Ex No: 5 Experiment on Packet
Date: 9:8:24 Capture tool: wire Shark

AIM:

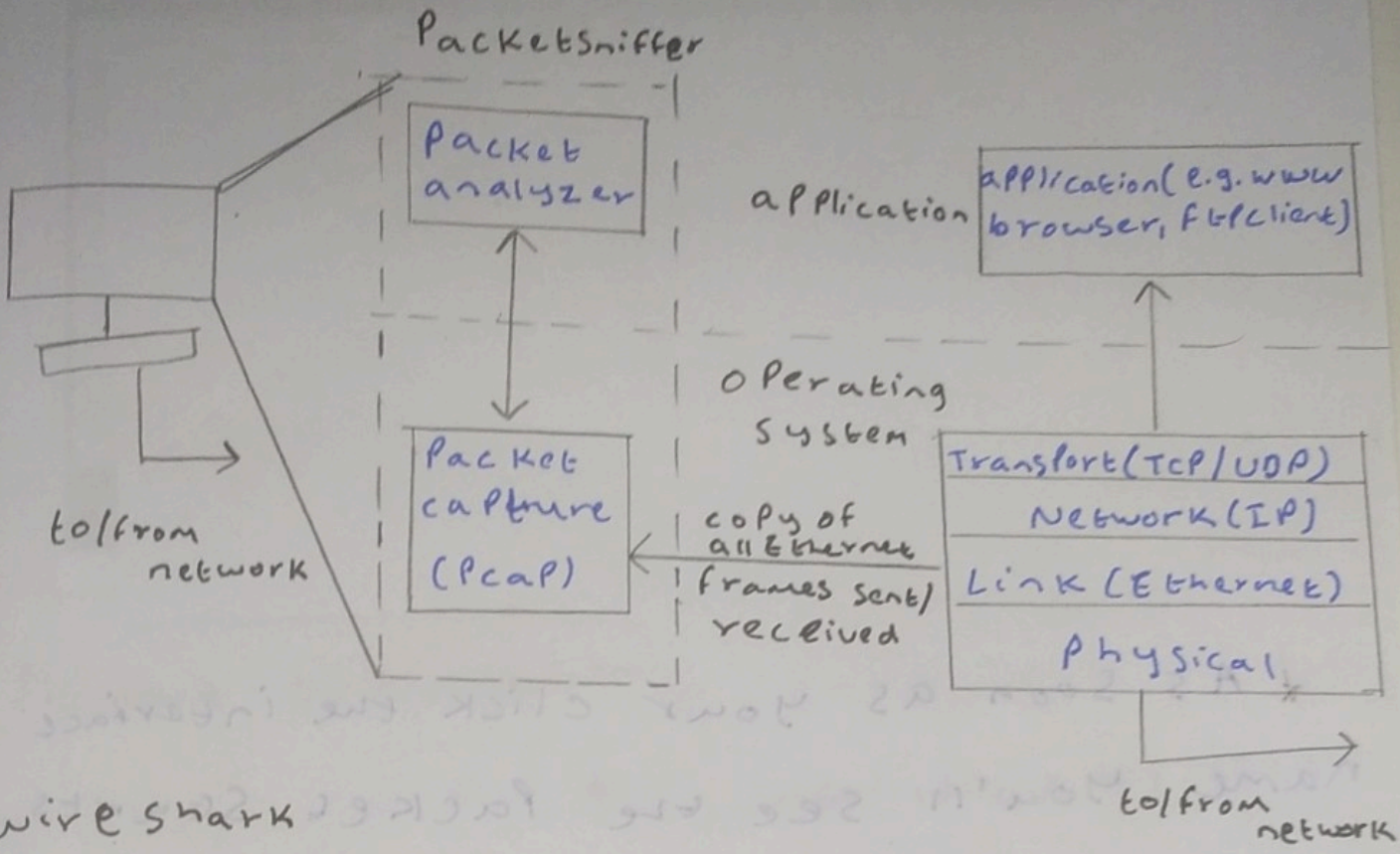
Experiment on Packet Capture tool: Wire Shark

Packet Sniffer

- Sniffs messages being sent/received from/by your computer
- Store and display the contents of the various Protocol field in the messages.
- Passive Program
  - never sends Packets itself
  - no Packets addressed to it
  - receives a copy of all Packets (Sent/received)

Packet Sniffer Structure Diagnostic Tools

- TCPdumP
  - E.g. tcpdumP -enx host 10.129.41.2 -w exe3.
- wireshark
  - wire Shark -r exe3.out



Wireshark

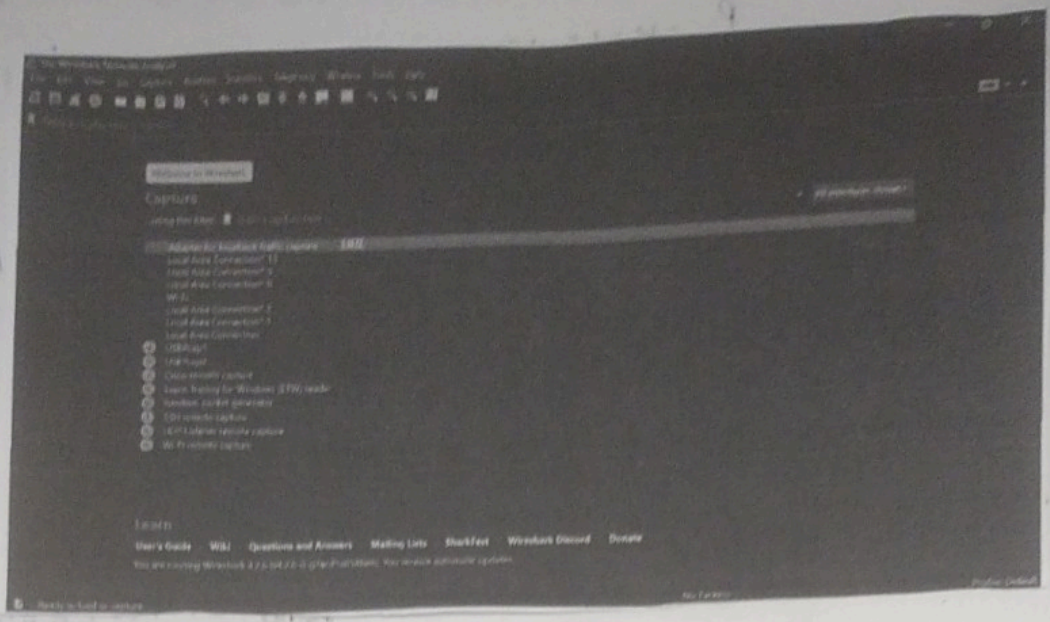
* network analysis tool
* formerly known as Ethereal
* capture packets in real time display in human readable form
* include formals, filter, color coding etc.

Download wireshark

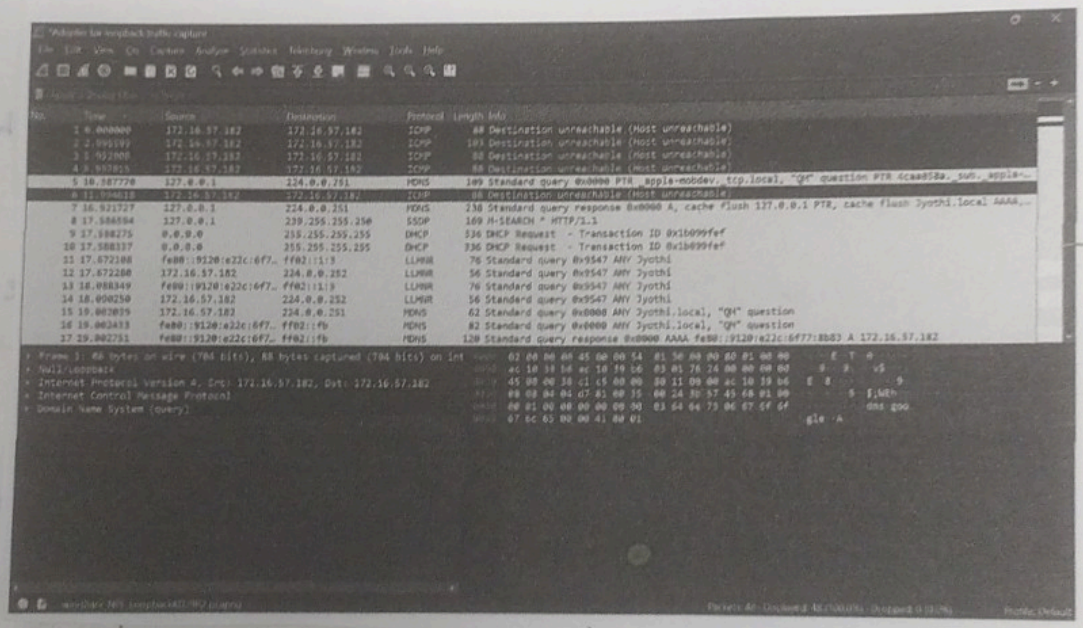
- download & install from www.wireshark.org

Capturing Packets

- Laangh wireshark & double click on name of network interface.



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



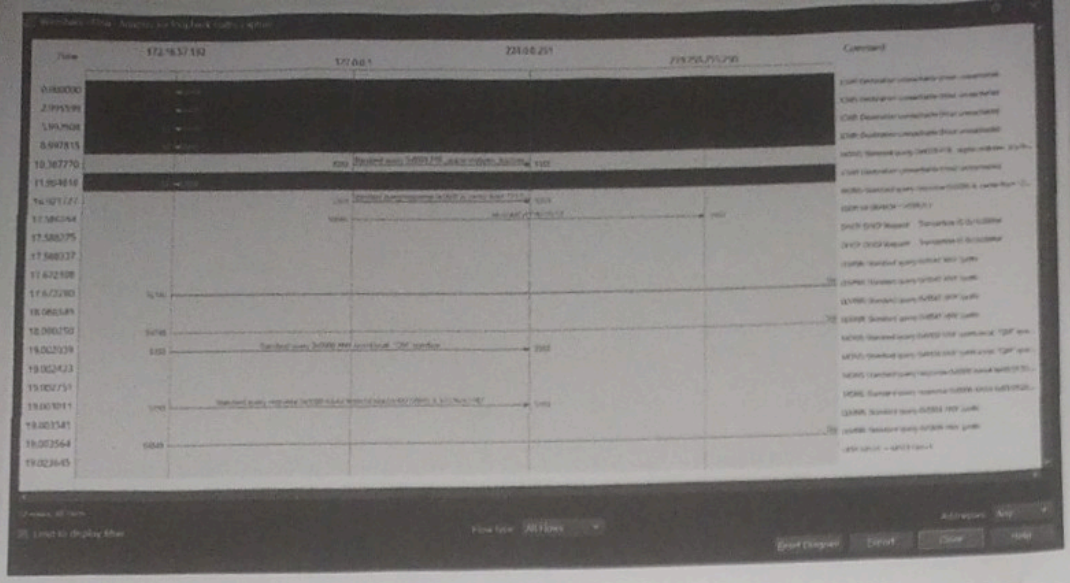
Packet details

Packet Byte

Packet list

Flow graph

→ Network interface → Statistics → flow graph



Student observation:

1) what is Promiscous mode?

A network Internet card mode that allow it to capture all traffic intended for its own mac address

2) Dose 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 data gram 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 or IPV4, It is highest address in a subnet.

Result:

thus the packet capturing tool wireshare is installed & studied.

9/8/24