EXP-NO: 05

DATE: 09-08-24

EXPERIMENTS ON PACKET CAPTURE TOOL: WIRESHARK

AIM:

Experiments on Packet capture tool: Wireshark.

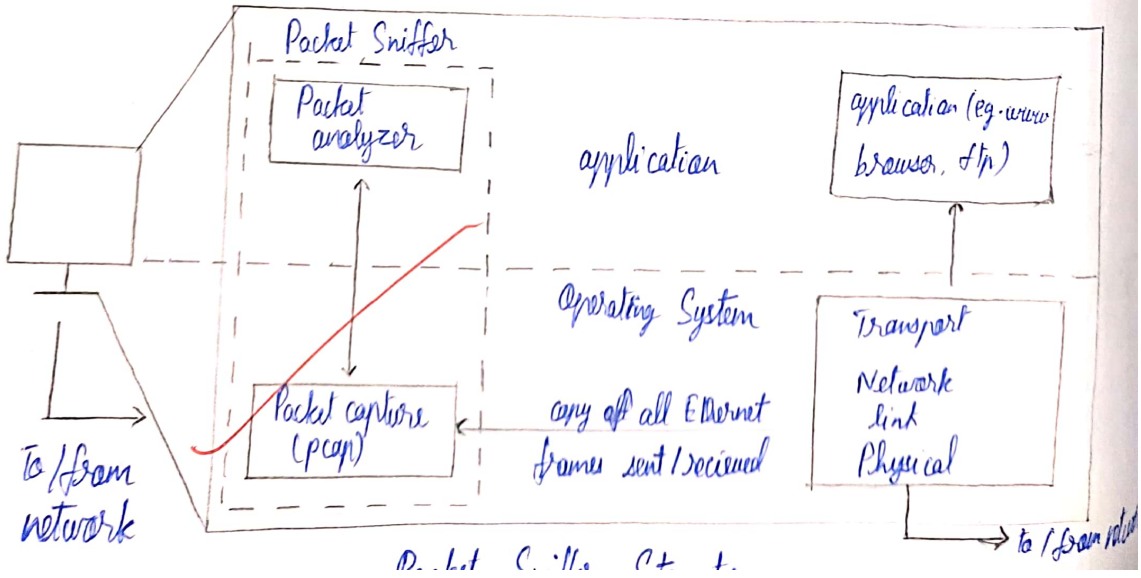
Packet Sniffer

→ Sniff message being sent / recieved from / by computer.
→ Store & display content of various protocol
→ Passive program
- never send packet itself
- no packet addressed to it
- recieved a copy of all program

Packet Sniffer Structures Diagonistic tools

→ Tcpdump
- eg: tcpdump -env host 10.129.41.2 -w exes.out

→ Wireshark
- wireshark -r exe3.out



Inspect Packet

→ click on packet to view details of packet & dig down.

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

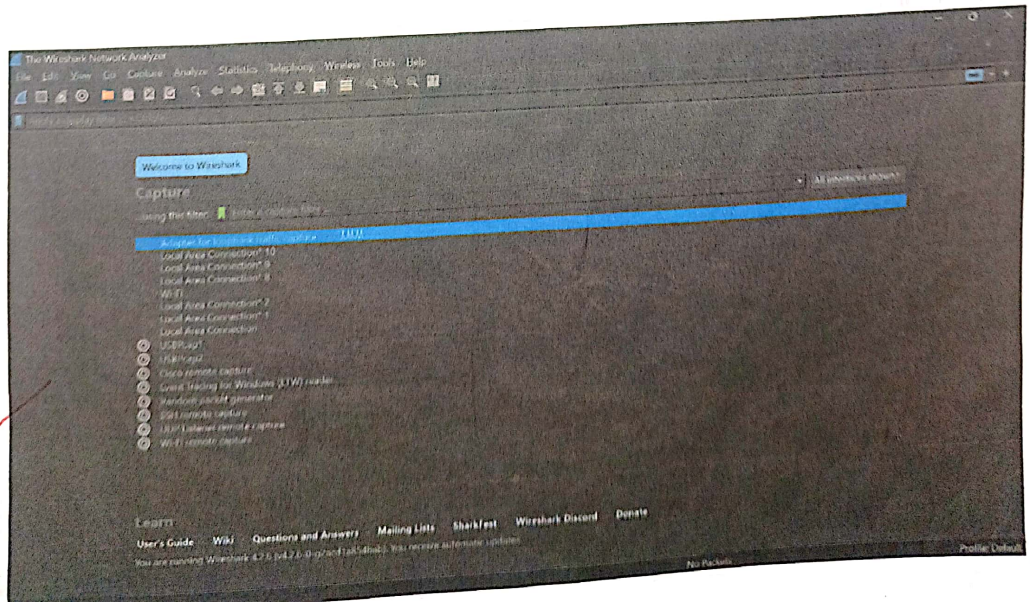
* Troubleshoot
* Examine security problems

Download Wireshark

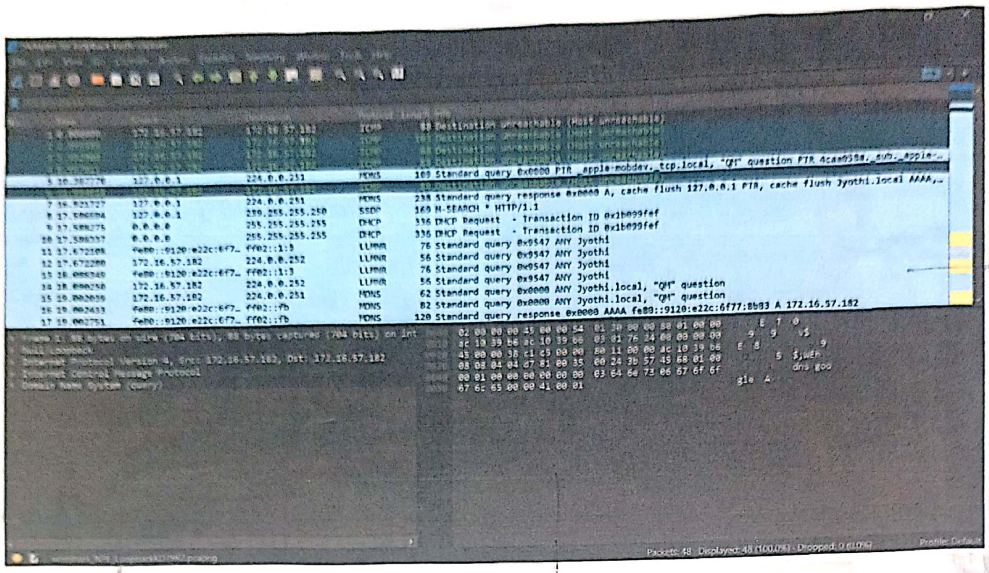
* Download & install from www.wireshark.org

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

Color coding rules

* Colors have been assigned for each packets viewer → coloring ru

Filtering Packets

* Display orderly

→ type into filter box at top of window & clicking Apply.

TCP Conversation

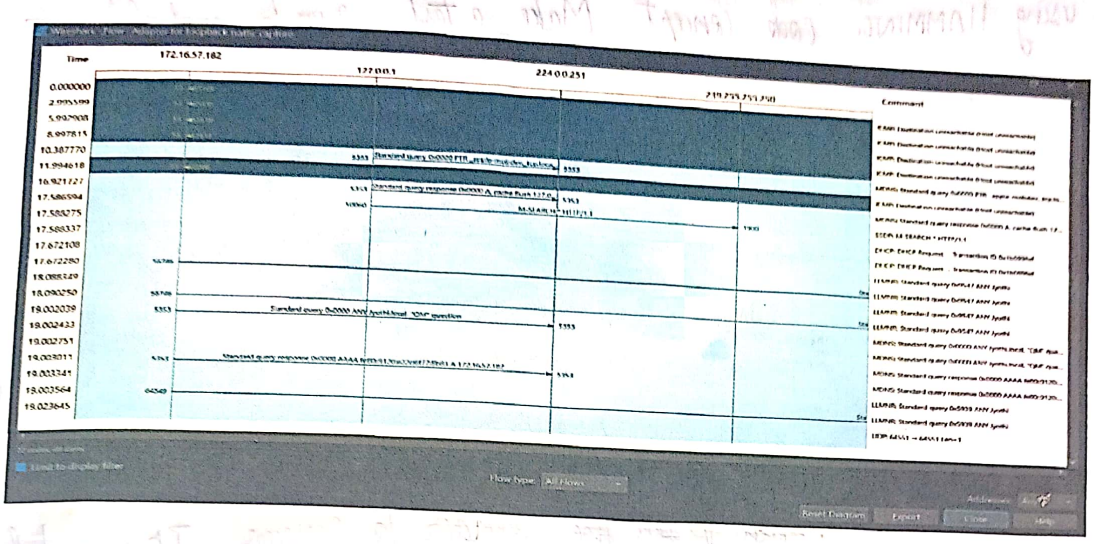
→ right click on a packet → follow → TCP stream

Inspect Packet

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

Flow graph

→ network interface → Statistics → flow graph



Student Observation:

1. Promiscous mode is a An network interface card mode that allows it to capture all traffic on the network. not just the traffic intended for it's own mac address.

No. ARP packets do not have transport layer header.

UDP (User datagram Protocal).

80.

→ Used to send data to all devices on a network. For ~~IPv4~~ it is highest address in a subnet.

9/8/24.

RESULT:

Thus the packet capturing tool wireshark is installed & studied.