Experiment 5
Date 9-8-24

AIM

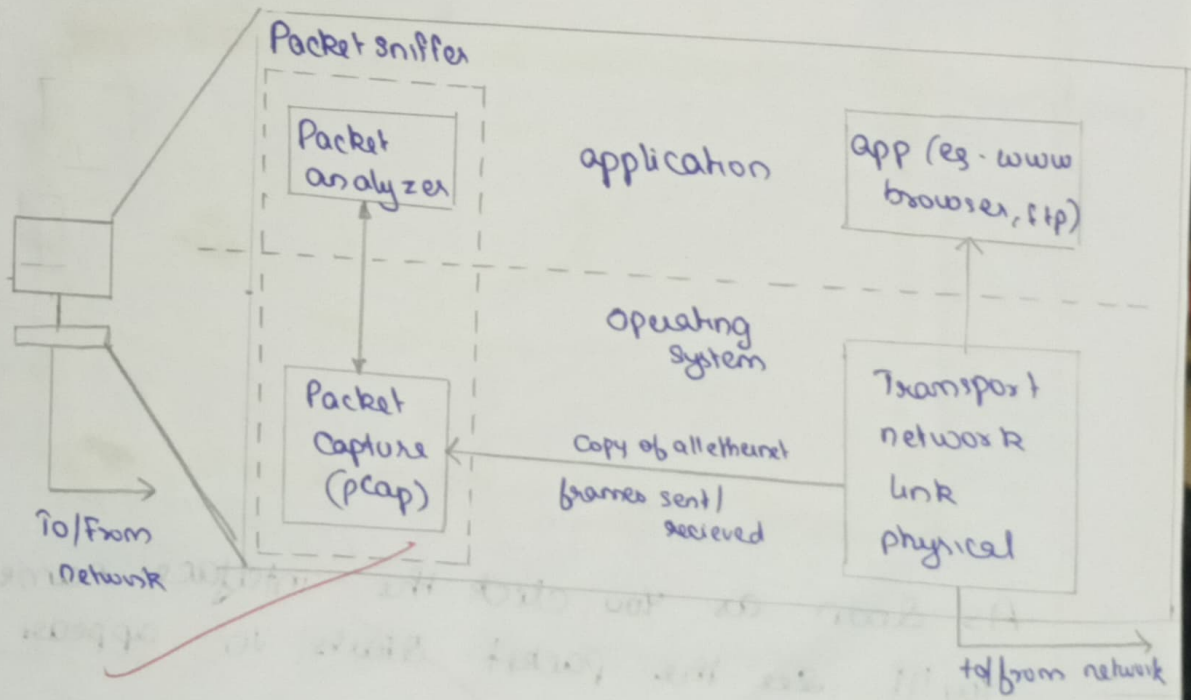
Experiment on Packet Capture tool : Wireshark

Packet Sniffer.

- Sniff message being sent/recieved from/by computer
- Stores & display content of various protocol
- passive programs
  - never send packet itself
  - no packet addressed to it
  - recieved a copy of all packets

Packet Sniffer structure Diagnostic tools

- tcpdump
  - eg : tcpdump -enx host 10.129.41.2 -w exe3.out
- wireshark
  - wireshark -r exe3.out



Wireshark

* network analysis tool
* formerly known as Ethereal
* capture packets in real time & display in human readable form
* include formats, filter, color coding etc

Uses

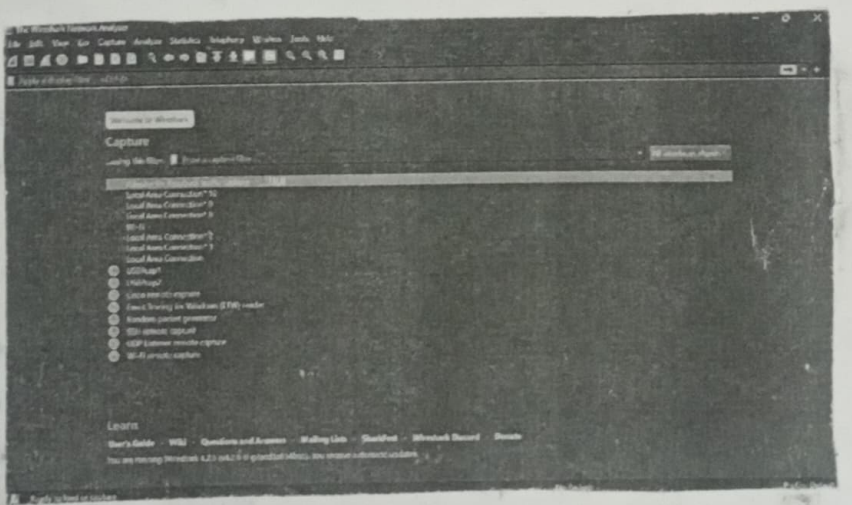
* troubleshoot
* examine security problems

Download Wireshark

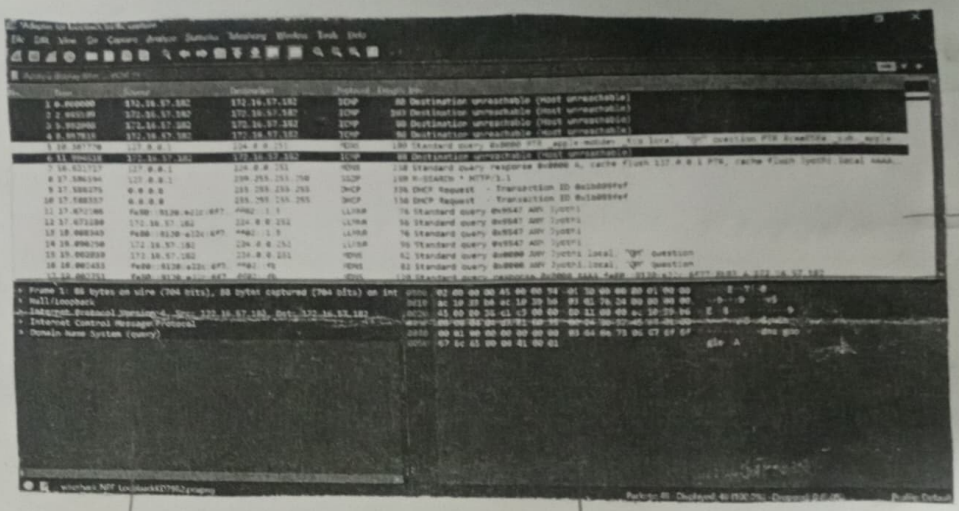
- download & install from www.wireshark.org

Capturing packets

- Launch wireshark & double click on name of network interface



As soon as you click the interface name you'll see the packet starts to appear in real time



Packet details

Packet Byte

Packet List

Colorcoding rules

* colours have been assigned for each packets

  view → Colorizing Rules

Filtering packets

* display orderly

  → type into filter box at top of window

* clicking Apply

TCP Conversation

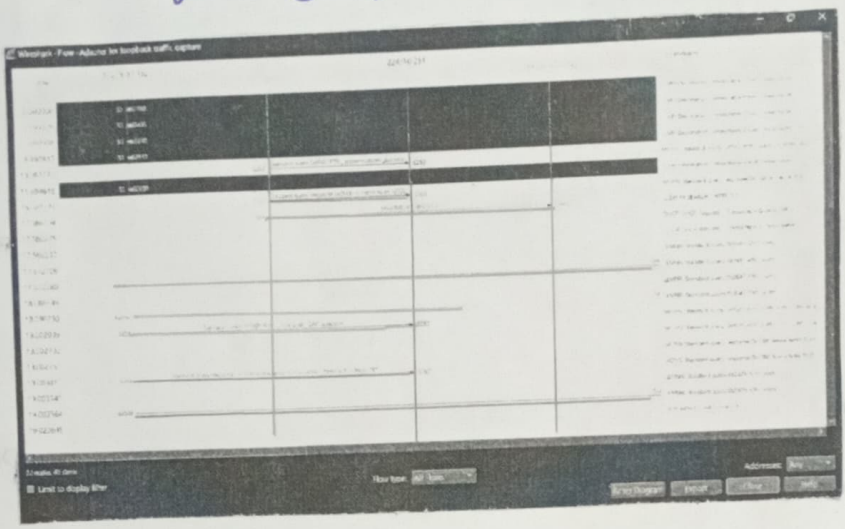
→ right click on a packet → follow → TCP stream.

Inspect Packet

→ click a packet to view details of packet & dig down

Flow graph

→ network interface → statistics → flow graph



Student Observation

1) What is promiscous Mode?

A network interface card mode mode that allows it to capture all traffic on the network, not just the traffic intended for its own mac address

2) Does ARP packets has transport layer header? Explain.

No, ARP packets do not have transport layer header

3) Which transport layer protocol is used by DNS

→ UDP (User datagram Protocol)

4) Port number used by HTTP protocol

→ 80

5) What is a broadcast IP address?

→ used to send data to all devices on a network. ~~for~~ for IPV4, it is highest address in a subnet

8 Ile
9/8/24.

Result

Thus the packet capturing tool - Wireshark is installed & studied.