Task 5

Capture and Analyze Network Traffic Using Wireshark

Objective:

Capture live network packets and identify basic protocols and traffic types using Wireshark.

Tools Used:

- Kali Linux
- Wireshark

Steps Performed:

1. Installed Wireshark

- Verified Wireshark installation on Kali Linux with:

```
 >> sudo apt update
       sudo apt install wireshark\
```

2. Started Wireshark with root privileges

- Launched Wireshark to avoid permission issues:

```
>> sudo wireshark
```

3. Selected active network interface

- Selected the Wi-Fi interface (wlan0) for packet capturing.

4. Captured live traffic

- Started packet capture on the selected interface.
- Generated network traffic by pinging google.com:

```
>> ping -c 5 google.com
```

5. Stopped the capture

- After sufficient traffic was captured (about one minute), stopped the packet capture in Wireshark.

6. Filtered captured packets by protocol

- Applied filters to analyze specific protocols in the captured traffic:
    - icmp — to view ping packets.
    - dns — to view domain name lookup packets.
    - tcp — to view connection-oriented packets.
    - http — to view web traffic (if any browsing was done).

7. Exported the capture file

- Saved the captured data as a .pcap file named capture.pcap via:
    - **File > Save As** in Wireshark.

Protocols Identified:

- **ICMP (Internet Control Message Protocol):**
  Used by the ping command to send echo requests and receive echo replies, confirming network connectivity.
- **DNS (Domain Name System):**
  Translates domain names (e.g., google.com) into IP addresses, enabling the system to locate servers on the network.
- **TCP (Transmission Control Protocol):**
  Manages reliable, connection-oriented communication between devices, including connection establishment and termination.

Observations:

- The ping command generated ICMP packets showing successful communication with google.com's IP address.
- DNS queries were observed resolving domain names to IP addresses before pinging.
- TCP packets were visible as part of underlying communication protocols during browsing or other network activity.