Wireshark Network Traffic Analysis Report

Date: 11 August 2025

Analyst: Chandan Kumar

Tool Used: Wireshark (latest version)

1. Objective

The objective of this analysis was to capture live network traffic, filter it by protocol, and identify details about at least three different protocols in use.

2. Procedure

1. Installed Wireshark from the official website (https://www.wireshark.org/) and verified installation. 2. Opened Wireshark and selected the active network interface (Wi-Fi / Ethernet). 3. Clicked 'Start Capture'. 4. Opened a web browser and visited a sample website. 5. Performed a 'ping' command to an external server to generate ICMP traffic. 6. Stopped the capture after approximately 1 minute. 7. Applied filters: http, dns, and tcp. 8. Identified DNS, TCP, and ICMP packets among others. 9. Exported the capture as a .pcap file using 'File → Export Specified Packets'.

3. Findings

Protocol	Description	Example Packet Info
DNS	Domain Name System, used to resolve domain names to IP addresses	Standard query for a website domain
HTTP	HyperText Transfer Protocol, used for web browsing	HTTP GET request to a web page
TCP	Transmission Control Protocol, provides reliable communication	SYN, SYN-ACK, ACK handshake observed
ICMP	Internet Control Message Protocol, used for diagnostics	Echo request and echo reply from ping test

4. Packet Details Example

DNS Query Packet: - Frame Number: 15 - Query: Domain resolution request - Response: Domain resolution reply HTTP GET Packet: - Frame Number: 122 - Method: GET - Path: /index.html - Response Code: 200 OK ICMP Packet: - Frame Number: 65 - Type: Echo Request (Type 8) - Reply: Echo Reply (Type 0) - Round Trip Time: ~12 ms

5. Summary

Successfully captured and analyzed live network traffic. Identified multiple protocols in use: DNS, HTTP, TCP, ICMP. Observed DNS name resolution for visited websites, HTTP GET requests, TCP handshakes, and ICMP ping packets. The .pcap file has been exported for further offline analysis.