**Objective**

Capture live network packets, identify protocols, and summarize findings using Wireshark.

**Tools Used**

* **Wireshark** – Packet analyzer
* **Command Prompt** – Ping test
* **Web Browser** – To generate network traffic

**Steps Performed**

1. Installed Wireshark on the system.
2. Started packet capture on the active Wi-Fi interface.
3. Generated network traffic by:
   * Browsing google.com
   * Running ping google.com in Command Prompt
4. Stopped capture after ~1 minute.
5. Filtered packets by protocol: dns, tcp, udp, tls, ssdp, mdns.
6. Identified multiple protocols: TCP, UDP, DNS, TLS/SSL, SSDP, mDNS.

Ping Test Results

Pinging google.com [142.250.77.142] with 32 bytes of data:

Reply from 142.250.77.142: bytes=32 time=163ms TTL=117

Reply from 142.250.77.142: bytes=32 time=643ms TTL=117

Reply from 142.250.77.142: bytes=32 time=387ms TTL=117

Reply from 142.250.77.142: bytes=32 time=283ms TTL=117

Ping statistics:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Round-trip times: Minimum = 163ms, Maximum = 643ms, Average = 369ms

**Protocol Analysis**

| **Protocol** | **Purpose** | **Observation** |
| --- | --- | --- |
| **DNS** | Domain name resolution | Queries and responses observed |
| **TCP** | Reliable transport | Three-way handshake and ACKs observed |
| **UDP** | Fast, connectionless transport | Traffic for DNS, mDNS, SSDP observed |
| **TLS/SSL** | Encrypts HTTPS traffic | Client Hello and Server Hello observed |
| **SSDP** | UPnP service discovery | NOTIFY and M-SEARCH messages observed |
| **mDNS** | Local network discovery | Multicast queries/responses on UDP 5353 observed |

**Conclusion**

* Successfully captured and analyzed live network traffic.
* Multiple protocols identified (TCP, UDP, DNS, TLS, SSDP, mDNS).
* DNS resolution and TLS encryption verified.
* Ping test confirms stable connectivity with no packet loss.