Network Traffic Capture and Analysis Report

# Objective

Capture live packets using Wireshark, identify network protocols, and understand basic traffic patterns.

# Tools Used

• Wireshark   
• Active Network Interface -Wi-Fi  
• Web Browser

# Process

1. Installed and launched Wireshark.  
2. Captured live packets on the active Wi-Fi interface for ~1 minute.  
3. Generated traffic by browsing websites and pinging a server.  
4. Stopped the capture and applied filters (HTTP, DNS, TCP).  
5. Exported capture as a .pcap file.

# Findings

The following protocols were identified in the capture:

• DNS – Domain name resolution queries (A/AAAA requests).

• HTTP/HTTPS – Web browsing traffic (GET requests, TLS handshake).

• TCP – Reliable transport layer communication (SYN, ACK, FIN packets).

• ICMP (optional) – Ping request/reply packets.

# Conclusion

The capture and analysis were successfully completed. Multiple protocols were identified, confirming understanding of how applications use transport and network services for communication.

# Browsed github.com

