Ex:04
Date:
4/8/25

PRACTICAL-5

WIRESHARK.

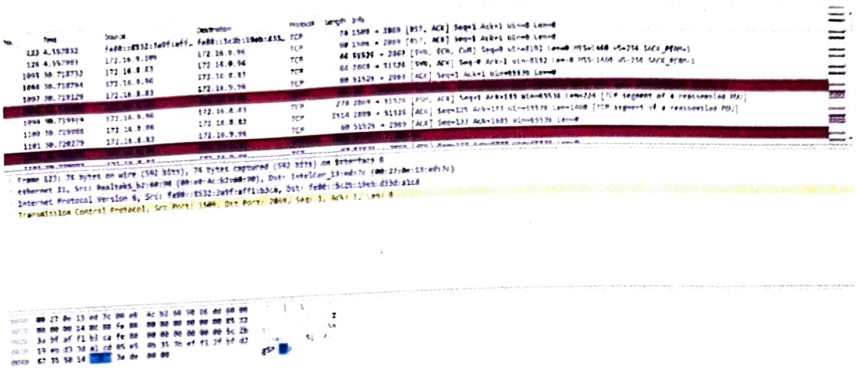
AIM:-

To filter, capture, view, packets in wiresha tool.

1) Create a filter to display only TCP/UDP packets, inspect the packets, inspect the packets and provide the flow graph.

- Select local area connection in wireshark.
- Go to capture → option
- Select stop capture automatically afte 100 packets
- Then click start capture.
- Search TCP packets in search bar.
- To see flow graph click statistics → Flow graph
- Save the packet.

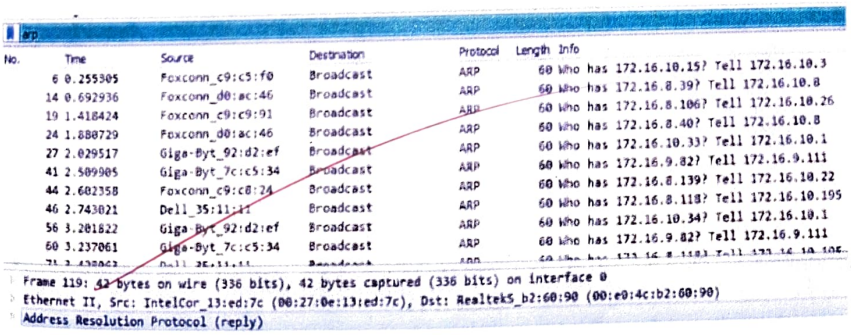
O/P:-



2) Create a filter to display only ARP packets and inspect the packets Procedure.

- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click start capture.
- Search ARP packets in search bar.

O/P:-

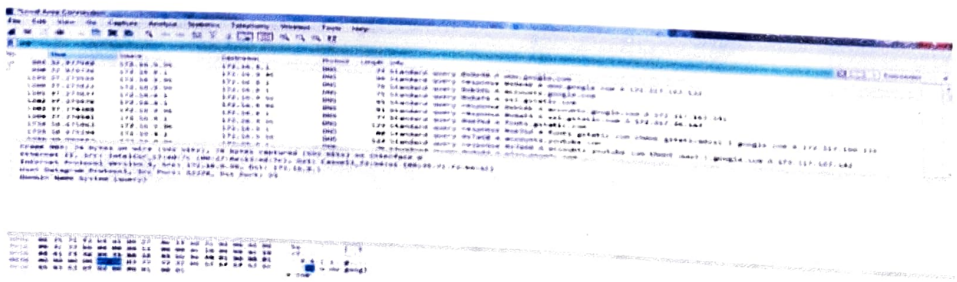


3. Create a filter to display only DNS packets and provide the flow graph.

procedure.

- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics → Flow graph.
- Save the packets.

o/p:-

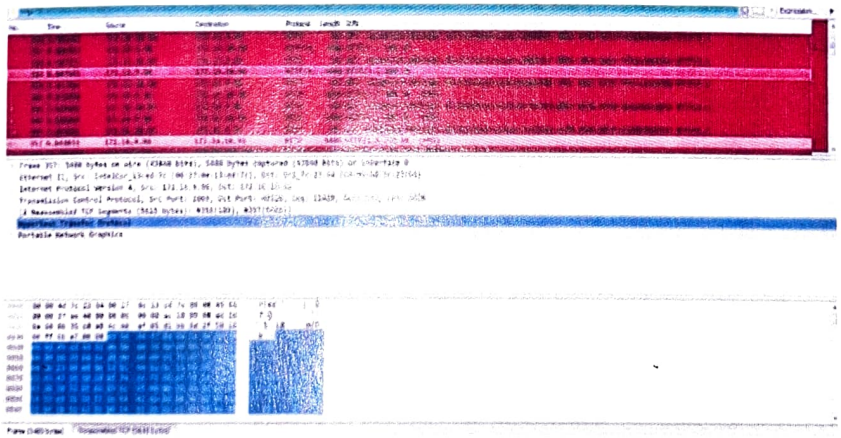


4. Create a filter to display only HTTP packets

Procedure:

- Select Local Area connection in wireshark.
- go to capture → option.
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in search bar.
- Save the packets.

O/P:-



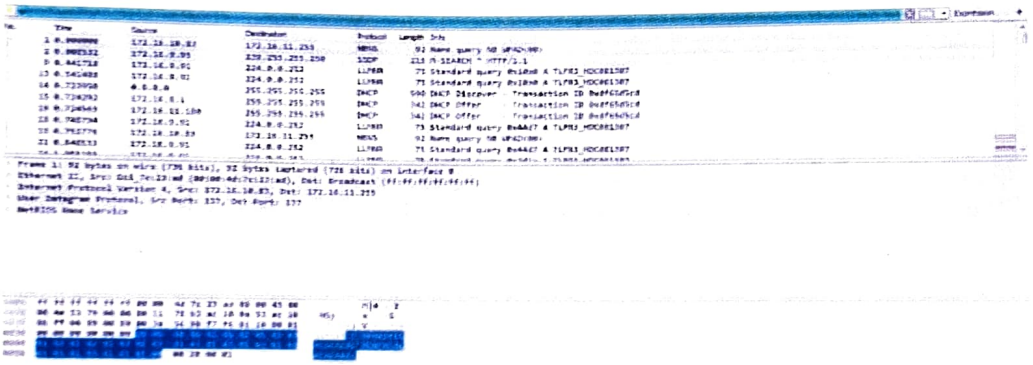
5. Create a filter to display only IP/ICMP packets and inspect the packets.

Procedure:

- Select Local Area connection in Wireshark
- Go to capture → option.

- Select stop capture automatically after 100 packets.
- Then click start capture.
- Search ICMP / IP packets in search bar.
- Save the packets.

O/P:-



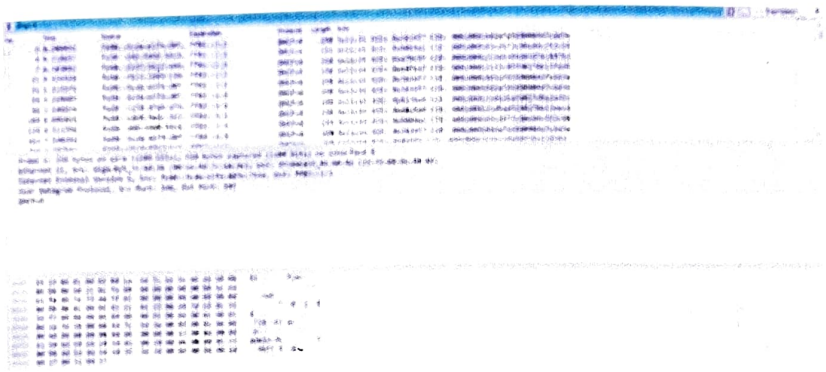
6. Create a filter to display only DHCP packets and inspect the packets.

Procedure:

- Select Local Area connection in Wireshark.
- Go to capture → option.
- Select stop capture automatically after 100 packets.

- Then click start capture.
- Search DHCP packets in search bar.
- Save the packets.

OP:-



Student Observation :-

1) What is promiscuous mode ?

It is a network interface mode in which a network card (NIC) captures all network packets that pass through it, regardless of the destination MAC address.

2) Does ARP packets have a transport layer header? Explain.

No, ARP packets do not have a transport layer header.

- ARP works the Data Link Layer (Layer 2) of the OSI model, and in TCP/IP terms, it's part of the link layer.
- It's purpose is to map an IP address to a MAC address.

3) Which transport layer protocol is used by DNS?

DNS can use both UDP and TCP at the transport layer.

4) What is the port number used by HTTP protocol?

- HTTP uses port number 80 by default.
- HTTPS uses port number 443.

5) What is a broadcast IP address?

A broadcast IP address is an address used to send data to all hosts on a network segment at once.

RESULT:-

Successfully simulated and analyzed the experiment on Packet capture tool : Wireshark.

18/9/25