7/8/20 Practical - 5

Aim
Experiments on Packet capture tool : wireshark

Packet sniffer

→ sniffs messages being sent / receive
from / by protocol fields in the message

→ store & displays the contents of
the Variance protocols fields in the me

→ Passive Program

↳ never send packets itself

↳ no packets addressed to it

↳ receives a copy of all packets

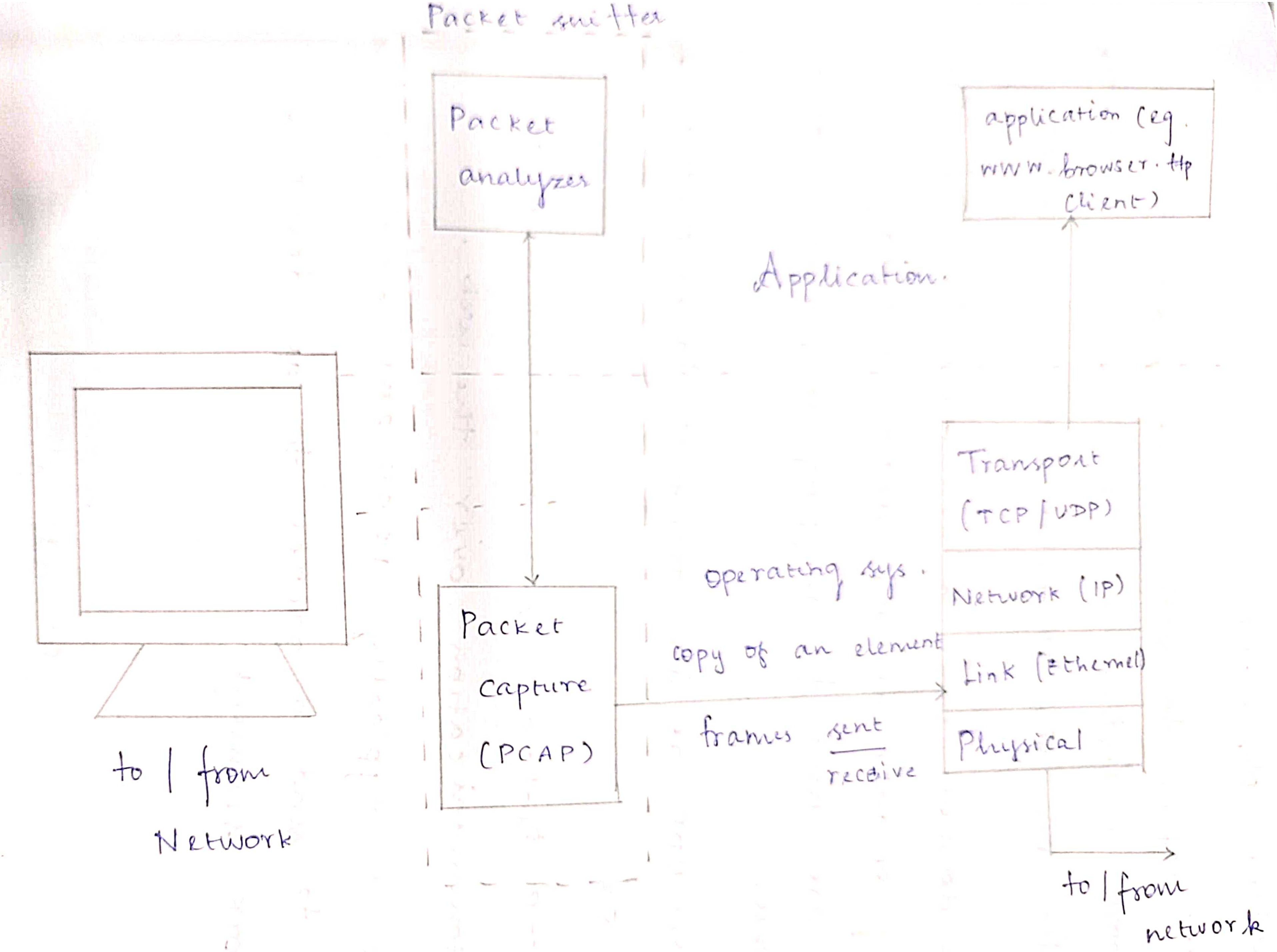
Packet sniffer structure diagnostic to

* TCP dump

→ tcpdump - exn host 10.129.41.2.

* wire shark

→ wireshark - r - exe 3 . out


Packet sniffer
Packet analyzer
Packet capture (PCAP)
Application.
application (eg. www. browser. ftp client)
operating sys.
Transport (TCP / UDP)
Network (IP)
Link (Ethernet)
Physical
copy of an element
frames sent / receive
to | from network
to | from Network

Student Observation :

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

2) It doesnot have a transport layer head they operate at the data link layer and are used for mapping IP address to MA address.

3) Uses UDP as its transport layer protocol Port 53

4) HTTP Protocol uses port number 80 for communication over the web.

5) It is typically 1255.255.255-255 used to send a packet to all device in network segment.

Result :

This, Wireshark ~~tool~~ has been experi on packet captured ~~ad~~ studied.

28/8/24