EXNO: 05

DATE: 0~~8~~9.08.2024

Wrieshark.

AIM:

→ Experiment on Packet capture tool: Wrieshark.

Packet sniffer

→ Sniff message bring sent / received from / by computer

→ Stores & display content of various protocol

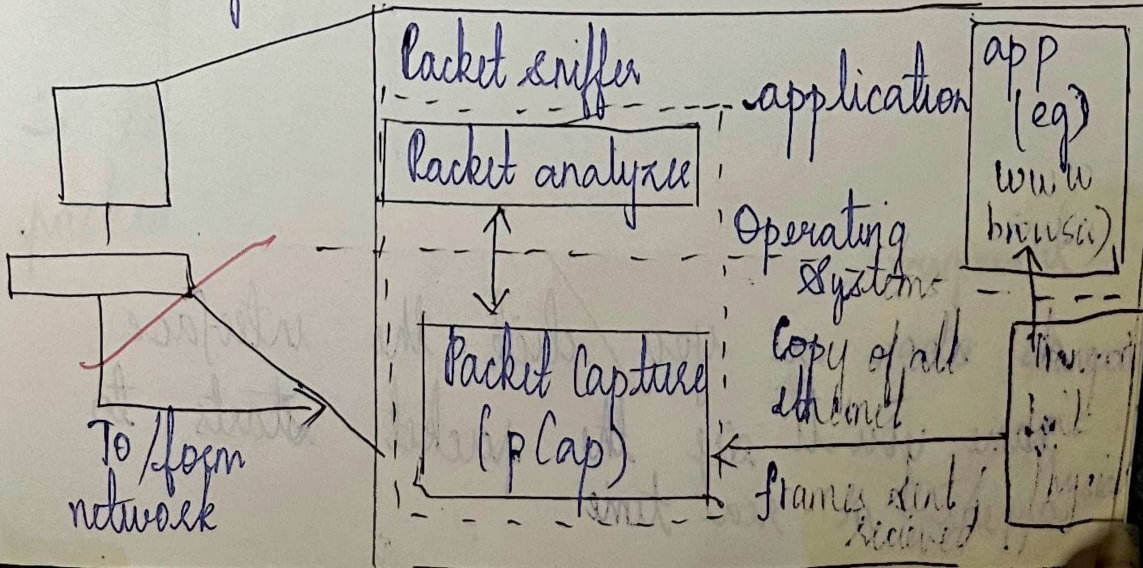
→ Passive program

→ never send packet itself

→ no packet adressed to it

→ recieve a copy of all protocols

- Tc pdump.
  - eg: tcdump - enx host 10.129.41.2 _to exe 3.00t
- Wrieshark
  - eg: exe 3.out



Wireshark

→ network analysis tool

→ formerly known as Ethereal

→ Capture packets in real time and display in human readable form

→ Include formats, filter, color coding etc

Uses

→ troubleshoot

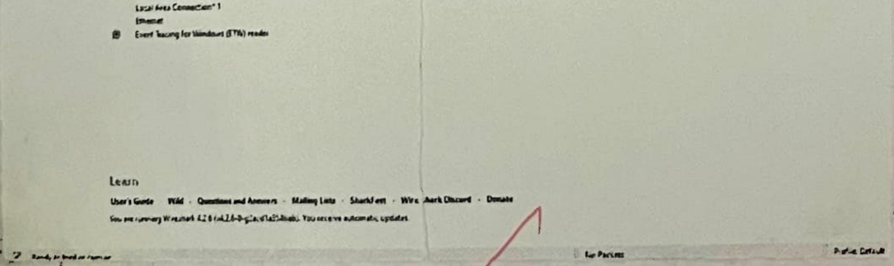
→ examine security problems

Download Wireshark

download and install from www.wireshark.org

Capturing Packets

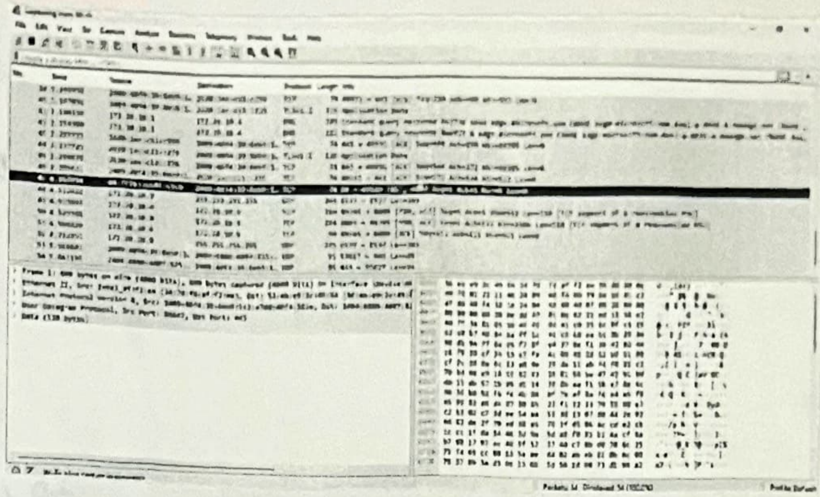
Launch wireshark and double click on name of network interface



Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 1
Ethernet
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.6 (v4.2.6-0-g[illegible]). You receive automatic updates.

soon as you click the interface you'll see the packet starts to [illegible] real time



Colorcoding rules

→ Colours have been assigned for each packets

View → Colouring Rules

Filtering packets

→ display orderly

→ type into filter box at top of window and clicking apply

TCP Conversion

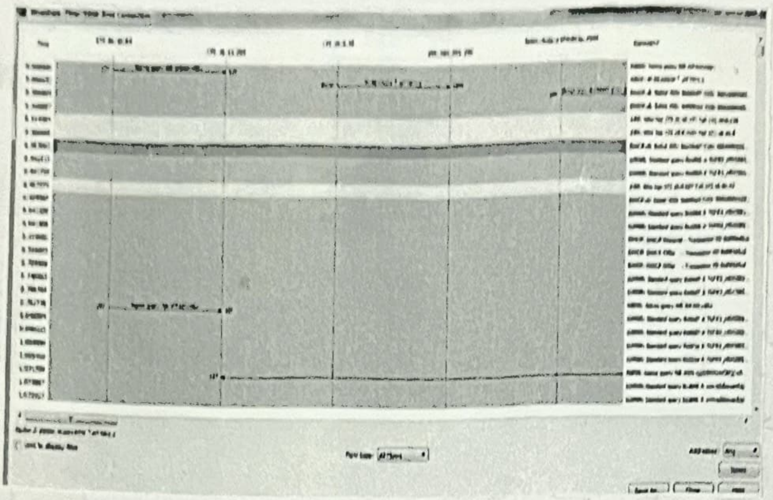
→ Right click on a packet → follow → TCP stream

Inspect packet

→ Click a packet to view details of packed ~~and~~ dig down

Flowgraph

→ network interface → Statistics → flow graph



Student Observation

1. What is promiscous Mode?

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

2) Does ARP ~~can~~ packets is 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 Procotocol

4) Port number used by HTTP Protcol?

→ 80

5) What is a broadcast IP address?

→ Used to send ~~addre~~ data to all devices on a network. for IPV4, it has highest address in a subnet.

Result:

8

9/8/24

Thus the packet capturing tool Wireshark is installed and studied.