Wireshark Network Traffic Analysis Report

Name: Aryan Vats **,ROLL:** 2301MC52

Objective

The goal of this assignment was to capture, filter, and analyze live network traffic using Wireshark. The objective was to identify different network protocols and interpret packet-level details to understand fundamental network communication patterns.

Task 1: Packet Capture

Live network traffic was captured for approximately two minutes using Wireshark. During the capture, traffic was generated by browsing websites (`https://example.com`, `https://wikipedia.org`) and using the `ping 8.8.8.8` command. The resulting capture was saved as `capture_lab1.pcapng`.

Task 2: Protocol Identification

Display filters were used to isolate and inspect traffic for specific protocols.

- **ICMP:** The `icmp` filter successfully isolated the echo request and reply packets generated by the `ping` command.
- **DNS:** The `dns` filter revealed the Domain Name System queries used to resolve website names into IP addresses.
- **HTTP:** The `http` filter was used to view unencrypted web traffic.

Task 3: Detailed Packet Analysis

A representative packet from each of the filtered protocols was selected for detailed analysis.

Protocol	Source IP	Destination IP	TTL	Packet Length	Flags
ICMP	`192.170.9.73`	`8.8.8.8`	`64`	`74 bytes`	`N/A`
DNS	`192.170.9.73`	`192.170.0.1`	`64`	`79 bytes`	`0x0100` (Standard Query)
HTTP	`193.228.3.43`	`192.170.9.73`	`49`	`1326 bytes`	`0x018` (PSH, ACK)

Task 4: Custom Filter Creation

A custom display filter was created to show only packets sent from the source system (`192.170.9.73`) over standard web ports (80 for HTTP and 443 for HTTPS).

Filter Used: `ip.src == 192.170.9.73 && (tcp.port == 80 || tcp.port == 443)`

This filter effectively isolated all outgoing web traffic originating from the local machine.

Summary and Key Insights

- **Most Active Protocols:** An analysis of the protocol hierarchy showed that **TCP** and **TLSv1.2/1.3** (Transport Layer Security for HTTPS) were the most active protocols, accounting for the majority of the traffic due to web browsing. **UDP** was also prominent, primarily used for DNS queries.
- **Suspicious Traffic:** No suspicious or unusual traffic was detected during the capture. All observed communications were directly related to the user-initiated actions of web browsing and network diagnostics.
- **Key Network Insights:**

1. **DNS Precedes Connection:** The capture clearly shows that for every new website visited, a DNS query is first sent to resolve the domain name into an IP address. The TCP connection to the web server only begins after a successful DNS reply is received.
2. **HTTPS is Dominant:** The vast majority of web traffic was encrypted using TLS over TCP port 443. This highlights the modern web's reliance on secure communication.
3. **Communication is a Conversation:** A single click on a webpage does not generate one packet, but rather a long "conversation" of packets, including the TCP 3-way handshake, TLS negotiation, and multiple HTTP requests and responses to load all page elements.