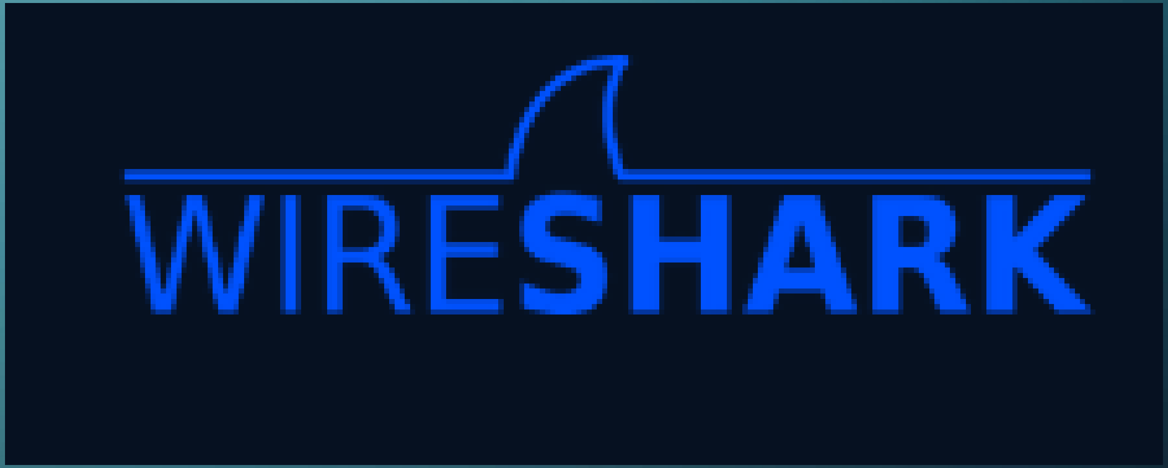
<HOW TO WIRESHARK>

<CORAL S. SCHMIDT MONTILLA>

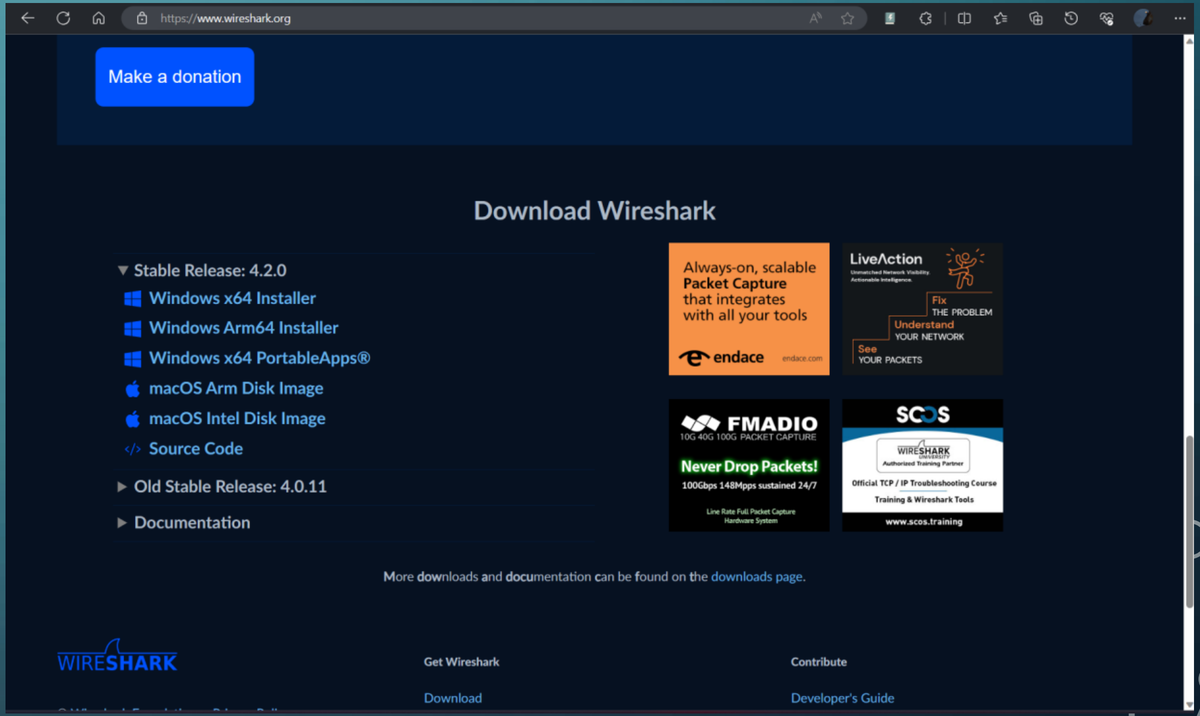
<WHAT IS IT?>

- Analyzing network protocols is what Wireshark® is for. It allows you to capture and interactively browse computer network traffic. It has a vast and robust feature set and is the most popular tool of its kind in the world. It is compatible with the majority of computing platforms, including Windows, macOS, Linux, and UNIX. It is used on a daily basis by network professionals, security specialists, developers, and educators all over the world. It is open source and distributed under the GNU General Public License, version 2.



<DOWNLOADING>

- First off you must go to https://www.wireshark.org/ to download it.
- Scroll down and you should be able to find the download links as shown in the photo. →



Download Wireshark

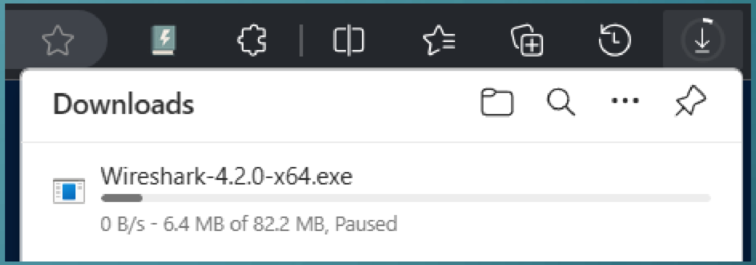
- ▼ Stable Release: 4.2.0
  - Windows x64 Installer
  - Windows Arm64 Installer
  - Windows x64 PortableApps®
  - macOS Arm Disk Image
  - macOS Intel Disk Image
  - Source Code
- ▶ Old Stable Release: 4.0.11
- ▶ Documentation

More downloads and documentation can be found on the downloads page.

Always-on, scalable Packet Capture that integrates with all your tools
endace endace.com
LiveAction
Fix THE PROBLEM
Understand YOUR NETWORK
See YOUR PACKETS
FMADIO
10G 40G 100G PACKET CAPTURE
Never Drop Packets!
100Gbps 148Mpps sustained 24/7
Line Rate Full Packet Capture Hardware System
SCOS
WIRESHARK
Official TCP / IP Troubleshooting Course
Training & Wireshark Tools
www.scos.training

<DOWNLOADING>

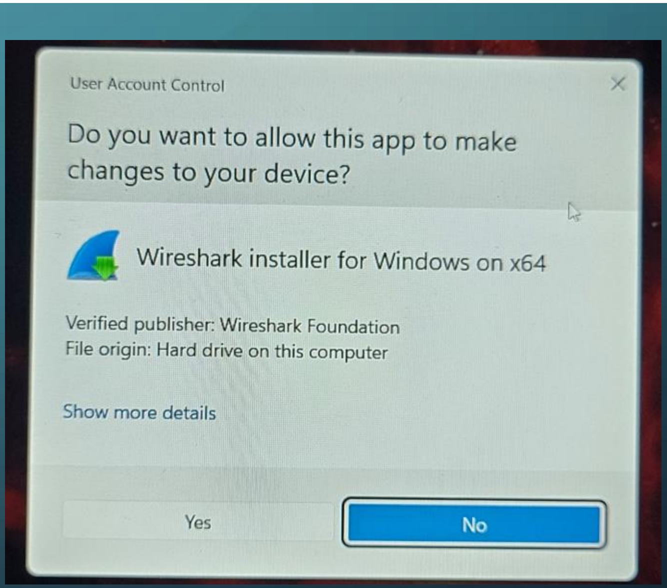
- Once you click your preferred Stable release it should start downloading and it will show up in your download files.→
- Once downloaded go to your download folder and double click the Wireshark file. Then click yes to allow the app to make changes to your device. →



Downloads

Wireshark-4.2.0-x64.exe

0 B/s - 6.4 MB of 82.2 MB, Paused



User Account Control

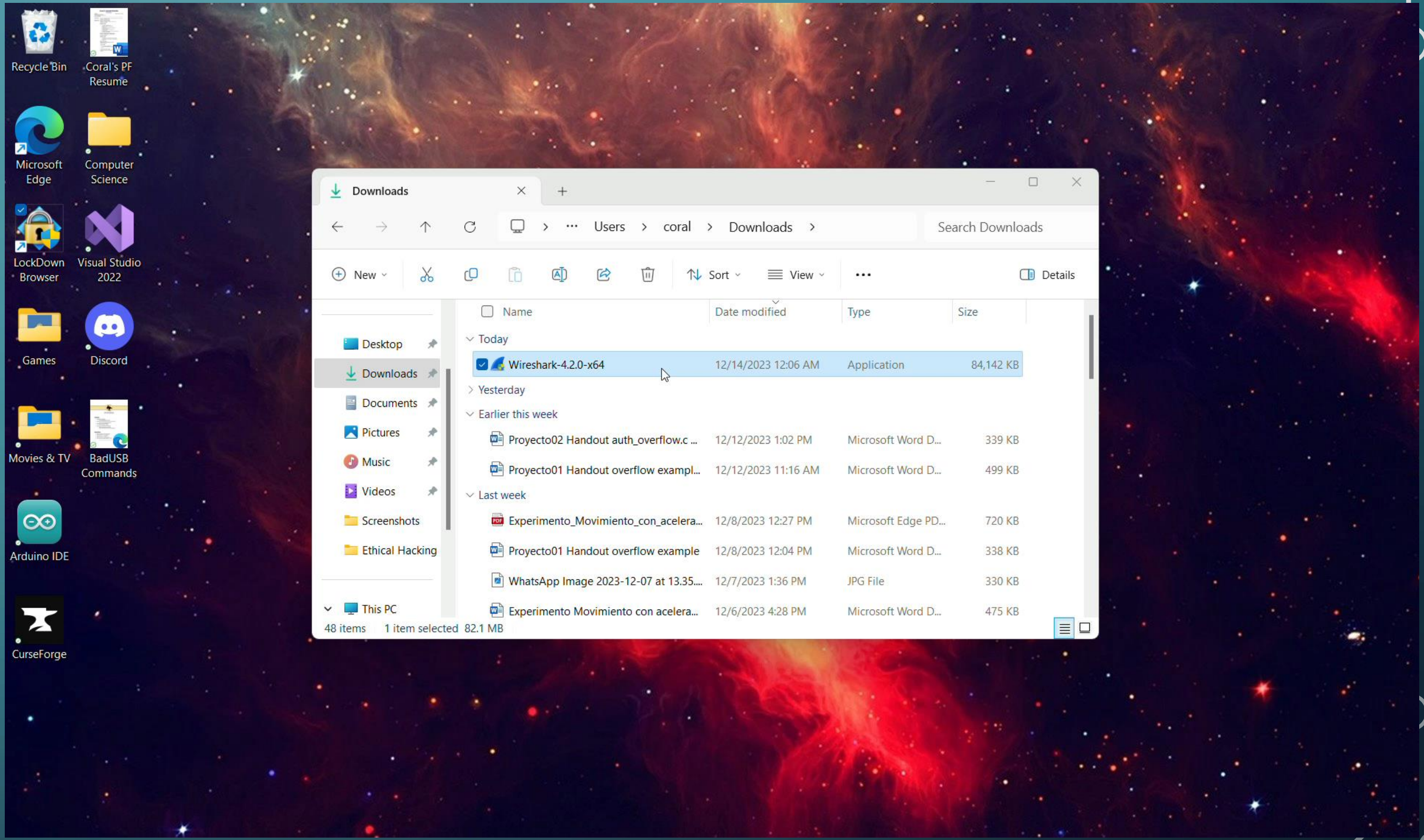
Do you want to allow this app to make changes to your device?

Wireshark installer for Windows on x64

Verified publisher: Wireshark Foundation
File origin: Hard drive on this computer

<DOWNLOADING>

- Here is a video on the installation prosses if you wish to leave it in the default settings. →

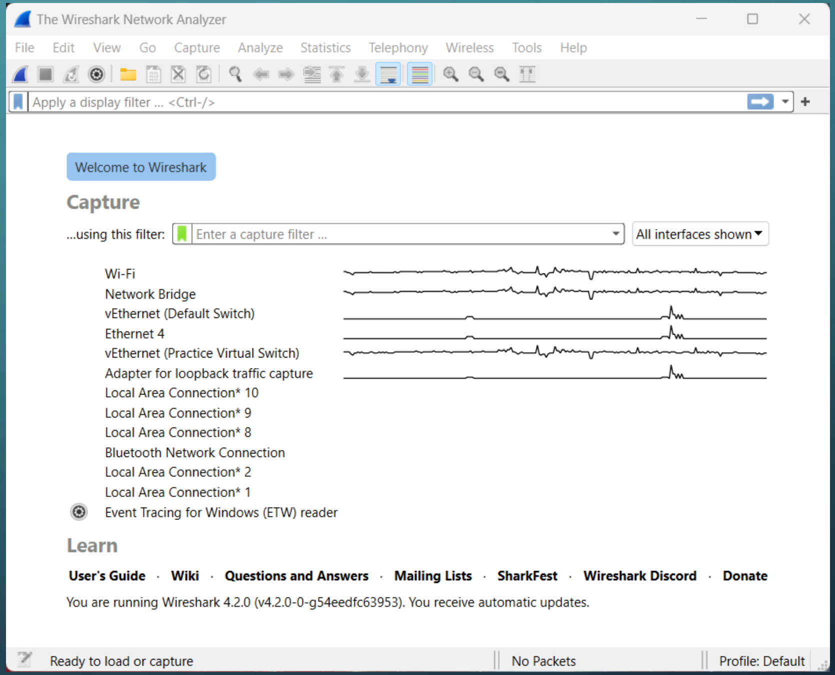


Name	Date modified	Type	Size
Today			
☑ Wireshark-4.2.0-x64	12/14/2023 12:06 AM	Application	84,142 KB
Yesterday			
Earlier this week			
Proyecto02 Handout auth_overflow.c ...	12/12/2023 1:02 PM	Microsoft Word D...	339 KB
Proyecto01 Handout overflow exampl...	12/12/2023 11:16 AM	Microsoft Word D...	499 KB
Last week			
Experimento_Movimiento_con_acelera...	12/8/2023 12:27 PM	Microsoft Edge PD...	720 KB
Proyecto01 Handout overflow example	12/8/2023 12:04 PM	Microsoft Word D...	338 KB
WhatsApp Image 2023-12-07 at 13.35....	12/7/2023 1:36 PM	JPG File	330 KB
Experimento Movimiento con acelera...	12/6/2023 4:28 PM	Microsoft Word D...	475 KB

48 items 1 item selected 82.1 MB

<DOWNLOADING>

- Once finished this icon should appear on your desktop. →
- Then double click it to open it, and this should pop up. →
- It should start showing you different networks connected to the machine.
- Wireshark is only going to show you the networks that are connected to your machine. So, it will appear differently to mine.



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

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi
Network Bridge
vEthernet (Default Switch)
Ethernet 4
vEthernet (Practice Virtual Switch)
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Event Tracing for Windows (ETW) reader

Learn

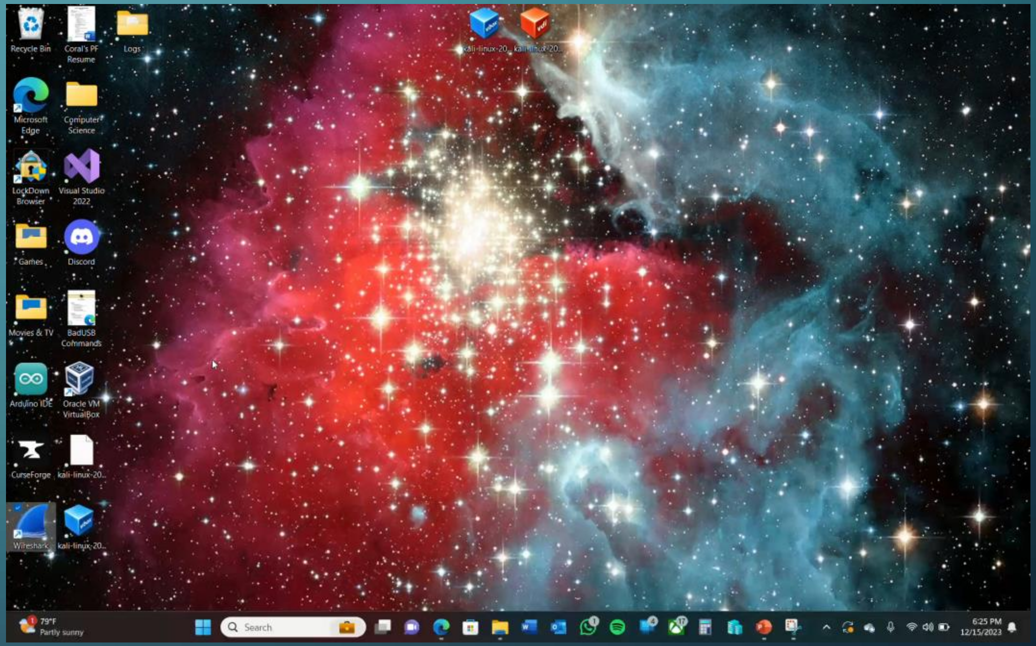
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.0 (v4.2.0-0-g54eedfc63953). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

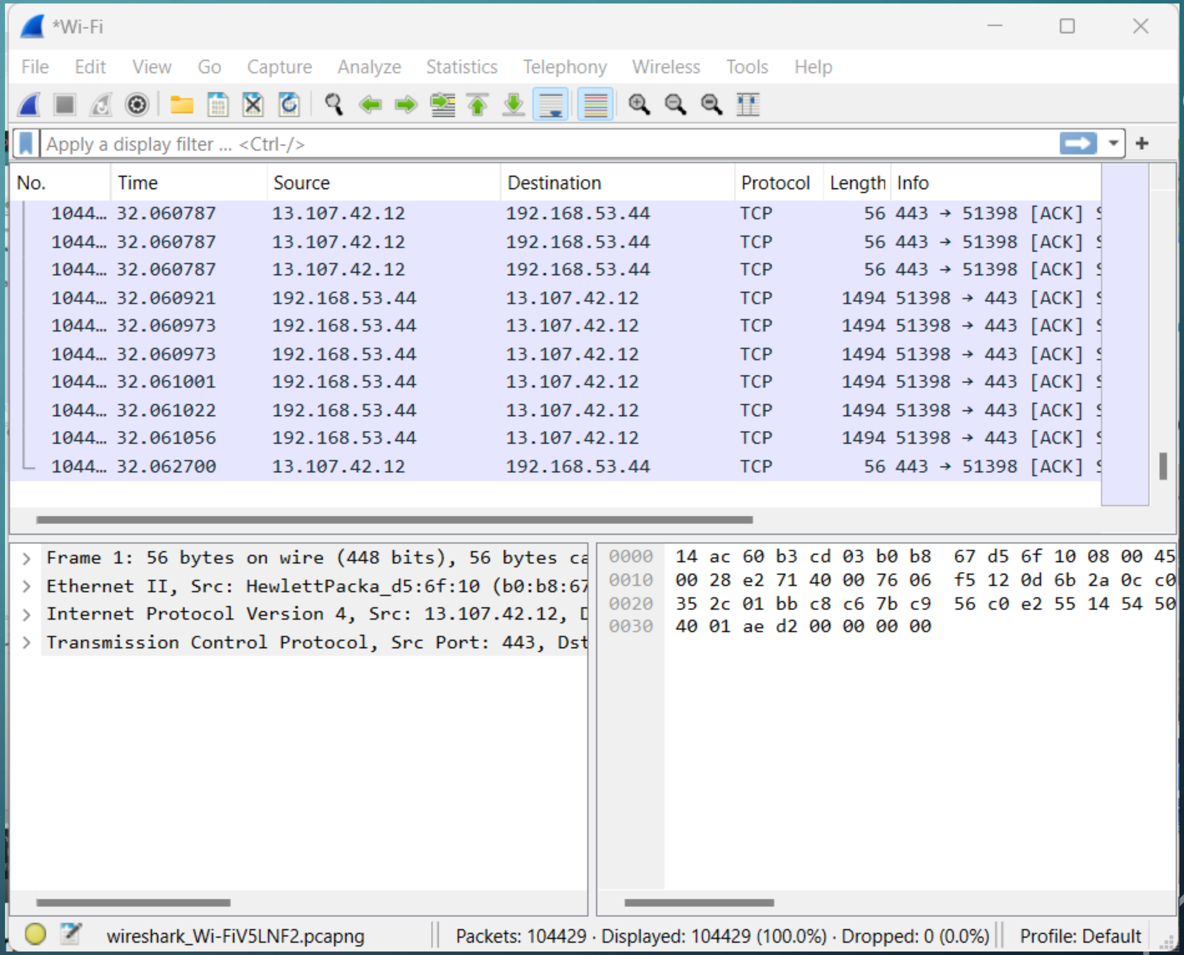
<USAGE>

- Since my machine is a laptop that is currently connected to the Wi-Fi, that will be my network with the most traffic.
- To start with the basics, click on the network that you have traffic on. →
- This will automatically put it into capturing mode.
- To stop capturing just click this button on the top left corner. → 🟥



<USAGE>

- This is the number of pages that we have captured.
- To start a new capturing prosses just click on this button just beside the one to stop it from capturing. →



No.	Time	Source	Destination	Protocol	Length	Info
1044…	32.060787	13.107.42.12	192.168.53.44	TCP	56	443 → 51398 [ACK]
1044…	32.060787	13.107.42.12	192.168.53.44	TCP	56	443 → 51398 [ACK]
1044…	32.060787	13.107.42.12	192.168.53.44	TCP	56	443 → 51398 [ACK]
1044…	32.060921	192.168.53.44	13.107.42.12	TCP	1494	51398 → 443 [ACK]
1044…	32.060973	192.168.53.44	13.107.42.12	TCP	1494	51398 → 443 [ACK]
1044…	32.060973	192.168.53.44	13.107.42.12	TCP	1494	51398 → 443 [ACK]
1044…	32.061001	192.168.53.44	13.107.42.12	TCP	1494	51398 → 443 [ACK]
1044…	32.061022	192.168.53.44	13.107.42.12	TCP	1494	51398 → 443 [ACK]
1044…	32.061056	192.168.53.44	13.107.42.12	TCP	1494	51398 → 443 [ACK]
1044…	32.062700	13.107.42.12	192.168.53.44	TCP	56	443 → 51398 [ACK]

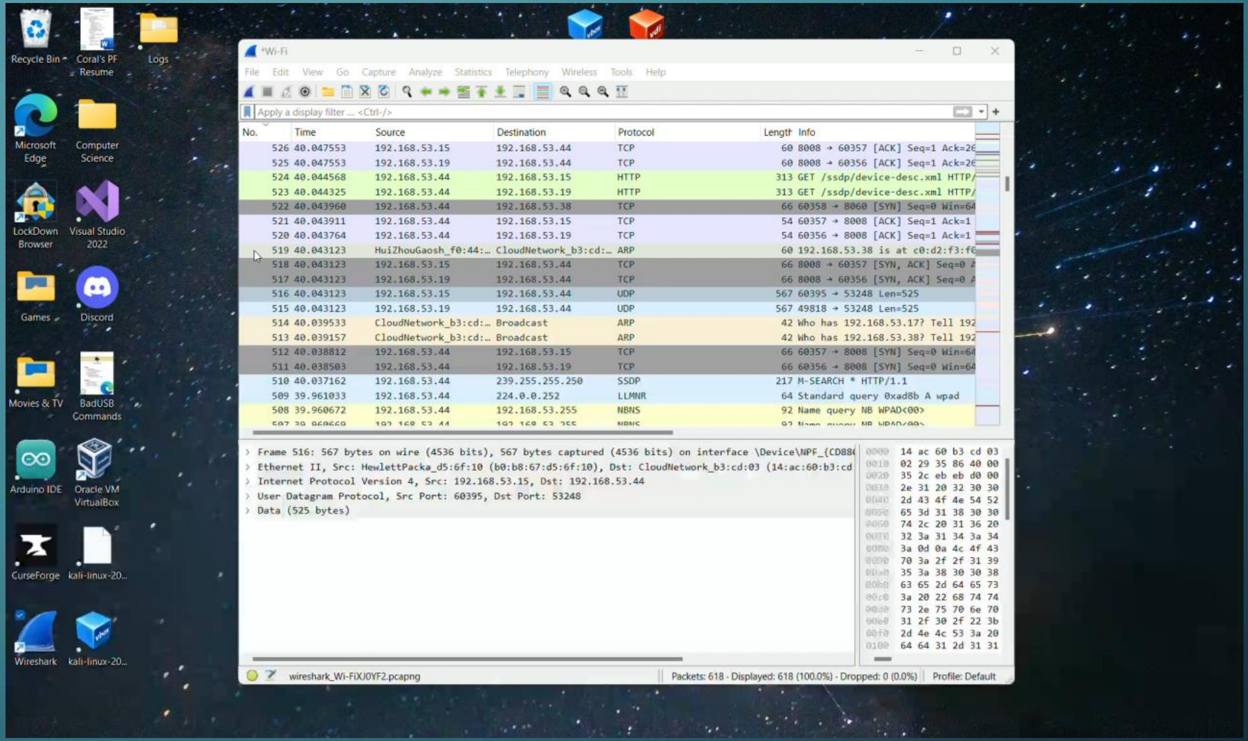
```
> Frame 1: 56 bytes on wire (448 bits), 56 bytes ca
> Ethernet II, Src: HewlettPacka_d5:6f:10 (b0:b8:67
> Internet Protocol Version 4, Src: 13.107.42.12, D
> Transmission Control Protocol, Src Port: 443, Dst
```

```
0000  14 ac 60 b3 cd 03 b0 b8  67 d5 6f 10 08 00 45
0010  00 28 e2 71 40 00 76 06  f5 12 0d 6b 2a 0c c0
0020  35 2c 01 bb c8 c6 7b c9  56 c0 e2 55 14 54 50
0030  40 01 ae d2 00 00 00 00
```

wireshark_Wi-FiV5LNF2.pcapng | Packets: 104429 · Displayed: 104429 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

<USAGE>

- Since there is a lot of traffic, we can filter it to only see the ones we are interested in.
- For this basic example we will filter it to http packets. →
- Once filtered it will show you all the packets that specifically has to do with web pages.



```
No.     Time         Source                  Destination             Protocol   Length Info
    526 40.047553    192.168.53.15           192.168.53.44           TCP          60 8008 → 60357 [ACK] Seq=1 Ack=26
    525 40.047553    192.168.53.19           192.168.53.44           TCP          60 8008 → 60356 [ACK] Seq=1 Ack=26
    524 40.044568    192.168.53.44           192.168.53.15           HTTP        313 GET /ssdp/device-desc.xml HTTP/
    523 40.044325    192.168.53.44           192.168.53.19           HTTP        313 GET /ssdp/device-desc.xml HTTP/
    522 40.043960    192.168.53.44           192.168.53.38           TCP          66 60358 → 8060 [SYN] Seq=0 Win=64
    521 40.043911    192.168.53.44           192.168.53.15           TCP          54 60357 → 8008 [ACK] Seq=1 Ack=1
    520 40.043764    192.168.53.44           192.168.53.19           TCP          54 60356 → 8008 [ACK] Seq=1 Ack=1
    519 40.043123    HuiZhouGaosh_f0:44:…    CloudNetwork_b3:cd:…    ARP          60 192.168.53.38 is at c0:d2:f3:f6
    518 40.043123    192.168.53.15           192.168.53.44           TCP          66 8008 → 60357 [SYN, ACK] Seq=0 A
    517 40.043123    192.168.53.19           192.168.53.44           TCP          66 8008 → 60356 [SYN, ACK] Seq=0 A
    516 40.043123    192.168.53.15           192.168.53.44           UDP         567 60395 → 53248 Len=525
    515 40.043123    192.168.53.19           192.168.53.44           UDP         567 49818 → 53248 Len=525
    514 40.039533    CloudNetwork_b3:cd:…    Broadcast               ARP          42 Who has 192.168.53.17? Tell 192
    513 40.039157    CloudNetwork_b3:cd:…    Broadcast               ARP          42 Who has 192.168.53.38? Tell 192
    512 40.038812    192.168.53.44           192.168.53.15           TCP          66 60357 → 8008 [SYN] Seq=0 Win=64
    511 40.038503    192.168.53.44           192.168.53.19           TCP          66 60356 → 8008 [SYN] Seq=0 Win=64
    510 40.037162    192.168.53.44           239.255.255.250         SSDP        217 M-SEARCH * HTTP/1.1
    509 39.961033    192.168.53.44           224.0.0.252             LLMNR        64 Standard query 0xad8b A wpad
    508 39.960672    192.168.53.44           192.168.53.255          NBNS         92 Name query NB WPAD<00>
    507 39.960669    192.168.53.44           192.168.53.255          NBNS         92 Name query NB WPAD<00>
```

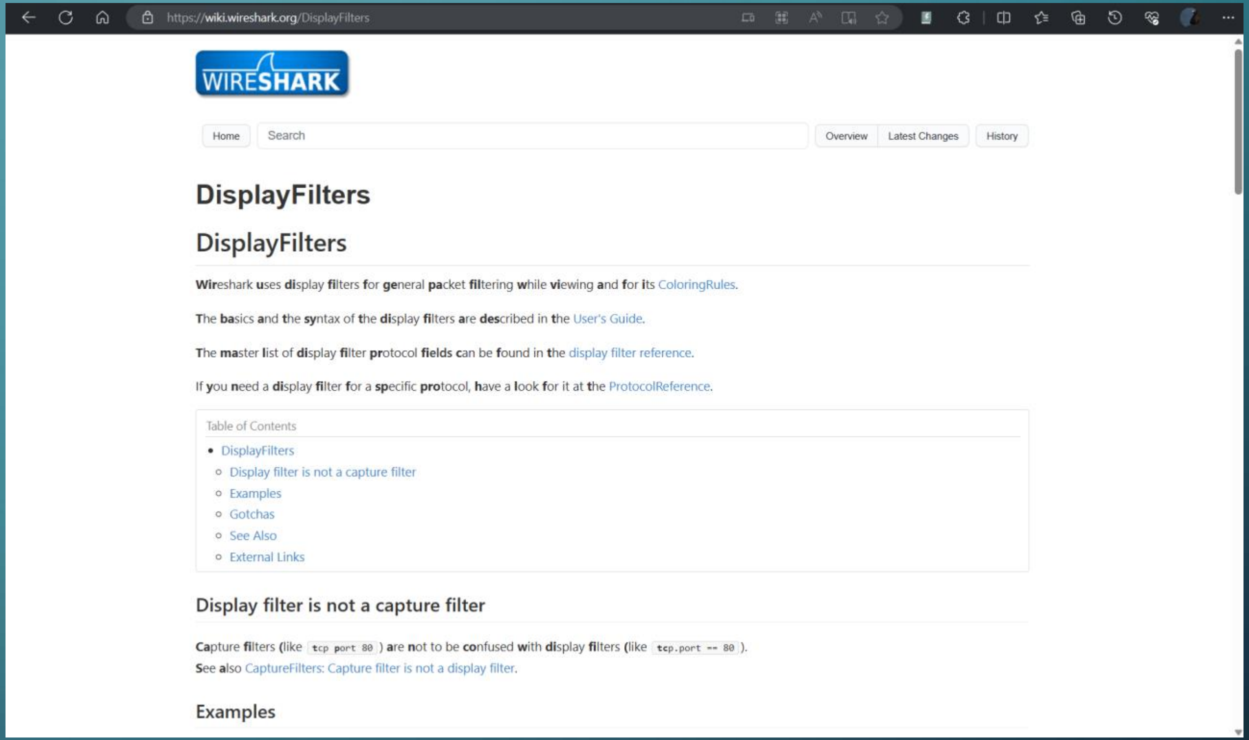
```
> Frame 516: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface \Device\NPF_{CD88(
> Ethernet II, Src: HewlettPacka_d5:6f:10 (b0:b8:67:d5:6f:10), Dst: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd
> Internet Protocol Version 4, Src: 192.168.53.15, Dst: 192.168.53.44
> User Datagram Protocol, Src Port: 60395, Dst Port: 53248
> Data (525 bytes)
```

```
0000  14 ac 60 b3 cd 03
0010  02 29 35 86 40 00
0020  35 2c eb eb d0 00
0030  2e 31 20 32 30 30
0040  2d 43 4f 4e 54 52
0050  65 3d 31 38 30 30
0060  74 2c 20 31 36 20
0070  32 3a 31 34 3a 34
0080  3a 0d 0a 4c 4f 43
0090  70 3a 2f 2f 31 39
00a0  35 3a 38 30 30 38
00b0  63 65 2d 64 65 73
00c0  3a 20 22 68 74 74
00d0  73 2e 75 70 6e 70
00e0  31 2f 30 2f 22 3b
00f0  2d 4e 4c 53 3a 20
0100  64 64 31 2d 31 31
```

wireshark_Wi-FiXJ0YF2.pcapng | Packets: 618 · Displayed: 618 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

<USAGE>

- If you want to know more about other filters and what it shows here is the link to them: https://wiki.wireshark.org/DisplayFilters



DisplayFilters

DisplayFilters

Wireshark uses display filters for general packet filtering while viewing and for its ColoringRules.

The basics and the syntax of the display filters are described in the User's Guide.

The master list of display filter protocol fields can be found in the display filter reference.

If you need a display filter for a specific protocol, have a look for it at the ProtocolReference.

Table of Contents

- DisplayFilters
  - Display filter is not a capture filter
  - Examples
  - Gotchas
  - See Also
  - External Links

Display filter is not a capture filter

Capture filters (like `tcp port 80`) are not to be confused with display filters (like `tcp.port == 80`).
See also CaptureFilters: Capture filter is not a display filter.

Examples

<REFERENCES>

- [1]“Wireshark · Frequently Asked Questions,” *Wireshark*, 2019. https://www.wireshark.org/faq.html#_what_is_wireshark (accessed Dec. 14, 2023).
- [2]“Wireshark · Go Deep,” *Wireshark*, 2023. https://www.wireshark.org/ (accessed Dec. 14, 2023).