Wireshark Packet Analysis Report

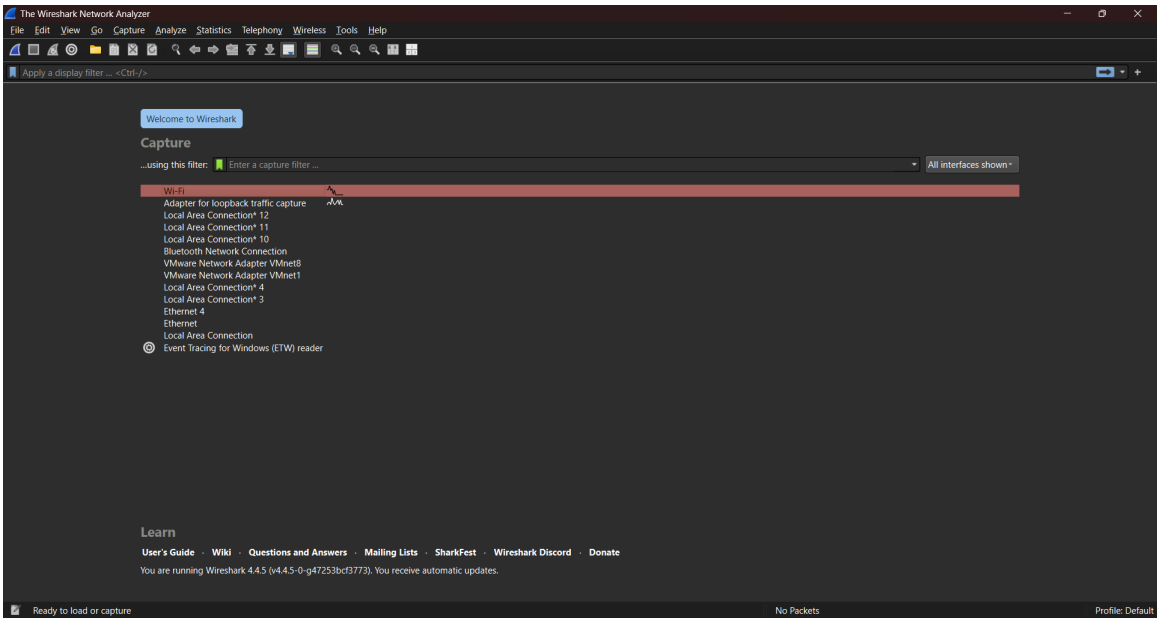
Objective

To perform a hands-on network traffic capture using Wireshark and analyze packets across various protocols.

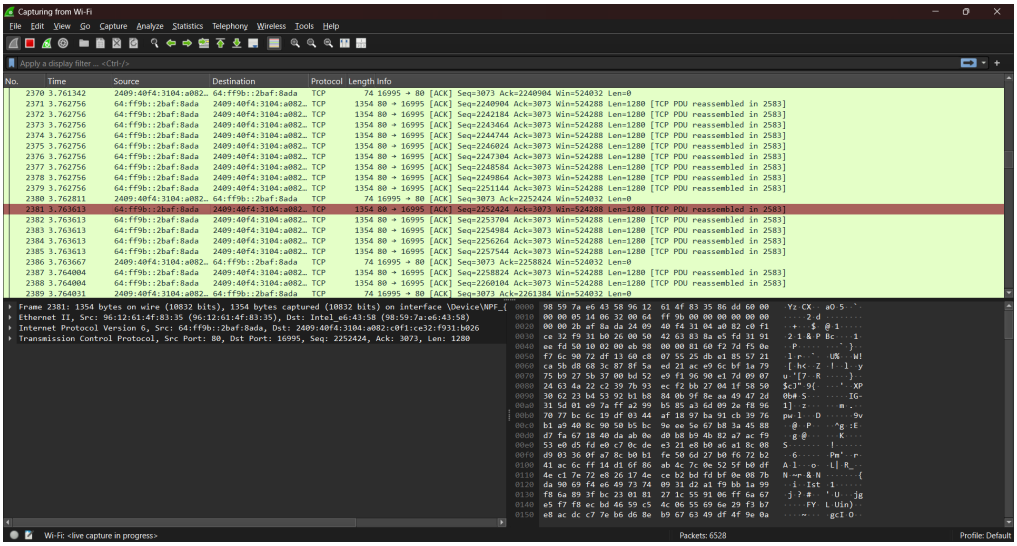
Procedure

1. 1. Installed Wireshark from the official website (https://www.wireshark.org/).
2. 2. Launched Wireshark and started capturing packets on the active network interface.
3. 3. Opened a browser and visited a website (e.g., https://example.com) or executed 'ping google.com' to generate network traffic.
4. 4. After about a minute of activity, stopped the packet capture.
5. 5. Applied display filters such as 'http', 'dns', and 'tcp' to analyze specific protocol packets.
6. 6. Identified at least three different protocols from the captured traffic.
7. 7. Exported the captured data as a .pcap file for documentation and future reference.

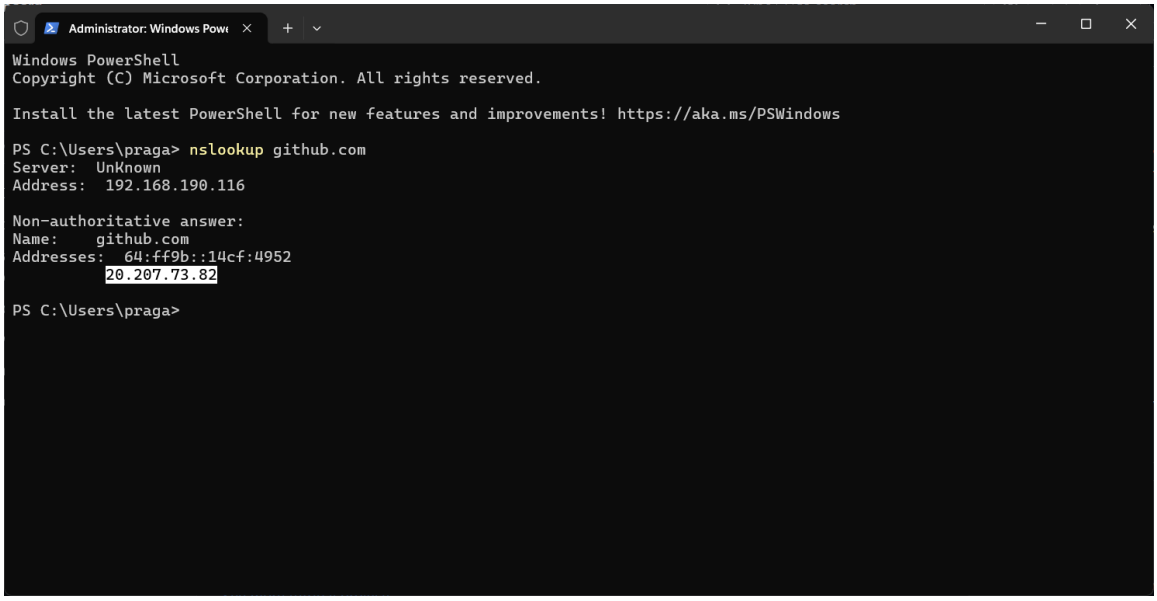
Screenshots



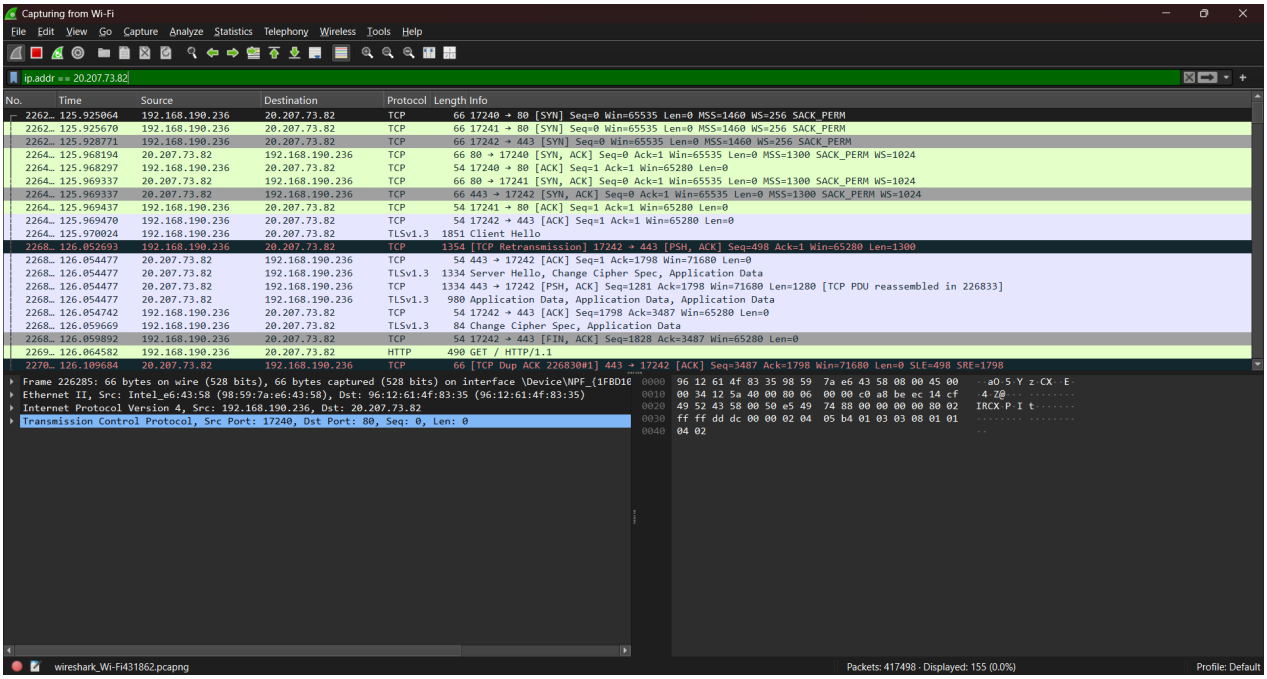
All incoming and outgoing network traffics :



Capturing the network traffic of github.com using the command :



ip.addr == 20.207.73.82



I/O graph

Protocols Identified

From the captured network traffic, the following protocols were observed:

- • HTTP (HyperText Transfer Protocol)
- • DNS (Domain Name System)
- • TCP (Transmission Control Protocol)

Packet Summary

Each protocol carried specific types of data:

• HTTP packets included GET and POST requests for web content.

• DNS packets resolved domain names to IP addresses.

• TCP packets established and maintained connections with acknowledgments and sequence numbers.

Conclusion

This hands-on task demonstrated the basics of capturing and analyzing network traffic. The identification of different protocols and packet-level inspection helped in understanding how data flows through a network.