install Wireshark by running:

```
sudo apt install wireshark
```

Open Wireshark:

- Type this in the terminal:

```
Wireshark
```

Select the Network Interface:

- In Wireshark, you will see a list of network interfaces. Choose the one that corresponds to the interface you're using (for example, eth0 for Ethernet or wlan0 for Wi-Fi).
- Double-click the interface to start capturing packets.

(or open new terminal , write “ip a” to see if its eth0,wlan0, etc)

Step 2: Open Another Terminal for tcpdump

1. **Open a new Terminal window** (you can use Ctrl + Alt + T to open a new terminal).

Run tcpdump in this new terminal. For example, to capture packets on a specific interface, use:

```
sudo tcpdump -i interface
```

Step 3: Analyze Traffic in Wireshark

- **View the captured packets** in Wireshark. Since you started capturing packets from Wireshark, you should see live traffic displayed in real-time.

Basic Commands

1. **Capture Packets on a Specific Interface**:

```
sudo tcpdump -i eth0
```

Capture Packets with a Specific Protocol (e.g., TCP):

```
sudo tcpdump -i eth0 tcp
```

Capture Only UDP Packets:

```
sudo tcpdump -i eth0 udp
```

Capture Packets from a Specific Host:

```
sudo tcpdump -i eth0 host 192.168.1.10
```

Capture Traffic on a Specific Port (e.g., HTTP on port 80):

```
sudo tcpdump -i eth0 port 80
```