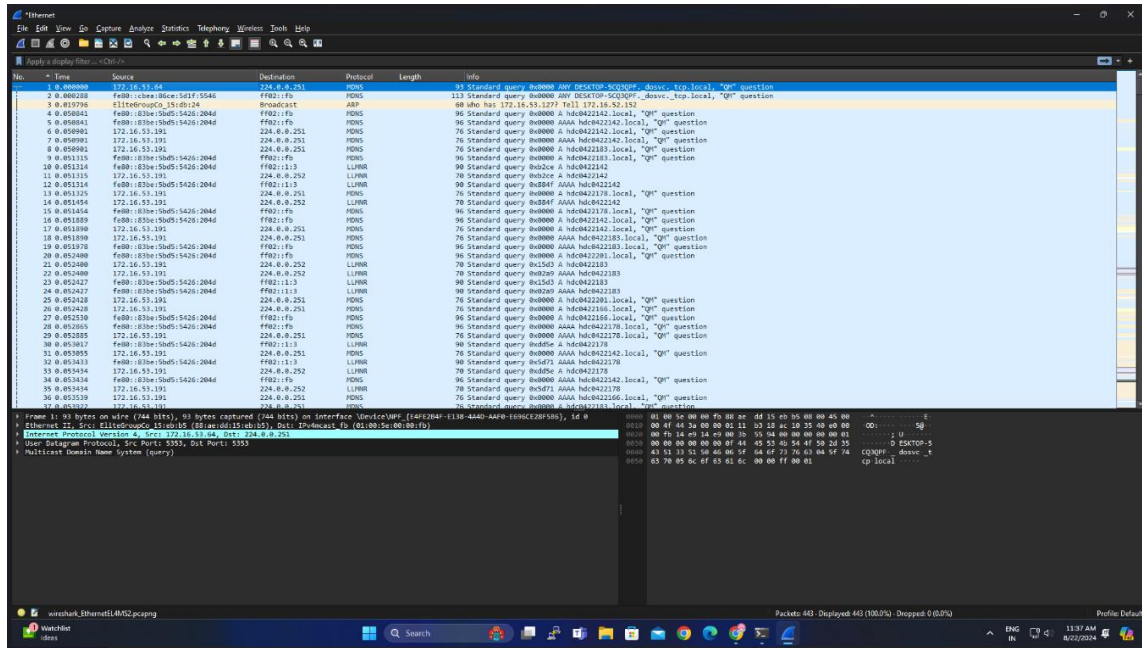


EXPERIMENT – 5

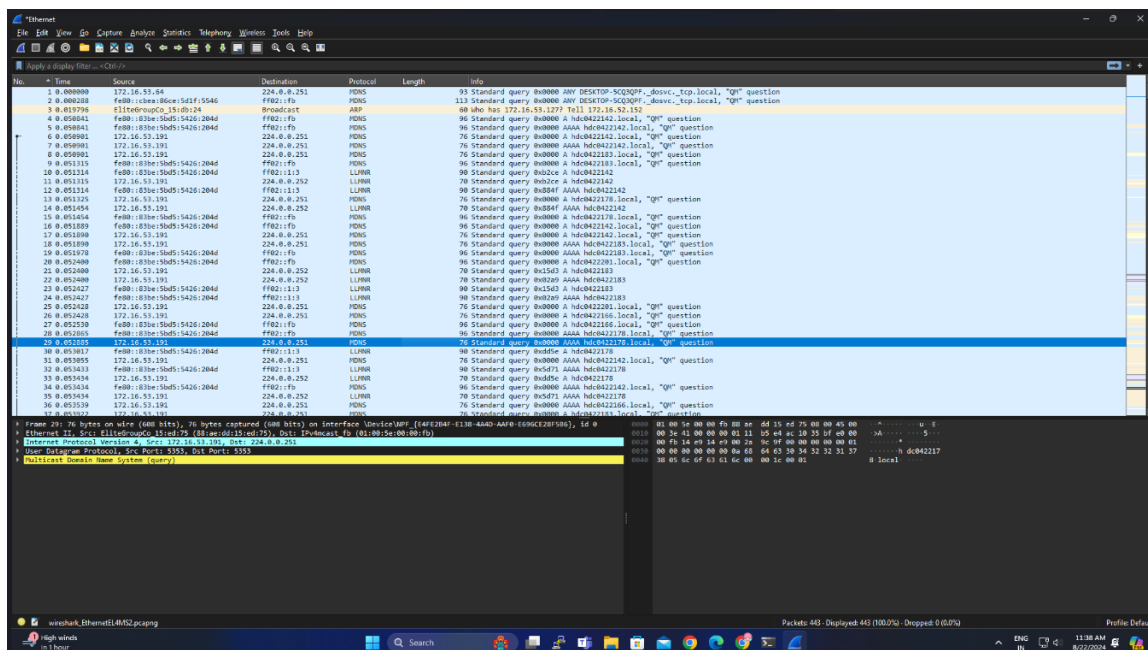
AIM: - Experiments on Packet capture tool: Wireshark

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL:

Packet 1:



Packet 2:



Packet 3:

The screenshot shows a Wireshark packet capture on the 'Ethernut' interface. The packet list on the left shows packet 31, which is a DNS query from 10.0.0.114 to 224.0.0.252. The packet details pane shows the following structure:

- Frame 31: 96 bytes on wire (720 bits), 96 bytes captured (720 bits) on interface Udp0/WP (f4f1204f-1130-4040-AA00-E696C220F580), Id 0
- Ethernet II, Src: Ethernut01:00:00:00:00:00, Dst: 224.0.0.252 (33:33:00:00:00:00)
- Internet Protocol Version 4, Src: 10.0.0.114, Dst: 224.0.0.252
- User Datagram Protocol, Src Port: 54321, Dst Port: 5353
- Link-Local Multicast Name Resolution (Query)

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

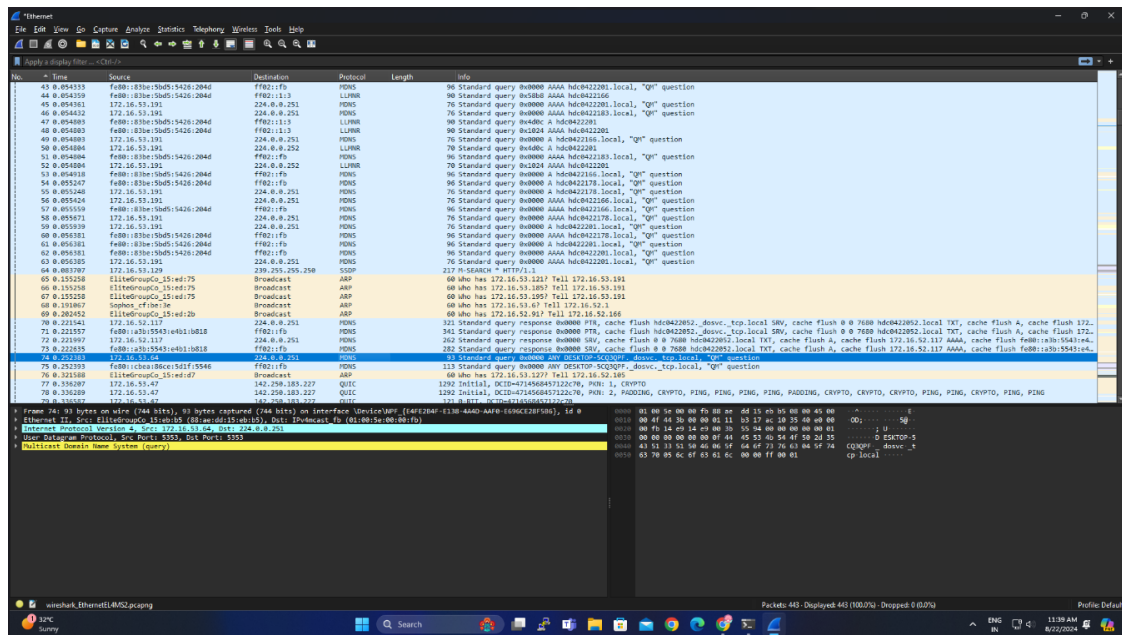
Packet 4:

The screenshot shows a Wireshark packet capture on the 'Ethernut' interface. The packet list on the left shows packet 32, which is a DNS query from 10.0.0.114 to 224.0.0.252. The packet details pane shows the following structure:

- Frame 32: 96 bytes on wire (720 bits), 96 bytes captured (720 bits) on interface Udp0/WP (f4f1204f-1130-4040-AA00-E696C220F580), Id 0
- Ethernet II, Src: Ethernut01:00:00:00:00:00, Dst: 224.0.0.252 (33:33:00:00:00:00)
- Internet Protocol Version 4, Src: 10.0.0.114, Dst: 224.0.0.252
- User Datagram Protocol, Src Port: 54321, Dst Port: 5353
- Link-Local Multicast Name Resolution (Query)

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

Packet 5:



RESULT: -

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