Practical-5

Aim:
Experiments on packet capture tool: wireshark.

wireshark:
wireshark, a network analysis tool formely known as ethereal, captures packets in real time and display them in human readable format. wireshark includes filters, colour coding and other features that let you dig deep into network traffic and inspect individual packets.

capturing packets:
After downloading and installing wireshark launch it and double click the name of a network interface.

colour coding:
wireshark uses colours to help you identify the type of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic and black identifies packets with errors.

Filtering packets:
If you are trying to inspect something specific such as the traffic a program sends when phoning home. It helps to close down all other

applications using the network. so you can narrow down the traffic. still, you will likely have a large amount of packets to shift through. That's where wireshark's filters come in.

Inspecting Packets:

click a packet to select it and you can dig down to view its details.

Observations:

1) Promiscuous mode - It is a configuration of a network interface card where NIC is set to pass all traffic it receives to CPU rather then just the packets addressed to it.

2) ARP packets do not have a transport layer header. It operates at data link layer of OSI model and its purpose is to map an IP address to a MAC address.

3) DNS uses both TCP and UDP transport layer protocols

4) HTTP uses port number 80.

5) A broadcast IP address is an address that allows transmission of data to all hosts on a network.

Result:

Thus experiment on packet capture tool. wireshark is performed and observations are noted.

31/3/21.