

ASSIGNMENT  
NETWORKING AND SYSTEM ADMINISTRATION  
LAB

Analyzing network packet stream using nc and wireshark

SILJA C K  
ROLL NO:20  
RMCA B

## Step 1:

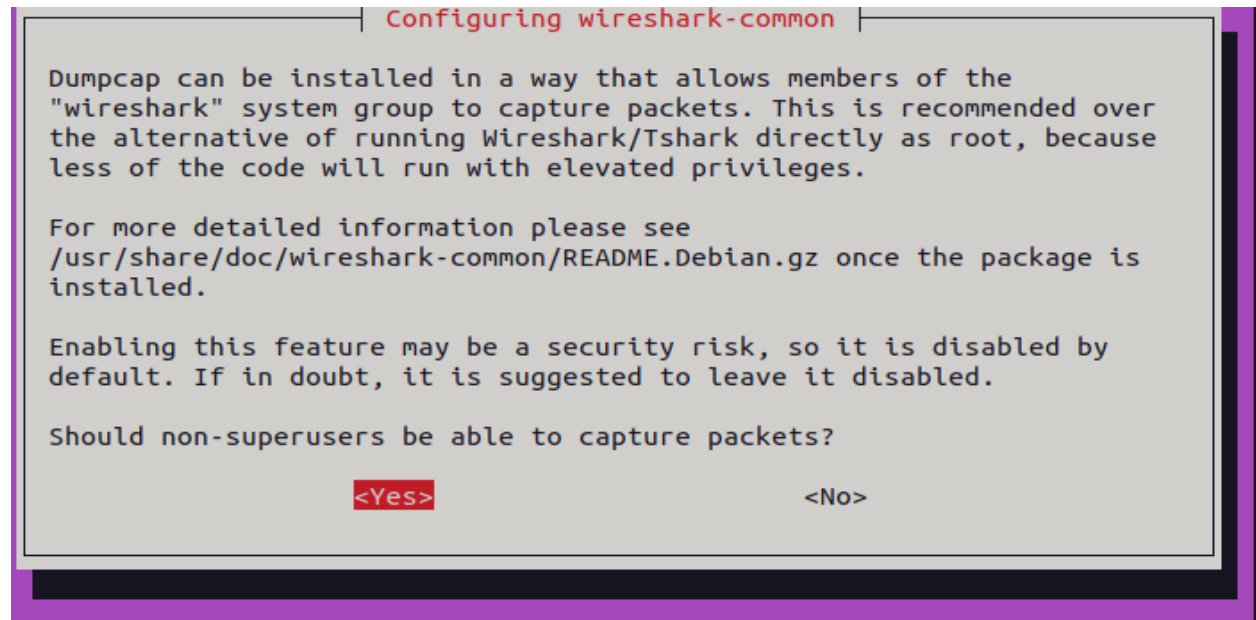
sudo apt-get install wireshark

```
silja@silja-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for silja:
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 libqt5sprintsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark14 libwiretap11 libwsutil12 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW 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 libqt5sprintsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark14 libwiretap11 libwsutil12 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
```

```
Setting up libqt5network5:amd64 (5.15.2+dfsg-5ubuntu1) ...
Setting up libwiretap11:amd64 (3.4.4-1ubuntu1) ...
Setting up libwireshark14:amd64 (3.4.4-1ubuntu1) ...
Setting up wireshark-common (3.4.4-1ubuntu1) ...
Setting up libqt5gui5:amd64 (5.15.2+dfsg-5ubuntu1) ...
Setting up libqt5widgets5:amd64 (5.15.2+dfsg-5ubuntu1) ...
Setting up qt5-gtk-platformtheme:amd64 (5.15.2+dfsg-5ubuntu1) ...
Setting up libqt5multimedia5:amd64 (5.15.2-3) ...
Setting up libqt5sprintsupport5:amd64 (5.15.2+dfsg-5ubuntu1) ...
Setting up libqt5multimediawidgets5:amd64 (5.15.2-3) ...
Setting up libqt5multimediagsttools5:amd64 (5.15.2-3) ...
Setting up libqt5multimedia5-plugins:amd64 (5.15.2-3) ...
Setting up libqt5svg5:amd64 (5.15.2-3) ...
Setting up wireshark-qt (3.4.4-1ubuntu1) ...
Setting up wireshark (3.4.4-1ubuntu1) ...
Processing triggers for libc-bin (2.33-0ubuntu5) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for shared-mime-info (2.0-1) ...
Processing triggers for mailcap (3.68ubuntu1) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
silja@silja-VirtualBox:~$
```

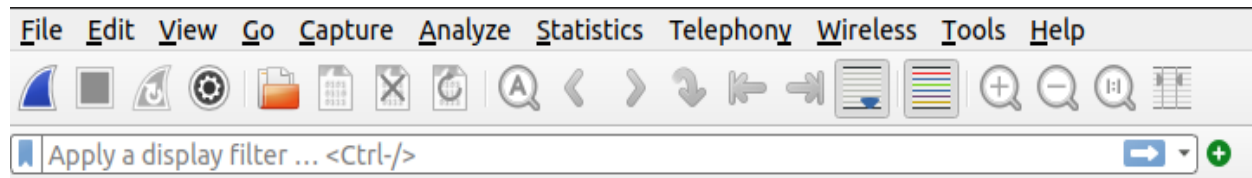
Step 2:

`sudo dpkg-reconfigure wireshark-common`



Step3 :

open wireshark from the applist.



Welcome to Wireshark

## Capture

...using this filter:

	Cisco remote capture: ciscodump	_____
	DisplayPort AUX channel monitor capture: dpauxmon	_____
	Random packet generator: randpkt	_____
	systemd Journal Export: sdjournal	_____
	SSH remote capture: sshdump	_____
	UDP Listener remote capture: udpdump	_____

## Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.4.4 (Git v3.4.4 packaged as 3.4.4-1ubuntu1).