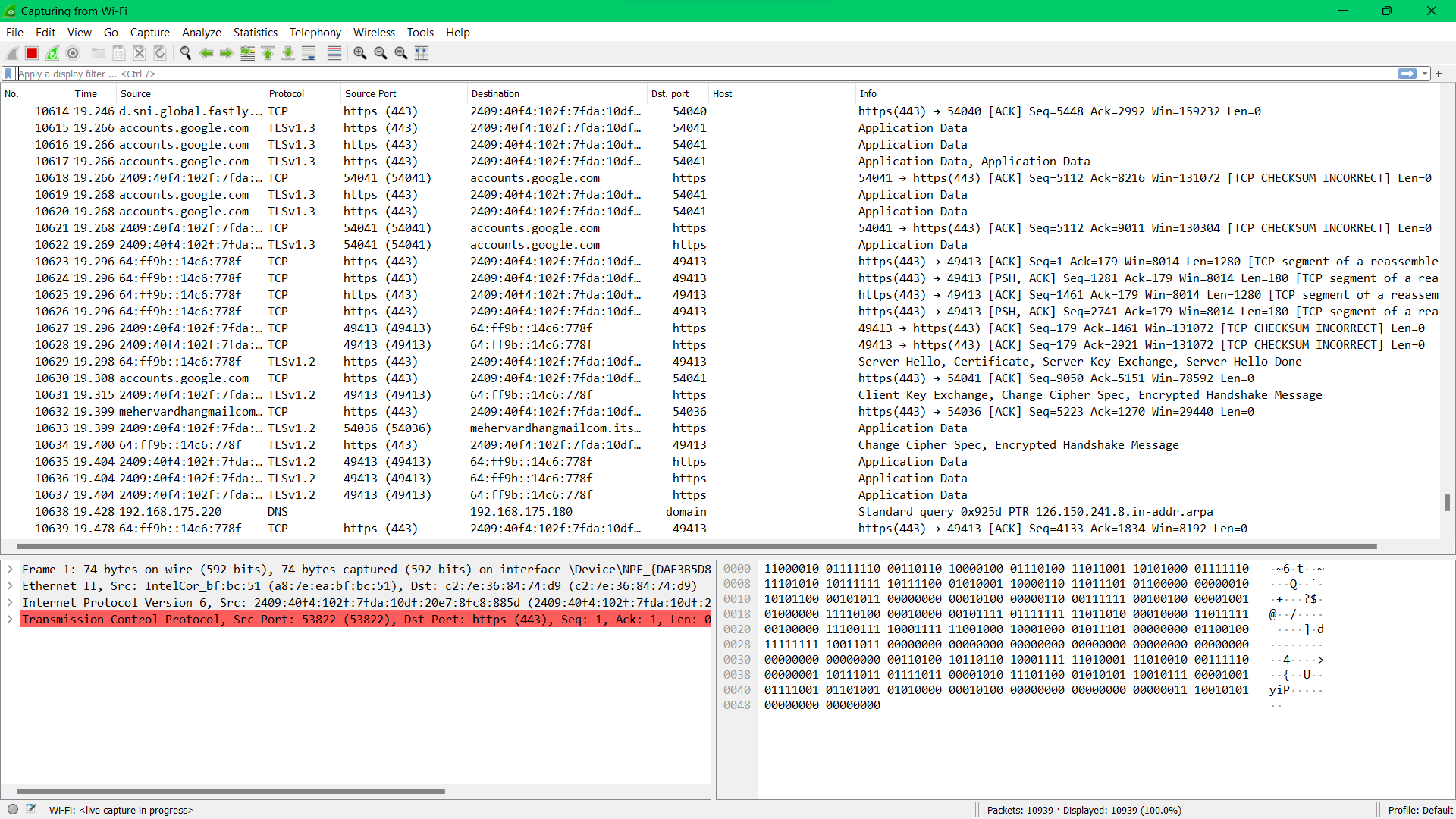
**WIRESHARK ASSIGNMENT**

NAME: T SAI SRINIDHI

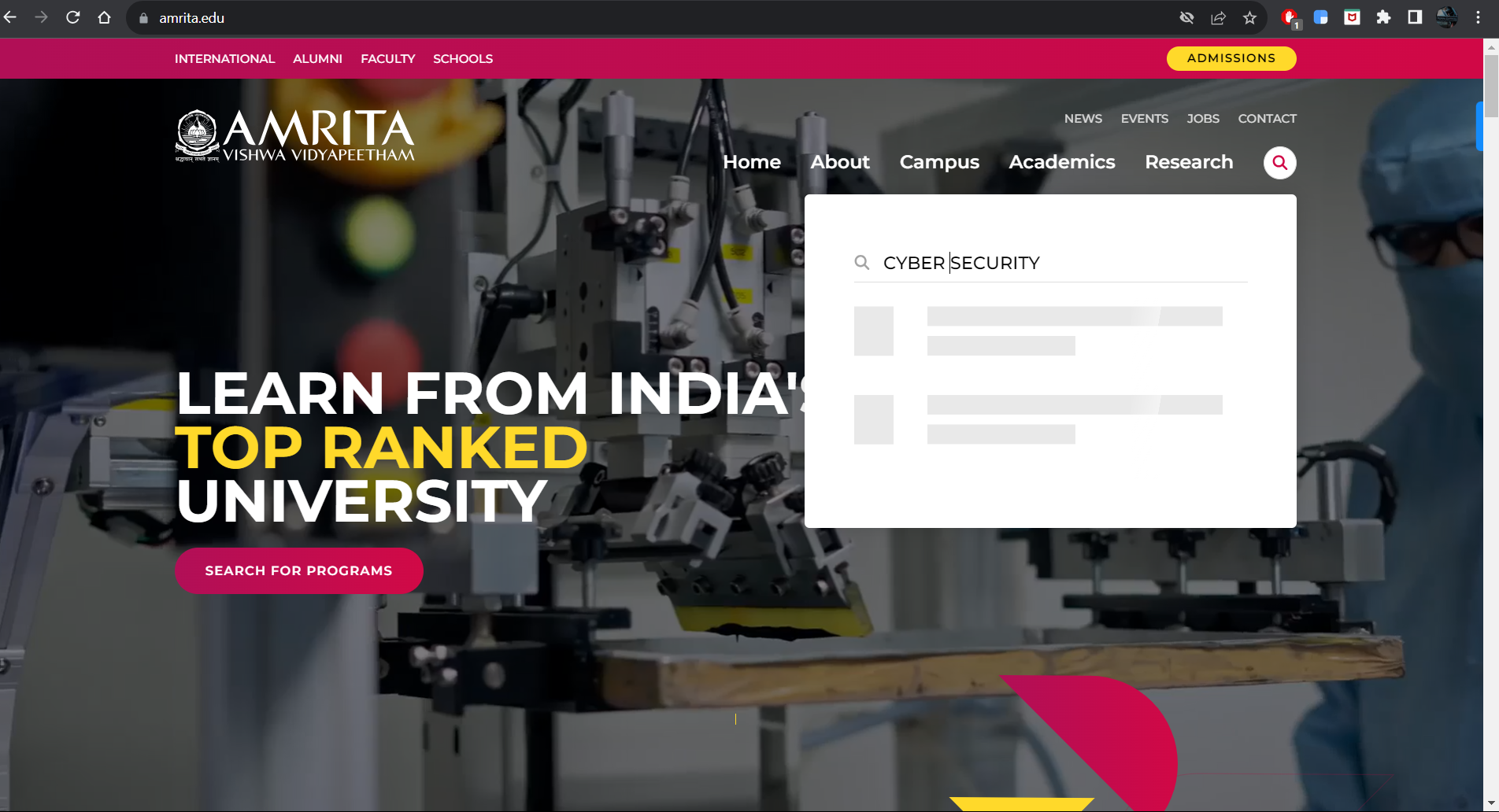
ROLL NO: AM.EN.U4CSE21150

Q1)



Here we are using Wi-Fi interface, and sniffing the traffic. 

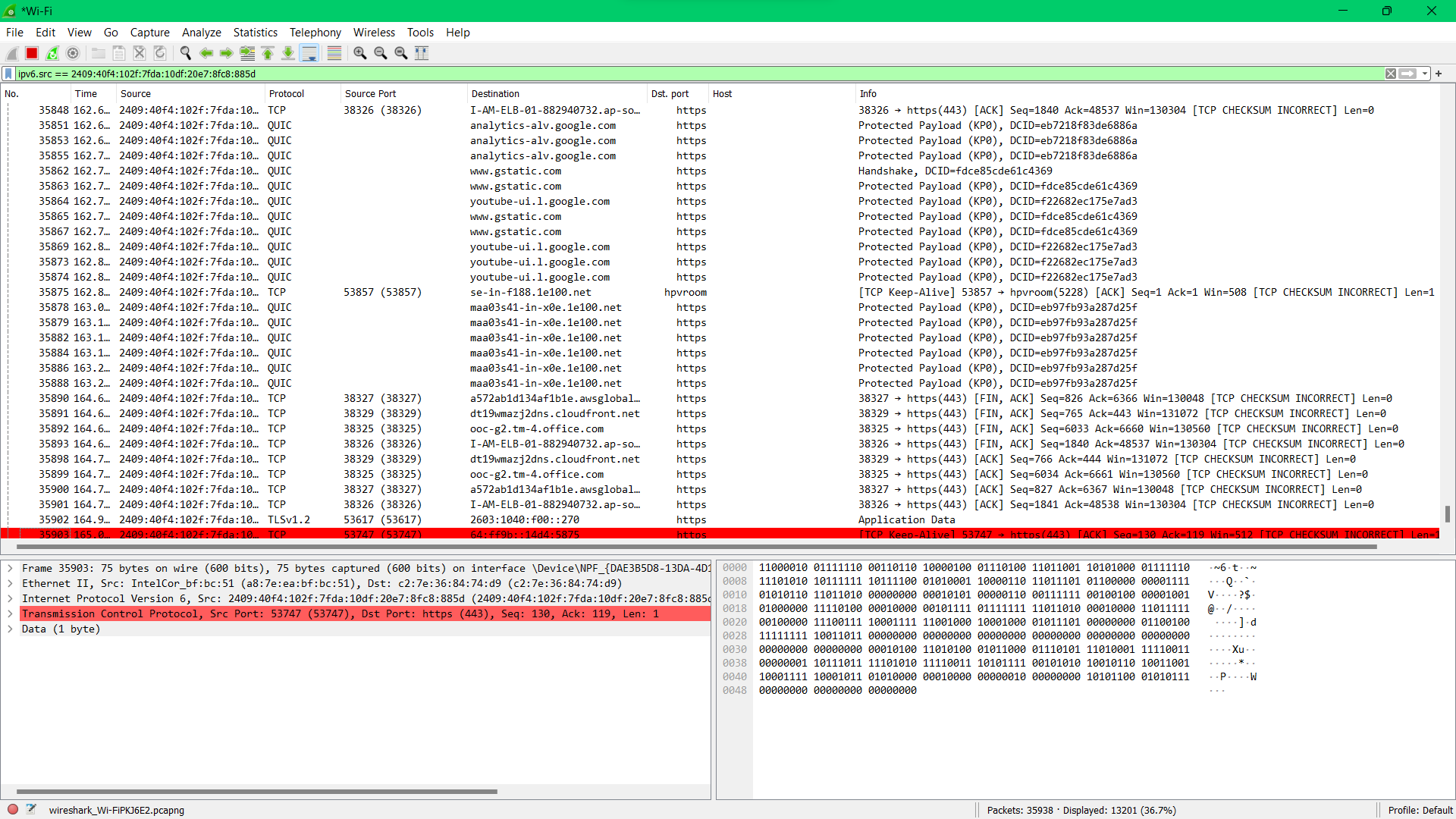
Q2)



Here we are browsing the domain amrita.edu and searching the keyword “**cyber security**”.



Here on searching the keyword cyber security in the webpage “**AMRITA.EDU**”, we got redirected into [B. Tech. in Computer Science and Engineering (Cyber Security) | Amrita Vishwa Vidyapeetham](https://www.amrita.edu/program/btech-computer-science-and-engineering-cyber-security/) with ipv6 2409:40f4:102f:7fda:10df:20e7:8fc8:885d



Q3)

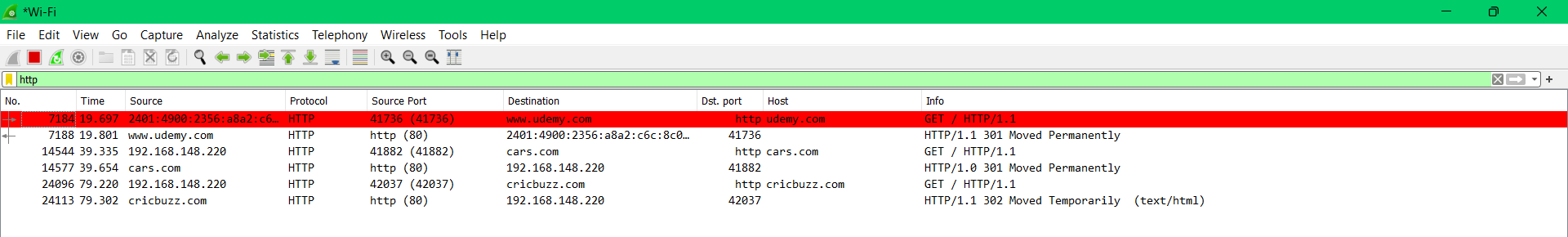
**HTTP GET Request:**

The primary purpose of a GET request is to retrieve data from the server. It's used when you want to request information from a specified resource.

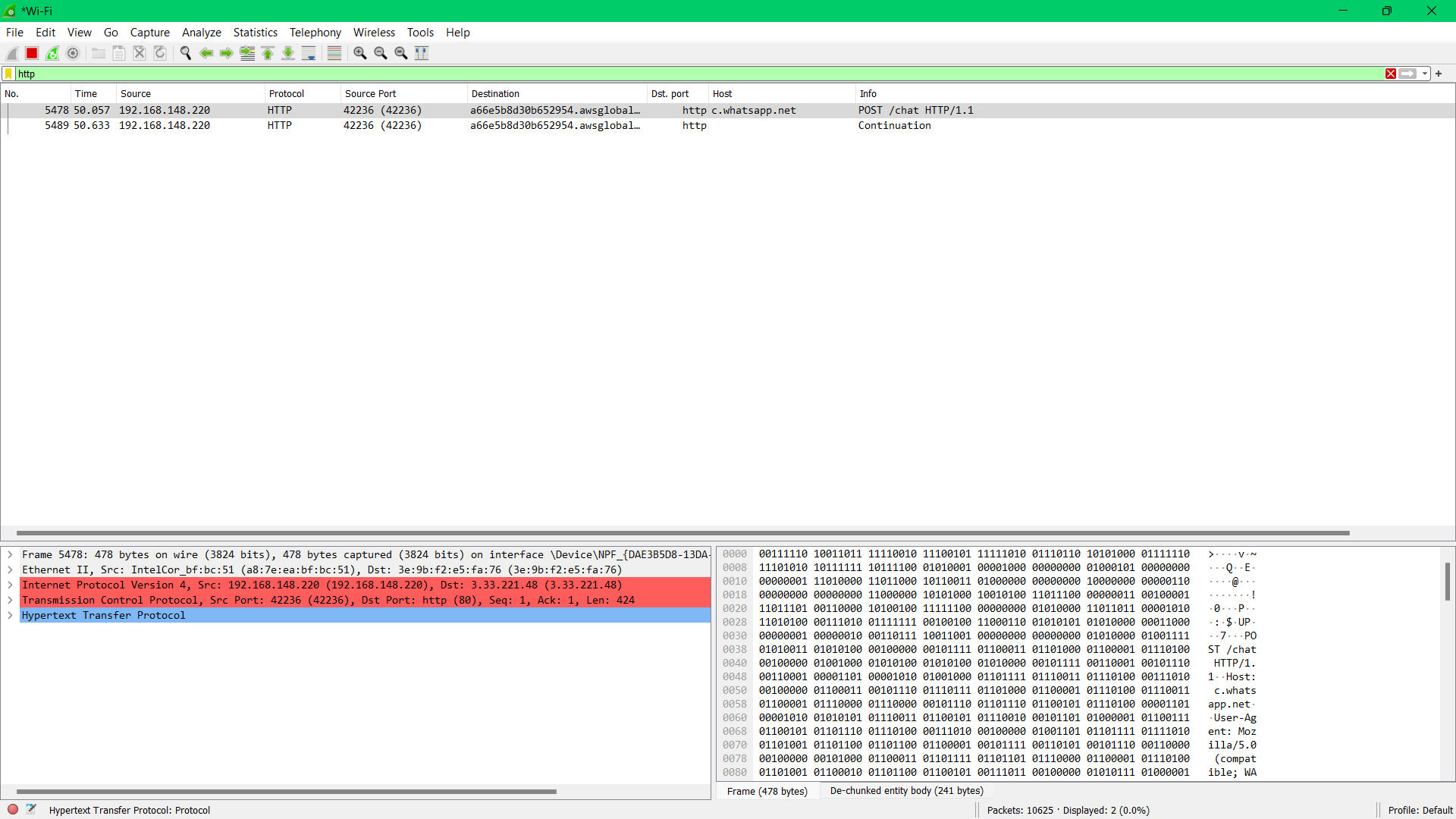
**HTTP POST Request:**

The primary purpose of a POST request is to submit data to be processed to a specified resource. It's used when you want to send data to the server to create/update a resource.

GET-REQUEST

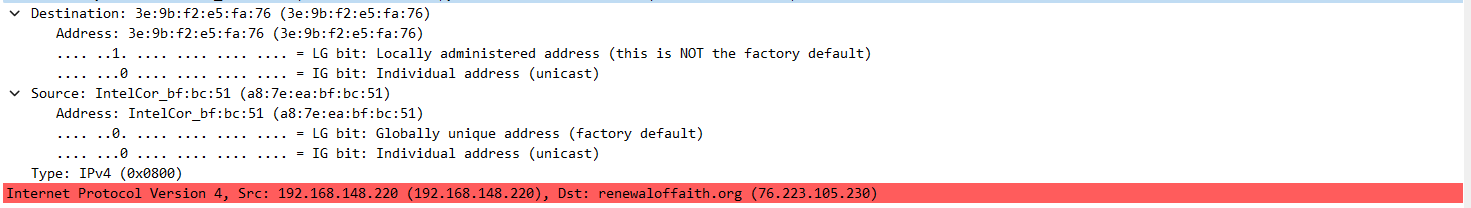


POST – REQUEST



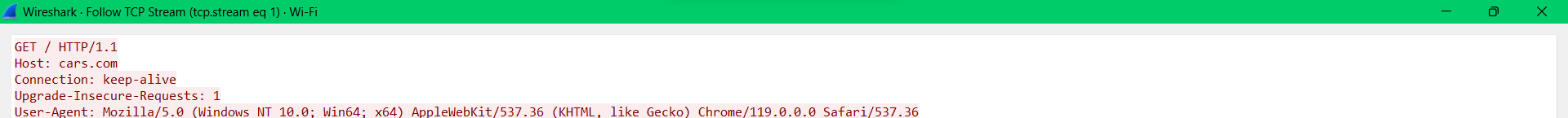
3 a) src port and destination port are: 42666 and http (80)

Physical address of both source and destination



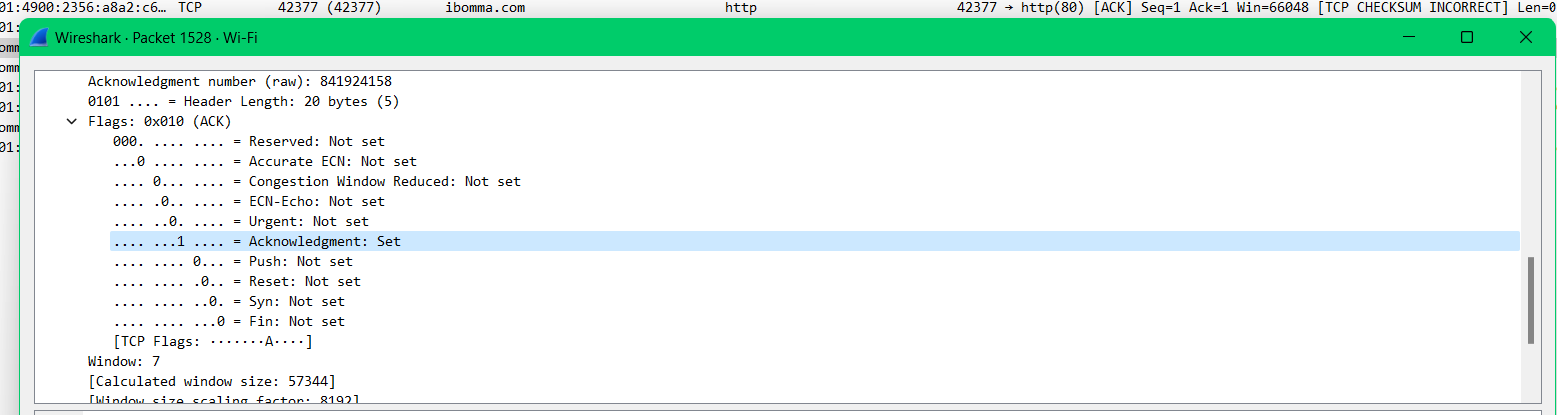


3b)

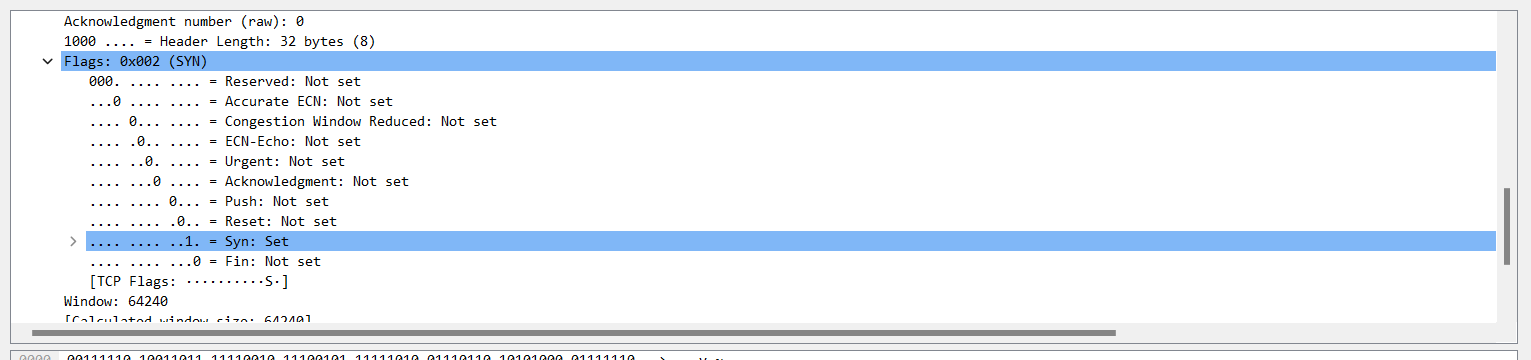


3 C)

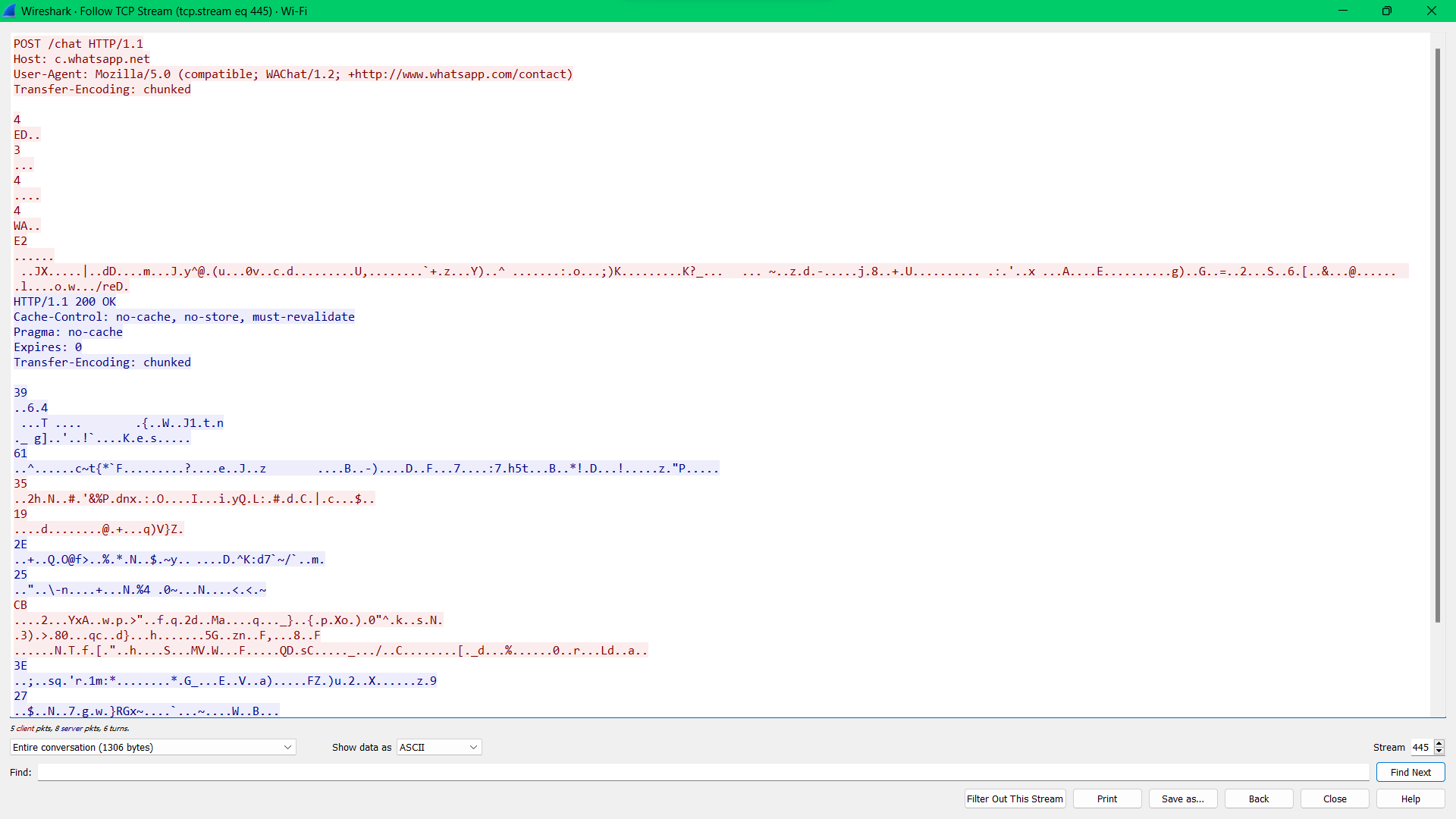
There are cases where the acknowledgment will be 1 in this case (flag at ACK == 1)



There is a case where there is no acknowledgement in the ACK (flag at ACK == 0)

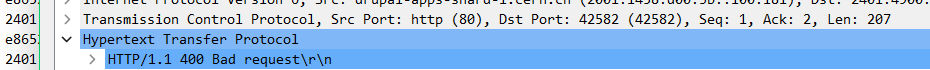


3 d)

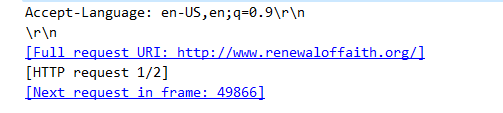


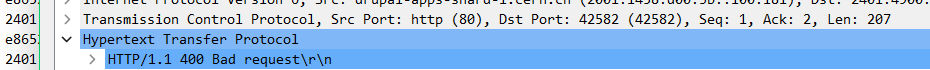
3 e)

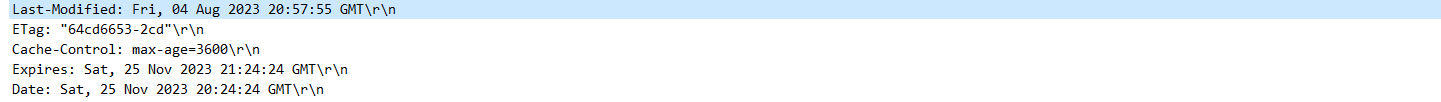
1. HTTP 1.1 is the version running



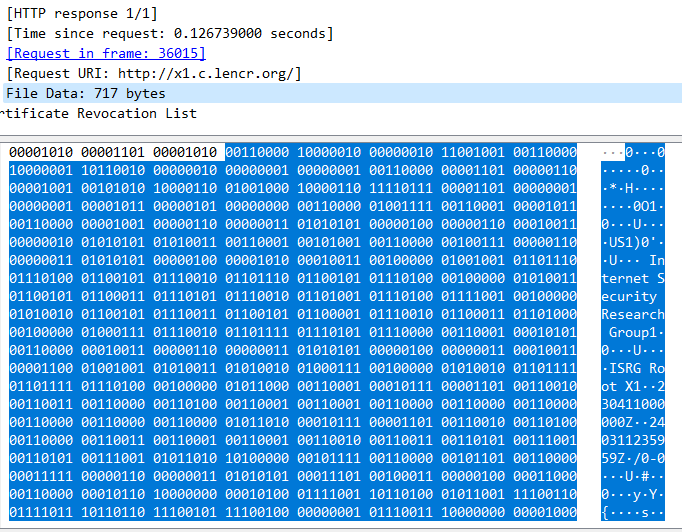
1. En -US is the language browser accept to the server.



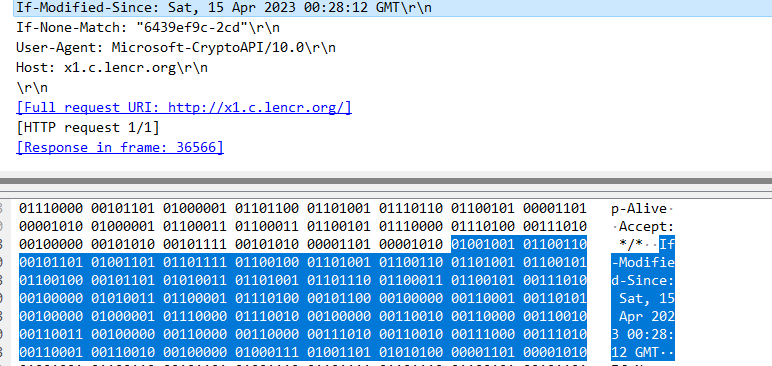
1. here there is bad-request with status code 400
2. Last modified by the server at

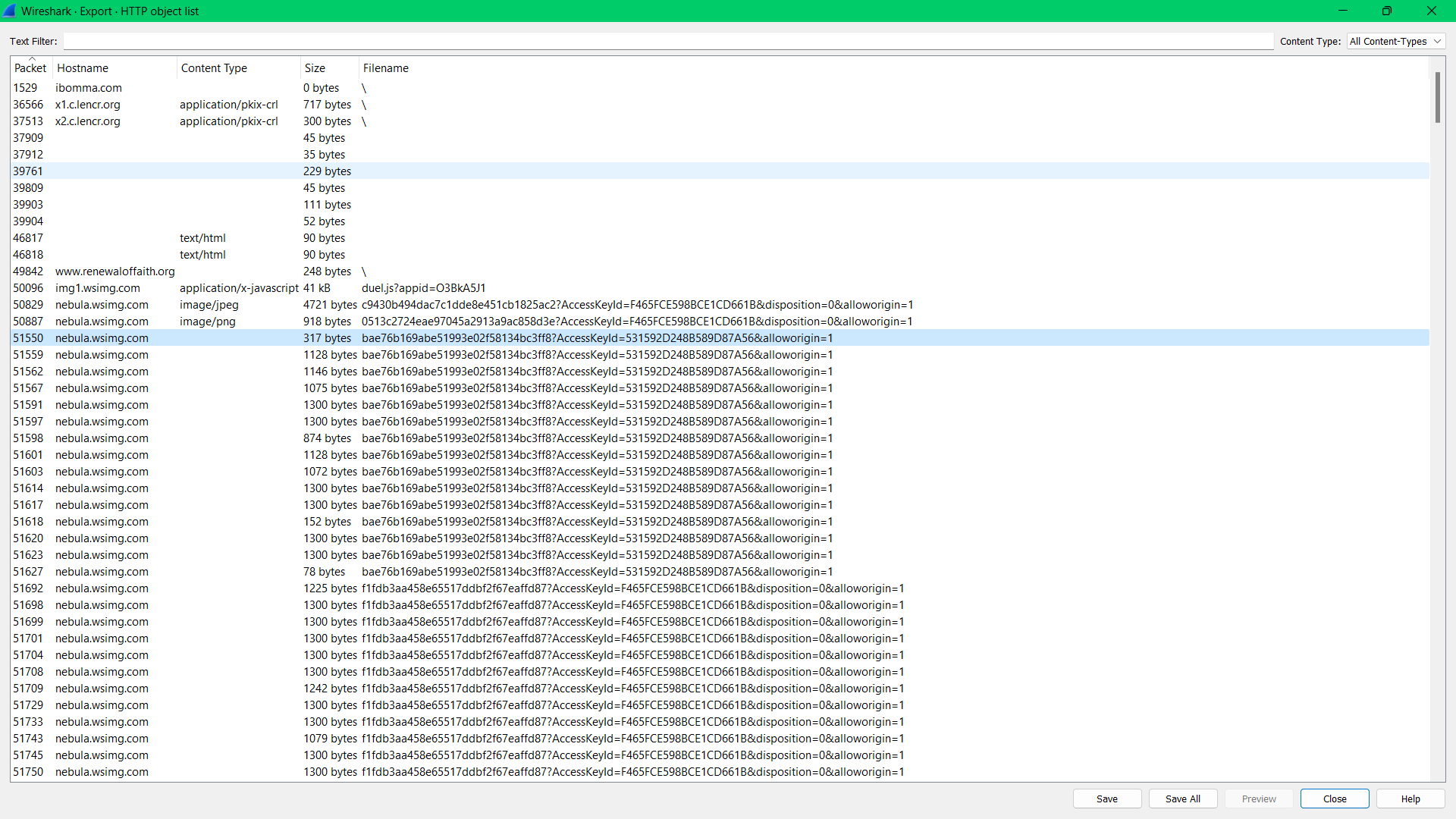


1. Bytes received by the browser



Vi



vii) here there are multiple objects from same websites the objects can be images, videos or any files in any format. Here this is a “SERIES”

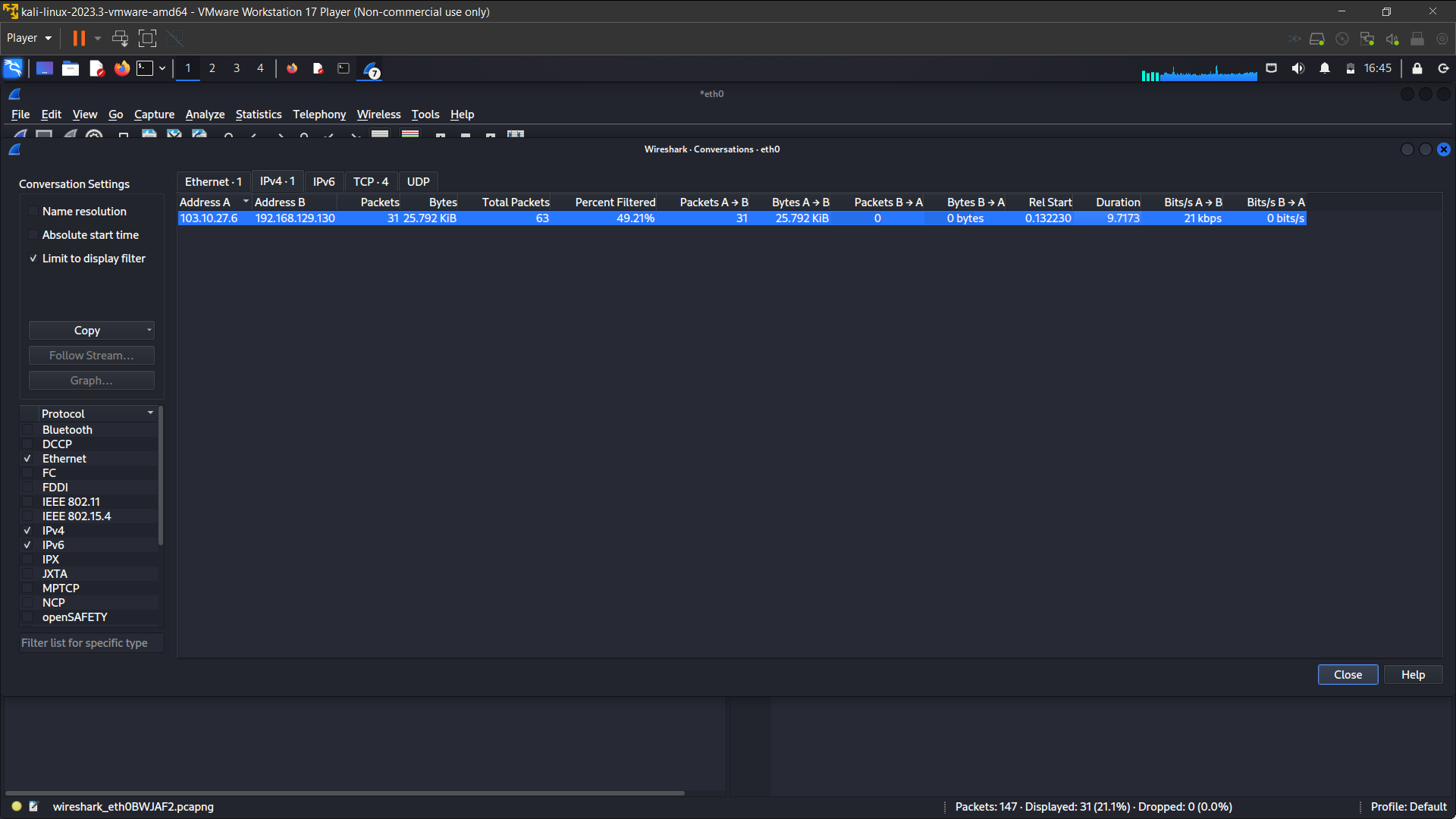
viii)

This is the server response for the http GET-MESSAGE



4)

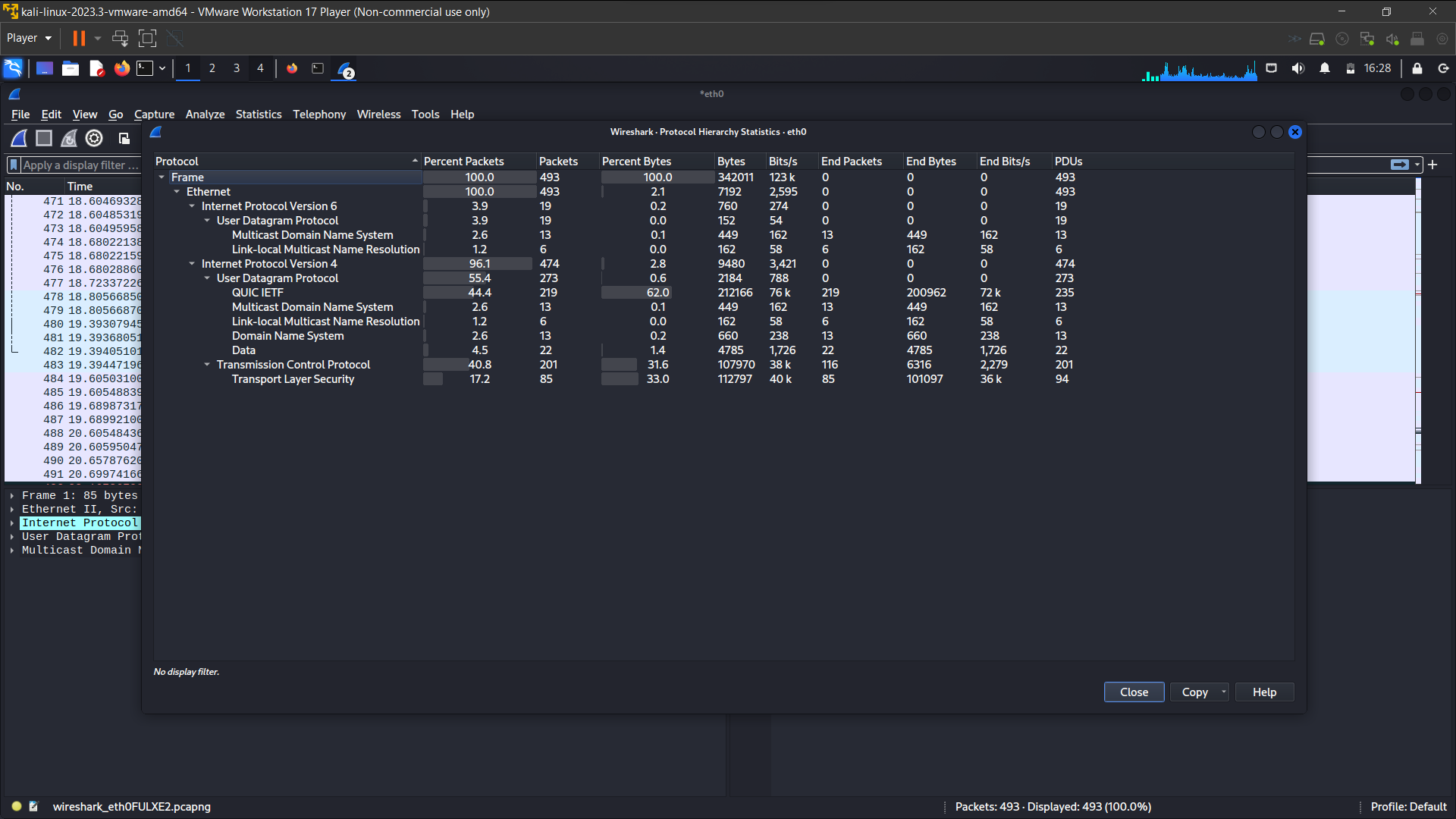
Here on connecting to AUMS and downloading a file, we took aums server IP: 103.10.27.6 and host ip: 192.168.129.130 and downloaded a file after clearing the cache in the browser.



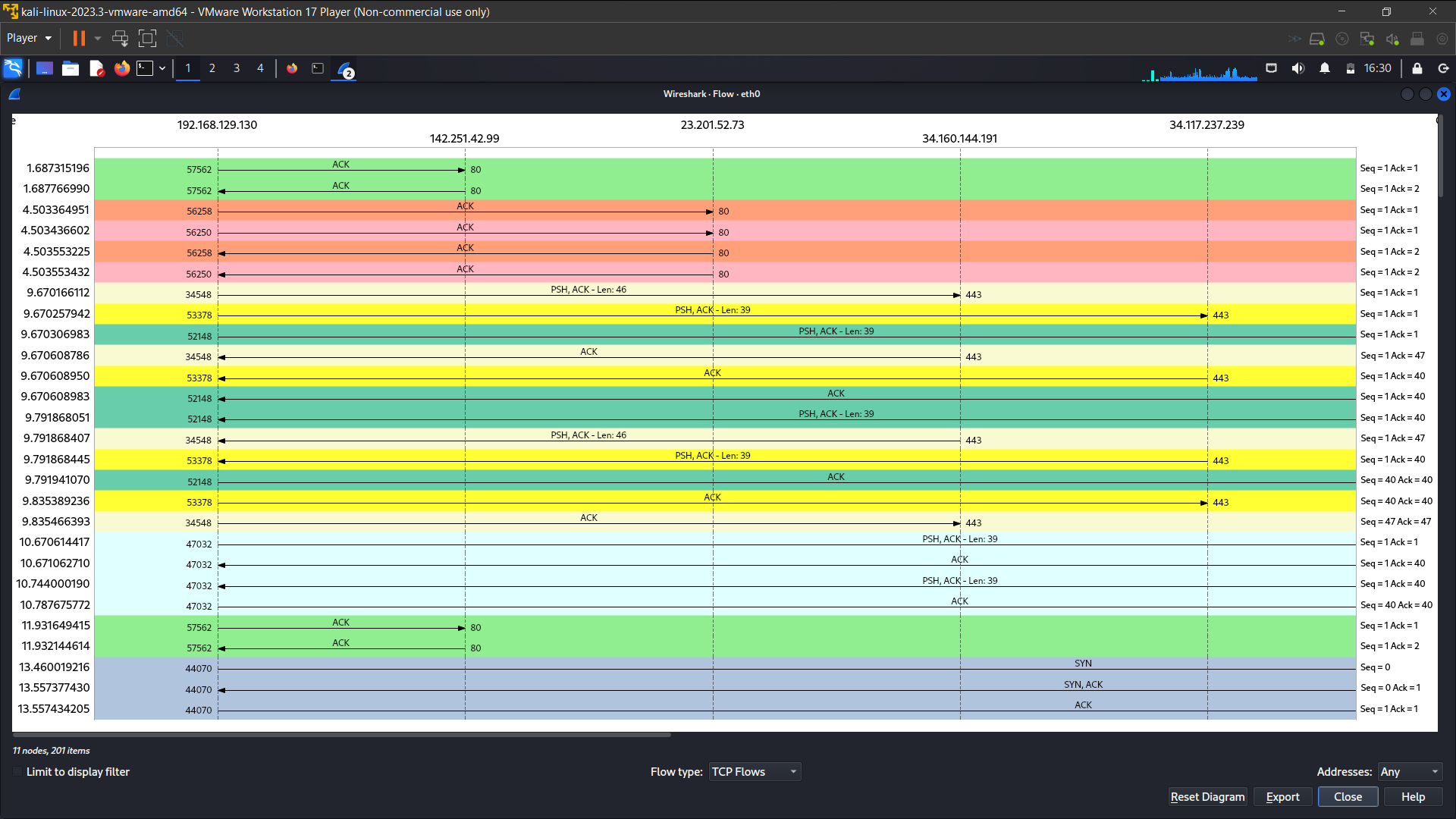
5)

Here we took many websites in getting the packet captures, so we took a gif download and sites and here is the protocol hierarchy and flow graphs of the download file and other sites

Protocol hierarchy

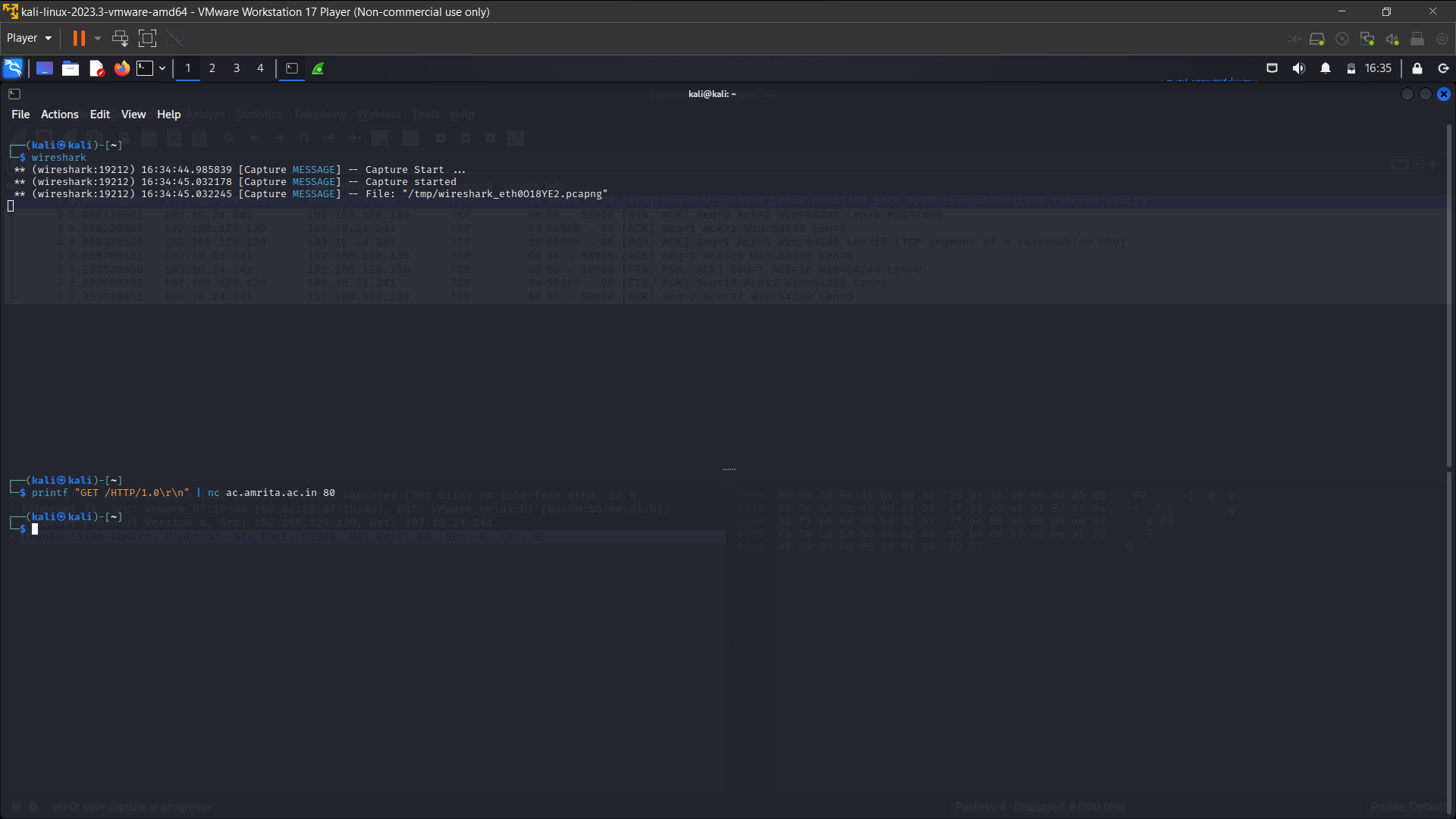


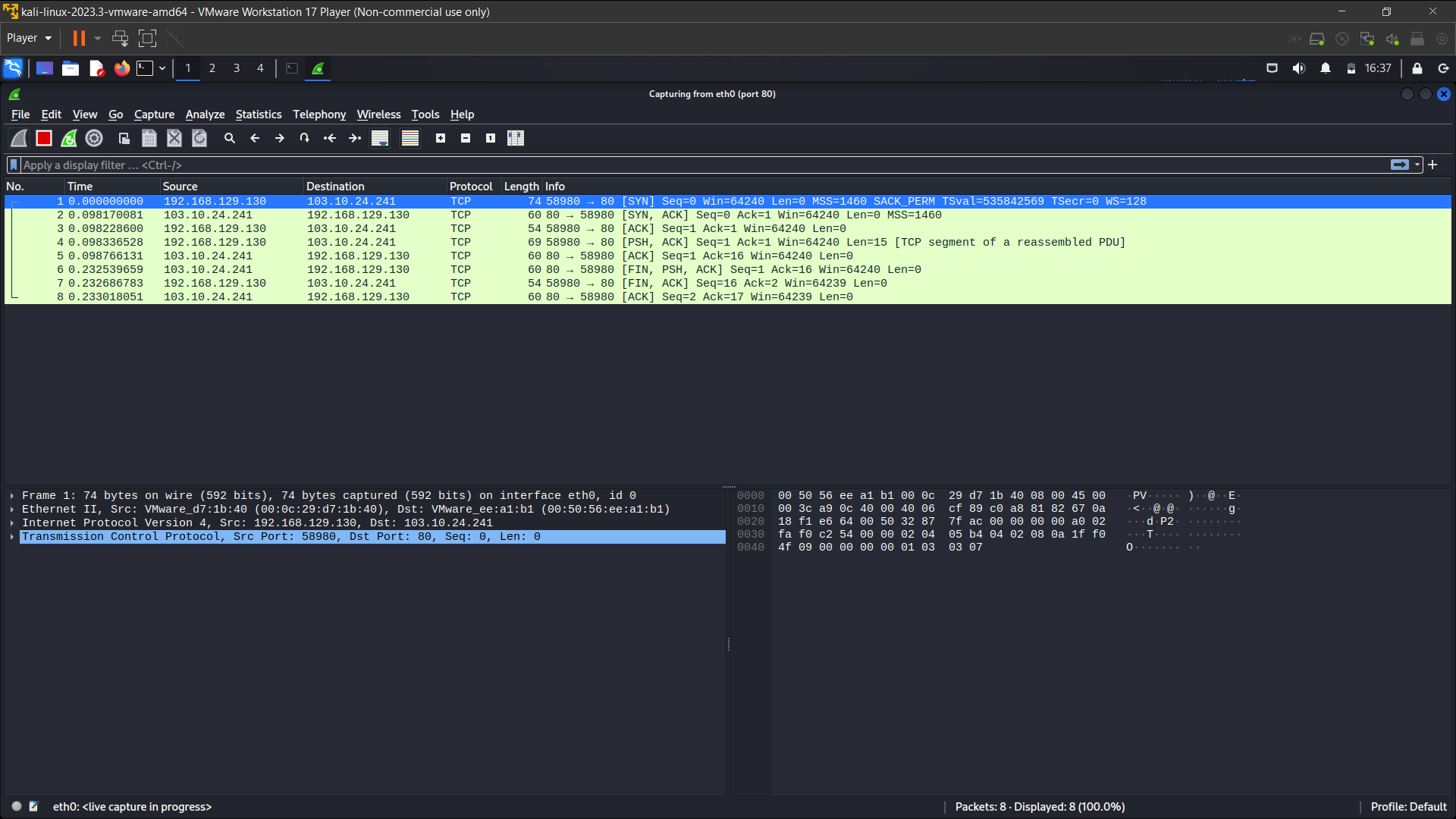
Flow graphs



6)

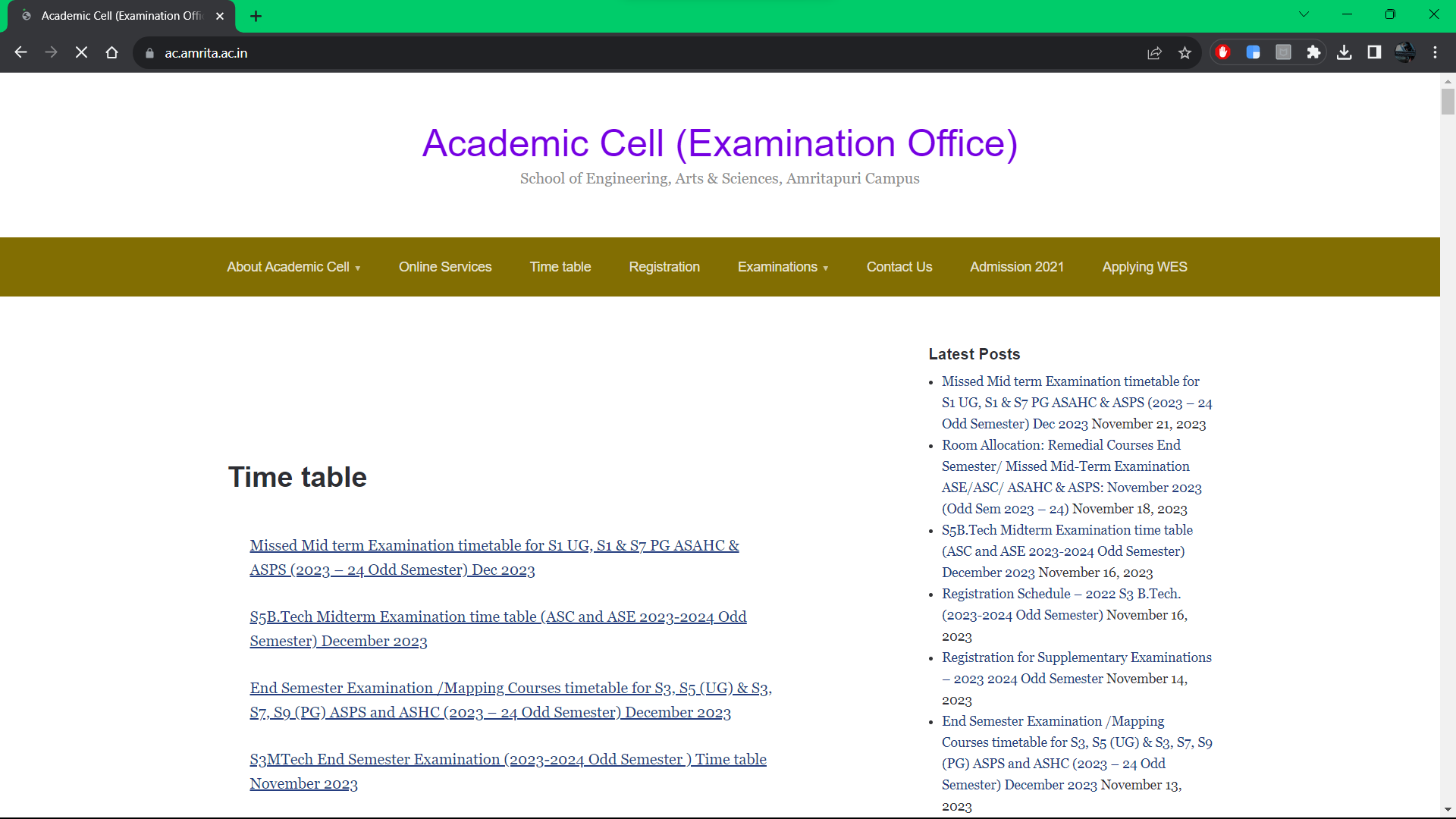
As the cache is cleared again to set the new capture, we are using kali again to run the NC (netcat) command and then as we are running wireshark and display filter (port 80) and after the capture begins..



****

7)

a.



b. on refreshing the page



c. on stopping the wireshark and display filter == “**http**”

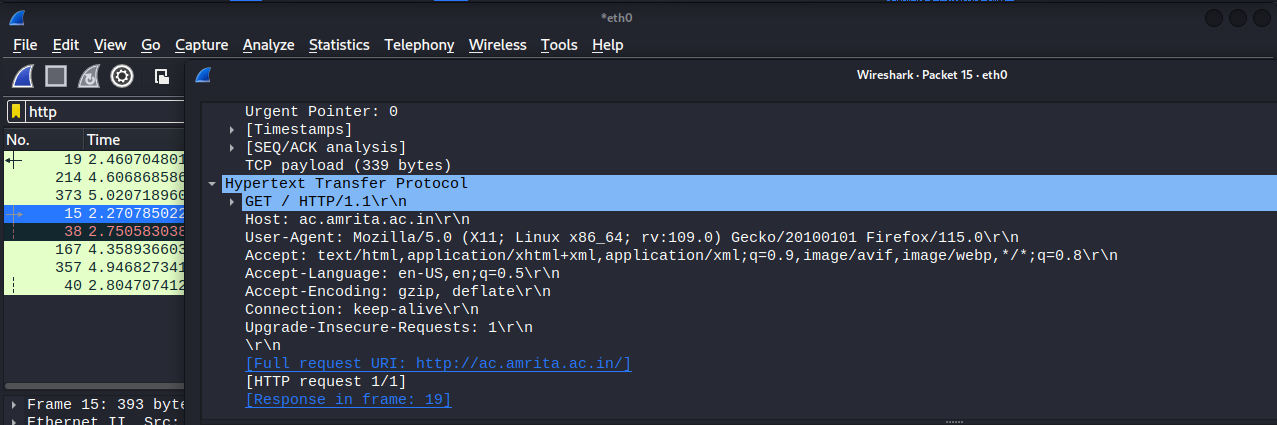
**for the purpose of clearing of cache we are using VIRTUAL MACHINE “KALI” to solve this packet sniffing exercise**



7d)

There is only one GET request even on multiple times of refresh cause the cache is getting stored on the first request itself

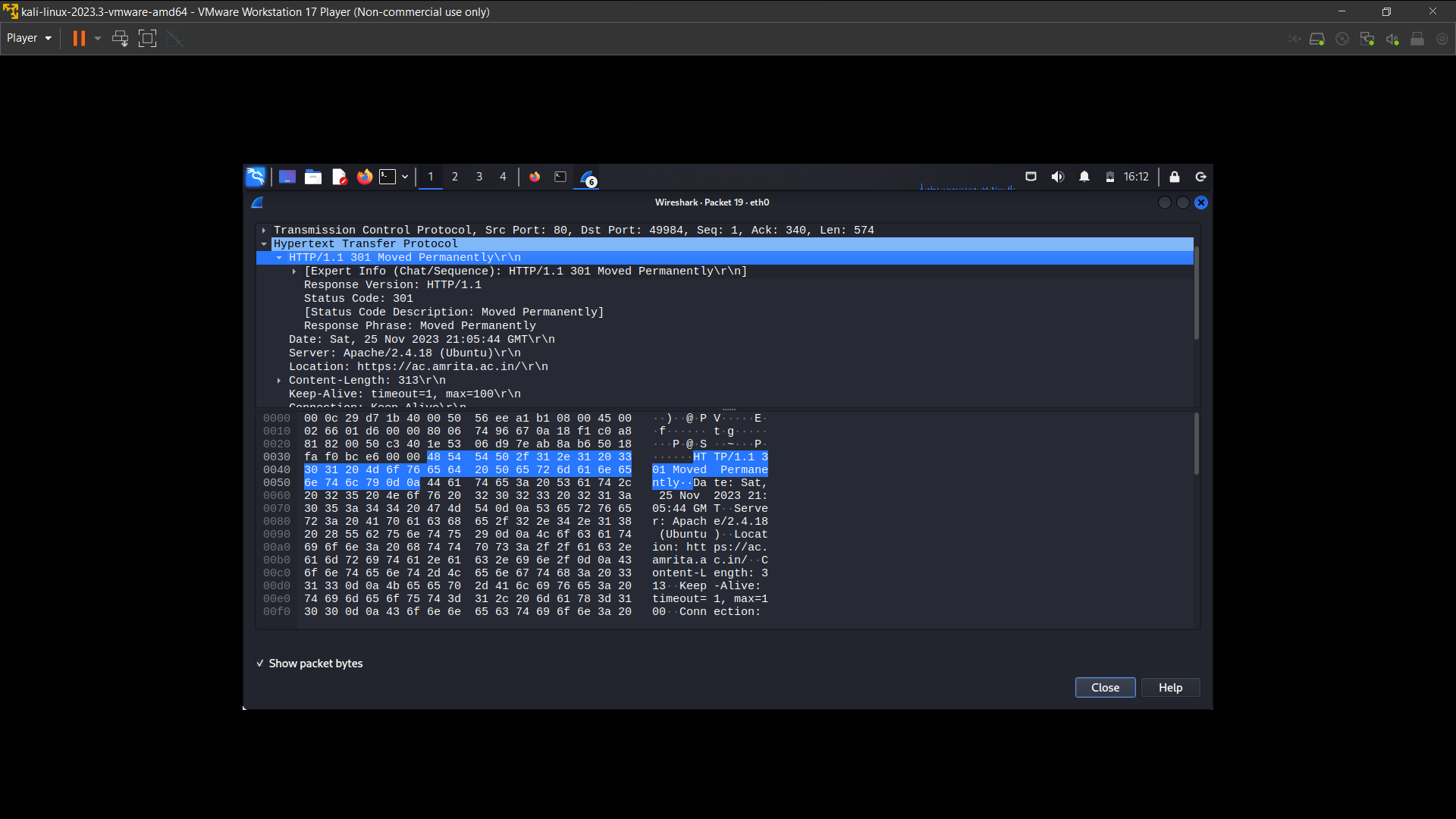
1. There is no IF-MODIFIED SINCE in this capture



2. No, there is no contents from the server received.

3. There is no second http-get REQUEST in this capture.

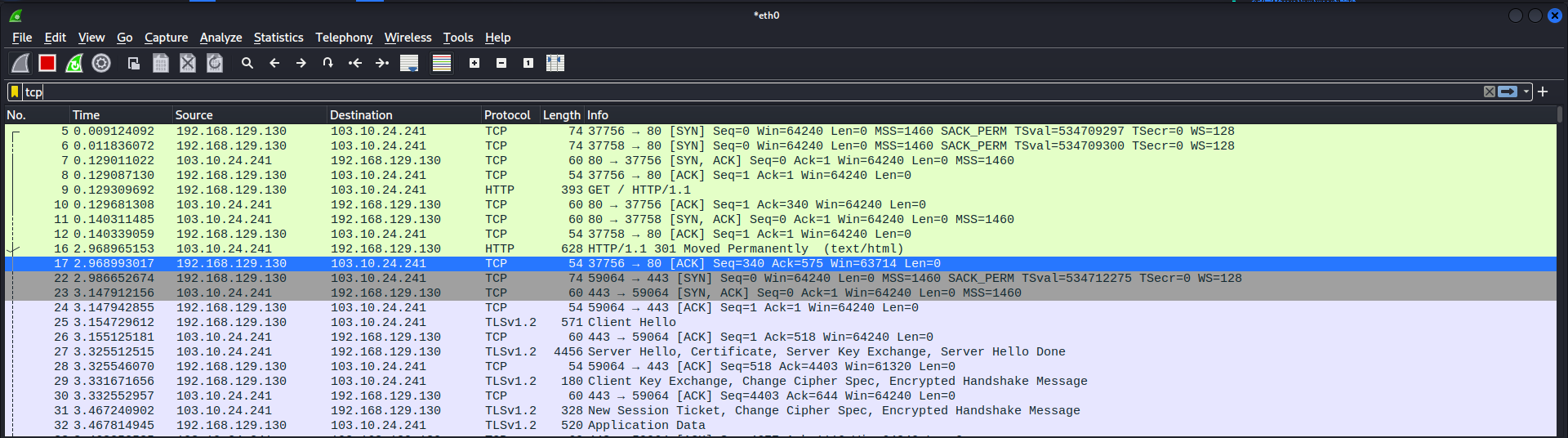
4. There is no second http GET request in this case, here in this http the status code is “**MOVED PERMANENTLY**”, Which means this is used for permanent redirecting, meaning that links or records returning this response should be updated. And the new URL should be provided in the Location field, included with the response.



5. here there is only one GET request in the capture.



6. here there Is a HTTP after a 3-way handshake of TCP (“**SYN SYN-ACK ACK**”)



7. 301 moved permanently

