WEEK 17

Tool Exploration -Wireshark

OBSERVATION:

wireshark.

wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocal development, and networks troubleshooting

it is used to track The packets so that each one is filtered to meet our specific needs. it is commonly called as a sniffer, network Protocal analyzer, and network analyzer

uses of wireshark:

-> it is used by network security engineers to examine secerety Problems.

-> it allows The User to watch all The traffic being passed over The network

-> it is used by network engineers to troubleshoot network issues.

-> it also helps to troubleshoot latency issues and malicious activities on your network

-> it can also analyze dropped packets.

A packet is a unit of data which is transmit over a networks b/w The orgin and The destina network packets are small, i.e. maximum 1.5 kilobytes for Ethernet packet and 64 kilobytes for IP packets

The bottom window called the packet contents window, which displays the content in a low is the filter field which is at the top of the display. The capture packet on the screen can be filtered based on any components according to your requirements

Packet list

No. This field indicate which packets are part of same conversation

Source: This column contains the address where the packet originated

Destination: This column contains the address that produce is being sent to

Protocal

The Packet Protocal name, such as TCP can be found in this colum

length

The packet length in bytes is displayed in the colum

info:

Additional details about packet are present in this column The contents of this column are very greatly depending on Packet contents