Step 1: Install and Setup Wireshark

1. Download Wireshark from https://www.wireshark.org.
2. Install it with the default options.
3. Open Wireshark and select your **wired network interface (Ethernet / LAN)**.

   If you're using Wi-Fi, choose the **Wireless LAN** interface instead.

Step 2: Capture Packets

1. Click **Start Capture** on your network interface.
2. Perform some activities on your Intranet (open a website hosted inside, ping a machine, transfer a file).
3. Stop the capture after you have enough packets.

Step 3: Filter Packets

Wireshark lets you filter by protocol:

- Ethernet frames: `eth`
- IP packets: `ip`
- TCP packets: `tcp`
- UDP packets: `udp`

Example:

- Use `tcp` to see only TCP traffic.
- Use `udp` to see only UDP traffic.

Step 4: Analyze Packet Formats

Click on any packet → Expand different layers in the middle panel.
You will see the protocol stack:

1. **Ethernet II (Data Link Layer)**
   - Destination MAC Address
   - Source MAC Address
   - Type (e.g., IPv4 = 0x0800)
2. **Internet Protocol (IP) (Network Layer)**
   - Version (IPv4 / IPv6)
   - Header Length
   - Source IP Address

- Destination IP Address
- TTL (Time to Live)
- Protocol (6 = TCP, 17 = UDP)

3. **Transmission Control Protocol (TCP) (Transport Layer)**
   - Source Port
   - Destination Port
   - Sequence Number
   - Acknowledgment Number
   - Flags (SYN, ACK, FIN, etc.)
   - Window Size

   or

   User Datagram Protocol (UDP)

   - Source Port
   - Destination Port
   - Length
   - Checksum

Step 5: Compare TCP vs UDP

- TCP has extra fields like sequence/ack numbers, flags (reliable, connection-oriented).
- UDP has only source/destination ports, length, checksum (faster, connectionless).

Step 6: Export or Document

- Right-click → "Export Packet Dissections → As Plain Text" to include in your report.
- Or take screenshots of packet details (Ethernet + IP + TCP/UDP headers).

ip.addr ==142.250.192.133