Wireshark Traffic Capture and Protocol Analysis Summary

# 1. Objective

The purpose of this activity was to capture and analyze network traffic using Wireshark, identify various protocols in use, and summarize key findings based on observed packets.

# 2. Tools Used

- Wireshark Network Protocol Analyzer  
- Web Browser (Chrome/Edge)  
- Command Prompt (Ping Utility)

# 3. Steps Performed

1. Wireshark Installation: Wireshark was successfully installed on the system.  
2. Capture Initiated: Packet capture was started on the active network interface (e.g., Ethernet/Wi-Fi).  
3. Traffic Generation:  
 - A website (e.g., www.example.com) was visited.  
 - A ping request was sent to 8.8.8.8 (Google DNS server).  
4. Capture Stopped: After approximately one minute of traffic generation, the capture was stopped.  
5. Filtering: Protocol filters such as http, dns, and tcp were used to isolate relevant traffic.  
6. Protocol Identification: At least three different protocols were observed and analyzed.

# 4. Protocols Identified

|  |  |  |
| --- | --- | --- |
| Protocol | Description | Purpose |
| HTTP | Hypertext Transfer Protocol | Used for browsing websites. Observed several GET/POST requests. |
| DNS | Domain Name System | Used for resolving domain names. Multiple DNS queries/responses captured. |
| TCP | Transmission Control Protocol | Observed as the underlying transport for HTTP and other protocols. SYN, ACK, and FIN flags noted. |

# 5. Export

The capture file was exported in .pcap format for archival and further analysis.

# 6. Key Findings

- Network communication primarily occurred over TCP and involved DNS name resolution.  
- The HTTP protocol was used when accessing the website, showing clear GET/POST traffic.  
- Multiple DNS queries were sent to resolve domain names used during web browsing.  
- The TCP handshake and teardown processes were clearly visible in the capture.  
- No suspicious traffic was identified during this short session.

# 7. Conclusion

This Wireshark session successfully demonstrated how to capture, filter, and analyze network traffic. Identifying and understanding the interaction between DNS, TCP, and HTTP protocols provided insights into standard internet communications.