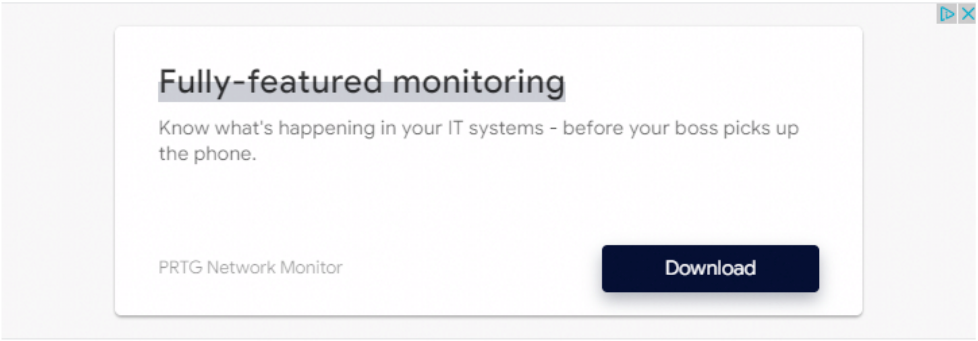
Install and Use Wireshark on Ubuntu Linux

Community
29 Oct 2020 · 6 min read

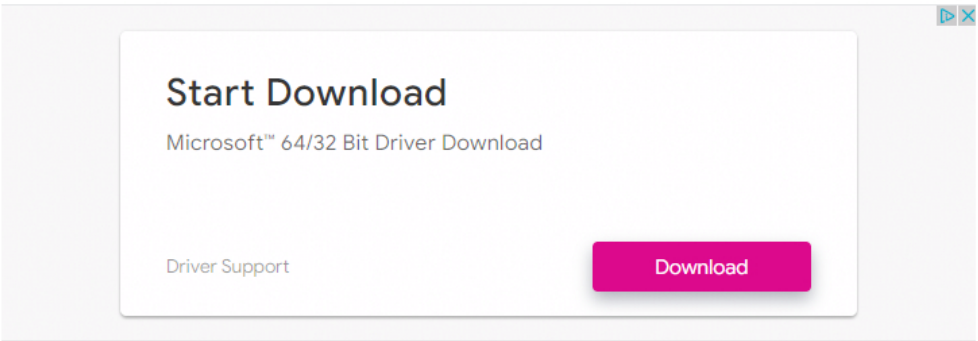


Brief: You'll learn to install the latest Wireshark on Ubuntu and other Ubuntu-based distribution in this tutorial. You'll also learn how to run Wireshark without sudo and how to set it up for packet sniffing.

Wireshark is a free and open-source network protocol analyzer widely used around the globe.

With Wireshark, you can capture incoming and outgoing packets of a network in real-time and use it for network troubleshooting, packet analysis, software and communication protocol development, and many more.

It is available on all major desktop operating systems like Windows, Linux, macOS, BSD and more.



In this tutorial, I will guide you to install Wireshark on Ubuntu and other Ubuntu-based distributions. I'll also show a little about setting up and configuring Wireshark to capture packets.

Installing Wireshark on Ubuntu based Linux distributions

Featured


Best Linux Books For Beginners to Advanced Linux Users


13 Free Training Courses to Learn Linux Online


20 Best Linux Books You Can Download For Free Legally

Latest


How to Install Go Language on Ubuntu
15 Jan 2023


Best Accessories to Supercharge Your Raspberry Pi
12 Jan 2023

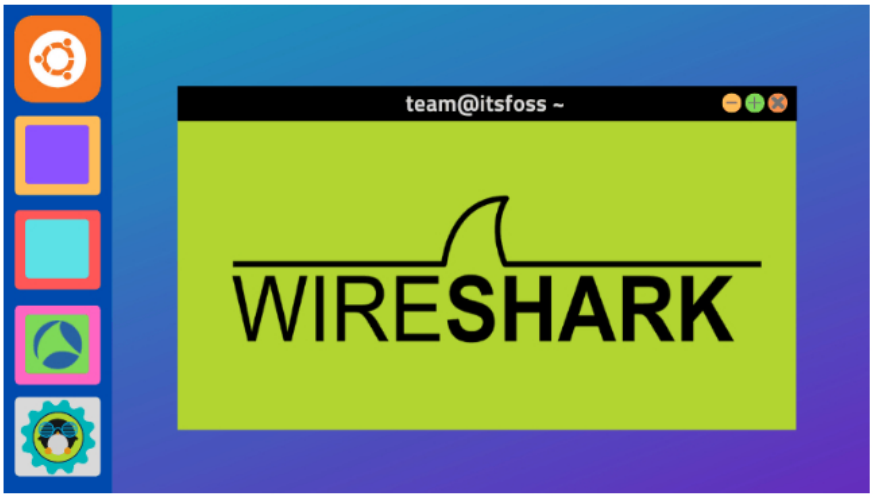

Using Emojis on Ubuntu Linux
10 Jan 2023

Become a Better Linux User

With the FOSS Weekly Newsletter, you learn useful Linux tips, discover applications, explore new distros and stay updated with the latest from Linux world

Your email address

Subscribe



Wireshark is available on all major Linux distributions. You should check out the official installation instructions. because in this tutorial, I'll focus on installing the latest Wireshark version on Ubuntu-based distributions only.

Wireshark is available in the Universe repository of Ubuntu. You can enable universe repository and then install it like this:

```
sudo add-apt-repository universe
sudo apt install wireshark
```

One slight problem in this approach is that you might not always get the latest version of Wireshark.

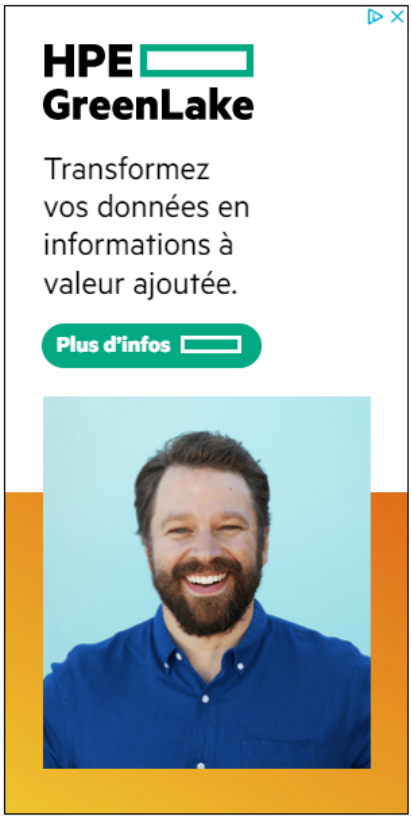
For example, in Ubuntu 18.04, if you use the apt command to check the available version of Wireshark, it is 2.6.

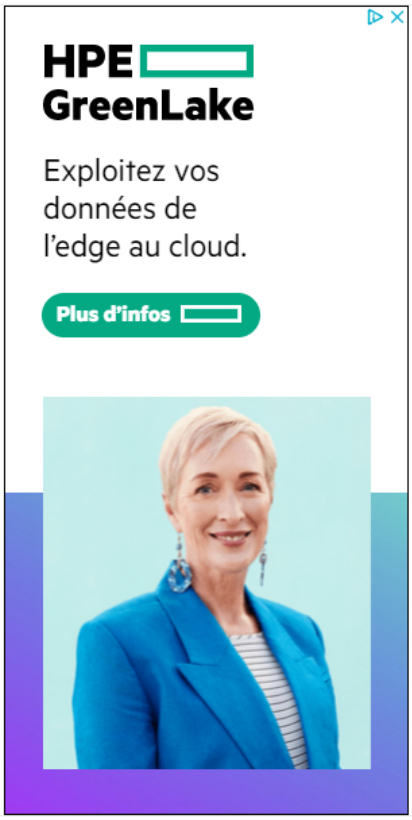
```
abhishek@nuc:~$ apt show wireshark
Package: wireshark
Version: 2.6.10-1~ubuntu18.04.0
Priority: optional
Section: universe/net
Origin: Ubuntu
Maintainer: Balint Reczey <rbalint@ubuntu.com>
```

However, Wireshark 3.2 stable version has been released months ago. New release brings new features, of course.

So, what do you do in such case? Thankfully, Wiresshark developers provide an official PPA that you can use to install the latest stable version of Wireshark on Ubuntu and other Ubuntu-based distributions.

I hope you are acquainted with PPA. If not, please read our excellent guide on PPA to





understand it completely.

Open a terminal and use the following commands one by one:

```
sudo add-apt-repository ppa:wireshark-dev/stable
sudo apt update
sudo apt install wireshark
```

Even if you have an older version of Wireshark installed, it will be updated to the newer version.

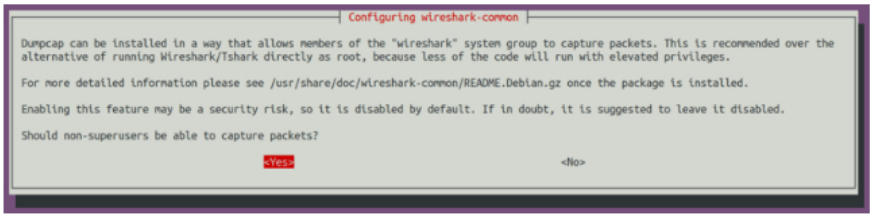
While installing, you will be asked whether to allow non-superusers to capture packets. Select Yes to allow and No to restrict non-superusers to capture packets & finish the installation.

Running Wireshark without sudo

If you have selected **No** in the previous installation, then run the following command as root:

```
sudo dpkg-reconfigure wireshark-common
```

And select **Yes** by pressing the tab key and then using enter key:



Since you have allowed the non-superuser to capture packets, you have to add the user to wireshark group. Use the usermod command to add yourself to the wireshark group.

```
sudo usermod -aG wireshark $(whoami)
```

Finally, restart your Ubuntu system to make the necessary changes to your system.

Trivia

First released in 1998, Wireshark was initially known as Ethereal. Developers had to change its name to Wireshark in 2006 due to trademark issues.

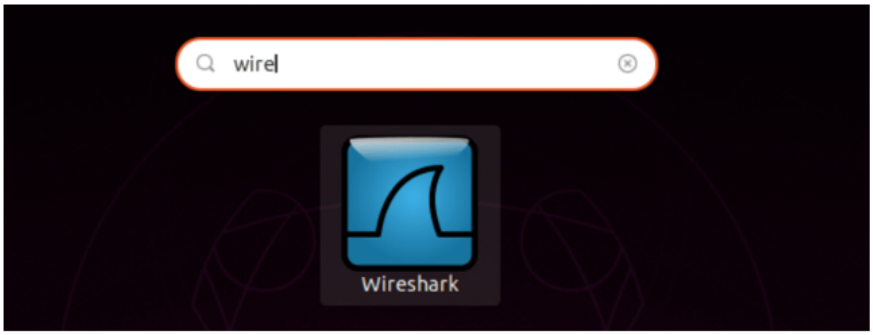
Starting Wireshark

Launching Wireshark application can be done from the application launcher or the CLI.

To start from CLI, just type **wireshark** on your console:

```
wireshark
```

From **GUI**, search for Wireshark application on the search bar and hit enter.

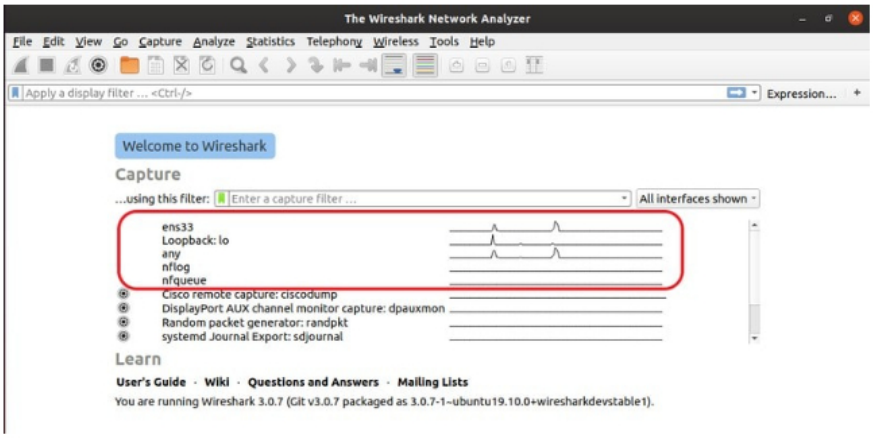


Now let's play with Wireshark.

Capturing packets using Wireshark

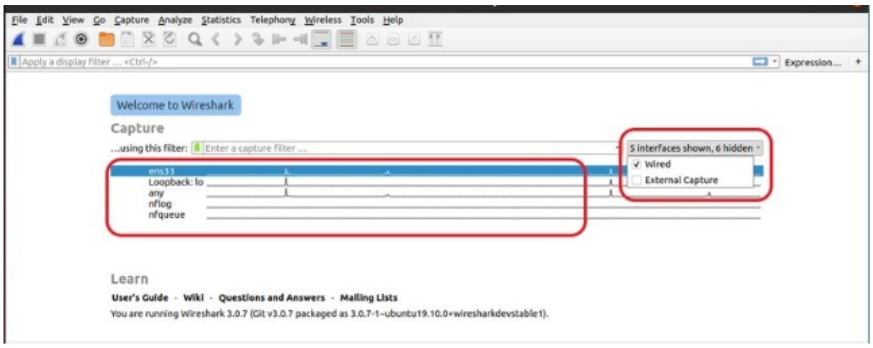
When you start Wireshark, you will see a list of interfaces that you can use to capture packets to and from.

There are many types of interfaces available which you can monitor using Wireshark such as, Wired, External devices, etc. According to your preference, you can choose to show specific types of interfaces in the welcome screen from the marked area in the given image below.

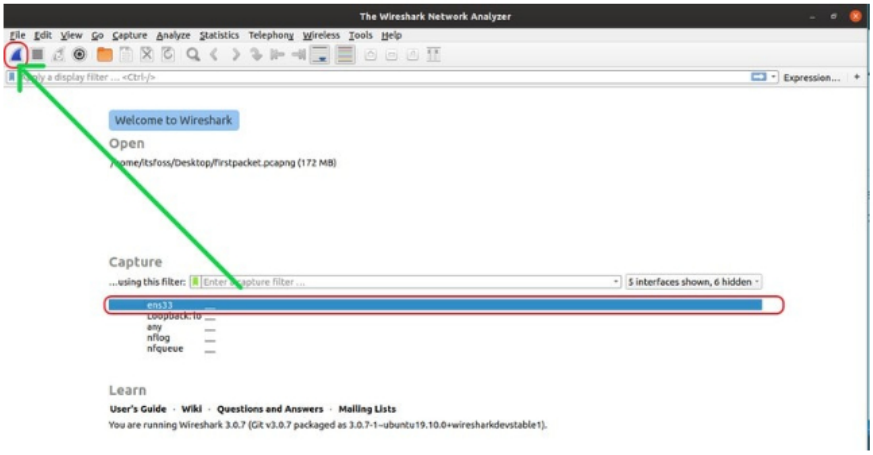


Select interface

For instance, I listed only the **Wired** network interfaces.

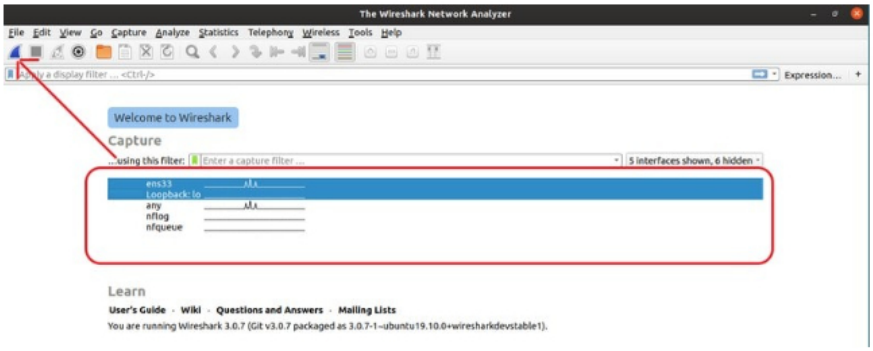


Next, to start capturing packets, you have to select the interface (which in my case is ens33) and click on the **Start capturing packets** icon as marked in the image below.

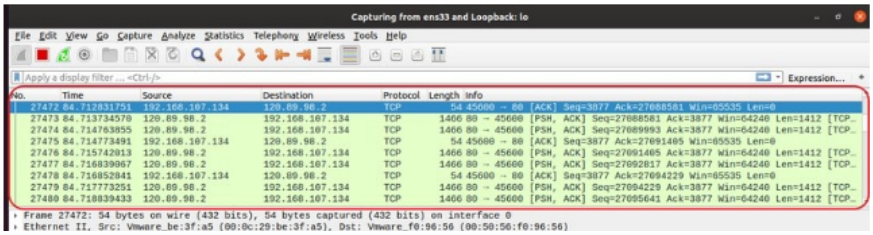


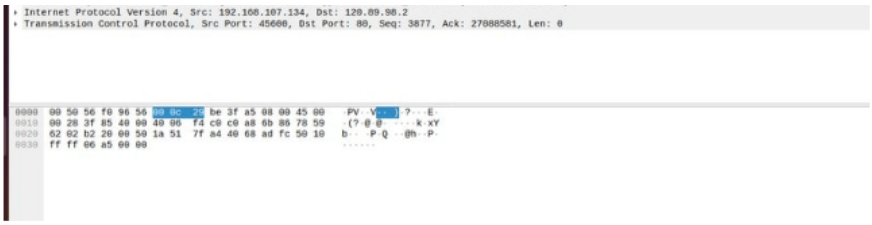
Start capturing packets with Wireshark

You can also capture packets to and from multiple interfaces at the same time. Just press and hold the **CTRL** button while clicking on the interfaces that you want to capture to and from and then hit the **Start capturing packets** icon as marked in the image below.



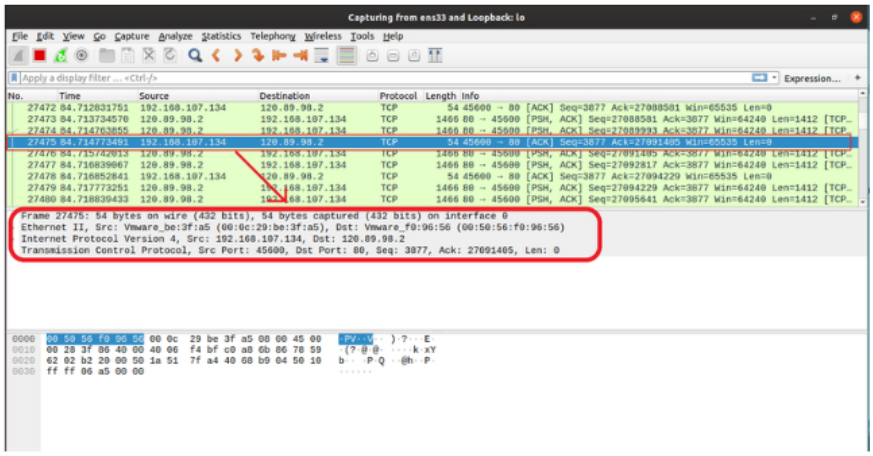
Next, I tried using **ping google.com** command in the terminal and as you can see, many packets were captured.





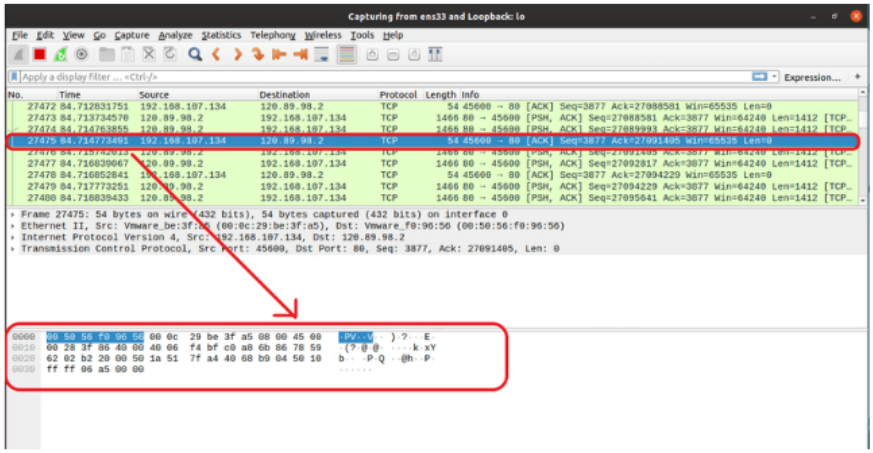
Captured packets

Now you can select on any packet to check that particular packet. After clicking on a particular packet you can see the information about different layers of TCP/IP Protocol associated with it.

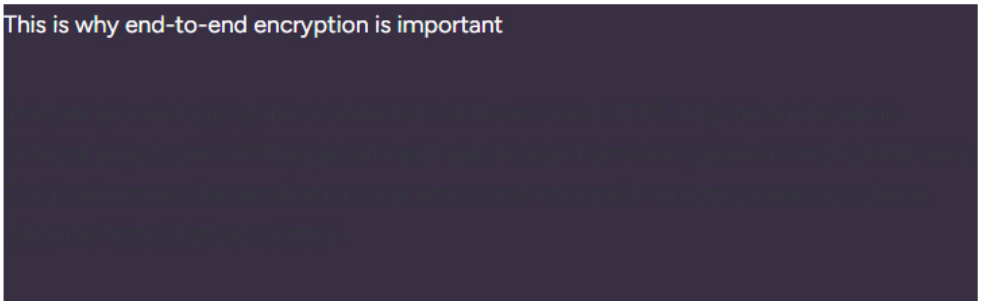


Packet info

You can also see the RAW data of that particular packet at the bottom as shown in the image below.

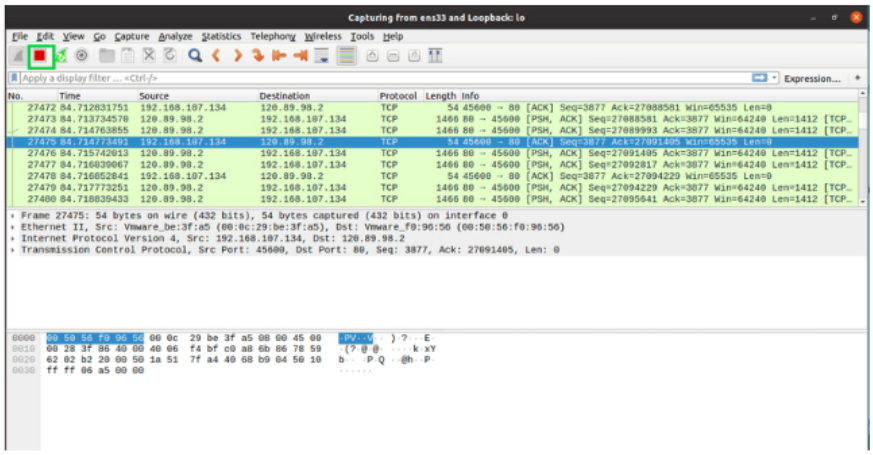


Check RAW data in the captured packets



Stopping packet capture in Wireshark

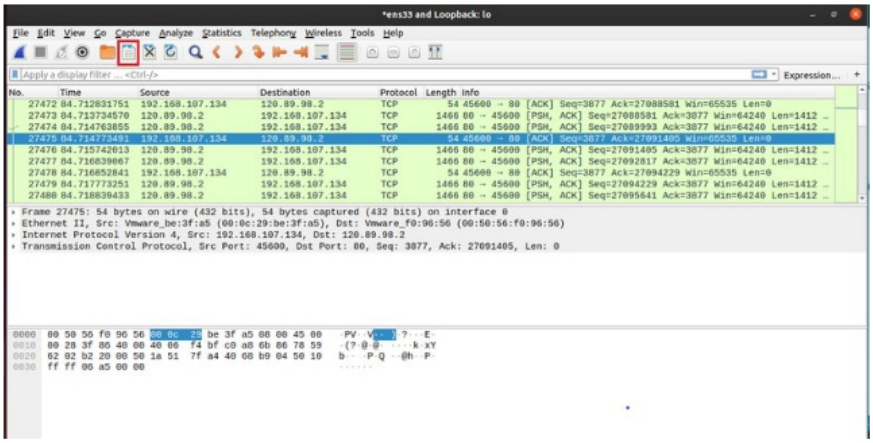
You can click on the red icon as marked in the given image to stop capturing Wireshark packets.



Stop packet capture in Wireshark

Save captured packets to a file

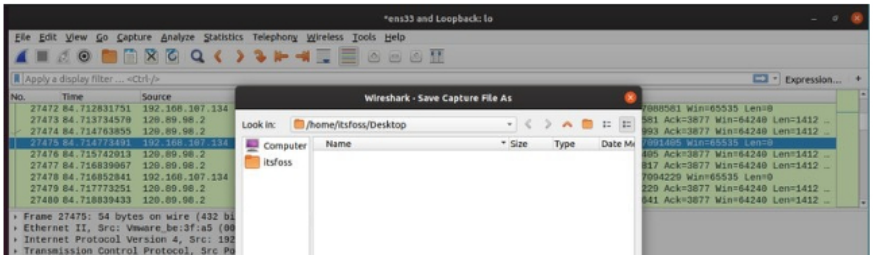
You can click on the marked icon in the image below to save captured packets to a file for future use.

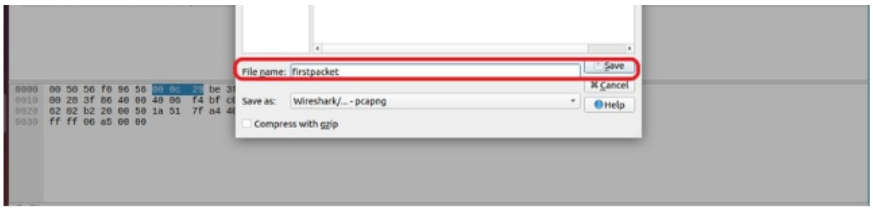


Save captured packets by Wireshark

Note: *Output can be exported to XML, PostScript®, CSV, or plain text.*

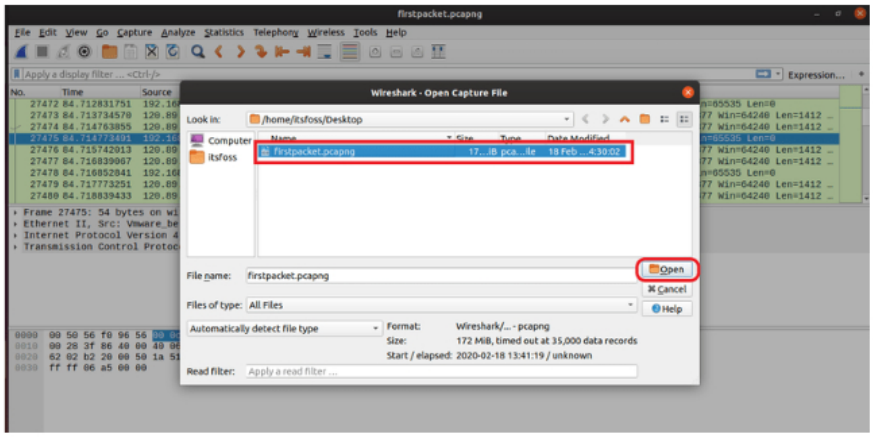
Next, select a destination folder, and type the file name and click on **Save**.
Then select the file and click on **Open**.





Now you can open and analyze the saved packets anytime. To open the file, press **\ + o** or go to **File > Open** from Wireshark.

The captured packets should be loaded from the file.



Conclusion

Wireshark supports many different communication protocols. There are many options and features that provide you the power to capture and analyze the network packets in a unique way. You can learn more about Wireshark from their official documentation.

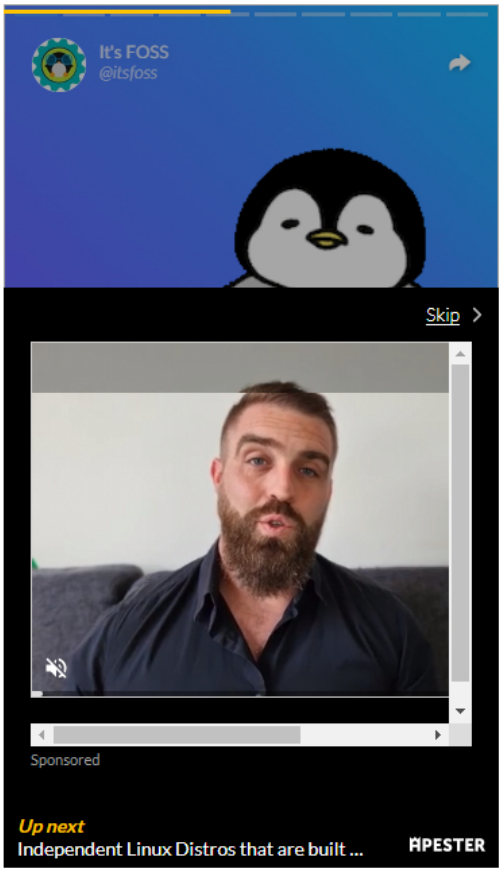
I hope this detailed helped you to install Wireshark on Ubuntu. Please let me know your questions and suggestions.

Kushal Rai

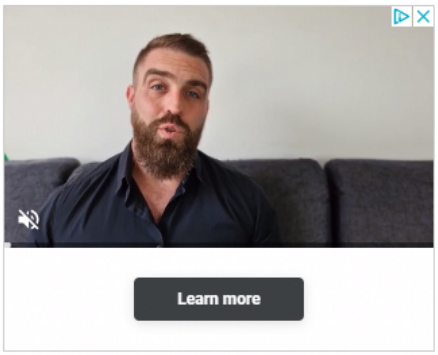
A computer science student & Linux and open source lover. He likes sharing knowledge for he believes technology shapes the perception of modern world. Kushal also loves music and photography.

Sponsored

Sponsored

Sponsored

Sponsored

What's your reaction?

0 0 0 0 0 0

8 Comments 10 ONLINE

Sort By Best

Write your comment... LOGIN SIGNUP

log10 8 months ago
cool

Reply Share 0 0

H **Hans Jansen** 2 years ago
By the way, the above result is when I run as root. Otherwise, the reason is stated as "insufficient privileges"...
Reply Share 0 0

H **Hans Jansen** 2 years ago
Whatever I try, I cannot get it to start capturing. The message is: The capture session could not be initiated on interface 'usbmon1' (Can't open USB bus file /sys/kernel/debug/usbmon/1t: No such file or directory). I am running on XUbuntu 18.04, with all necessary privileges; I even tried running as root (sudo), but with the same result. What can I do ?
Reply Share 0 0

 **Abhishek Prakash** 2 years ago
Are you trying to capture USB traffic? It seems there is more efforts for that: https://wiki.wireshark.org/CaptureSetup/USB
Reply Share 0 0

H **Hans Jansen** 2 years ago
Yes, that is what I want to do. The link you provided has helped me a lot; I can now see what is happening. Hans. Thanks a lot!
Reply Share 0 0

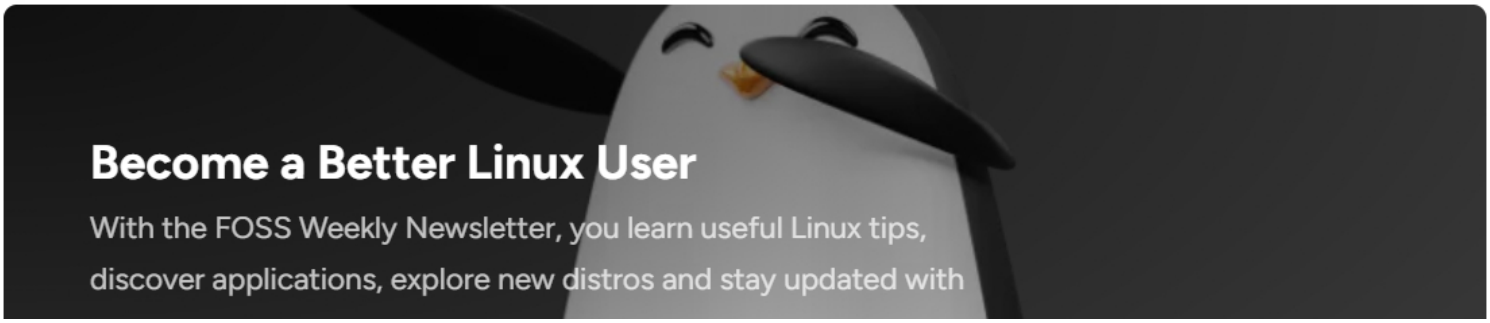
 **Abhishek Prakash** 2 years ago
Happy to help :)
Reply Share 0 0

D **DoorsXP** 2 years ago
This is rather scary.
Reply Share 0 0

s **sacioz** 2 years ago
Lovely , many thanx , will make good use of it...)))
Reply Share 0 0

by Hyvor Talk

Tweet Share Share Email Copy



IT'S FOSS

Making You a Better Linux User

Your email address Subscribe

Navigation

- Home
- About
- News
- Linux Server Side
- Community Forum
- It's FOSS en Español
- Privacy Policy

Resources

- Alternatives
- Distro Resources
- Software Recommendation

Social

- Facebook
- Twitter
- RSS
- Instagram
- Telegram
- Youtube

Buy From the Industry Leader
CrowdStrike is the proven leader in major 3rd party tests including Ransomware Protection CrowdStrike®
Learn More