

# How to Use Wireshark: Network Analysis, 2019 Style

*By Eric Hamilton*

*— Last Updated: 05 Feb'19*



Over 20 years ago, Gerald Combs announced Ethernet 0.2.0, the first public version of what we now know as Wireshark. Developed for Solaris and Linux, Wireshark is an open source network and packet analyzer. The project started life as Ethernet in 1998, but its name was changed to Wireshark in 2006 because of trademark rights issues.

Today, Wireshark is the world's foremost network analyzer, with over 600 contributing authors, multiple awards and its own developer

## Table of Contents

1. [Download and Set Up Wireshark](#)
2. [How to Capture Packets with Wireshark](#)
3. [View Captured Packets with Wireshark](#)
4. [Filtering Packets With Wireshark](#)
5. [Color Coding with Wireshark](#)
6. [Viewing Network Statistics in Wireshark](#)
7. [Final Thoughts](#)

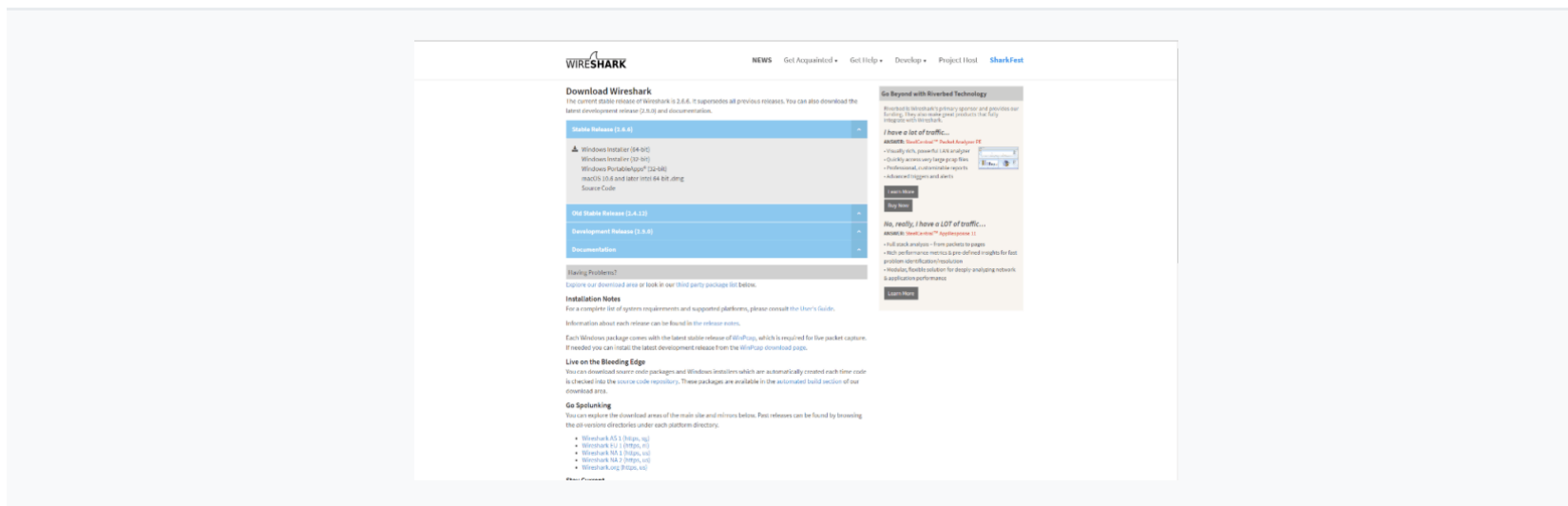
conference, SharkFest.

This guide is will help you get up and running with Wireshark. We'll go over the basics, such as how to download it and capture, view and filter packets. Wireshark has many advanced features that can't be covered within the scope of this article, but there are plenty of tutorials on them at [wireshark.org](https://www.wireshark.org).

---

## Download and Set Up Wireshark

Wireshark is available for download via its [download page](#). To get it for Windows or macOS, click their respective links under the “stable release” section. If you need a source for Linux, scroll to the bottom of the page and find the download for your version under “third-party packages.”



Once you've downloaded the application, you can begin the setup process. If you're a Windows user, you'll need to install the WinPcap library, which is what allows you to capture live network traffic. Without it, you'll only be able to view captured packets that have been saved. The latest version of Wireshark should install WinPcap by default.

Likewise, make sure to install USBPcap, which lets Wireshark capture traffic from USB devices.

# How to Capture Packets with Wireshark

Wireshark is built on its ability to capture network packets and display them in a format that can be interpreted by mere mortals. If you're unsure what network packets are, we go over them in our [IPv4 vs. IPv6](#) guide.

After downloading and installing, you're ready to launch Wireshark and begin capturing packets.

To begin the capture process, you'll need to select your network interface. Upon launching the application, you'll see the available network connections in the launch screen. You can also see advanced features by clicking "capture," then selecting "options".

Select a connection for capturing by:

- ➔ Double-clicking its name.
- ➔ Using the keyboard shortcut CTRL + E.
- ➔ Clicking on the shark fin in the toolbar, located in the far left corner.

Once done, the connection to be recorded will be shaded in blue or gray and Wireshark will start recording network traffic and detailing it. To stop the recording process, press the red

stop button next to the shark fin button. Alternatively, you can use the CTRL + E keyboard shortcut.

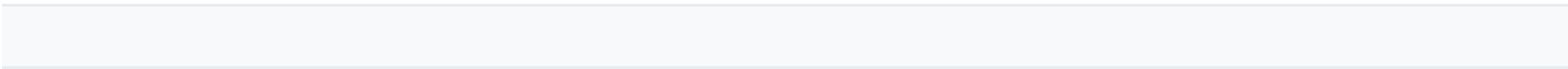
When capturing with Wireshark, promiscuous mode is enabled by default. It allows for the capture of all packets on a network, rather than just those addressed to your computer or network adapter. That said, promiscuous mode isn't supported by all network hardware and interfaces. It can be changed by clicking "edit," then "preferences...".

Check the [Wireshark FAQ](#) for more details on promiscuous mode.

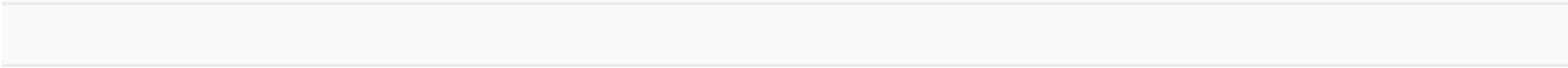
---

## View Captured Packets with Wireshark

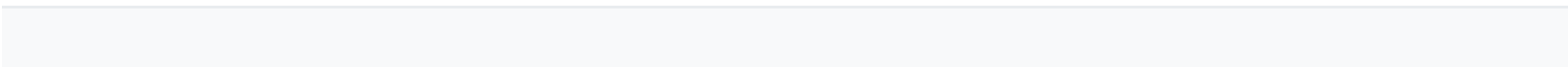
Now that you've recorded data, it's time to view it. When viewing packets, you'll see information spread across three panes: the packet list, the packet details and the packet bytes. The packet list pane is the top one and it displays the time, source, destination, protocol and additional information.



The packet details pane sits in the middle. As the name suggests, it displays details regarding the packet selected. It shows the protocol type, such as IPv4 or IPv6, and addresses, such as IP or MAC, in a collapsible list format.



The packet bytes pane is at the bottom. It contains the raw data from the packet and displays it in a hexadecimal or bit format.



---

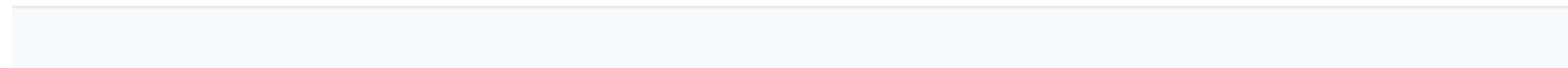
## Filtering Packets With Wireshark

Any time you're analyzing network traffic, you'll want to shut down applications sending packets you don't want to see to narrow the traffic. Even then, you'll likely be left with a lot of

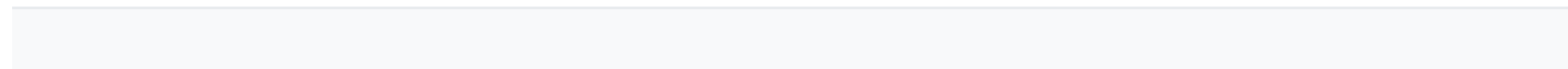
residual packets to sift through. That's where Wireshark's filters come into play. It offers capture filters and display filters, and both affect the capture file differently.

Capture filters are applied to the capture file before the recording process begins, allowing you to decide which packets Wireshark will capture. Display filters, on the other hand, are applied to a capture file after the fact, allowing you to only see packets that meet your specific criteria.

To add a capture filter, click in the entry field above the interfaces shown in the launch window. You can type a filter in, such as TDP, or click the bookmark icon to the left and pick from a drop-down list. For more options, after clicking the green bookmark icon, select "manage capture filters."



Above the capture field, you'll see another entry field that says "apply a display filter..." where you can apply display filters in the same way described for applying capture filters.

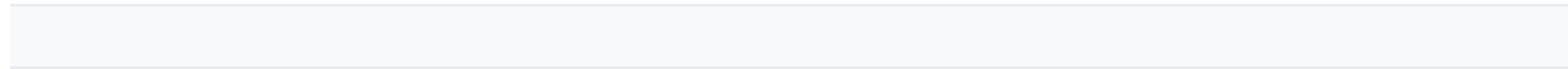


# Color Coding with Wireshark

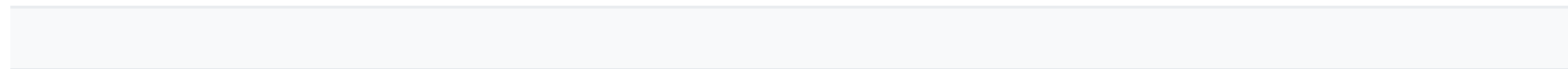
Wireshark's color rules allow you to further separate and individualize packets based on their highlighted color. That way, you can identify certain types of traffic or errors at a glance.

Wireshark's built-in color library offers about 20 shades, all of which can be edited, disabled or deleted.

You can access the colorization options by clicking "view" in the toolbar, than selecting "coloring rules."



Packet colorization can be disabled by clicking "view" and toggling the "colorize packet list" option in the drop-down menu.



---

## Viewing Network Statistics in Wireshark



Wireshark offers a variety of data and metrics about your network, which are accessible via the “statistics” drop-down menu in the toolbar. The metrics include resolved addresses, IPv4 statistics, IPv6 statistics, and other charts and graphs. You can also use display filters there. Statistics can be exported in different file formats, such as .txt, .csv and .xml, as well.

---

## Final Thoughts

Wireshark is a simple but versatile network analyzer and, best of all, it's free. While this guide is meant to show you the basics, we've only begun to scratch the surface of what Wireshark can do. If you're looking to master Wireshark and code your own protocol dissectors, the official [Wireshark user guide](#) is the authoritative reference.



**Sign up for our newsletter**  
to get the latest on new releases and more.

The [Wireshark wiki](#) is another great resource to use alongside the program because it has tutorials, sample captures and tools and plugins.

For more software, look at our [best antiviruses](#), [best password managers](#) and [best accounting software](#). Otherwise, thanks for reading, and let us know in a comment or [tweet](#) if you have Wireshark tips or tricks.

### Leave a Reply

Your email address will not be published. Required fields are marked \*

Comment

Name\*

Email\*

Website

Post Comment

## Also interesting



[best-password-manager](#)

**The Best Password Manager 2019:  
How to Secure Your Online  
Accounts**



[best-antivirus-reviews](#)

**The Best Antivirus Software 2019:  
Getting Security and Speed**



[best-antivirus-for-android](#)

**The Best Antivirus For Android  
2019: Defending Your Droid from  
Malware**



[best-VPN-reviews](#)

**The Best VPN Providers of 2019:  
Protect Your Privacy Online**

# Most popular on Cloudwards

[Free Cloud Storage in 2019: Top Five Providers with Large Free Service Plans](#)

[Best of The Big Three: Dropbox vs Google Drive vs Onedrive](#)

[How to Beat the Netflix VPN Ban](#)

[How to Unblock YouTube: Video Streaming for Everyone](#)



[Cloudwards.net](#) / [Articles](#) / [Online Security](#) / [How to Use Wireshark: Network Analysis, 2019 Style](#)

[!\[\]\(ec9132f1d27c8919987d92907322654d\_img.jpg\) facebook](#) [!\[\]\(9db1a20e6fdae9c15975d240125424df\_img.jpg\) youtube](#) [!\[\]\(69e745cb555ee0441d11497d43826bd7\_img.jpg\) twitter](#) [!\[\]\(f61e8db1ecee0cced7166a49f3b25c88\_img.jpg\) linkedin](#)

[About Us](#) [How we work](#) [Write for us!](#) [Terms and Conditions](#)

[Privacy Policy](#)

Cloudwards.net featured on

THE HUFFINGTON POST

**Inc.**

**Forbes**

  
TechRepublic

  
about.com

  
WHIR  
HOSTING | CLOUD

 AppleWorld.Today

© 2007-2019 Cloudwards.net

We are a professional review site that receives compensation from the companies whose products we review.

We test each product thoroughly and give high marks to only the very best.

We are independently owned and the opinions expressed here are our own.