Wireshark Lab Tutorial

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today.

There are many reasons why Wireshark is so popular :

- It has a great GUI as well as a conventional CLI(T Shark).
- It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)
- It is open-source with a large community of backers and developers.
- All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

Install wire shark

- sudo apt-get install wireshark

The basic features of Wireshark are:

Packet Monitor:

- This segment visually shows the packets flowing inside the network. There are color codes for each type of packet.
- The packets are shown with the following information :
    1. Source address
    2. Destination address
    3. Packet type
    4. Hex dump of the packet
    5. Contents of the packet in text
    6. Source port(if applicable)
    7. Destination port(if applicable)

Import from a capture file:

This feature lets you import packets dump from a capture file to analyse further. There are many formats supported by Wireshark, some of them are:

1. pcapng
2. libpcap
3. Oracle snoop and atmsnoop
4. Finisar (previously Shomiti) Surveyor captures
5. Microsoft Network Monitor captures
6. Novell LANalyzer captures
7. AIX iptrace captures
8. Cinco Networks NetXray captures
9. Network Associates Windows-based Sniffer and Sniffer Pro captures
10. Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures

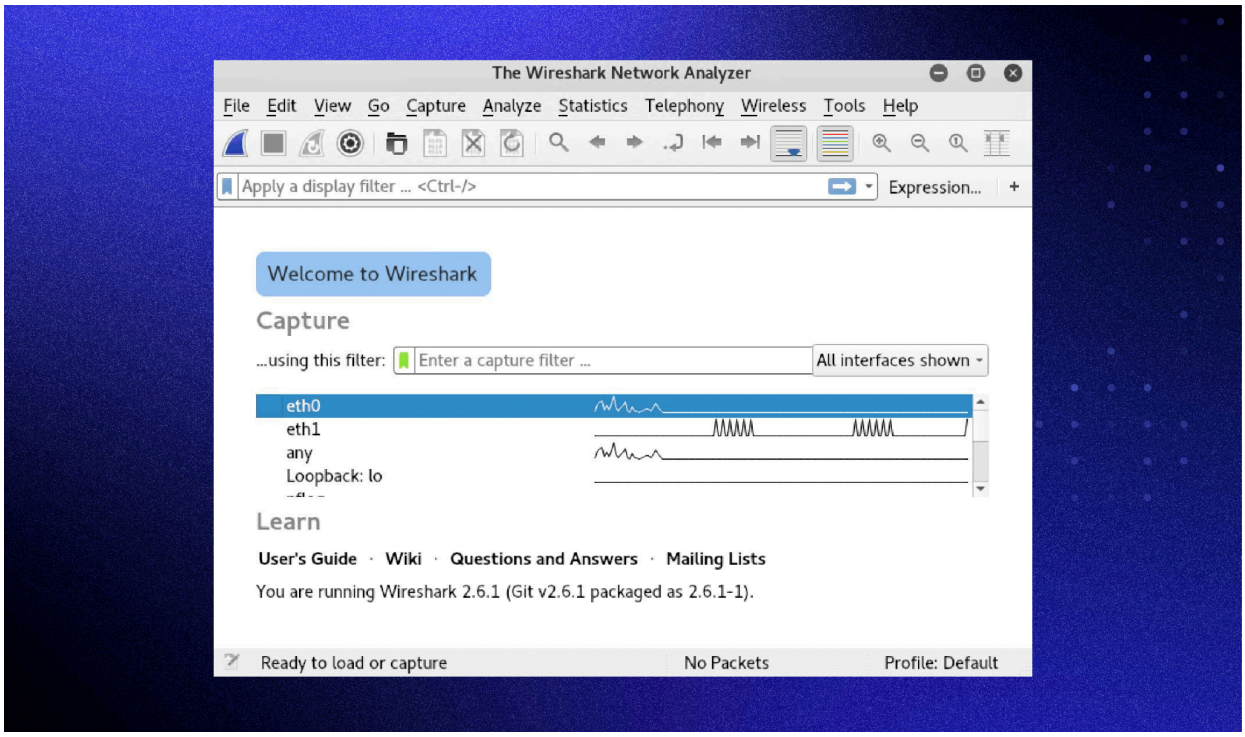
11. AG Group/WildPackets/Savvius EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captures
12. RADCOM's WAN/LAN Analyzer captures
13. Network Instruments Observer version 9 captures
14. Lucent/Ascend router debug output
15. HP-UX's nettl
16. Toshiba's ISDN routers dump output
17. ISDN4BSD i4btrace utility
18. Traces from the EyeSDN USB S0
19. IPLog format from the Cisco Secure Intrusion Detection System
20. the output from VMS's TCPIPtrace/TCPtrace/UCX$TRACE utilities
21. the text output from the DBS Etherwatch VMS utility
22. Visual Networks' Visual UpTime traffic capture
23. the output from CoSine L2 debug
24. the output from Accellent's 5Views LAN agents
25. Endace Measurement Systems' ERF format captures
26. Linux Bluez Bluetooth stack hcidump -w traces
27. Catapult DCT2000 .out files
28. Gammu generated text output from Nokia DCT3 phones in Netmonitor mode
29. IBM Series (OS/400) Comm traces (ASCII & UNICODE)
30. Juniper Netscreen snoop captures
31. Symbian OS btsnoop captures
32. Tamosoft CommView captures
33. Textronix K12xx 32bit .rf5 format captures
34. Textronix K12 text file format captures
35. Apple PacketLogger captures
36. Captures from Aethra Telecommunications' PC108 software

Export to a capture file:

Wireshark lets you save the results as a capture file to continue working on them at later point of time. The supported formats are:

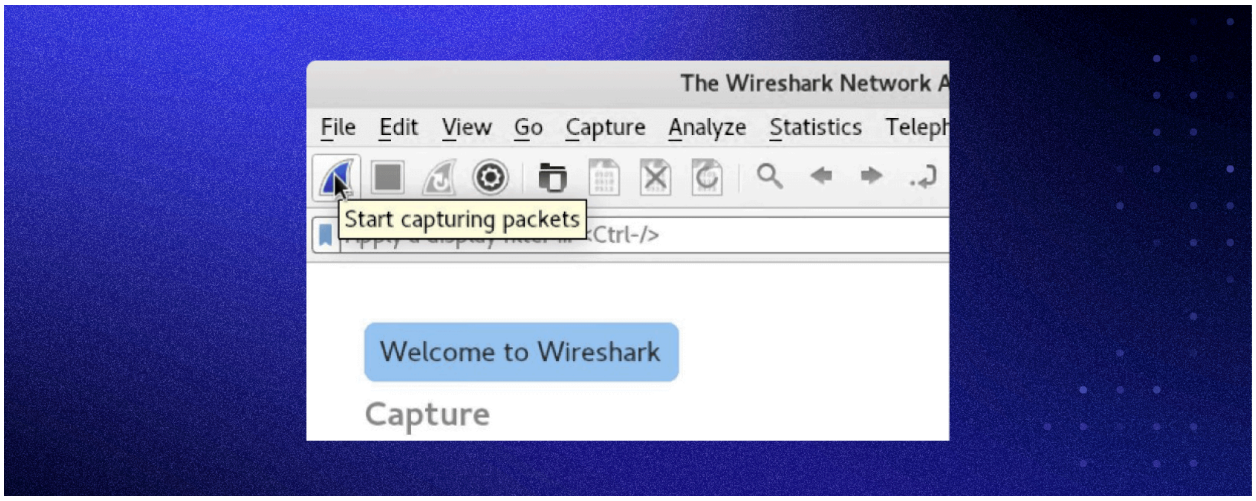
1. pcapng (*.pcapng)
2. libpcap, tcpdump and various other tools using tcpdump's capture format (*.pcap, *.cap, *.dmp)
3. Accellent 5Views (*.5vw)
4. HP-UX's nettl (*.TRC0, *.TRC1)
5. Microsoft Network Monitor - NetMon (*.cap)
6. Network Associates Sniffer - DOS (*.cap, *.enc, *.trc, *fdc, *.syc)
7. Network Associates Sniffer - Windows (*.cap)
8. Network Instruments Observer version 9 (*.bfr)
9. Novell LANalyzer (*.tr1)
10. Oracle (previously Sun) snoop (*.snoop, *.cap)
11. Visual Networks Visual UpTime traffic (*.*).

Capturing data packets on Wireshark:

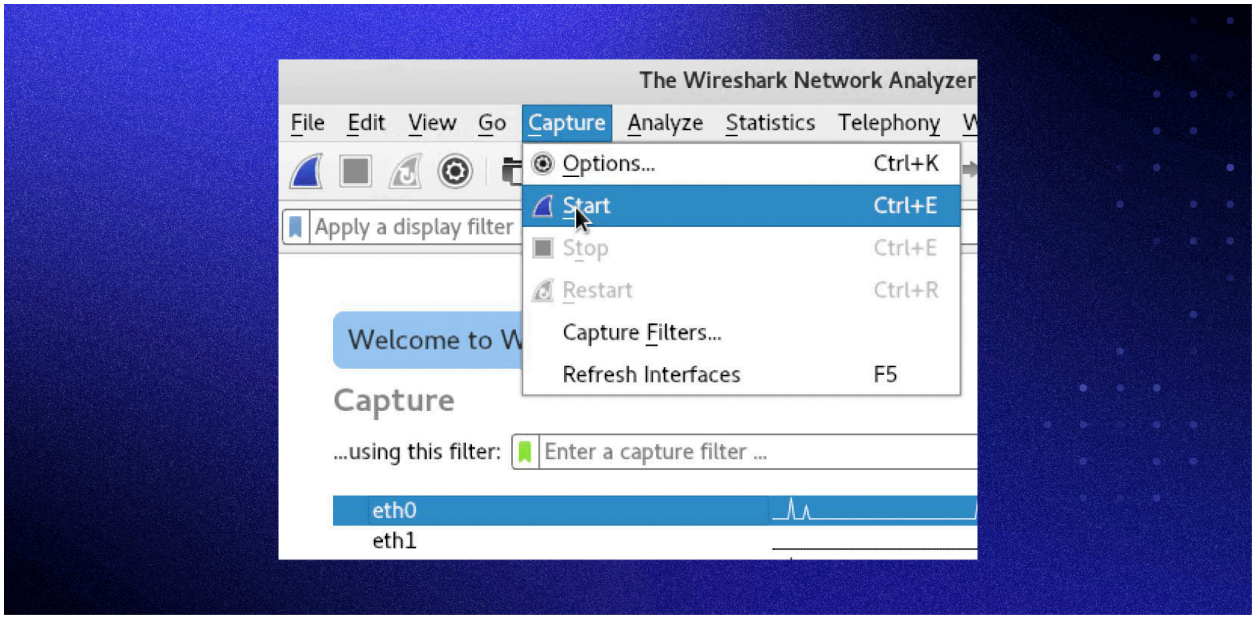


You can select one or more of the network interfaces using shift+left-click. Once select the network interface, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled "Start capturing packets.

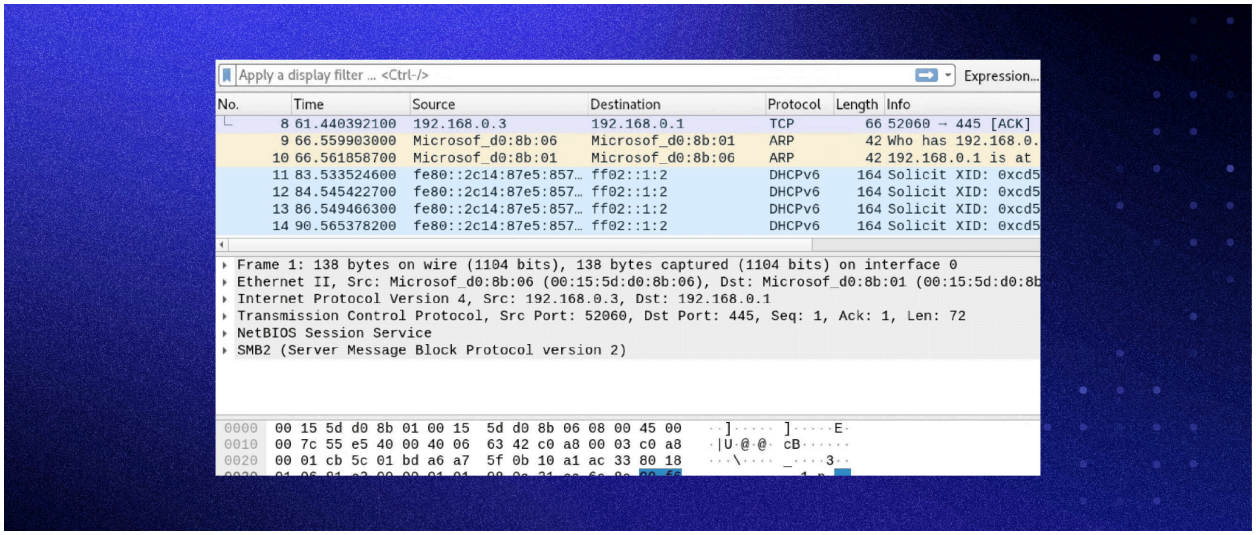


You can select the menu item Capture -> Start.



Or you could use the keystroke Control+E.

During the capture, Wireshark will show you the packets captured in real-time.



Once you have captured all the packets needed, use the same buttons or menu options to stop the capture as you did to begin.