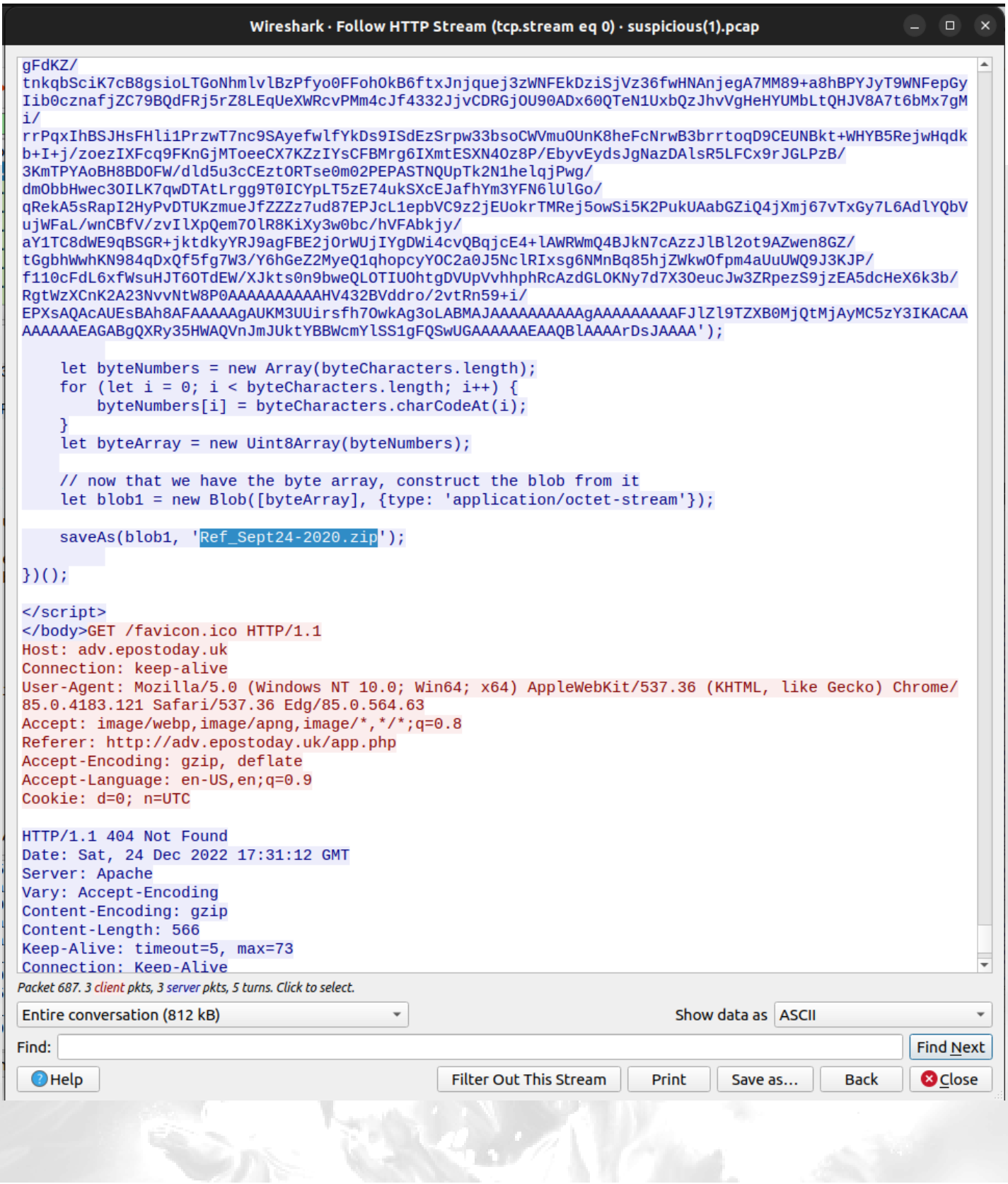
@badposeidon1
https://github.com/brunopelegrini

The window Follow is opened, searching anything related to this, I found this stranger block of code.

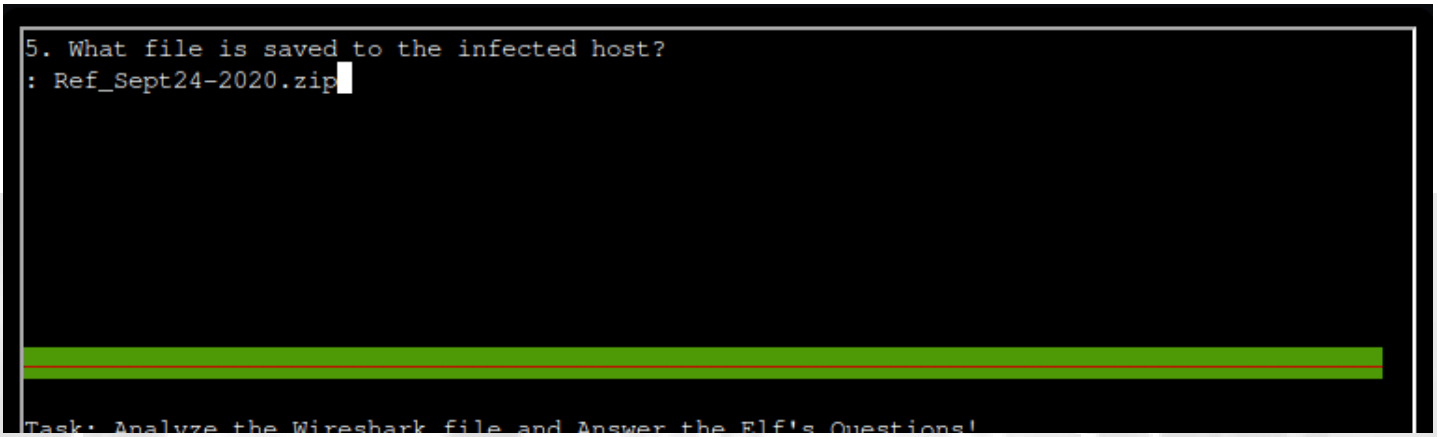


@badposeidon1
https://github.com/brunopelegrini

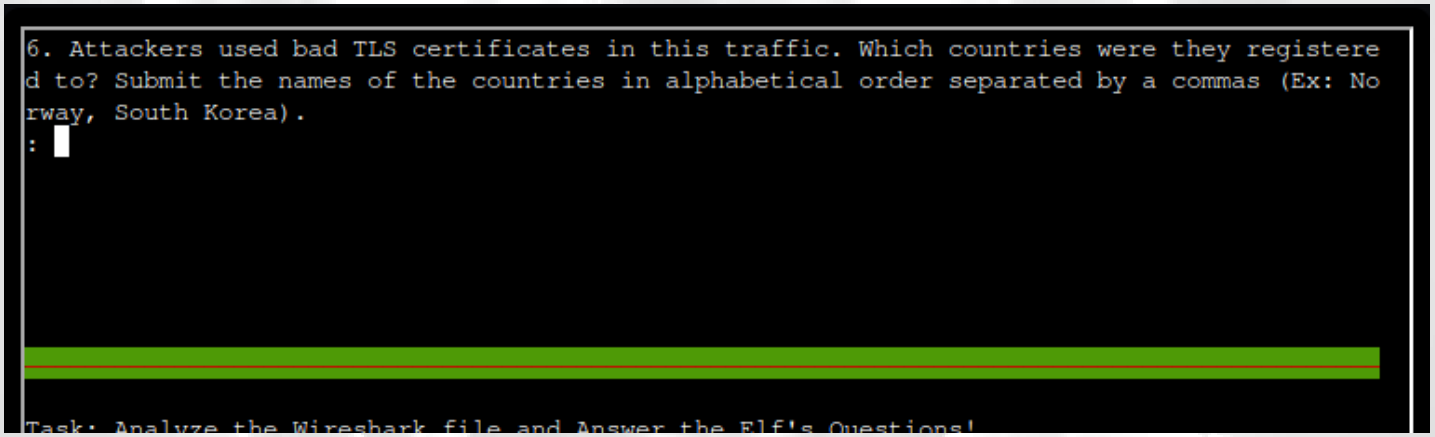
Looking a little bit, I found the file .zip.



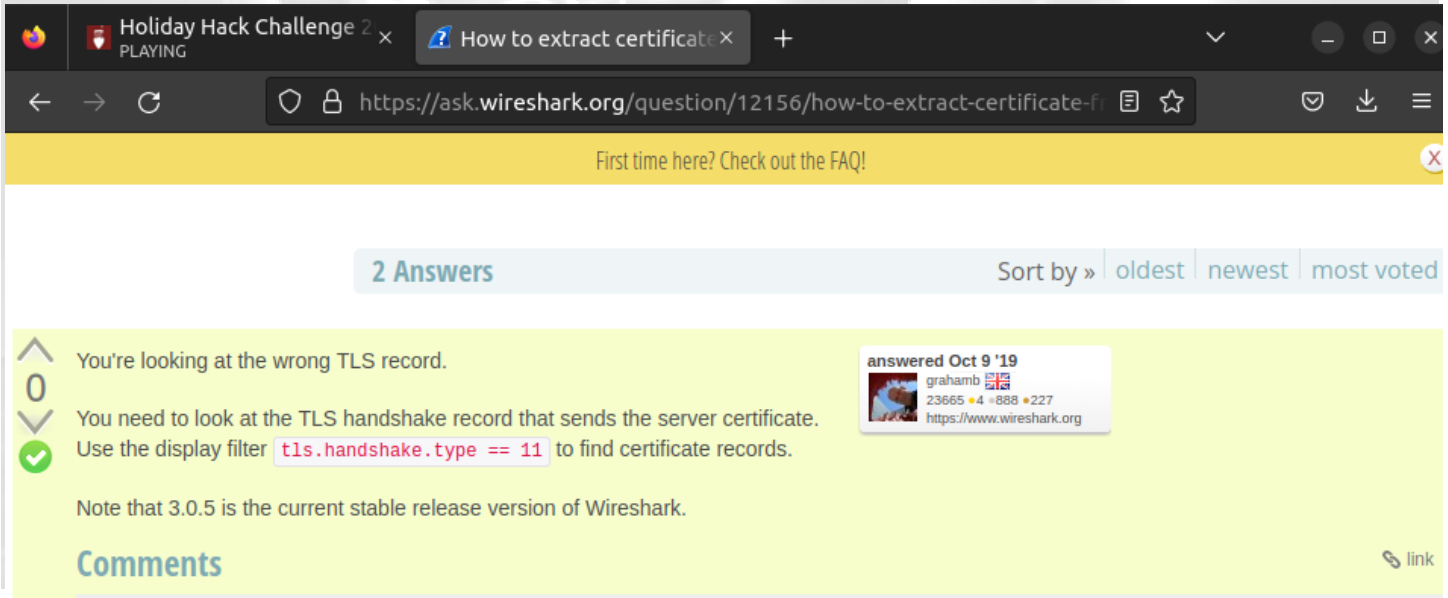
Type Ref_Sept24-2020.zip in the terminal and press Enter.



We have question number 6.



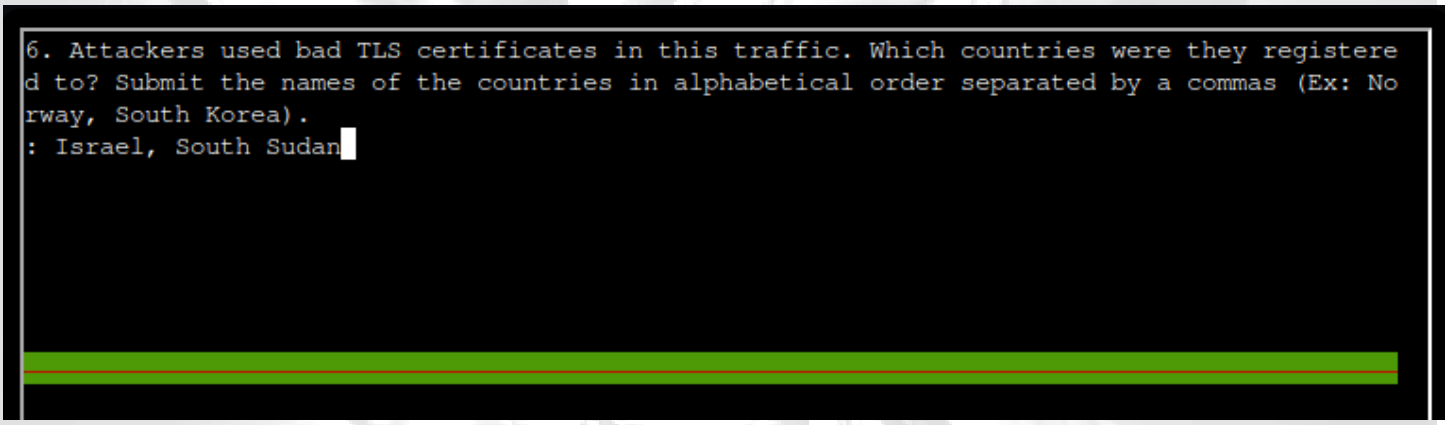
I made a search in Google about “How to extract bad certificates Wireshark”, then I found the filter below.



Using the filter, I found some companies that use bad TLS certificates. But I have two that get my attention, because they use a atypical location.

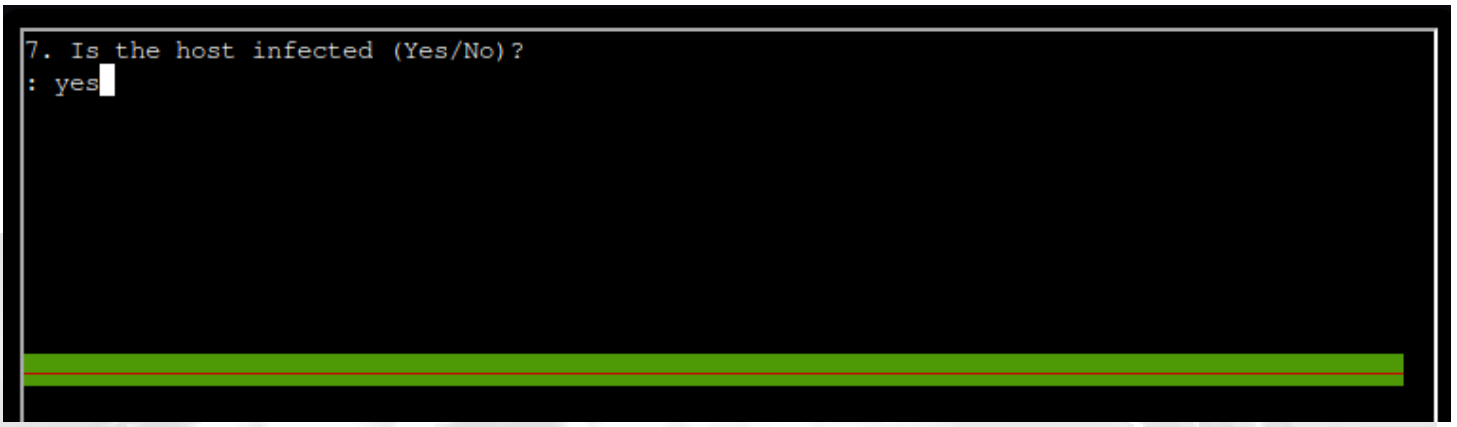
- Nagoya - IL (Israel)
- Aquarelle - SS (South Sudan)

So, I put it in alphabetic order and send it to the terminal. Type “Israel, South Sudan”.

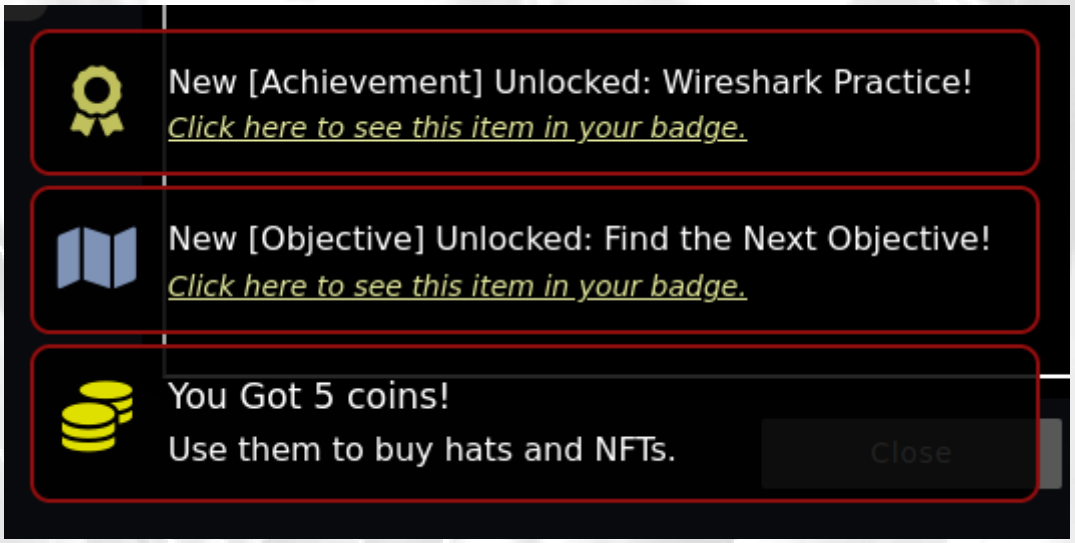


Now the terminal asks me if the endpoint is compromised.

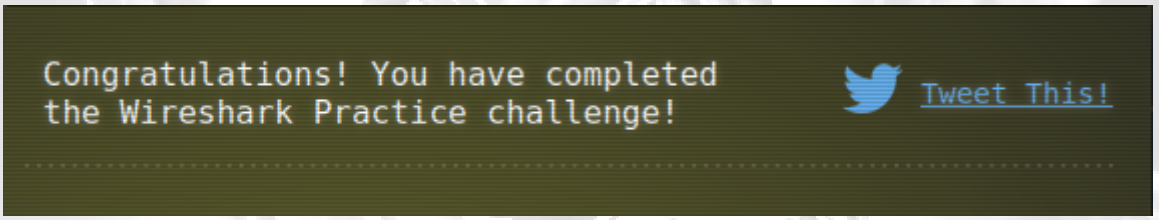
In my opnion, yes! So I type it the terminal!



The challenge is done!



Now share it with your friends!



@badposeidon1
https://github.com/brunopelegrini