Ex No: 4B **NAME:NAVEEN C H**
DATE:19.8.24 **ROLL NO:231901033**

PACKET SNIFFING USING WIRESHARK

AIM:

To capture, save, filter and analyze network traffic on TCP / UDP / IP / HTTP / ARP /DHCP /ICMP /DNS using Wireshark Tool

Exercises

1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save

it. Procedure

Select Local Area Connection in Wireshark.
Go to capture ✇option
Select stop capture automatically after 100 packets.
Then click Start capture. Save
the packets.

Output

2.Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.
Procedure

Select Local Area Connection in Wireshark.

Go to capture ☢option

Select stop capture automatically after 100 packets.

Then click Start capture.

Search TCP packets in search bar.

To see flow graph click Statistics☢Flow graph.

Save the packets.

Output:

Inspecting packets

Flow Graph output

3.Create a Filter to display only ARP 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 ARP packets in search bar.
Save the packets.

Output

Inspecting packets

4.Create a Filter to display only DNS packets and provide the flow graph. Procedure

Select Local Area Connection in Wireshark.

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.

Output

Flow Graph output

5.Create a Filter to display only HTTP 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 HTTP packets in the search bar.
Save the packets.

Output

Inspecting packets

Flow Graph output

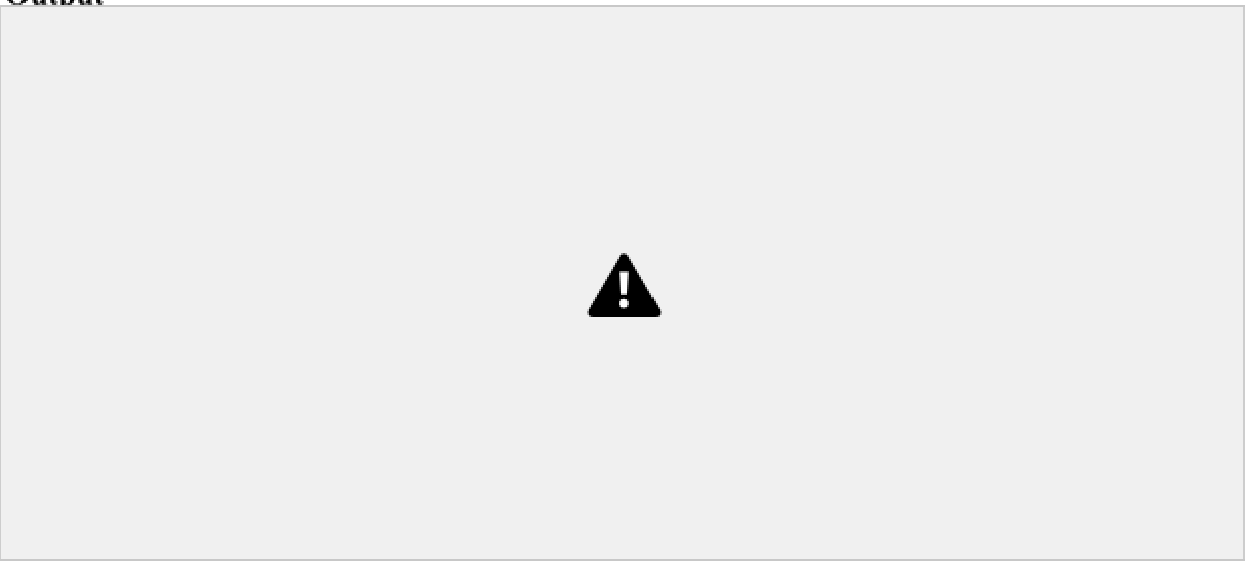
6.Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

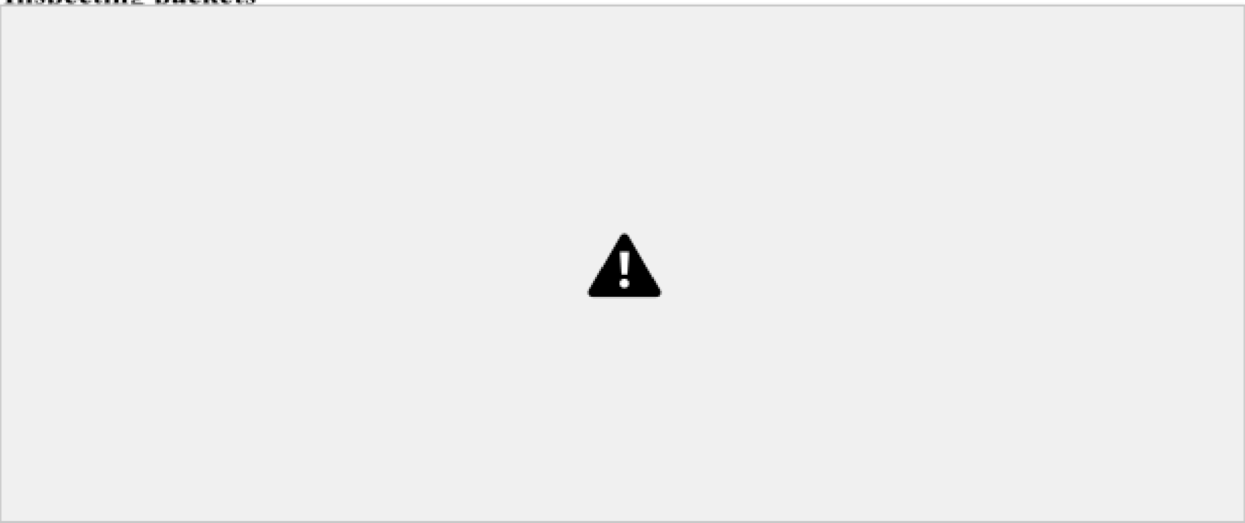
Select Local Area Connection in Wireshark.

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

Output



Inspecting packets



Flow Graph output

7.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

Output

Inspecting packets

RESULT:

capture, save, filter and analyze network traffic on TCP / UDP / IP / HTTP / ARP /DHCP /ICMP /DNS using Wireshark Tool is executed successfully.