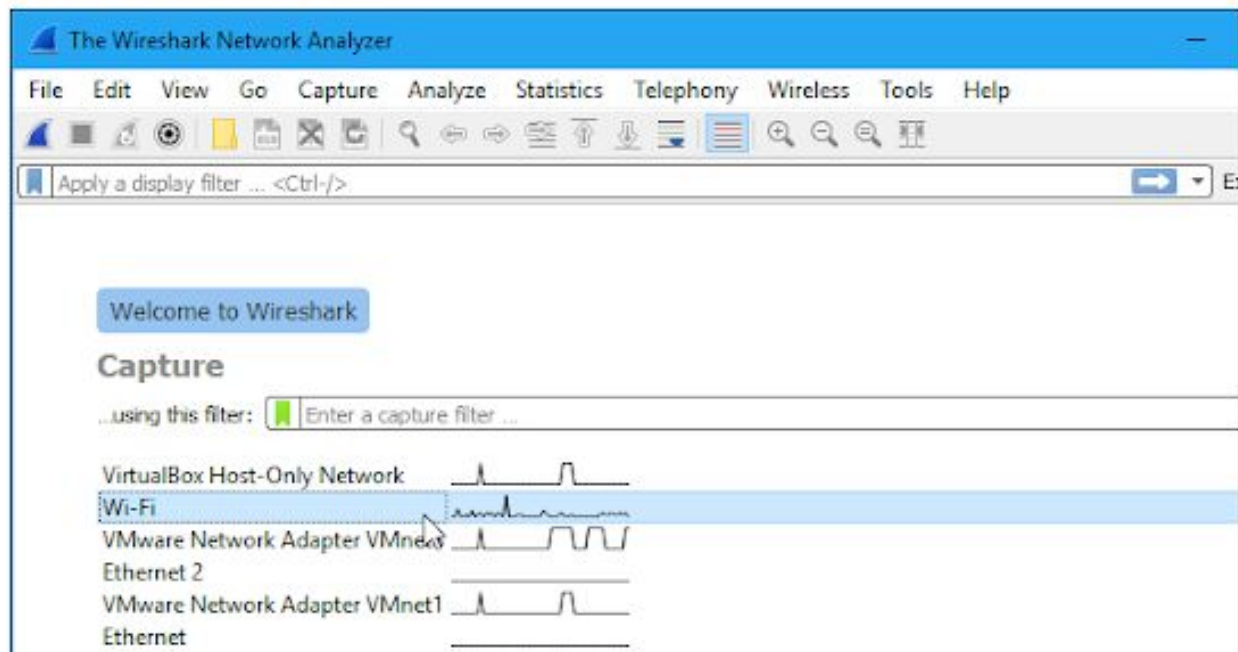


Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2031	36.951443	2607:f8b0:400e:c04:...	2601:1c0:cf00:8961:...	TLSv1.2	120	Application D
2032	36.951504	2601:1c0:cf00:8961:...	2607:f8b0:400e:c04:...	TCP	74	58841 → 443 [
2033	36.951770	2601:1c0:cf00:8961:...	2607:f8b0:400e:c04:...	TLSv1.2	120	Application D
2034	37.017175	2607:f8b0:400e:c04:...	2601:1c0:cf00:8961:...	TCP	74	443 → 58841 [
2035	37.216674	2601:1c0:cf00:8961:...	2607:f8b0:400e:c05:...	TCP	127	[TCP cement

> Frame 2032: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 > Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8)
 > Internet Protocol Version 6, Src: 2601:1c0:cf00:8961:e182:3669:c103:5336, Dst: 2607:f8b0:400e:c04:...

```

0000  1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 86 dd 60 04  ..,5..|\ .8....`.
0010  31 8f 00 14 06 40 26 01 01 c0 cf 00 89 61 e1 82  1....@&. ....a..
0020  36 69 c1 03 53 36 26 07 f8 b0 40 0e 0c 04 00 00  6i..S6&. ..@.....
0030  00 00 00 00 00 68 e5 d9 01 bb 91 1f c7 c3 4e 79  ....h.. .....Ny
0040  b8 21 50 10 01 04 50 42 00 00                    .!P...PB ..
  
```

Wi-Fi: <live capture in progress> | Packets: 2422 · Displayed: 2422 (100.0%) |

Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

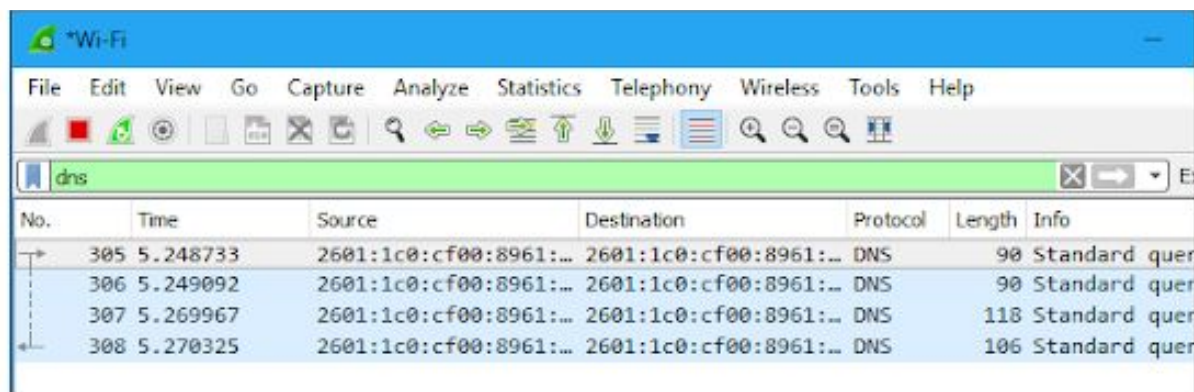
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::1e87:2cff:fe3...	ff02::1	ICMPv6	134	Router Advert
2	3.063059	192.168.29.250	72.165.61.185	UDP	126	54656 → 27017
3	3.075895	192.168.29.250	23.92.23.135	TCP	66	59500 → 443 [
4	3.175677	23.92.23.135	192.168.29.250	TCP	66	443 → 59500 [
5	3.175782	192.168.29.250	23.92.23.135	TCP	64	59500 → 443 [

> Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
 > Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8)

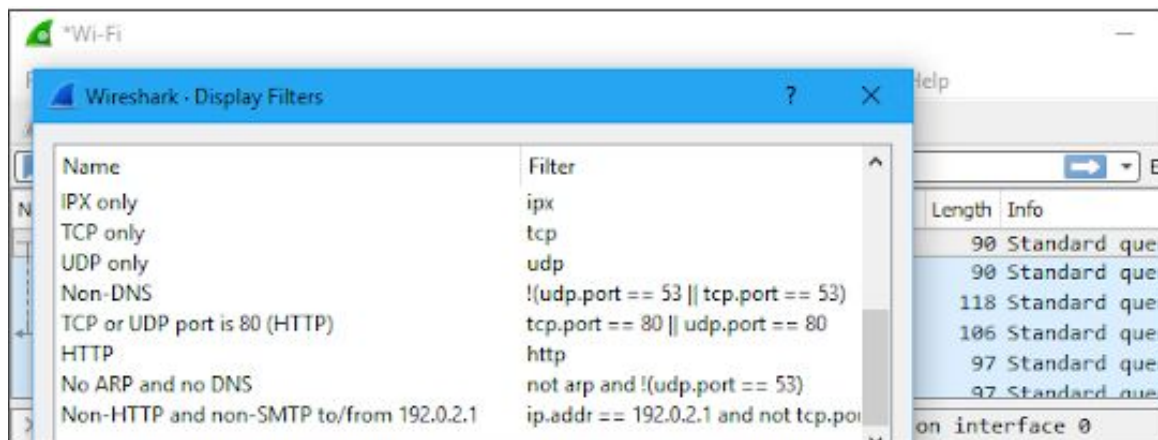
Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

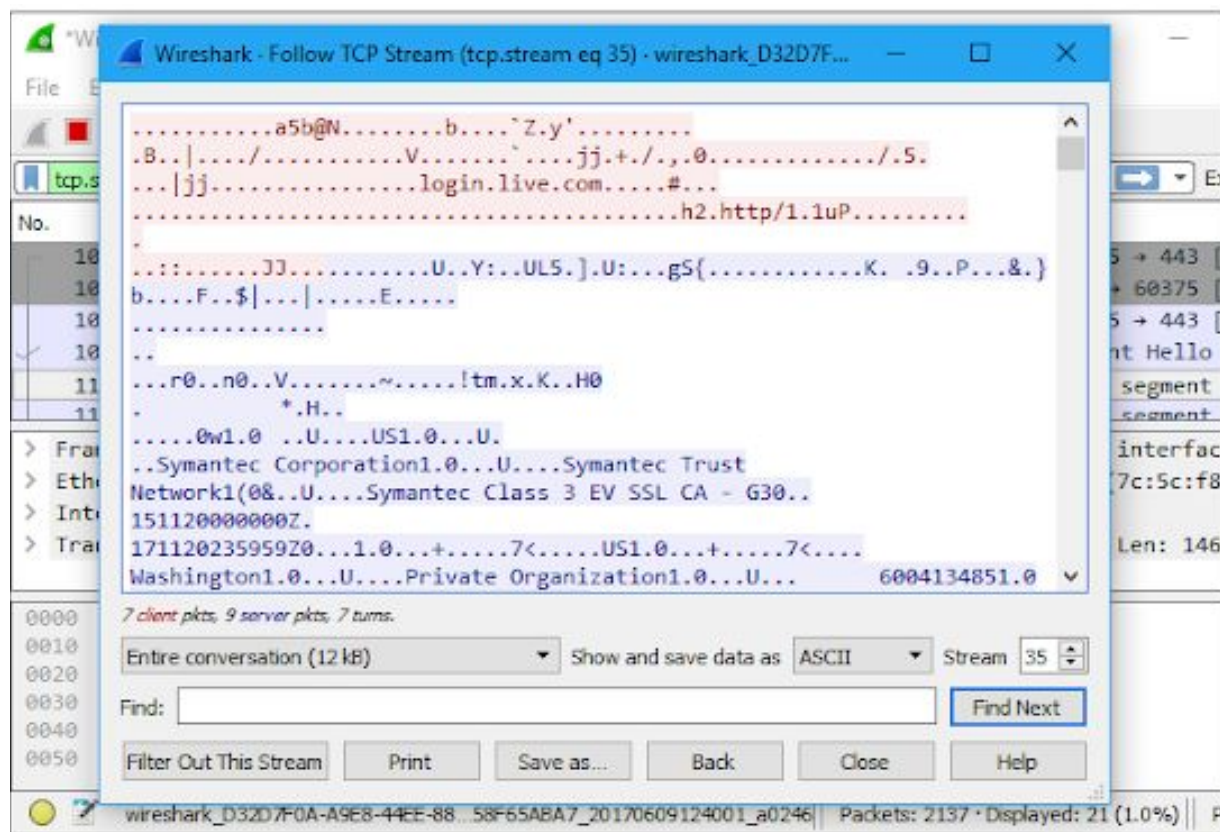


You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

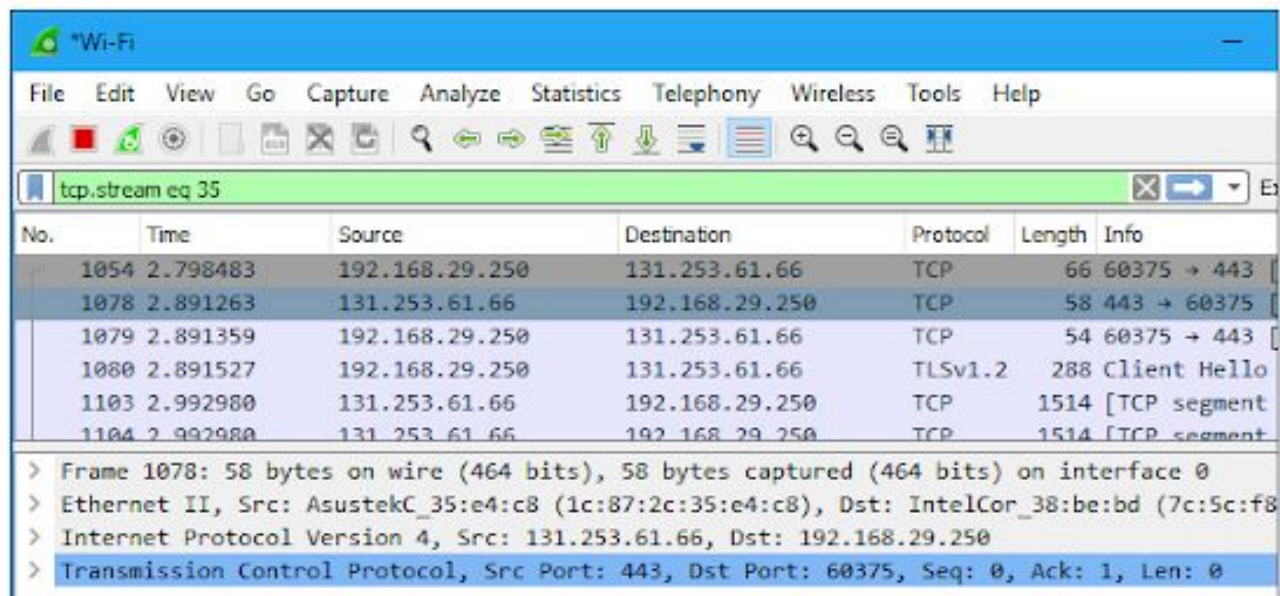


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.



Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

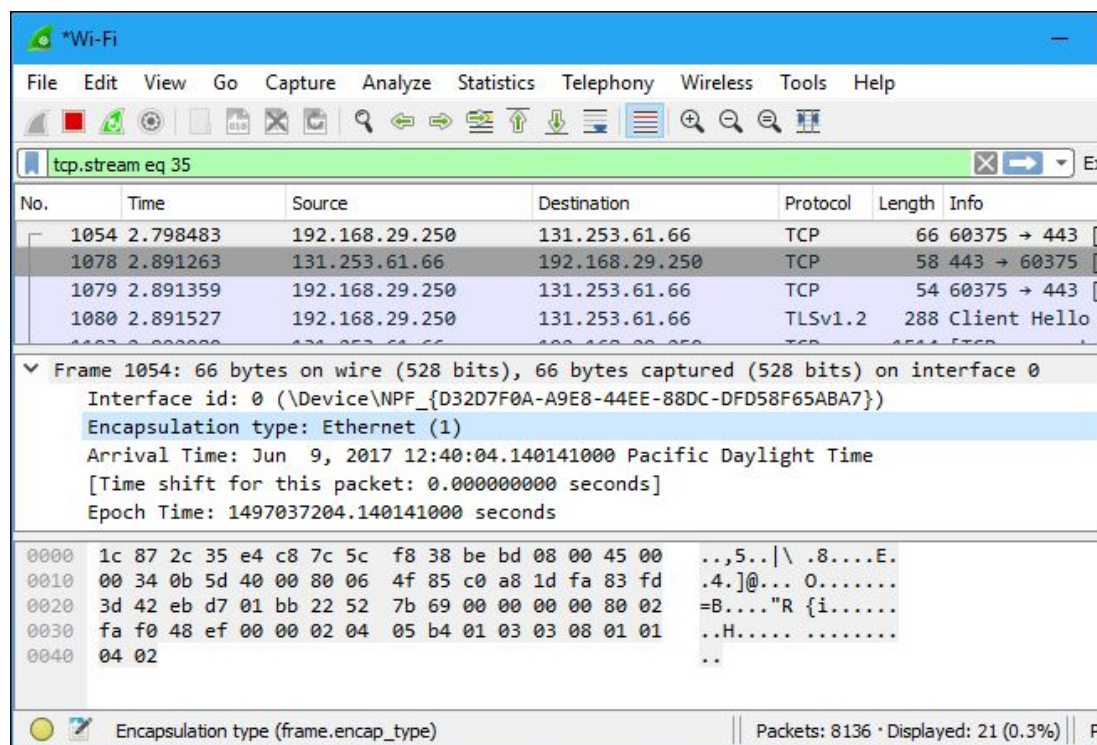


No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello
1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment
1104	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment

> Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
 > Ethernet II, Src: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor_38:be:bd (7c:5c:f8
 > Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250
 > Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0

Inspecting Packets

Click a packet to select it and you can dig down to view its details.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 35

No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
 Encapsulation type: Ethernet (1)
 Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1497037204.140141000 seconds

0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00	...5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd	.4.]@... 0.....
0020	3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02	=B...."R {i.....
0030	fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01	..H.....
0040	04 02	..

Encapsulation type (frame.encap_type) | Packets: 8136 · Displayed: 21 (0.3%) |

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

