Computer Networks

Momina Atif Dar P18-0030
Section: B

Wireshark

Wireshark is a tool which is used to analyze traffic on a network. It analyzes different sort of data packets and protocols. User can analyze WiFi as well as Bluetooth.

Pros:

- Filter – User can filter the results according to their own needs
- Color Codes – There are different color codes for different protocols to distinguish
- Stop Analysis – User can stop the service at any point to carefully analyze data sent and received
- Save Results – User can save the analysis to view later or to keep as a record.

Wireshark has all the information about data sent and received. It shows what is the number of data packet sent, to whom it is sent, from whom a packet is received, what protocol is used, at what time it is sent or received, how many bytes are received or sent, whether checksum is verified or not, ports used at sender and receiver's end, IPs of sender and receiver, length of data.
User can apply filter on results. For example if user wants to monitor only TCP connections then they may write 'TCP' on the bar below the menu bar. The results will be of data sent or received using TCP protocol only.

Default Color Codes:

Light blue: UDP connections
Light purple: TCP connections
Grey: flags related to TCP
Half Dutch White: Routing information / ARP
Purple: for DCERPC
Pale Pink: IPX
Light Green: HTTP / protocols which use port 80
Lemon yellow: SMB / NBSS / NBNS / NBIPX / IPXSAP / NETBIOS
Black background with Vermilion foreground: Checksum Errors / Bad TCP
Maroon background with White foreground: TTL
Maroon background with Yellow foreground: SCTP ABORT / TCP RST
Baby Pink: ICMP
Black background with Green foreground: ICMP errors
Black background with Yellow foreground: OSPF state change / Spanning Tree topology change / HSRP state change
White background with Grey foreground: Broadcast (eth[0] and 1)

User can change color codes according to their needs as well. It is a great tool to monitor one's network and keep in check what data is being sent and received. User can monitor somebody else's network as well. There are some 'sample capture files' found over the internet or in documentation of Wikishark which you can use to test drive the software or maybe learn more about its functionalities.