Date:

Experiment 5:

Packet capture tool - Wireshark

Wireshark is a powerful widely used network protocol analyzer that allows users to capture and analyze data packets travelling to a network in real-time.

Why Wireshark is used?

1) Network Troubleshooting
2) Learning and education

Student observation:

1) Promiscuous mode is a network interface card (NIC) setting that allows card to intercept and read all network packets on network segment
2) No. ARP packets do not have transport layer header
3) DNS (Domain Name System) primarily uses UDP for its transport layer protocol.
4) HTTP protocol uses port number 80 by default.
5) It is a broadcast IP address which is used to send packets to all devices on a specific network segment.

Result: Thus the experiment is studied and observed.