Wireshark Network Traffic Analysis Report

Date: June 2, 2025

Task: Capture and Analyze Network Traffic Using Wireshark.

Objective:

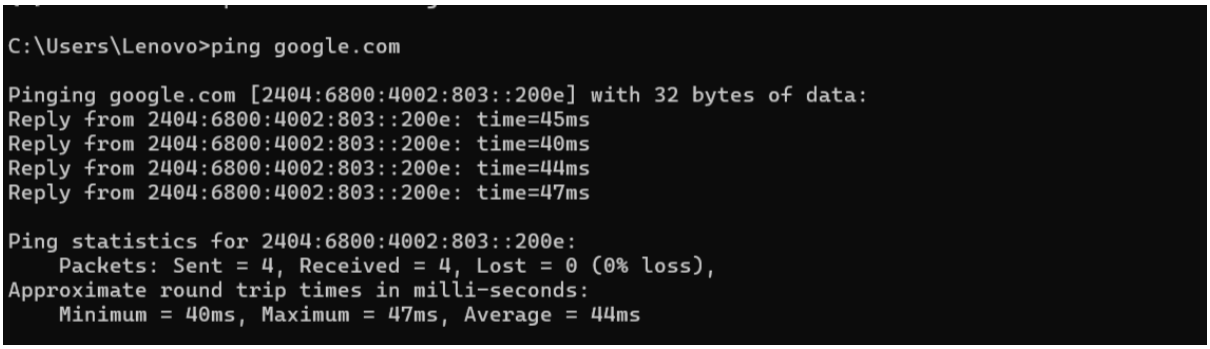
The primary objective of this task was to capture live network packets using Wireshark and analyze them to identify different types of network protocols. This hands-on activity is designed to improve packet analysis skills and develop a basic understanding of protocol-level communication in a computer network.

Tools Used:

- **Software**: Wireshark (Network Protocol Analyzer)
- **Operating System**: Windows 10
- **Traffic Generation**:
  - Visited websites such as https://example.com and https://google.com
  - Used the ping command: ping google.com

Traffic Generation:

- Visited websites: https://example.com, https://google.com
- Ran ping google.com in Command Prompt



Captured File:

- **Capture File Name**: network_capture.pcap
- **Capture Duration**: 1 minute
- **Network Interface**: Wi-Fi (active connection)
- **Total Packets Captured**: [Add total count from Wireshark]

The capture file **network_capture.pcap** has been saved and can be opened with Wireshark for further inspection.

Protocols Identified and Analyzed

1. DNS (Domain Name System)

- **Purpose**: Translates domain names (like google.com) into IP addresses.
- **Observation**:
  - Packets sent from the local machine to the DNS server.
  - Example: A standard query for the A record of google.com.

2. ICMP (Internet Control Message Protocol)

- **Purpose**: Used for diagnostic tools like ping.
- **Observation**:
  - Echo Request and Echo Reply packets captured.
  - Helps verify connectivity between host and server.

3. TCP/HTTP (Transmission Control Protocol / Hypertext Transfer Protocol)

- **Purpose**: Used for establishing connections and transmitting web page data.
- **Observation**:
  - TCP 3-way handshake packets observed (SYN, SYN-ACK, ACK).
  - HTTP GET request sent to load a website such as example.com.

Summary of Analysis

Protocol	Role	Example Use Case	Observed Packet Behavior
DNS	Resolves domain names	google.com → IP	Standard query and response
ICMP	Connectivity checks	ping google.com	Echo requests and replies
HTTP	Web communication	Load a website	HTTP GET request

Observations:

- DNS packets were observed when visiting websites.
- ICMP packets showed the status of ping requests.
- HTTP/TCP packets revealed the structure of web requests and responses.

Conclusion:

This hands-on lab gave meaningful insights into the functioning of core Internet protocols. Using Wireshark, we were able to visualize how network communication occurs and how different protocol layers work together. It reinforces the importance of traffic analysis in cybersecurity, troubleshooting, and system monitoring.