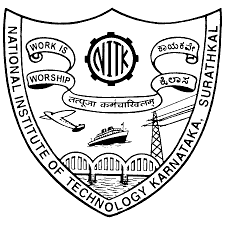
**UNIX MINI PROJECT REPORT**



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA**

**COURSE TITLE**

Unix Programming And Practice (IT202)

**SUBMITTED TO :**

MsDeepthi L

**SUBMITTED BY :**

1.BADRI RAVALI (15IT207)

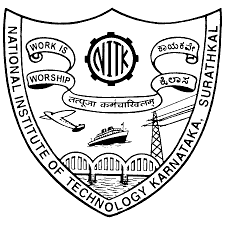
2.SHIVANI SHRIVASTAVA (15IT243)

3.SNEHA PATIL (15IT245)

4.PADMASALI ALEKHYA(15IT226)

**SUBMISSION DATE :**

12 NOVEMBER 2016



**NATIONAL INSTITUTE OF TECHNOLOGY,KARNATAKA**

**CERTIFICATE**

THIS IS TO CERTIFY THAT

**BADRI RAVALI(15IT207)**

**SHIVANI SHRIVASTAVA (15IT245)**

**SNEHA PATIL (15IT243)**

**PADMASALI ALEKHYA (15IT226)**

HAS SATISFACTORILY COMPLETED THE PROJECT WORK IN UNIX PROGRAMMING & PRACTICE ASSIGNED BY THE INSTITUTE FOR THIRD SEMESTER MINI PROJECT IN THE YEAR 2016-2017.

**DATE: 12/11/2016**

SIGNATURE OF THE FACULTY HEAD OF THE DEPARTMENT

**ABSTRACT**

The basic idea behind the project involves:

1. Capturing the traffic of the network using Wireshark Software and saving it in the form of a text file.
2. Extracting the data from the trace file on the basis of the specified IP Address or Domain names.
3. Displaying the Input-Output Graph depicting the number of packets sent and received per second.
4. Displaying the Statistics of the data of the Captured Trace File.

**Design Tools Used:**

**Wireshark:**

Wireshark, a network analysis tool formally known as Ethereal, captures packets in real time and displays them in human readable format. Wireshark includes filters, color coding and other features that let you dig deep into network traffic and inspect individual packets. It has the ability to capture all of those packets that are sent and received on your network and it can decode them for analysis.

We can use Wireshark to inspect a suspicious program’s network traffic, analyze the traffic flow on your network or trouble shoot network problems.

Wireshark gives different information about the packet like the protocol used, Source IP, Destination IP, time at which the packet is sent,etc.

**AWK**

**AWK** is a programming language designed for text processing and typically used as a data extraction and reporting tool. It is a standard feature of most Unix-like operating systems. It is very powerful and specially designed for text processing.

**Typical Uses of AWK**

Myriad of tasks can be done with AWK. Listed below are just a few of them −

* Text processing,
* Producing formatted text reports,
* Performing arithmetic operations,
* Performing string operations, and many more.

**ALGORITHM**

1) Read the Trace File Name and display the contents.

2) Available choices are -

i) Search via IP Address

ii) Search via Domain Name

iii) Input Output Graph Plot

iv) Statistics of the data in the Captured Trace File and Exit

3) Read choice

4) Choice 1:

i) Enter the corresponding trace filename

ii) Display the list of all IP Addresses available as source corresponding to the captured file

iii) Read the IP Address to display its corresponding details

iv) If the IP Address entered does not match the available IP Address then read the IP address again

v) In order to extract the details , we feed the IP Address to awk (line by line interpreter)

vi) The details corresponding to a particular IP Address include :

-Time at which the packet was sent or received

-Destination IP Address

-Protocols

-Length of Packet

Choice 2:

i) Enter the corresponding trace filename

ii) Display the list of domain names(Source or Destination) corresponding to the captured file

iii) Read the domain name(Source or Destination) to display its corresponding details

iv) If the domain name(Source or Destination) entered does not match the available source domain names then read the domain name again

v) In order to extract the details , we feed the Domain Name(Source or Destination) to awk (line by line interpreter)

vi) The details corresponding to a particular IP Address include :

-Time at which the packet was sent or received

-Destination IP Address/Source IP Address

-Protocols

-Length of Packet

-Information

vii) The number of packets corresponding to source domain names or destination domain names are displayed

Choice 3:

i) Read the filename with the Graph

ii) Display the Input Output Graph depicting the number of packets sent or received per second

Choice 4:

i) Enter the filename

ii) Display the statistics of data in trace file

iii) Exit

**Other Unix Commands Used:**

**sort** :

The **sort** command is a command line utility for sorting lines of text files.

To sort by number pass –n option to “**sort**” command.This will sort from lowest number to highest number and write the result to standard output.

**uniq**:

**uniq** filters out adjacent, matching lines from input file, writing the filtered data to the output file.

If input is not specified, **uniq** reads from the standard input.

If output is not specified, output reads from the standard output.

**cat**:

It is used to display text files, copy text files into a new document, append the contents of a text file to the end of another text file, combing them .It will display the contents of the text file on the screen.

**wc**:

**wc** prints newline , word, and byte counts for each FILE, and a total if more than one file is specified.With no file ,or when file is a dash (“-”) , **wc** operates on standard input.”**wc -l**” is used to print the newline counts.

**eog**:

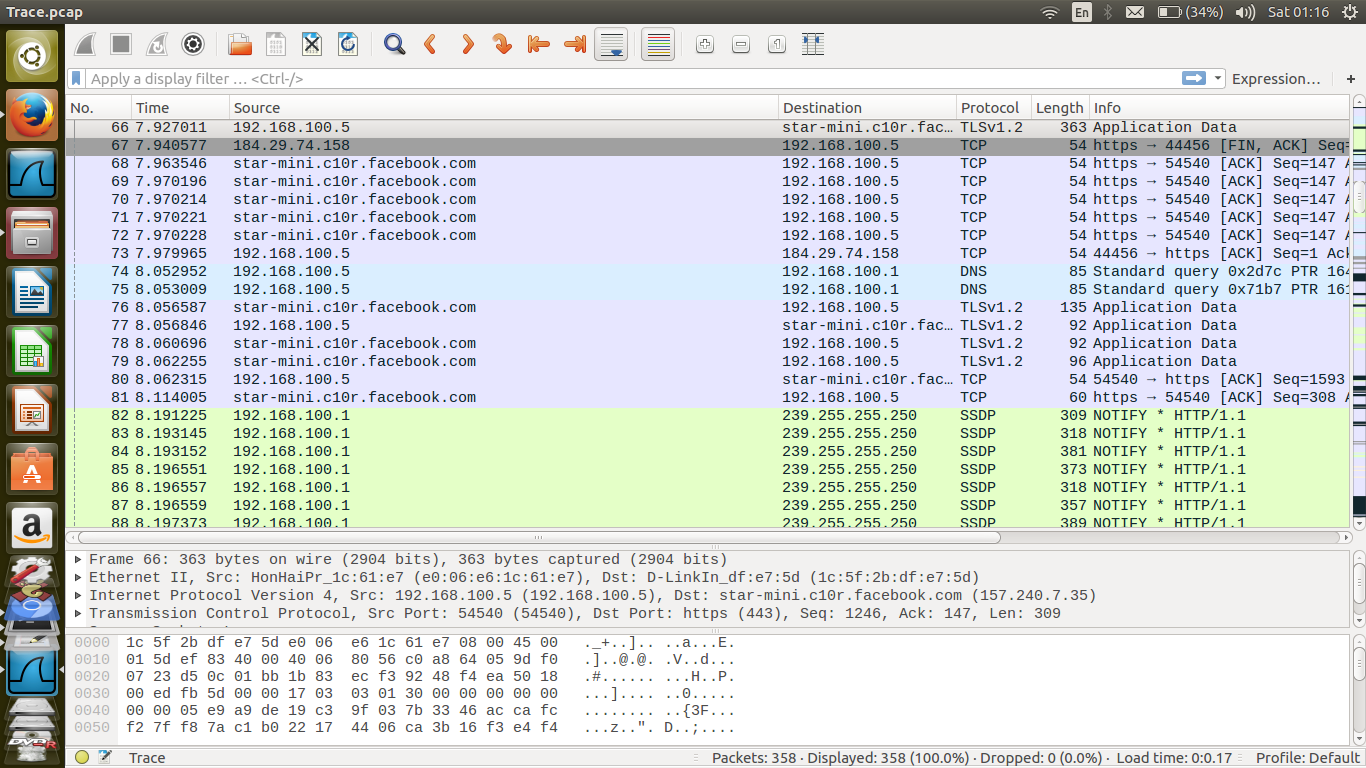
**eog** command is used to start the Image Viewer from the terminal.You can specify file by typing the filename after the **eog** command.

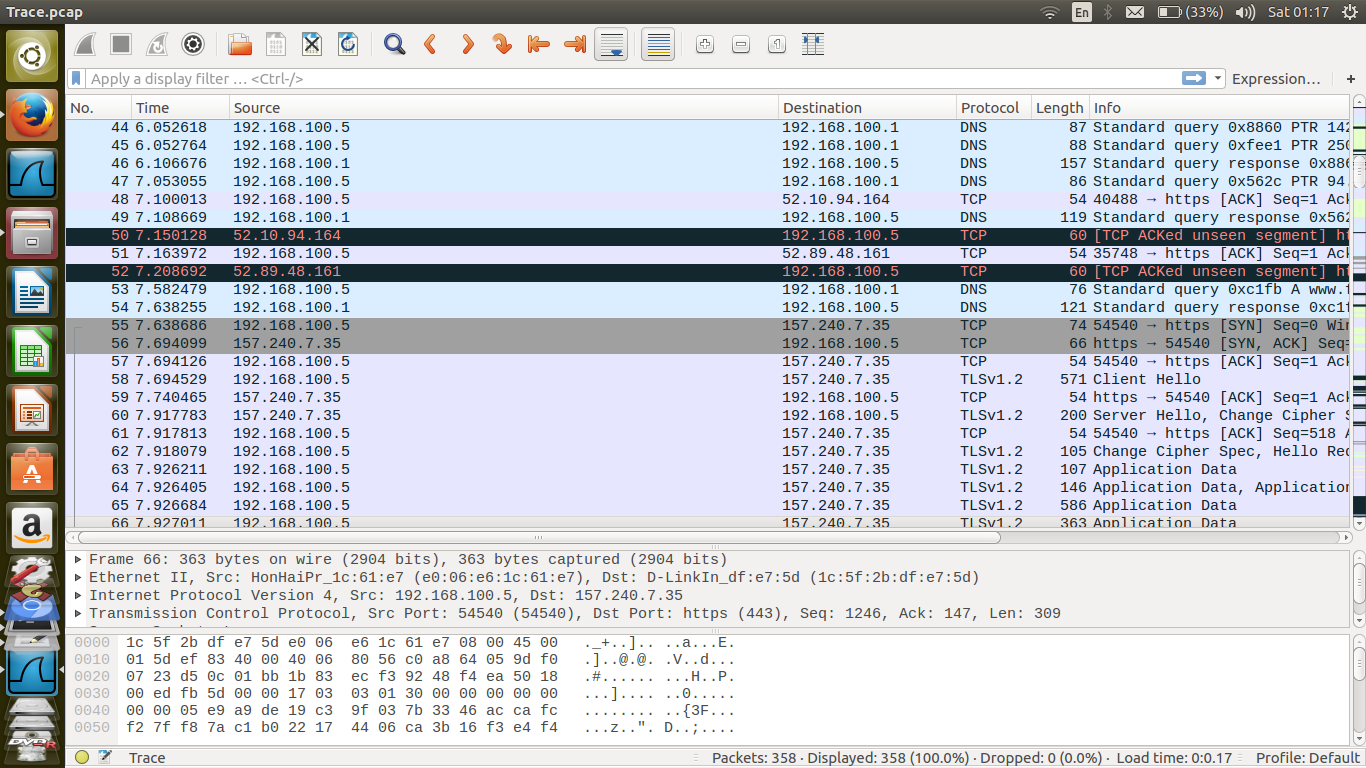
**capinfos**:

It’s a program that reads one or more capture files and returns some or all available statistics in one of two types of output formats : long or table.

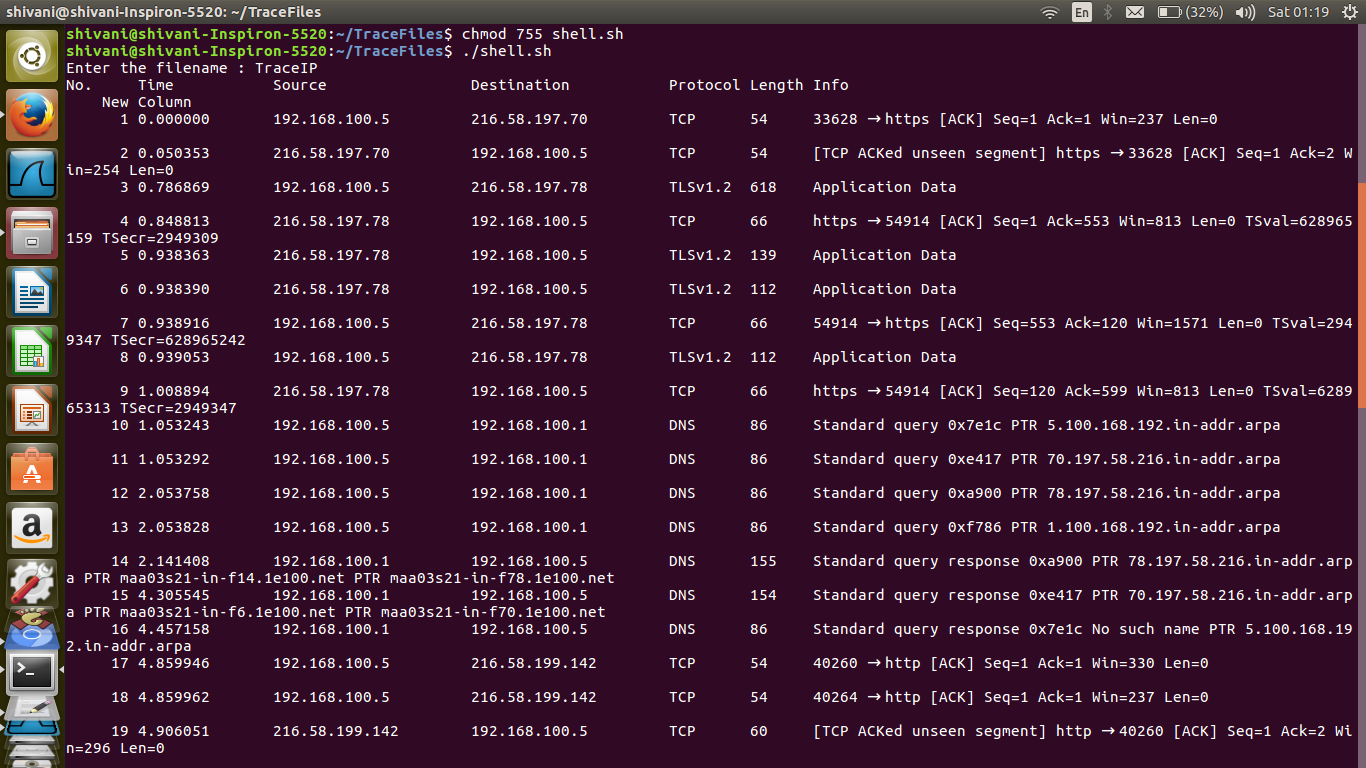
**OUTPUT**

1.Capturing packets using Wireshark

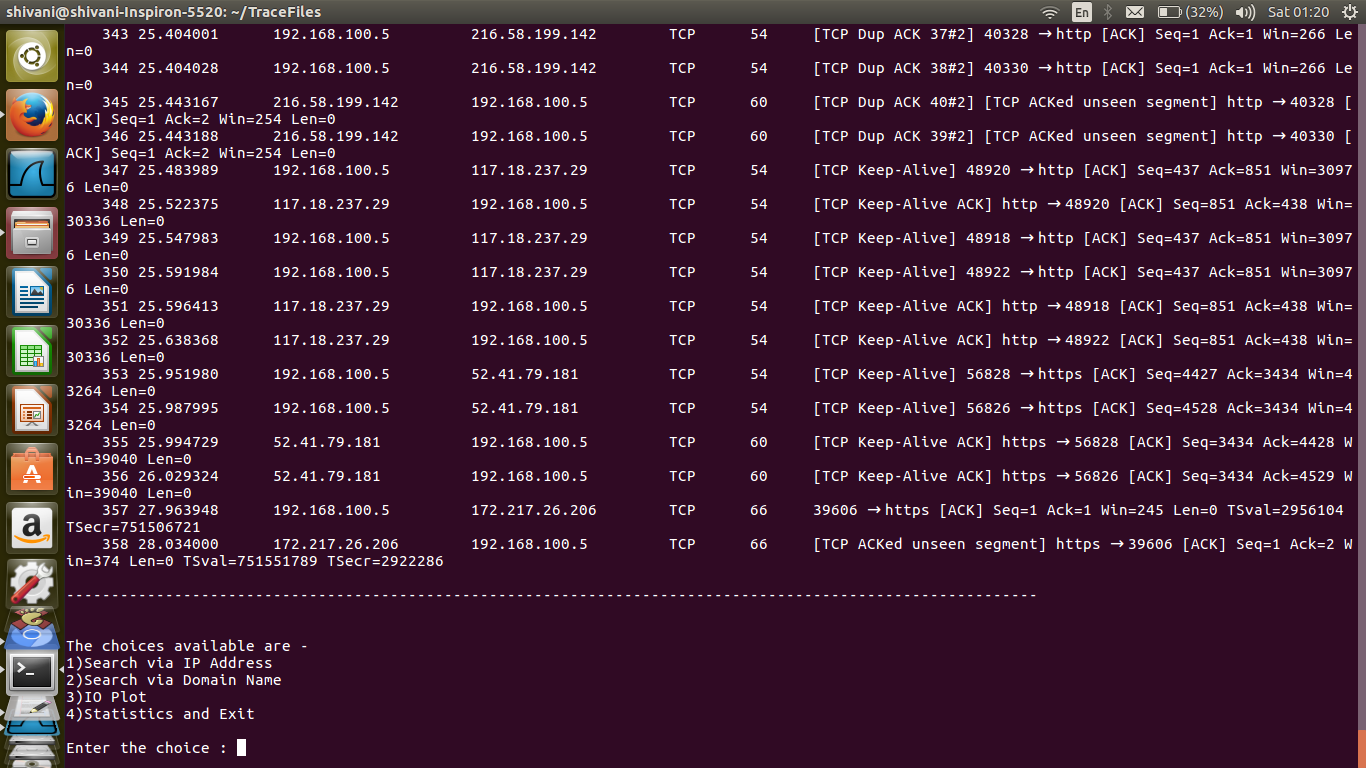


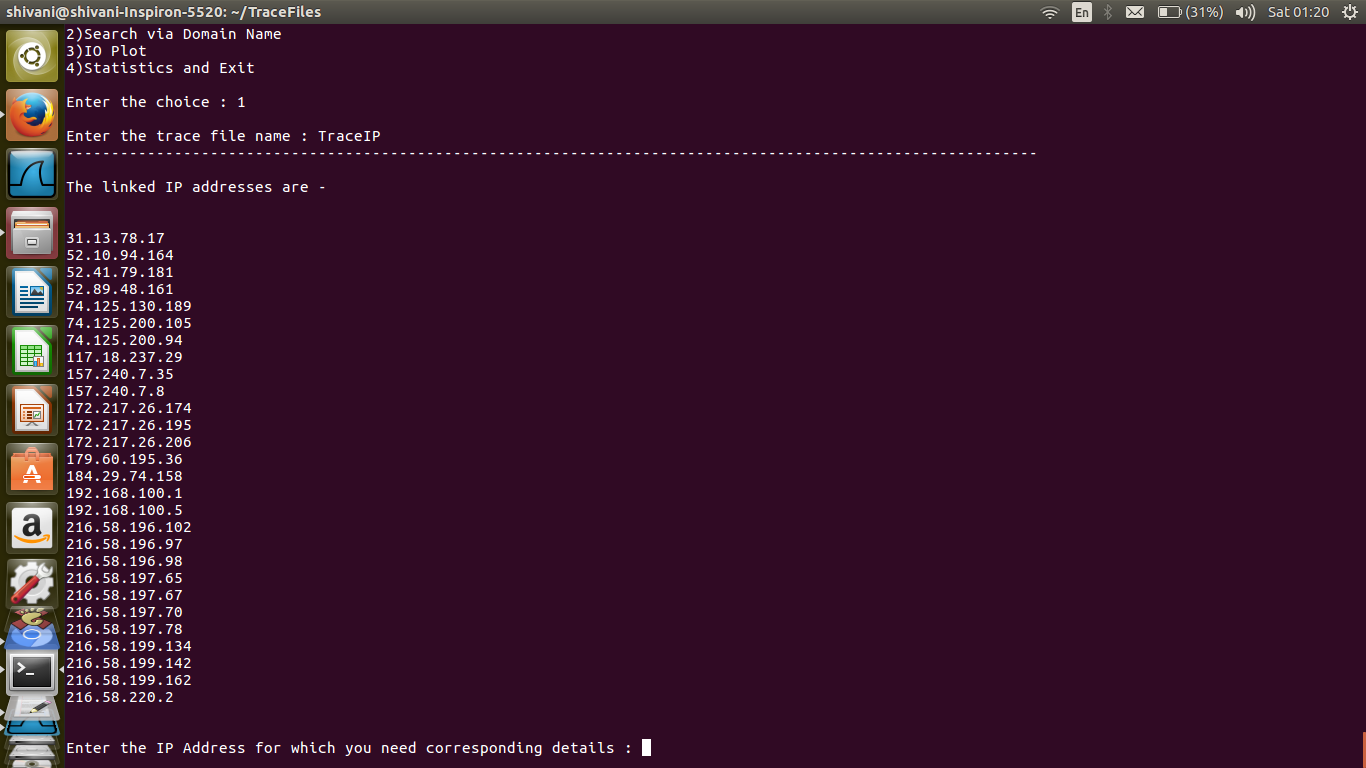


2.Displaying the trace file in text format on the terminal



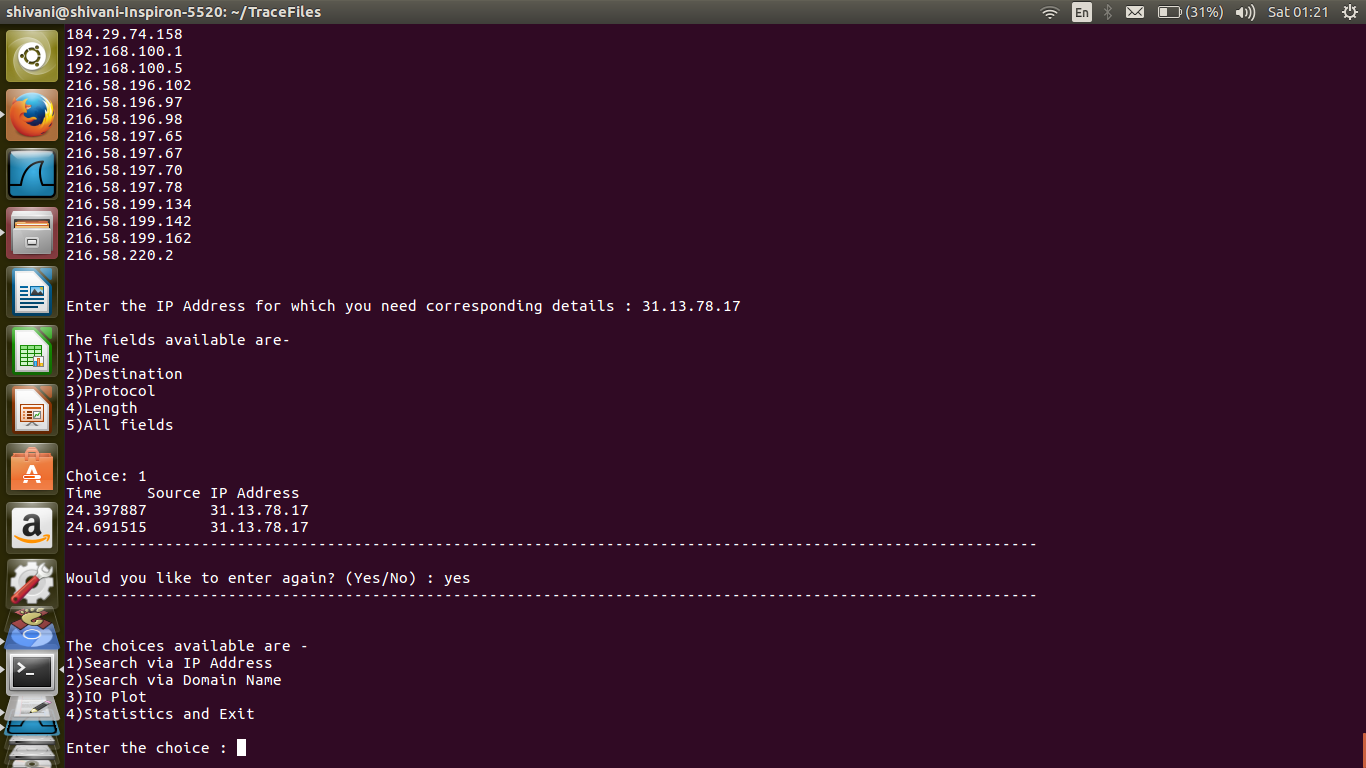
3.Menu



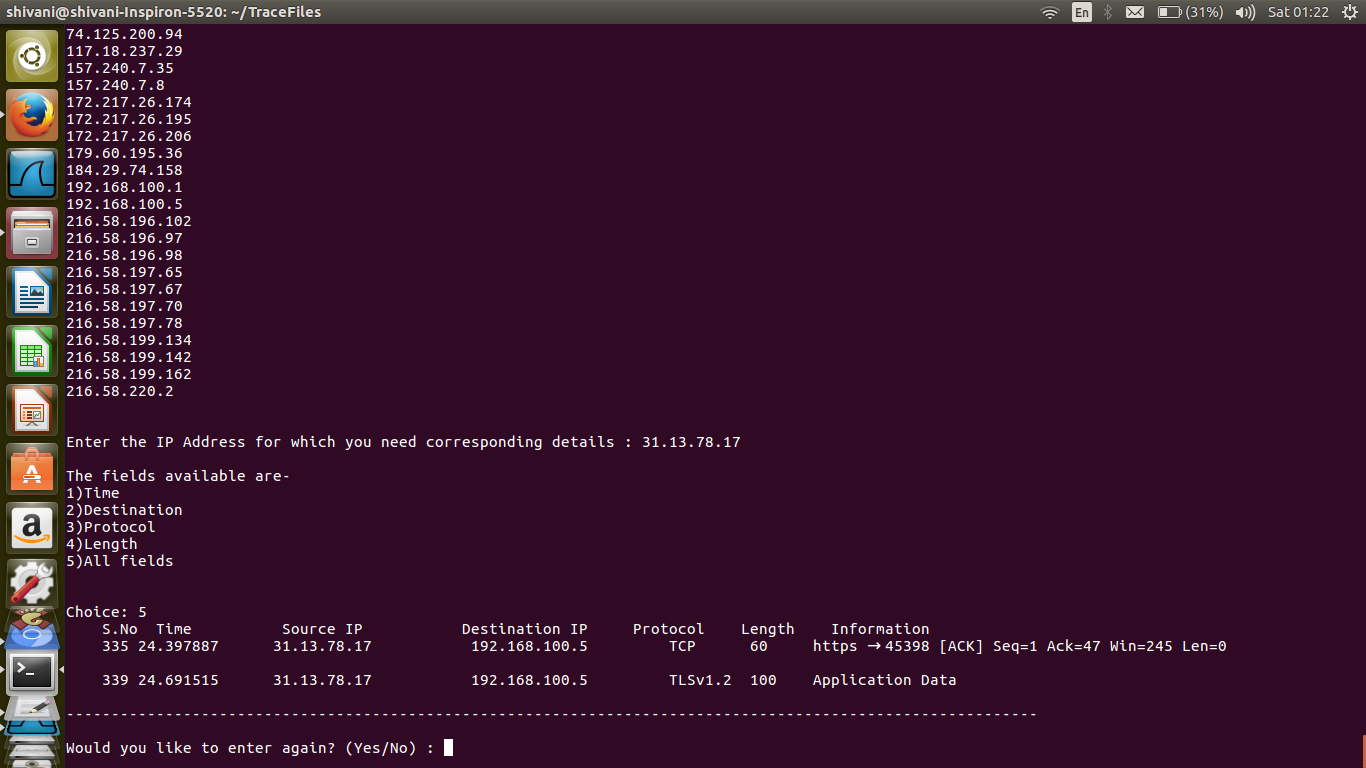
4.On choosing option “1” : “Search via IP Address”

5.Displaying different details corresponding to the entered IP Address

(i) Time:



(ii)All Field

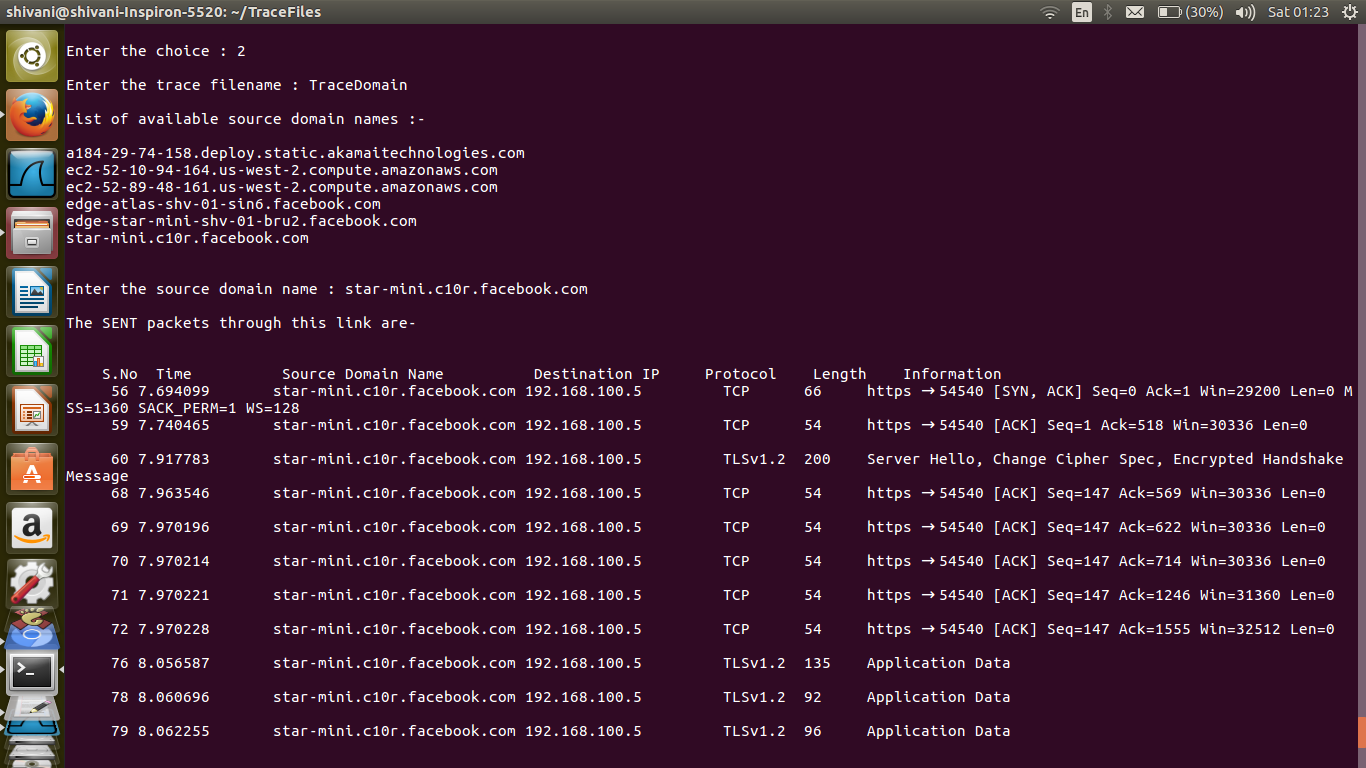


6.On choosing option ”2” : “Search via Domain Name”

(i)Searching via Source Domain Names:

->First all the availabale source domain names are displayed.

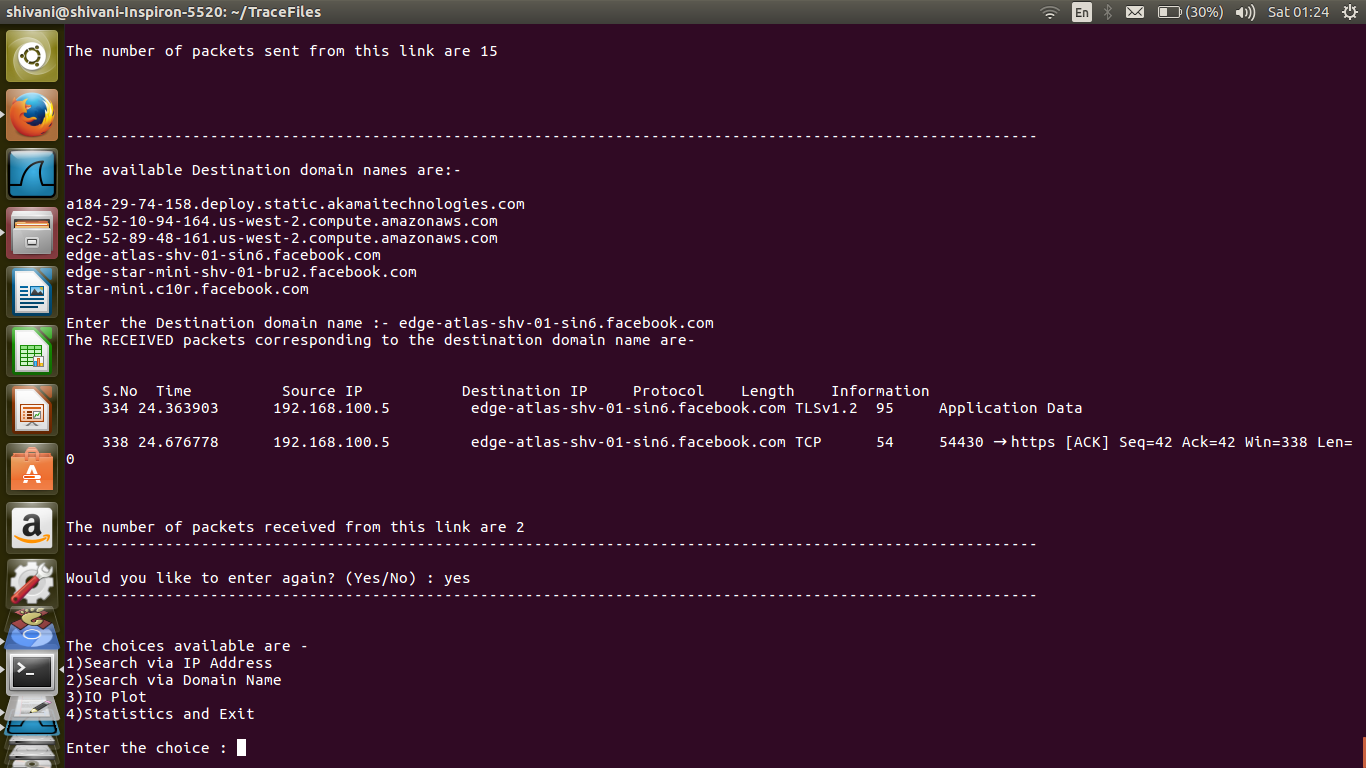
->When a particular domain name is entered all the corresponding details pertaining to that domain name are displayed as below:



(ii)Searching via Destination domain names:

->Now, it displays the available destination domain names

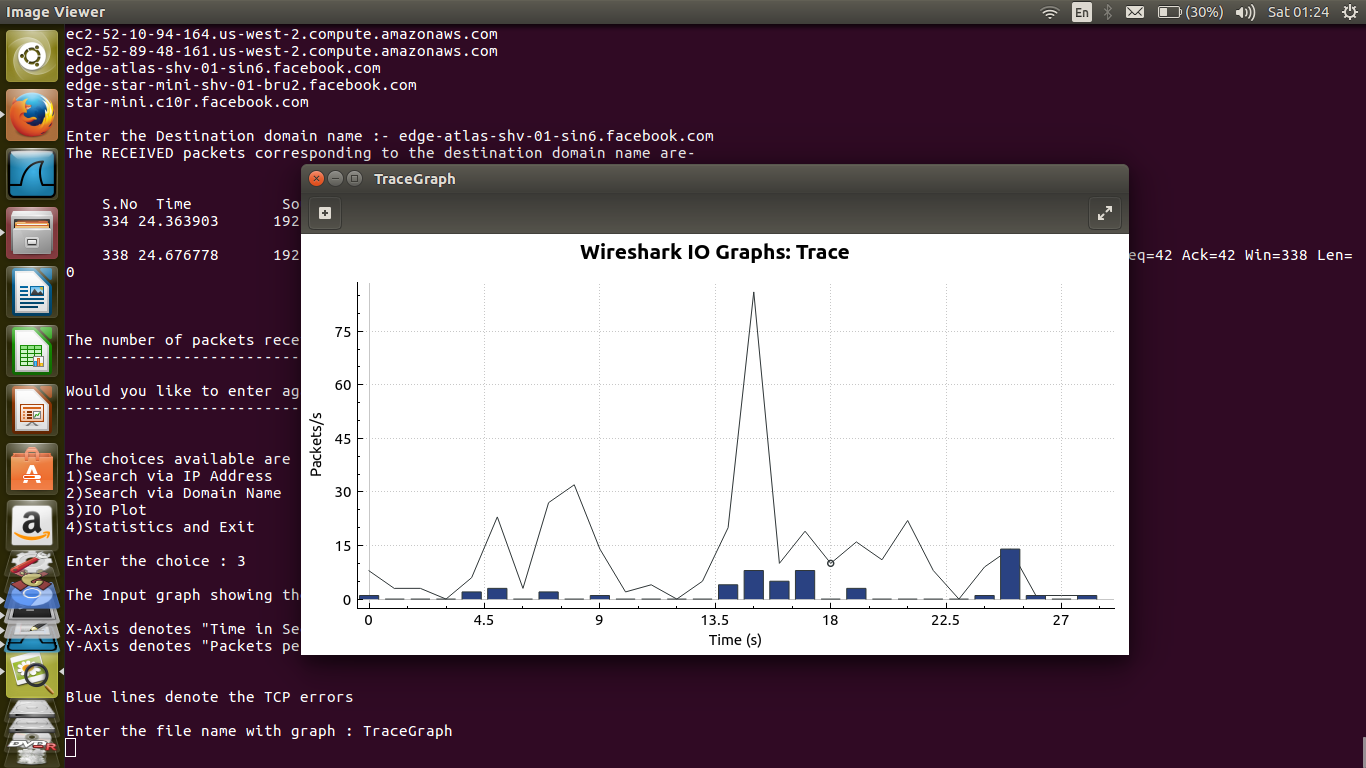
->When a particular destination domain name is entered all the corresponding details pertaining to that domain name are displayed.



7.On choosing option “3” : “Graph”

-> Displays graph depicting the No. of packets sent and received per second

->The graph also shows TCP errors (in blue) if there are any.



8.On choosing option “4” : “Statistics and Exit”

->Displays the statistics of the captured file and exits the program.

