Lab-17

wireshark functionalities

wireshark is similar to tcpdump in networking.

Tcpdump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to computer. ~~It has~~

It has a graphic end and some sorting & filtering functions.

wireshark users can see all traffic passing through the network.

wireshark can also monitor the unicast traffic which is not sent to network's MAC address interface.

It is multi-platform software, i.e it can run on Linux, Windows, OS X, Free BSD, Net BSD, etc.

3/8/2023

It is a standard three ~~p~~ packet browser

It performs deep inspection of hundreds of protocols.

It performs live analysis

It makes the user ~~v~~ view the data easily.