Wireshark Tutorial

Wireshark is an open source packet analyzer, which is used for education, analysis, software development and network troubleshooting.

It is used to track the packets so that ~~then~~ each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer.

Functionality

(1) Packet capture and filtering

Primary function lies in capturing network packets from various interfaces. Its flexible option enable users to capture specific types of traffic based on protocols, source destination address.

(2) Real time analysis

Wireshark's real time feature aids in detecting - sudden traffic spikes and unauthorized network usage.

(3) Protocal analysis

It decrypts encrypted protocol offering insights into source communication methods.

(4) Packet reconstruction

(5) Statistical information

(6) Colour coded visualisation :
To indicate various aspects such as error.

Interface of wireshark

(1) menu bar and options displayed, Capture and file menu.

(2) Packet listing window - Determines the packet flow/ captured packets in the traffic.

(3) Packet header - detailed window, contains info about the components of the packet.

(4) Bottom window called as packet contents win which contains contents in ASCII and hexadeci format.

(5) Filter field at the top, which helps filtering packets based on any component according to your requirements.

Procedure :

→ select ethernet

→ Filter TCP or any required protocol

→ Click on it, new window opens

→ Drop down : Transmission control protocol,
Src Port 62148, DST port : 443, seq : 2,
Ack : 65, Len : 0

→ This is available in the free window in the left split of screen

→ Clicking on dropdown highlights its counterpart in right split side of screen.

→ In CMD, type > ip config.

Result :
Windows IP configuration
Ethernet adapter ethernet
connection - specific DNS suffix
link - local IPV8 Address . . . . Fe80 :: be78 : 609 ; ed25 ✓
IPV4 address 10.129.2.58
subnet mask . . . 255.255.0.0
Default Gateway . . . 10 . 124 . 0.11