Vidyavardhini's College of Engineering & Technology
Department of Information Technology

Experiment No. 10

Aim: To analyze packet header using Wireshark Network Analyzer.

Apparatus (software): System with Ubuntu, Wireshark Network Analyzer

Procedure:

1. Open Terminal in Ubuntu. Type following command to start Wireshark in Terminal

   ```
   $ sudo wireshark
   ```

2. It will display “The Wireshark Network Analyzer” window and we will see wavy lines beside ‘ens33’.
3. Go to Wireshark and click on the first option ‘Start capturing packets’ (shown with Blue shark tail) to start capturing packets.
4. You can see a window with various source and destination IP addresses, protocols, lengths, etc. This is where you are capturing the protocols. In case there are now packets shown, open the browser and perform some activity online to generate packets.
5. To stop capturing packets click on ‘Stop capturing packets’ (shown with Red square).
6. To analyze the packet, double click on the row.
7. It will display details of the packet.
8. You can also apply filters by protocol names to see only the packets you want to see.

Conclusion:

Q. What packet information is shown in Wireshark?

Ans.- Wireshark will display following information of the packet:

- total length of the packet,
- physical addresses of source and destination,
- IP addresses of source and destination,
- transport layer protocol,
- source and destination ports,
- application layer protocol which generated packet etc.