# Experiment - 5

Aim:

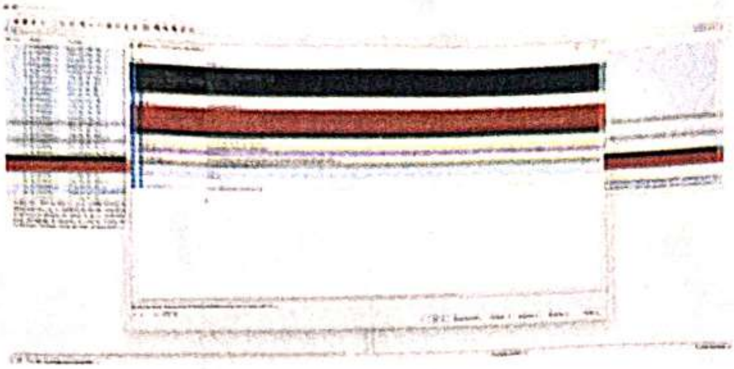
experiments on packet capture tool : wireshark.

## Capturing packets:

After downloading and installing wireshark launch it and double click the name of a network interface.

As soon as you click the interfaces name, you'll see the packets start to appear in real time

To view exactly what the colour codes mean. click viewer colourizing rules.



Capturing & analysing packets using wireshark tool

1. Filter TCP/ UDP packets

-> select local area connection in wireshark capture -> option.

-> select stop capture automatically after 100 packets

· The click stop capture

· Search TCP packets in search bar

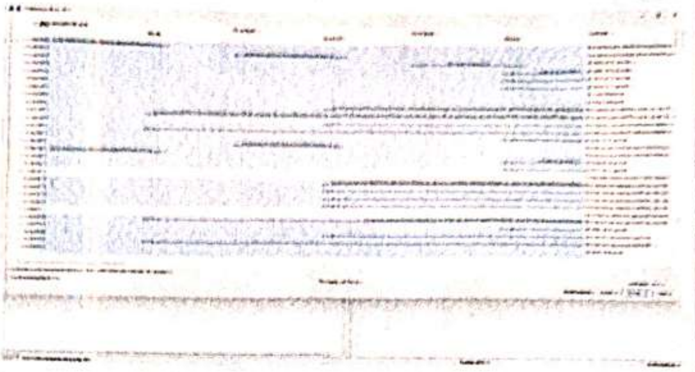
· To see flow graph click statistics -> flow graph

· save the packets

5) Filter to display IP / SCHP packets

- search ICMP / IP in search bar

6) Filter no display only DHCP packets.



Student observation

1) What is promiscous mode?

It is a network interface mode in which a network card capture all the network packets regardless of their destination MAC address

2) Does ARP header have transport layer header

NO ARP is a part of network layer

3) Which transport layer protocol is used by DNS?

DNS uses both: UDP and TCP

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

Port 80

5) What is broadcast IP address?

It is used to send data to all host on specific network segments.

15/10/25

Result: