**Aim:** To study Wireshark Tool: Network analysis using Windows Operating System and

Linux Operating System

**Theory:**

**Wireshark** is a [free](https://en.wikipedia.org/wiki/Free_software) and [open-source](https://en.wikipedia.org/wiki/Open-source_software) [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](https://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) development, and education. Originally named **Ethereal**, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is [cross-platform](https://en.wikipedia.org/wiki/Cross-platform), using the [Qt](https://en.wikipedia.org/wiki/Qt_(software)) [widget toolkit](https://en.wikipedia.org/wiki/Widget_toolkit) in current releases to implement its user interface, and using [pcap](https://en.wikipedia.org/wiki/Pcap) to capture packets; it runs on [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS), [BSD](https://en.wikipedia.org/wiki/BSD), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)), some other [Unix-like](https://en.wikipedia.org/wiki/Unix-like) operating systems, and [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are [free software](https://en.wikipedia.org/wiki/Free_software), released under the terms of the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License).

Wireshark is very similar to [tcpdump](https://en.wikipedia.org/wiki/Tcpdump), but has a [graphical](https://en.wikipedia.org/wiki/Graphical_user_interface) [front-end](https://en.wikipedia.org/wiki/Front-end_and_back-end), plus some integrated sorting and filtering options.

Wireshark lets the user put [network interface controllers](https://en.wikipedia.org/wiki/Network_interface_controller) into [promiscuous mode](https://en.wikipedia.org/wiki/Promiscuous_mode) (if supported by the [network interface controller](https://en.wikipedia.org/wiki/Network_interface_controller)), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's [MAC address](https://en.wikipedia.org/wiki/MAC_address). However, when capturing with a [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer) in promiscuous mode on a port on a [network switch](https://en.wikipedia.org/wiki/Network_switch), not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. [Port mirroring](https://en.wikipedia.org/wiki/Port_mirroring) or various [network taps](https://en.wikipedia.org/wiki/Network_tap) extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

On GNU/Linux, BSD, and macOS, with [libpcap](https://en.wikipedia.org/wiki/Pcap) 1.0.0 or later, Wireshark 1.4 and later can also put [wireless network interface controllers](https://en.wikipedia.org/wiki/Wireless_network_interface_controller) into [monitor mode](https://en.wikipedia.org/wiki/Monitor_mode).

If a remote machine captures packets and sends the captured packets to a machine running Wireshark using the [TZSP](https://en.wikipedia.org/wiki/TZSP) protocol or the protocol used by [OmniPeek](https://en.wikipedia.org/wiki/OmniPeek), Wireshark dissects those packets, so it can analyze packets captured on a remote machine at the time that they are captured

**Approach:**

1. Capture packets from interface with GUI or TCPDUMP command as follows

**tcpdump -i eth0 \_w ex.pcap**

1. Analyze o/p directly on comsol or on GUI of wireshark.

|  |
| --- |
| **Post lab:**   1. **What is the next hop router's IP address and MAC address? How did you get this information?** 2. **What is the local DNS server's host name and IP address? How did you get this information?** |

Signature of Faculty