* + 1. Wireshark is a network packet analyzer which presents captured packet data in detail.
    2. Capture live packet data from network interface.

Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.

Import packets from text files containing hex dumps of packet data.

Display packets with very detailed protocol information.

Save packet data captured.

Export some or all packets in a number of capture file formats.

Filter and search for packets on many criteria.

Colorize packet display based on filters.

Create various statistics.

* + 1. Wireshark isn’t an intrusion detection system; it will not warn you when someone does strange things on your network that he isn’t allowed to do. But it might help you figure out what is really going on.

It will not manipulate things on the network, it will only measure things, it doesn’t send packets on the network or do other active things(except domain name resolution).

1.2.2 It’s the packet list pane which display a summary of each packet captured.

1.2.3 The packet details pane displays the packet selected in the packet list pane in more detail.

1.2.4 The packet bytes pane displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.

1.2.5 Begin the packet capture, stop the capture, restart the current capture, capture option.

1.2.7 2

1.2.8 2

1.2.9 We ask 8.8.8.8 two times a reply and 8.8.8.8 replied us 2 times.

1.3.2 src host 1.2.3.4

1.3.3 dst host 6.7.8.9

1.3.4 src host 1.2.3.4 and dst host 6.7.8.9

1.3.5 host 1.2.3.4 or host 6.7.8.9

1.3.7 80

1.3.8 22

1.3.9 tcp port 80

1.3.10 tcp port 22 and host 1.2.3.4 or host 6.7.8.9

2.1.2 nc 1.2.3.4 80

2.1.3 nc -u 1.2.3.4 53

2.1.4 nc -l 25

2.1.5 nc -ul 53

2.2.1 7

2.2.2 nc -u 127.0.0.1 7

2.2.3 udp port 7 and host 127.0.0.1

2.2.5 2 packet captured from 127.0.0.1 to 127.0.0.1, there are 2 because the sever is setting to answer us with what we send, src and dsl are the same because we are actually in the server 127.0.0.1.

2.2.6 0

2.2.7 0

2.2.8 2

2.2.9 our hello is in the end, before hello is something that we can’t understand.

2.2.10 7

2.2.11 48214

2.3.1 7

2.3.2 nc 127.0.0.1 7

2.3.3 tcp port 7 and host 127.0.0.1

2.3.5 we get reply and 4 packet appear.

2.3.6 0

2.3.7 a packet with tcp protocol is send by the server to client.

2.3.8 a packet with tcp protocol is send by the client to server.

2.3.9