Wireshark Packet Analysis Project

Project Overview

This project demonstrates how to capture and analyze network packets using Wireshark. The goal was to capture live network traffic, filter for HTTP packets, and extract important details such as source/destination IPs and request methods.

Tools Used

- Wireshark

- Web Browser

Steps Taken

1. Installed Wireshark from https://www.wireshark.org/download.html.

2. Opened Wireshark and selected the active network interface (Wi-Fi/Ethernet).

3. Started capturing packets while visiting a sample website (example.com).

4. Applied a filter 'http' to view only HTTP packets.

5. Selected one packet for detailed analysis.

6. Expanded Ethernet, IP, TCP, and HTTP layers in the Packet Details pane.

7. Documented packet number, source/destination IPs, protocol, request method, and purpose.

Findings

- The analyzed packet was an HTTP GET request from my local machine to a target web server.

- The TCP handshake ensured a stable connection before data transfer.

What I Learned

- How to capture live network packets.

- How to filter traffic in Wireshark for specific protocols.

- How to interpret different layers of packet data.