EXPRIMENT – 28

Network Layer protocol header analysis USING Wire shark - ICMP

AIM: To analysis capturing of transparent layer protocol analysis using wireshark ICMP

SOFTWARE REQUIREMENT:wireshark network layer analysis

Procedure:

1.open wire shark.

2.click on the list available capture interface.

3.choose the LAN interface.

4.click on the start button.

5.active packets will be displayed.

6.capture the packets and select any IP address from the source.

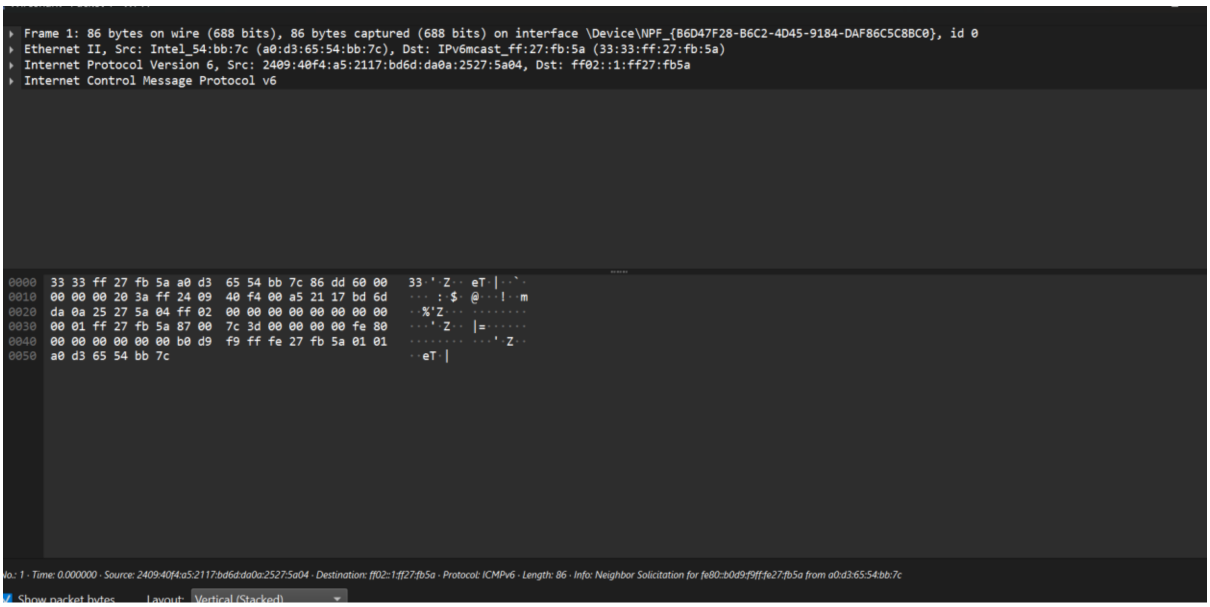
7.click on the expreesion and select IP, Source address in the field name.

8.select the double equals (==) from the selection and enter the selected IPaddress.

9.click on the apply address.

10.all the packets will be filtered using source address.

RESULT: Here the capturing of packets wireshark network analyzer was analysed for ICMP.



```
Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{B6D47F28-B6C2-4D45-9184-DAF86C5C8BC0}, id 0
Ethernet II, Src: Intel_54:bb:7c (a0:d3:65:54:bb:7c), Dst: IPv6mcast_ff:27:fb:5a (33:33:ff:27:fb:5a)
Internet Protocol Version 6, Src: 2409:40f4:a5:2117:bd6d:da0a:2527:5a04, Dst: ff02::1:ff27:fb5a
Internet Control Message Protocol v6
```

```
0000  33 33 ff 27 fb 5a a0 d3  65 54 bb 7c 86 dd 60 00   33·'·Z·· eT·|··`·
0010  00 00 00 20 3a ff 24 09  40 f4 00 a5 21 17 bd 6d   ··· :·$· @···!··m
0020  da 0a 25 27 5a 04 ff 02  00 00 00 00 00 00 00 00   ··%'Z··· ········
0030  00 01 ff 27 fb 5a 87 00  7c 3d 00 00 00 00 fe 80   ···'·Z·· |=······
0040  00 00 00 00 00 00 b0 d9  f9 ff fe 27 fb 5a 01 01   ········ ···'·Z··
0050  a0 d3 65 54 bb 7c                                  ··eT·|
```

No.: 1 · Time: 0.000000 · Source: 2409:40f4:a5:2117:bd6d:da0a:2527:5a04 · Destination: ff02::1:ff27:fb5a · Protocol: ICMPv6 · Length: 86 · Info: Neighbor Solicitation for fe80::b0d9:f9ff:fe27:fb5a from a0:d3:65:54:bb:7c

☑ Show packet bytes   Layout: Vertical (Stacked)
]