Experiment: 8
Date: 9/8/24

Aim:

Experiment on ~~on~~ packet capture tool Wireshark.

Packet Sniffer:

=) Sniff message being sent/recieved from/by computer.

=) Stores & display content of various protocol.

=) Passive program

(*) never send packet itself

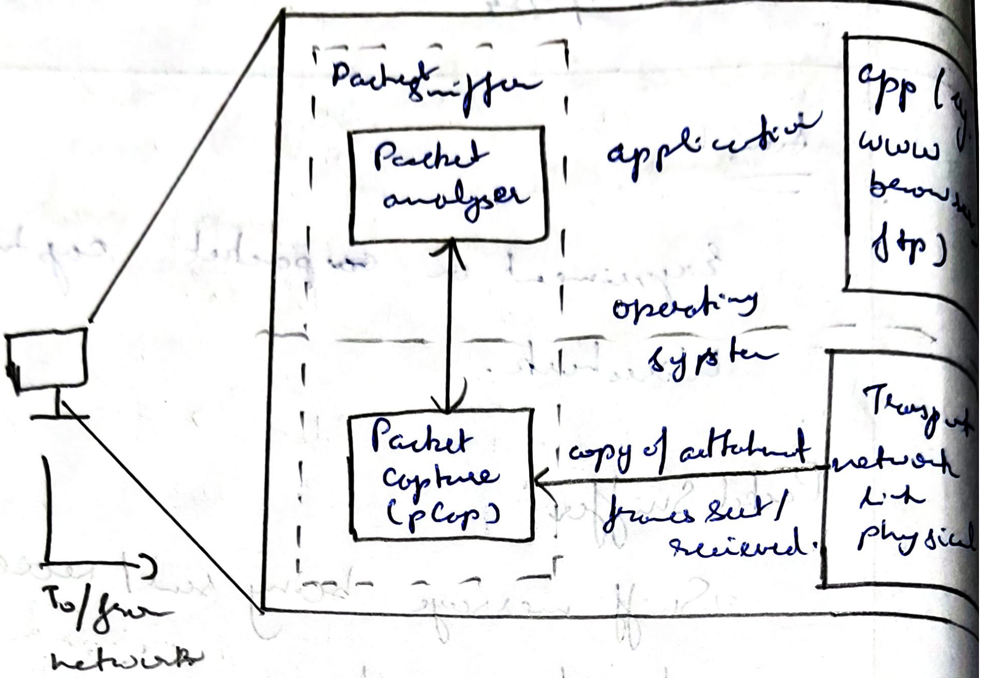
(*) no packet addressed to it

(*) recieves a copy of all packets.

Packet sniffer structure diagonistic tools.

(*) tcpdump

(*) wireshark.



Wireshark:

(i) network analysis tool.
(ii) formerly known as ethereal.
(iii) captures packets in real time & display in human readable form
(iv) include formats, filters, color coding etc.

Uses:

(i) troubleshoot
(ii) examine security protocol.

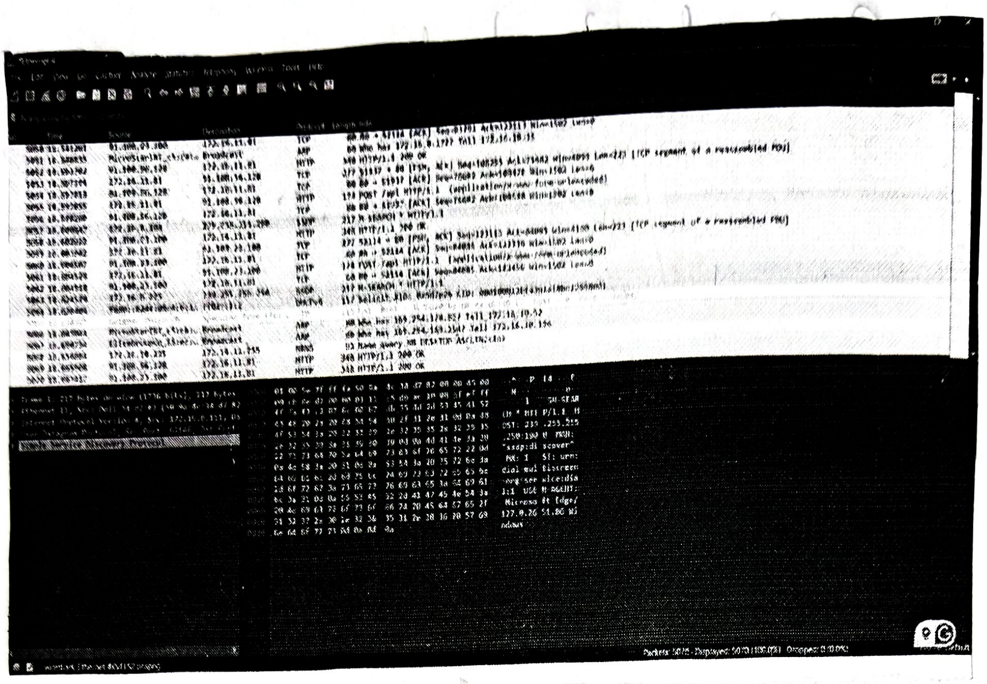
Download Wireshark:

(*) Download & install from www.wireshark.org.

(*) Capturing packets:

(i) 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.



Colourcoding Rules:

(i) colours have been merged for each packets view → colouring rules.

Filtering Packets:

(i) Display orderly.

(ii) type into filter box at the top of the window & ~~clicking~~ clicking apply.

TCP conversation:

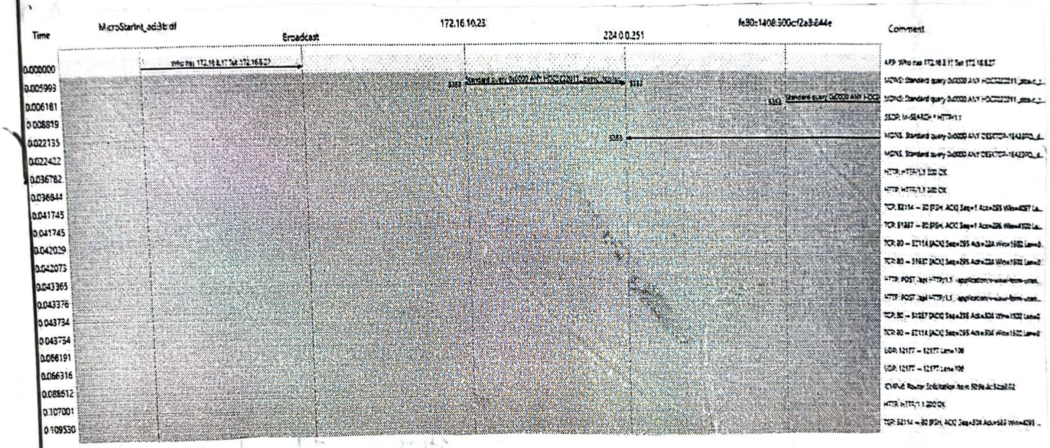
→ right click on a packet → follow → tcp → stream.

Inspect packet:

Click packets to view details of packet & dig down.

Flowgraph

→ network interface → statistics → flow graph



Student Observation:

(1) What is promiscuous mode?

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

(2) Does ARP packets has transport layer header? explain?

No, ARP ~~pip~~packets do not have transporter layer header.

(3) Which transport layer protocol is used by DNS?

-> UDP

(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 IPV_4, it is highest address in a subnet.

8/8/24

Result

Thus the packet capturing tool wireshark is installed & studied.