Assignment-6:Wireshark

Aim: To Install wireshark and perform analysis of Packet heaIP

Theory:

Wireshark is a network protocol analyzer that allows us to capture and inspect packets flowing through a network. When analyzing a packet, Wireshark displays information at various layers of the OSI model. Here's how packet header analysis typically proceeds:

1. Frame Layer (Physical + Data Link Layer)

This is the raw capture metadata. It shows the total number of bytes transmitted, the network interface that captured the packet, and the length of the captured data.

2. Ethernet Header (Data Link Layer)

The Ethernet header includes:

- Source MAC address: Identifies the sender's hardware address.
- Destination MAC address: Identifies the receiver's hardware address.
- EtherType: Indicates the next protocol layer (e.g., IPv4 or IPv6).

3. IP Header (Network Layer)

If the packet uses IPv6, the header contains:

- Source IP address: The IPv6 address of the sender.
- Destination IP address: The IPv6 address of the receiver.
- Traffic class, flow label, payload length, next header type, and hop limit.

4. Transport Layer Header

If the protocol used is UDP (User Datagram Protocol), this header will include:

- Source port: The port number on the sender's side.
- Destination port: The port number on the receiver's side.
- Length and checksum: Used for error checking and ensuring data integrity.

5. Data/Payload

The payload contains the actual data being transmitted. For encrypted or compressed traffic, the contents might not be human-readable.

Steps:

For windows:

1. Go to wireshark.org.
2. Click the Download button.
3. Select Windows Installer (64-bit).
4. Run the downloaded .exe file.
5. Follow the installation wizard.
6. Install Npcap when prompted.
7. Finish setup and launch Wireshark.

For linux:

1. Open Terminal
2. Update package list:

```
sudo apt update
```

3. Install Wireshark:

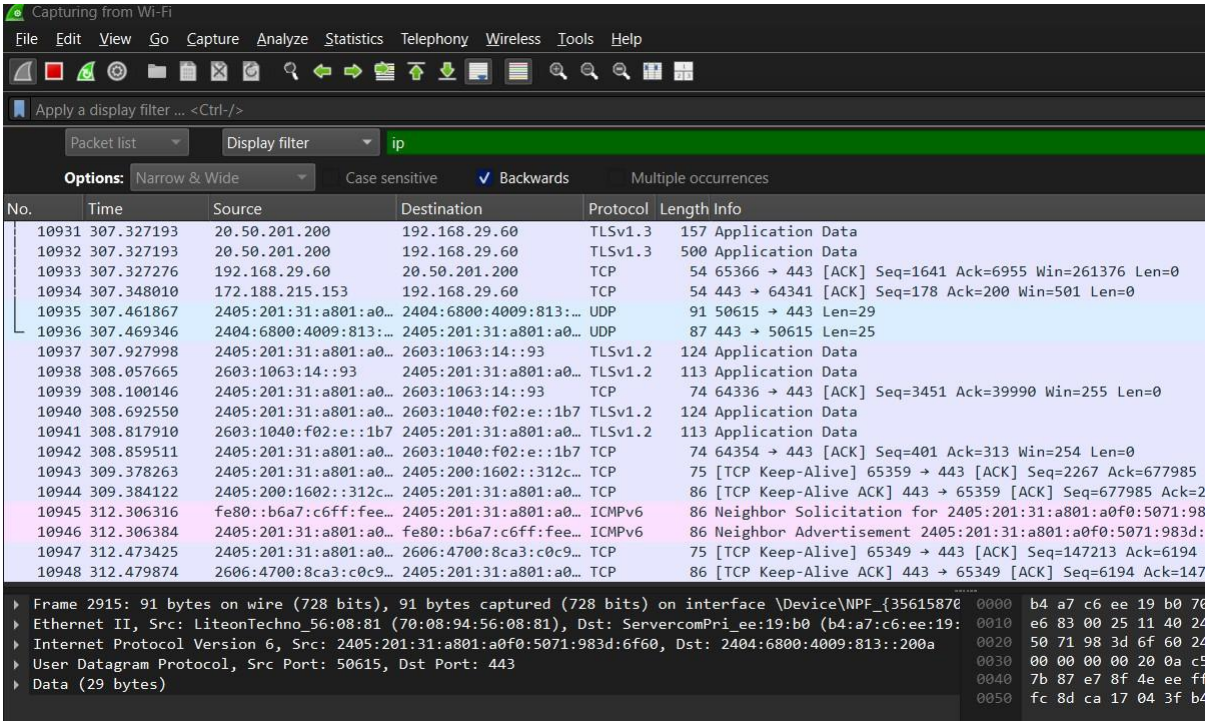
```
sudo apt install wireshark
```

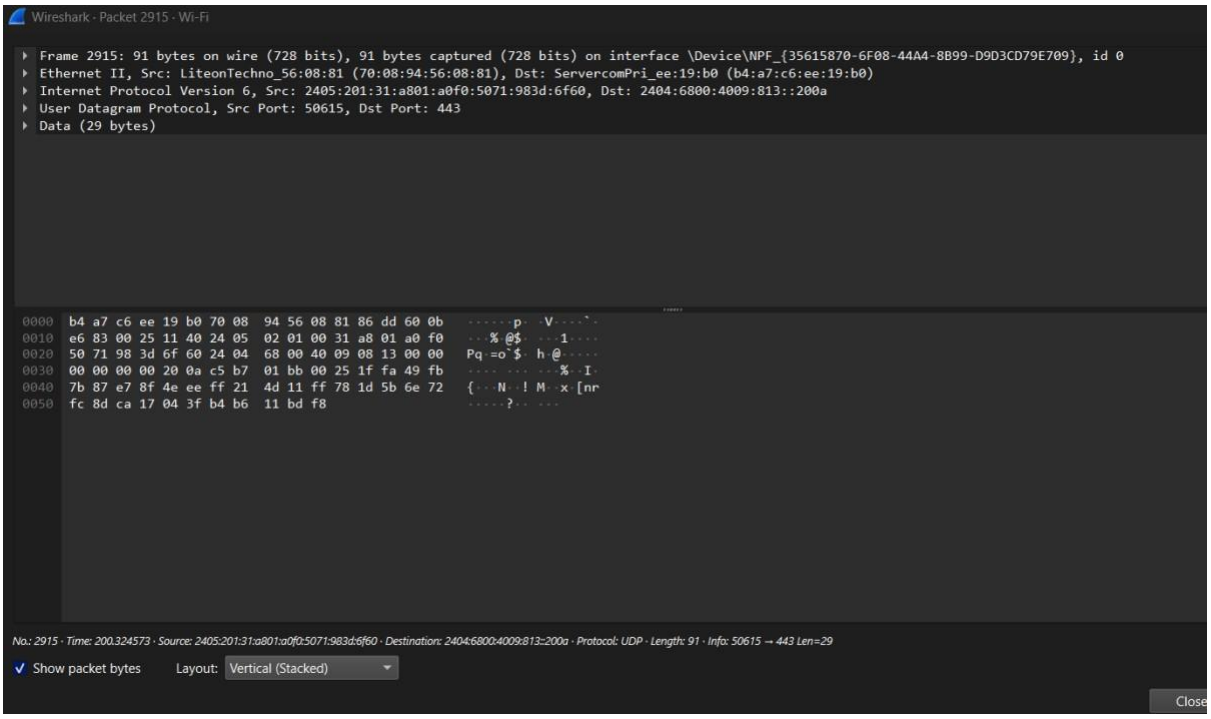
4. Allow non-root users to capture packets (optional but recommended):

```
sudo dpkg-reconfigure wireshark-common
sudo usermod -aG wireshark $USER
```

5. Reboot or log out and log back in.

Analysis of Packet:





Conclusion: Thus we have installed and performed analysis in Wireshark.