Wireshark Packet Analysis Report

This report documents the packet analysis task performed using Wireshark. The objective was to capture live network traffic, filter by different protocols, and analyze at least three protocols to understand how data flows across the network.

Steps Performed:

- Installed Wireshark on the system.
- Started capturing packets on the active network interface.
- Browsed a website and pinged a server to generate traffic.
- Stopped the capture after one minute.
- Filtered captured packets by protocol (HTTP, DNS, TCP).
- Identified at least 3 protocols in the capture: HTTP, DNS, TCP.
- Exported the capture as a .pcap file for documentation.
- Summarized findings and packet details.

Protocol Analysis:

Protocol	Description	Sample Observation
HTTP	Used for web communication	Captured GET request to a website
DNS	Resolves domain names to IP addresses	Observed DNS query for example.com
TCP	Reliable transport protocol	Captured SYN, ACK handshake packets

Summary:

The packet analysis successfully identified multiple protocols in the network traffic. HTTP was used for website communication, DNS resolved domain queries, and TCP handled reliable data transmission. This exercise provided hands-on experience with packet capturing and filtering in Wireshark.