Name: Solanki Bhumirajsinh
Date: [16-12-2025]
Course/Subject: Computer Networks

Objective

The objective of this task is to capture live network packets using Wireshark and analyze them to identify basic protocols and traffic types. This exercise provides practical skills in packet analysis and network troubleshooting.

Tools Used

- Wireshark (Free Network Protocol Analyzer)

Procedure

1. Installed Wireshark on the system.
2. Selected the active network interface and started capturing packets.
3. Browsed websites and pinged a server to generate network traffic.
4. Captured packets for approximately one minute.
5. Applied protocol filters such as HTTP, DNS, and TCP to analyze specific traffic.
6. Exported the captured packets as a .pcap file for further analysis.

Protocols Identified

1. HTTP (Hypertext Transfer Protocol)

- Used for communication between web browsers and servers.
- Observed GET and POST requests while browsing websites.

2. DNS (Domain Name System)

- Resolves domain names to IP addresses.
- Captured queries and responses for visited domains.

3. TCP (Transmission Control Protocol)

- Ensures reliable transmission of data across networks.

- Observed multiple packet exchanges between the PC and servers.

Packet Analysis Summary

- Total captured packets: 300
- Majority of packets were TCP and HTTP.
- DNS packets showed queries and responses for accessed websites.
- HTTP packets contained request and response information for web pages.
- Wireshark allowed filtering, inspecting headers, and detailed packet analysis.

Conclusion

This task provided hands-on experience in capturing and analyzing network traffic. It enhanced understanding of network protocols, packet structures, and practical use of Wireshark for monitoring and troubleshooting network communication.