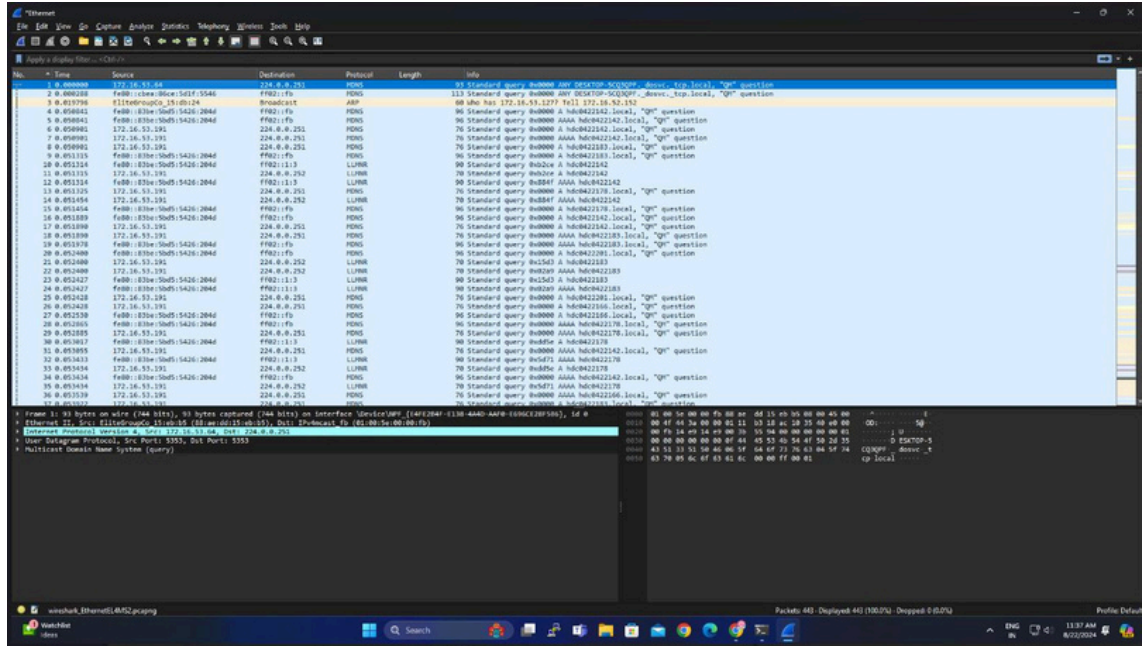


# EXPERIMENT – 5

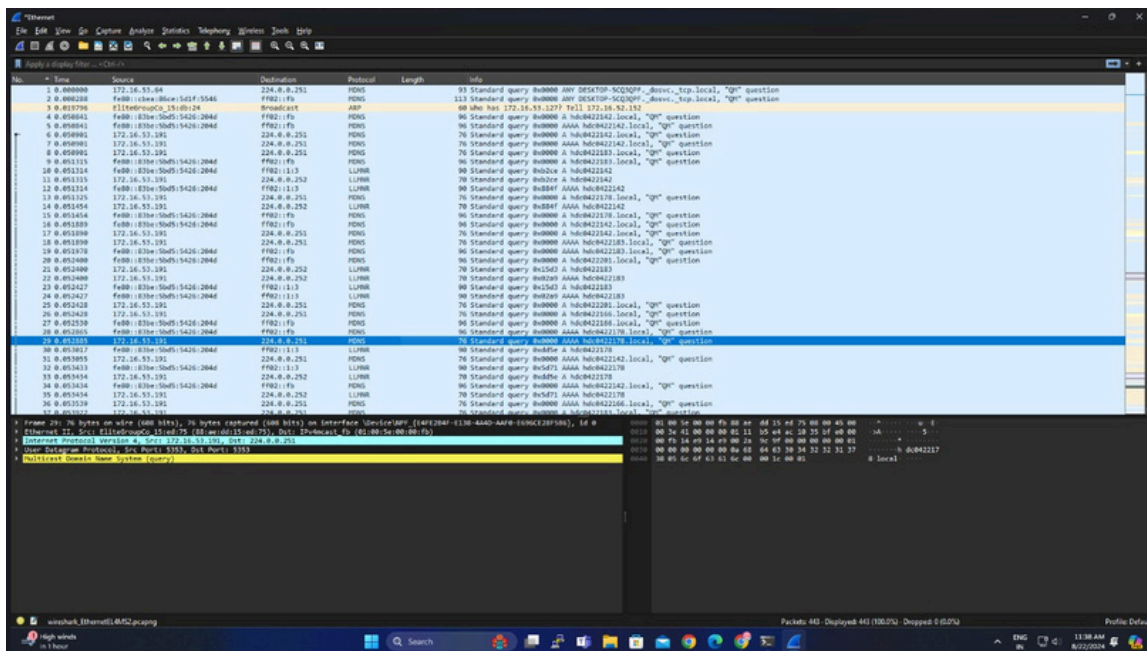
**AIM:** - Experiments on Packet capture tool: Wireshark

## CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL:

### Packet 1:



### Packet 2:



## Packet 3:

The screenshot shows a Wireshark packet capture of a DNS query. The packet list on the left shows 33 packets. Packet 3 is selected, showing a DNS query from 192.168.1.101 to 192.168.1.1. The packet details pane shows the following structure:

- Ethernet II, Src: RealtekUplink (08:00:00:00:00:00), Dst: Telemach\_4 (08:00:00:00:00:00)
- Internet Protocol version 4, Src: 192.168.1.101, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 5555, Dst Port: 53
- Link-Local Multicast Name Resolution (query)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, UDP header, and the DNS query payload.

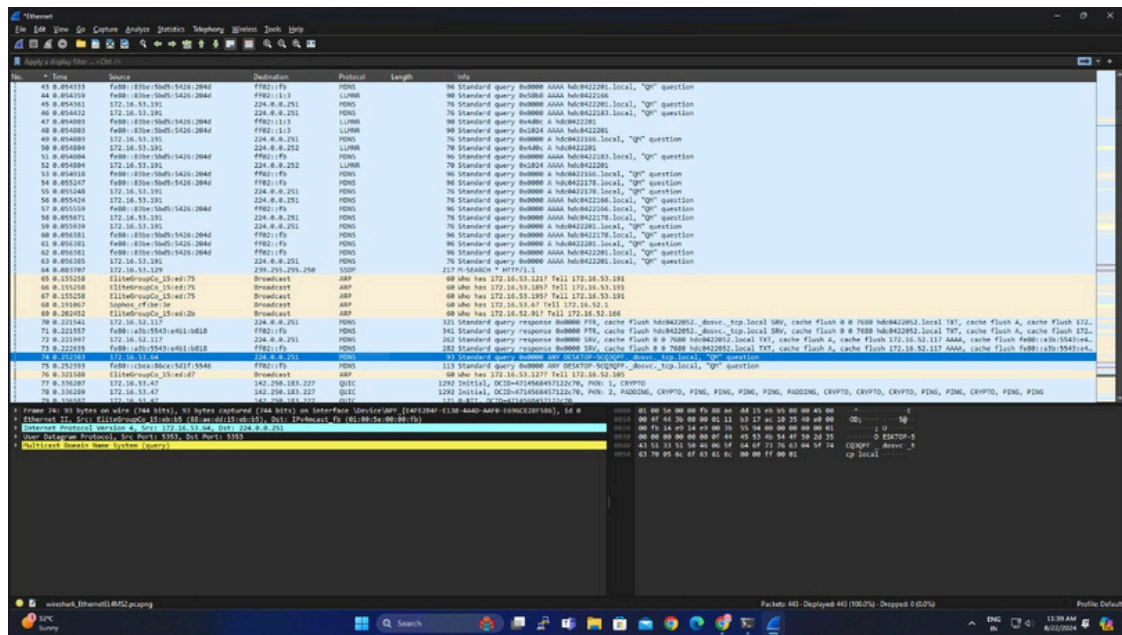
## Packet 4:

The screenshot shows a Wireshark packet capture of a DNS query. The packet list on the left shows 33 packets. Packet 4 is selected, showing a DNS query from 192.168.1.101 to 192.168.1.1. The packet details pane shows the following structure:

- Ethernet II, Src: RealtekUplink (08:00:00:00:00:00), Dst: Telemach\_4 (08:00:00:00:00:00)
- Internet Protocol version 4, Src: 192.168.1.101, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 5555, Dst Port: 53
- Link-Local Multicast Name Resolution (query)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, UDP header, and the DNS query payload.

## Packet 5:



## RESULT: -

Capturing and analysing the packets have been done successfully using Wireshark.