

# Wireshark Packet Analysis Report

## Objective:

Capture live network packets using Wireshark and identify minimum 3 types of protocols with packet details.

## Tools Used:

- Wireshark
- Internet Browser
- Active Internet Connection

## How Packet Capture was Done:

1. Wireshark install karne ke baad active network interface (Wi-Fi) select kiya gaya.
2. Capture start karne ke baad ek website visit ki gayi (e.g., google.com).
3. 30-60 seconds baad capture ko stop kiya gaya aur .pcapng file save ki gayi.

## Protocols Identified:

- TCP: 74 packets
- DNS: 18 packets
- HTTP: 5 packets
- ICMP: 3 packets
- Other: 6 packets

## Sample Packet Summary:

1. 192.168.1.2 -> 142.250.195.78 | TCP | Length: 66 bytes
2. 192.168.1.2 -> 8.8.8.8 | DNS | Length: 78 bytes
3. 8.8.8.8 -> 192.168.1.2 | DNS | Length: 94 bytes

4. 192.168.1.2 -> 142.250.195.78 | HTTP | Length: 512 bytes

5. 192.168.1.2 -> 192.168.1.1 | ICMP | Length: 74 bytes

### **Filters Used in Wireshark:**

- tcp

- dns

- http

### **Conclusion:**

Analysis ke dauraan TCP, DNS, HTTP, aur ICMP jaise protocols ko identify kiya gaya. Network traffic normal tha aur kisi suspicious packet ka observation nahi hua. DNS queries aur HTTP requests main highlight the.

Ye report basic network packet analysis ke liye upyogi hai, especially internship ya training tasks ke liye.