How to Install Wireshark on Debian 11

Wireshark is a free and open source packet analyzer. It allows users to check data from the network directly or from the capture file on the drive.

Wireshark can be used as a simple network troubleshooting tool, as well as for security analysis and software development.

Installing Wireshark on Debian 11 is easy. Follow this step-by-step guide to install Wireshark on Debian 11.

Condition

To follow this guide to install Wireshark on Debian 11, you need:

1. Connect to the Internet (to download and install packages)
2. An account with sudo privileges to install and remove packages.

Update source list

Wireshark depends on a number of open source libraries. Make sure they are updated before installing the program. Debian 11 keeps all its packages up to date through regular updates, so do the update first.

```
sudo apt update -y
```

During the installation process, you will be asked to allow non-superusers to collect data from network interfaces. Select Yes to continue.

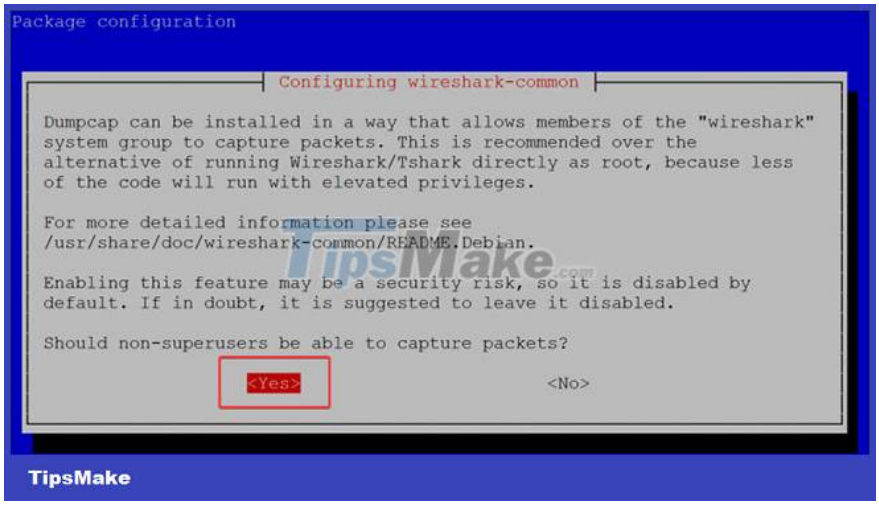
Installing Wireshark on Debian 11

Once updated, you can proceed to download and install Wireshark.

Wireshark is distributed as a .deb file. This means there is no need to download anything manually. Instead, it can only be installed through apt, like any other program on Debian 11.

```
sudo apt install wireshark -y
```

During the installation process, you will be asked to allow non-superusers to collect data from network interfaces. Select Yes to continue.



Check out Wireshark

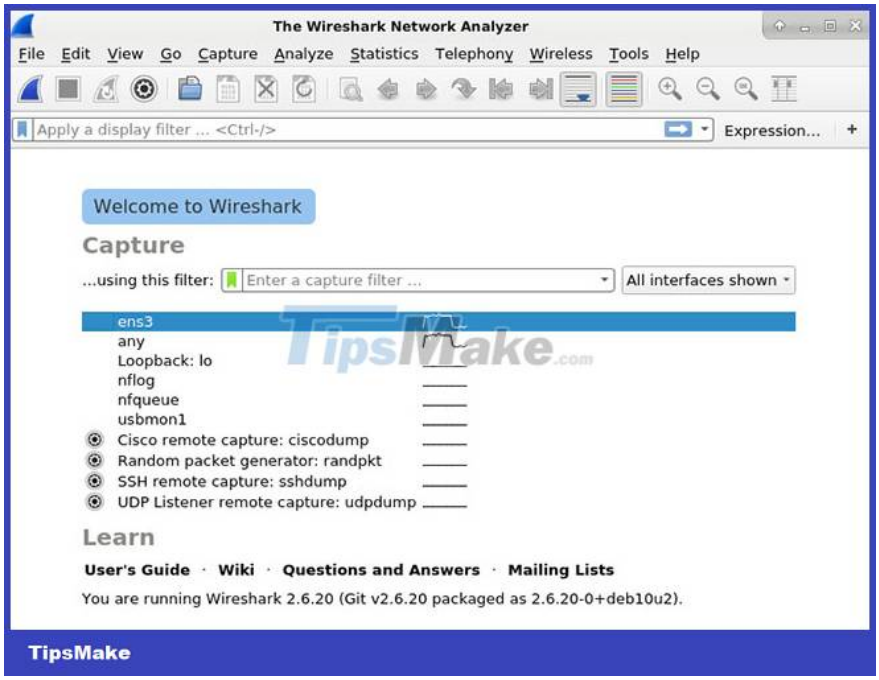
Now, after installing Wireshark, let's quickly experiment.

First, start the program by typing sudo wireshark. This will open Wireshark in its own window.

```
sudo wireshark
```

You can also open Wireshark from the desktop environment's menu system.

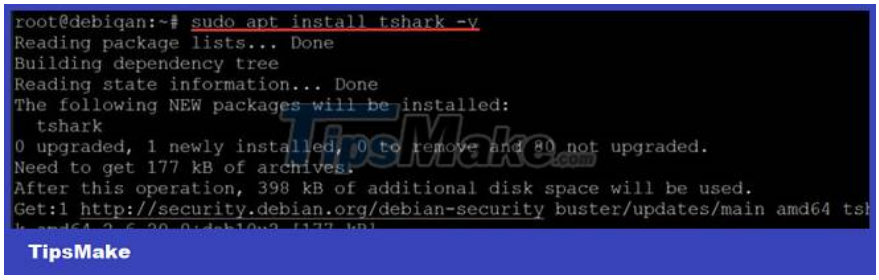
Wireshark has a graphical user interface (GUI) to capture packets, as shown below. You will see a list of available network interfaces that Wireshark understands. If you want to monitor the interface where the web browser is receiving the Internet connection (e.g. wlan0), select the interface and click the Start button.



However, you can also use it from the terminal by typing tshark followed by the command to capture some traffic. Tshark is a command line program for monitoring network traffic. Along with TShark, it is part of the Wireshark suite. Just like the GUI equivalent, it can capture packages and then display descriptions in a terminal window or save them to a file in binary format.

You can install tshark by entering the following command in a terminal window:

```
sudo apt install tshark -y
```



Run the tshark –help command below to see the different options tshark offers.

```
root@debiqan:~# tshark --help | head -20
Running as user "root" and group "root". This could be dangerous.
TShark (Wireshark) 2.6.20 (Git v2.6.20 packaged as 2.6.20-0+deb10u2)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: appropriate maximum)
  -p                       don't capture in promiscuous mode
  -I                       capture in monitor mode, if available
  -B <buffer size>         size of kernel buffer (def: 2MB)
  -y <link type>           link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit
  --list-time-stamp-types  print list of timestamp types for iface and exit
```

TipsMake

Run the tshark -D command below to check if the network interfaces are recognized by tshark.

```
root@debiqan:~# tshark -D
Running as user "root" and group "root". This could be dangerous.
1. ens3
2. any
3. lo (Loopback)
4. nflog
5. nfqueue
6. usbmon1
7. ciscodump (Cisco remote capture)
8. randpkt (Random packet generator)
9. sshdump (SSH remote capture)
```

TipsMake

You will get a list of network interfaces like below. Note that some network interfaces may be in the "disabled" state. Not all network interfaces are active by default. You will have to find the active interfaces. In this demo, it's interface ens3 and lo.

You can tell which interface is active by typing ifconfig in the terminal.

`ifconfig`

```
root@debiqan:~# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]134  netmask 255.255.254.0  broadcast 69.28.83.255
        inet6 [redacted]:5386  prefixlen 64  scopeid 0x20<link>
        ether 00:00:45:1c:53:86  txqueuelen 1000  (Ethernet)
        RX packets 55261  bytes 246070120 (234.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49116  bytes 73179155 (69.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 131  bytes 6925 (6.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 131  bytes 6925 (6.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

TipsMake

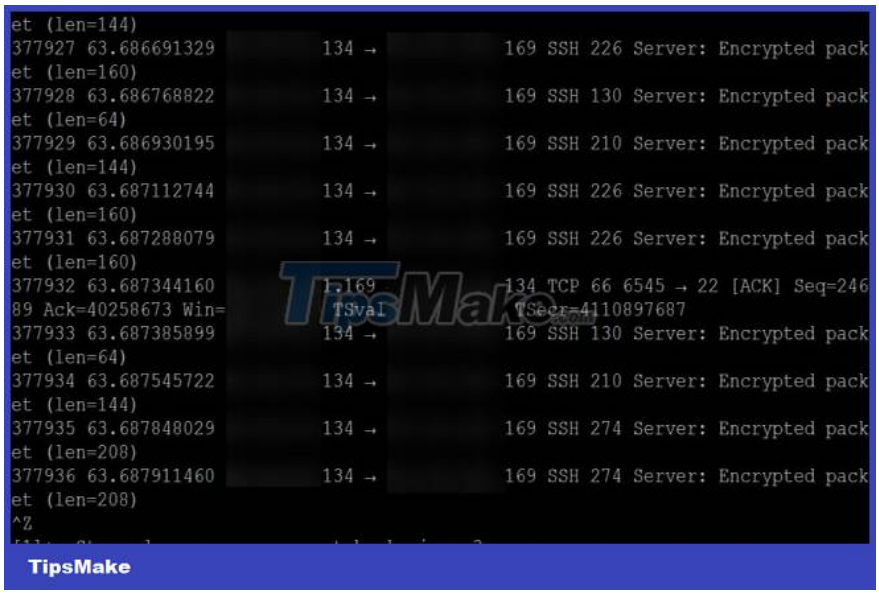
Once you have identified the desired interface, run the following command to start capturing packets:

```
tshark -i
```

Where is the name of the desired interface.

```
tshark -i ens3
```

When you are done with data collection, press Ctrl + C in the command line window. This will stop the capture and close tshark. You will see the captured data displayed in the command line window below.



You finished reading the article "**How to Install Wireshark on Debian 11**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
