Wireshark Network Traffic Analysis Report

Tool Used: **Wireshark**

File Name: **network_capture.pcap**

Objective

To capture live network traffic using Wireshark and identify at least three different protocols observed during the capture session.

Steps Followed

1. Installed and launched Wireshark.
2. Selected the active network interface (Wi-Fi/Ethernet).
3. Started packet capture.
4. Generated network traffic by:
   - Pinging google.com
   - Browsing a website (e.g., https://google.com)
5. Stopped the capture after approximately one minute.
6. Applied filters to isolate specific protocols.
7. Identified and documented protocol types.
8. Exported the capture as a .pcap file for submission.

Protocols Identified

1. DNS (Domain Name System)

Function: Resolves domain names to IP addresses.

Observation: Queries to google.com and other domains were captured.

Details:
- Source Port: Random high port (e.g., 51923)
- Destination Port: 53 (standard DNS)
- Protocol: UDP

2. HTTP (Hypertext Transfer Protocol)

Function: Facilitates communication between browser and web server.

Observation: Requests and responses captured during website browsing.

Details:
- Source Port: Random high port (e.g., 51924)

- Destination Port: 80
- Protocol: TCP

3. TCP (Transmission Control Protocol)

Function: Provides reliable, ordered delivery of data.

Observation: Used in HTTP communication and other transport processes.

Details:
- Three-way handshake observed.
- Source/Destination Ports varied.

Summary of Findings

The network traffic captured shows active use of DNS, HTTP, and TCP protocols.
DNS resolved domain names for website browsing and ping commands.
HTTP traffic confirmed successful access to web resources.
TCP was the underlying protocol ensuring reliable transmission.