Experiment 6: IP Traffic analysis

1. Aim: To analyze the IP traffic over a network by capturing IP packets.

2. Tools Used: Wireshark software

3. Related Theory:

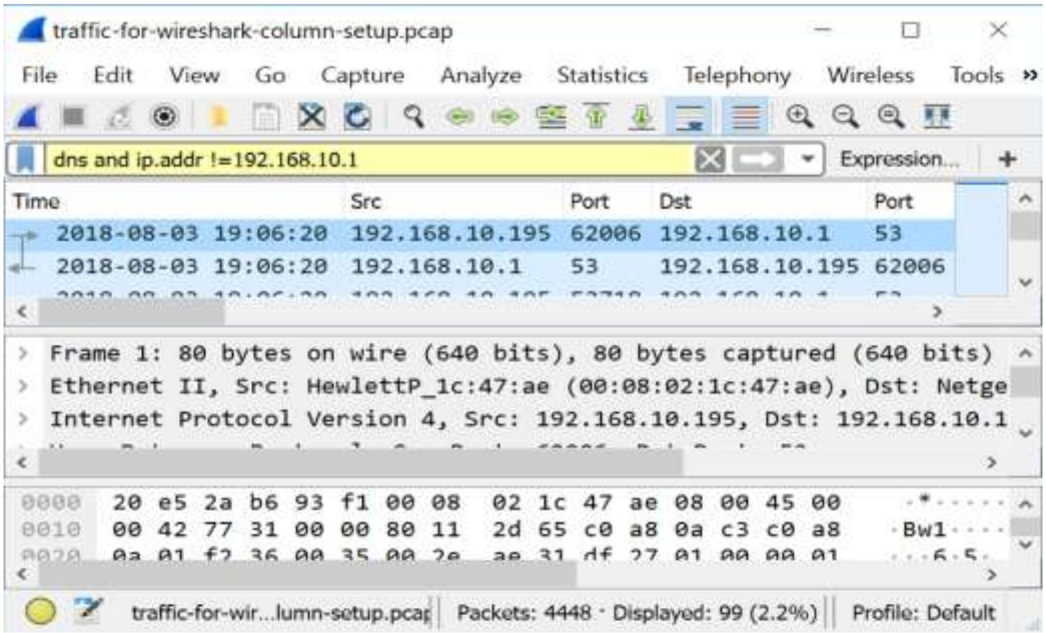
Few tools are as useful to the IT professional as Wireshark, the go-to network packet capture tool. Wireshark will help you capture network packets and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis. This tool lets you put your network traffic under a microscope, and then filter and drill down into it, zooming in on the root cause of problems, assisting with network analysis and ultimately network security.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture**: Wireshark listens to a network connection in real time & then grabs entire streams of traffic – quite possibly tens of thousands of packets.

2. **Filtering**: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying filter, you can obtain just the information you need to see.

3. **Visualization**: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.



dns and ip.addr !=192.168.10.1

```
Time                 Src             Port   Dst             Port
2018-08-03 19:06:20  192.168.10.195  62006  192.168.10.1    53
2018-08-03 19:06:20  192.168.10.1    53     192.168.10.195  62006
```

```
> Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netge
> Internet Protocol Version 4, Src: 192.168.10.195, Dst: 192.168.10.1
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*······
0010  00 42 77 31 00 00 80 11  2d 65 c0 a8 0a c3 c0 a8   ·Bw1····
```

traffic-for-wir...lumn-setup.pcap | Packets: 4448 · Displayed: 99 (2.2%) | Profile: Default

Fig: Sample capture using Wireshark

4. Laboratory Exercise:

i. Open Wireshark application
ii. Generate web traffics
iii. Capture the traffic using Wireshark
iv. Filter http packets
v. Analyze the traffic by noting down the info of different layers
vi. Take the screenshots of every information captured

5. Post-Experiment Exercise:

A. Conclusion

B. Questions:

1. List all the applications of Wireshark.
2. Explain any one use case of Wireshark tool with example.