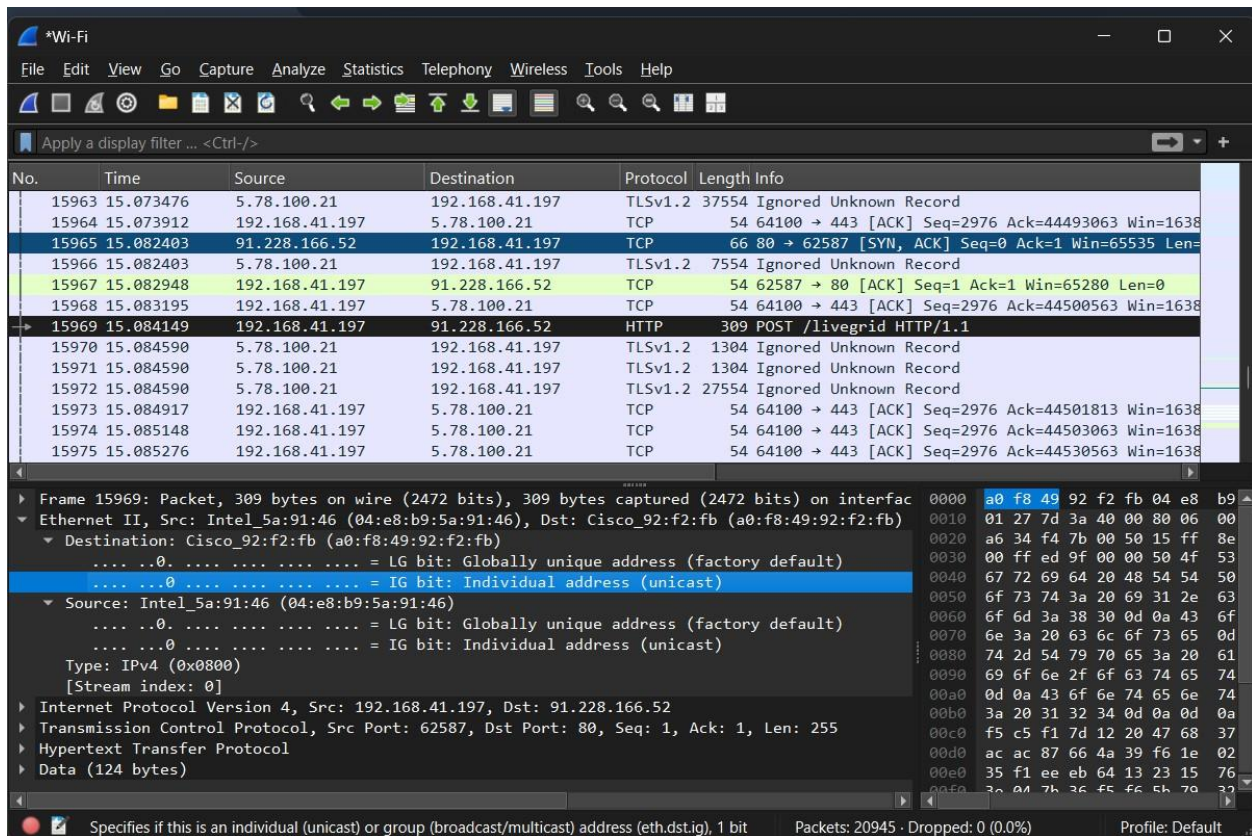


Lab Assignment – 02
Name:-Kumar Suryanshu
Roll No.:-2024IMG-026

Assignment – Packet Sniffing and Packet Analysis Using Wireshark: Physical layer and DLL

Task A: Packet Sniffing at Data Link Layer & Physical Layer



Source MAC address : 04:e8:b9:5a:91:46
Destination MAC address : a0:f8:49:92:f2:fb
Ether Type field : 0x0800
Frame Length: 309 bytes

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

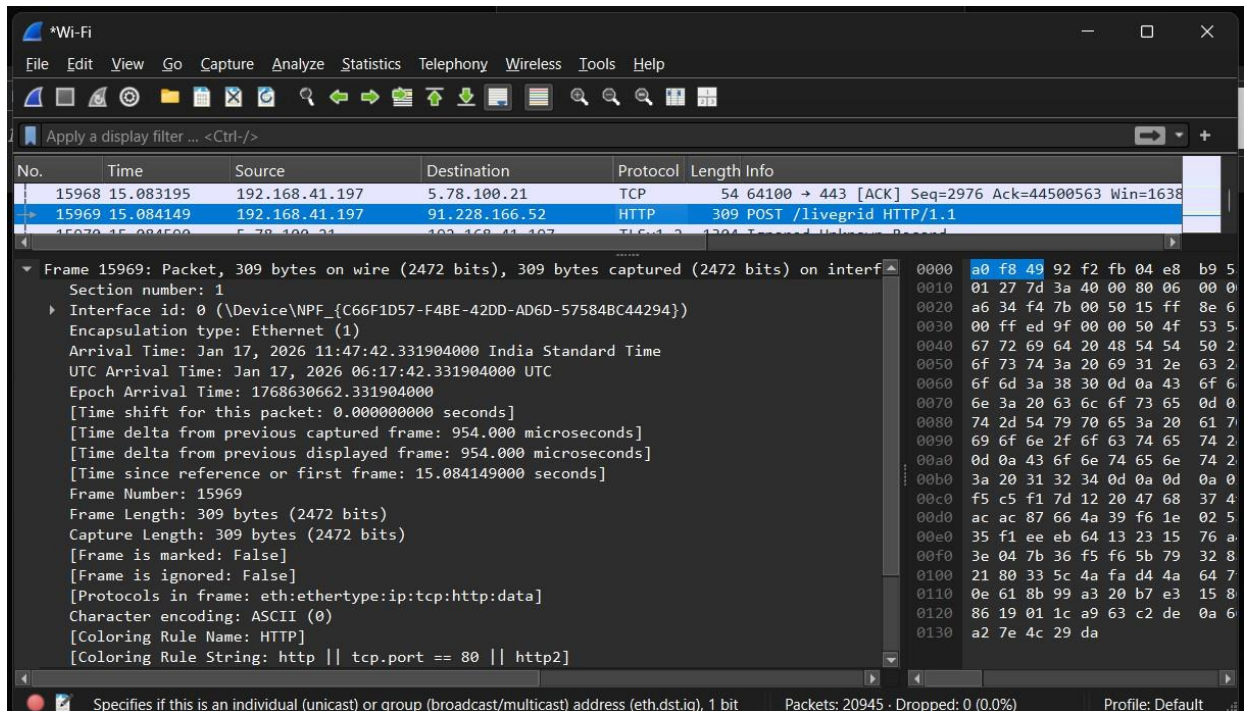
Packet List: Displays a list of captured packets. The selected packet is frame 5570, which is an ARP probe from source fe80::41d1:6d79:75f1:95fa to destination ff02::1. The packet length is 60 bytes.

Packet Details: Shows the hierarchical structure of the selected packet. The Ethernet II header is expanded, showing the source address (fe80::41d1:6d79:75f1:95fa) and the destination address (ff02::1). The ARP header is also visible, showing the operation type (0x0006) and the stream index (8).

Packet Bytes: Displays the raw data of the selected packet in hexadecimal and ASCII. The data starts with ff ff ff ff ff ff ff b8 1e a4 b...

Status Bar: At the bottom, the status bar indicates the current filter is 'Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit'. It also shows the number of packets (20945) and dropped packets (0).

Task C: Physical Layer Analysis



Observe **Frame Length** (in bytes) : 309 bytes

Analyze:

- Bit rate (from interface statistics) : 23Mbps
- Transmission medium (Ethernet/Wi-Fi) : The physical medium is Wi-Fi, but the logical frame format is Ethernet II.
- Frame arrival time and inter-frame delay:
Arrival Time : Jan 17, 2026 11:47:42.33190400
Inter-frame Delay: 954.000 microseconds

Question:

You are provided with a system connected to a LAN/Wi-Fi network. Using **Wireshark**, capture live network traffic and analyse packets at the **Data Link Layer** and **Physical Layer**.

Activity 1: (A) Ethernet Frame Analysis Data Link Layer Capture packets on the active network interface.

- Select any one **Ethernet frame** and record the following details:
- Source MAC Address : 04:e8:b9:5a:91:46
- Destination MAC Address : a0:f8:49:92:f2:fb
- Ether Type Field : 0x0800
- Frame Length (in bytes) : 309 bytes

a) Identify whether the destination MAC address is **unicast or broadcast**.

➔ The Destination MAC address for broadcast must be **ff:ff:ff:ff:ff:ff** but the Destination MAC address is not **ff:ff:ff:ff:ff:ff**; it specifies a particular device here hence Destination MAC address is a **unicast**.

b) State the protocol indicated by the Ether Type field.

➔ **IPv4**

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 15969 is selected, showing it is an HTTP POST request from 192.168.41.197 to 91.228.166.52. The bottom pane shows the detailed view of the selected packet, starting with the Ethernet II header. The Destination MAC address is a0:f8:49:92:f2:fb, and the Source MAC address is 04:e8:b9:5a:91:46. The Ether Type field is 0x0800, indicating an IPv4 payload. The packet length is 309 bytes. The right pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
15963	15.073476	5.78.100.21	192.168.41.197	TLSv1.2	37554	Ignored Unknown Record
15964	15.073912	192.168.41.197	5.78.100.21	TCP	54	64100 → 443 [ACK] Seq=2976 Ack=44493063 Win=1638
15965	15.082403	91.228.166.52	192.168.41.197	TCP	66	80 → 62587 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
15966	15.082403	5.78.100.21	192.168.41.197	TLSv1.2	7554	Ignored Unknown Record
15967	15.082948	192.168.41.197	91.228.166.52	TCP	54	62587 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
15968	15.083195	192.168.41.197	5.78.100.21	TCP	54	64100 → 443 [ACK] Seq=2976 Ack=44500563 Win=1638
15969	15.084149	192.168.41.197	91.228.166.52	HTTP	309	POST /livegrid HTTP/1.1
15970	15.084590	5.78.100.21	192.168.41.197	TLSv1.2	1304	Ignored Unknown Record
15971	15.084590	5.78.100.21	192.168.41.197	TLSv1.2	1304	Ignored Unknown Record
15972	15.084590	5.78.100.21	192.168.41.197	TLSv1.2	27554	Ignored Unknown Record
15973	15.084917	192.168.41.197	5.78.100.21	TCP	54	64100 → 443 [ACK] Seq=2976 Ack=44501813 Win=1638

Frame 15969: Packet, 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits) on interf...

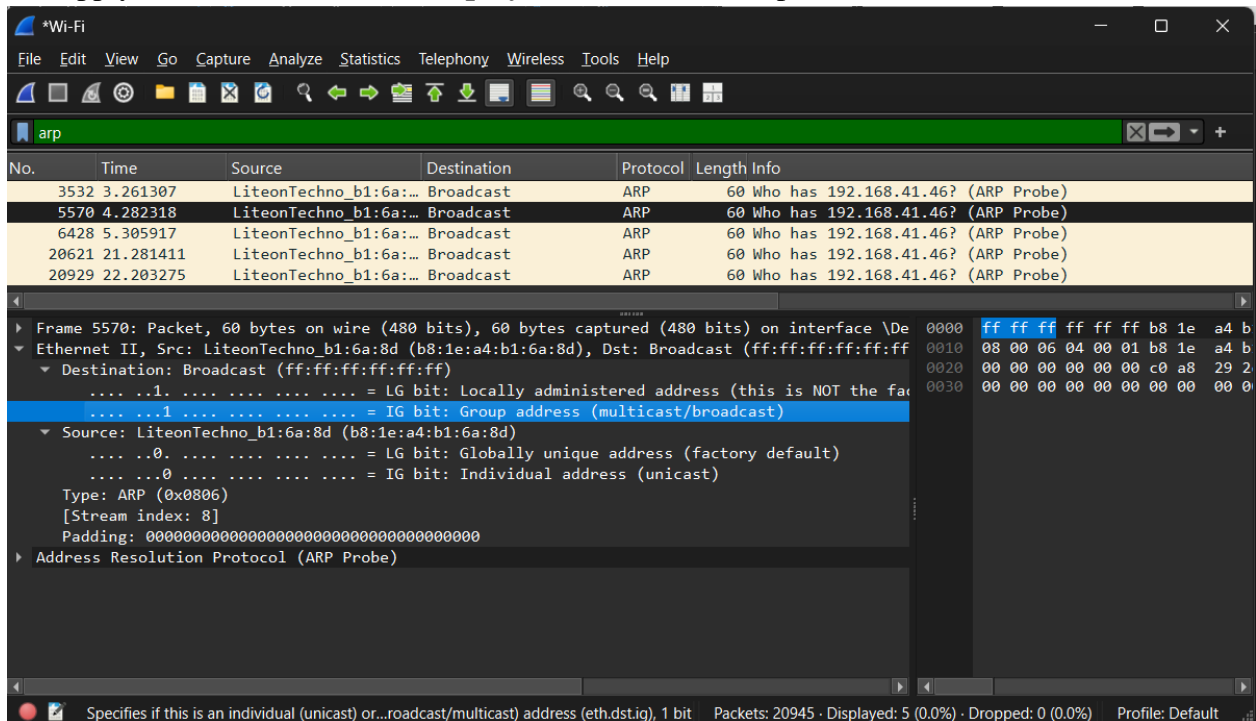
Ethernet II, Src: Intel_5a:91:46 (04:e8:b9:5a:91:46), Dst: Cisco_92:f2:fb (a0:f8:49:92:f2:fb)

- Destination: Cisco_92:f2:fb (a0:f8:49:92:f2:fb)
 - = LG bit: Globally unique address (factory default)
 - = LG bit: Individual address (unicast)
- Source: Intel_5a:91:46 (04:e8:b9:5a:91:46)
 - = LG bit: Globally unique address (factory default)
 - = LG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.41.197, Dst: 91.228.166.52
- Transmission Control Protocol, Src Port: 62587, Dst Port: 80, Seq: 1, Ack: 1, Len: 255
- Hypertext Transfer Protocol

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit Packets: 20945 · Dropped: 0 (0.0%) Profile: Default

Activity 2: (B) ARP Packet Observation

1. Apply a suitable **Wireshark display filter** to view ARP packets.



2. Select one **ARP Request** and one **ARP Reply** packet and record:

- Sender IP and MAC address: b8:1e:a4:b1:6a:8d
- Target IP and MAC address: ff:ff:ff:ff:ff:ff

3. Explain the role of **ARP** in local area network communication.

- ➔ ARP's role is to map devices logical IP addresses to its physical MAC addresses; allowing devices to find each other and send data frames directly on the same local network by broadcasting a request for the IP's MAC and receiving a direct reply to update its internal cache, ensuring efficient, targeted communication.