

EXPERIMENT-24

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – SMTP AND ICMP

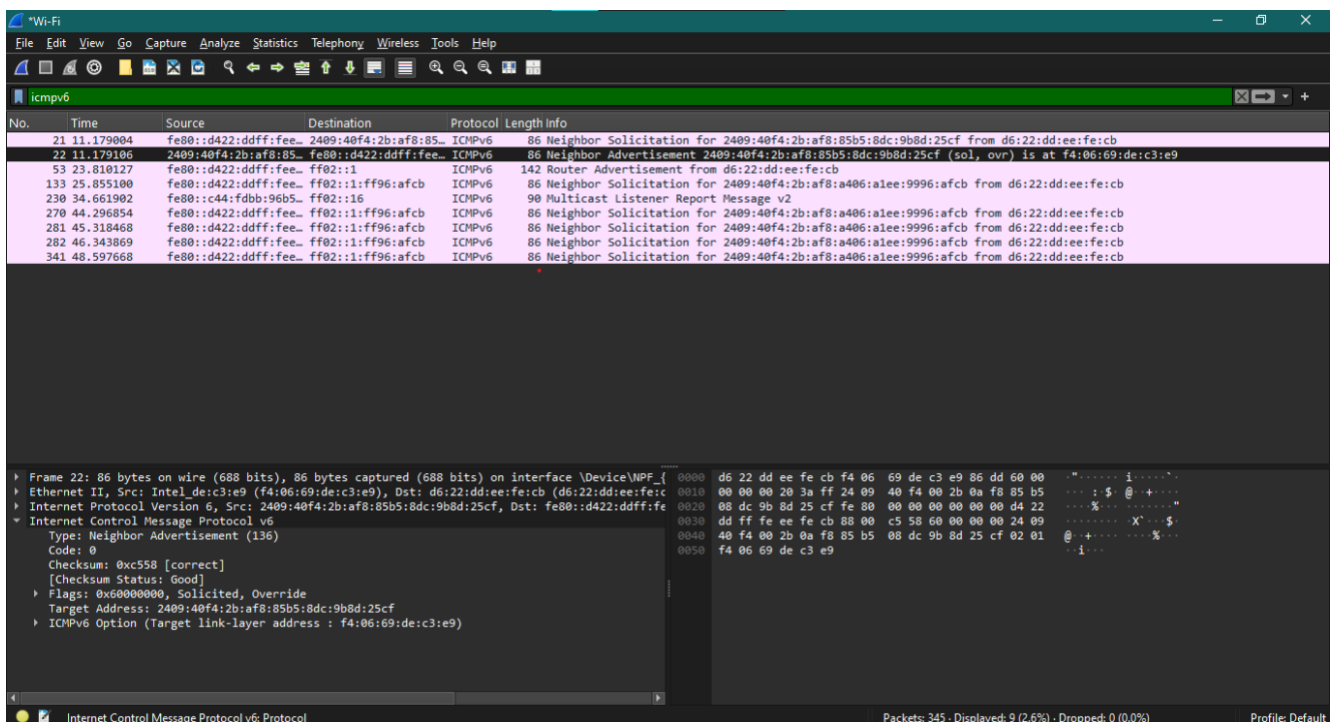
Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- SMTP and ICMP.

SOFTWARE USED:

Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 ☐ IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.



The image shows a Wireshark network analyzer interface with the following details:

- Top Pane (Packet List):** Displays a list of captured packets. Packet 2808 is selected, showing details for an SMTP session between 192.168.205.237 and 74.125.130.109.
- Middle Pane (Packet Details):** Shows the structure of the selected packet (Frame 2808):
 - Ethernet II:** Src: 2a:99:57:fb:7f:2a (2a:99:57:fb:7f:2a), Dst: Intel de:c3:e9 (f4:06:69:de:c3:ed).
 - Internet Protocol Version 4:** Src: 74.125.130.109, Dst: 192.168.205.237.
 - Transmission Control Protocol:** Src Port: 587, Dst Port: 53528, Seq: 242, Ack: 23, Len: 170. It includes fields for Stream Index, Conversation Completeness, TCP Segment Len, Sequence Number, Next Sequence Number, Acknowledgment Number, and Flags (PSH, ACK).
- Bottom Pane (Raw Data):** Displays the raw packet data in hexadecimal and ASCII. The ASCII column shows the SMTP command "EHLO" and the response "250 5.5.4 Empty HELO/EHLO argument not allowed, closing connection.".
- Status Bar:** Indicates 3212 packets displayed, 13 (0.4%) dropped, and 0 (0.0%) dropped.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for SMTP and ICMP.