9/8/24

Experiment-5

Packet Capture Tool

Aim: Experiments on Packet capture tools wireshark

Packet sniffer:

Sniffs messages being sent/ received from/by your Computer store and display the contents of the various protocol fields in the message

Passive program

never sends packets itself

no Packet addressed to it

receives a copy of packets [sent/received]

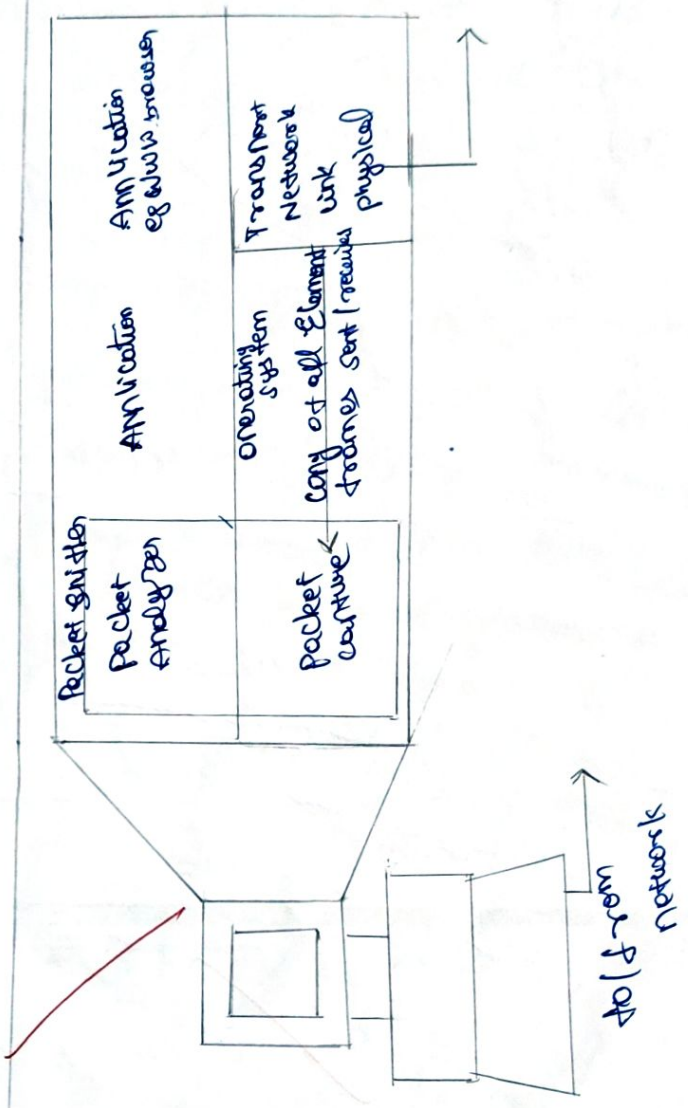
Packet Sniffer structure Diagnostic Tools

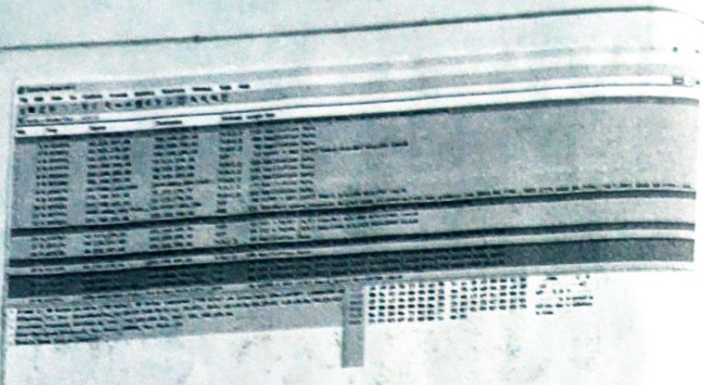
TCP dump:

Eg: Aptdump -ene host 10.129.41.2-W

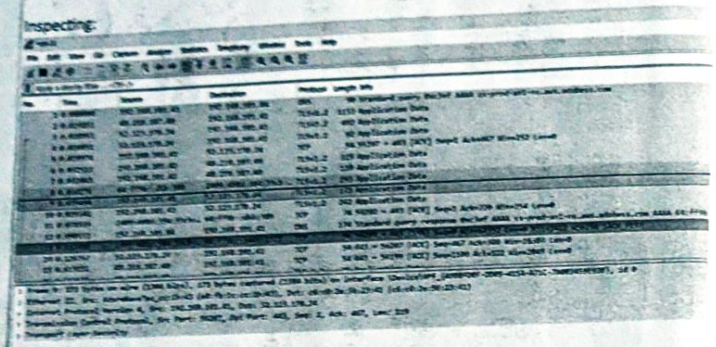
Wire Shark

wire Shark -r exe 3.out

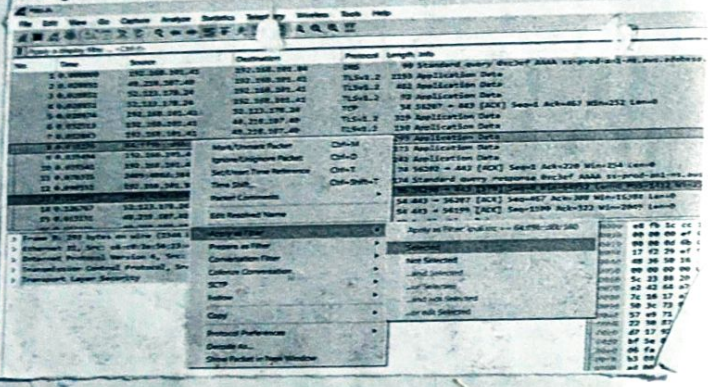


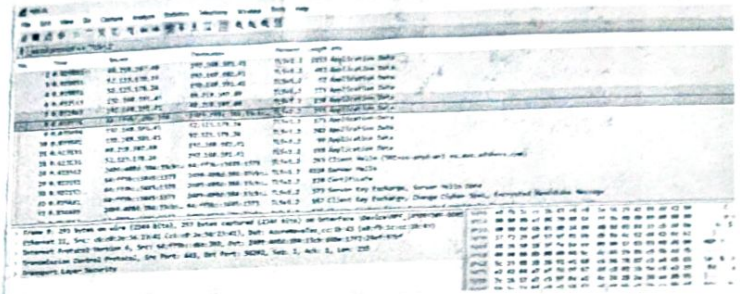


Inspecting:

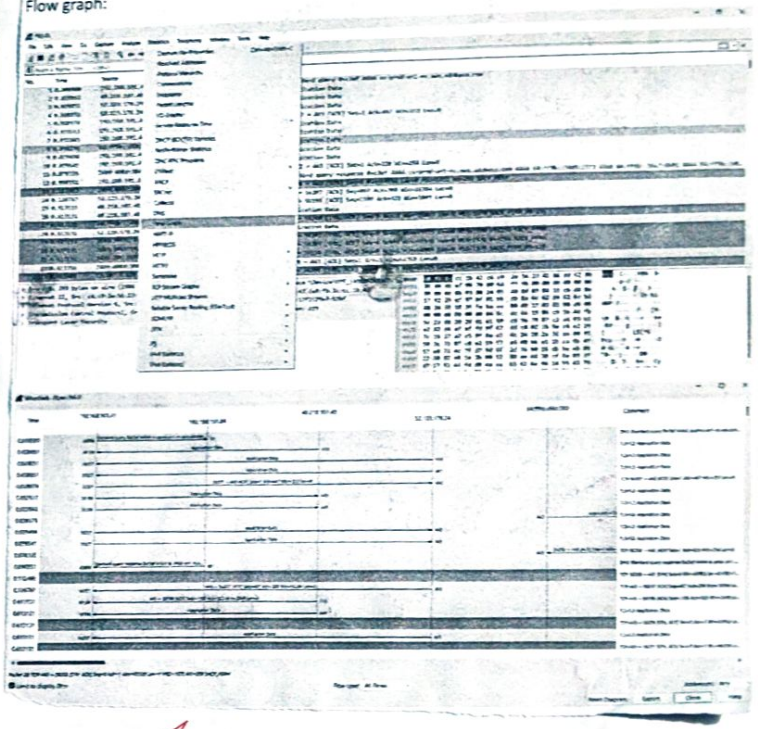


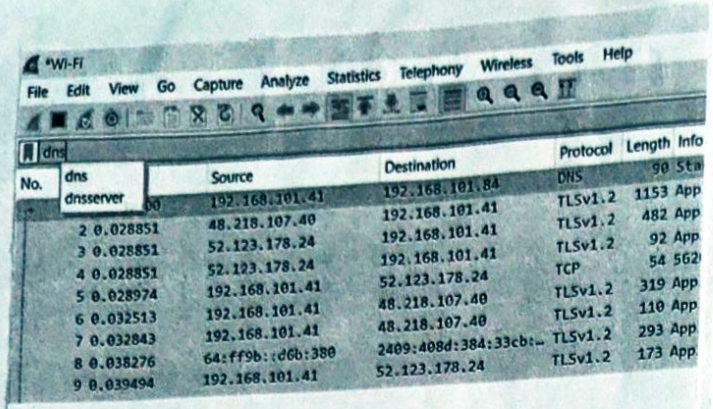
Filtering:

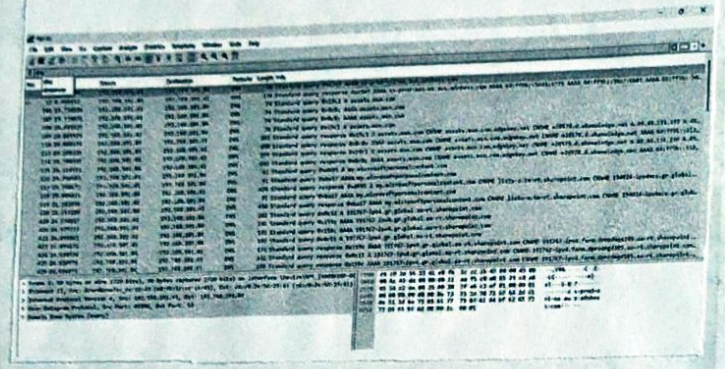


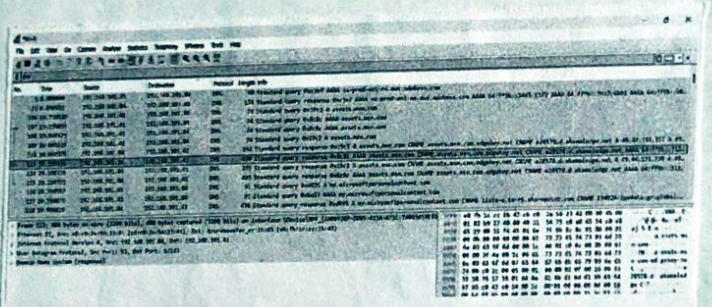


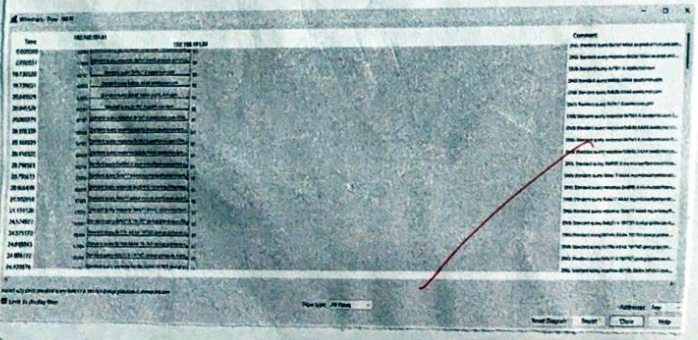
Flow graph:











Students Observation:

1) What is Promiscous mode?

Promiscuous mode is a welcome interface card (NIC) setting that allows Card to intercept and read all network Packets on network segments.

2) Does ARP packets has transport layer header? Explain

No, ARP Packets does not have transport layer header

3) Which transport layer protocol is used by DNS?

DNS (Domain name system) Primarily uses UDP for its transport layer protocol

4) What is the port number used http Protocol?

~~HTTP~~ Protocol uses Port number 80 by default.

5) What is broadcast IP address?

It is a broadcast IP address which is used to send packets to all devices on a specific network segment

Result:

Thus the packet capturing filtering and flow graph are observed using wireshark

9/8/24