

8/8/24

# Practical - 5

10/1/2024

Aim

Experiment on Packet Capture tool: wire shark

## Packet Sniffer

\* Sniff message being sent / received from my computer stores & display content of various protocol

\* passive program

- never send packet itself
- no packet address to it
- decrypted and copy of all packets

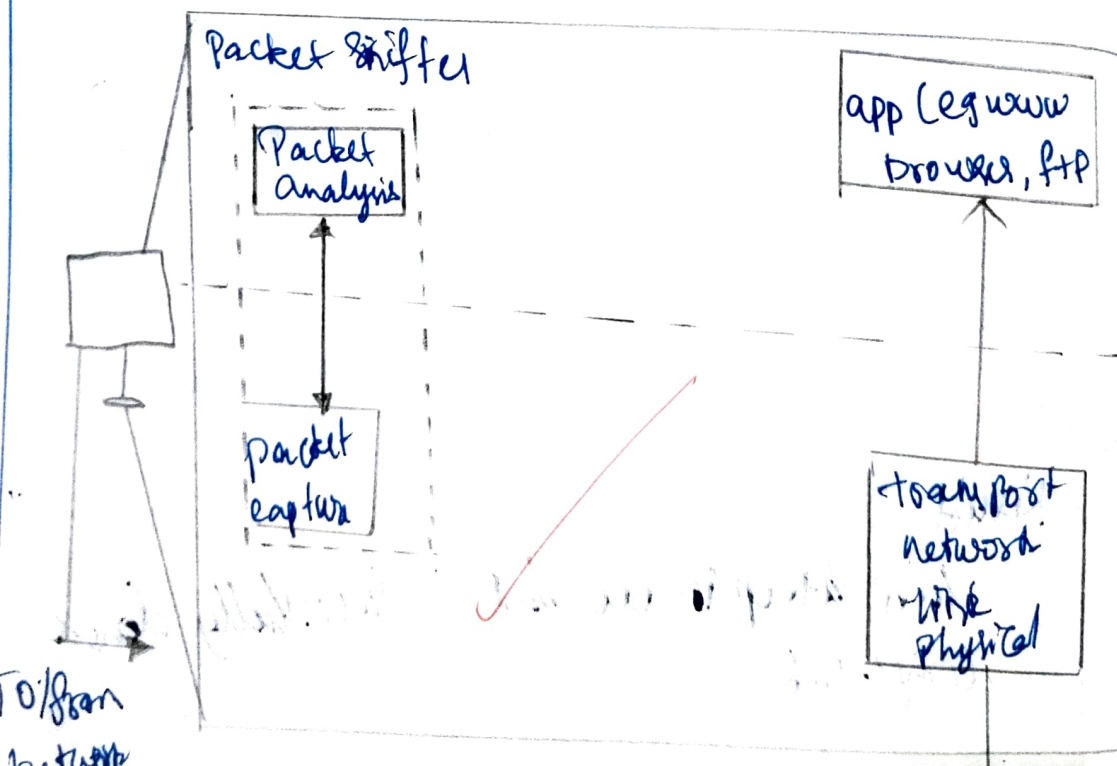
## Packet Sniffer Structure Diagnostic tool

\* Tcpdump

- eg tcpdump - enx host 10.129.41.2 -w exe3.out

\* wire shark

- wire shark - > exe3.out



## Wireshark

- \* network analysis tool
- \* formerly known as Ethereal
- \* Capture packets in real time & displaying human readable form
- \* include formats, filter, color coding etc

## Uses

- \* troubleshoot
- \* examine security problems


## Download Wireshark

- \* download & install from [www.wireshark.org](http://www.wireshark.org)

## Capturing packets

- \* Launch Wireshark \* 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



No.	Time	Size	Protocol	Details
1	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
2	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
3	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
4	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
5	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
6	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
7	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
8	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
9	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])
10	0.000000	60	Ethernet II	En1: [MAC] to [MAC] (Type: [Type])

↓  
Packet details

↓  
Packet Bytes

↓  
Packet list

## Color coding rules

\* Colours have been assigned for each packet  
View → Coloring Rules

## Filtering packets

\* display orderly  
⇒ type into filter box at top of windows  
& clicking Apply

## Top conversation

Bright click on a packets → follow stream

## Inspect Packet

⇒ Click a Packet to view details of packet  
dig down

## Flow graph

### Student observation

1) what is promiscuous 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 packets has transport layer headers?  
Explain

No, ARP packets do not have transport layer headers

3) which transport layer protocol is used by DNS

⇒ ~~UDP~~ (uses datagram protocol)

4) ~~Port number~~ used by HTTP protocol  
⇒ 80

Q) 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.

Result

Thus the packet capturing tool -

Wireshark is installed and studied