Wireshark.

Wireshark is a open-source network protocol analyzer used for network troubleshooting, analysis, software development and education. It allows users to capture and inspect data packets passing through a network in real-time or from previously saved capture files. It is a powerful tool for diagnosing network issues, verifying the correctness of network configurations and understanding the behaviour of networked applications.

features of Wireshark:

- Packet capturing
- Packet Analysis
- filtering and Search
- Statistics and Graphs
- IO Graph
- Packet Reconstruction
- Protocol Dissection
- Colorization and Marking
- VoIP Analysis
- Exporting Data
- follow TCP stream
- Live capture and offline Analysis.

Uses of Wireshark:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.

- It is used by networks engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyse dropped packets.

In GUI of Wireshark we can see. at menu are:- File, Edit, View, GO, Capture, Analyze, Statistics, Telephony, Wireless, Tools and Help.
And, we can see three segments.
i.) Packet list
ii.) Packet Details
iii.) Packet Bytes.
We can see one more segment alternately which is Packet ~~Datagram~~ Diagram.

When we capture packet, we can see packet list. from that we select one packet and know about its properties.
Selecting one packet from list.
In packet Details we see:-
> Frame 87: 86 bytes on wire (688 bits)
> Ethernet II, Src: Chongqin_ 69:5a:63
> Internet Protocol Version 6, Src: [redacted] Addr., Dst: MacAddr
> Transmission Control Protocol: Src Port: ___, Dst Port: ___

And we can each and every bytes transfering from one to one end.