EXP:14 Capturing & Analyzing Packets
12/9/25 Using Wireshark.

Aim: To capture, filter & inspect network packets using Wireshark & analyze different protocols like TCP, UDP, ARP, DNS, HTTP, ICMP & DHCP.

Procedure:

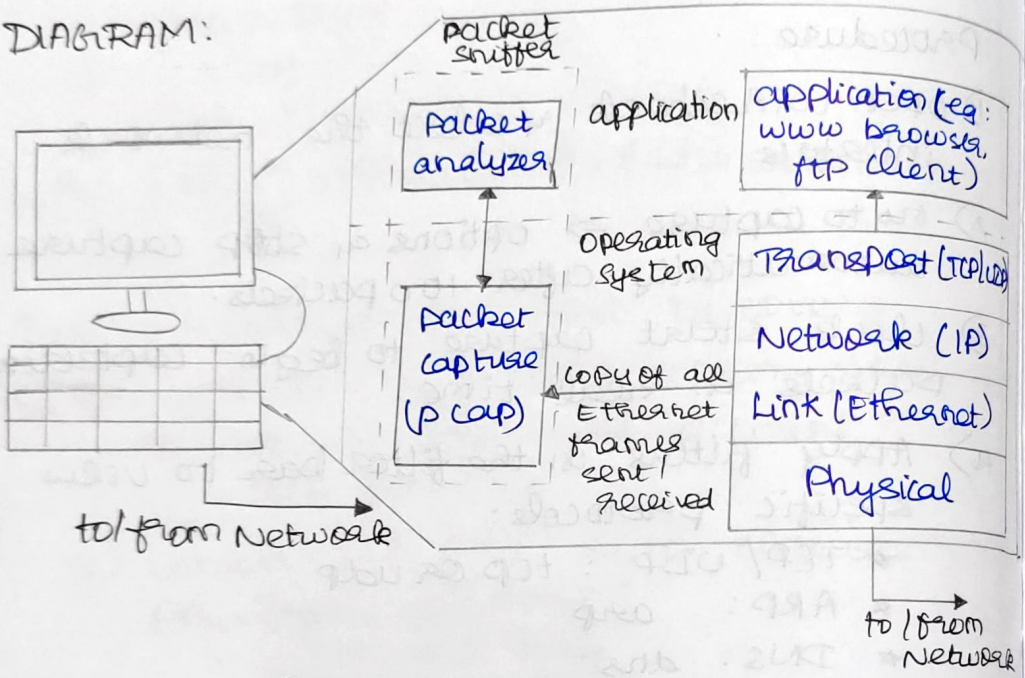
1) Open Wireshark & select the network interface
2) Go to Capture → Options & stop capture automatically after 100 packets.
3) Click start capture to begin capturing packets in real-time.
4) Apply filters in the filter bar to view specific protocols:
   - ★ TCP/UDP : tcp or udp
   - ★ ARP: arp
   - ★ DNS: dns
   - ★ HTTP: http
   - ★ ICMP/IP : icmp
   - ★ DHCP : bootp
5) Inspect each packet in the Packet Details pane to see protocol fields.
6) Use Statistics → Flow Graph to visualize communication between hosts.
7) Save captured packets for later analysis (File → Save).

Output:

- Packet List: Show all captured packets.
- Packet Details: Display protocol layers & fields
- Packet Bytes: Shows raw packet data in hex format.

- Filtered views display only the selected protocol packets.
- Flow graphs show the sequence of communication between the source to the destination

DIAGRAM:



Packet sniffer structure

STUDENT OBSERVATION:

1) Promiscuous mode: captures all packets on the network, not just those for your machine
2) ARP packets transport header: No, ARP operates at the Data Link layer.
3) Transport protocol used by DNS: UDP [mostly].
4) HTTP port number: 80
5) Broadcast IP address: 255.255.255.255

RESULT:

Wireshark captured & displayed network packets with protocol details & addresses successfully.

2 | 3 | X | 25 | 10/10