13/08/24 PRACTICAL - 5

WIRESHARK.

AIM:

Expirements on Packet Capture tool ; wireshark.

Packet Sniffer:

→ Sniffs messages being sent/received from / by your computer.

→ Store and display the connects of the various product fields in the message.

→ Passive program.

Packet Sniffer Structure Diagnostic Tool.

→ Tcpdump.

```
- tcpdump - enx host 10.122.41.2
```

→ Wireshark

```
- wireshark -r exe 3.out
```

Student Observation :-

(1) What is promiscuous mode?

* Promiscuous mode allows the network interface card to capture all traffic on a network segment, not just packets

2. Does ARP packets has transport layer header Explain ?

*. ARP packets do not have transport layer header they operate at the data link layer and are encapsulated directly in frames.

3. Which transport layer protocol is used by DNS ?

*. DNS primarily uses UDP for queries and responses but can use TCP for larger response zone transfer.

4. What is the port number used by http protoco

* HTTP uses port number 80 by default for communication.

5. What is a broadcast ip address ?

*. A broadcast IP address sends packets to all devices on a specific network segment in IPv4 it's determined by setting all host bits to 1

Result : The program is successfully executed and output is verified.

21/8