Wireshark Network Traffic Analysis Report

# 1. Introduction

This report documents the analysis of network traffic captured using Wireshark on a Windows system. The goal is to observe, filter, and summarize packet data to understand various protocols involved in internet communication.

# 2. Tools Used

• Wireshark (Windows version)  
• Windows Command Prompt / Web Browser

# 3. Steps Performed

1. 1. Installed and launched Wireshark on the Windows machine.
2. 2. Started packet capture on the active network interface (e.g., Wi-Fi or Ethernet).
3. 3. Generated network traffic by opening a browser and visiting websites, and also used the 'ping' command in Command Prompt (e.g., `ping google.com`).
4. 4. Allowed the capture to run for about one minute.
5. 5. Stopped the capture after sufficient packets were collected.
6. 6. Filtered the captured packets using protocol filters like `http`, `dns`, and `tcp`.
7. 7. Identified various protocols by observing the Protocol column in the capture pane.
8. 8. Exported the capture as a `.pcap` file for later reference and analysis.

# 4. Protocols Identified

At least three distinct protocols were identified during the capture:  
  
• HTTP (HyperText Transfer Protocol): Used for loading web pages.  
• DNS (Domain Name System): Resolves domain names to IP addresses.  
• TCP (Transmission Control Protocol): Ensures reliable delivery of data packets.

# 5. Packet Details Summary

Example summary of observed packets:  
• HTTP packets showed GET requests and responses to web servers.  
• DNS packets resolved names like www.google.com to IP addresses.  
• TCP packets showed three-way handshakes and session establishment.

# 6. Export Details

The captured packets were exported as a `.pcap` file using File > Export Specified Packets.

# 7. Conclusion

This exercise demonstrated basic usage of Wireshark for capturing and analyzing live network traffic. It helped identify key protocols and understand their roles in communication.