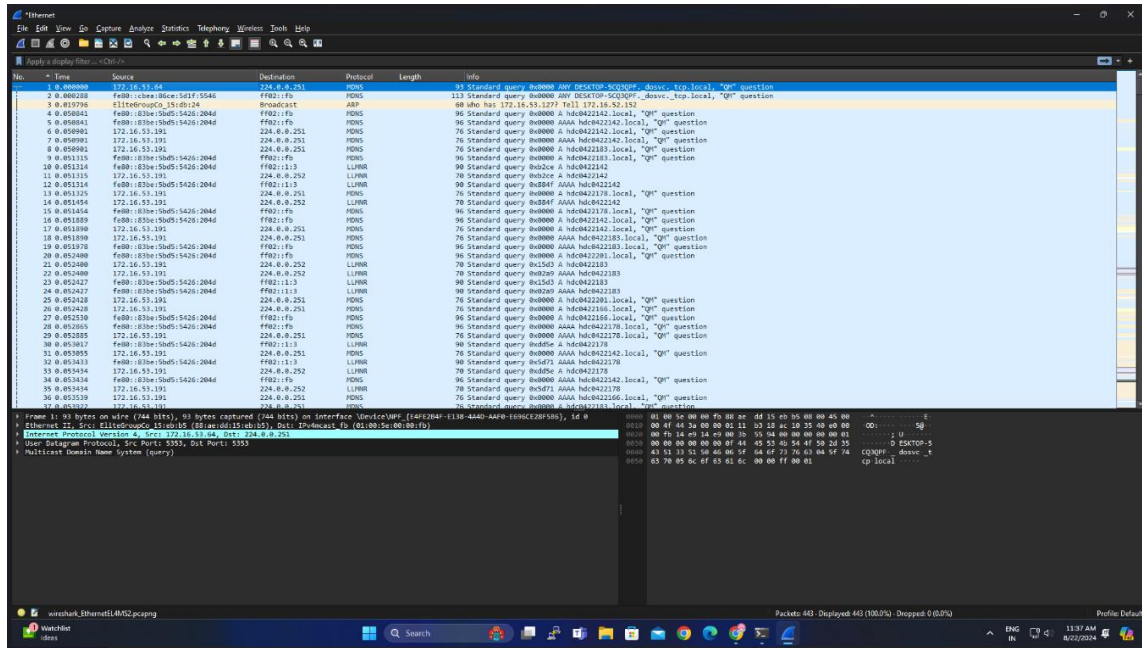


EXPERIMENT – 5

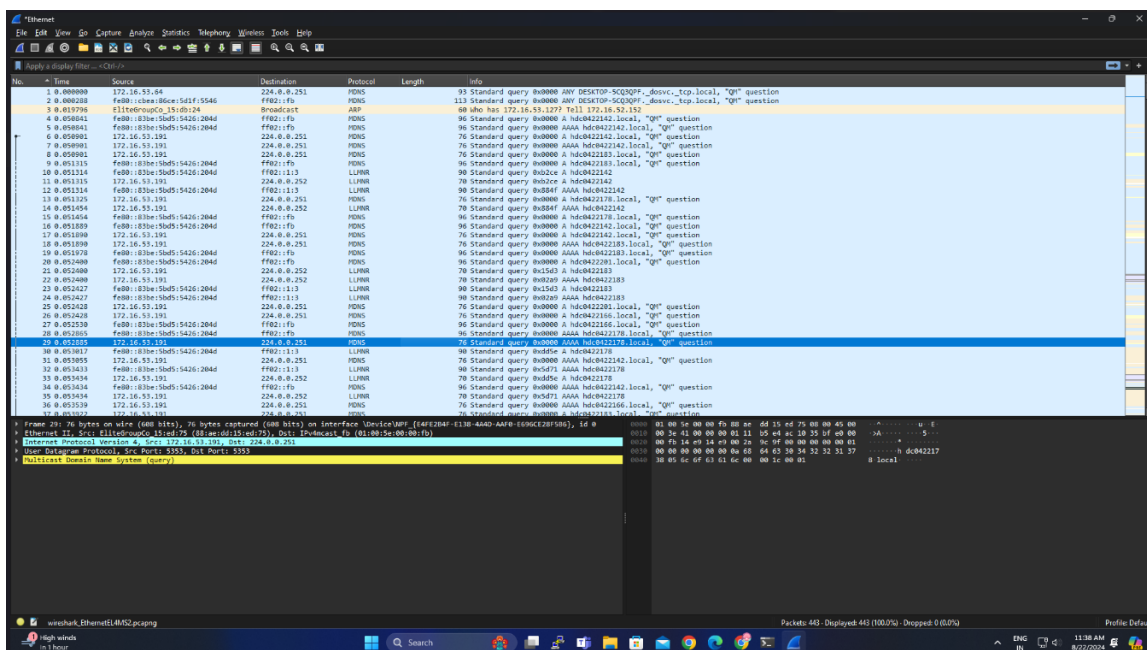
AIM: - Experiments on Packet capture tool: Wireshark

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL:

Packet 1:



Packet 2:



Packet 3:

The screenshot shows the Wireshark interface with Packet 3 selected. The packet list pane on the left shows a single entry: "Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1". The packet details pane on the right shows the structure of the packet: Ethernet II (Type: IPv4), Internet Protocol Version 4 (Length: 60), and ICMP Echo (ping) request (Length: 84). The packet bytes pane on the bottom shows the raw data of the packet, including the Ethernet II header, IPv4 header, and ICMP Echo request data.

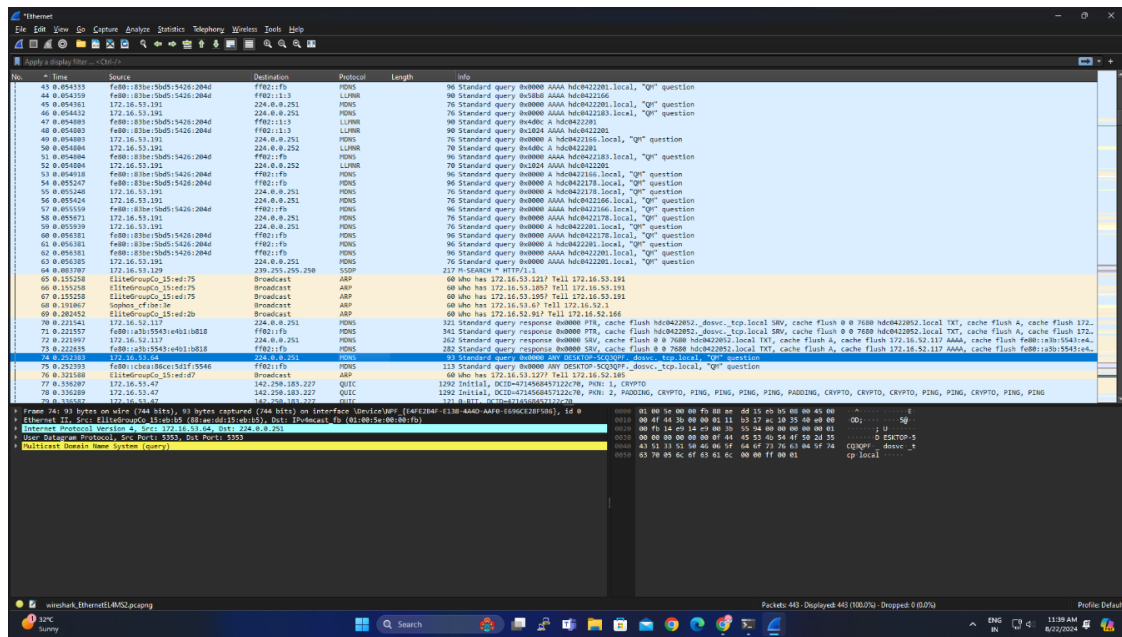
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	192.168.1.101	192.168.1.1	ICMP	84	Standard query 0x0000 AAAA h0c422178, local, "Q" question

Packet 4:

The screenshot shows the Wireshark interface with Packet 4 selected. The packet list pane on the left shows a single entry: "Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1". The packet details pane on the right shows the structure of the packet: Ethernet II (Type: IPv4), Internet Protocol Version 4 (Length: 60), and ICMP Echo (ping) request (Length: 84). The packet bytes pane on the bottom shows the raw data of the packet, including the Ethernet II header, IPv4 header, and ICMP Echo request data.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	192.168.1.101	192.168.1.1	ICMP	84	Standard query 0x0000 AAAA h0c422178, local, "Q" question

Packet 5:



RESULT: -

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