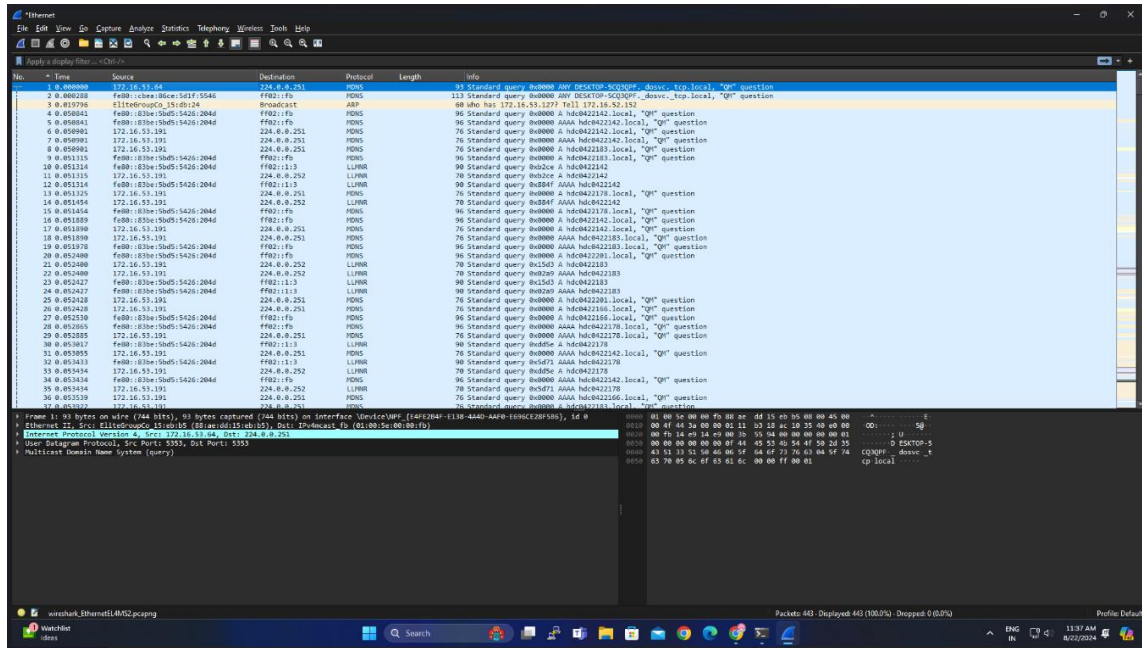


EXPERIMENT – 5

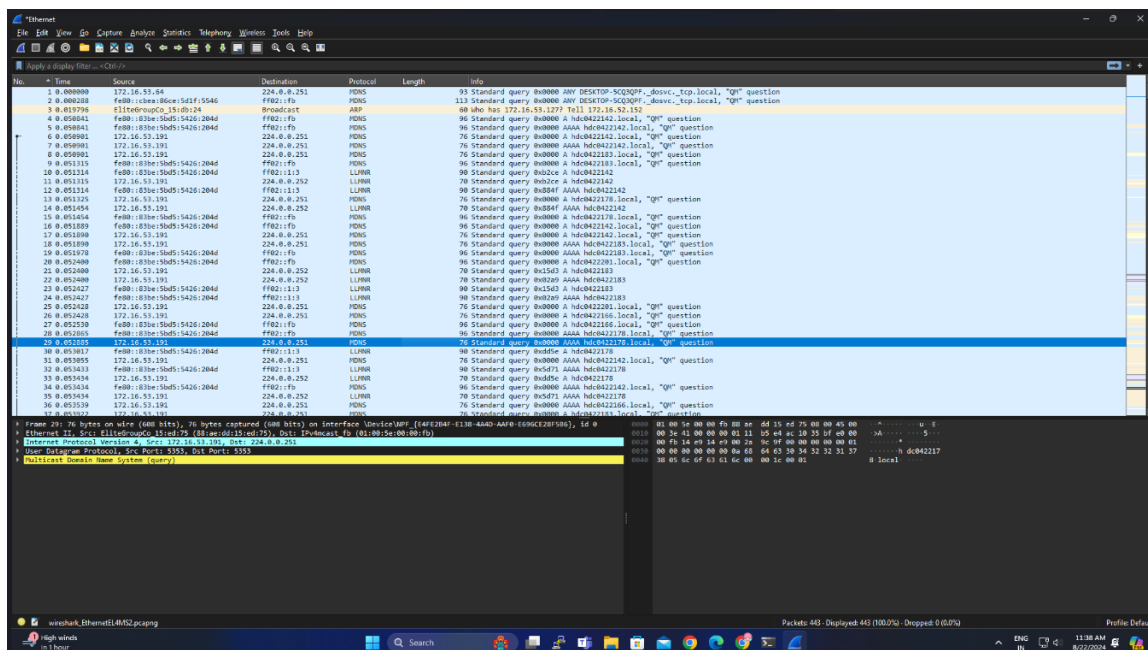
AIM: - Experiments on Packet capture tool: Wireshark

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 a single packet, No. 3, at time 0.0000000, from 192.168.1.101 to 192.168.1.1. The packet details pane shows the following structure:

- Frame 3: 108 bytes on wire (864 bits), 86 bytes captured (688 bits) on interface vethshark-Ethernet0, 0 bytes deferred
- Ethernet II, Src: vethshark-Ethernet0, Dst: 192.168.1.1 (08:00:27:00:00:01), Encapsulated: 100 bytes (800 bits)
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 54321, Dst Port: 53
- Link-Local Multicast Name Resolution (Query)

The packet bytes pane shows the raw data of the DNS query, including the query ID, flags, and the question section.

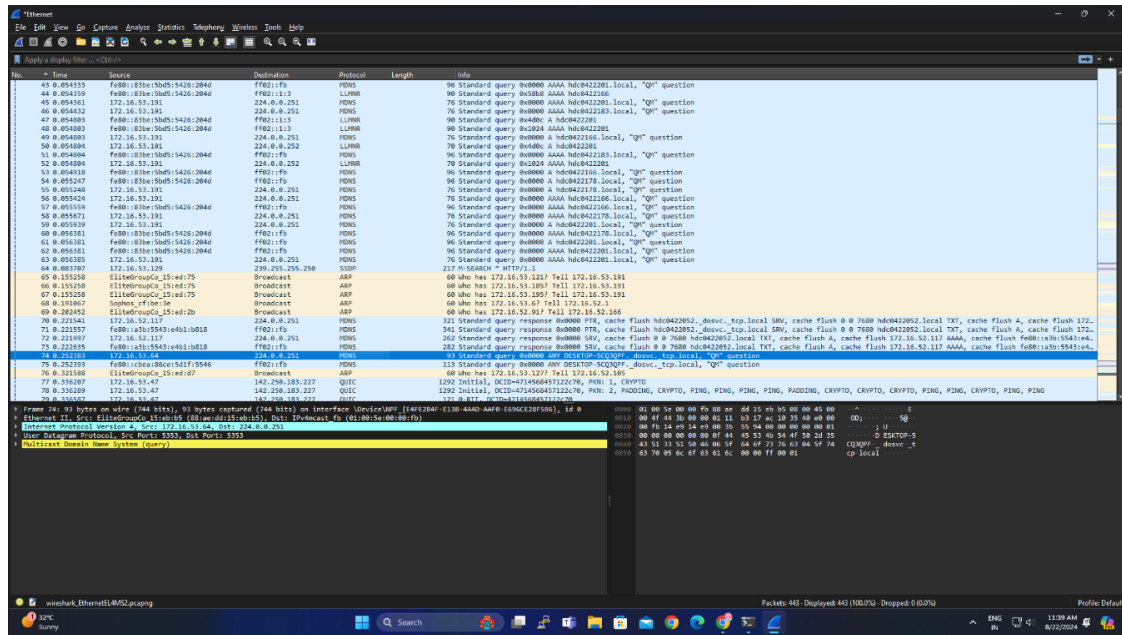
Packet 4:

The screenshot shows a Wireshark packet capture of a DNS query. The packet list on the left shows a single packet, No. 4, at time 0.0000000, from 192.168.1.101 to 192.168.1.1. The packet details pane shows the following structure:

- Frame 4: 108 bytes on wire (864 bits), 86 bytes captured (688 bits) on interface vethshark-Ethernet0, 0 bytes deferred
- Ethernet II, Src: vethshark-Ethernet0, Dst: 192.168.1.1 (08:00:27:00:00:01), Encapsulated: 100 bytes (800 bits)
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 54321, Dst Port: 53
- Link-Local Multicast Name Resolution (Query)

The packet bytes pane shows the raw data of the DNS query, including the query ID, flags, and the question section.

Packet 5:



RESULT: -

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