Task 5. Capture and Analyze Network Traffic Using Wireshark.

1. Install Wireshark

- Download from: https://www.wireshark.org/
- Follow the installation instructions.
- Allow installation of **WinPcap/Npcap** (needed for packet capture).

---

2. Start Capturing Traffic

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

---

3. Generate Network Traffic

While Wireshark is capturing:

- Open a web browser and visit a few websites (e.g., https://example.com).
- Open a terminal/command prompt and type:- ping google.com
-

4. Stop Capture

- After 1 minute, click the **red square stop button**.

---

5. Filter by Protocol

- Use the **Display Filter bar** to filter specific protocols:
  - `http` – for web traffic
  - `dns` – for domain lookups
  - `tcp` – for general transport layer data
  - `icmp` – for ping requests

---

6. Identify At Least 3 Protocols

Look at the “Protocol” column and identify any 3 distinct ones. Common ones include:

- HTTP

- TCP
- DNS
- ICMP
- TLS
- ARP

---

7. Export as .pcap

- Go to `File` > `Save As`
- Save your capture with a name like: `internship_capture.pcap`

---

8. Summarize Your Findings

Here's a **sample summary** format:

🔍 Summary of Packet Capture

Capture Duration: 1 minute
Network Interface: Wi-Fi
File Name: `internship_capture.pcap`

📡 Identified Protocols:

1. **HTTP**
    - Used for communication between browser and websites.
    - Example: GET request to example.com
2. **DNS**
    - Resolves domain names to IP addresses.
    - Example: DNS query for `google.com`
3. **TCP**
    - Underlying transport protocol for HTTP and other services.
    - Example: TCP handshake between local machine and 142.250.64.110

📄 Interesting Packet Details:

Protocol	Source IP	Destination IP	Info
DNS	192.168.1.5	8.8.8.8	Standard query A google.com
HTTP	192.168.1.5	93.184.216.34	GET /index.html

Protocol	Source IP	Destination IP	Info
TCP	192.168.1.5	142.250.64.110	TCP SYN, ACK handshake