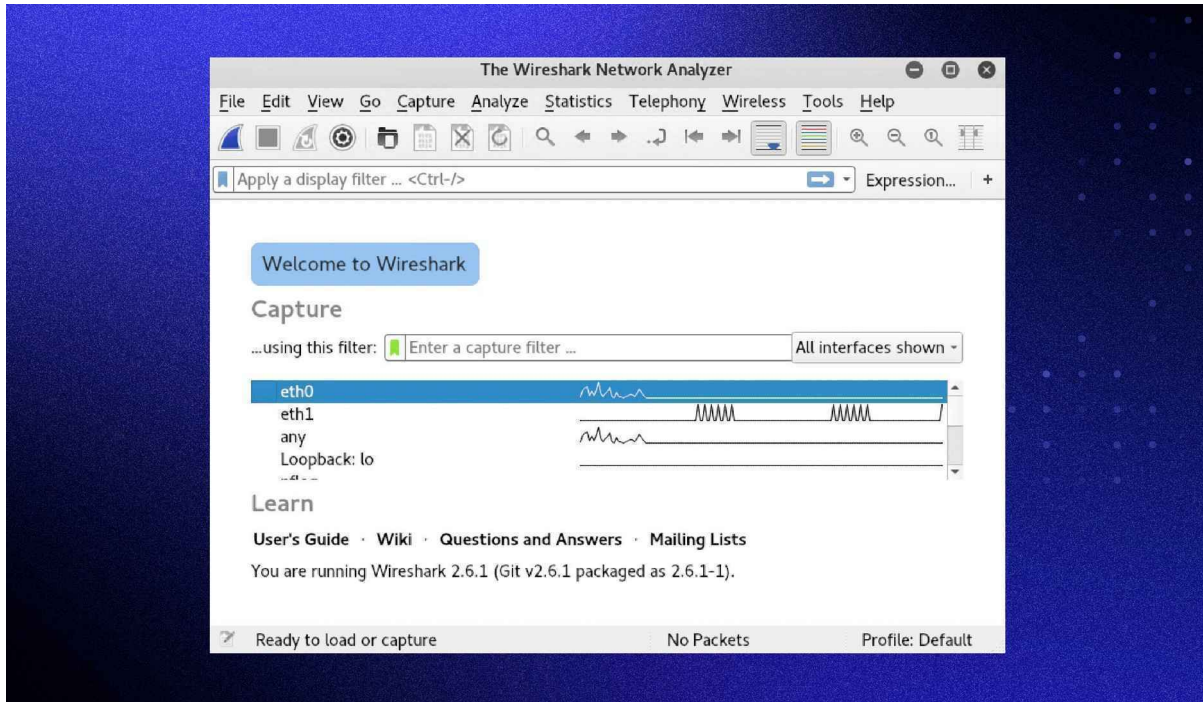


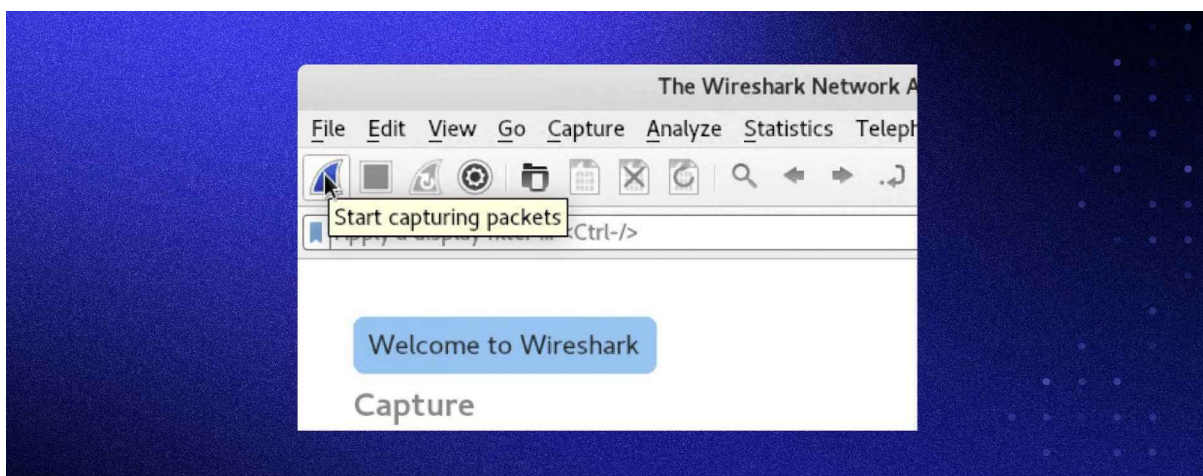
Capturing data packets on Wireshark

When you open Wireshark, you see a screen showing you a list of all the network connections you can monitor. You also have a capture filter field .to only capture the network traffic you want to see

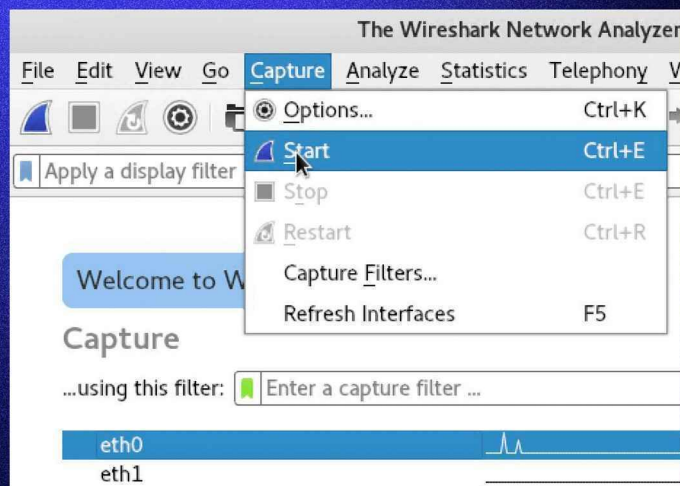


You can select one or more of the network interfaces using shift+left-click. Once select the network interface, you can start the capture, and there .are several ways to do that

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**

No.	Time	Source	Destination	Protocol	Length	Info
8	61.440392100	192.168.0.3	192.168.0.1	TCP	66	52060 → 445 [ACK]
9	66.559903000	Microsof_d0:8b:06	Microsof_d0:8b:01	ARP	42	Who has 192.168.0.1
10	66.561858700	Microsof_d0:8b:01	Microsof_d0:8b:06	ARP	42	192.168.0.1 is at
11	83.533524600	fe80::2c14:87e5:857...	ff02::1:2	DHCPv6	164	Solicit XID: 0xcd5
12	84.545422700	fe80::2c14:87e5:857...	ff02::1:2	DHCPv6	164	Solicit XID: 0xcd5
13	86.549466300	fe80::2c14:87e5:857...	ff02::1:2	DHCPv6	164	Solicit XID: 0xcd5
14	90.565378200	fe80::2c14:87e5:857...	ff02::1:2	DHCPv6	164	Solicit XID: 0xcd5

Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
 Ethernet II, Src: Microsof_d0:8b:06 (00:15:5d:d0:8b:06), Dst: Microsof_d0:8b:01 (00:15:5d:d0:8b:01)
 Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1
 Transmission Control Protocol, Src Port: 52060, Dst Port: 445, Seq: 1, Ack: 1, Len: 72
 NetBIOS Session Service
 SMB2 (Server Message Block Protocol version 2)

0000	00 15 5d d0 8b 01 00 15	5d d0 8b 06 08 00 45 00	...]	...	E
0010	00 7c 55 e5 40 00 40 06	03 42 c0 a8 00 03 c0 a8	...	U@	...	cB
0020	00 01 cb 5c 01 bd a6 a7	5f 0b 10 a1 ac 33 80 18	...	\	...	3

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

Best practice dictates stopping Wireshark's packet capture before
analysis