Exp :05

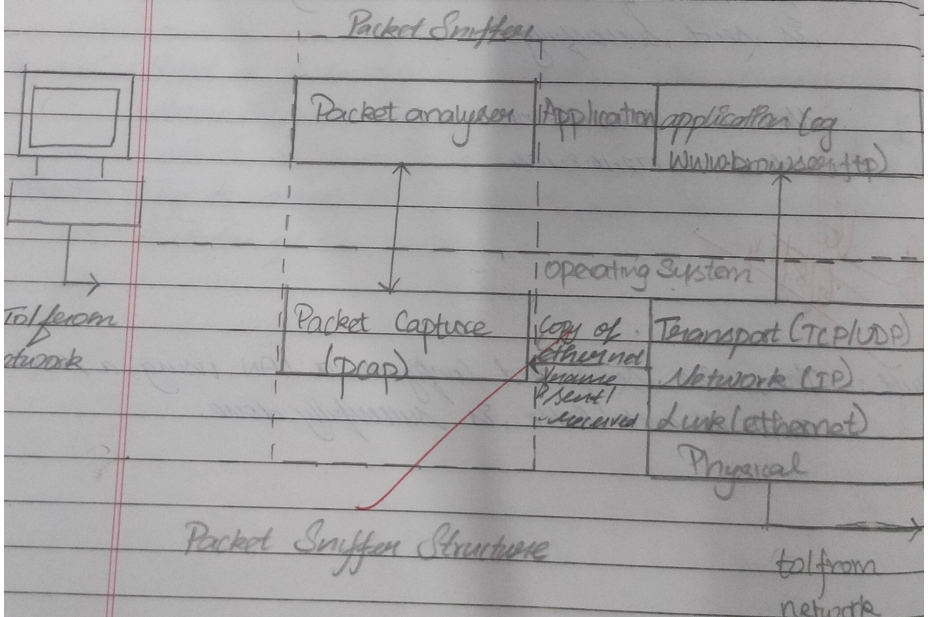
09-08-24. Experiments on Packet Capture tool : Wireshark.

Aim :- Experiment on packet capture tool : Wireshark.

Packet Sniffer :-

* Sniff messages being sent/received from/by your computer.
* Store and display the content of various protocol field in message.
* Passive program
  - Never send packet itself.
  - No packet addressed to it.
  - Receives a copy of all packets (sent/received).

Packet Sniffer Structure



Packet Sniffer Structure

Page
Date

Wireshark
* Network analysis tool
* Formally known as Ethereal
* Capture packet in real time and display in human readable form.

Uses
* Troubleshoot
* Examine security problem.

Download Wireshark
* Download & install from www.wireshark.org

Capturing packet
* Launch wireshark and double click on name of network interface.

Apply a display filter ... <ctrl-/>

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.57.182	172.16.57.182	TCMP	68	Destination Unr
2	2.958961	172.16.57.182	172.16.57.182	ICMP	105	Destination Unrea
3	5.078763	172.16.57.182	172.16.57.182	ICMP	88	Host unreachable
4	8.9686950	172.16.57.182	172.16.57.182	TCMP	88	Host unreachable
5	10.896540	127.0.0.1	224.0.0.251	MDNS	103	Host unreachable
6	11.986785	172.16.57.182	172.16.57.182	ICMP	76	Standard Query
7	16.763856	127.0.0.1	239.255.255.250	SSDP	73	Standard Query
8	17.968644	127.0.0.1	ff02::1:3	MDNS	82	Standard Query

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

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

... using this filter | Enter a capture filter | All interfaces

Adapter for loopback traffic capture

local area Connection* 10

local area Connection 9

local area Connection 8

Local area Connection 7

Color coding rules

* colours have been assigned for each packet

View → colouring rules

Filtering packet

* display orderly

→ Type into filter box at top of window

* click apply

TCP Conversation

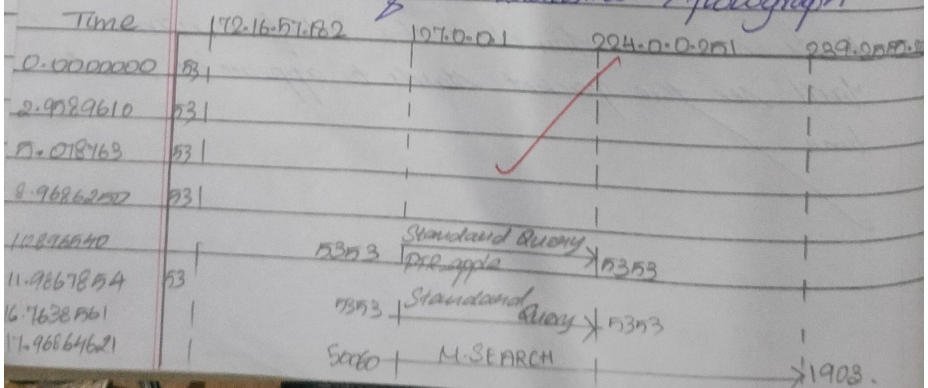
→ Right click on a packet → follow → TCP Stream

Inspect packet

→ click a packet to view details of packet

Flow graph

→ network interface → statistics → flow graph



Page
Date

Student observation

① what is promiscous mode?

A network Interface Caard mode that allows it to Capture all traffic on network, not just the traffic intended for its own mac address.

② Does ARP packet has transport layer header? Explain

No, it do not have 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 broadcast IP address?

Used to send data to all devices on network. For IPV4, it is highest address in subnet.

Result: Thus, the packet capturing tool wireshark is studied & installed.

9/8/24