**NAME:PRAVEEN V**

**ROLL NO.:241901082**

# Exercise 13

TO CAPTURE, SAVE, AND ANALYZE NETWORK TRAFFIC ON TCP / UDP / IP / HTTP / ARP/DHCP /ICMP /DNS USING WIRESHARK TOOL

**Aim:**

To study and analyze different network protocol packets such as TCP, UDP, IP, HTTP, ARP, DHCP, ICMP, and DNS by capturing live network traffic using **Wireshark** tool.

**Introduction:**

Wireshark is a powerful network protocol analyzer used to monitor and capture live network packets. It allows users to inspect protocols at each layer of the OSI model and understand how data is transmitted over the network.   
By analyzing captured packets, we can identify communication patterns, troubleshoot connectivity issues, and study protocol behavior such as TCP handshakes, DNS lookups, HTTP requests, and ICMP pings.

**Algorithm:**

1. Open Wireshark application on the system.
2. Select the active network interface (Wi-Fi or Ethernet) to capture packets.
3. Click on Start Capturing Packets.
4. Open Command Prompt in Windows and execute the commands to generate various types of traffic
5. After running the commands, return to Wireshark and click Stop Capture.
6. Save the captured packets as a .pcap file.
7. Observe packet details such as Source & Destination IP, MAC addresses, ports, and payload.

**Output**:

A screenshot of a computer

AI-generated content may be incorrect.

**Result**:

The experiment to capture and analyse network traffic using **Wireshark** was successfully performed.   
Packets for TCP, UDP, IP (IPv6), HTTP, ARP, ICMP, and DNS were captured and analysed.   
Hence, the objective of the experiment is achieved successfully.