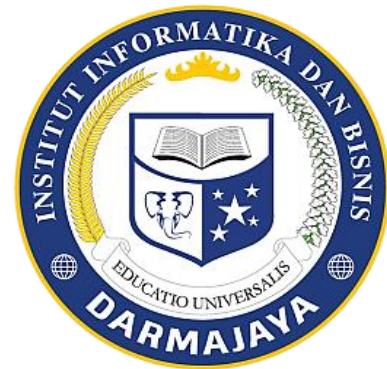


*Bahan Ajar*

## Modul Praktikum

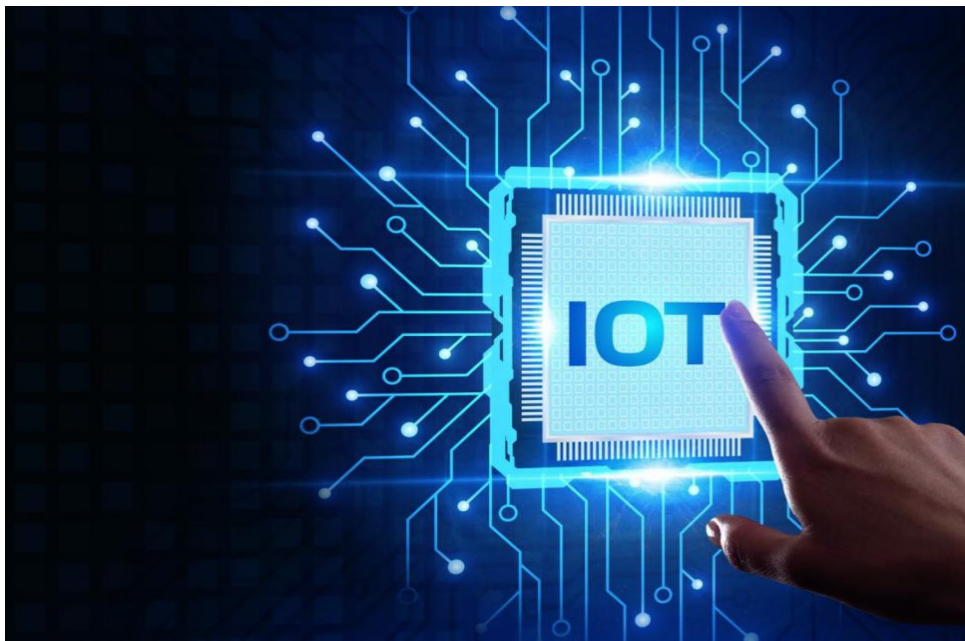
# INTERNET of THINGS (IoT Security)

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

Halaman Judul.....	1
DAFTAR ISI.....	2
Modul 1.....	4
Installation IoT Server (WMware).....	4
JOBSHEET 1.....	11
Modul 2.....	12
Installation IoT Server (Windows Server).....	12
JOBSHEET 2.....	21
Modul 3.....	22
Installation IoT Server (XAMPP).....	22
JOBSHEET 3.....	25
Modul 4.....	26
Wireshark Installation (Windows).....	26
JOBSHEET 4.....	36
Modul 5.....	37
Wireshark Installation (Linux).....	37
JOBSHEET 5.....	46
Modul 6.....	47
Wireshark Menu.....	47
JOBSHEET 6.....	52
Modul 7.....	54
Capturing Live Network Data (http Protocol).....	54
JOBSHEET 7.....	56

Modul 8.....	57
Ujian Tengah Semester (UTS).....	57
Modul 9.....	58
Capturing Live Network Data (tcp Protocol).....	58
JOBSHEET 9.....	58
Modul 10.....	59
Capturing Live Network Data (udp Protocol).....	59
JOBSHEET 10.....	59
Modul 11.....	60
Capturing Live Network Data (telnet Protocol).....	60
JOBSHEET 11.....	60
Modul 12.....	61
Capturing Live Network Data (ssh Protocol).....	61
JOBSHEET 12.....	61
Modul 13.....	62
Capturing Live Network Data (arp Protocol).....	62
JOBSHEET 13.....	62
Modul 14.....	63
IoT Controlling For Smart Home System.....	63
JOBSHEET 14.....	63
Modul 15.....	64
IoT Security For Smart Home System.....	64
JOBSHEET 15.....	64
Modul 16.....	65
Ujian Akhir Semester (UAS).....	65

# 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 [wiresark-dev@wireshark.org](mailto:wiresark-dev@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.

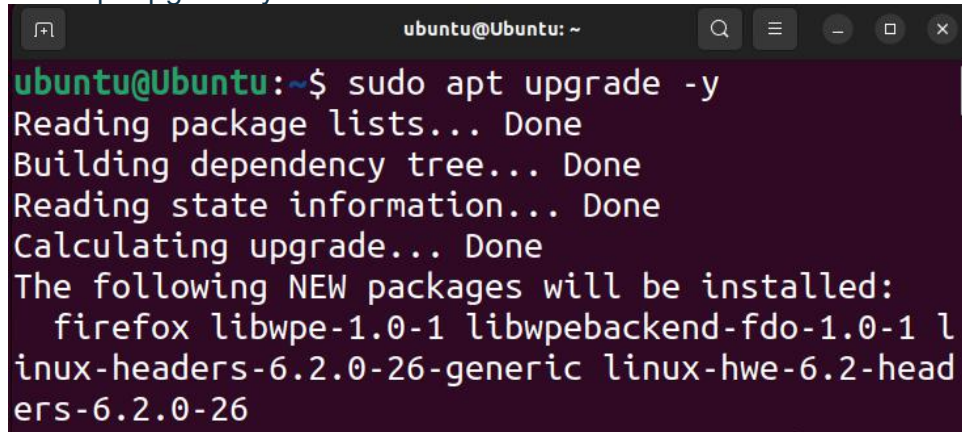
First, make sure your packages are up to date.

```
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:

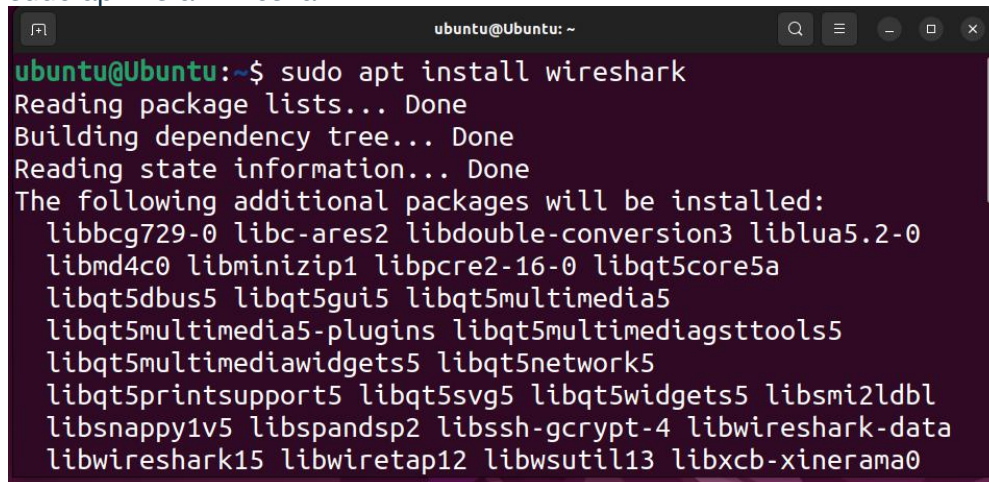
```
sudo apt upgrade -y
```



```
ubuntu@Ubuntu:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  firefox libwpe-1.0-1 libwpebackend-fdo-1.0-1 l
  inux-headers-6.2.0-26-generic linux-hwe-6.2-head
  ers-6.2.0-26
```

To install Wireshark, simply run the following command.

```
sudo apt install wireshark
```



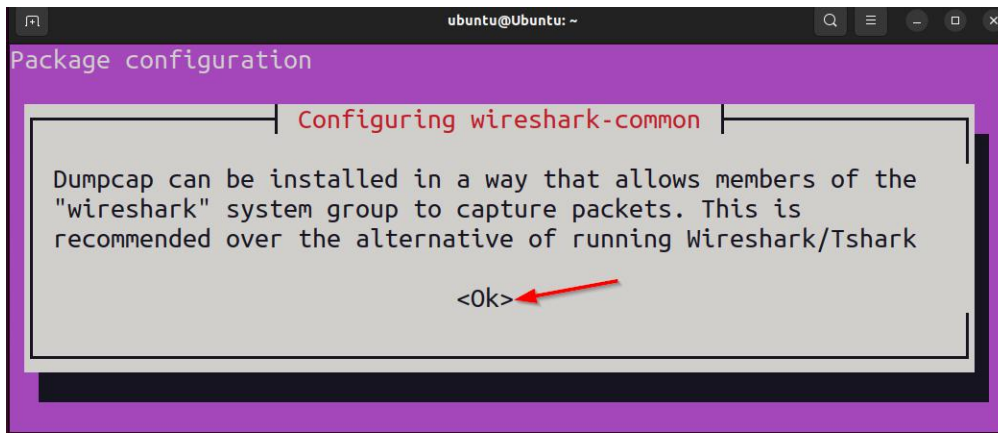
```
ubuntu@Ubuntu:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0
  libmd4c0 libminizip1 libpcre2-16-0 libqt5core5a
  libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5
  libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0
```

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

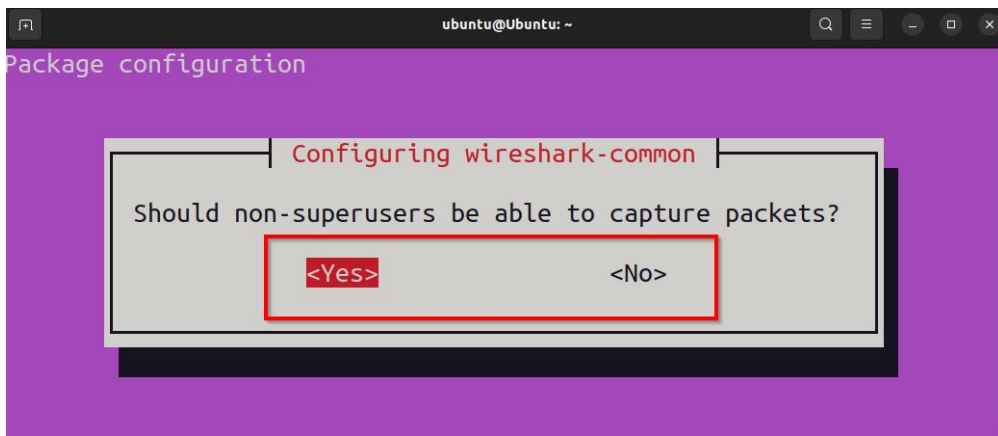
Select “Y” to continue with the installation.

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.)

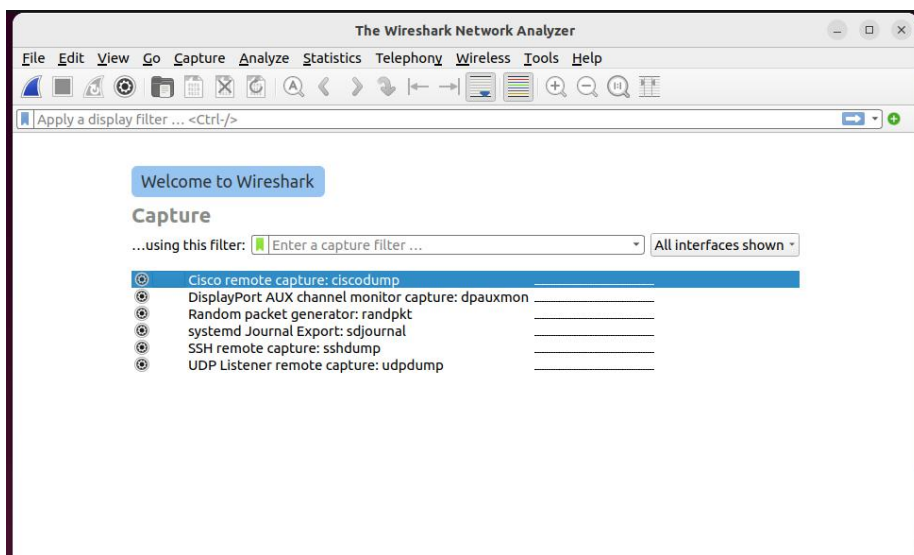
Select “Ok” to continue



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.



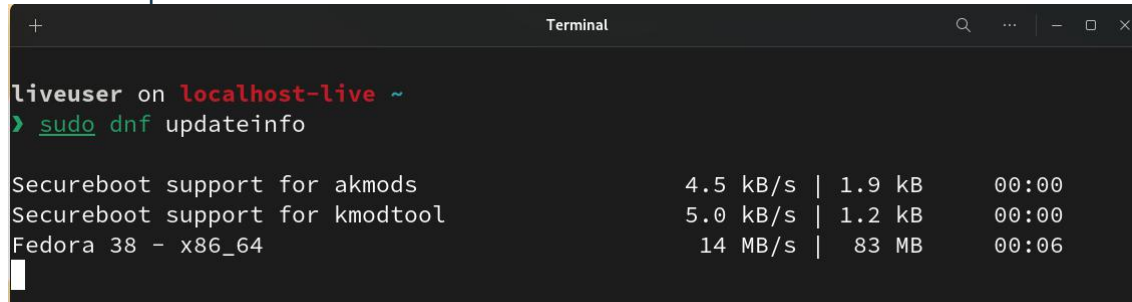
## How to Install Wireshark on Fedora-Based Systems

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
```

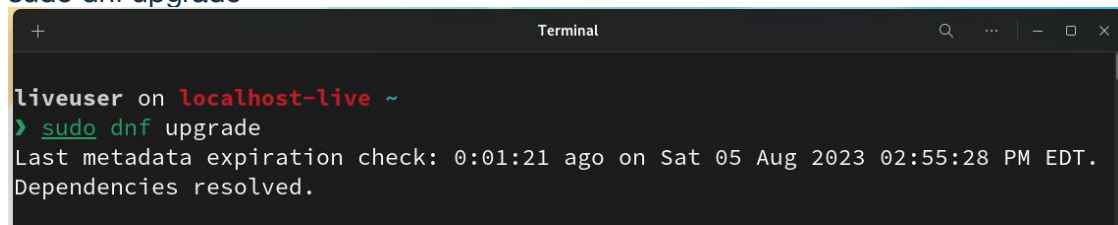


```
Terminal
liveuser on localhost-live ~
> sudo dnf updateinfo

Secureboot support for akmods          4.5 kB/s | 1.9 kB    00:00
Secureboot support for kmodtool        5.0 kB/s | 1.2 kB    00:00
Fedora 38 - x86_64                     14 MB/s | 83 MB     00:06
```

To upgrade all packages, use the following command:

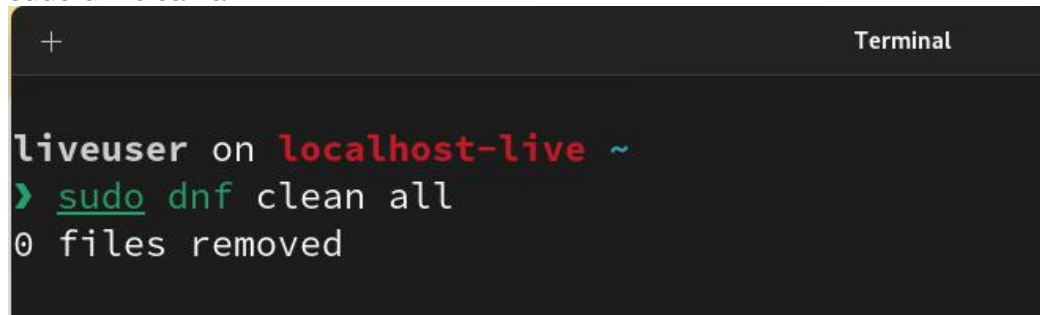
```
sudo dnf upgrade
```



```
Terminal
liveuser on localhost-live ~
> sudo dnf upgrade
Last metadata expiration check: 0:01:21 ago on Sat 05 Aug 2023 02:55:28 PM EDT.
Dependencies resolved.
```

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
```



```
Terminal
liveuser on localhost-live ~
> sudo dnf clean all
0 files removed
```

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
```

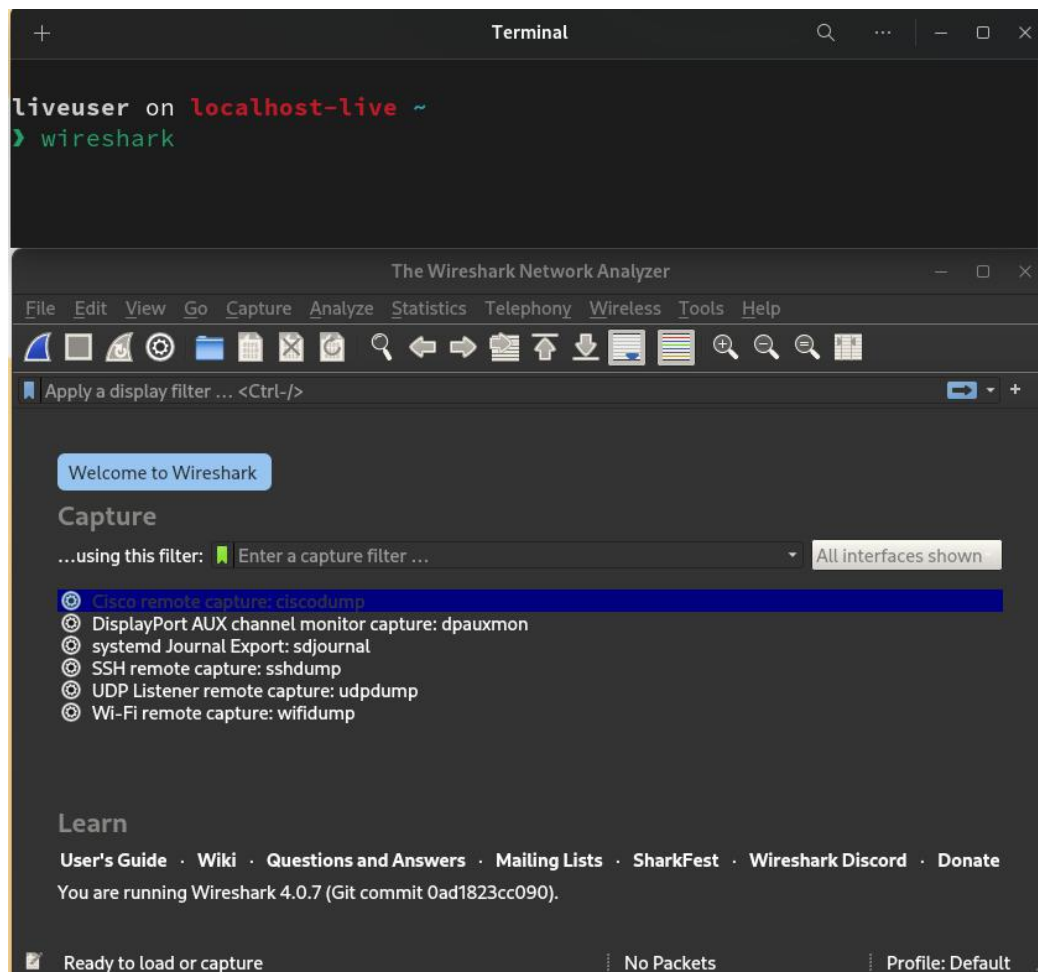
```
liveuser on localhost-live ~
> sudo dnf install wireshark
Last metadata expiration check: 0:00:48 ago on Sat 05 Aug 2023 03:33:35 PM EDT.
Dependencies resolved.
=====
Package                Arch      Version                Repository             Size
=====
Installing:
wireshark              x86_64    1:4.0.7-2.fc38        updates                4.4 M
Installing dependencies:
compat-lua-libs        x86_64    5.1.5-22.fc38        fedora                  167 k
double-conversion      x86_64    3.1.5-8.fc38         fedora                  49 k
libsmi                 x86_64    0.4.8-32.fc38        fedora                  2.1 M
pcre2-utf16            x86_64    10.42-1.fc38.1       fedora                  214 k
qt6-qt5compat         x86_64    6.5.2-1.fc38         updates                489 k
qt6-qtbase            x86_64    6.5.2-1.fc38         updates                3.8 M
qt6-qtbase-common     noarch    6.5.2-1.fc38         updates                10 k
qt6-qtbase-gui        x86_64    6.5.2-1.fc38         updates                7.3 M
qt6-qtdeclarative     x86_64    6.5.2-1.fc38         updates                9.2 M
qt6-qtmultimedia      x86_64    6.5.2-1.fc38         updates                945 k
qt6-qtshadertools     x86_64    6.5.2-1.fc38         updates                1.4 M
tslib                  x86_64    1.22-8.fc38          fedora                  152 k
wireshark-cli         x86_64    1:4.0.7-2.fc38        updates                23 M
=====
```

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

```
+ Terminal
Transaction Summary
=====
Install 19 Packages

Total download size: 53 M
Installed size: 224 M
Is this ok [y/N]: y
```

To start Wireshark, simply enter wireshark in the terminal.

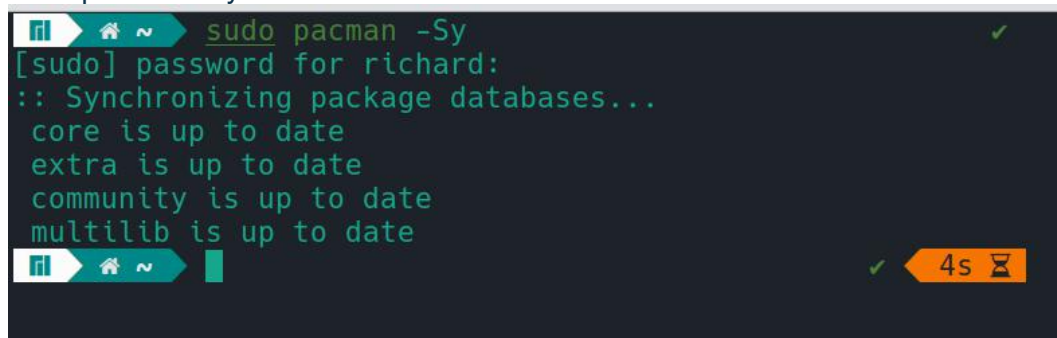


## How to Install Wireshark on Arch-Based Systems

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`

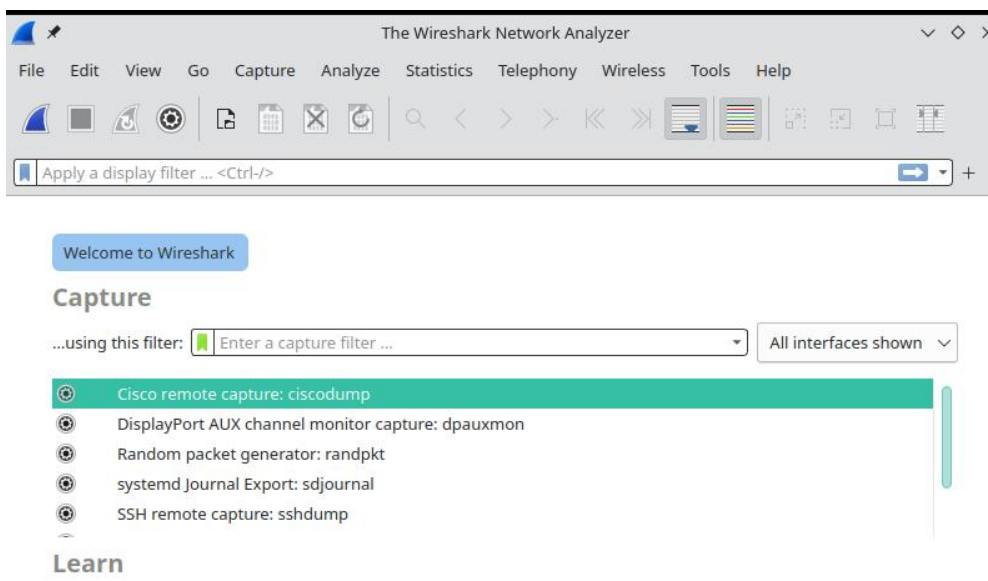
```
~$ sudo pacman -S wireshark-qt
resolving dependencies...
looking for conflicting packages...

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-4.0.7-1 22.8 MiB 14.1 MiB/s 00:02 [#] 100%
wireshark-qt-4.0.7-1  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-1.7.1-1 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 libcrypt20-dev libglib2.0-dev flex bison libpcre2-dev libnghttp2-dev
```

```
libspeexdsp-dev
```

```
Кеадрнр бэскаде фрзтз... done
5'0-деа фрех ргзюу фррбсде5-деа фррндрфрб5-деа фррзбеехзб-деа
^-фюргз дфе-фгю-фюргз фррдфекодезкомбате-деа фррбсэб-деа фррс-але2-деа фррдсрлнбт50-деа фррдфрр
оге фррдфззлде-деа дфвнфрфвсдфр2-деа дфе-рз26-деа дфе-внфрфвсдфр9-деа дфе-фюргз-деа дфе-фюргз-де
nрнузн@nрнузн:~$ знго эбс-деа фрзтзфрр -л рнфрр-е2зеуфрр дфс свэке дфрфюргз2-деа дфрфюргз2-деа-фю
```

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
```

```
ubuntu@Ubuntu: ~  
ubuntu@Ubuntu:~$ git clone https://github.com/wireshark/wireshark ~/wireshark  
Cloning into '/home/ubuntu/wireshark'...  
remote: Enumerating objects: 700762, done.  
remote: Counting objects: 100% (4372/4372), done.  
remote: Compressing objects: 100% (1932/1932), done.  
remote: Total 700762 (delta 2640), reused 4006 (delta 2438), pack-reused 696390  
Receiving objects: 100% (700762/700762), 895.46 MiB | 16.99 MiB/s, done.  
Resolving deltas: 100% (566878/566878), done.  
Updating files: 100% (6605/6605), done.  
ubuntu@Ubuntu:~$
```

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

```
ubuntu@Ubuntu:~/wireshark/build$ sudo cmake ../  
-- The C compiler identification is GNU 11.4.0  
-- The CXX compiler identification is GNU 11.4.0  
-- Detecting C compiler ABI info  
-- Detecting C compiler ABI info - done  
-- Check for working C compiler: /usr/bin/cc - skipped  
-- Detecting C compile features  
-- Detecting C compile features - done  
-- Detecting CXX compiler ABI info  
-- Detecting CXX compiler ABI info - done  
-- Check for working CXX compiler: /usr/bin/c++ - skipped  
-- Detecting CXX compile features  
-- Detecting CXX compile features - done
```

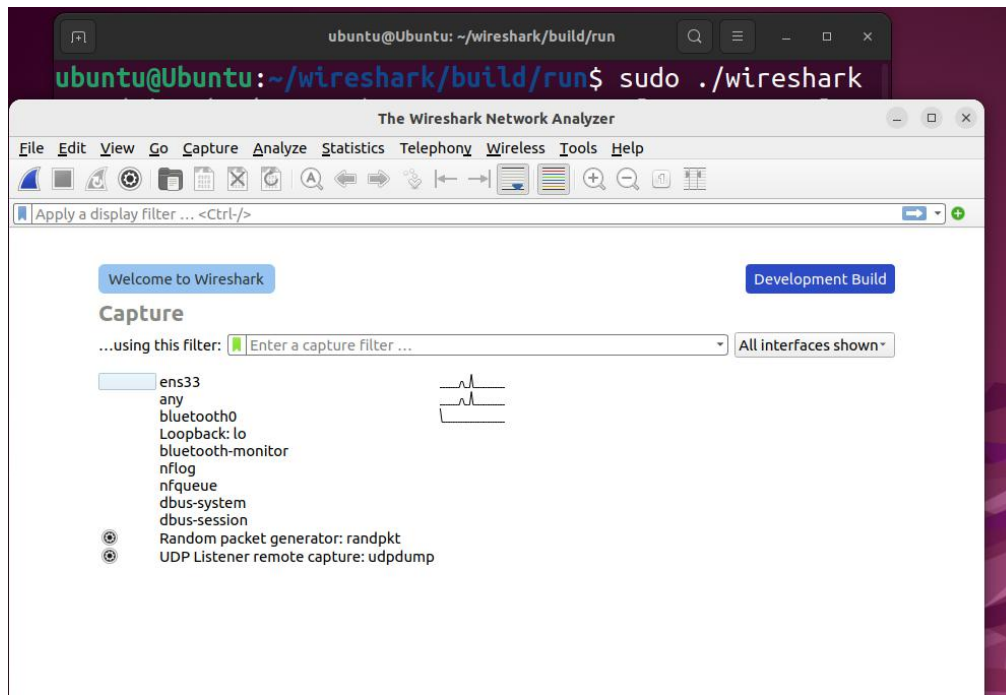
```
sudo make -j`nproc`
```

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 its magic.

```
ubuntu@Ubuntu:~/wireshark/build$ sudo make -j`nproc`  
[ 1%] Building C object CMakeFiles/shark_common.dir/cfile.c.o  
[ 1%] Built target docs  
[ 1%] Building C object CMakeFiles/cli_main.dir/cli_main.c.o  
[ 1%] Built target cli_main  
[ 1%] Building C object CMakeFiles/capture_opts.dir/capture_opts.c.o  
[ 1%] Building C object CMakeFiles/shark_common.dir/extcap_parser.c.o  
[ 1%] Built target capture_opts  
[ 1%] Generating wireshark_zh_CN.qm  
[ 1%] Generating wireshark_de.qm  
[ 1%] Building C object CMakeFiles/shark_common.dir/file_packet_provider.c.o  
[ 1%] Generating wireshark_en.qm  
[ 1%] Generating wireshark_es.qm  
[ 1%] Generating wireshark_fr.qm
```

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

```
sudo ./wireshark
```



Finish.

---

## JOB SHEET 5

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

LAPORAN HASIL PERCOBAAN: