Wireshark Network Analysis – Detailed Report

1. Basic networking concepts (IP, MAC, DNS, TCP/UDP)

IP Address: An IP address is a logical address assigned to each device connected to a network. It identifies the source and destination of data packets.

MAC Address: A MAC address is a unique physical address assigned to a network interface card (NIC). It is used for communication within a local network.

DNS (Domain Name System): DNS converts human-readable domain names such as google.com into IP addresses that computers can understand.

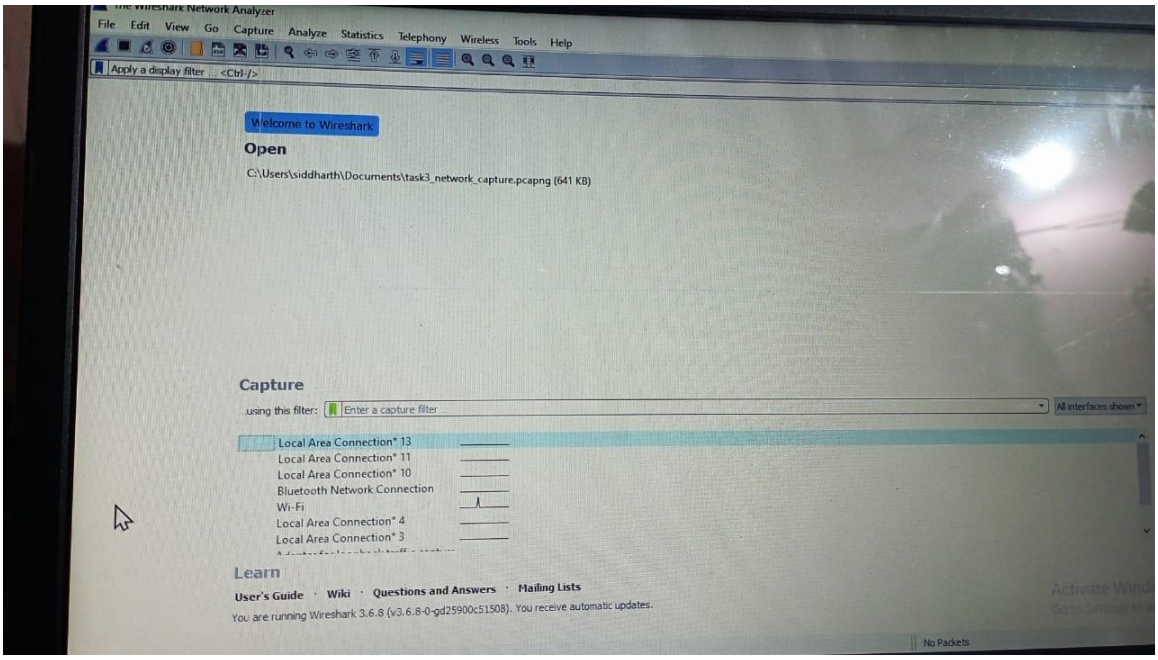
TCP (Transmission Control Protocol): TCP is a connection-oriented protocol that ensures reliable data transmission using acknowledgements and error checking.

UDP (User Datagram Protocol): UDP is a connectionless protocol that is faster than TCP but does not guarantee delivery.

2. Installing Wireshark and capture live network traffic

Wireshark was installed on the system along with the required packet capture driver (Npcap). After installation, Wireshark was launched and the active Wi-Fi interface was selected.

Once the capture started, packets began appearing immediately, confirming that live network traffic was being recorded successfully.



3. Filter packets by protocol (HTTP, DNS, TCP)

Display filters were applied to analyze specific types of traffic.

The 'dns' filter was used to observe DNS queries and responses.
The 'tcp' filter was used to analyze TCP connections.
The 'http' filter was used to check for unencrypted web traffic.

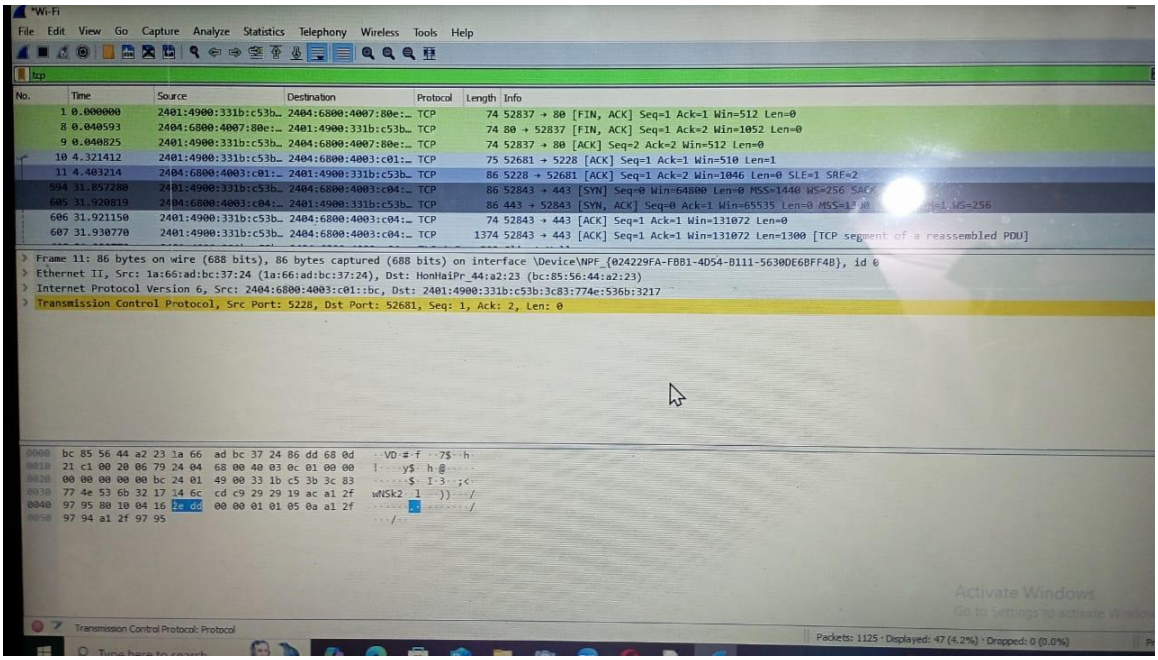
Filtering helped in focusing only on relevant packets.

4. Observe three-way TCP handshake

Using the TCP filter, the TCP three-way handshake was observed.

SYN – Client sends a connection request.
SYN-ACK – Server acknowledges the request.
ACK – Client confirms the connection.

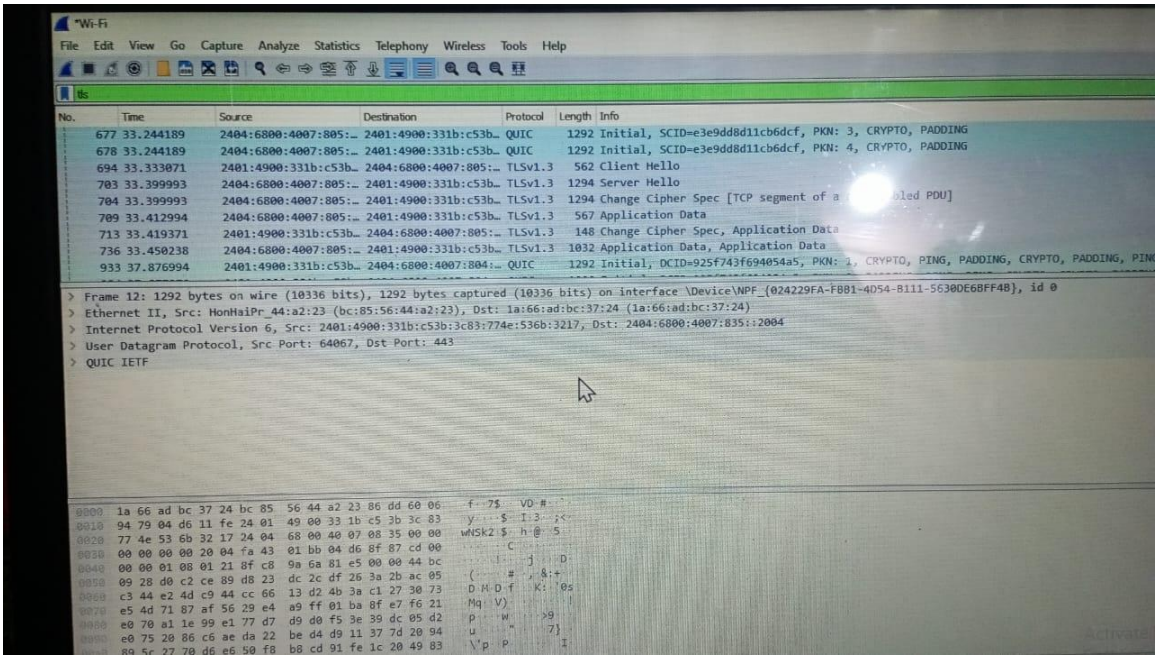
This process ensures reliable communication before data transfer begins.



5. Identify plain-text traffic vs encrypted traffic

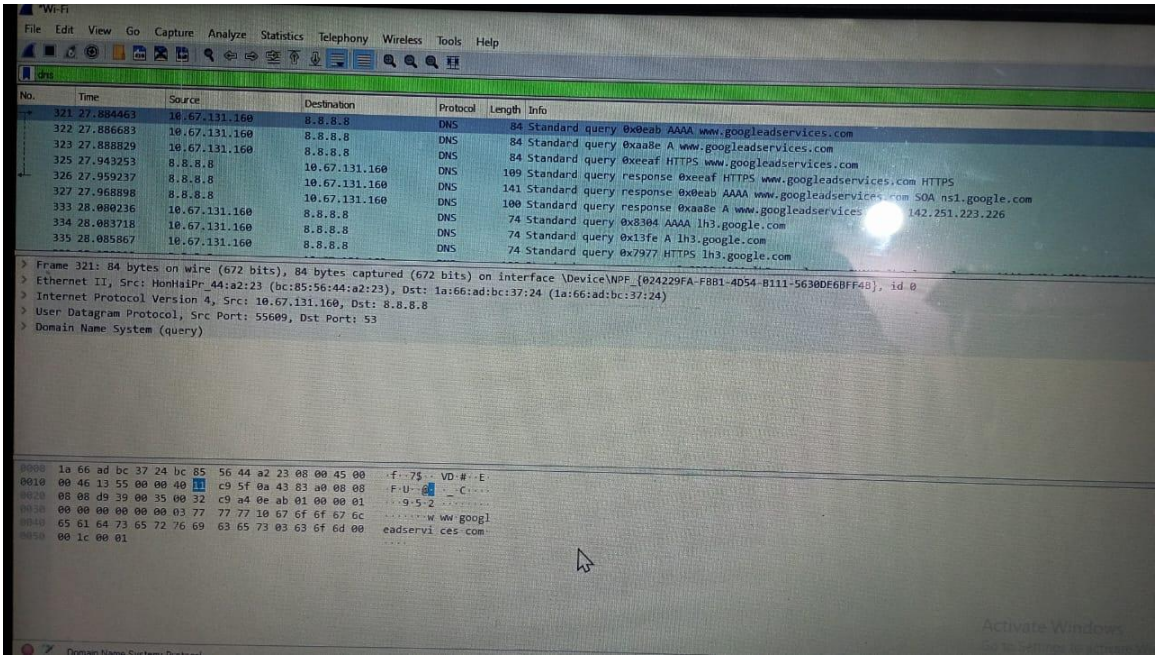
DNS traffic showed domain names in readable format, indicating plain-text communication.

HTTPS/TLS traffic was encrypted, and the content was not readable, demonstrating secure communication.



6. DNS queries and analysis

DNS queries were captured and analyzed.
Requests were sent to DNS servers such as 8.8.8.8 (Google DNS).
Domain names were resolved into IP addresses.
This showed how DNS enables internet communication.



7. Save packet captures for analysis

After analysis, the captured packets were saved in .pcapng format.
Saved capture files can be reopened later in Wireshark for further analysis or evidence.

8. Conclusion

This task provided hands-on experience in network traffic analysis using Wireshark. It improved understanding of networking protocols and highlighted the importance of encrypted communication.