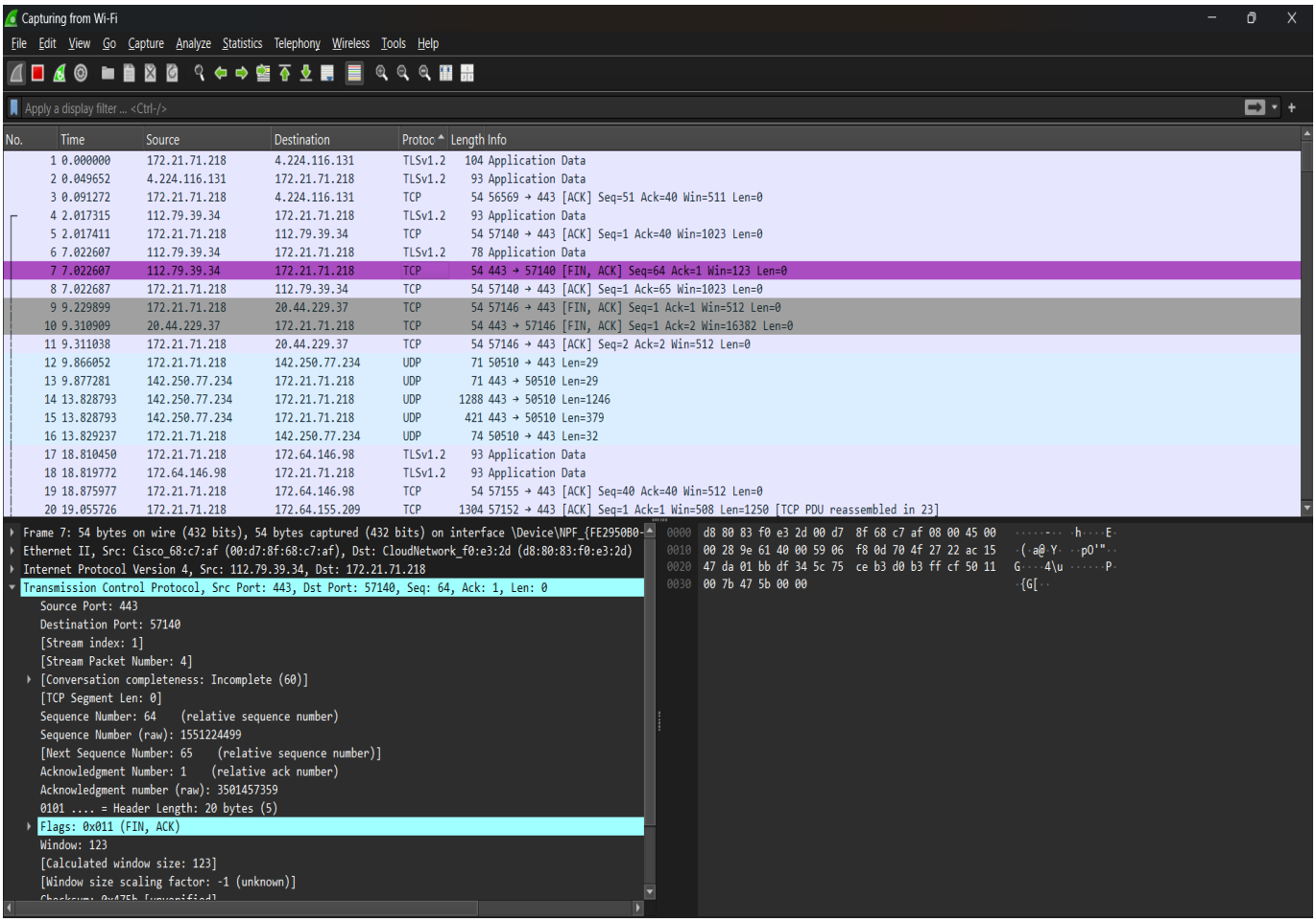
CS304- LAB ASSIGNMENT

Name: Palla Santhoshi Shalini

Roll.No: 2022csb1100

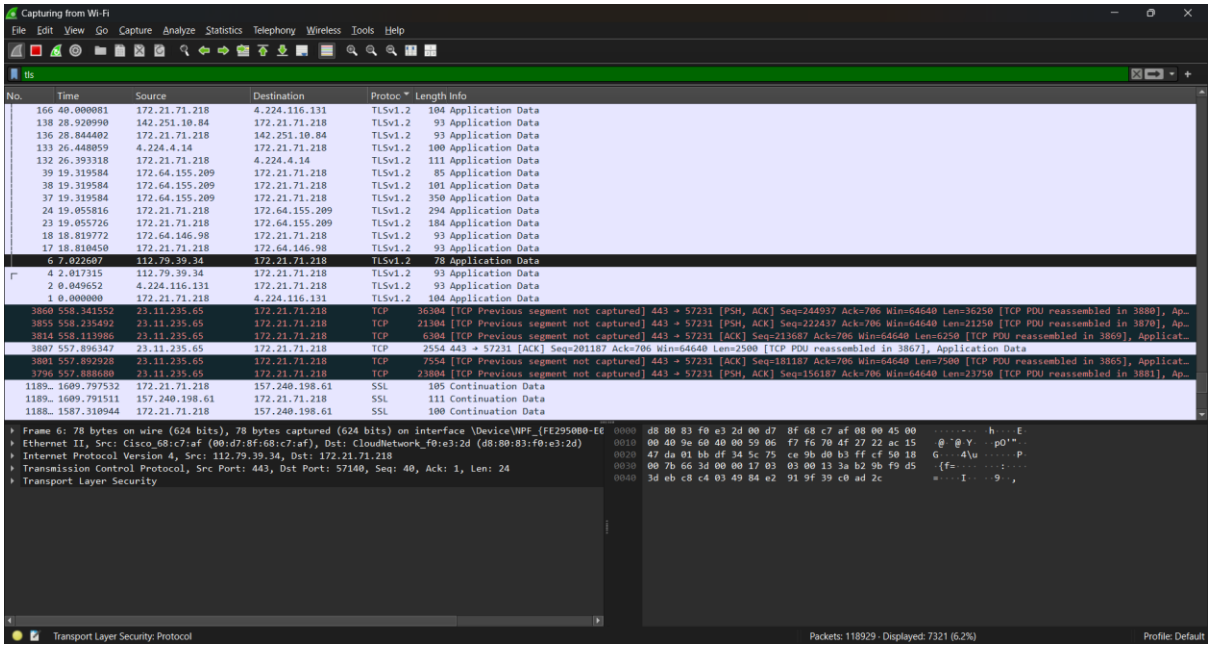
Instructor: Basant Subba

1) List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window. Take screenshots of all the 10 protocols using appropriate filters.(4 marks)

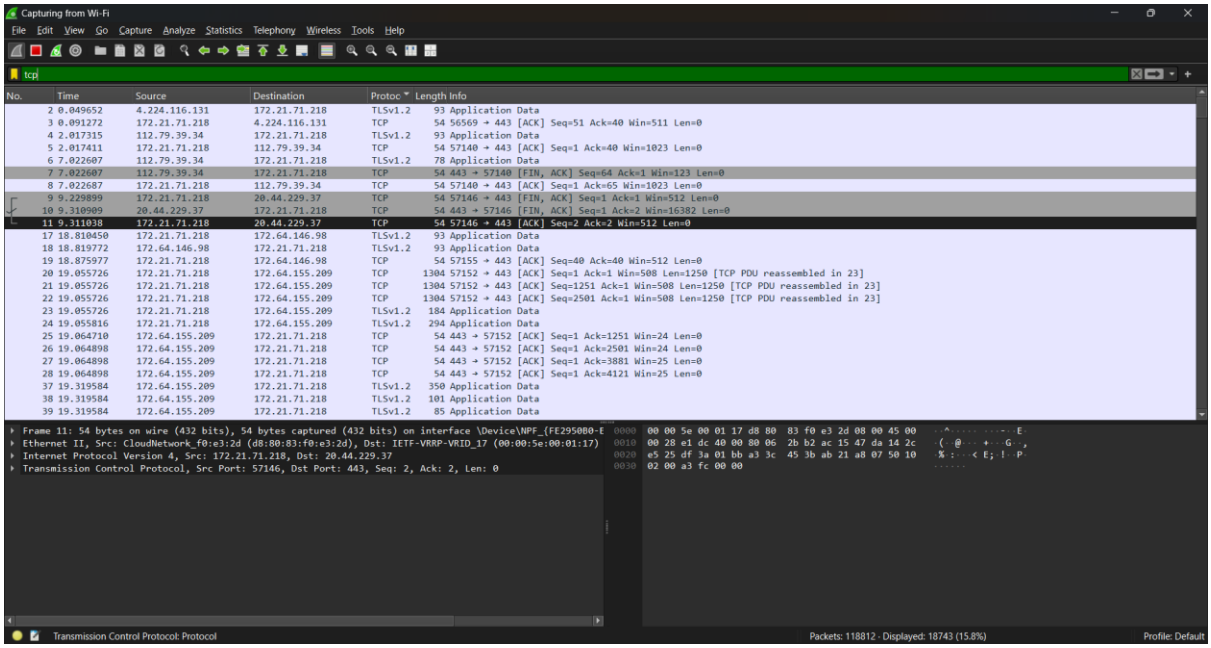


Identified Protocols in Wireshark Capture:

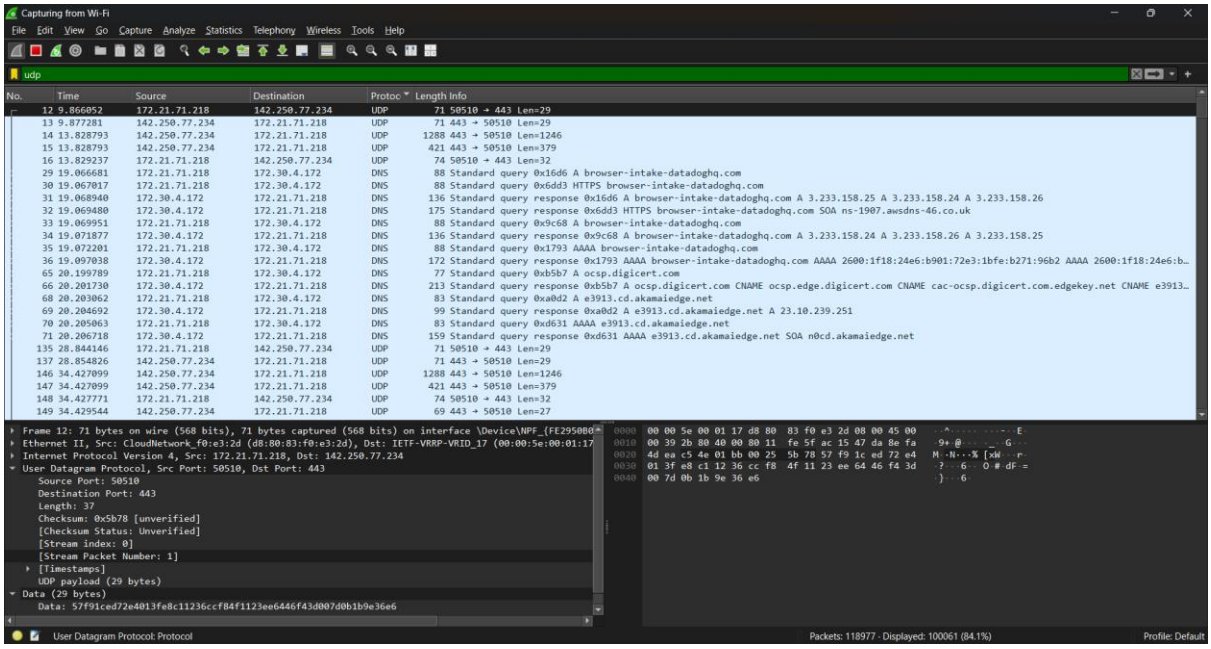
1. **TLSv1.2 (Transport Layer Security 1.2)** – Used for encrypting communication over HTTPS.



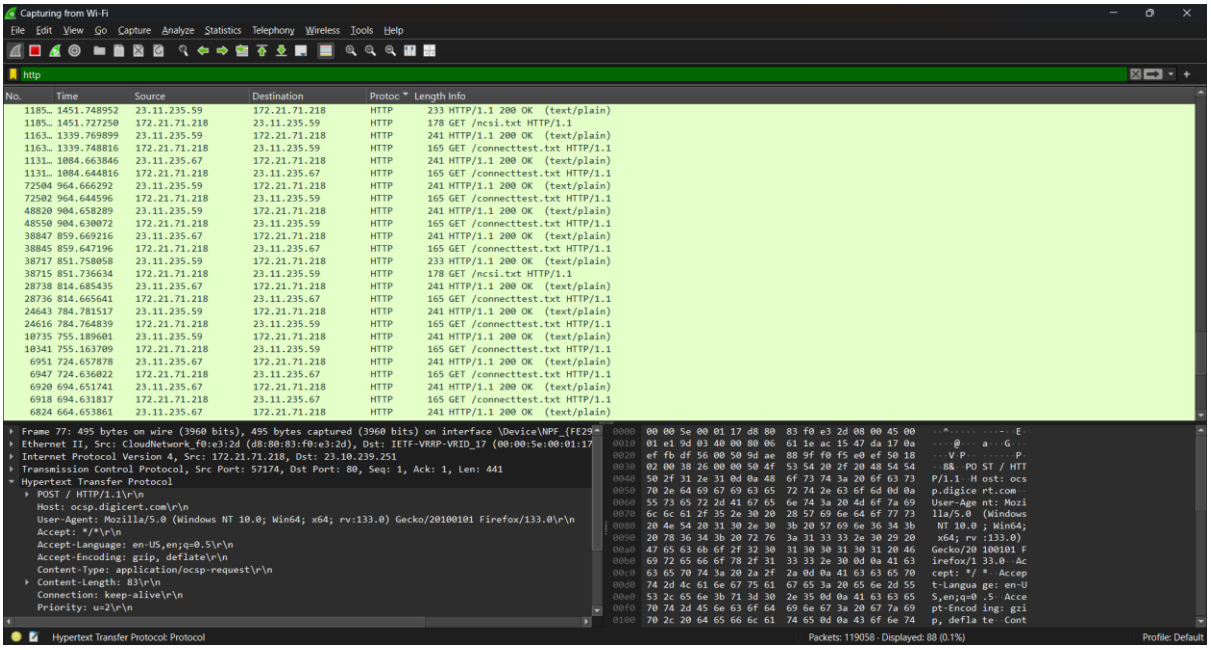
2. **TCP (Transmission Control Protocol)** – Ensures reliable communication between devices.



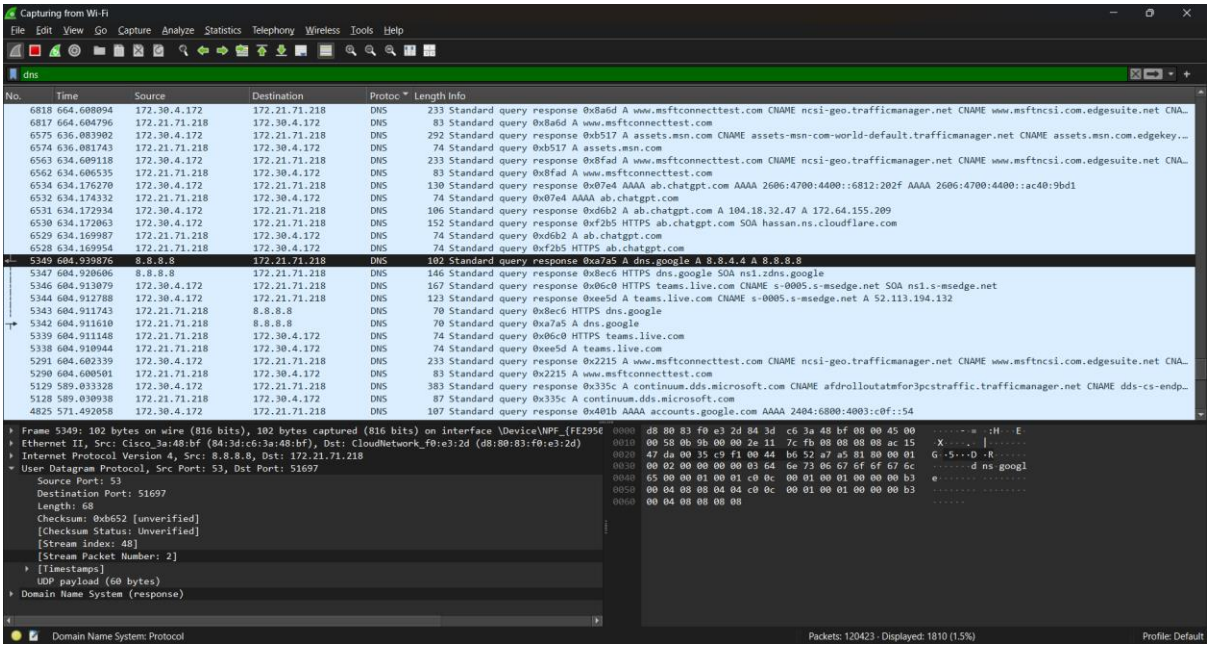
3. **UDP (User Datagram Protocol)** – A connectionless protocol used for fast data transfer.



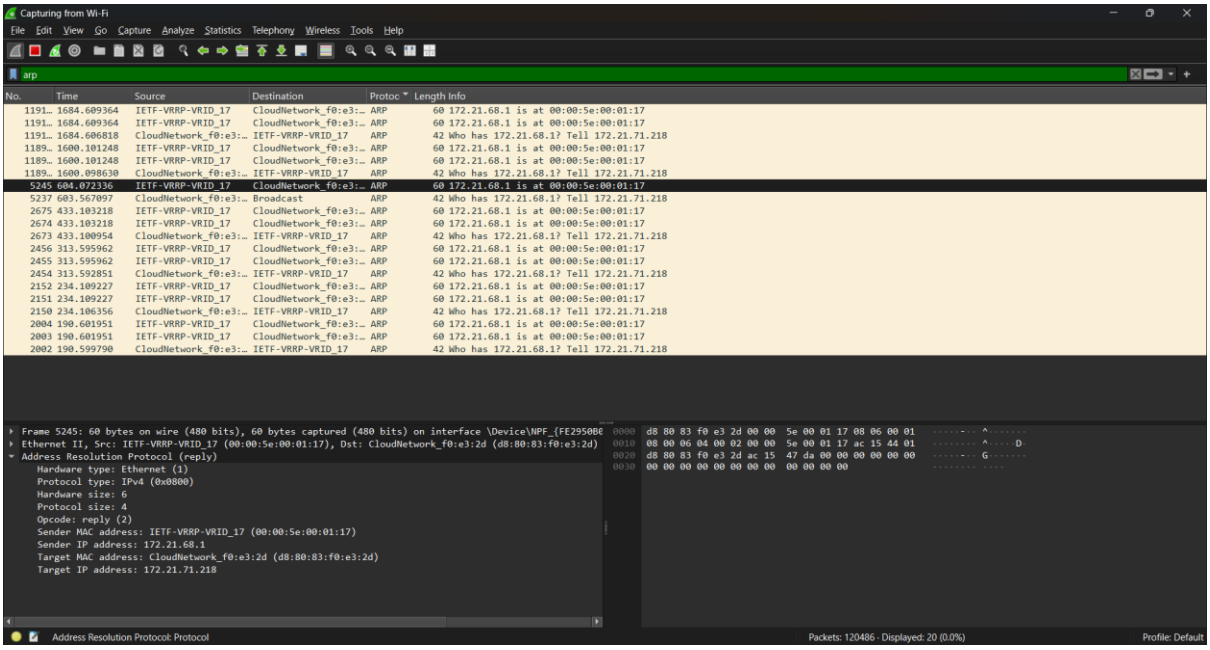
4. **HTTP (Hypertext Transfer Protocol)** – Used for web page communication (not seen in the screenshot, but should be captured).



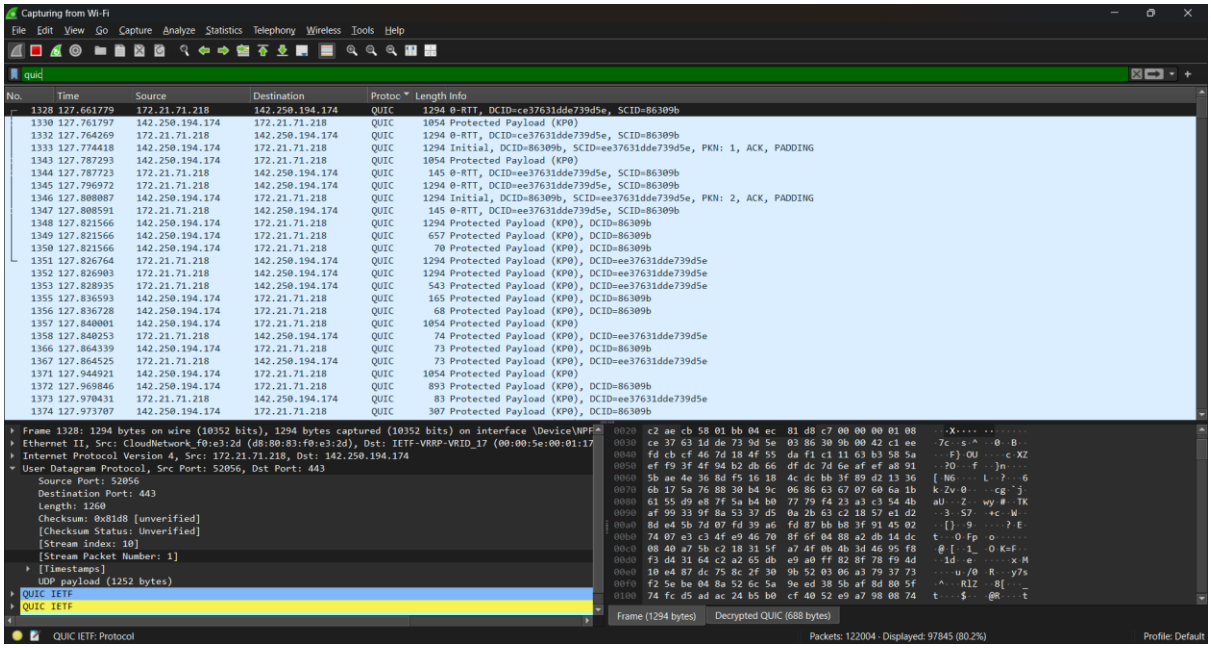
5. **DNS (Domain Name System)** – Resolves domain names to IP addresses.



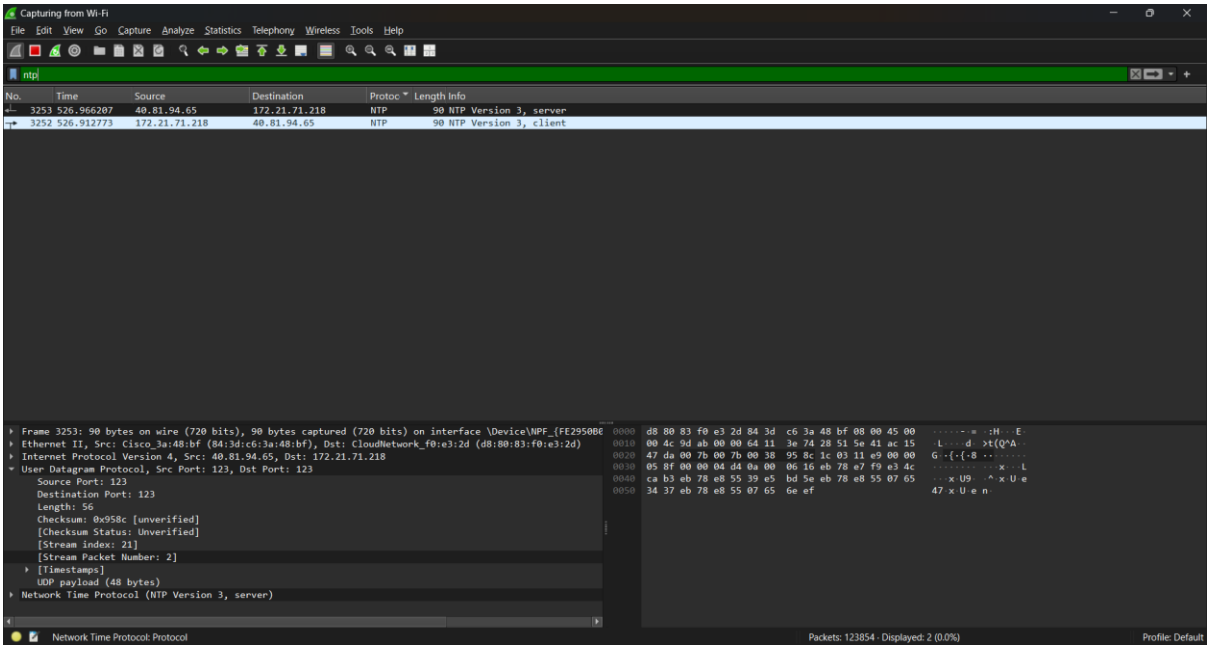
6. **ARP (Address Resolution Protocol)** – Maps IP addresses to MAC addresses.



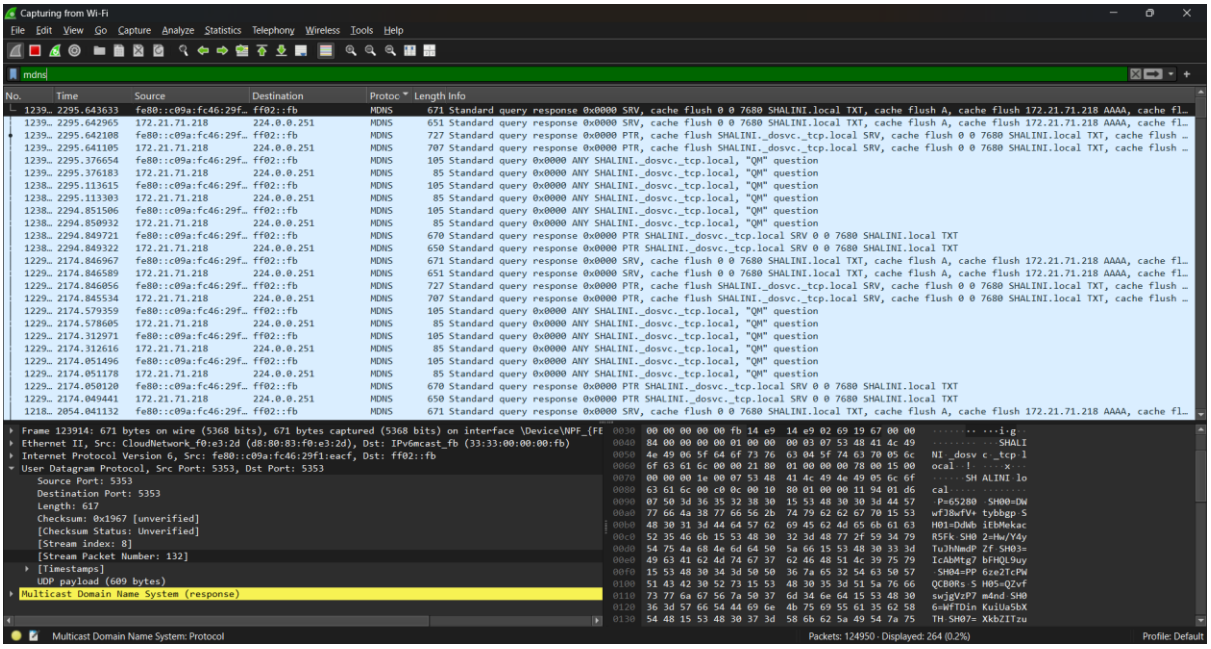
7. **QUIC : (Quick UDP Internet Connections, an alternative to TCP for faster web browsing)**



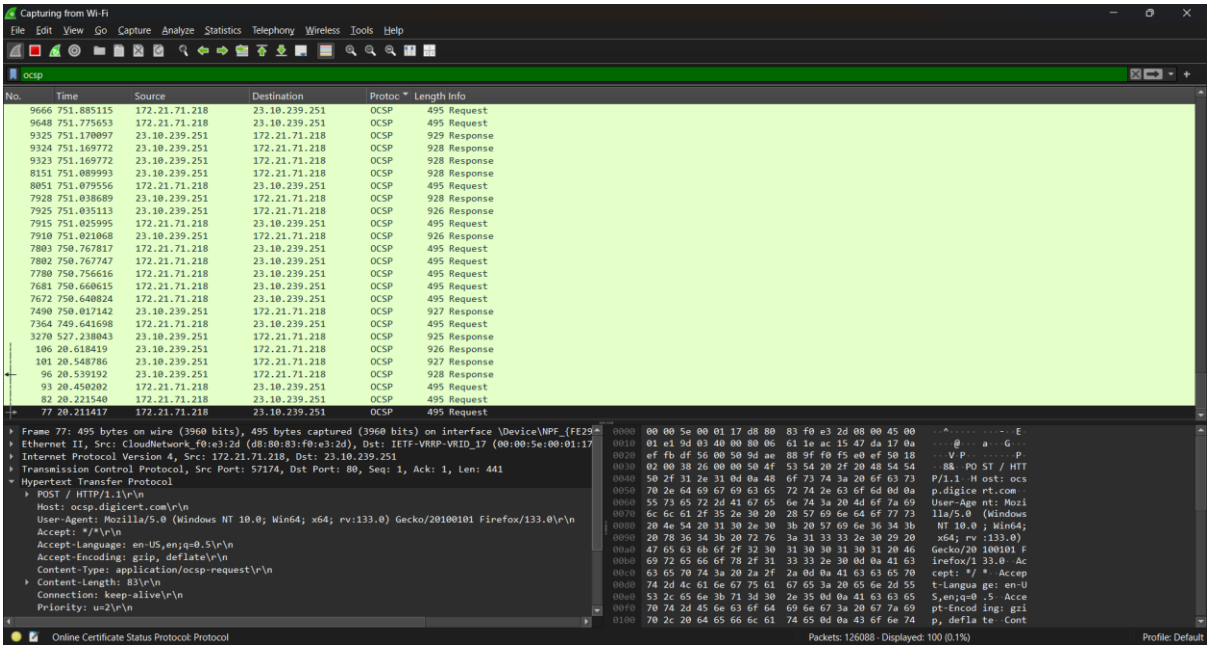
8.NTP: Used to synchronize the time between systems.



9.MDNS: (Multicast DNS) MDNS is used by devices to discover each other on local networks without a central DNS server.

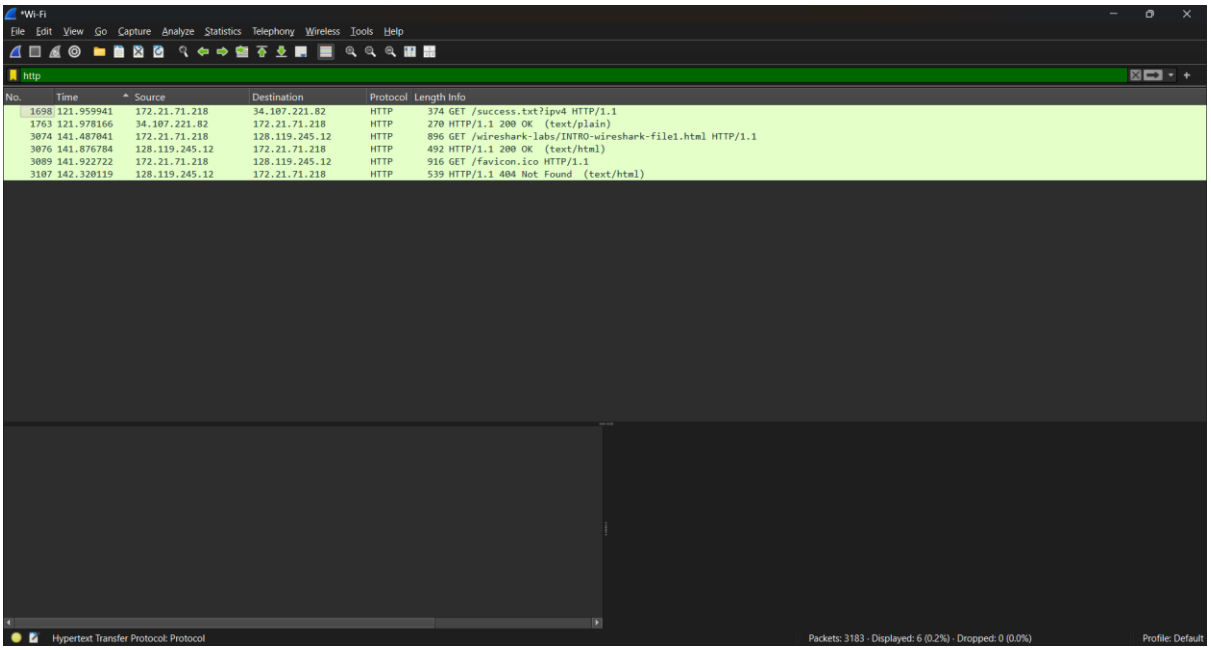


10. OCSP (Online Certificate Status Protocol): OCSP is a protocol used to **check the revocation status of SSL/TLS certificates** in real-time.



2) While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html, and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages will be captured by Wireshark. After your browser has displayed the INTRO-wireshark-file1.html page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. Type in "http" (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered "http"). This will cause only HTTP message to be displayed in the packet-listing window. How

long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? Include a screenshot and describe where you got the data to answer this question. (4 marks)



From the captured packets in Wireshark:

1. **GET Request (Packet No. 1698)**
    - Time: **121.959941**
    - Source: **172.21.71.218**
    - Destination: **34.107.221.82**
    - Info: **GET /success.txt?ipv4 HTTP/1.1**
2. **HTTP 200 OK Response (Packet No. 1763)**
    - Time: **121.978166**
    - Source: **34.107.221.82**
    - Destination: **172.21.71.218**
    - Info: **HTTP/1.1 200 OK (text/plain)**

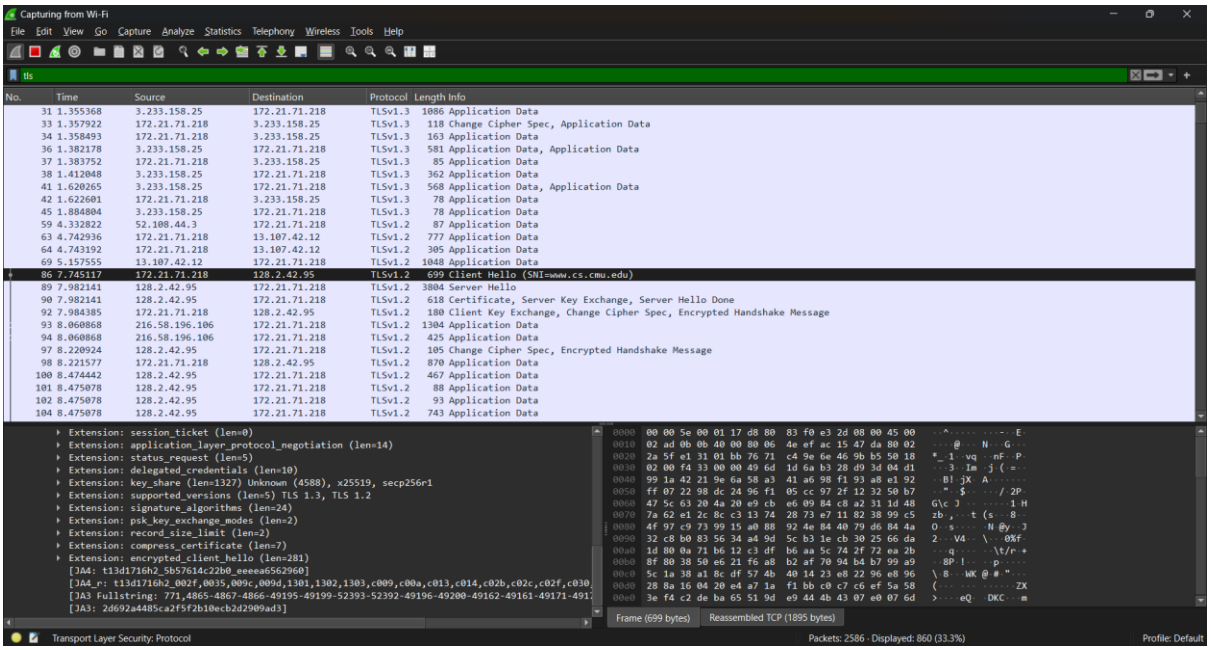
Calculation:

Time difference = **121.978166 - 121.959941**
= **0.018225 seconds (or 18.225 milliseconds)**

So, the response time for the HTTP request was **18.225 milliseconds**.

3) During the packet capturing session, open the www.cs.cmu.edu URL in the browser. What is the Internet address (IP address) of www.cs.cmu.edu? What is the Internet address of your computer (This

might be a private address, if you are behind a NAT device.)? Include a screenshot and describe where you got the data to answer this question. (4 marks)



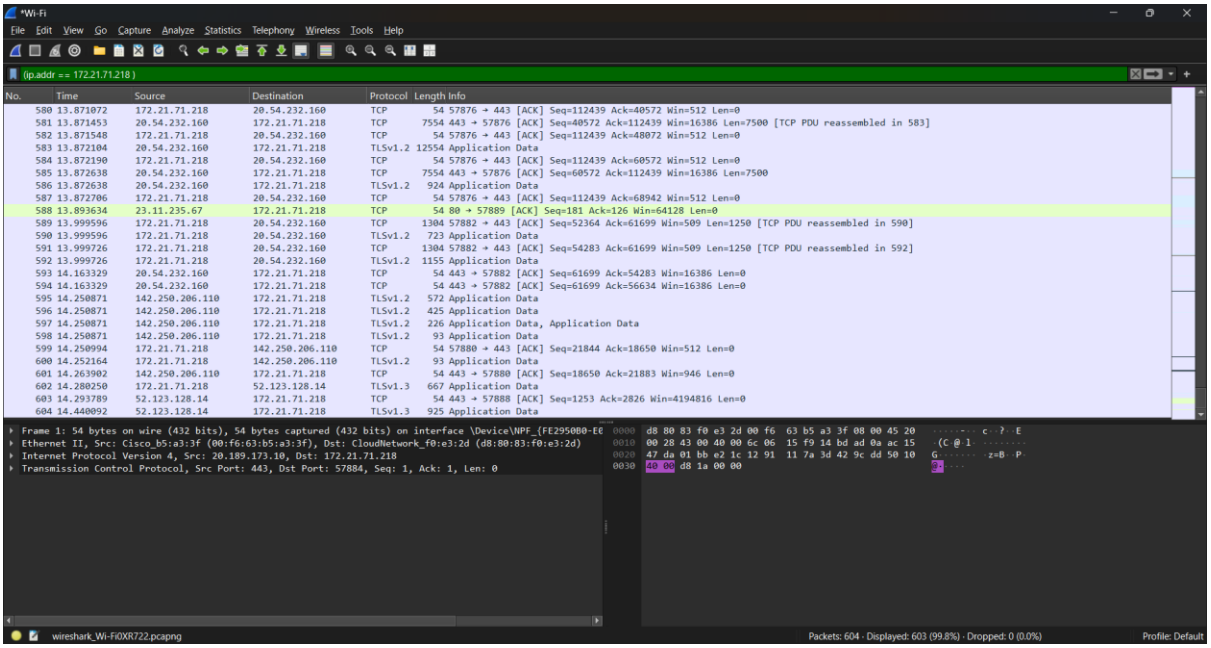
The screenshot provided clearly shows:

- The TLS handshake (Client Hello) request to www.cs.cmu.edu.
- The Destination column contains the IP address of www.cs.cmu.edu (128.2.42.42).
- The Source column contains your computer's IP address (172.21.71.218).

1. Finding the Internet Address (IP Address) of www.cs.cmu.edu.In the Destination column, there is an IP address (e.g., 128.2.42.33) associated with the website www.cs.cmu.edu.This IP address was retrieved when the browser accessed the website, likely through a DNS resolution request. The Protocol used includes **TLSv1.2**, indicating encrypted communication.

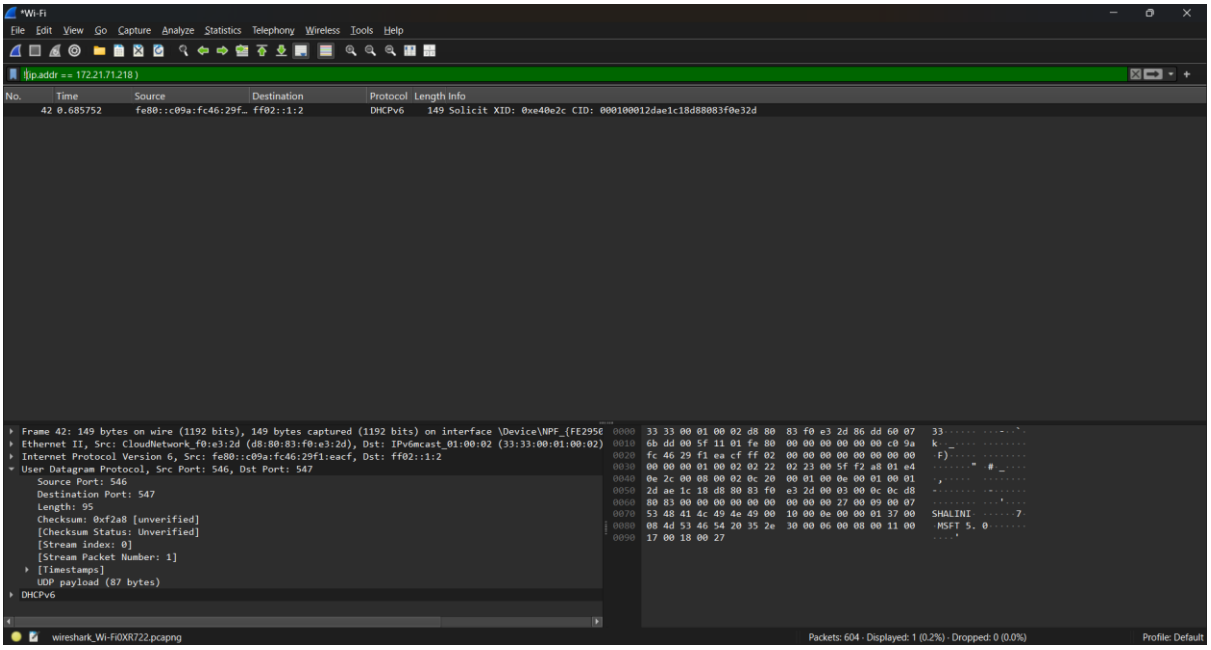
2. Finding the IP Address of the User's Computer. In the Source column, there is a private IP address (e.g., 172.21.32.203).This is the local IP of the user's computer, assigned by the internal network (likely behind a NAT device).This address appears in multiple packets, meaning it initiated the communication with www.cs.cmu.edu.The source and destination IPs were identified from the Wireshark packet list pane (top section).The packet details pane (middle section) provides information about protocols such as TLS. The hexadecimal pane (bottom section) shows raw packet data. The screenshot captures network packets exchanged while accessing www.cs.cmu.edu, displaying the IP addresses involved.

4) How many packets did you capture (total of all protocols, not just HTTP)? Now, use display filters to determine how many packets contain your IP address. What is the filter you used? Now, reverse the filter to determine how many packets don't contain your IP address. What is the filter you used? Include a screenshot and describe where you got the data to answer this question (4 marks)



Packets containing IP address = 603 in 604 packets

Used filter: ip.addr == 172.21.71.218



Packets not used the IP address : 1 In 604 packets

Filter used: !(ip.addr == 172.21.71.218)