How to install Wireshark

Asked 9 years, 4 months ago   Modified 1 year, 6 months ago   Viewed 407k times

90

I am new to Linux and have a need to install Wireshark 2.0.0 on VirtualBox's Xubuntu 14.04. I have already downloaded .tar.gz package and extracted it. Then I opened terminal in the `wireshark` folder and type `/.configure` with intention to follow it by make and `sudo make install` executions but the attempt as unsuccessful as `sudo apt-get install wireshark`. Could somebody help me how to install Wireshark step by step, please?

wireshark

Share Improve this question Follow

edited Nov 21, 2015 at 10:00
muru
206k 56 512 765

asked Nov 21, 2015 at 9:50
Stanislav Jirák
1,001 1 7 4

7 What went wrong with `sudo apt-get install wireshark`? – muru Nov 21, 2015 at 10:01

dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem. – Stanislav Jirák Nov 21, 2015 at 10:23

@StanislavJirák `cat /etc/sources` – Gayan Weerakutti Nov 21, 2015 at 10:52

cat: /etc/sources: No such file or directory – Stanislav Jirák Nov 21, 2015 at 12:31

@reversiblean `cat /etc/apt/sources.list` – Neil Nov 22, 2015 at 0:03

7 Answers

Sorted by: Highest score (default)

114

1. Add the stable official PPA. To do this, go to terminal by pressing Ctrl + Alt + T and run:

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

2. Update the repository:

   ```
   sudo apt-get update
   ```

3. Install wireshark 2.0:

   ```
   sudo apt-get install wireshark
   ```

4. Run wireshark:

```
sudo wireshark
```

If you get an error `couldn't run /usr/bin/dumpcap in child process: Permission Denied`, go to the terminal again and run:

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

Say `YES` to the message box. This adds a wireshark group. Then add user to the group by typing

```
sudo adduser $USER wireshark
```

Then restart your machine and open Wireshark. It works. Good Luck.

Share Improve this answer Follow

edited Aug 1, 2023 at 1:15
Gabriel Staples
11k 12 96 141

answered May 27, 2016 at 9:52
Thusitha Sumanadasa
1,658 1 13 14

This seems to work, I see `Setting up wireshark (2.4.4-1~16.04.0)`. But when I open it and do Help > About I see version 2.2.6 and it behaves quite differently from the one I have on Windows. For example, it mostly displays "unknown protocol". Am I missing something to get the latest version? – Nagev Apr 17, 2018 at 8:38

1 If you don't want to restart your machine for now, you can do `newgrp wireshark` temporarily. – Abhishek Kashyap Nov 5, 2018 at 9:26

3 This is outdated. – Goddard May 31, 2019 at 17:05

1 Upvoted. I've added some more troubleshooting info and details in my new answer here. Tested on Ubuntu 22.04.2. – Gabriel Staples Aug 1, 2023 at 1:13

9

Open terminal and type the commands:

1. `sudo apt-get install wireshark`
2. `sudo dpkg-reconfigure wireshark-common`
3. `sudo adduser $USER wireshark`
4. `wireshark`

If you getting `wireshark` running error, so close it and then just do the following:

5. Go to `usr/share/wireshark`
6. Open `init.lua` with a text editor
7. Change `disable_lua = false` to `disable_lua = true`

Share Improve this answer Follow

edited Sep 8, 2019 at 12:07
Simon Sudler
4,071 3 22 34

answered Jul 30, 2018 at 14:50
cybermizz
97 2 4

Where's the evidence to support the LUA changing bits? This tends to work out of the box, and you don't really have to go altering installed package bits typically to get this to work. – Thomas Ward ♦ Jul 30, 2018 at 20:20

8

For those on ubuntu 18.04, go to terminal and run:

```
sudo apt install wireshark
```

It will install wireshark (in my case v2.6.8) and you will be asked to add dumpcap in wireshark user group so you don't need to be root to execute it.

If you say:

NO > you're good to go, but you gonna need root privileges to run it.

YES > after installation finishes you should add yourself to wireshark user group:

```
sudo usermod -a -G wireshark YOUR_USERNAME
```

That's ALL!

Share Improve this answer Follow

answered Aug 2, 2019 at 16:53

Reginaldo Santos
261 4 9

5

I'd like a more thorough and modern answer. Many of the other answers here contain parts of my answer, and I've upvoted them, but none contain everything I'm going to show.

How to install the latest PPA-managed version of Wireshark on Ubuntu

Tested on Ubuntu 22.04.2.

Quick summary

1. Install Wireshark and add your user to the `wireshark` group:

```
# Add the latest managed package so you can get a newer version
sudo add-apt-repository ppa:wireshark-dev/stable

sudo apt update
sudo apt install wireshark

# When it says, "Should non-superusers be able to capture packets?",
# choose **Yes**.
# Add your user to the `wireshark` group. Run this command exactly as-is.
sudo usermod -a -G wireshark "$USER"

# Ensure your username is now part of the `wireshark` group. You should see
# that as an entry now in the response here.
groups "$USER"
```

Now log out of Ubuntu (or restart your computer), and log back in, to register your username in this new group.

2. Open Wireshark:

   Press the Windows (Super) key and type in "Wireshark". Click it to open it.

3. Capture some packets:

   In the window that opens up, click the blue shark fin icon in the top-left, which says "Start capturing packets" when you hover on it. This will start capturing packets. Press the red square (stop symbol) in the top-left to stop the packet capture. It will ask if you'd like to save your packet capture (pcap) file.

4. (Optional) Add Wireshark to your Ubuntu favorites bar:

   Press the Windows (Super) key and type in "Wireshark". Right-click it and go to "Add To Favorites". It will now show up permanently as an icon in your left-hand launcher bar. Click it to open it.

5. Done!

   If it works now, you're done! If not, check out my details below to see if you missed something.

   Again, since your username is part of the `wireshark` group, you can capture packets *without* running `sudo wireshark` to run it as root.

More details and notes

1. Getting the latest PPA version:

   If you run `sudo apt install wireshark` *without* first adding the latest PPA via `sudo add-apt-repository ppa:wireshark-dev/stable`, you'll get an older version of Wireshark. On Ubuntu 22.04.2, for instance, I can see from `sudo apt -s install wireshark` (a simulated install) that I would get only version `3.6.2-2`. However, if I add the PPA first and then run `sudo apt -s install wireshark`, I can see that I'd get version `4.0.6-1`, which is *nearly the newest*. At the time of these instructions, https://www.wireshark.org/ shows the latest stable relase downloadable for other OSs, such as Windows or Mac, as being `4.0.7`.

   For more info. on the `-s` option passed to `apt`, see my comment here (and the answer above it):

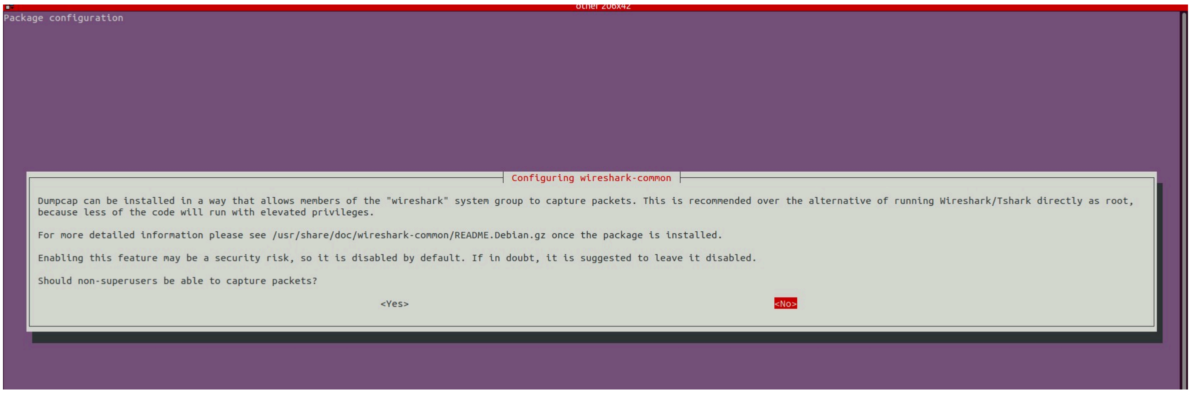
   > Upvoted. For anyone looking for a really concrete example, on Ubuntu 22.04, if you run `sudo apt -s install wireshark`, you'll see it will install version `3.6.2-2`. If you install the Wireshark PPA with `sudo add-apt-repository ppa:wireshark-dev/stable` first, however, and then run `sudo apt -s install wireshark`, you'll

see it will install version `4.0.6-1`. In this way you can clearly see that the PPA will help you get a much newer version.

2. The installation menu:

   When installing, you'll see this menu. Again, choose "Yes":

```
┌
Configuring wireshark-common
│

│ Dumpcap can be installed in a way that allows members of the "wireshark"
system group to capture packets. This is recommended over the alternative of
running Wireshark/Tshark directly as root,    │
│ because less of the code will run with elevated privileges.
│

│ For more detailed information please see /usr/share/doc/wireshark-
common/README.Debian.gz once the package is installed.
│

│ Enabling this feature may be a security risk, so it is disabled by default. If
in doubt, it is suggested to leave it disabled.
│

│ Should non-superusers be able to capture packets?
│

│                                                        <Yes>
<No>                                                       │
│
└
```



```
Package configuration

                         ┤ Configuring wireshark-common ├
 Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture packets. This is recommended over the alternative of running Wireshark/Tshark directly as root,
 because less of the code will run with elevated privileges.

 For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.gz once the package is installed.

 Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is suggested to leave it disabled.

 Should non-superusers be able to capture packets?

                                <Yes>                                    <No>
```

3. What if you chose "No" in the menu above, during installation?

   Not a problem, you have two ways to fix it:

   1. [brute-force] Close Wireshark, and then run it as root:

      ```
      sudo wireshark
      ```

   2. [recommended] Close Wireshark, and then reconfigure it to choose "Yes".

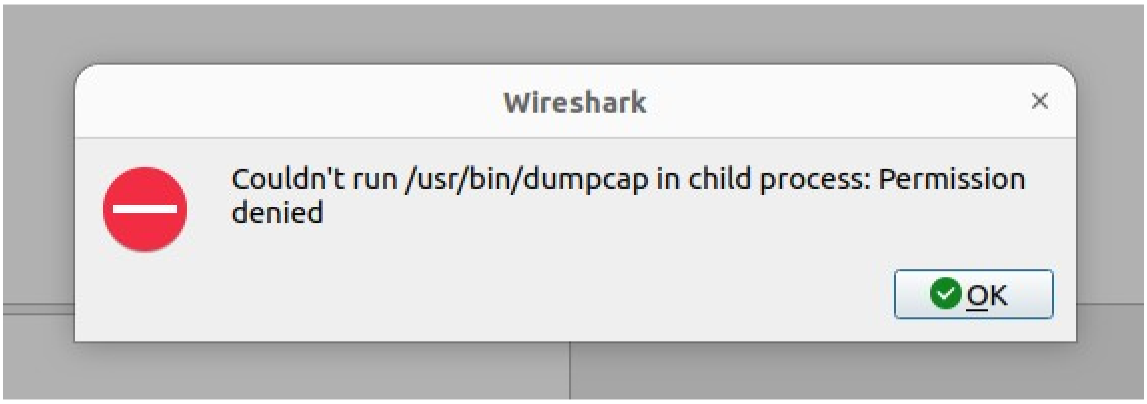
```
# run this, and be sure to choose "Yes" this time
sudo dpkg-reconfigure wireshark-common
```

Source where I learned this: from the `README.Debian` file contained on my local system here: `/usr/share/doc/wireshark-common/README.Debian.gz`. This path is mentioned in the menu above. You can see it online in the Wireshark repository here: https://github.com/wireshark/wireshark/blob/master/packaging/debian/README.Debian:

> The installation method can be changed any time by running:
>
> ```
> sudo dpkg-reconfigure wireshark-common
> ```
>
> The question mentioned above will be asked; answer "" to it.

4. Potential errors when trying to capture packets:

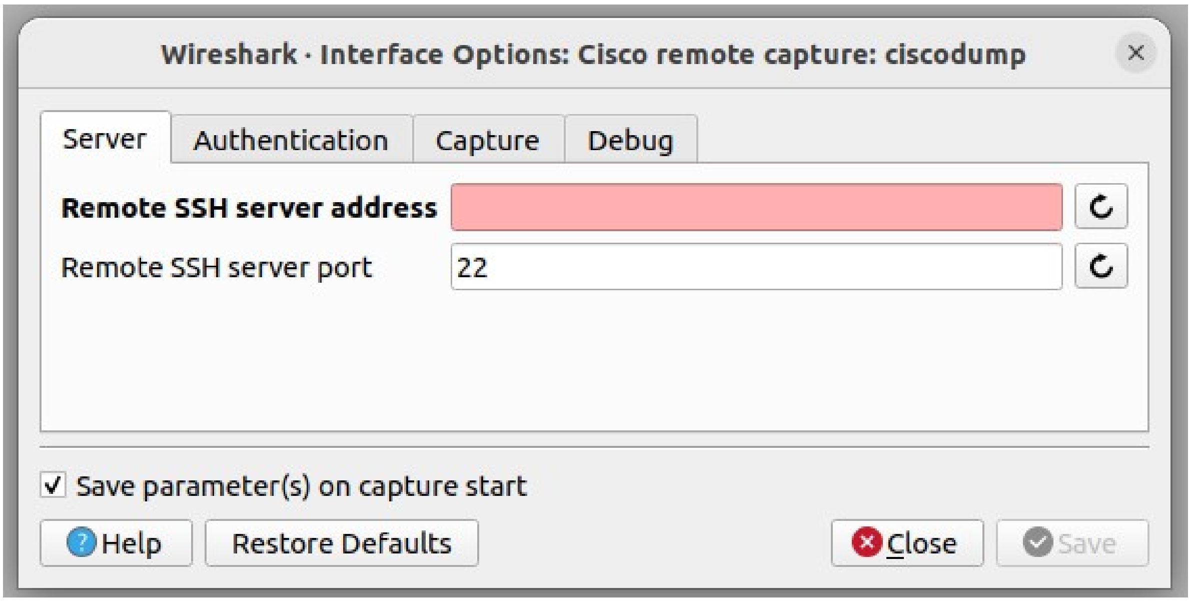
> Couldn't run `/usr/bin/dumpcap` in child process: Permission denied



Wireshark

Couldn't run /usr/bin/dumpcap in child process: Permission denied

Or:



Wireshark · Interface Options: Cisco remote capture: ciscodump

Remote SSH server address

Remote SSH server port: 22

☑ Save parameter(s) on capture start

Solution:

Either of those things above means that you need root permissions to capture packets. You can do this:

1. [brute-force run it as root] Close Wireshark, and then run it as root:

   ```
   sudo wireshark
   ```

2. OR: [recommended] Close Wireshark, and then configure it to not require root:

   ```
   # 1. run this, and be sure to choose "Yes" this time
   sudo dpkg-reconfigure wireshark-common

   # 2. Add your username to the `wireshark` group:
   sudo usermod -a -G wireshark "$USER"
   ```

   Now log out of Ubuntu (or restart your computer), and log back in, to register your username in this new group.

Now for how to *use* Wireshark?--I have no idea. This is my first time using it.

Share Improve this answer Follow

edited Sep 6, 2023 at 18:53

answered Aug 1, 2023 at 1:10

Gabriel Staples

11k 12 96 141

1 Best answer for now! It's strange but for me on Ubuntu 20.04 to apply `sudo usermod -a -G wireshark "$USER"` reboot was required to properly update groups for current user. Only logging out and logging in does not help. – Anton Samokat May 24, 2024 at 11:01

4

To do this, go to terminal by pressing Ctrl + Alt + T and run:

```
sudo apt install wireshark
```

Apt should take care of all of the dependency issues for you.

Use the following command to install downloaded Wireshark debs:

```
dpkg -i wireshark-common_2.0.5.0-1_i386.deb wireshark_wireshark-2.0.5.0-1_i386.deb
```

`dpkg` doesn't take care of all dependencies, but reports what's missing. You can usually resolve problems by then running

```
sudo apt install -f
```

Share Improve this answer Follow

edited Feb 10, 2019 at 20:54

Zanna ♦

72k 60 223 330

answered Feb 5, 2019 at 7:53

Muhammad Bahroz Ahmad

41 1

3

To add to Thusitha's answer, in Step 4 you either run as sudo or if you do not want to run all processes as root, then you set the message box to 'YES' (to install dumpcap in such a way that it allows users of the wireshark group to run it without sudo) and add user to wireshark group. (be sure to log out and log in before running wireshark so that the group privileges are reloaded). You can then just run wireshark without root.

Share Improve this answer Follow

edited Aug 2, 2017 at 8:06
Pierre.Vriens
1,137 37 16 21

answered Aug 2, 2017 at 6:33
pooya13
131 2

0

1. Type `sudo apt update` The APT package repository cache should be updated.
2. Now, Run the following command to install Wireshark on your Ubuntu machine: `sudo apt install wireshark`

By default, Wireshark must be started as root (can also be done with sudo) privileges in order to work. If you want to run Wireshark without root privileges or without sudo, then select and press .

3. Wireshark should be installed.

Share Improve this answer Follow

answered Aug 2, 2019 at 17:41
ANCHOVY
1