Exp: No: 5

8/9/25

Experiments on Packet Capture tool: Wiresh

Aim:

Experiments on Packet capture tool: Wireshark.

Packet Sniffer:

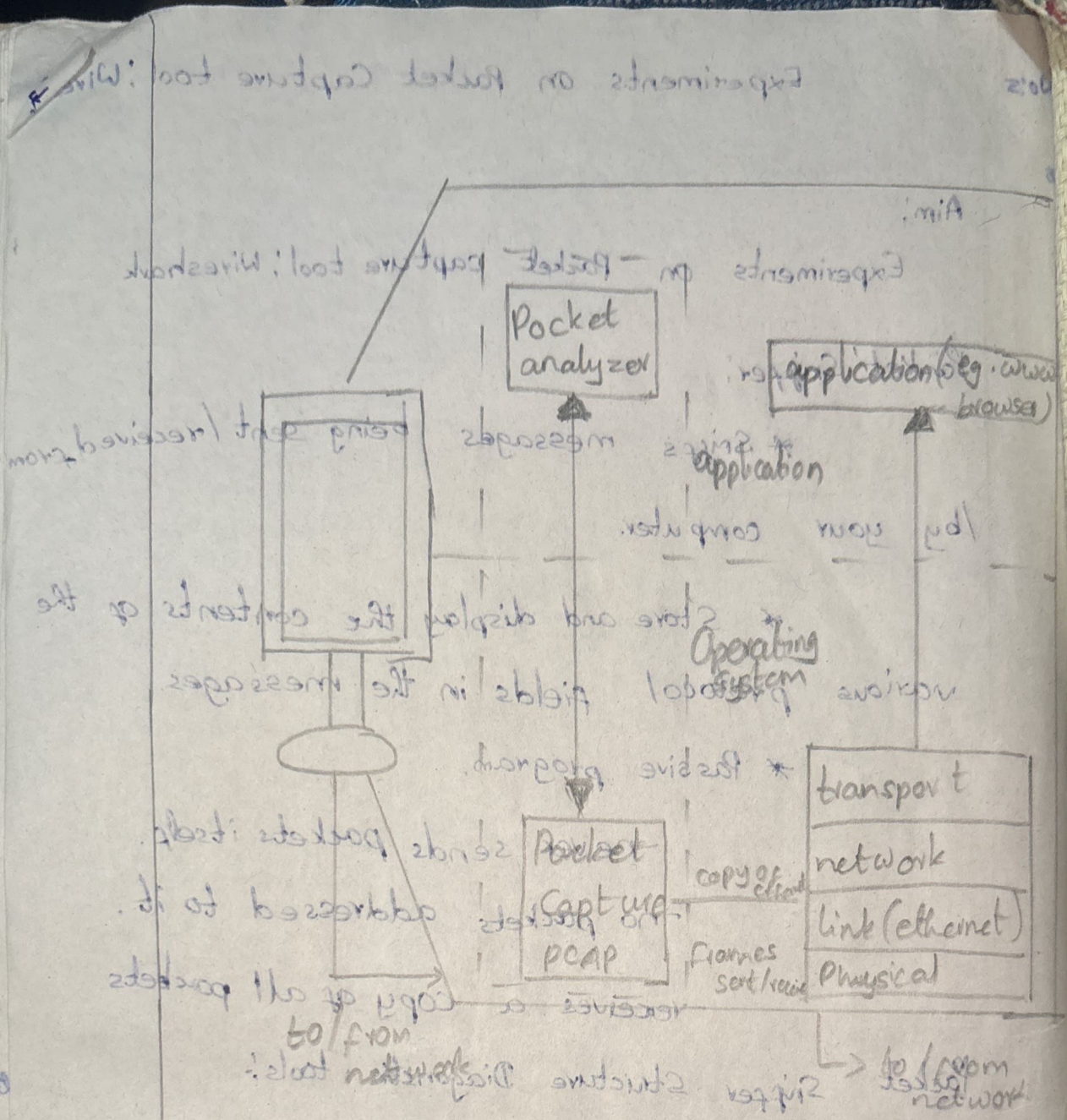
* Sniffs messages being sent/received from /by your computer.
* Store and display the contents of the various protocol fields in the messages.
* Passive program.
  - never sends packets itself.
  - no packets addressed to it.
  - receives a copy of all packets

Packet Sniffer Structure Diagonstic tools:

* Tcpdump
  - Eg. tcpdump -enx host 10.129.41.2 -w exe3.out.
* Wireshark
  - wireshark -r exe3.out.

Description:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding and other features that let you dig deep into network traffic and inspect individual packets. You can use


Pocket analyzer
application (eg. web browser)
application
Operating system
transport
network
link (ethernet)
Physical
Packet Capture
pcap
copy of frames sent/received
copy of all packets received
to/from network

wireshark to inspect a suspicious program's ne traffic, analyze the traffic flow on your network or troubleshoot network problems.

1) What is Promiscuous mode?

Promiscuous mode is a network interface mode that allows a network device typically a network Interface card (NIC) to pass all traffic it receives to the CPU, not just the traffic addressed to it.

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

No, ARP packets do not have a transport layer header because ARP operates at the Data Link layer (layer 2), not the Transport layer (layer 4). It is used to map IP addresses to MAC addresses & is encapsulated directly in Ethernet frames not in IP, TCP, UDP.

3) Which transport layer protocol is used by DNS?

DNS mainly uses UDP on port 53

However, DNS also uses TCP incases zone transfers or when the response data its too larger for UDP.

4) What is the port number used by HTTP protocol?

HTTP uses port 80 by default.

It the site is secured with SSL/TLS then it uses HTTPS on port 443.

5) What is a broadcast IP address?

A broadcast IP address is an address that allows information to be sent to all devices in a network at once.

Eg: In a network 192.168.1.0/24 the broadcast address is 192.168.1.255

All hosts in the sub net receive the packet.

Result:

Wireshark was used to capture & study network traffic. It showed how data moves between devices the tool helped understand how the internet & network protocols work.