31-8-23

Wireshark

Originally known as Ethereal. Wireshark displays data from hundreds of different protocols on all major network types. Data packets can be viewed in Real-time or analyzed offline. Wireshark supports dozens of capture / trace file formats, including CAP and ERF. Integrated decryption tools display the encrypted packets for several common protocols including WEP & WPA/WPA2

Packet List:

The packet list pane, located at the top of the window, shows all packets found in active capture file. Each packet has its own row & corresponding number assigned to it; along with each of these data points

No:
This field indicates which packets are part of same conversation

Time: stamp of
The timestamp of when the packet was captured is displayed in that column.

Source: This column contains the address (IP or other) where the packet originated.

31-8-23

Bafna Gold
Date: Page:

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

- Protocol:
The packet's protocol name, such as TCP, can be found in this column.

- Length.
The packet length, in bytes, is displayed in this column.

Info:
Additional details about packet are presented in this column. The contents of this column are vary greatly depending on packet contents.

Packet Details

The details pane, found in the middle presents the protocol and protocol fields of the selected packet in a collapsible format. In addition to expanding each section, one can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right clicking the desired item

Wireshark is free and opensource packet analyzer. It is used to track, filter and view packets that are exchanged in

a network.

31/8/23