6/8/24

Exp-5
Wireshark

Aim
Experiment on packet capture tool : Wireshark

Packet Sniffer

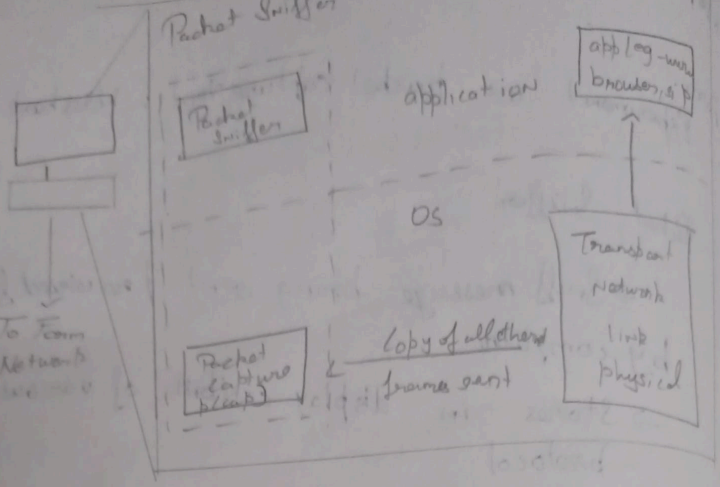
→ Sniff message being sent / received from/ by computer
→ Stores in display content of various protocol

→ Passive program
→ Never send packet itself
→ No packet addressed to it
→ Receive a copy of all protocols

Tcp dump

eg : tcdump -ex host 10.129.4.2 -to exe 3.out

Wireshark
- Eg : exe 3.out



Wireshark

network analysis tool

formerly known as Ethereal

Capture packets in real time & display in human readable

Include formats, filters, color coding

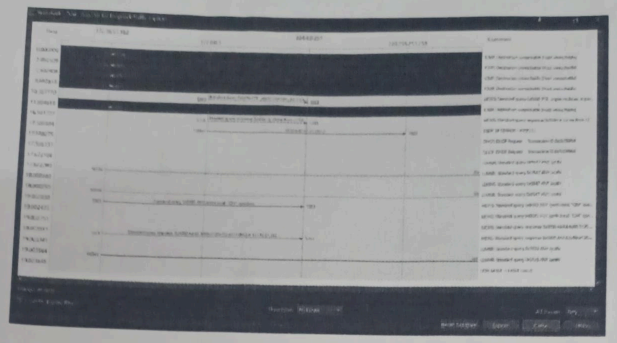
Uses

- troubleshoot
- examine security problems.

Download Wireshark

Capturing packets

- Launch Wireshark, double click on name of network interface



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

Color coding rules

Colors have been assigned for each packets view - coloring Rules

Filtering packets

* Display orderly

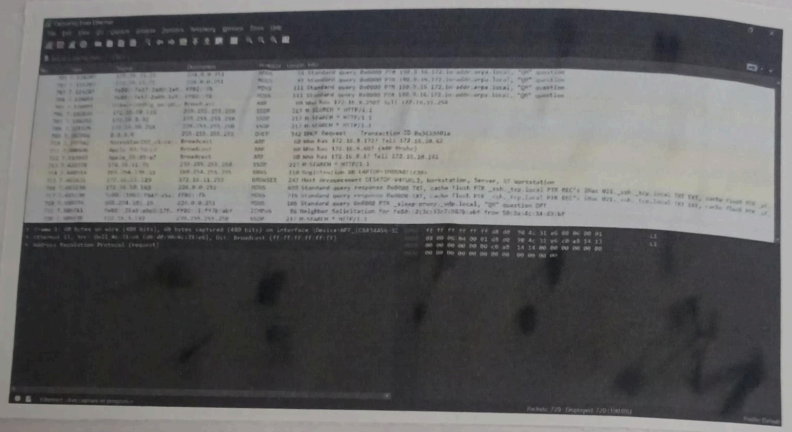
-> type into filter box at top of window & clicking apply

TCP Conversion

Bright click on a packet → follow → TCP Stream

Flow graph

→ network interface → statistics → flow graph



Student Observation

1) A network interface card mode mode that allows it to capture all traffic on that network

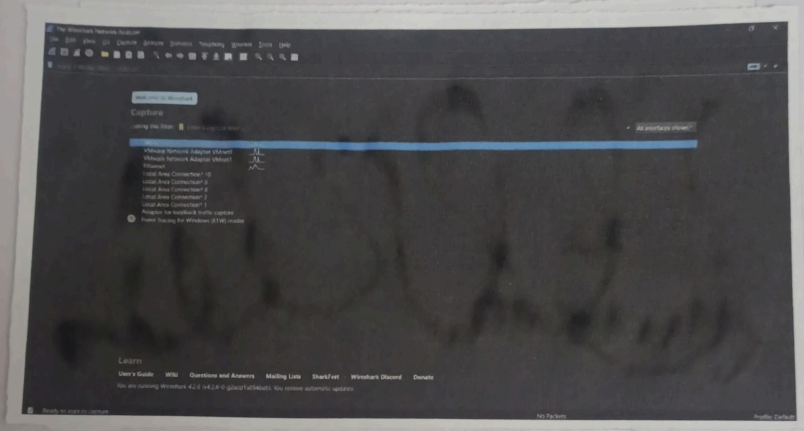
2) No, ARP packets do not have tran layer header.

3) → UDP (User diagram Protocol)

4) Port Number used by HTTP

→ 80

5) Used to send data to all devices on a network. For IPV4, if its highest address in a subnet.



Result

Thus the packet capturing tool - Wireshark is installed.