Wireshark

Aim :- To explore wireshark.

Overview :- Wireshark is an open source application that captures & displays data travelling back & forth on a network. Wireshark is a packet sniffer and network analyzer.

Capturing Packets

-> First select a network from which we require to sniff packets.

-> Wireshark begins capturing packets from selected network. All captured packets are shown in top section of panel.

-> On selecting a particular packet, we observe the structure of the packet in the middle section of the panel. Various structures can be seen with respect to protocol.

-> The packet details displayed as

- -> Time stamp
- ~~-> Source IP~~
- -> Destination IP
- -> Protocol name
- -> Length of packet

Filtering

Wireshark provides a filter function to better analyze network data. Wireshark also allows custom filters.

An example of filter is to select only packets for HTTP port

tcp.port == 80 || udp.port == 80

Packet details:-

The middle section of panel is packet detail panel, presents the protocol and protocol fields of selected packet in a collapsible format. We can apply additional filters by right click on protocol for a detailed view.

At the bottom panel, raw data of selected packet is given in hexadecimal format. It is called hexdump. It contains 16 hexadecimal digits of 16 ASCII bytes alongside the data offset.

01/09/2023