EXPERIMENT -5

AIM Experiments on Packet capture tool: Wireshark

Packet Sniffer

● Sniffs messages being sent/received from/by your computer

● Store and display the contents of the various protocol fields in the messages

● Passive program

– never sends packets itself

– no packets addressed to it

– receives a copy of all packets (sent/received)

Packet Sniffer Structure Diagnostic Tools

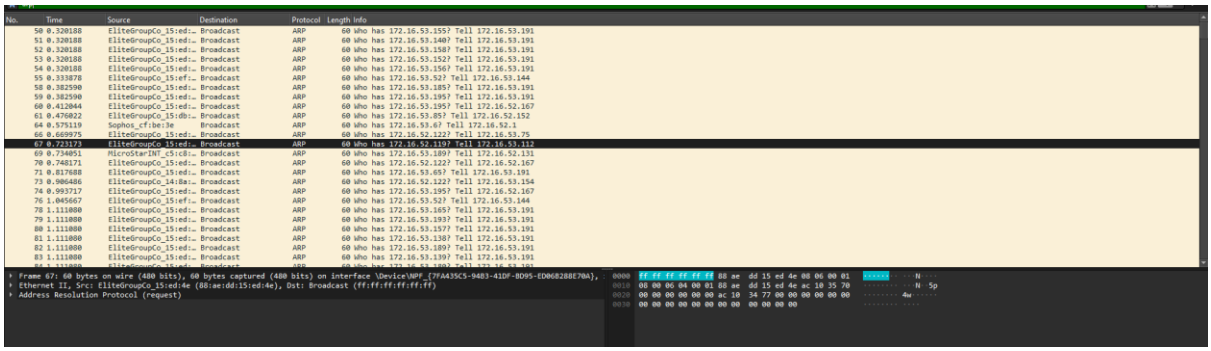
● Tcpdump

– E.g. tcpdump -enx host 10.129.41.2 -w exe3.out

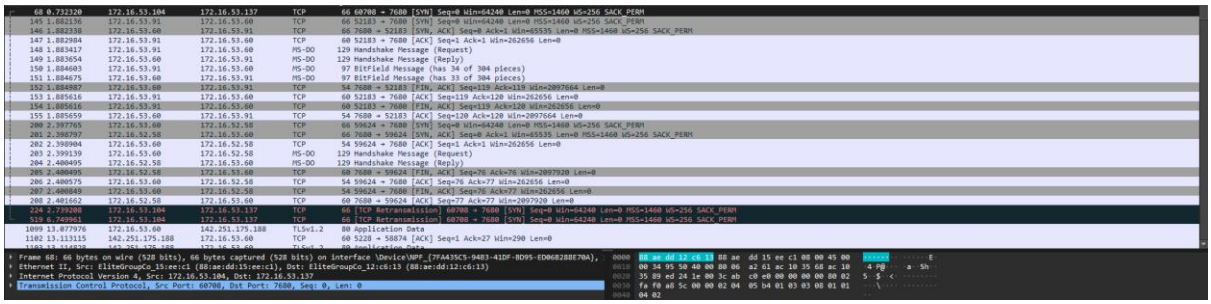
● Wireshark

– wireshark -r exe3.out

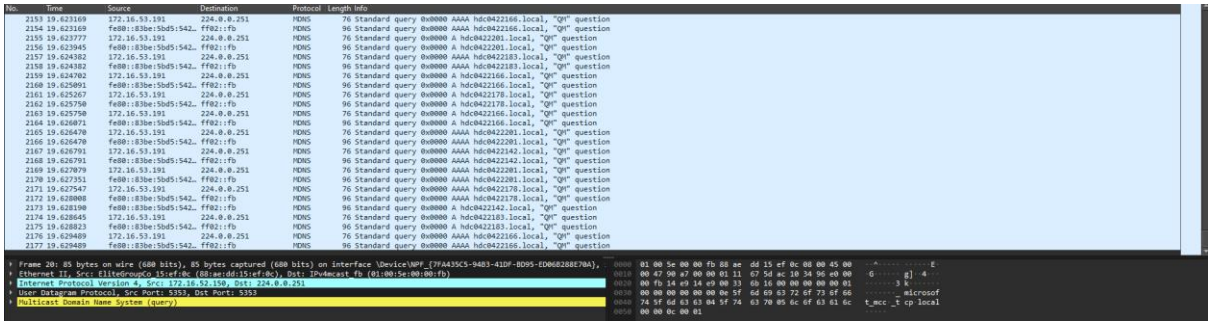
Packet 1(ARP):



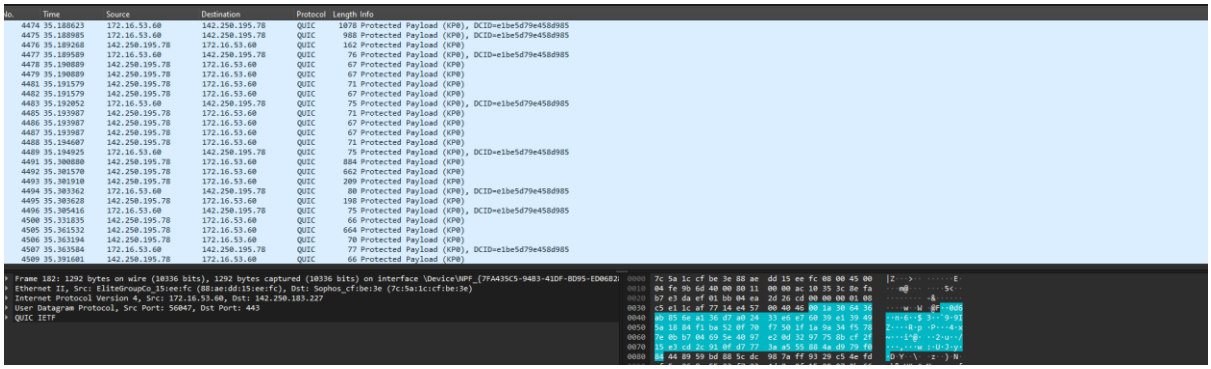
Packet 2(TCP):



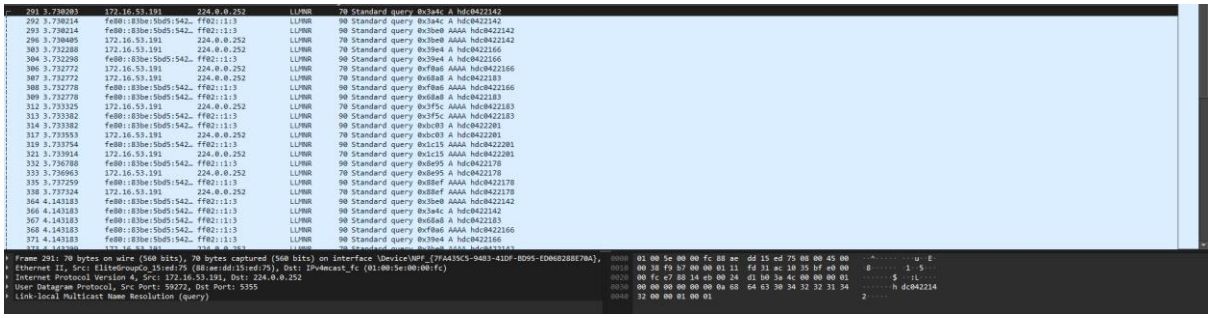
Packet 3(MDNS):



Packet 4(QUIC):



Packet 5(LLMNR):



<u>RESULT:</u> -

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