Wireshark Packet Capture Report

# 1. Objective

The objective of this exercise was to capture live network packets using Wireshark and analyze the protocols involved in basic network communication.

# 2. Tools Used

- Wireshark (latest version)  
- Windows 10/11  
- Active Internet Connection

# 3. Steps Performed

1. Installed Wireshark on Windows system.  
2. Started capturing packets on the active network interface (Wi-Fi/Ethernet).  
3. Generated traffic by browsing websites and using ping command.  
4. Stopped capture after around 1 minute.  
5. Applied protocol filters such as HTTP, DNS, TCP, ICMP.  
6. Identified multiple protocols from the capture.  
7. Saved the capture file in .pcap format.

# 4. Protocols Identified

At least three protocols were identified in the capture:  
- DNS (Domain Name System): Used to resolve domain names to IP addresses.  
- TCP (Transmission Control Protocol): Ensures reliable data transfer.  
- HTTP/HTTPS (Hypertext Transfer Protocol): For web browsing.  
- ICMP (Internet Control Message Protocol): For ping requests/replies.

# 5. Packet Details (Examples)

Example packets observed:  
- DNS Query: A request sent to resolve 'google.com'.  
- TCP Handshake: SYN, SYN-ACK, ACK sequence observed.  
- HTTP Request: GET request sent to fetch a web page.  
- ICMP Echo Request/Reply: Ping packets to/from server.

# 6. Conclusion

The exercise helped in understanding how Wireshark captures and displays network traffic in real-time. Protocol filters made it easier to analyze specific communication. This builds awareness of common protocols used in everyday network activity.