EX.NO:3
29/08/24

Experiments on Packet Capture tool: Wireshark.

AIM:

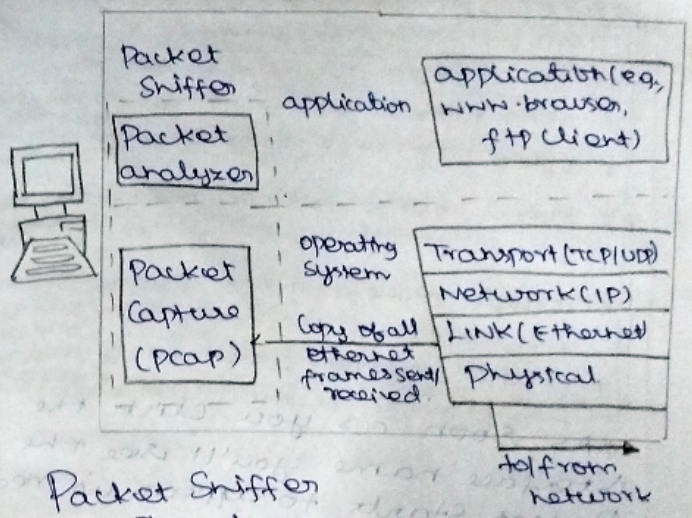
Experiments on Packet Capture tool: Wireshark

Packet Sniffer

* Sniffs message being sent/received from/by your computer
* Store and display the contents of the various protocol fields 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.out
* Wireshark
  - wireshark -r exe3.out



Packet Sniffer Structure.

Wireshark

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

Uses

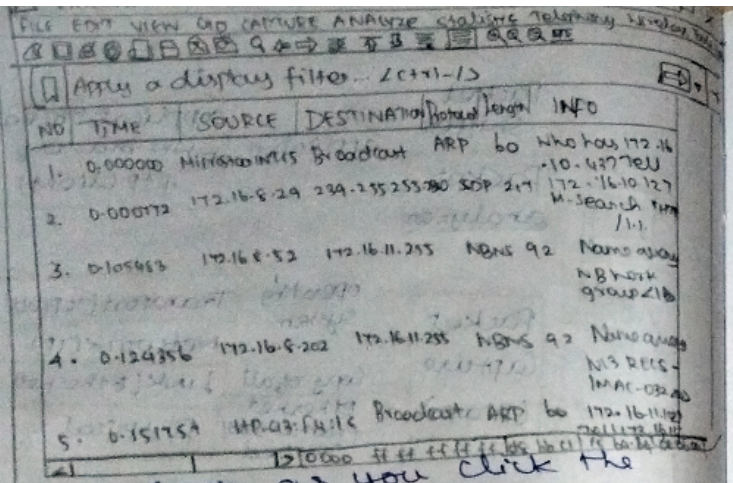
* Trouble shoot
* Examine securely form

Download wireshark

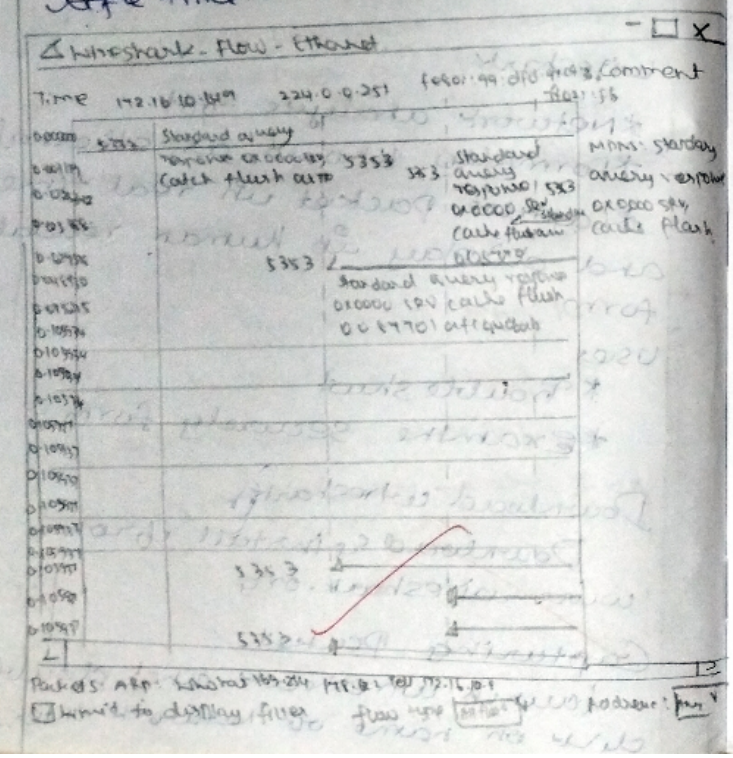
Download & install from www.wireshark.org

Capturing Packet

launch wireshark and 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.



Color loading rules

*Colours have been assigned for each packets 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

→ flowgraph.

Student Observation.

① What is promiscuous mode?

A network interface card 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 headers.

③ Which transport layer protocol is used by DNS

UDP (user datagram protocol)

④ Port number used by http protocol?

The HTTP protocol typically uses port 80. For secure HTTP, which is HTTPS, the default port is 443

⑤ What is a 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.

8/8/24