Task-5

Ques-Capture and AnalStep 1: Install Wireshark.

Step 1: Install Wireshark.

**Step 2: Start a Packet Capture**

* Open Wireshark.
* Select your active network interface (usually Wi-Fi or Ethernet).
* Click the blue **shark fin icon** to start capturing.

Step 3: Generate Some Network Traffic.

Step 4: Stop the Capture

**Step 5: Apply Protocol Filters**

Use the filter bar to analyze specific protocols:

* http – for web traffic
* dns – for domain name system lookups
* icmp – for ping (Internet Control Message Protocol)
* tcp – for general TCP traffic
* udp – for UDP traffic

**Step 6: Identify at Least 3 Different Protocols**

* You should see some or all of these in your capture:
* **DNS** (domain lookups)
* **HTTP/HTTPS** (web browsing)
* **TCP** (underlying transport for many protocols)
* **ICMP** (from ping command)
* **TLS** (used in HTTPS)
* **Step 7: Export the Capture as a .pcap File**
* Go to **File → Save As**
* Choose the format **Wireshark/tcpdump/... .pcap**
* Name your file (e.g., my\_traffic\_capture.pcap) and save.

