

Assignment-6:Wireshark

Aim: To Install wireshark and perform analysis of Packet healP

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](https://www.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`

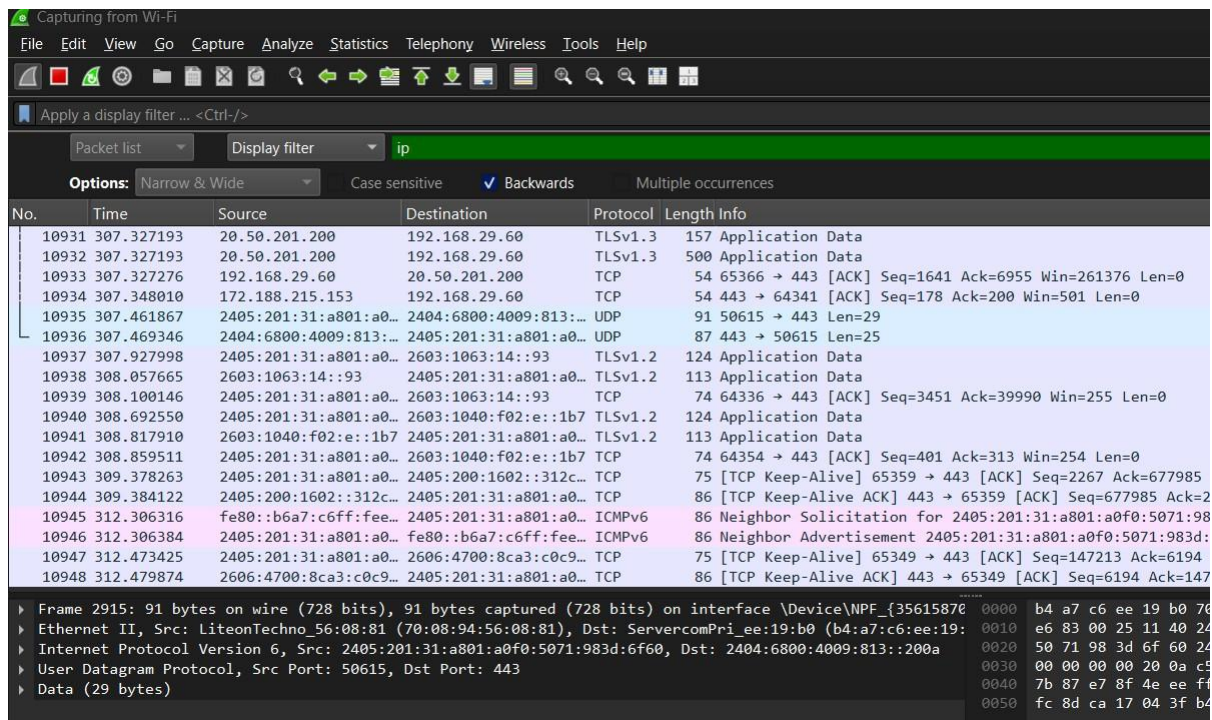
4. Allow non-root users to capture packets (optional but recommended):

`sudo dpkg-reconfigure wireshark-common`

`sudo usermod -aG wireshark $USER`

5. Reboot or log out and log back in.

Analysis of Packet:



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet list Display filter ip

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Info
10931	307.327193	20.50.201.200	192.168.29.60	TLSv1.3	157	Application Data
10932	307.327193	20.50.201.200	192.168.29.60	TLSv1.3	500	Application Data
10933	307.327276	192.168.29.60	20.50.201.200	TCP	54	65366 → 443 [ACK] Seq=1641 Ack=6955 Win=261376 Len=0
10934	307.348010	172.188.215.153	192.168.29.60	TCP	54	443 → 64341 [ACK] Seq=178 Ack=200 Win=501 Len=0
10935	307.461867	2405:201:31:a801:a0...	2404:6800:4009:813:...	UDP	91	50615 → 443 Len=29
10936	307.469346	2404:6800:4009:813:...	2405:201:31:a801:a0...	UDP	87	443 → 50615 Len=25
10937	307.927998	2405:201:31:a801:a0...	2603:1063:14::93	TLSv1.2	124	Application Data
10938	308.057665	2603:1063:14::93	2405:201:31:a801:a0...	TLSv1.2	113	Application Data
10939	308.100146	2405:201:31:a801:a0...	2603:1063:14::93	TCP	74	64336 → 443 [ACK] Seq=3451 Ack=39990 Win=255 Len=0
10940	308.692550	2405:201:31:a801:a0...	2603:1040:f02:e::1b7	TLSv1.2	124	Application Data
10941	308.817910	2603:1040:f02:e::1b7	2405:201:31:a801:a0...	TLSv1.2	113	Application Data
10942	308.859511	2405:201:31:a801:a0...	2603:1040:f02:e::1b7	TCP	74	64354 → 443 [ACK] Seq=401 Ack=313 Win=254 Len=0
10943	309.378263	2405:201:31:a801:a0...	2405:200:1602::312c...	TCP	75	[TCP Keep-Alive] 65359 → 443 [ACK] Seq=2267 Ack=677985
10944	309.384122	2405:200:1602::312c...	2405:201:31:a801:a0...	TCP	86	[TCP Keep-Alive ACK] 443 → 65359 [ACK] Seq=677985 Ack=2
10945	312.306316	fe80::b6a7:c6ff:fee...	2405:201:31:a801:a0...	ICMPv6	86	Neighbor Solicitation for 2405:201:31:a801:a0f0:5071:98
10946	312.306384	2405:201:31:a801:a0...	fe80::b6a7:c6ff:fee...	ICMPv6	86	Neighbor Advertisement 2405:201:31:a801:a0f0:5071:983d:
10947	312.473425	2405:201:31:a801:a0...	2606:4700:8ca3:c0c9...	TCP	75	[TCP Keep-Alive] 65349 → 443 [ACK] Seq=147213 Ack=6194
10948	312.479874	2606:4700:8ca3:c0c9...	2405:201:31:a801:a0...	TCP	86	[TCP Keep-Alive ACK] 443 → 65349 [ACK] Seq=6194 Ack=147

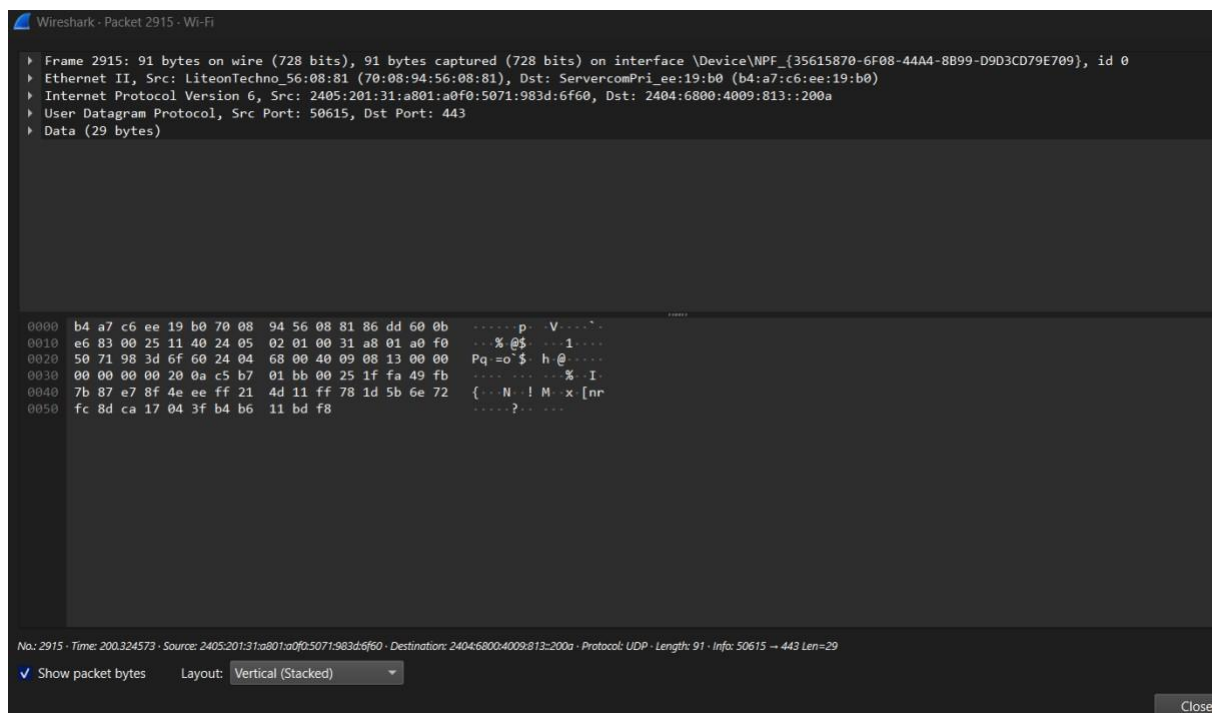
Frame 2915: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{35615870-6F08-44A4-8B99-D903CD79E709}, id 0

Ethernet II, Src: LiteonTechno_56:08:81 (70:08:94:56:08:81), Dst: ServercomPri_ee:19:b0 (b4:a7:c6:ee:19:b0)

Internet Protocol Version 6, Src: 2405:201:31:a801:a0f0:5071:983d:6f60, Dst: 2404:6800:4009:813::200a

User Datagram Protocol, Src Port: 50615, Dst Port: 443

Data (29 bytes)



Wireshark - Packet 2915 - Wi-Fi

Frame 2915: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{35615870-6F08-44A4-8B99-D903CD79E709}, id 0

Ethernet II, Src: LiteonTechno_56:08:81 (70:08:94:56:08:81), Dst: ServercomPri_ee:19:b0 (b4:a7:c6:ee:19:b0)

Internet Protocol Version 6, Src: 2405:201:31:a801:a0f0:5071:983d:6f60, Dst: 2404:6800:4009:813::200a

User Datagram Protocol, Src Port: 50615, Dst Port: 443

Data (29 bytes)

0000 b4 a7 c6 ee 19 b0 70 08 94 56 08 81 86 dd 60 0bp..V.....
0010 e6 83 00 25 11 40 24 05 02 01 00 31 a8 01 a0 f0 ...%@\$...1....
0020 50 71 98 3d 6f 60 24 04 68 00 40 09 08 13 00 00 Pq=0\$ h@.....
0030 00 00 00 00 20 0a c5 b7 01 bb 00 25 1f fa 49 fb%..I..
0040 7b 87 e7 8f 4e ee ff 21 4d 11 ff 78 1d 5b 6e 72 {...N..!M..x[nr
0050 fc 8d ca 17 04 3f b4 b6 11 bd f8?.....

No: 2915 - Time: 200.324573 - Source: 2405:201:31:a801:a0f0:5071:983d:6f60 - Destination: 2404:6800:4009:813::200a - Protocol: UDP - Length: 91 - Info: 50615 → 443 Len=29

Show packet bytes Layout: Vertical (Stacked)

Close

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