31/8/23

Wireshark Demonstration

- Wireshark is a free and open source packet analyzer.
- It is used for network troubleshooting, analysis, software and communication protocol development and education.

- It provides following functionality -
- It lets the user put network interface controllers that support promiscous mode into that mode, so they can see all the traffic visible on that interface.
- If a remote machine captures packets and sends the captured packets to a machine running Wireshark, it dissects the packets so it can analyze packets captured on a remote machine at the time they are captured.
- It understands the structure of different networking protocols. It can parse and display fields along with their meanings as specified by different protocols.
- It also supports capture formats from several other commerical and open source network sniffers.

Some of the features of wireshark are -

- Data can be captured from the wire from a live network connection or read from a

file of already captured packets.

- Live data can be read from a number of types of networks including Ethernet, IEEE 802.11, PPP and loopback.
- Data display can be refined using a display filter.
- The IP address of the device can be used in the filter to capture only the packets sent out and to that IP address.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Various settings, timers and filters can be set that ensure only triggered traffic appear.
- The information of the packets include ID number, time (standard), source IP address, destination IP address, protocol name, length and other important information.

✓

N
26/23