# Task 5 – Capture and Analyze Network Traffic Using Wireshark

## Objective

Capture live network packets using Wireshark, identify protocols such as DNS, HTTP, and TCP, and analyze packet details for deeper understanding of network communication.

## Tools Used

- Wireshark 4.4.8 (Windows 10)

- Wi-Fi network interface

- Browser for website visits and ping test

- Online ping test (ping-test.net)

## Steps Performed

- Installed Wireshark from the official site with default components (Wireshark and TShark) and Npcap for packet capturing.

- Started packet capture by selecting the Wi-Fi interface showing waveform activity and clicking the blue shark fin icon.

- Generated network traffic by visiting websites and running a ping test on ping-test.net, resulting in DNS, TCP, and HTTP/HTTPS packets.

- Stopped capture after approximately 1 minute and saved it as network\_capture.pcap.

## Protocol Analysis

### 1. DNS (Domain Name System)

Filter Applied: dns

Purpose: Resolves domain names to IP addresses.

Observed Queries: ping-test.net, storagegfed.dsx.mp.microsoft.com

|  |  |  |  |
| --- | --- | --- | --- |
| Source IP | Destination IP | Query Name | Type |
| 2401:4900:ac7:9c0:... | 8.8.8.8 | ping-test.net | A |
| 2401:4900:ac7:9c0:... | 8.8.8.8 | storagegfed.dsx.mp.microsoft.com | AAAA |

### 2. HTTP (Hypertext Transfer Protocol)

Filter Applied: http

Purpose: Transfer unencrypted web content.

Example from capture: GET / to host o.pki.goog with Keep-Alive and Accept-Encoding headers.

|  |  |  |  |
| --- | --- | --- | --- |
| Source IP | Destination IP | Method | Host |
| 2401:4900:ac7:9c0:... | 2404:6800:4009:80a:2003 | GET | o.pki.goog |

### 3. TCP (Transmission Control Protocol)

Filter Applied: tcp

Purpose: Provide reliable, ordered delivery of data.

Observed: TCP 3-way handshake between client and multiple servers.

|  |  |  |
| --- | --- | --- |
| Source IP | Destination IP | Flags |
| 2401:4900:ac7:9c0:... | 2404:6800:4009:80a:2003 | SYN |
| 2404:6800:4009:80a:2003 | 2401:4900:ac7:9c0:... | SYN/ACK |
| 2401:4900:ac7:9c0:... | 2404:6800:4009:80a:2003 | ACK |

## Outcome / Learning

Successfully installed and configured Wireshark, captured DNS, HTTP, and TCP traffic during real network activity, observed HTTP GET requests and TCP handshakes, and learned to use filters to isolate protocol traffic.