WEEK 15

Tool Exploration -Wireshark

Observation:

Date 31/08/2023
Page

PROGRAMS

Tool Exploration - Wireshark

Wireshark :-

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.

Wireshark is the most often-used packet sniffer in the world.

→ Open Browser :-

And type wireshark download.

and select the appropriate software for your system and download it.

And install it.

Uses of the wireshark :-

1. It is used by network security, engineers, to examine security problems
2. It allows users to watch all the traffic being passed over the network
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency and malicious activities on your network
5. It can also analyze dropped packets
6. It helps us to know how all the devices, like laptop, mobile phones, desktop, switch, routers etc. communicate in a local network or the rest of the world.

→ Open wireshark
And click on capture → start
Now we can see the packets that are sent by the system and received by the system and the protocol being used.

→ And we can view the source and destination address of the packet.
→ If we click on a particular packet. now you can see the ASCII code in the bottom

→ And wireshark uses different colours for the different protocols to represent

→ To see only your system participation in network in display filter type ip.addr == (ip address of the PC

ex:- ipaddr = 10.124.7.1

NOTE : To know the ip address of the system open cmd and type ipconfig.
You can now see the ip address of your system

31/8/2023

→ And we can even filter packets by the type of the protocol

Go to Analyze and display filters to see the filters
To stop capturing go to capture and click on stop

To colorize packet list go to view and click on colorize packet list