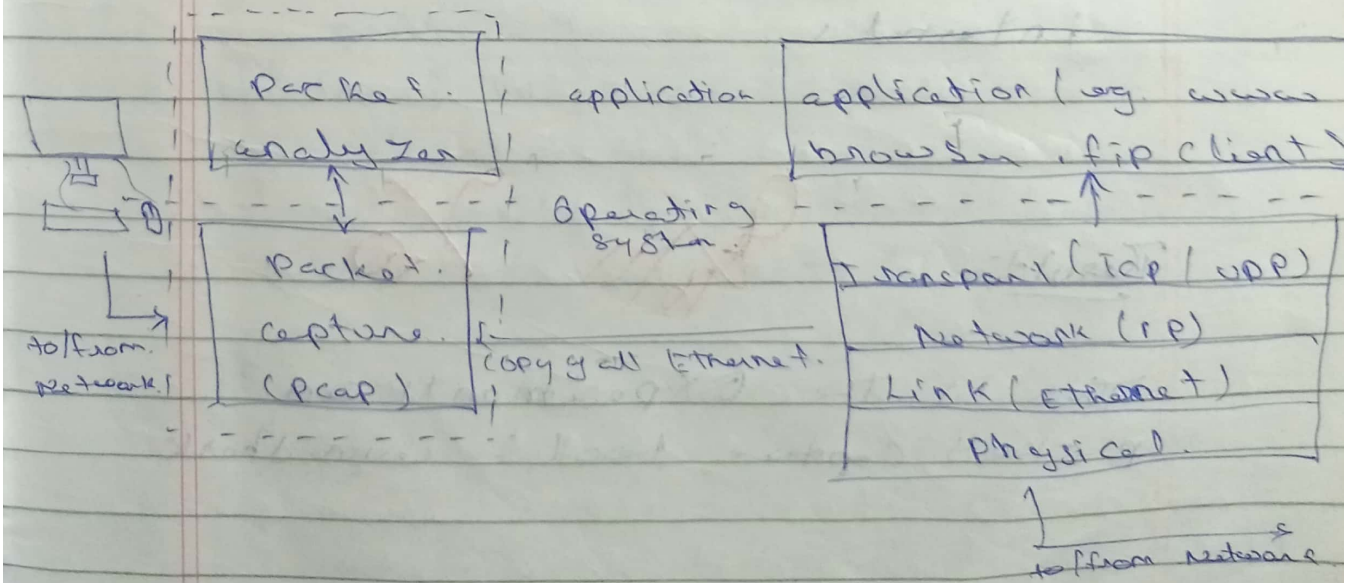
Ex. No: 5

Packet Sniffer

-> Sniffs message being sent / received from / by your computer
-> Store and display the contents of the various protocol fields in the message passing program.
-> Passive program.
    * Never sends packet itself.
    * No packet addressed to it.
    * Receives a copy of all packets

Packet Sniffer structure Diagnostic tools
-> Tcpdump
    - Eg tcpdump -ienx host 10.129.41.2 -w
-> Wireshark
    - wireshark -r exec 3.out



WIRESHARK.

- Capture Network traffic
- Decode packet protocol using dissectors
- Define filters - capture and display
- Watch packet statistics
- Analyze problems
- Interactively browse that traffic

Wireshark used for

- Network administrators: trouble shoot Network problems
- Network security engineers: Examine security problems
- Developers: debug protocol implementations
- People: learn network protocol internals.

Result:-

This is the Experiments on packet capture tool: wireshark.