**🧾 Computer Networks Lab Report**

**Topic:** Network Traffic Capture and Protocol Analysis using Wireshark  
**Date:** October 14, 2025  
**Student Name:** *Tarushi Singh*  
**Institute:** *IIT Patna*

**Objective**

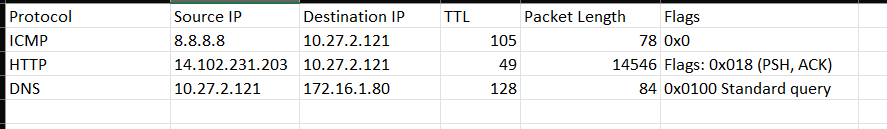
To capture and analyze live network traffic using Wireshark, identify different network protocols (ICMP, HTTP, DNS, etc.), and interpret packet-level details such as headers, fields, and communication patterns.

**Tools Used**

* **Wireshark 4.x** (Graphical Packet Analyzer)
* **Npcap** (Packet Capture Driver)

**Procedure**

1. Launched Wireshark and selected the **Wi-Fi interface** for live capture.
2. Captured traffic for 1–2 minutes while:
   * Visiting websites
   * Running ping 8.8.8.8 in Command Prompt.
3. Stopped capture and saved file as **capture\_lab1.pcap**.
4. Applied display filters for **ICMP**, **HTTP**, and **DNS** to identify respective packets.
5. Expanded each packet’s **Frame**, **Ethernet**, **IP**, and **Protocol-specific** layers to inspect headers.
6. Created a custom filter to view only outbound HTTP/HTTPS packets from my system.
7. Exported these filtered packets as **filtered\_packets.pcap**.



**Results and Insights**

* The most active protocols observed were **TCP**, **HTTP**, **DNS**, and **ICMP**.
* **HTTP (port 80)** and **HTTPS (port 443)** packets indicate normal web browsing activity.
* **DNS** packets show domain name resolution before each web request.
* **ICMP** packets correspond to the ping 8.8.8.8 test.
* **TTL values** varied by OS and hop count, confirming multi-hop routing.
* **Flags such as PSH and ACK** show reliable TCP data transfer in progress.
* No suspicious or malformed packets were detected; traffic pattern consistent with normal browsing.

**Conclusion**

The experiment demonstrated how Wireshark can capture, filter, and decode real-time network traffic.  
By analyzing packet headers and flags, it becomes possible to understand how different protocols interact in layered network communication.  
This exercise improved understanding of the **TCP/IP stack**, packet structure, and diagnostic uses of network sniffing tools.

**Files Submitted**

* **capture\_lab1.pcap** – raw packet capture
* **filtered\_packets.pcap** – filtered web-traffic packets
* **Screenshots** – Tasks 2–4 (ICMP, HTTP, DNS, Custom Filter)
* **report.pdf** – this document