**Name - Gaurang A Raorane Roll No - 49**

**Class - D15A Batch - C**

**CA Experiment 03**

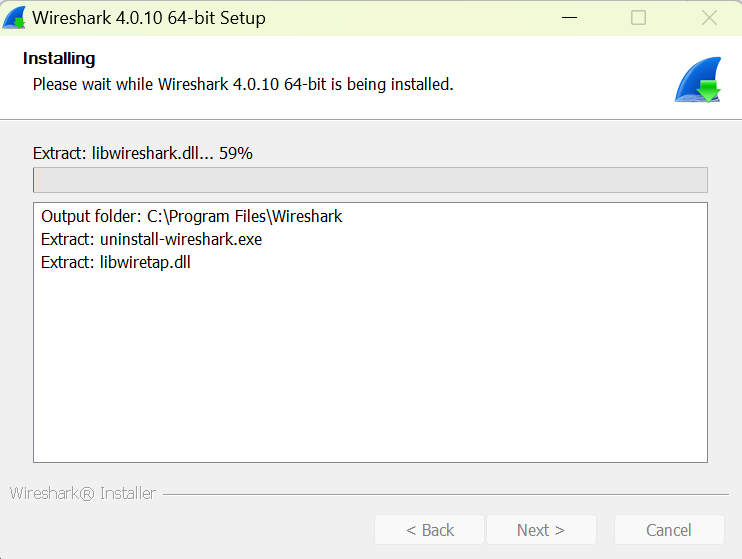
**Aim:** Implement Wireshark as Network Packet Analyzer and analyze network traffic.

**Introduction:**

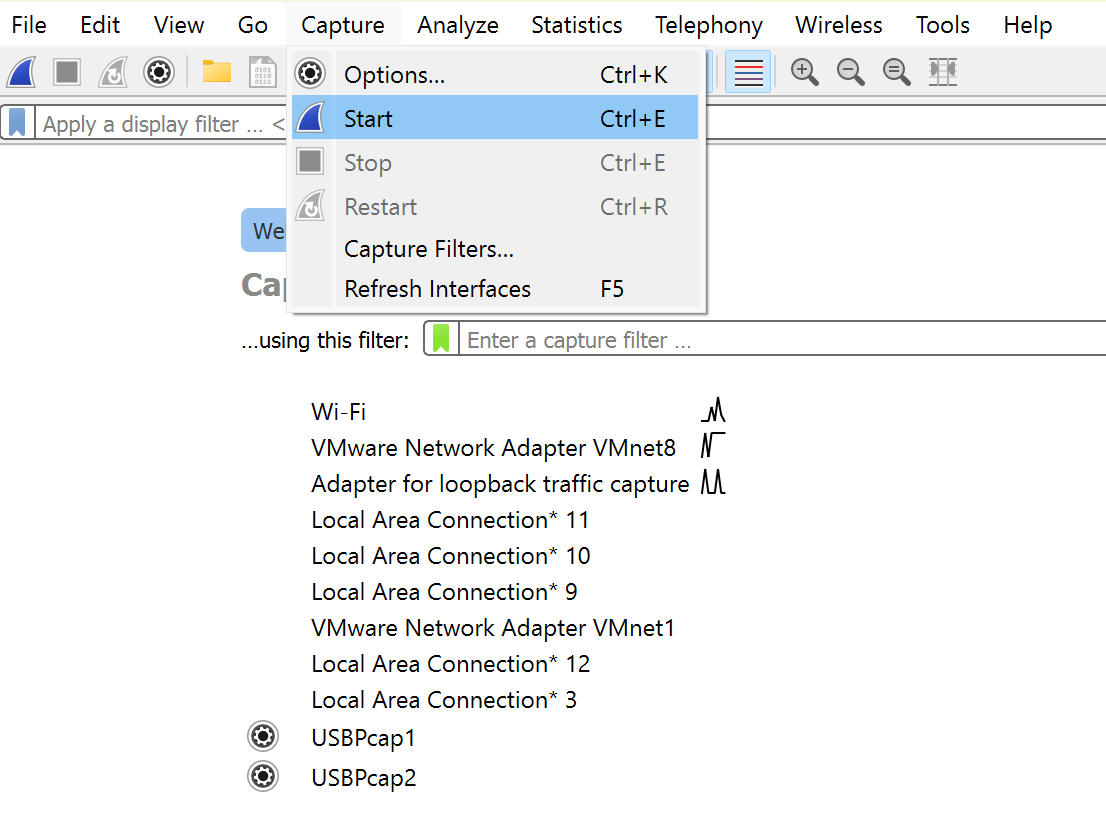
Wireshark is a complex and powerful network packet analyzer that requires specific software installation and usage on a local machine. It's not something that can be implemented or executed within a text-based environment like this one.

To use Wireshark as a network packet analyzer, you would typically follow these steps:

* Step 1: Download and Install Wireshark: Go to the official Wireshark website (<https://www.wireshark.org/>)

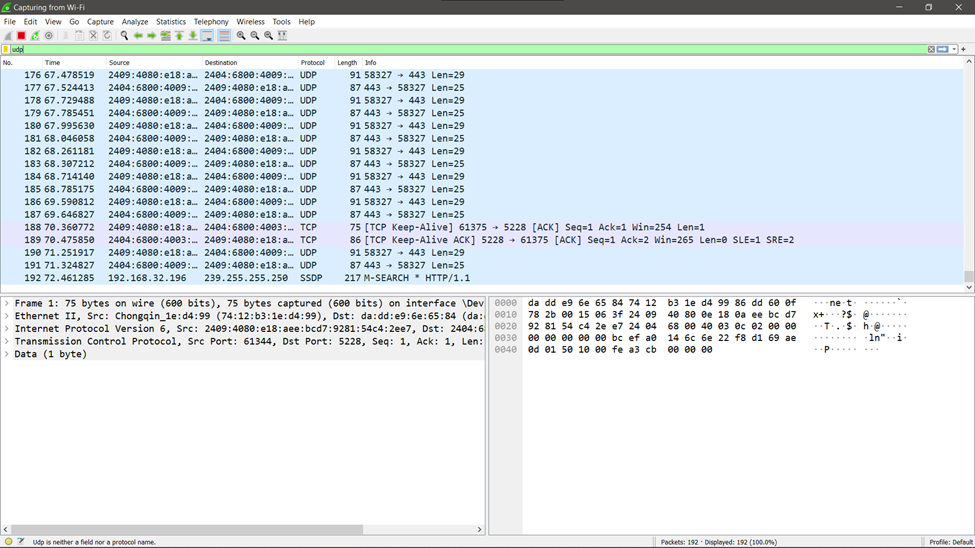


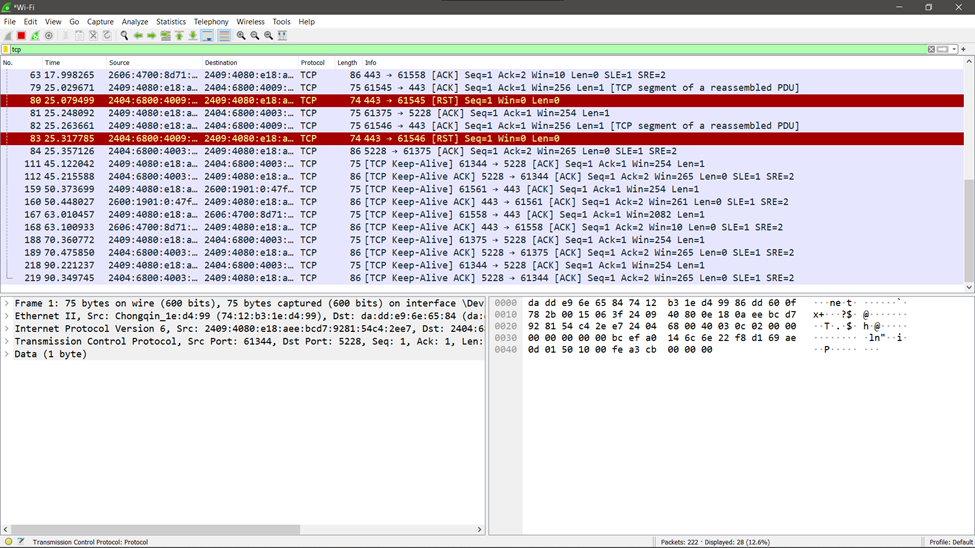
* Step 2: Launch Wireshark: After installation, launch Wireshark.
* Capture Network Traffic: Start a new capture session by selecting a network interface (e.g., Ethernet, Wi-Fi) and clicking the "Start" button. Wireshark will begin capturing network packets.

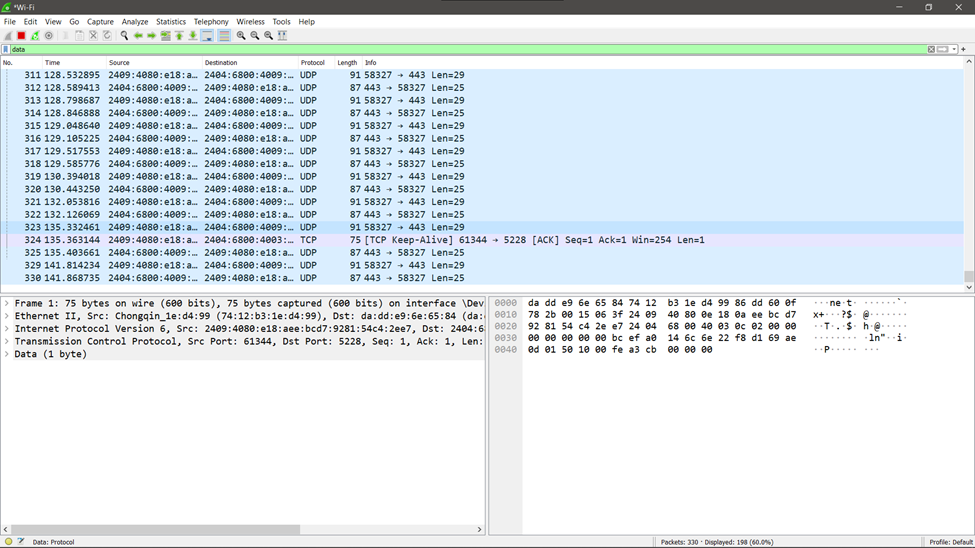


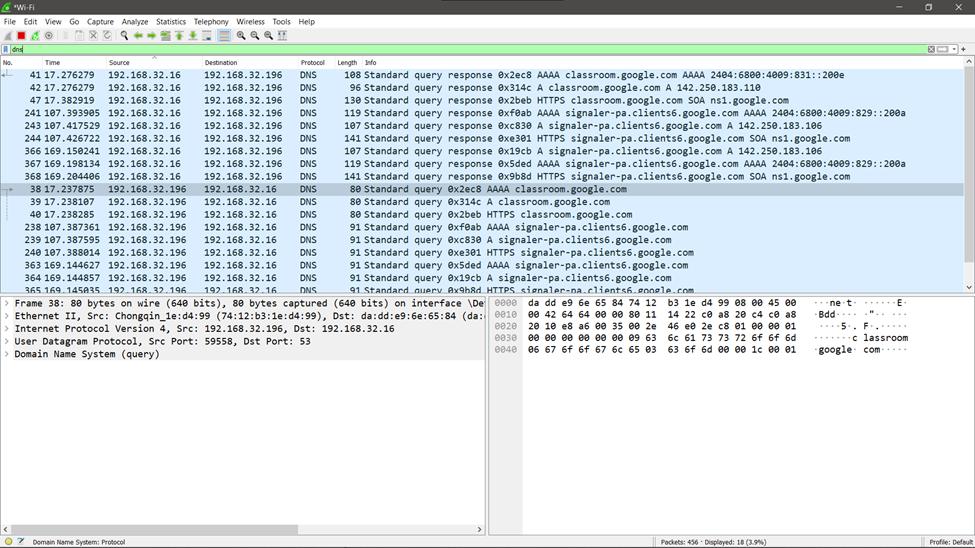
* View Packet Details: You can click on individual packets to view detailed information about each packet, including its source and destination, protocol used, and the content of the packet.

Apply Filters: You can apply filters to narrow down the packets you want to analyze. For example, you can filter by IP address, port number, dns, udp, tcp.









Analyze Packets: Once you've captured some packets, you can stop the capture and start analyzing the data.

**Conclusion:**

Implemented Wireshark as a network analyzer tool and analyzed network traffic by narrowing down scan using various filters.