Wireshark Network Traffic Analysis Report

Task Objective

Capture and analyze live network traffic using Wireshark on macOS to identify basic internet communication protocols.

Steps Performed

1. Opened Wireshark and selected the active network interface: Wi-Fi (en0)
2. Started live packet capture
3. Visited several websites and used ping google.com to generate traffic
4. Stopped the capture after approximately one minute
5. Applied filters to identify protocols such as DNS, TCP, and HTTPS
6. Saved the capture file as: networktrafficanalysis.pcapng

Protocols Identified

Protocol	Description	Observation
DNS	Resolves domain names to IP addresses.	Queries to google.com
TCP	Ensures reliable data transmission.	Connection setup (SYN, ACK) packets observed.
HTTPS	Secure web communication using TLS.	Encrypted packets while browsing websites.

Summary of Findings

• DNS packets revealed the hostname lookups performed by my system
• TCP connections established communication channels for web browsing
• HTTPS packets carried encrypted web traffic, showing secure connections to websites
• This experiment demonstrated the flow of data across multiple layers of the TCP/IP model and provided insights into how everyday web activity appears at the packet level

Outcome

Developed hands-on skills in:

• Packet capturing using Wireshark
• Applying protocol filters
• Understanding different layers of the TCP/IP model
• Analyzing and interpreting real network communication

Files Included

• networktrafficanalysis.pcapng - Captured traffic file
• Wireshark_Network_Traffic_Analysis_Report.pdf - Summary of analysis