Task 5: Network Traffic Capture and Analysis

Objective: Capture live network packets and identify basic protocols and traffic types using Wireshark.

Protocols Identified

The capture generated traffic using common internet activities (browsing, pinging) and successfully identified at least three different protocols:

Protocol	Layer	Key Function & Reliability	Packet Details Observed	Notable Observation
Domain Name System (DNS)	Application	Translates domain names to IP addresses (often uses UDP for speed).	Standard queries sent from the local machine and corresponding standard query responses containing the target IP address.	—
Transmission Control Protocol (TCP)	Transport	Provides **reliable**, connection-oriented delivery.	Identified by the **three-way handshake** (SYN, SYN-ACK, ACK).	Observed the three-way handshake sequence establishing a connection for web traffic.
Internet Control Message Protocol (ICMP)	Network	Sends control and error messages, such as the **Echo Request** and **Echo Reply** used by the ping utility.	Observed pairs of Echo Request and Echo Reply packets confirming network connectivity to a remote server.	—

Outcome

The task was completed successfully, providing hands-on experience with packet analysis, filtering techniques in Wireshark, and protocol awareness.