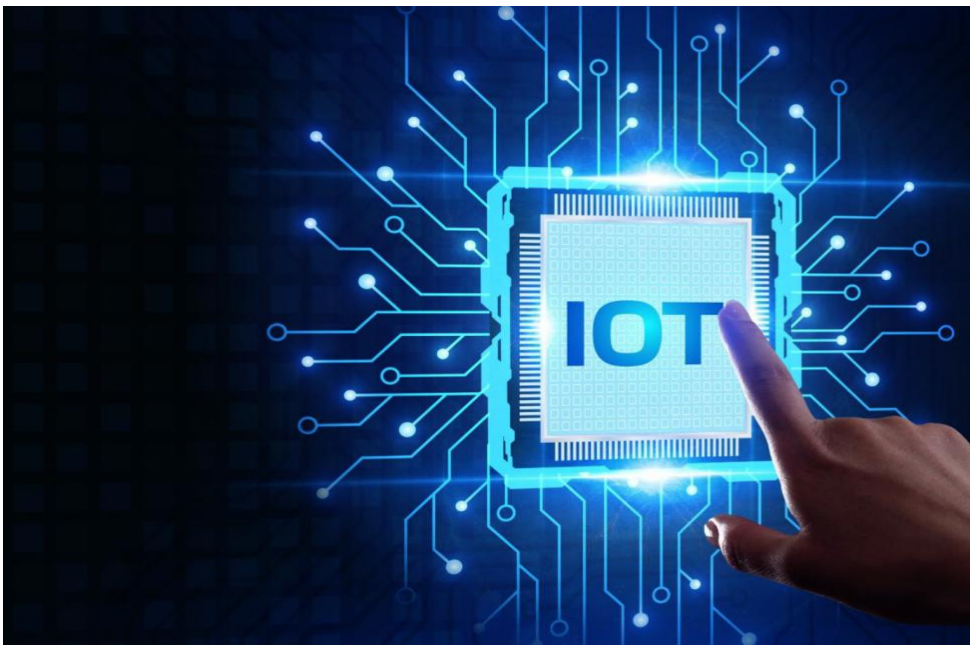
Bahan Ajar

Modul Praktikum

INTERNET of THINGS
(IoT Security)

Kode Matakuliah: SKO21431

Penyusun:
Bayu Nugroho. S.Kom., M.Eng



PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA
2023

DAFTAR ISI

Modul 5

Wireshark Installation (Linux)

UNIX, Linux, and BSD:

Wireshark runs on most UNIX and UNIX-like platforms including Linux and most BSD variants. The system requirements should be comparable to the specifications listed above for Windows. Binary packages are available for most Unices and Linux distributions including the following platforms:

1. Alpine Linux
2. Arch Linux
3. Canonical Ubuntu
4. Debian GNU/Linux
5. FreeBSD
6. Gentoo Linux
7. HP-UX
8. NetBSD
9. OpenPKG
10. Oracle Solaris
11. Red Hat Enterprise Linux / CentOS / Fedora

If a binary package is not available for your platform you can download the source and try to build it. Please report your experiences to wireshark-dev[AT]wireshark.org.

How to Install Wireshark on Debian-Based Systems

Now, let's show you how to install Wireshark on Debian-based systems. These include OS's such as Ubuntu, Kali, Mint, and others.

For our demo, we will be using Ubuntu. To install packages on Debian systems, you must use the apt package manager, designed to handle software installation, upgrade, and removal.

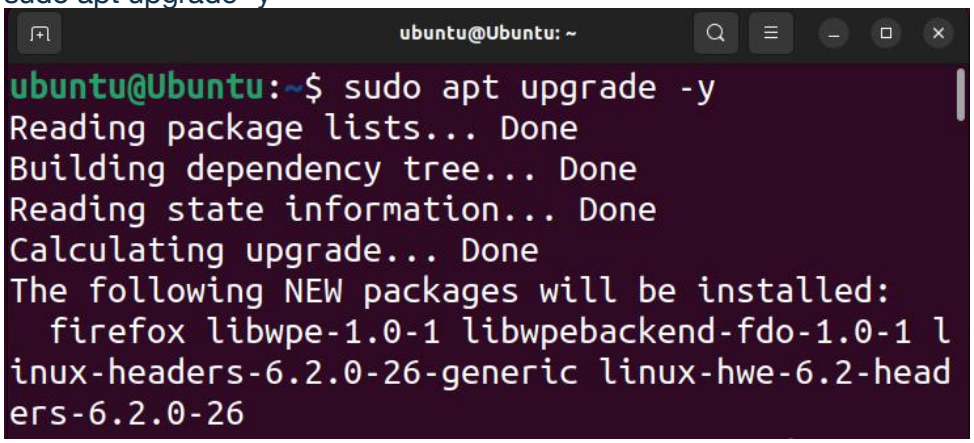
Ensure your system is up to date by using the following commands.

First, make sure your packages are up to date.

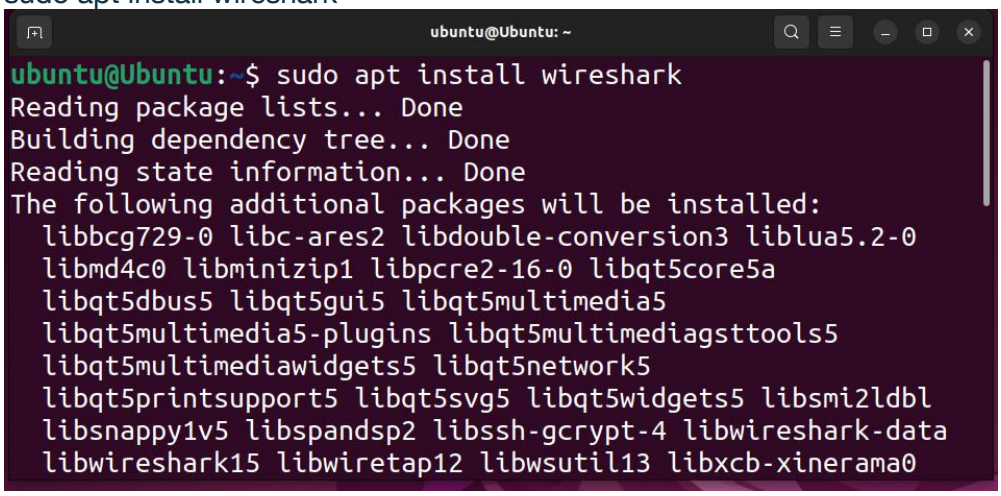
```
sudo apt update -y
```

```
ubuntu@Ubuntu:~$ sudo apt update -y
[sudo] password for ubuntu:
Get:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy/main i386 Packages [1,040 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1,395 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu jammy/main Translation-en [510 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 DEP-11 Metadata [423 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu jammy/main DEP-11 48x48 Icons [100.0 kB]
```

And then update the system with the following:
sudo apt upgrade -y



To install Wireshark, simply run the following command.
sudo apt install wireshark

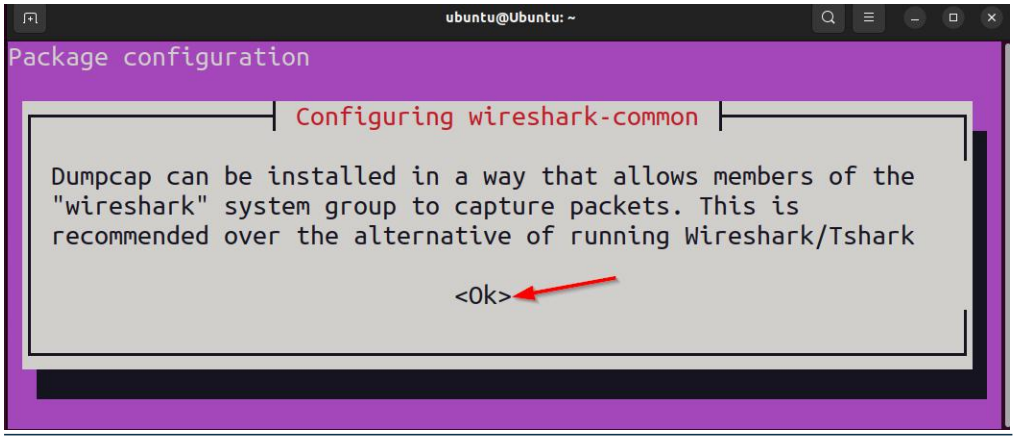


The installer will tell you how many MB will be used and if you want to continue.

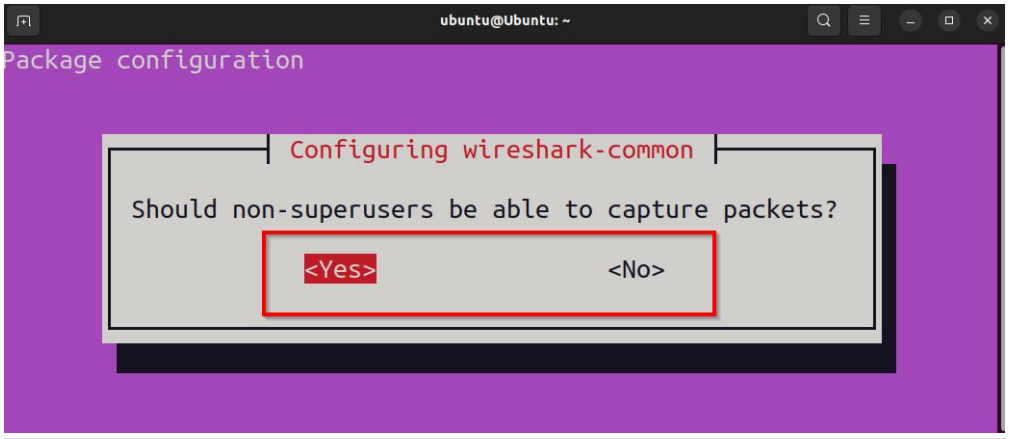
Select “Y” to continue with the installation.

You will be presented with a package configuration screen informing you about Dumpcap (a component of the Wireshark suite that does the heavy lifting when capturing packets.)

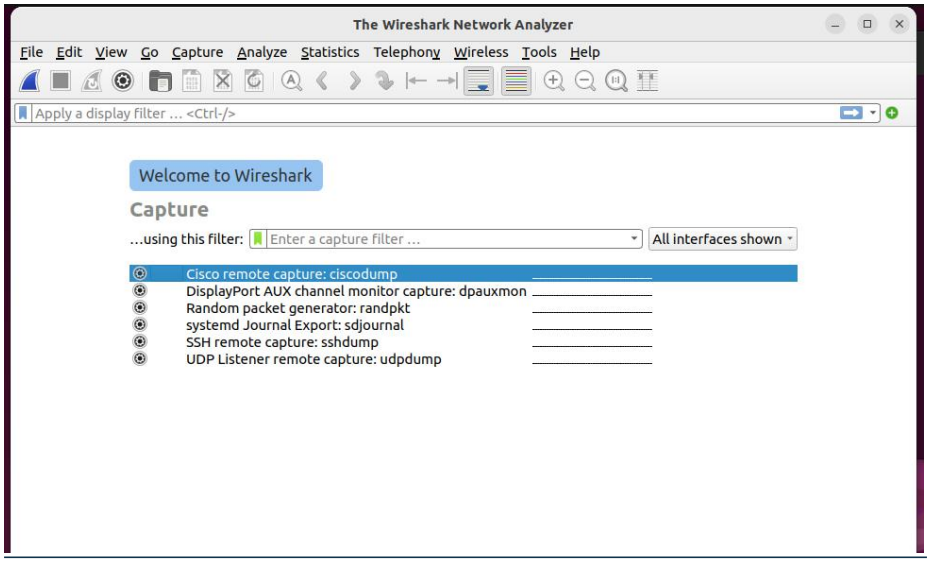
Select “Ok” to continue



The next screen will ask if non-superusers should be allowed to capture packets. This essentially asks if you want to give users without administrative or “root” privileges the ability to capture packets using Wireshark. Choose “Yes” or “No.”



Wireshark will now be installed. Enter wireshark in the command line to open Wireshark.

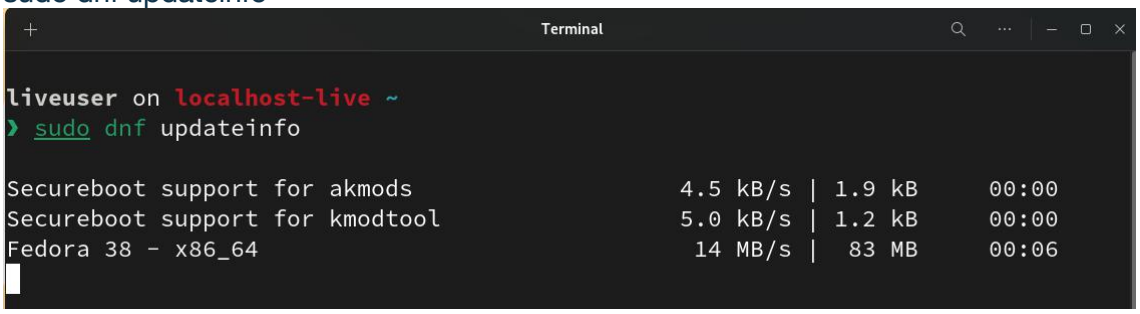


How to Install Wireshark on Fedora-Based Systems

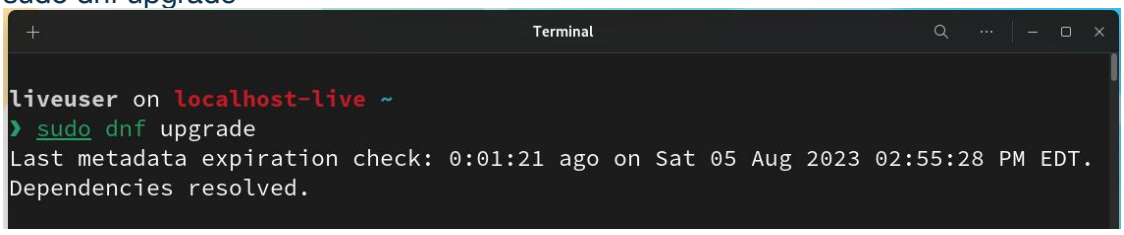
Next, we’ll show you how to install Wireshark on a Fedora-based system, including RHEL, CentOS, and others. For our demo, we are using Ultramarine.

Fedora uses the DNF (Dandified Yum) package manager as its primary tool for managing software packages. DNF replaced YUM in Fedora 22, but you may still encounter YUM if you use an older specific Red Hat-based distribution.
Before installing Wireshark, ensure your system is up to date by running the following commands.

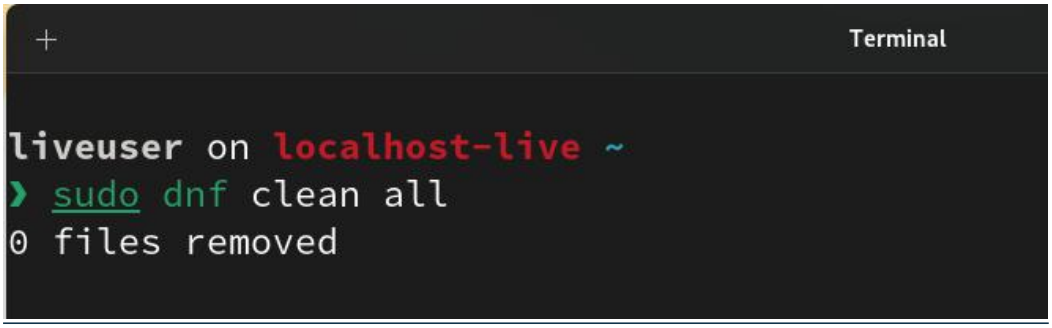
To update the DNF package repository information, use the following:
sudo dnf updateinfo



To upgrade all packages, use the following command:
sudo dnf upgrade

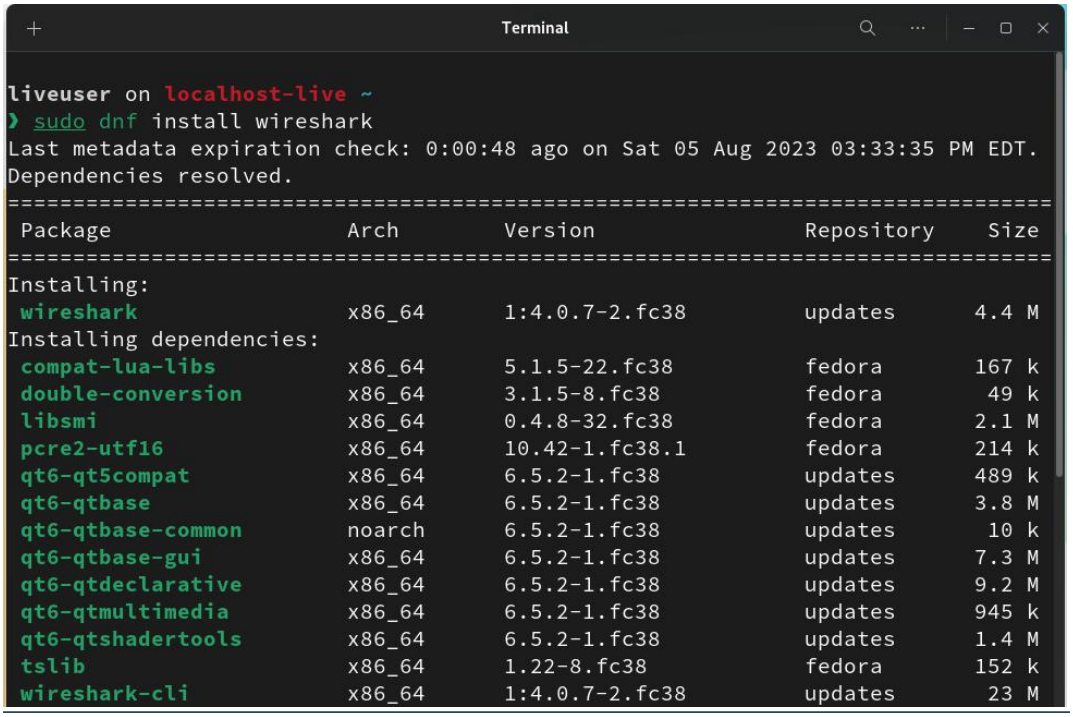


Sometimes, cleaning the cache to ensure no outdated metadata or packages are lingering around is a good idea. To do this, run the following:
sudo dnf clean all

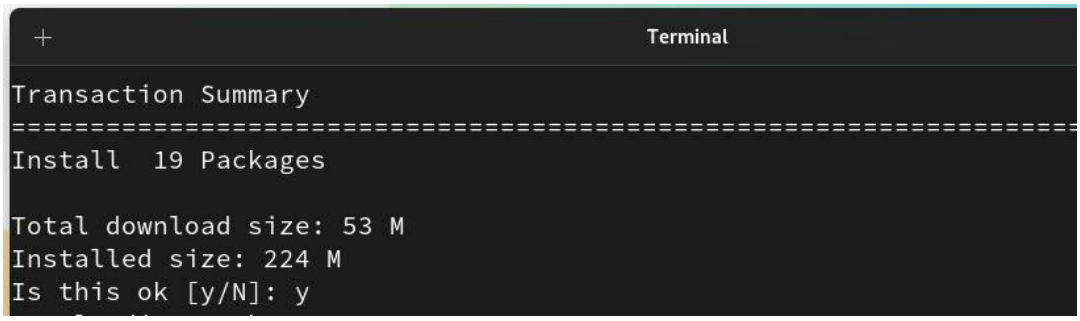


Now you're ready to install Wireshark. This can be done with the following command to install Wireshark and all the necessary dependencies.

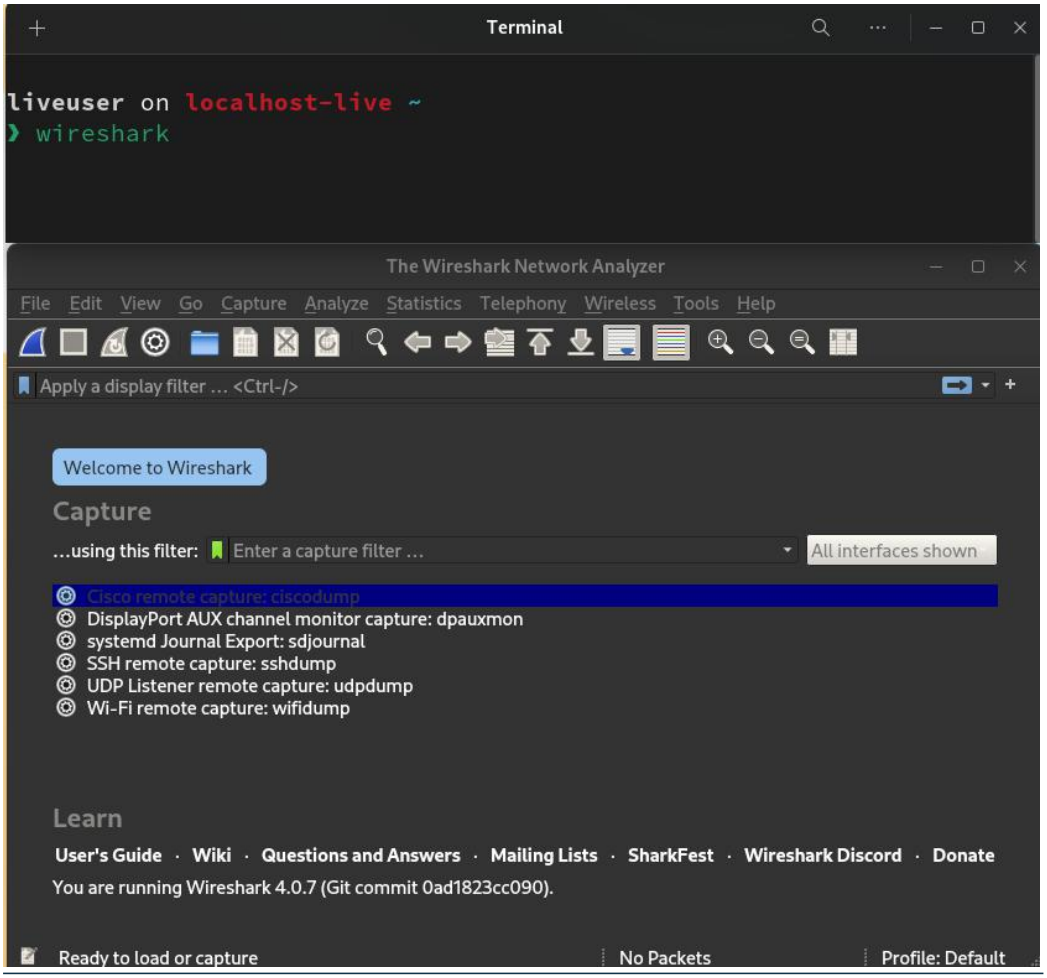
sudo dnf install wireshark



You will be asked if you want to install the packages. Simply enter “y” to continue.



To start Wireshark, simply enter wireshark in the terminal.

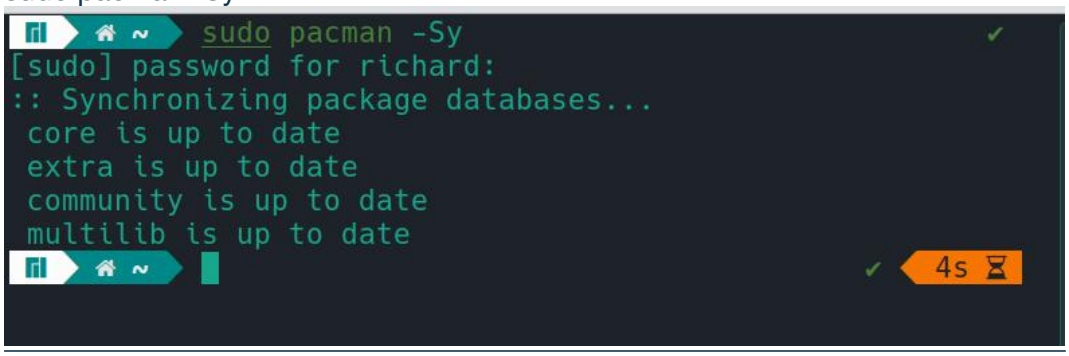


How to Install Wireshark on Arch-Based Systems

We will now show you how to install Wireshark on an Arch-based system, including Manjaro, Garuda, and EndeavourOS. For our demo, we will be using Manjaro.Arch-based systems use pacman to manage software packages. This package manager is responsible for handling installations, updates, and removals. Before we install Wireshark, let's make sure the system is updated. We must synchronize the package database and upgrade the system to do this.

To synchronize the database, use the following command.

sudo pacman -Sy



We must update all installed packages to their latest versions with the following command.

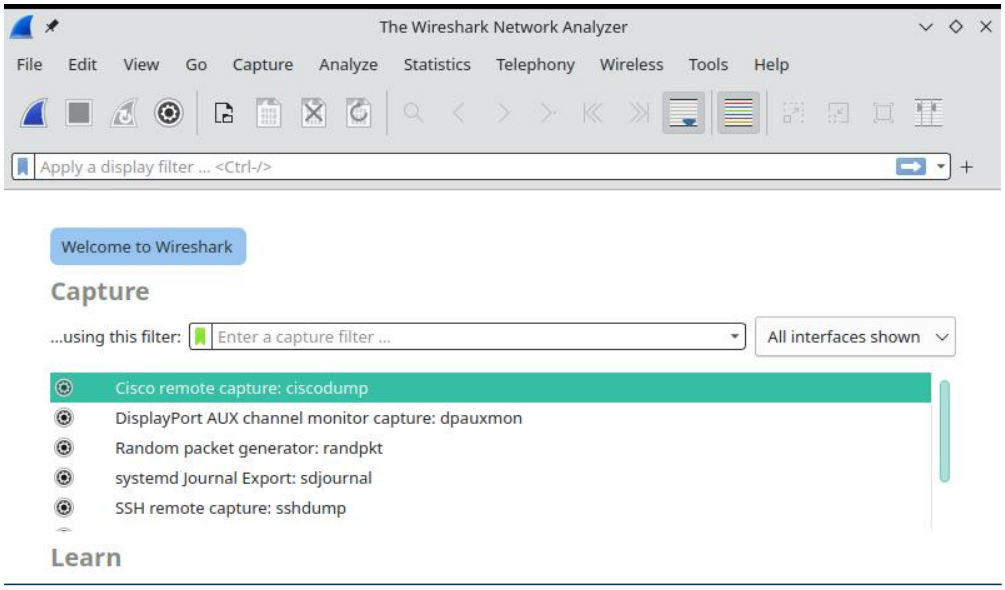
sudo pacman -Su

```
sudo pacman -Su
:: Starting full system upgrade...
 there is nothing to do
```

Now we can install Wireshark and all the required packages by running the below command.
sudo pacman -S wireshark-qt

```
sudo pacman -S wireshark-qt

resolving dependencies...
looking for conflicting packages...

Packages (5) bcg729-1.1.1-1  c-ares-1.19.1-1
             libmaxminddb-1.7.1-1  wireshark-cli-4.0.7-1
             wireshark-qt-4.0.7-1

Total Download Size:    27.16 MiB
Total Installed Size:  132.31 MiB

:: Proceed with installation? [Y/n] Y
:: Retrieving packages...
 wireshark-cli-4....    22.8 MiB  14.1 MiB/s 00:02 [#] 100%
 wireshark-qt-4.0...     4.1 MiB  27.0 MiB/s 00:00 [#] 100%
 c-ares-1.19.1-1-...   206.8 KiB  2.08 MiB/s 00:00 [#] 100%
 bcg729-1.1.1-1-x...    37.6 KiB   400 KiB/s 00:00 [#] 100%
 libmaxminddb-1.7...    23.9 KiB   254 KiB/s 00:00 [#] 100%
```

Enter wireshark in the terminal to load Wireshark.



How to Compile Wireshark From Source on Linux Systems

The easiest way to install Wireshark on Linux is with the package manager, but If you want to build Wireshark from source, we will show you a method on Ubuntu 22.04.

The steps should generally be similar for other Linux distributions.

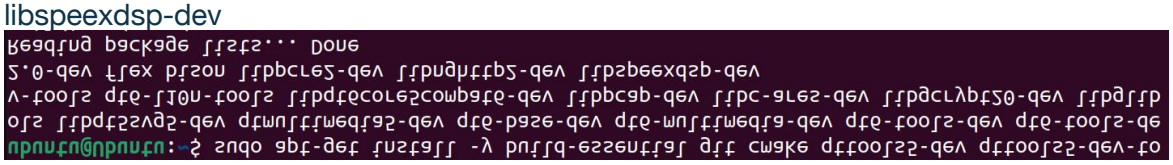
You would want to use this method instead of a package manager for a few reasons.

- It lets you access the newest features and bug fixes directly from the developers.
- Building from source allows you to enable or disable specific features based on your needs or the environment you're deploying in.
- It can provide a deeper understanding of the software, its dependencies, and the overall system architecture. It's a good learning experience.

Ensure you have the latest software packages installed from the system's repositories:
sudo apt-get update
Set the system's timezone according to your IP address:
export DEBIAN_FRONTEND=noninteractive
sudo ln -fs /usr/share/zoneinfo/$(curl http://ip-api.com/line?fields=timezone) /etc/localtime
sudo apt-get install -y tzdata

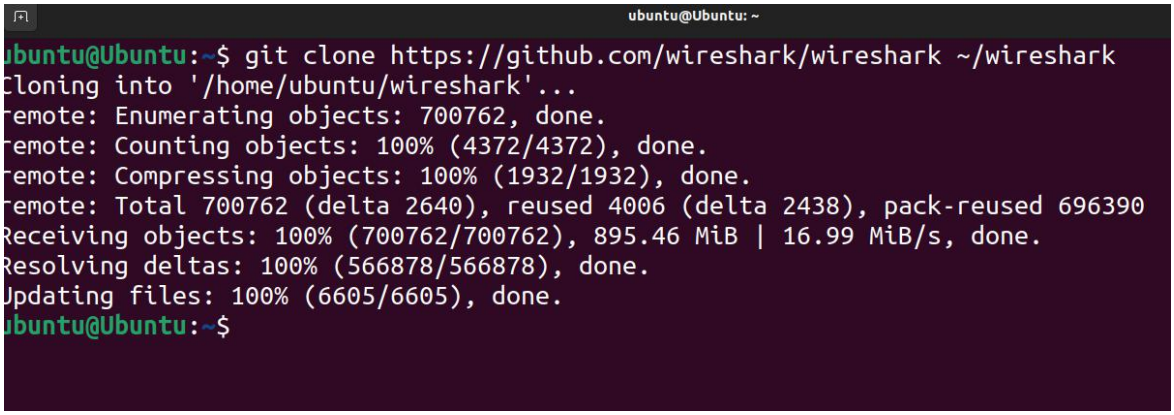
```
ubuntu@Ubuntu:~$ sudo ln -fs /usr/share/zoneinfo/$(curl http://ip-api.com/line?fields=timezone)
 /etc/localtime
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    16  100    16    0     0    131      0 --:--:-- --:--:-- --:--:--   132
ubuntu@Ubuntu:~$ sudo apt-get install -y tzdata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Next, install the necessary packages that are needed to build Wireshark:
sudo apt-get install -y build-essential git cmake qttools5-dev qttools5-dev-tools libqt5svg5-dev qtmultimedia5-dev \
qt6-base-dev qt6-multimedia-dev qt6-tools-dev qt6-tools-dev-tools qt6-l10n-tools libqt6core5compat6-dev libpcap-dev \
libc-ares-dev libgcrypt20-dev libglib2.0-dev flex bison libpcre2-dev libnghttp2-dev libspeexdsp-dev

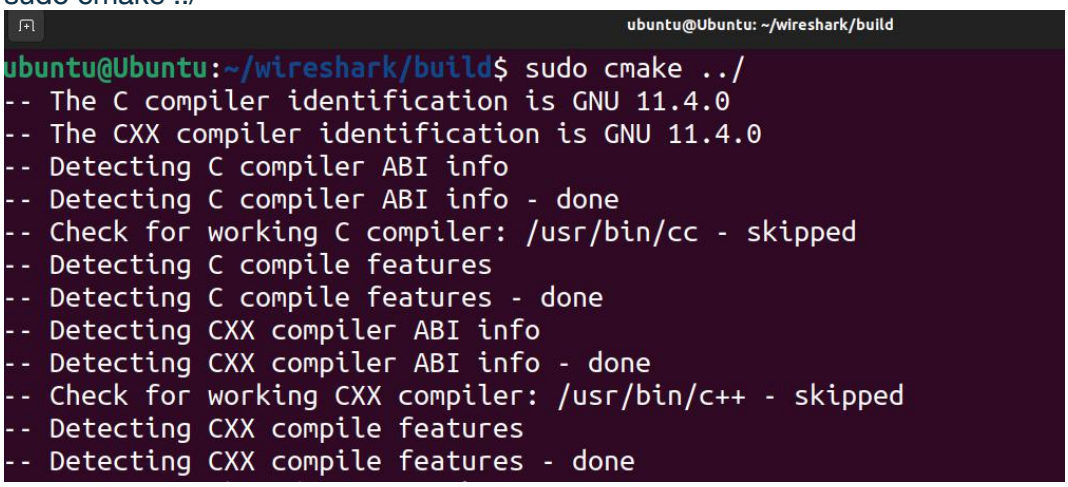


The following commands clone the Wireshark repository, navigate into it, create a build directory, move into that directory, run the cmake command to generate the build files, and then make to build the software.

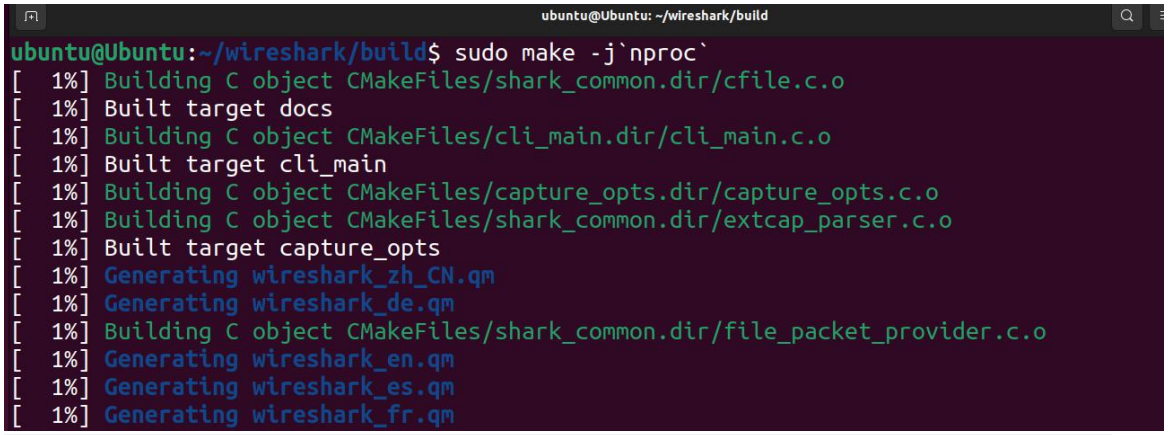
git clone https://github.com/wireshark/wireshark ~/wireshark



cd ~/wireshark
sudo mkdir build
cd build
sudo cmake ../

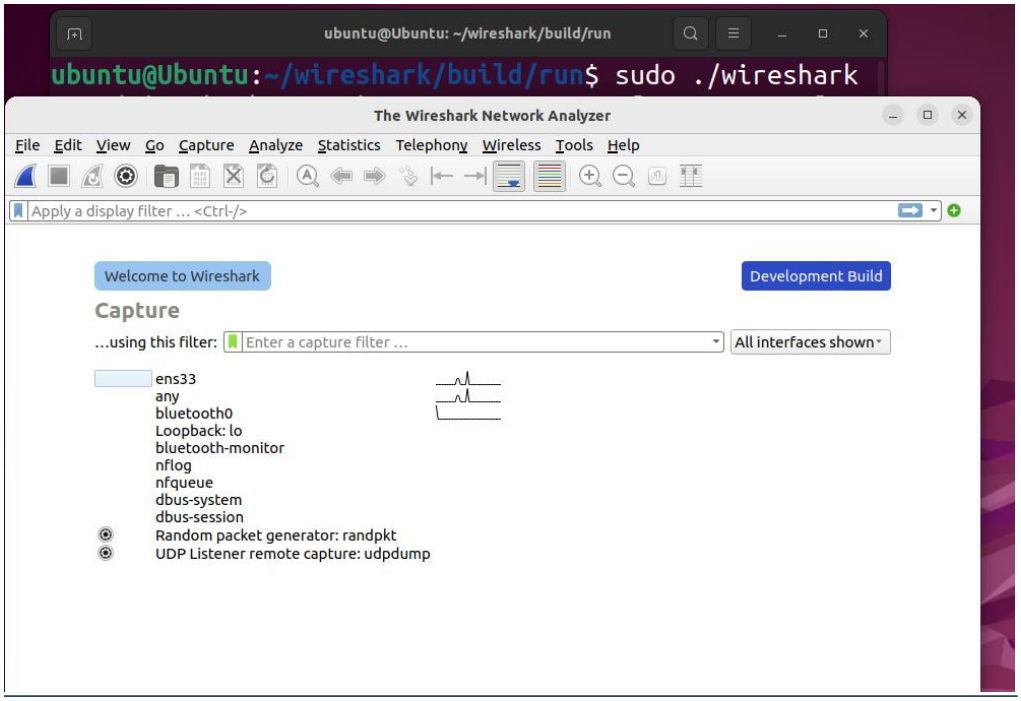


sudo make -j`nproc`
This command will take a while to complete, so grab a cup of coffee, tea, or your favorite beverage, sit back, and let the compiling work it's magic.



You can now run Wireshark by running the following command from the /wireshark/build/run directory.

sudo ./wireshark



Finish.

JOBSHEET 5

Lakukan installasi wireshark jelaskan tahapan, hasil installasi dan analisis nya.

LAPORAN HASIL PERCOBAAN: