Finolex Academy of Management and Technology, Ratnagiri

Department of Information Technology

Subject:	**Networking Lab (ITL401)**		
Class:	**SE IT / Semester – IV (CBCGS) / Academic year: 2017-18**		
Name of Student:	**Kazi Jawwad A Rahim**		
Roll No:	**28**	**Date of performance (DOP) :**	
Experiment No:	**09**	**Date of checking (DOC) :**	
Title: To install Wireshark on Ubuntu.			
Marks:		**Teacher's Signature:**	

1. Aim: **To install Wireshark on Ubuntu.**

2. Prerequisites:

Knowledge of

1. Ubuntu Commands
2. NS2 commands

3. Hardware Requirements:

1. PC with minimum 2GB RAM

4. Software Requirements:

1. Linux (Ubuntu 10.04)
2. ns-2.34 package
3. Wireshark package

5. Learning Objectives:

1. Configure Linux operating system for Wireshark installation
2. To install packet sniffer Wireshark on Ubuntu.

6. Course Objectives Applicable: LO 4

7. Program Outcomes Applicable: PO2, PO4

8. Program Education Objectives Applicable: 1, 3

9. Theory:

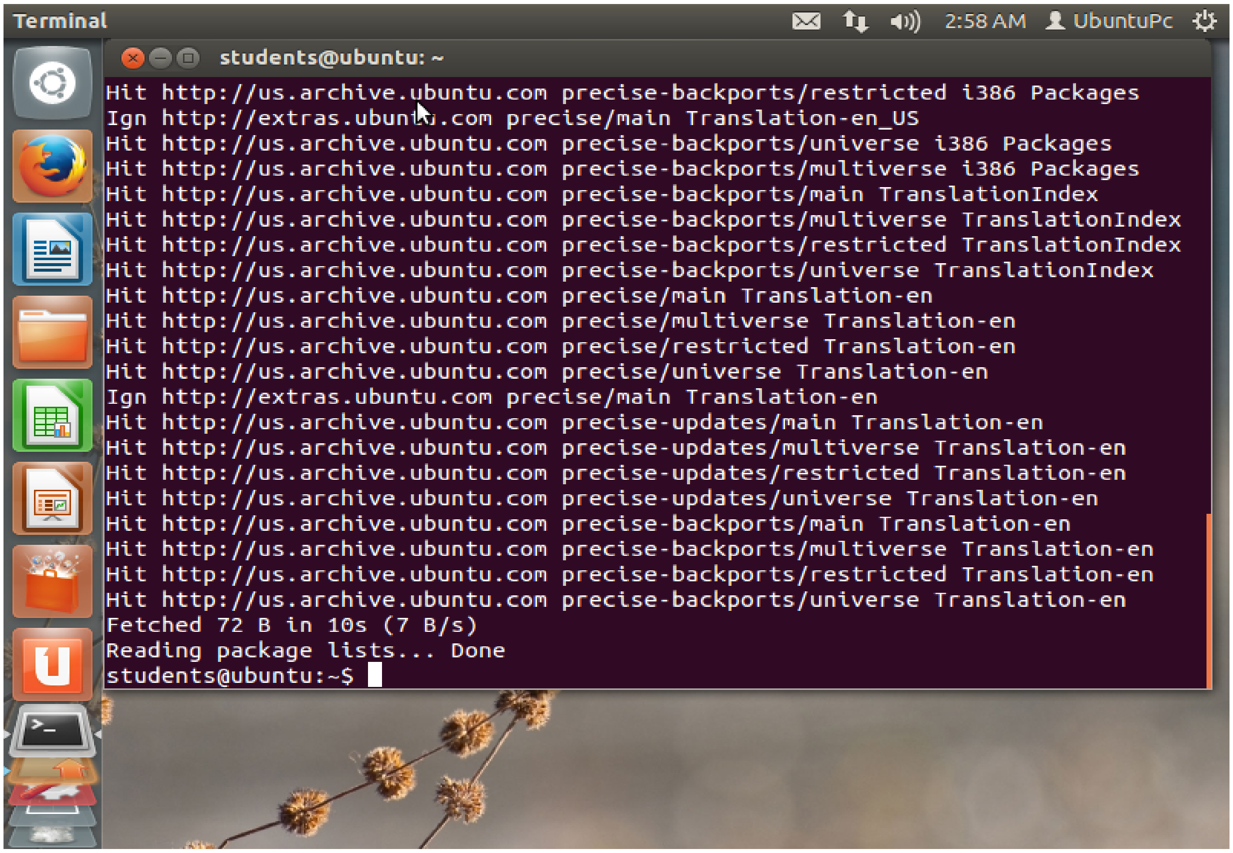
Type following command on terminal

1. sudo apt-get install Wireshark

2. Type y to continue

3. Type following command on terminal

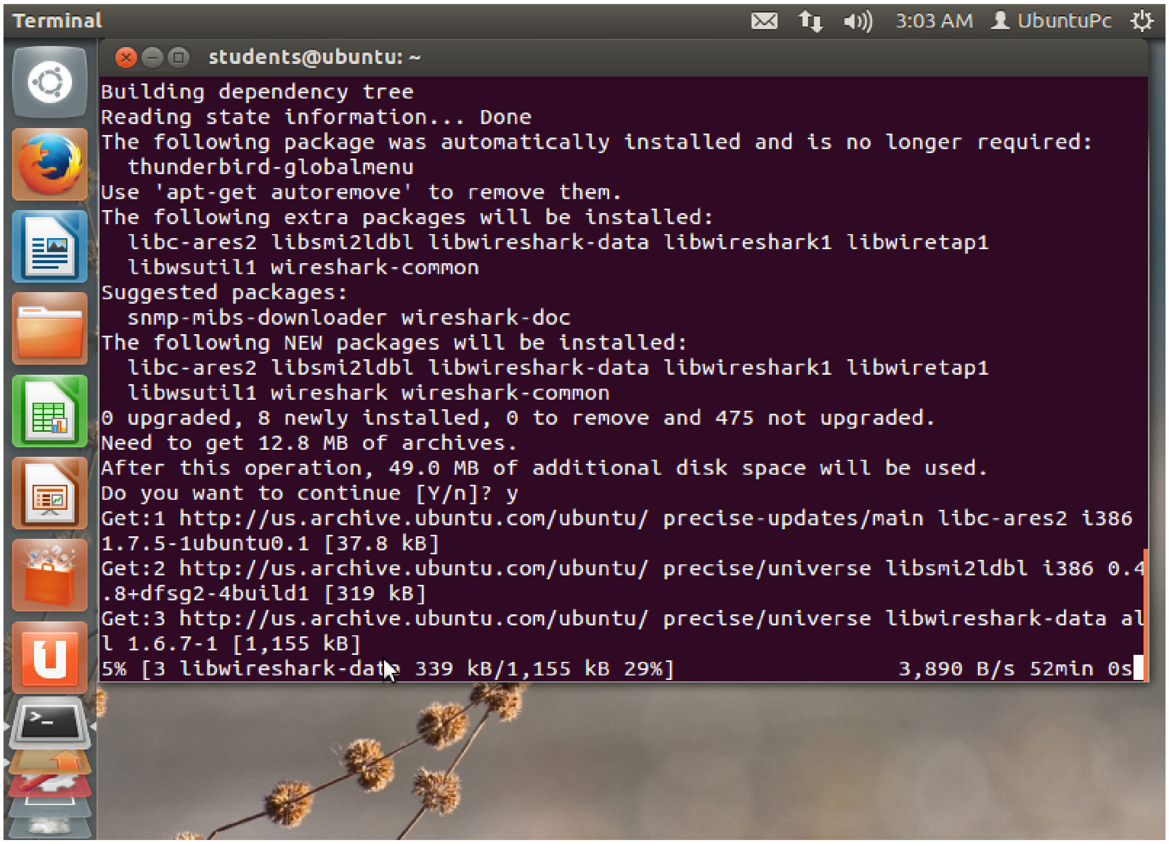
sudo apt-get install Wireshark Type y to continue



```
Hit http://us.archive.ubuntu.com precise-backports/restricted i386 Packages
Ign http://extras.ubuntu.com precise/main Translation-en_US
Hit http://us.archive.ubuntu.com precise-backports/universe i386 Packages
Hit http://us.archive.ubuntu.com precise-backports/multiverse i386 Packages
Hit http://us.archive.ubuntu.com precise-backports/main TranslationIndex
Hit http://us.archive.ubuntu.com precise-backports/multiverse TranslationIndex
Hit http://us.archive.ubuntu.com precise-backports/restricted TranslationIndex
Hit http://us.archive.ubuntu.com precise-backports/universe TranslationIndex
Hit http://us.archive.ubuntu.com precise/main Translation-en
Hit http://us.archive.ubuntu.com precise/multiverse Translation-en
Hit http://us.archive.ubuntu.com precise/restricted Translation-en
Hit http://us.archive.ubuntu.com precise/universe Translation-en
Ign http://extras.ubuntu.com precise/main Translation-en
Hit http://us.archive.ubuntu.com precise-updates/main Translation-en
Hit http://us.archive.ubuntu.com precise-updates/multiverse Translation-en
Hit http://us.archive.ubuntu.com precise-updates/restricted Translation-en
Hit http://us.archive.ubuntu.com precise-updates/universe Translation-en
Hit http://us.archive.ubuntu.com precise-backports/main Translation-en
Hit http://us.archive.ubuntu.com precise-backports/multiverse Translation-en
Hit http://us.archive.ubuntu.com precise-backports/restricted Translation-en
Hit http://us.archive.ubuntu.com precise-backports/universe Translation-en
Fetched 72 B in 10s (7 B/s)
Reading package lists... Done
students@ubuntu:~$
```

Terminal Window Output- 1

4. Select yes and Press enter

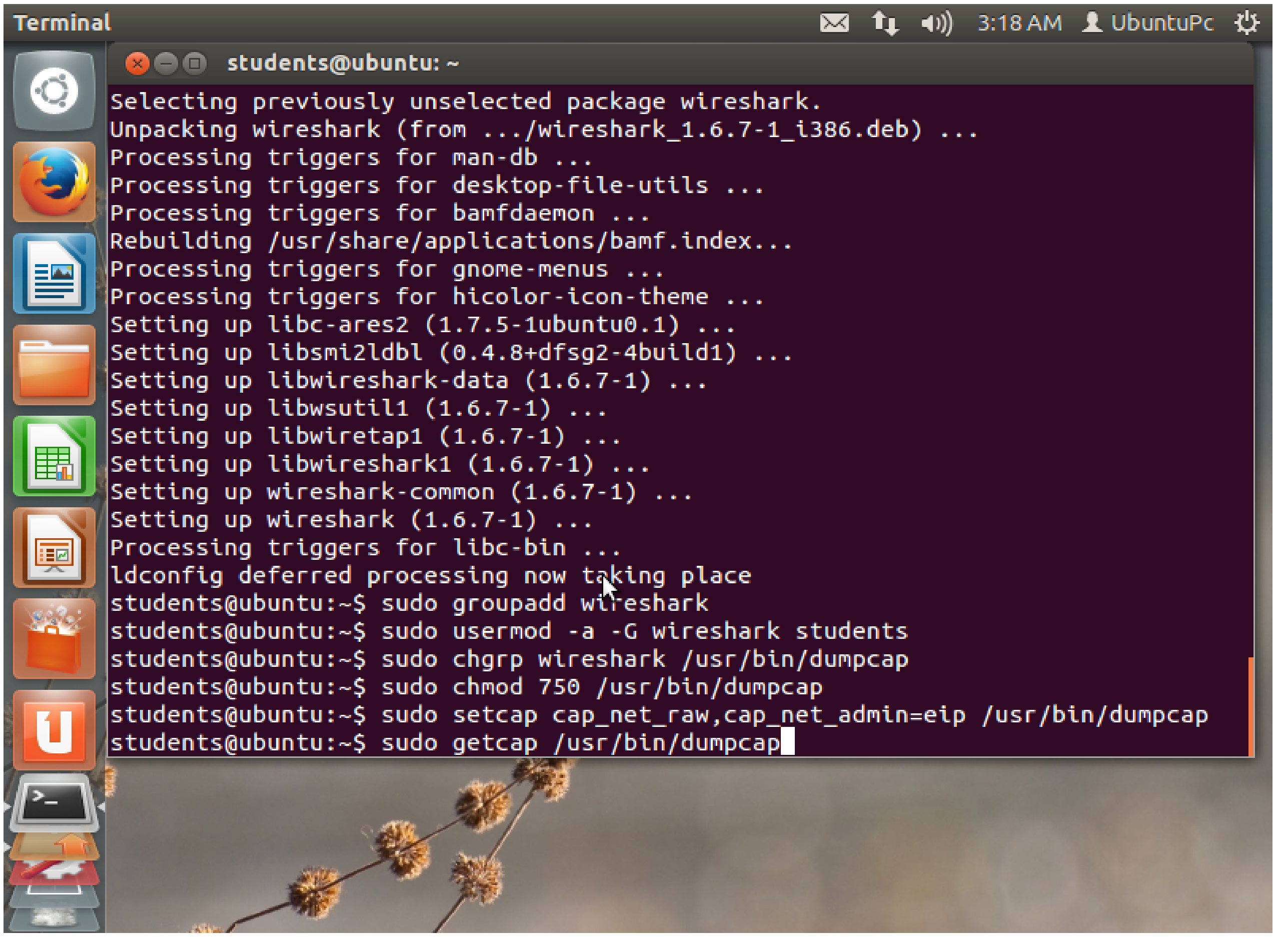


```
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  thunderbird-globalmenu
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark1 libwiretap1
  libwsutil1 wireshark-common
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark1 libwiretap1
  libwsutil1 wireshark wireshark-common
0 upgraded, 8 newly installed, 0 to remove and 475 not upgraded.
Need to get 12.8 MB of archives.
After this operation, 49.0 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://us.archive.ubuntu.com/ubuntu/ precise-updates/main libc-ares2 i386
1.7.5-1ubuntu0.1 [37.8 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ precise/universe libsmi2ldbl i386 0.4
.8+dfsg2-4build1 [319 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ precise/universe libwireshark-data al
l 1.6.7-1 [1,155 kB]
5% [3 libwireshark-data 339 kB/1,155 kB 29%]                 3,890 B/s 52min 0s
```

Terminal Window Output- 2

Now type following commands on terminal:-

1. sudo groupadd Wireshark
2. sudo usermod -a -G wireshark YOUR_USER_NAME
3. sudo chgrp wireshark /usr/bin/dumpcap
4. sudo chmod 750 /usr/bin/dumpcap
5. sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
6. sudo getcap /usr/bin/dumpcap

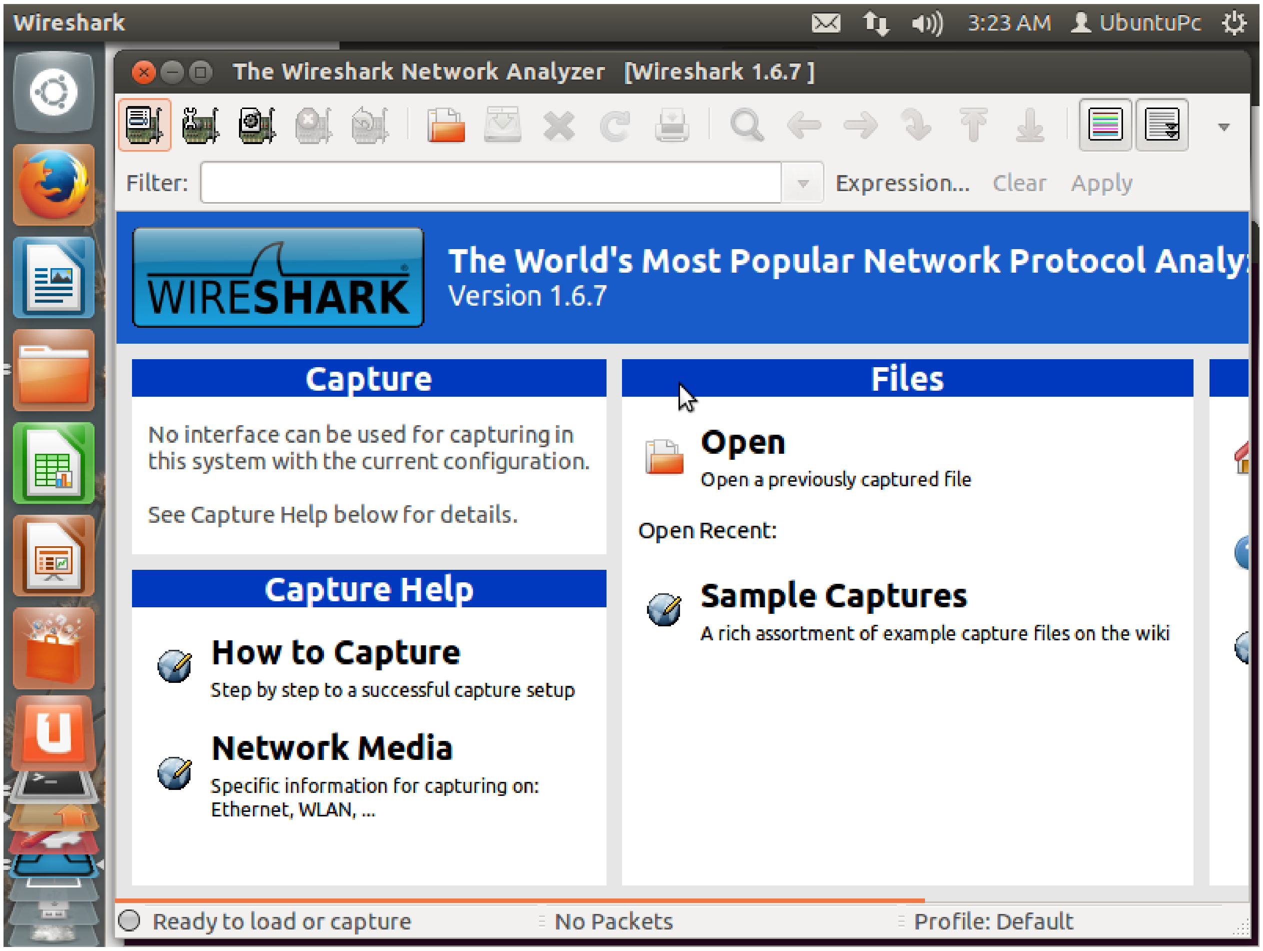


```
Selecting previously unselected package wireshark.
Unpacking wireshark (from .../wireshark_1.6.7-1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for desktop-file-utils ...
Processing triggers for bamfdaemon ...
Rebuilding /usr/share/applications/bamf.index...
Processing triggers for gnome-menus ...
Processing triggers for hicolor-icon-theme ...
Setting up libc-ares2 (1.7.5-1ubuntu0.1) ...
Setting up libsmi2ldbl (0.4.8+dfsg2-4build1) ...
Setting up libwireshark-data (1.6.7-1) ...
Setting up libwsutil1 (1.6.7-1) ...
Setting up libwiretap1 (1.6.7-1) ...
Setting up libwireshark1 (1.6.7-1) ...
Setting up wireshark-common (1.6.7-1) ...
Setting up wireshark (1.6.7-1) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
students@ubuntu:~$ sudo groupadd wireshark
students@ubuntu:~$ sudo usermod -a -G wireshark students
students@ubuntu:~$ sudo chgrp wireshark /usr/bin/dumpcap
students@ubuntu:~$ sudo chmod 750 /usr/bin/dumpcap
students@ubuntu:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
students@ubuntu:~$ sudo getcap /usr/bin/dumpcap
```

Terminal Window Output- 3

7. Restart the Ubuntu

8. In terminal type Wireshark and Wireshark window will be open. ,



The World's Most Popular Network Protocol Analy
Version 1.6.7

No interface can be used for capturing in this system with the current configuration.

See Capture Help below for details.

Open a previously captured file

A rich assortment of example capture files on the wiki

Step by step to a successful capture setup

Specific information for capturing on: Ethernet, WLAN, ...

Ready to load or capture | No Packets | Profile: Default

Wireshark Interface in Ubuntu Linux

13. Experiment/Assignment Evaluation

SR	**Parameters**	**Weight**	**Excellent**	**Good**	**Average**	**Poor**	**Not as per requirement**
		Scale Factor ->	5	4	3	2	0
1	Technical Understanding	25					
2	Performance / Execution	25					
3	Question Answers	20					
4	Punctuality	20					
5	Presentation	10					
	Total out of 100 --> #(to be converted as per term-work evaluation applicable to the subject)		**∑ (Weight * Scale Factor)/5 = ________**				

References:

[1] https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

[2] https://www.wireshark.org/download.html

[3] http://www.cs.wayne.edu/fengwei/16sp-csc5991/labs/lab1-instruction.pdf

Viva Questions

1. What is the use of Packet sniffer?
2. What is open source software?
3. What are the system requirements for Wireshark?