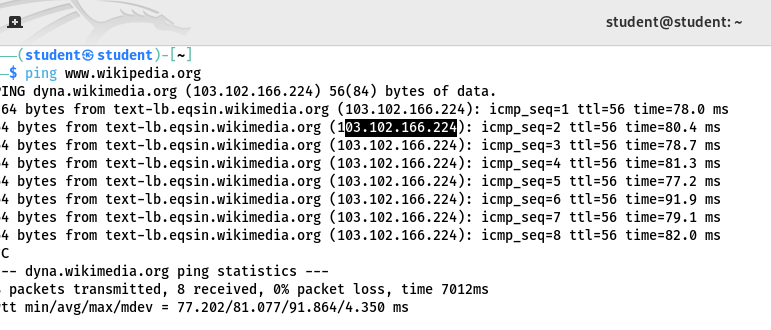
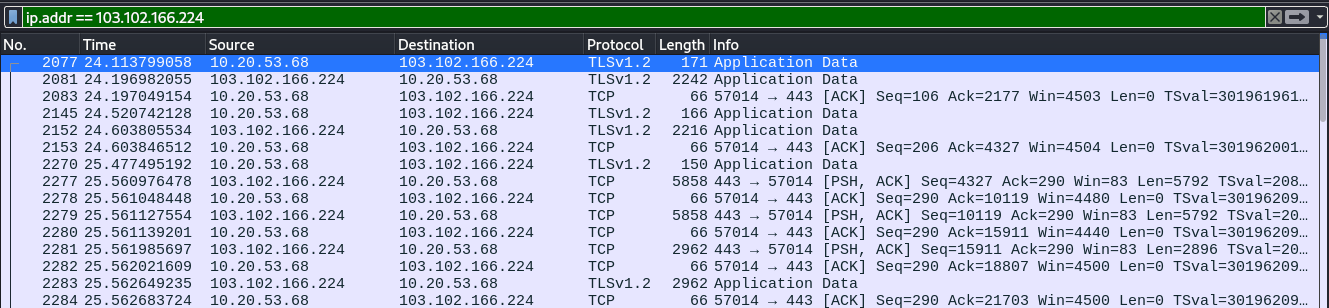
**Name:- Ritesh Lakhani EnrollmentNo:- 22010101099**

**Date:- 21/02/2025**

Lab-11 : **Wireshark Tool Exercises**

**1. Capturing Live Traffic – Use any website.**

****

### **Capturing Wikipedia Traffic**

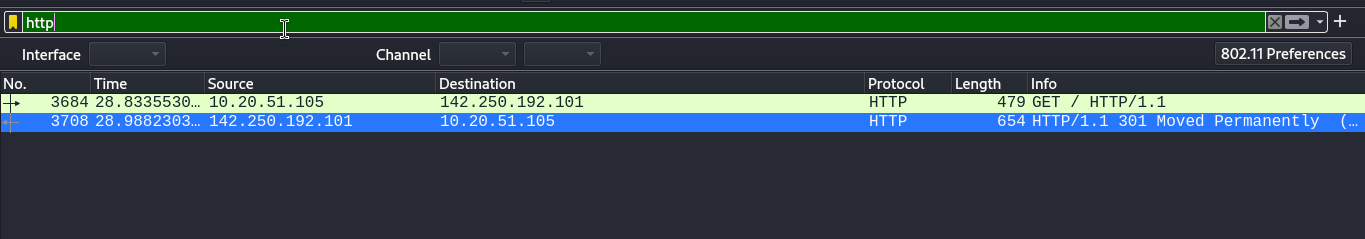
1. Start Wireshark – Select the network interface and begin capturing.
2. Filter Traffic – Use ip.addr == 103.102.166.224 for Wikipedia or http/tcp.port == 443 for HTTP/HTTPS.
3. Analyze Packets – Inspect HTTP GET requests or TLS handshake for HTTPS.
4. Verify Connectivity – Use ping www.wikipedia.org to check response time and packet loss.

**2. Applying Capture Filters:**

**a. HTTP traffic: hAp**

i. For HTTP - Inspect request and response headers, URLs, and status codes.

ii. For HTTPS, observe the handshake process (TLS).



**Description:-**

**Request:** The client (10.20.51.105) sends an HTTP GET request to 142.250.192.101.

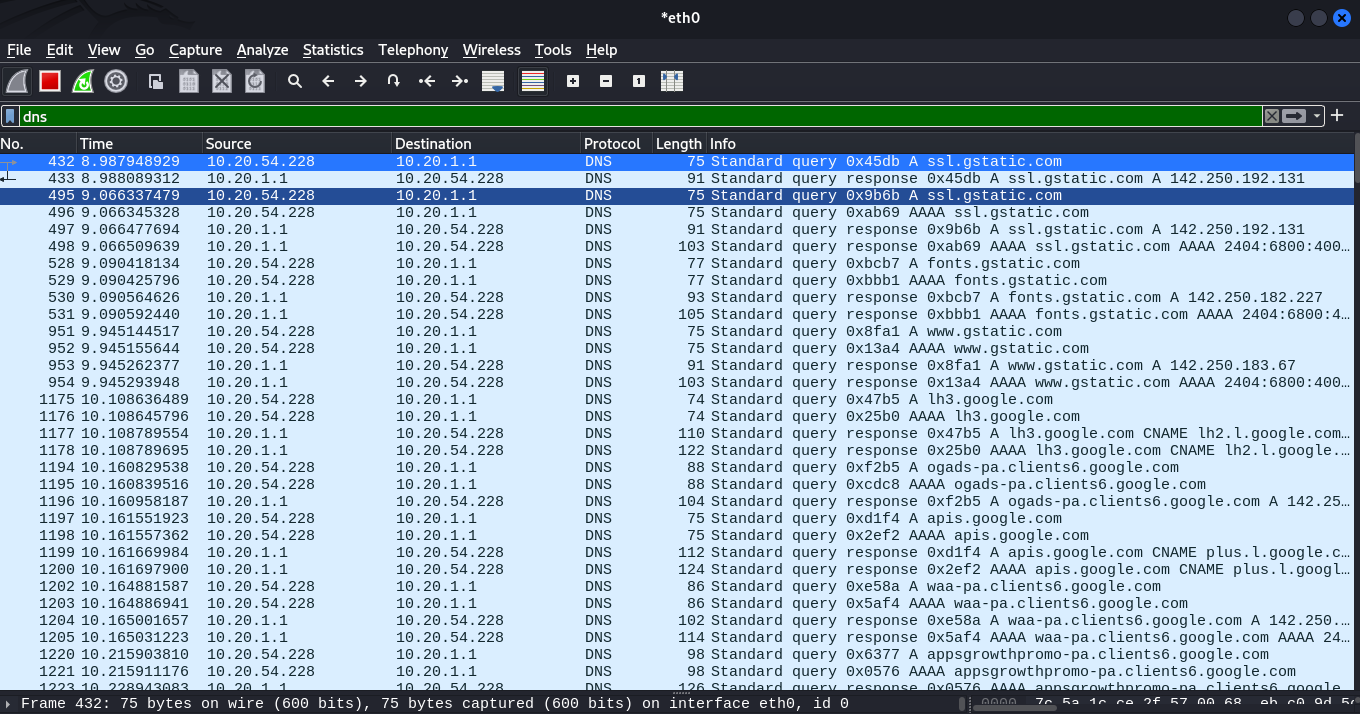
**Response:** The server replies with HTTP 301 Moved Permanently, indicating redirection to another URL.

**Observation:** HTTP traffic is unencrypted, allowing inspection of headers, URLs, and status codes.

**b. DNS requests: dns**

i. Observe how domain names are translated into IP addresses.

ii. IdenQfy DNS request and response packets.



**Description:-**

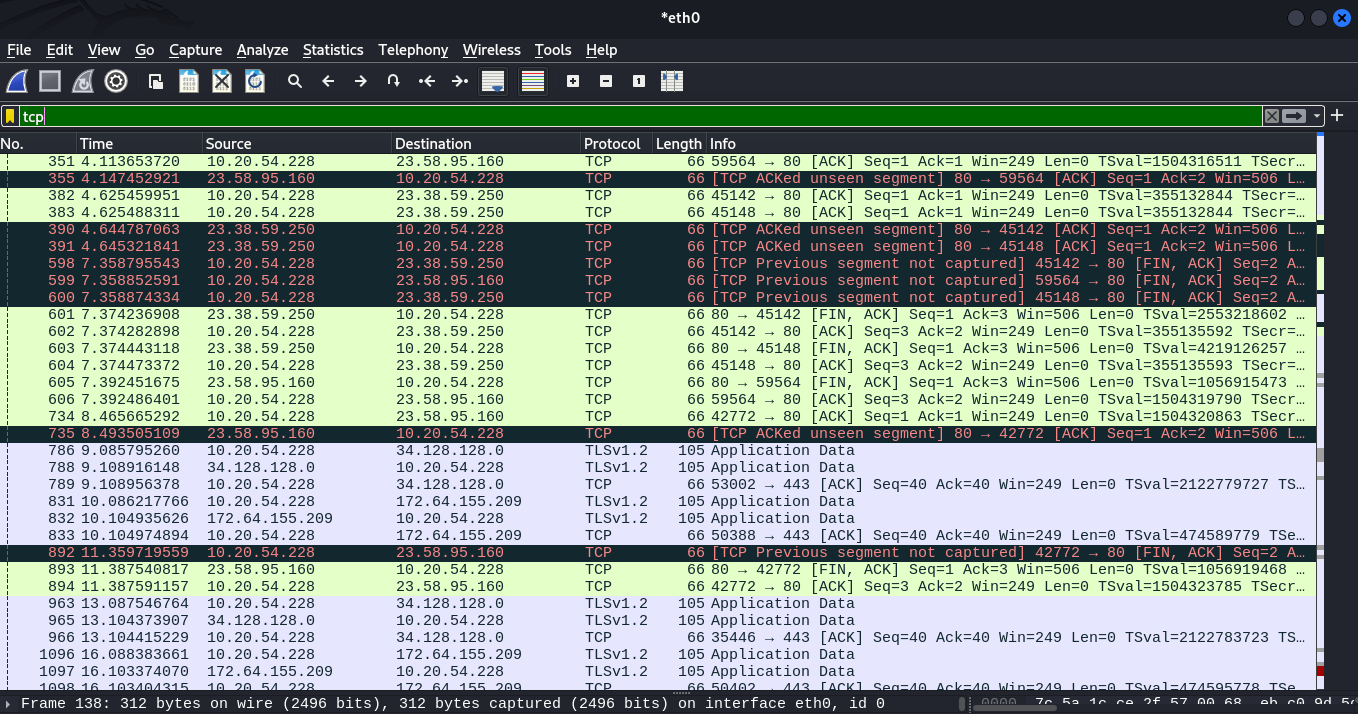
### **DNS Requests and Responses Overview:**

* **DNS Request:** The client (10.20.54.228) queries the DNS server (10.20.1.1) for domain name resolution (e.g., ssl.gstatic.com).
* **DNS Response:** The server replies with the corresponding IP address (e.g., 142.250.192.131).
* **Process:** Converts domain names to IP addresses for network communication.

**c. TCP packets: tcp**

i. Observe the 3-way handshake (SYN, SYN-ACK, ACK).

ii. IdenQfy sequence numbers and acknowledgment numbers.



**Description:-**

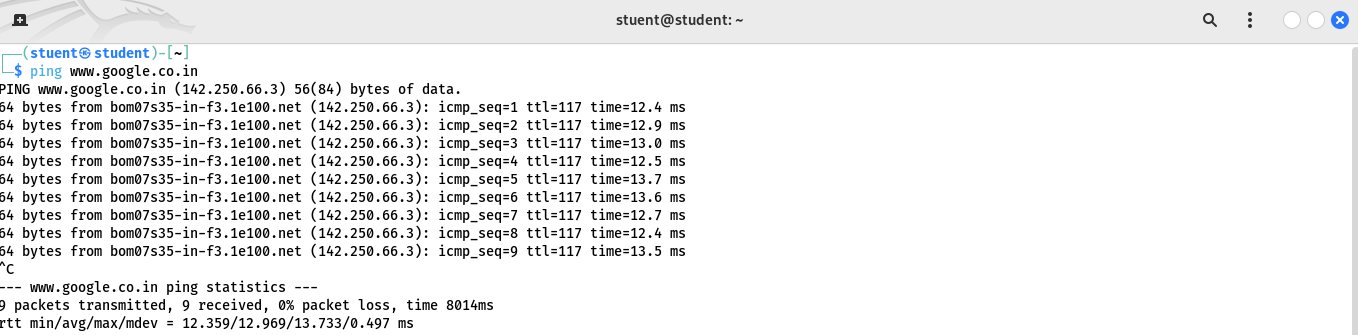
In the Wireshark capture, the **TCP 3-way handshake** is observed with the following steps:

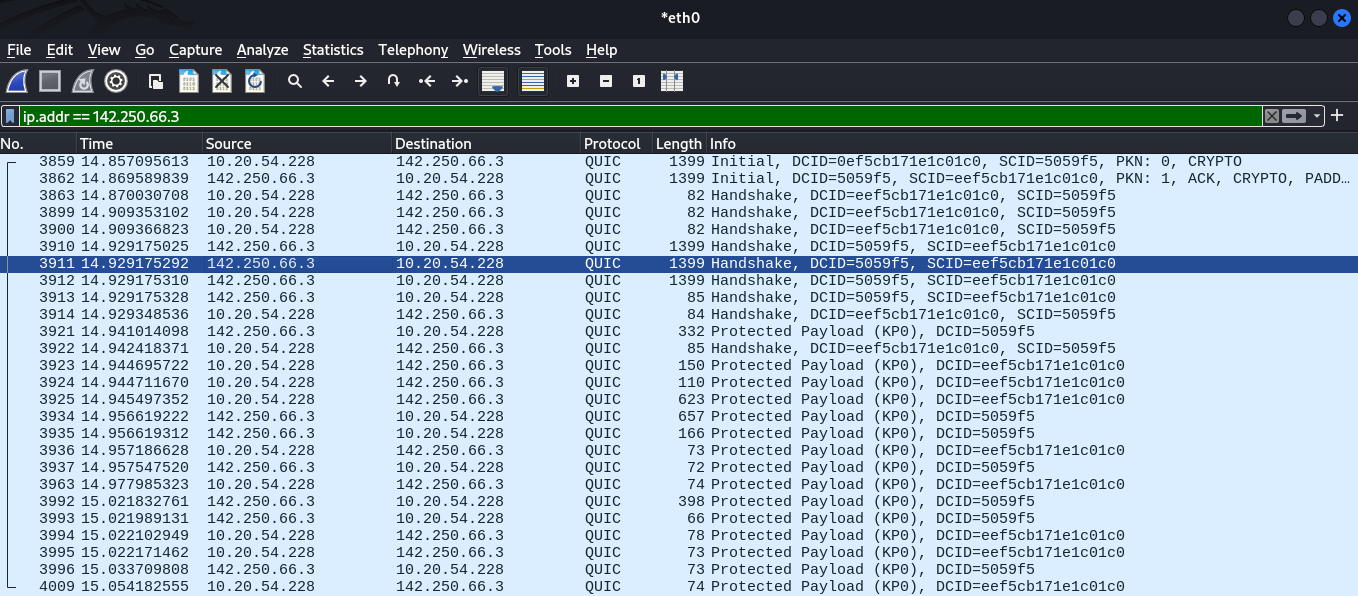
1. **SYN**: The client (IP 10.20.54.228) sends a SYN packet to initiate the connection.
2. **SYN-ACK**: The server (IP 23.58.95.160) responds with a SYN-ACK packet to acknowledge the request.
3. **ACK**: The client sends an ACK packet to confirm the connection.

Additionally, **sequence numbers** (Seq) track the data being sent, starting from Seq=1 for the SYN packet, and **acknowledgment numbers** (Ack) confirm the receipt of data, such as Ack=249 to acknowledge the data received. This process ensures reliable and ordered data exchange in TCP communication.

**d. ICMP (ping): icmp**

i. Send ping requests (ping google.com) and observe request/reply packets.





**Description:-**

### **ICMP (ping) Packets:**

The first image demonstrates the use of the ping command to test connectivity with google.co.in. The system sends ICMP Echo Request packets, and Google’s server responds with ICMP Echo Reply packets. Each response includes sequence numbers (icmp\_seq), Time-to-Live (ttl), and round-trip time (time). The ping statistics at the end indicate no packet loss, confirming successful communication.