Assignment – 2

Name – Sayak Sen

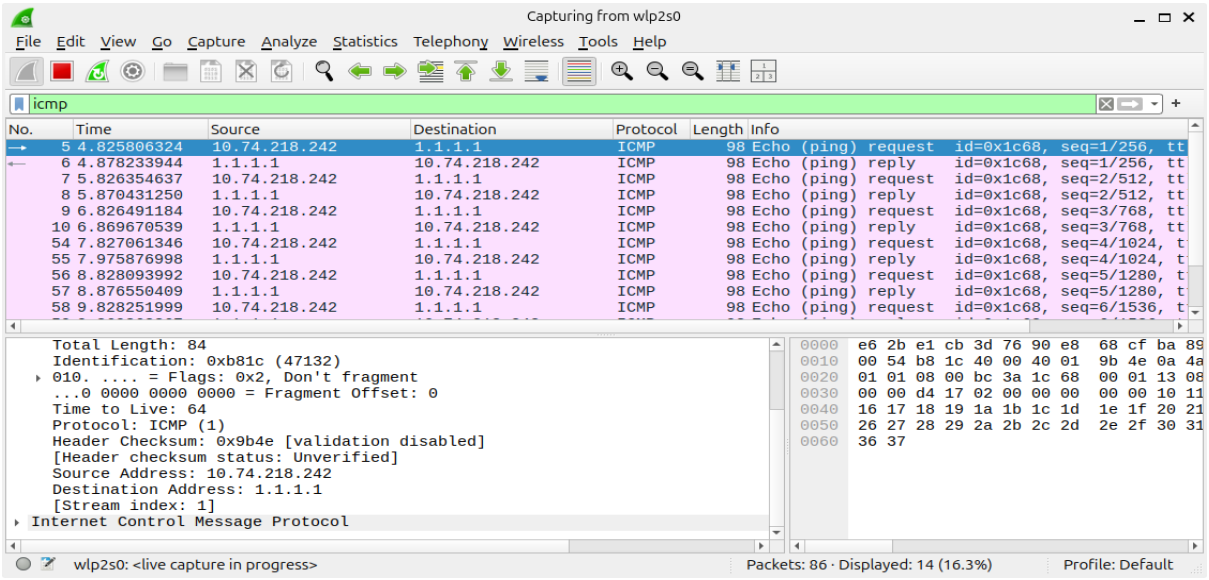
Enrollment No – 2023CSB047

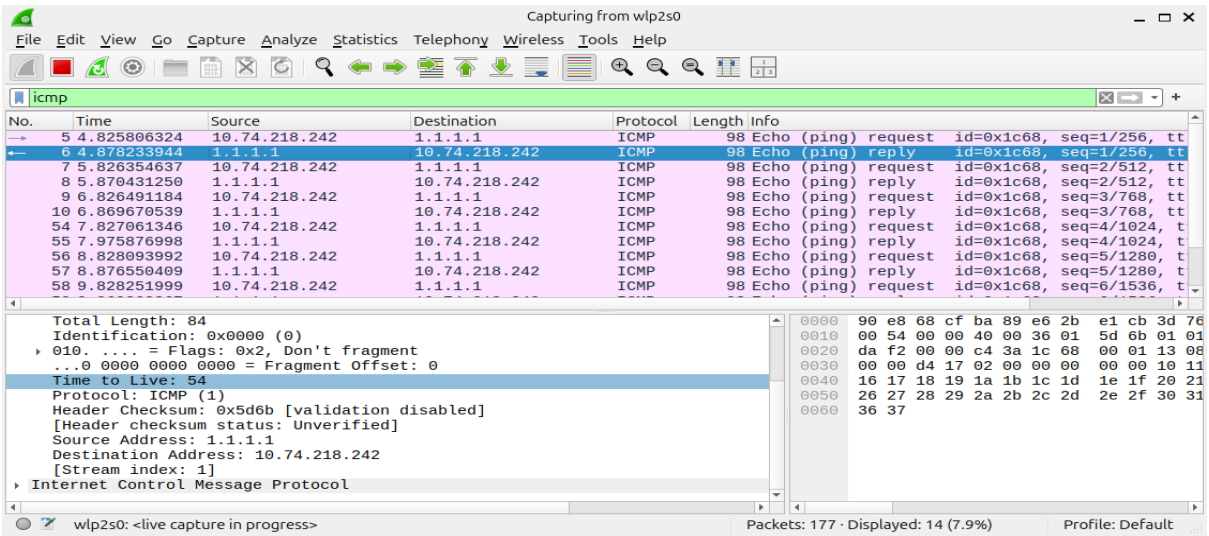
Subject – Computer Networks Lab

1. Analyse the packets (across all layers) exchanged with your computer while executing the

following commands: (i) ping (ii) traceroute (iii) dig (iv)arp (v)wget.

(i) ping





The ping command uses the **ICMP (Internet Control Message Protocol)** at the network layer.

In Wireshark, filtering with icmp shows two packets for each ping:

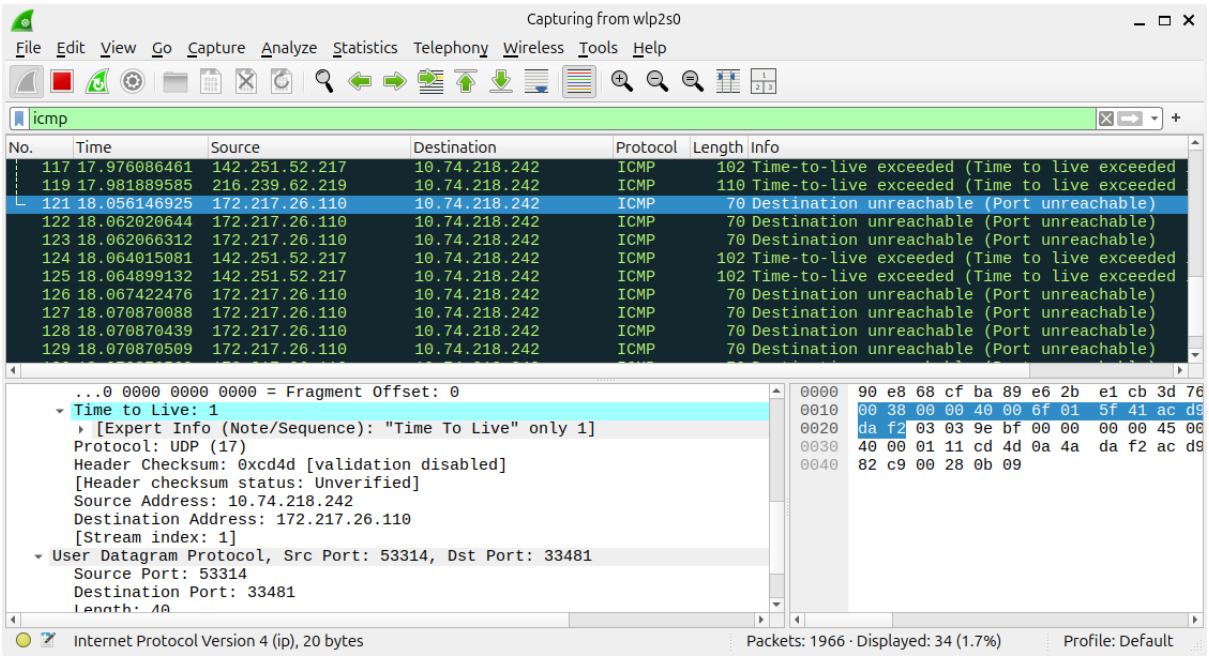
- **ICMP Echo Request (Type 8)** from the source to destination
- **ICMP Echo Reply (Type 0)** from destination back to source

Encapsulation observed:

- **Ethernet Layer:** Source and Destination MAC addresses
- **IP Layer:** Source IP (10.74.218.242) and Destination IP (1.1.1.1)
- **ICMP Layer:** Type, Code, Checksum, Sequence Number

This confirms ping checks connectivity and round-trip time without using TCP/UDP.

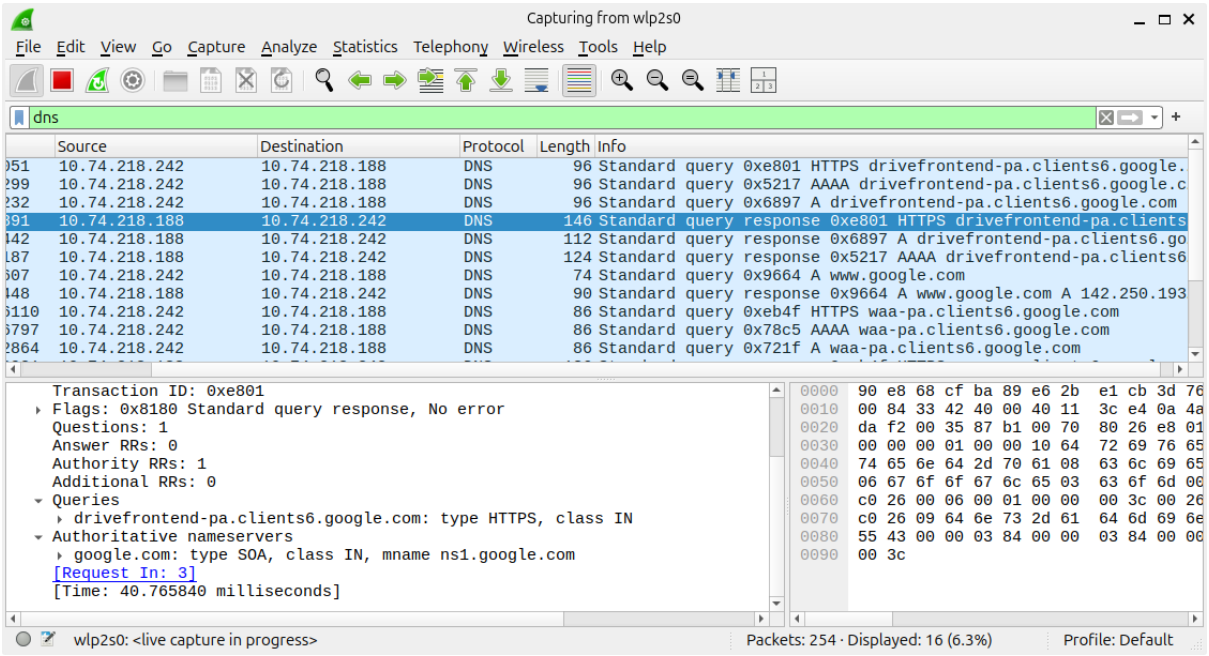
(ii) traceroute



Behavior seen:

- **Packets are sent with TTL = 1, 2, 3…**
- **Each router where TTL becomes 0 sends back ICMP Time Exceeded**
- **When the destination is reached, it sends ICMP Port Unreachable.Thus, traceroute reveals each router (hop) along the path to the destination.**

(iii) dig

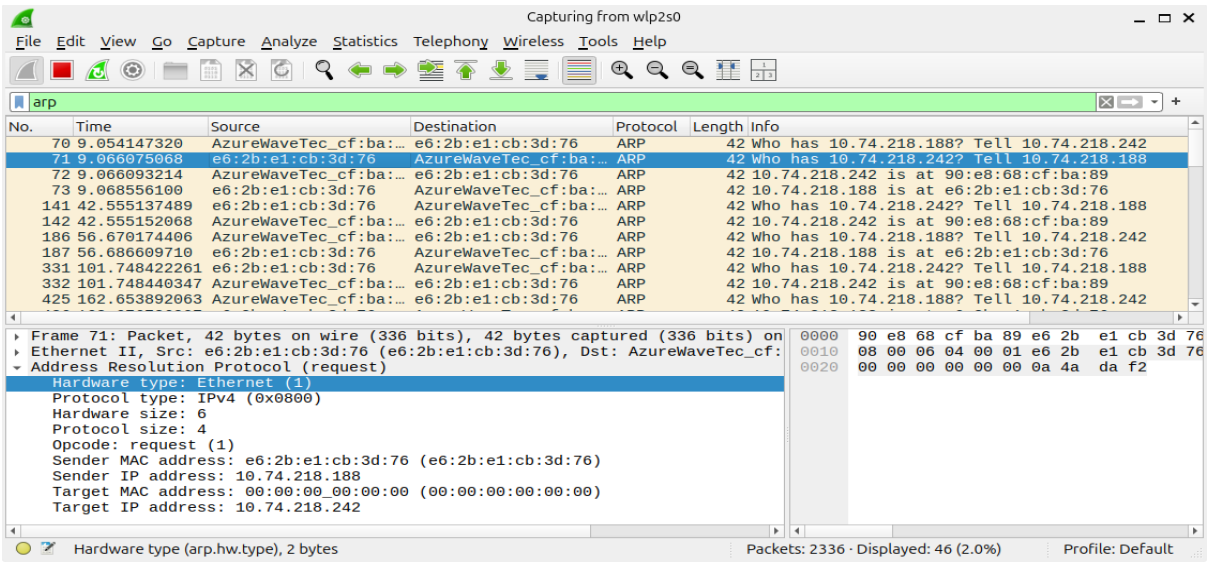


Observed:

- **DNS Query packet from my system to DNS server (UDP port 53)**
- **DNS Response packet containing the A record (IPv4 address)**

This shows how domain names are translated into IP addresses.

(iv) arp

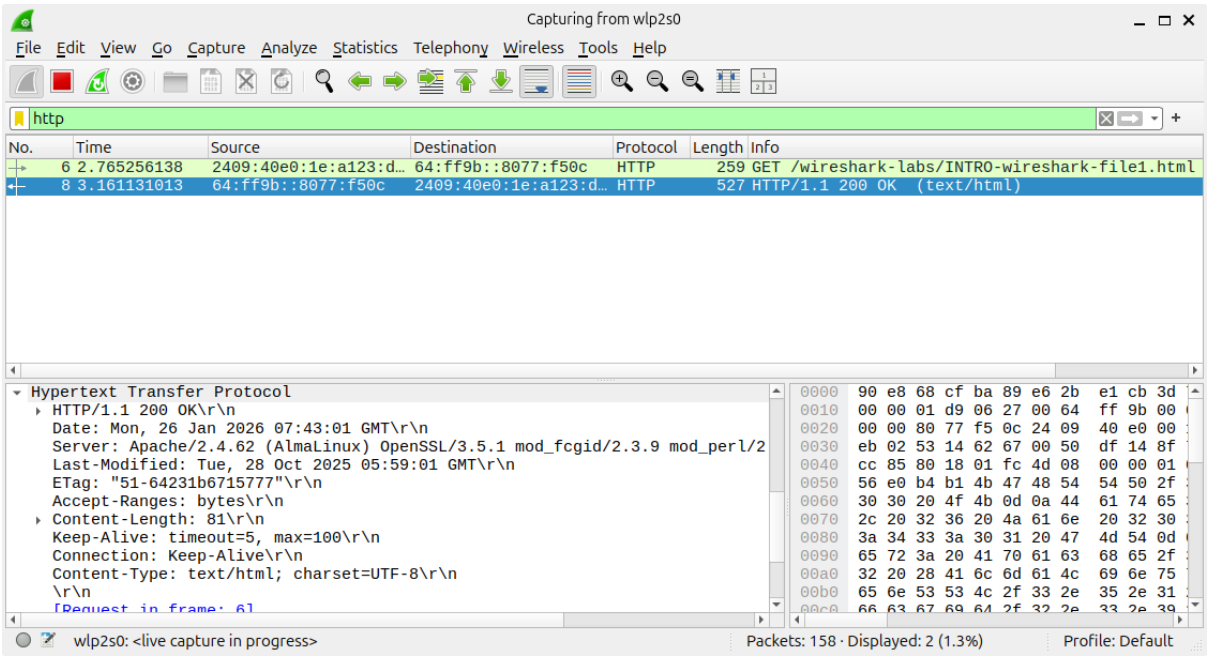


Observed:

- **ARP Request (Broadcast): "Who has <gateway IP>?"**
- **ARP Reply (Unicast): "<gateway IP> is at <MAC address>"**

This demonstrates that before sending packets outside the network the system must know the gateway's MAC address.

(v) wget

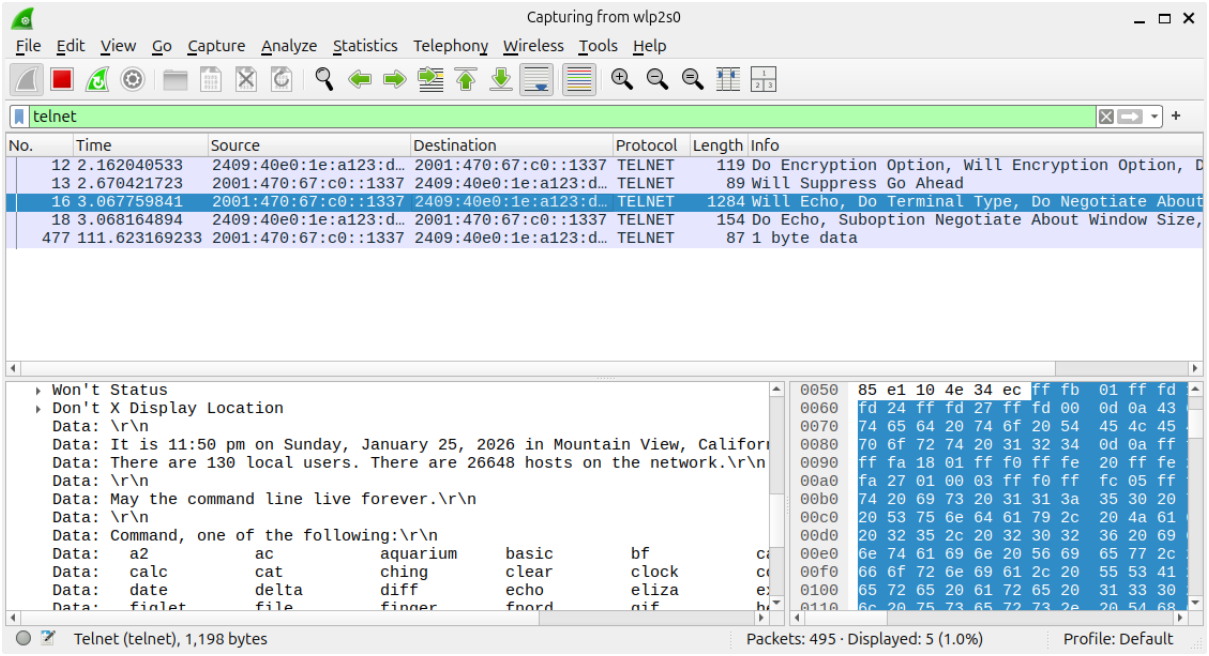


Process observed:

1. **TCP 3-way handshake**
2. **HTTP GET request sent to server**
3. **HTTP 200 OK response received**
4. **File data transferred**
5. **TCP connection closed**

The HTTP data is visible in plain text, showing headers and content.

2. Capture the packets while sending/receiving telnet request/response between your computer and a custom server running the telnet daemon. What is your observation while analysing the application layer data?



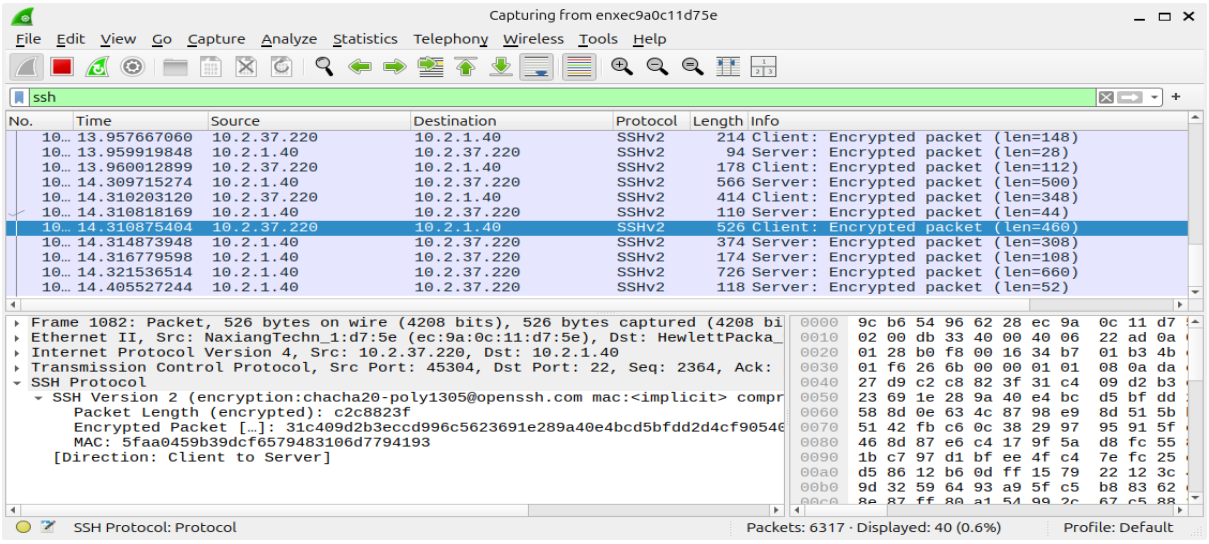
Telnet uses TCP port 23 and does not encrypt data.

In Wireshark:

- **Filter: telnet or tcp.port == 23**
- **Application layer data is fully visible**
- **Username, password, and typed commands can be read in plain text**

Observation: Telnet is insecure because data is transmitted without encryption.

3. Capture the packets while sending/receiving sshrequest/response between your computer and one of the department servers. What is your observation while analysing the application layer data?



SSH uses TCP port 22 and provides encrypted communication.

Observed:

- **SSH handshake packets**
- **All application data appears as encrypted payload**
- **No readable usernames or commands**

Observation: Unlike Telnet, SSH secures data using encryption.

4. Enter the URL:http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html andcapture packets using Wireshark. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture.

Answer the following from the captured packets:

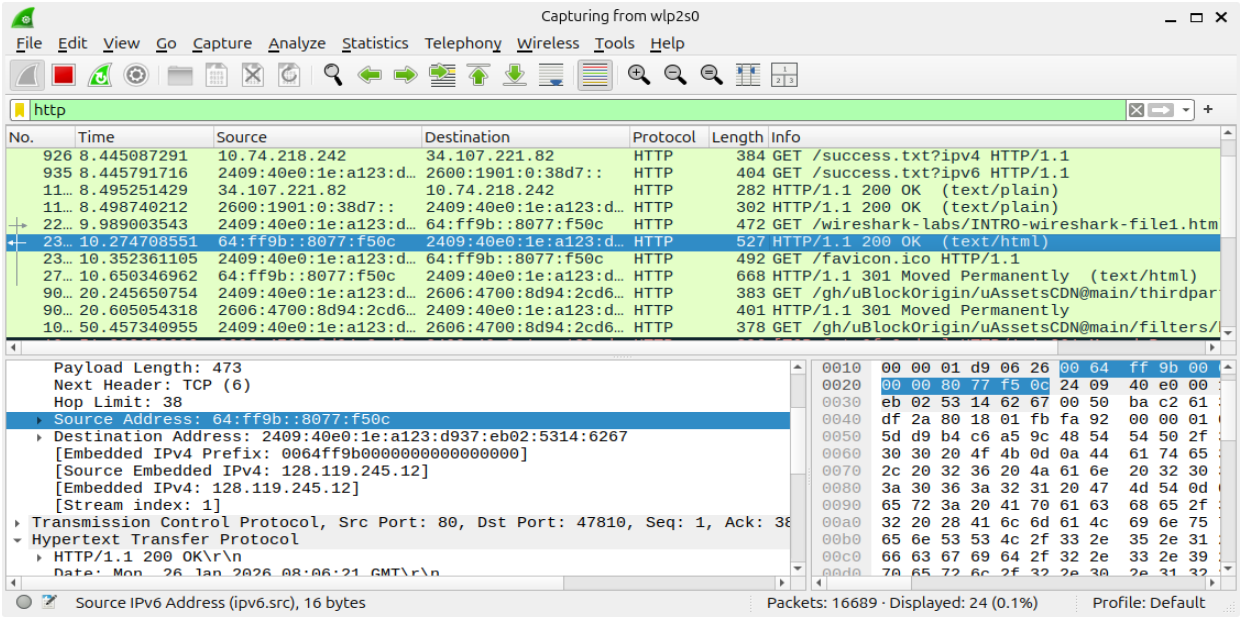
a. How long did it take from when the HTTP GET message was sent until the

HTTP OK reply was received?

b. What is the Internet address of the gaia.cs.umass.edu? What is the Internet

address of your computer? Support your answer with an appropriate screenshot

from your computer.



(a) Time between HTTP GET and HTTP OK

By comparing timestamps:

- **Time when HTTP GET was sent**
- **Time when HTTP/1.1 200 OK was received**

The difference gives the server response time which is 0.05 seconds.

(b) IP Addresses

From the IP header:

- **Source IP = 34.107.221.82**
- **Destination IP = 10.74.218.242**

These can be verified from packet details in Wireshark.

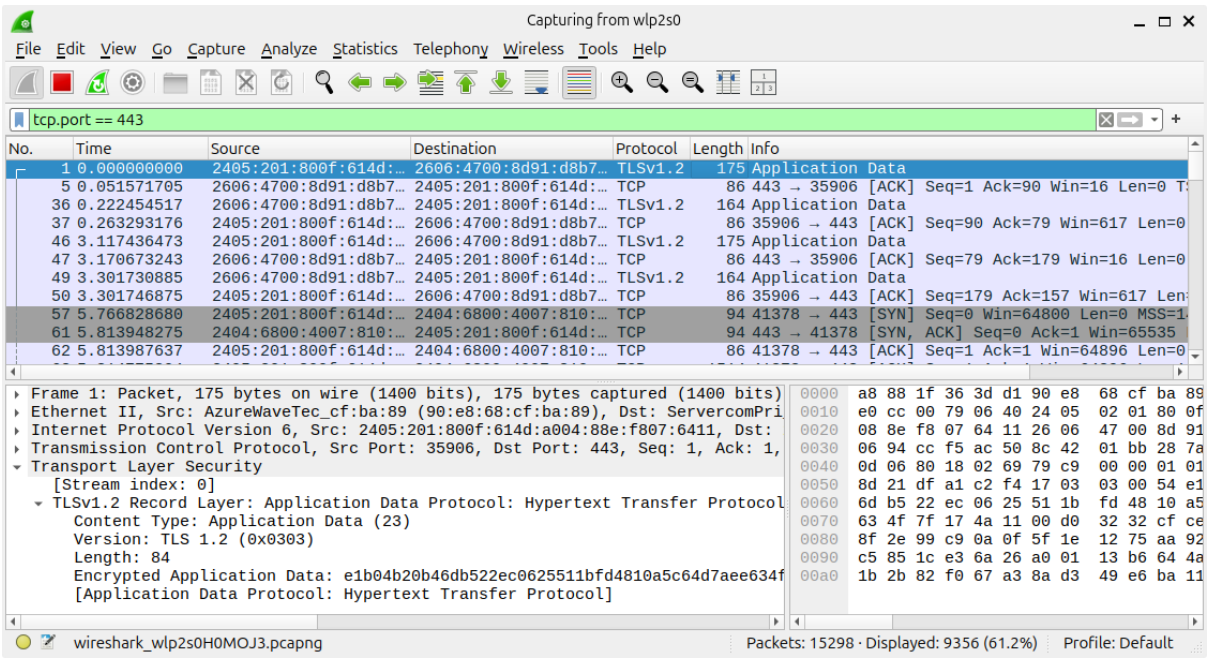
5. Start the Wireshark packet capturing service. Enter the URL:

https://www.gmail.com on your browser and sign-in to your gmail account by providing credentials (Username/Password).

Answer the following from the captured packets:

a. Is there any difference in the application layer protocol?

b. How it is different from the HTTP data you analysed in the above problem?



(a) Difference in Application Layer Protocol

Yes. The protocol is HTTPS, which uses TLS encryption, instead of plain HTTP.

(b) Difference from Previous HTTP Capture

Feature	HTTP (Task 4)	HTTPS (Task 5)
Encryption	No	Yes (TLS)
Data visibility	Visible	Encrypted
Credentials visible	Yes	No
Port	80	443

Only TLS handshake and encrypted application data packets are visible in Wireshark.