**Wireshark Network Traffic Analysis Report**

**Task:** Capture and Analyze Network Traffic Using Wireshark

**Tool Used:** Wireshark (Free, Open-source)

**Date of Capture:** 11/08/20025

# Objective

The objective of this task was to capture live network packets using Wireshark, identify the basic protocols in use, and summarize the packet details for analysis.

# Procedure

* Installed Wireshark on the system.
* Selected the active network interface (Wi-Fi) for packet capture.
* Started capture and generated network traffic by browsing multiple websites and pinging a publicserver (ping google.com).
* Stopped the capture after 1 minute.
* Applied filters to view specific protocols: http, dns, tcp.
* Identified and recorded packet details.
* Exported the capture as a .pcap file.

# Protocols Observed

|  |  |
| --- | --- |
| **Protocol** | **Description** |
| HTTP | HyperText Transfer Protocol - Used for web browser |
| DNS | Domain Name System - Resolves domain names to IP addresses |
| TCP | Transmission Control Protocol - Reliable,  connection-based transport layer protocol |

# 4 .Packet Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Time** | **Source IP** | **Destination IP** | **Protocol** | **Length** | **Info** |
| 4.222095 | 2405:201:c042:8c8:219e:7e74:640e:870c, | 2405:200:1630:a01::b854:dd32 | TCP | 74 | SYN, Seq=1Len=0 |

# Summary & Observations

Successfully captured packets using Wireshark. Observed at least three different protocols: HTTP, DNS, and TCP. Packets included web browsing requests, DNS lookups, and TCP handshake messages. The traffic captured was normal for web browsing and basic network usage.

.