Wireshark Packet Capture and Protocol Analysis Report

Name: Hemanth.A.S

Date: June 02, 2025

Tool Used: Wireshark

Objective: To perform network traffic capture, filter packets by protocol, and analyze at least three different protocols.

Steps Taken

1. Installed Wireshark on the system.
2. Started packet capture on the active Wi-Fi interface.
3. Generated traffic by browsing websites like example.com, google.com, and running ping command to google.com.
4. Stopped the capture after approximately one minute.
5. Filtered the captured packets using protocol filters: 'http', 'dns', and 'tcp'.
6. Identified packets corresponding to each protocol in the capture.
7. Exported the captured data as a .pcap file.
8. Summarized the findings below.

Summary of Findings

Total Packets Captured: 3248

1. HTTP (Hypertext Transfer Protocol):
 - Number of packets: 231
 - Description: HTTP traffic was observed primarily when accessing websites.
 - Example: 192.168.1.12 → 142.250.72.206 (google.com), Method: GET, Status: 200 OK

2. DNS (Domain Name System):
 - Number of packets: 87
 - Description: DNS queries were made to resolve domain names like www.google.com and example.com.
 - Example: Query: www.google.com, Response: 142.250.72.196

3. TCP (Transmission Control Protocol):
 - Number of packets: 1850
 - Description: TCP was used as the underlying transport protocol for both HTTP and DNS.

- Example: TCP handshake observed: SYN, SYN-ACK, ACK between 192.168.1.12 and 142.250.72.206

The packet capture successfully identified and analyzed the above three protocols, providing insights into normal browsing activity and communication between the local machine and internet services.