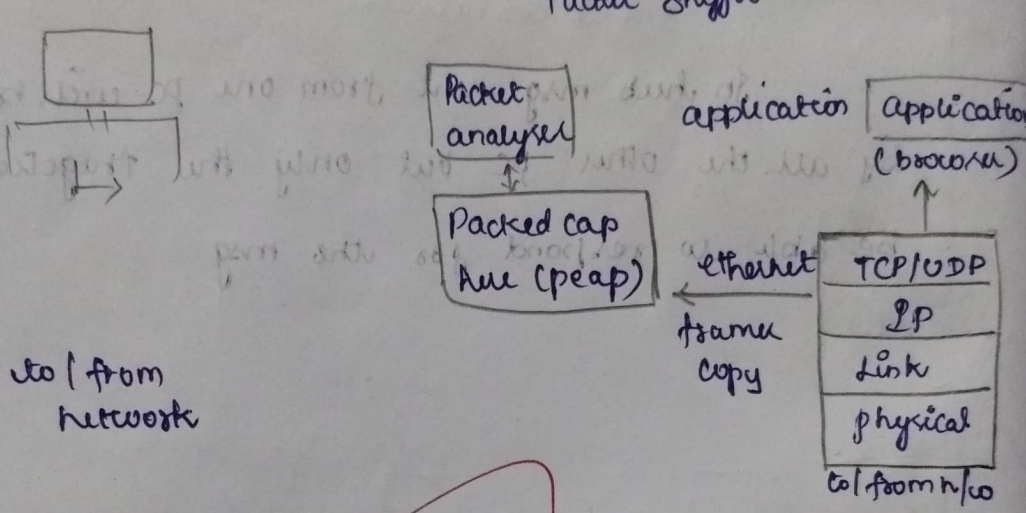
# WIRESHRK

AIM

Experimenting the packet capture tool wireshark

Wireshark -r ere 3.out

PACKETSNIFFER STRUCTURE




Wireshark, a network analysis tool known as ethereal, capture packets in real time and display them in human readable format.

Getting Wireshark

Install and configure from official website

Capturing packets

Enabling promiscous mode on all interfaces then double click to start capturing

It has "packet list pane", "packet details pane" and "packet bytes pane"

Color coding ⇒ to depict different traffic

Filtering packets ⇒ to filter packets accordingly

Derive flow graphs

Repeat the procedure for all the protocols

TCP/IP, ARP, DNS, HTTP, ICMP/ICMP

DHCP

Thus save all the flow graphs.

Promiscuous mode: A network interface mode where the network card passes all traffic to the CPU, not just the packet addressed to it.

No, ARP packets do not have transport, they operate at the datalink layer.

DNS primarily uses the UDP protocol on port 53

HTTP protocol use port 80

A broadcast IP address is used to send data to all possible recipient in network.

RESULT 10/10

29/9/24

Hence, the installation, operation and observation of wireshark is done successfully