EX:5

Date: 9/8/2024

EXPeriments on Packet capture tool: wireshark

Aim:

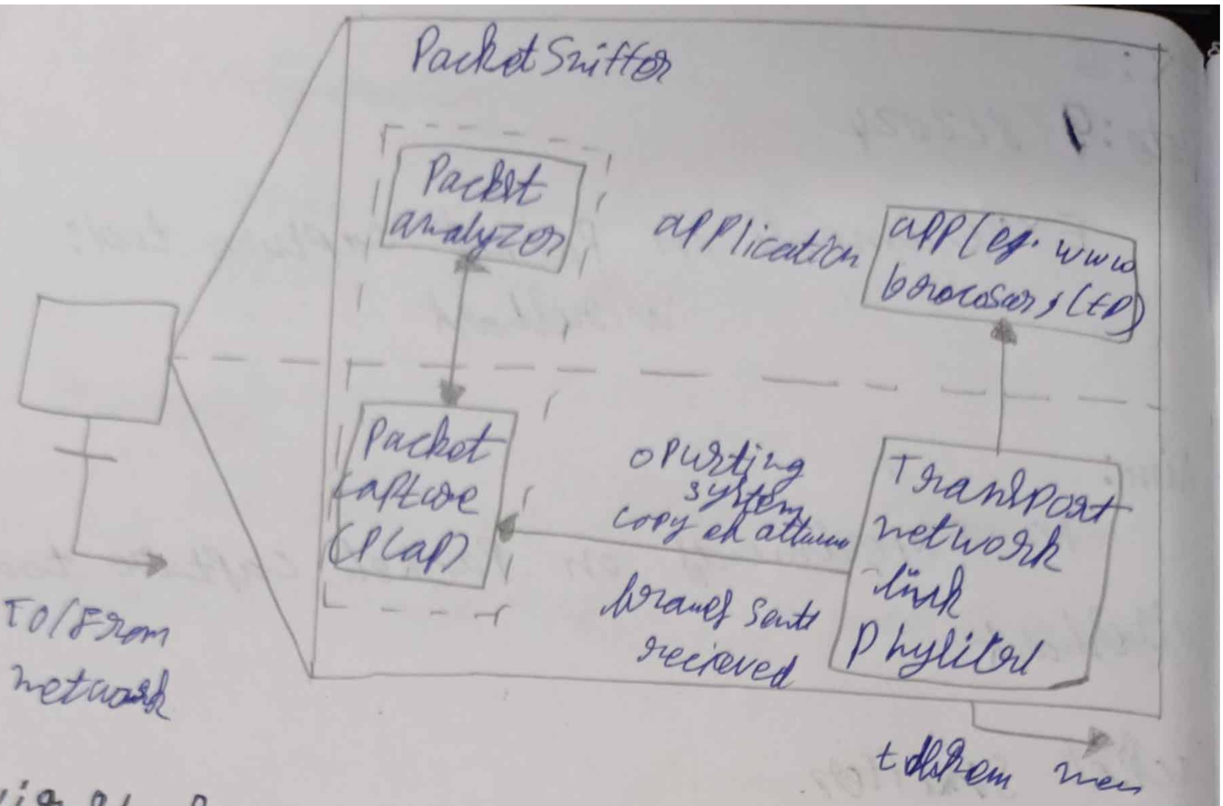
TO Experiments on Packet capture tool: wireshark

Packet Sniffer.

- Sniff message being sent/recieved from/by compilers
- Stored & desplay content of various Protocol
- Passive Program
  - never send Packes itslf
  - no Packet addressed to it
  - recieved a copy of all Packets

Packet Sniffer Structure Diagnostic tools

- Tcpdump
  - eg. tcdump -enx host 10.129.41.2 -w exe3.out ~~wireshark~~
- wireshark
  - wireshark -r exe3.out



wireshark

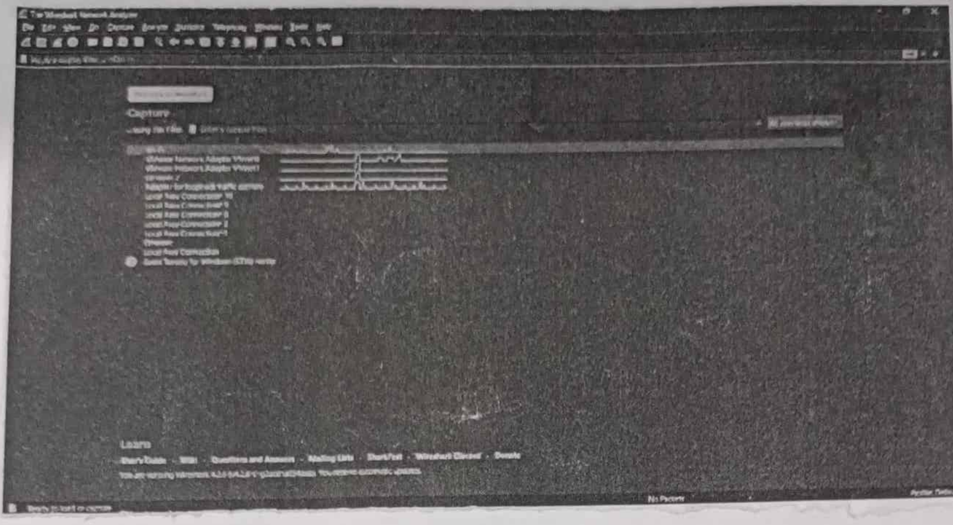
- ✩ network analysis tool
- ✩ formerly known as Etherial
- ✩ Capture Packets in real time & display in human readable form
- ✩ include formats, filter, color coding etc uses
- ✩ troubleshoot
- ✩ examine Security Problems

Download wireshark

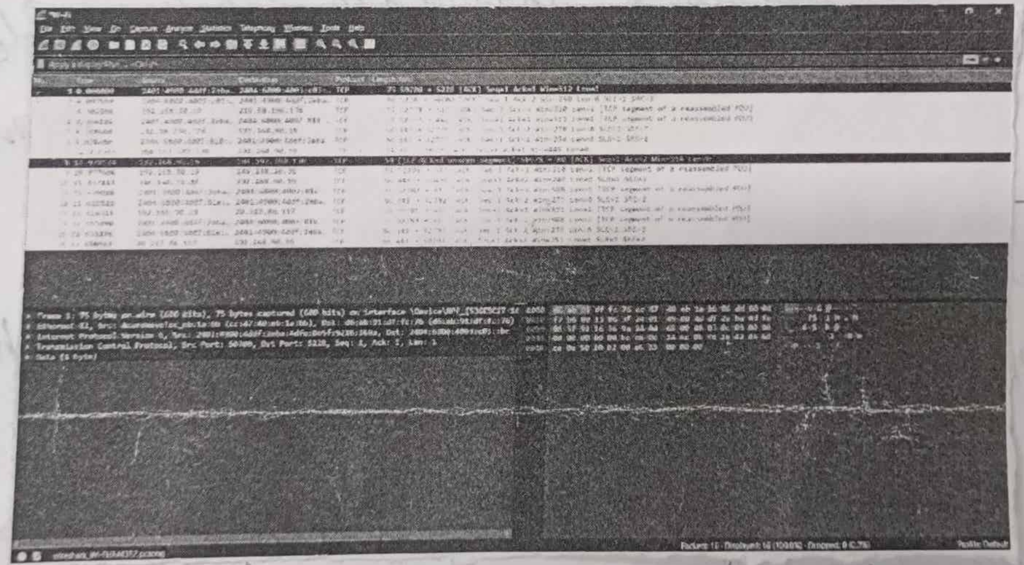
- download & install from www.wireshark.org

Capturing Pockets

- Launch wireshak & double click on name ob network inteyace.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture
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* 2
Local Area Connection* 1
Ethernet
Local Area Connection
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default

As Soon as you click the interface name You'll See the Packet starts to appear in real time


Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Profile: Default

```
Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{53CE5C27-1E
Ethernet II, Src: [illegible], Dst: [illegible]
Internet Protocol Version 6, Src: 2401:4900:[illegible], Dst: 2404:6800:4003:c03::bc
Transmission Control Protocol, Src Port: 50300, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
Data (1 byte)
```

Packet details

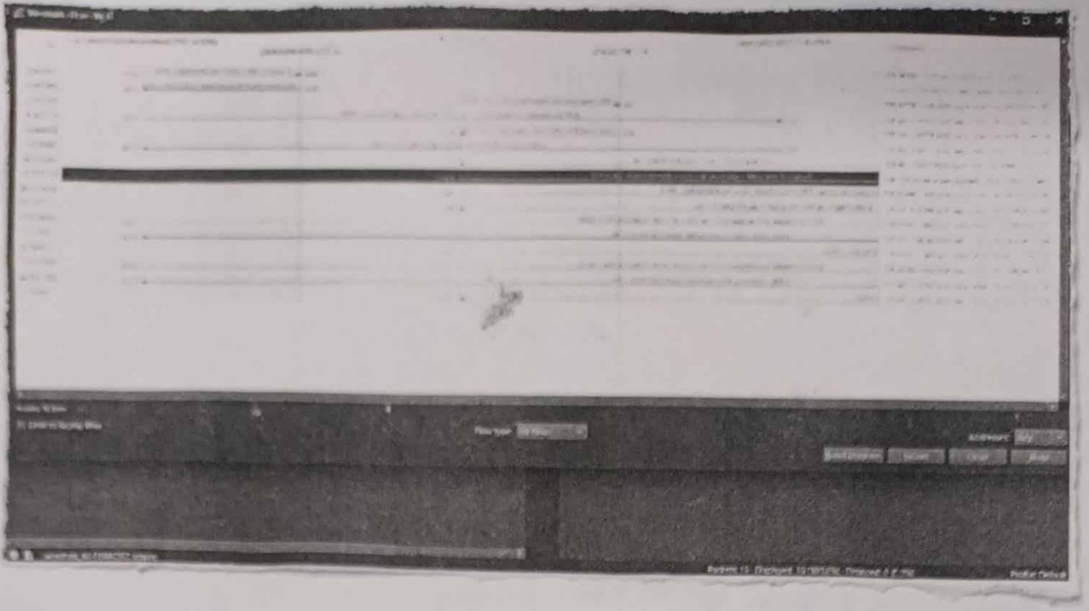
Packet Byte

Packet list

Flow graph

→ network interface → statistics →

flow graph



Student Observation

1, What is Promiscous Mode?

A network Interface card mode that allows it to capture all 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 IPV4, It is highest address in a subnet.

8

9/8/24

Result:

thus the packet capturing tool - wireshark is installed & studied.