9-8-24

PRACTICAL - 5

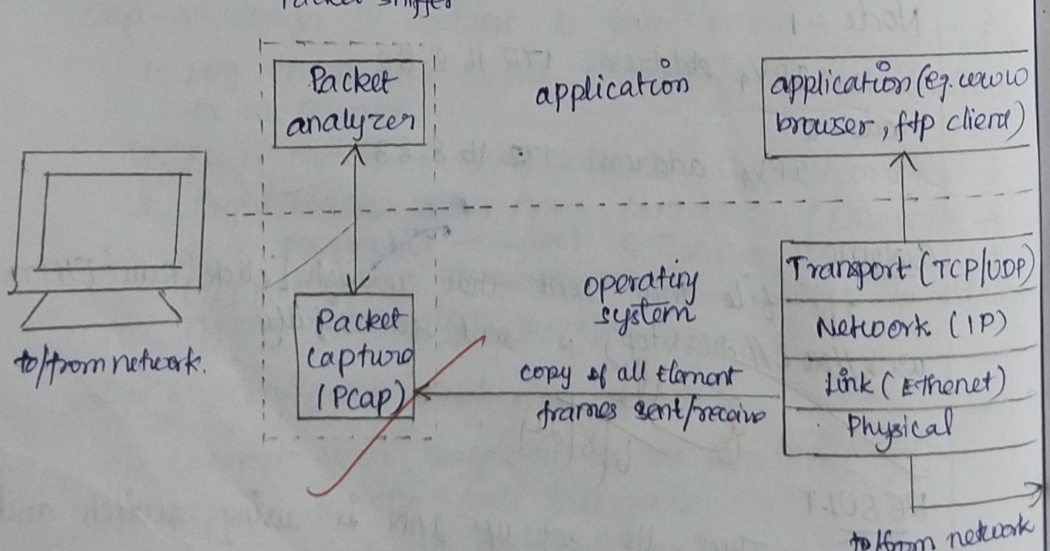
AIM: Experiments on Packet capture tool: Wireshark

Packet Sniffer:

* Sniffs messages being sent/received from/by your computer.
* store and display the contents of the various protocal fields in the messages.
* Passive program.
  - → never sends packets intself
  - → no packets addressed to it
  - ⇒ receives a copy of all packets (sent/received)

Packet Sniffer structure Diaganostic Tools:

* Tcpdump
  - → Eg: tcpdump -exn host 10.129.41.2-10.
* Wireshark
  - ⇒ wireshark -r- exe3. out.



Wireshark

* Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display that in human-relatable format.

What we can do with Wireshark?

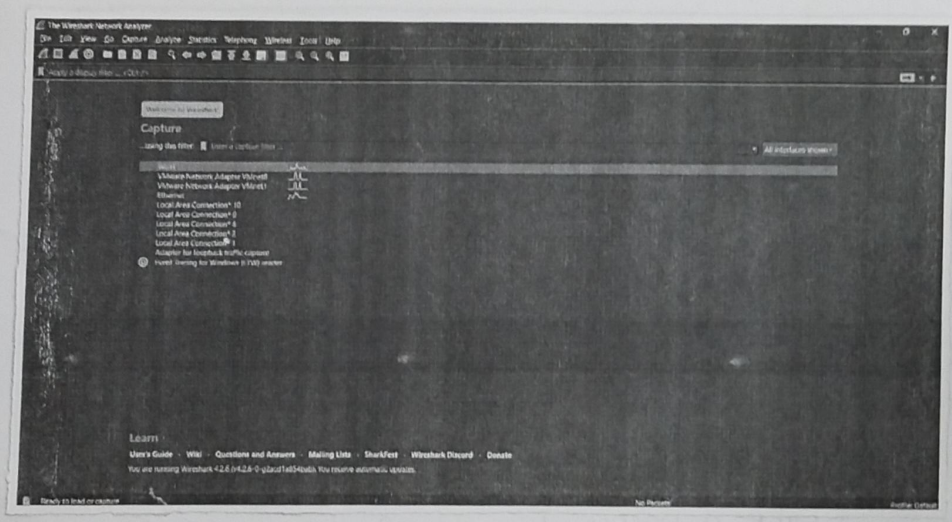
* Capture network traffic
* Decode packet protocals using dissectors

Wireshark used for:

* Network administrators: troubleshoot network problem
* Network security engineers: examine security problems

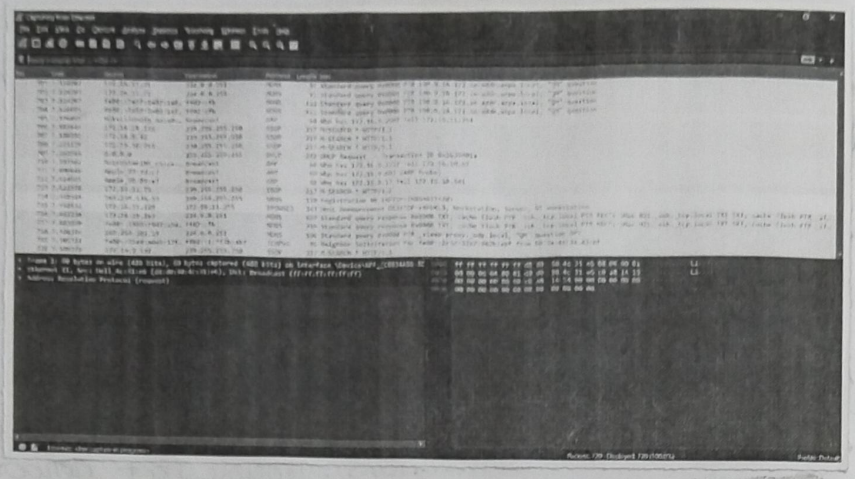
Capturing Packets

* After downloading and installing, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface.



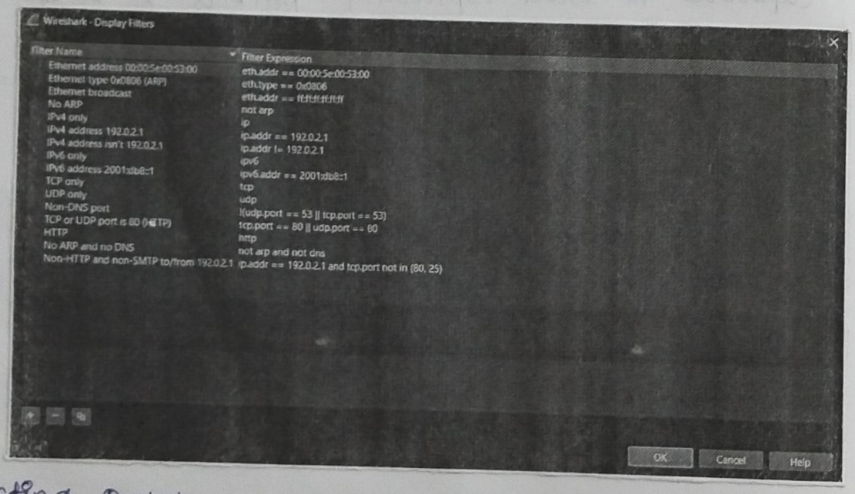
Color coding

* Wireshark uses color to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifiers packets with errors.



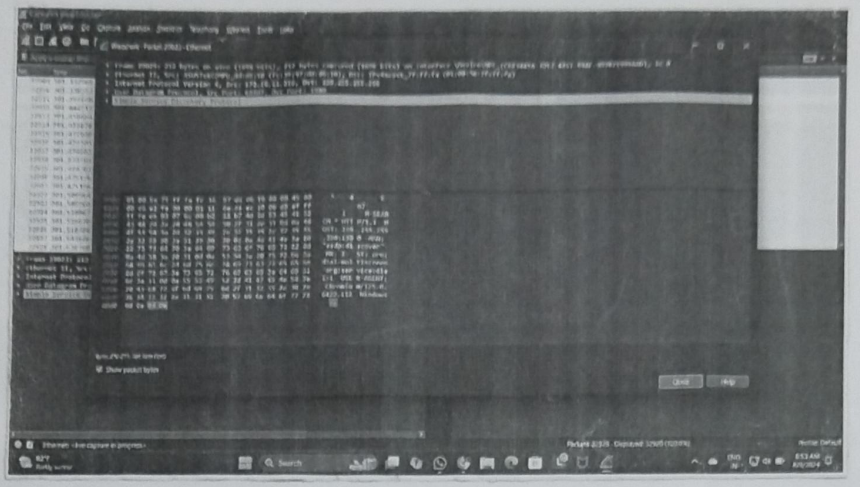
Filtering packets

* the boost basic way to apply a fibre is by typing, it into the filter box at the top of the window and clicking apply.



Inspecting Packets

* click a packet to select it and you can dig down to view its details.



Student Observation:

1. What is promiscuous mode?

→ It refers to setting that allows the network interface card to capture all network traffic on the segment it is connected.

2. Does ARP packets has transport layer header? Explain.

⇒ It do not have a transport layer header. They operate at the data link layer (layer 2) and are used for mapping IP address to MAC address.

3. Which transport layer protocal is used DNS?

⇒ Uses UDP as its transport layer protocal on port 53.

4. What is the port number used by http protocal?

→ HTTP protocal uses port number 80 for communication over the web.

5. What is a broadcast ip address?

→ It typically '255.255.255.255', is used to send a Packet to all device in network segment.

RESULT :-

Thus, Wireshark tool has been experiments on packet captured and studied.

9/8/24