INDEX

NAME: A.Kavin STD: III nd year SEC.: CSE-B ROLL NO.: 220701122

S.No.	Date	Title	Page No.	Teacher's Sign/ Remarks
1.	16/7/24	Study of various network commands used in Linux & windows		
2.	23/7/24	Study of network cables		
3.	30/7/24	Experiments on CISCO PACKET TRACER (simulation tool)		
4.	6/8/24	Setup and configure a LAN using a switch and Ethernet cable		
5.	9/8/24	Experiments on packet capture tool: wireshark		

Exp. No 05

Date : 09-08-2024

Practical- 5

Aim

Experiments on packet capture tool: Wireshark

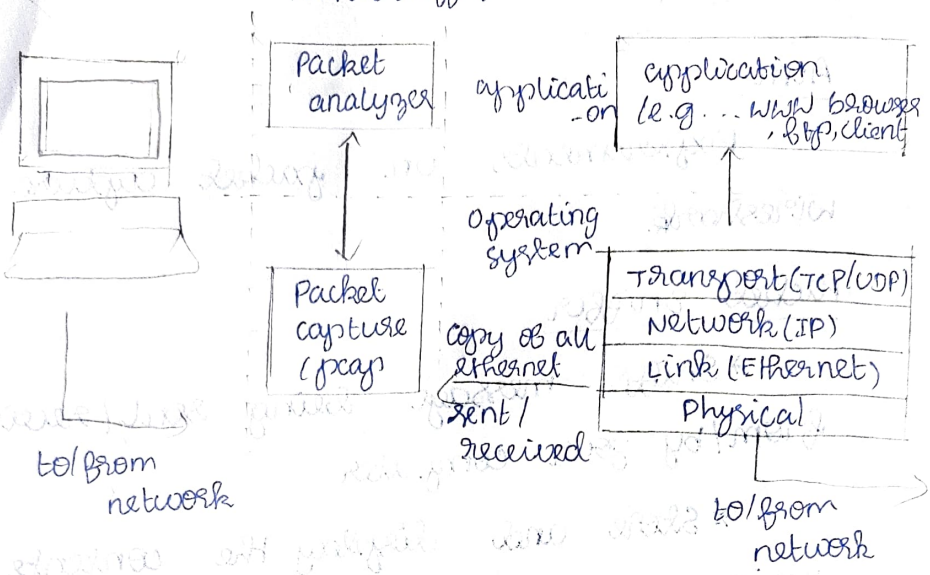
Packet Sniffer

* Sniffs message being sent/received from/by your computer
* Store and display the contents of the various protocol fields in the messages
* Passive program
  - never sends packets itself
  - no packets addressed to it
  - receives a copy of all packets

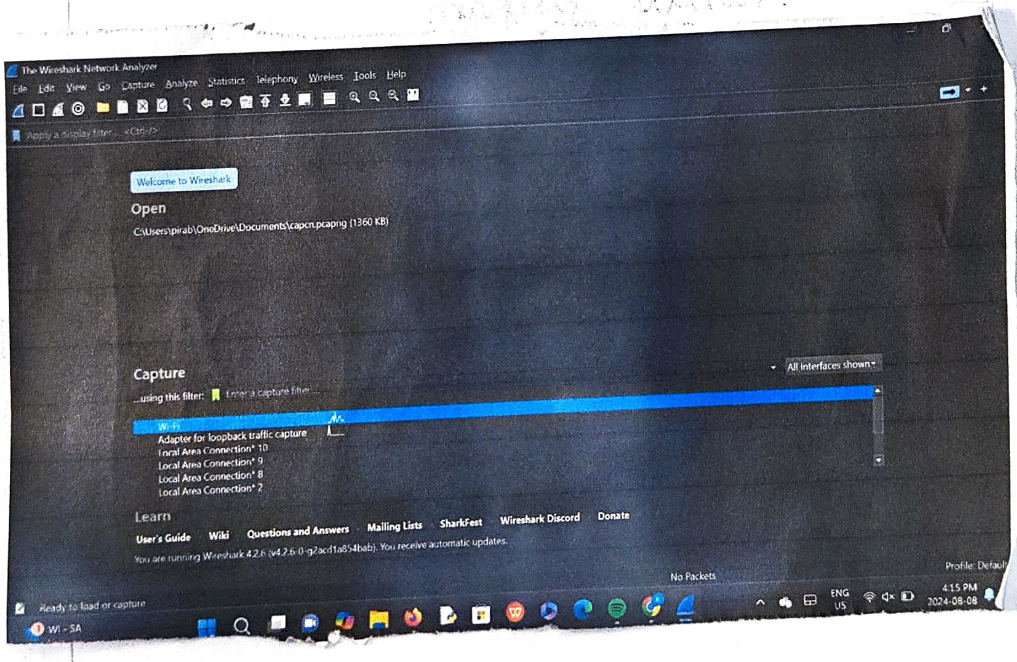
Packet sniffer structure diagnostic tool

* Tcpdump
  - E.g. tcpdump -enx host 10.129.41.2 -w exe3.out
* Wireshark
  - wireshark -r exe3.out

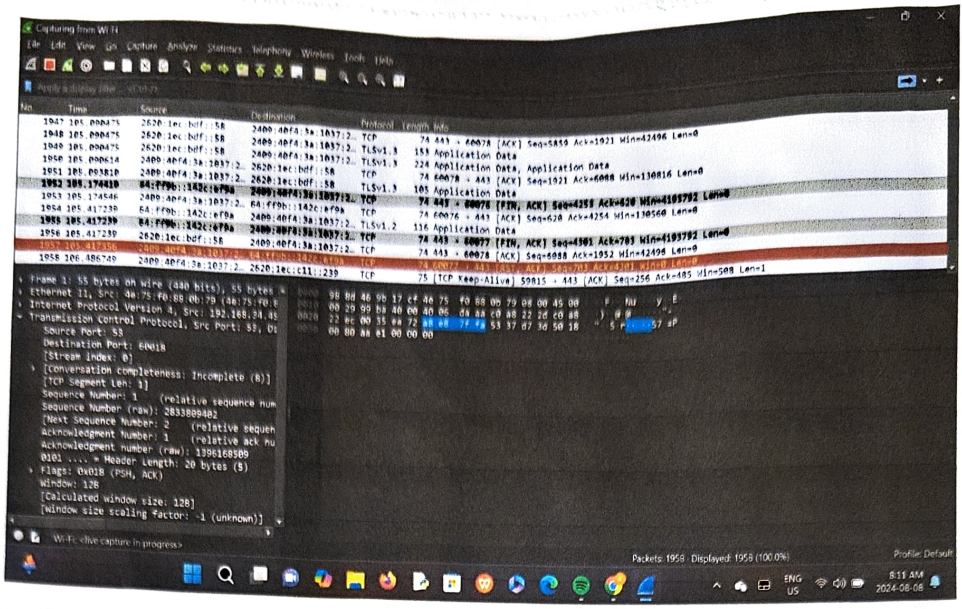
Packet Sniffer



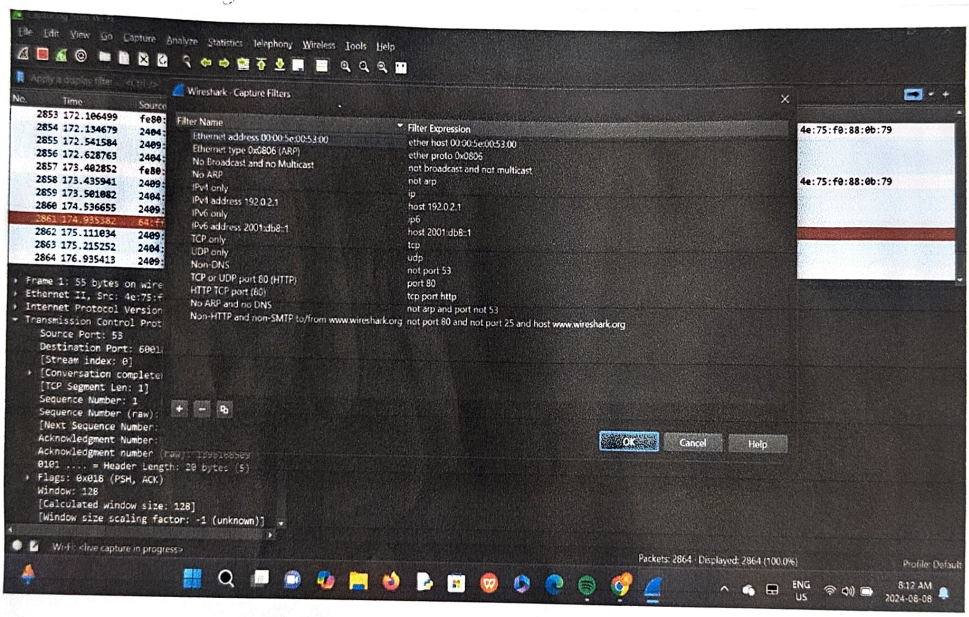
Capturing Packets

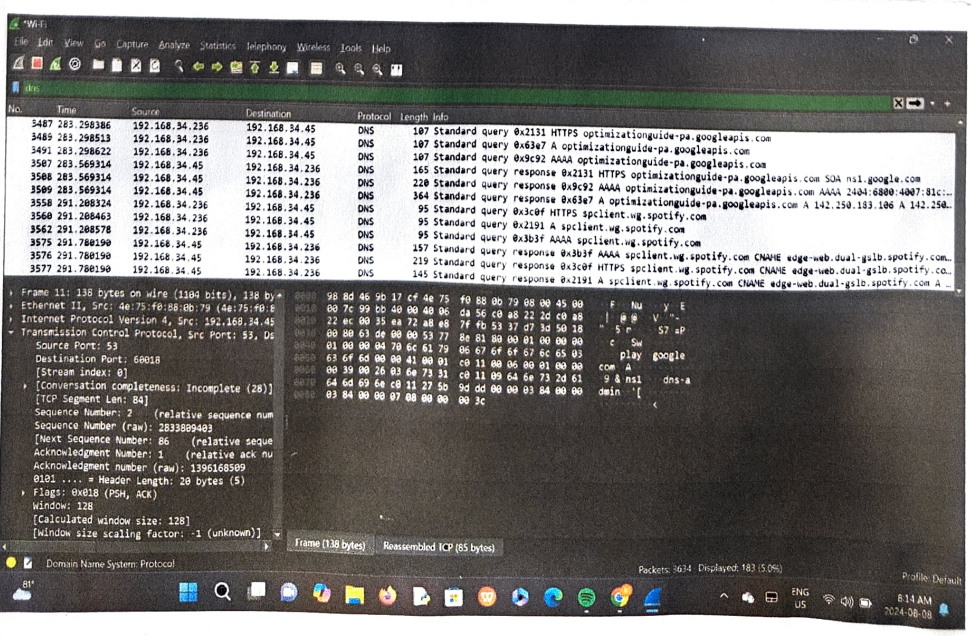


Packet Loss, Details and Bytes

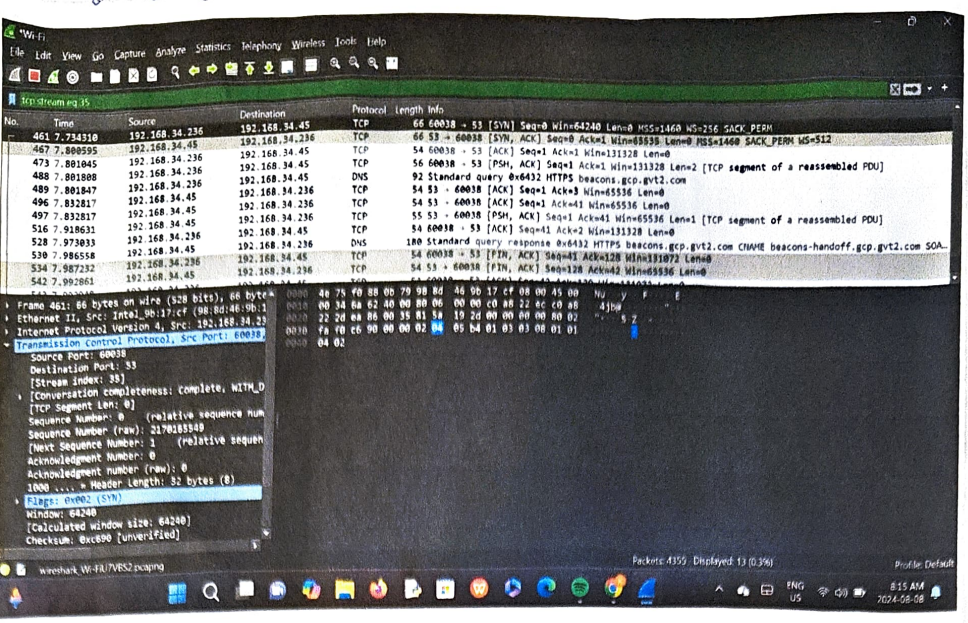


Capturing Filters

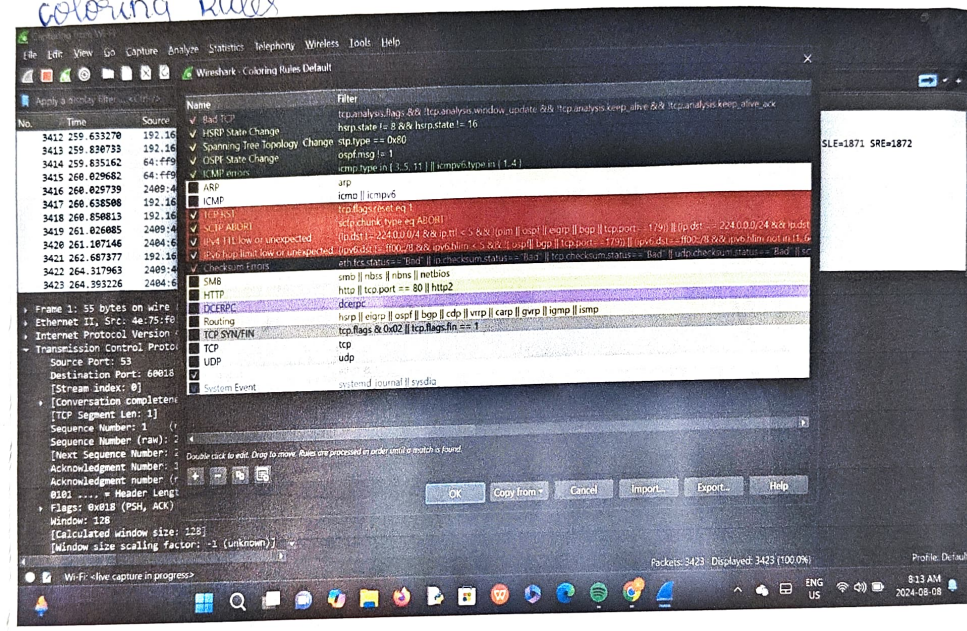




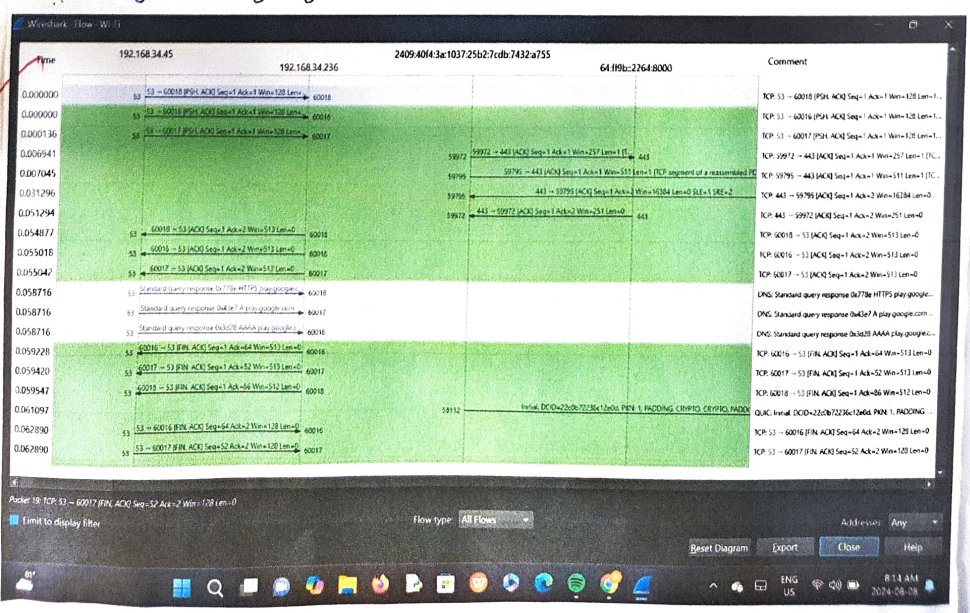
Displaying Filters



Coloring Rules



Workflow graph



Student's Observation

1. Promiscuous mode is a network interface setting that allows card to intercept and read all network packets on network segment
2. NO ARP packets do not have transport layer header
3. DNS primary user UDP for its transport layer protocol
4. HTTP protocol uses port number 80 by default
5. It is a broadcast IP address which is used to send packets to all devices on a specific network segment

Result

9/8/24

Thus the experiments on packet capture tool wireshark is studied and observe