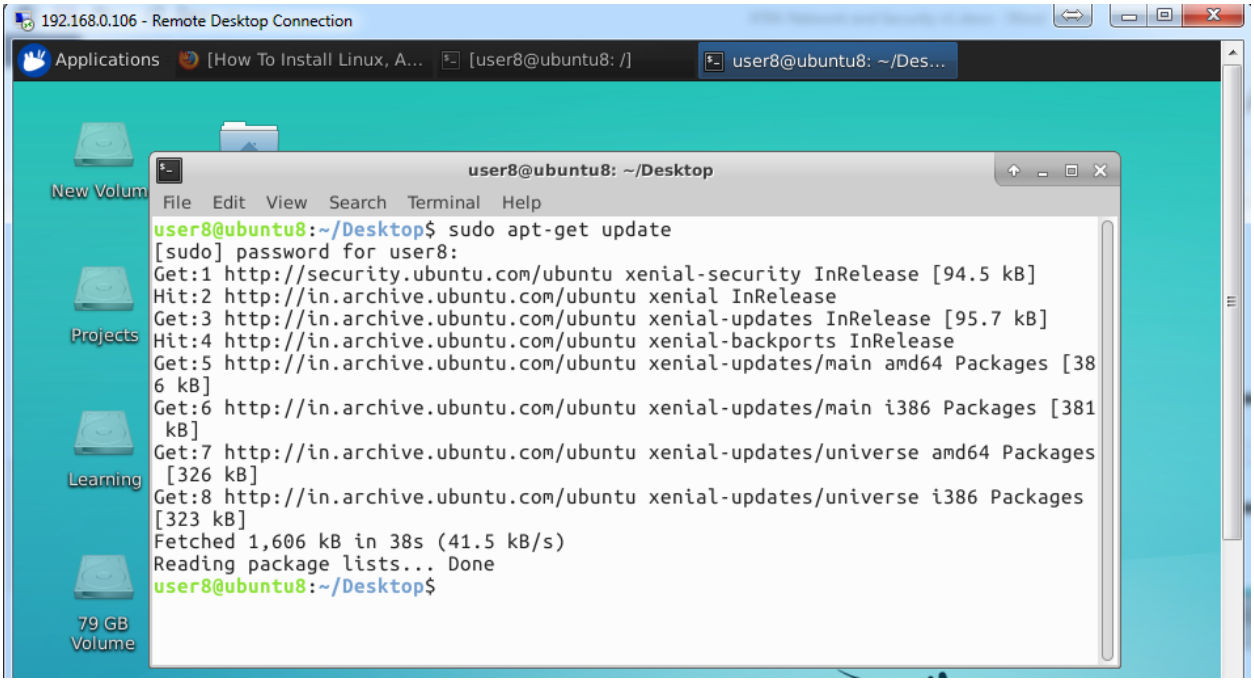
LAMP Server

LAMP is an acronym of Linux, Apache, MySQL, and PHP. The group of open source software called as LAMP, which is mainly used for getting web servers up and run. Ubuntu already run by a virtual private server. The below steps are used to described the installation of the LAMP (Kaeo, 1999).

Task-1: Web Server Configuration

Logged into the Ubuntu Server



Installation of Apache

The Apache is one of the web server software. It is implemented by Software Foundation.
In world, the apache runs in 67% of all web servers. It is secure and fast. It can meet the different environment by using extensions and modules.

It distributed the "open source" license.

The Apache implemented as compiled modules. The Graphical User Interfaces supported by Apache. Features of Apache are content negotiation and configurable error messages.

The apache supports authentication of password, authentication of digital certificate.

The open community developers are developing and maintaining Apache. It is a free and open source software. The External extension module included the popular compression methods on apache; it helps to reduce web pages size. The Apache installation allowed by virtual hosting, to serve the different websites. The web browser analyzed the apache logos by using free scripts, the free scripts are W3Perl or visitors. The multi-processing modules are provided by apache, It allows the event-hybrid modes or hybrid. The Linux operating system development is similar to Apache. Its run many operating system such as Unix-based operating system, windows, Unix-derives systems. It designed to create the web server. The Apache web server manipulating the multiple extensions. The web Hosting Companies widely using the Apache web server.

The Apache widely used by Word Press hosting providers.

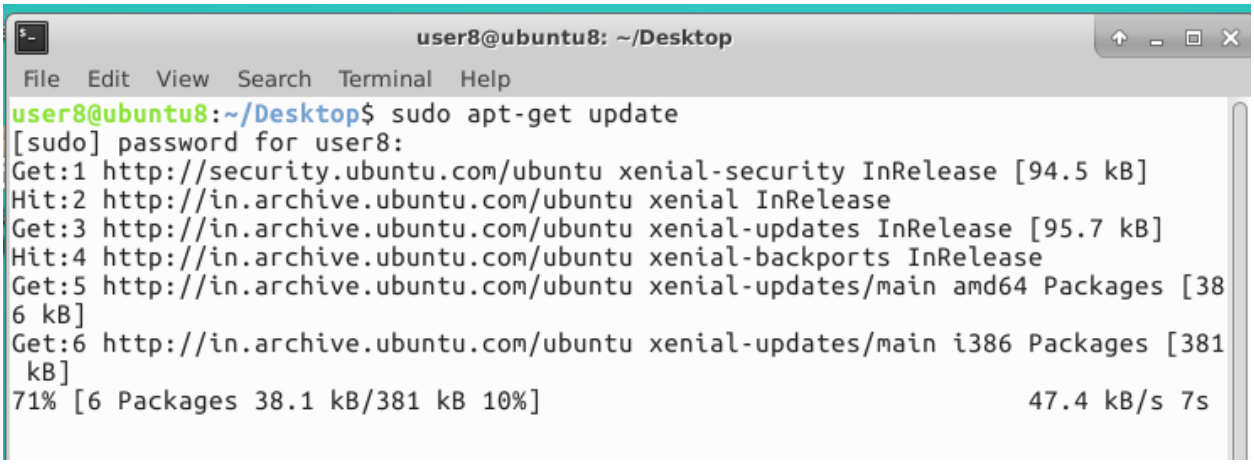
EssayCorp 5 years

This is the free and open source software. In web server, it is run in more than 50%.

For an installation of apache, open the terminal. Type the below commands in the terminal screen.

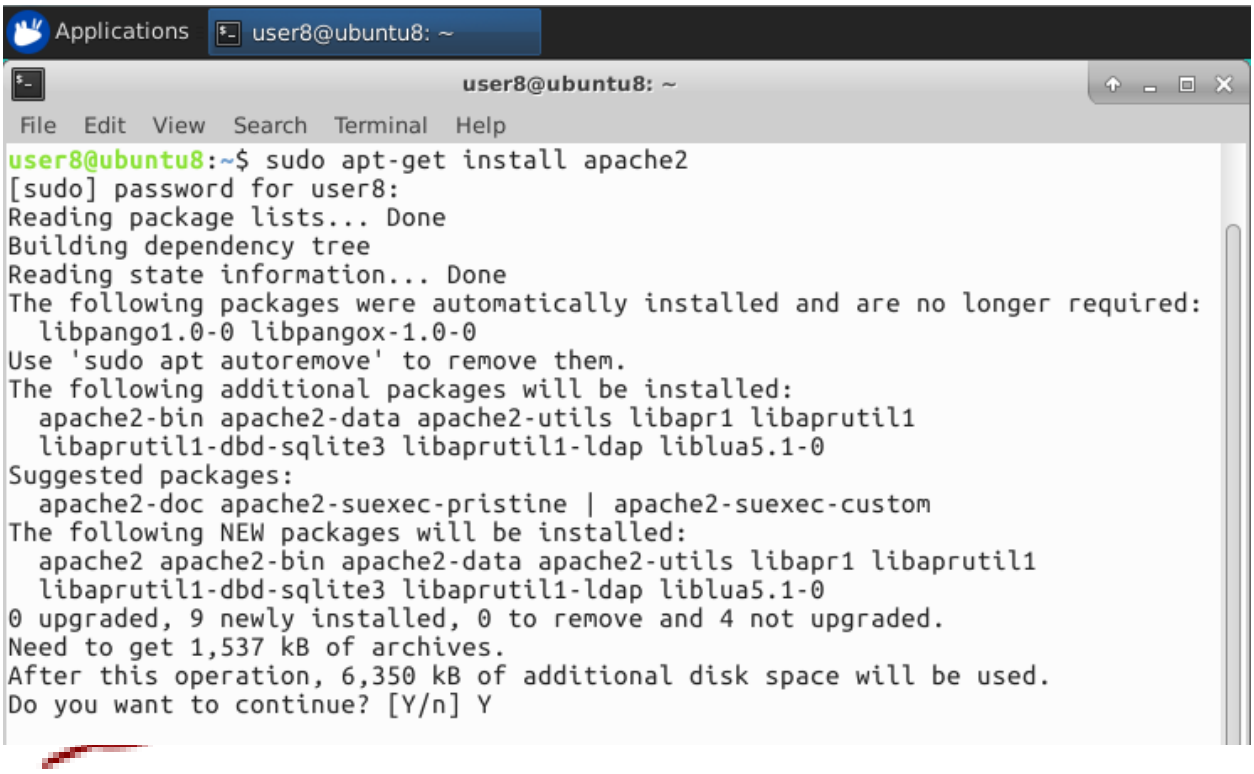
The commands are,

```
sudo apt-get update
```

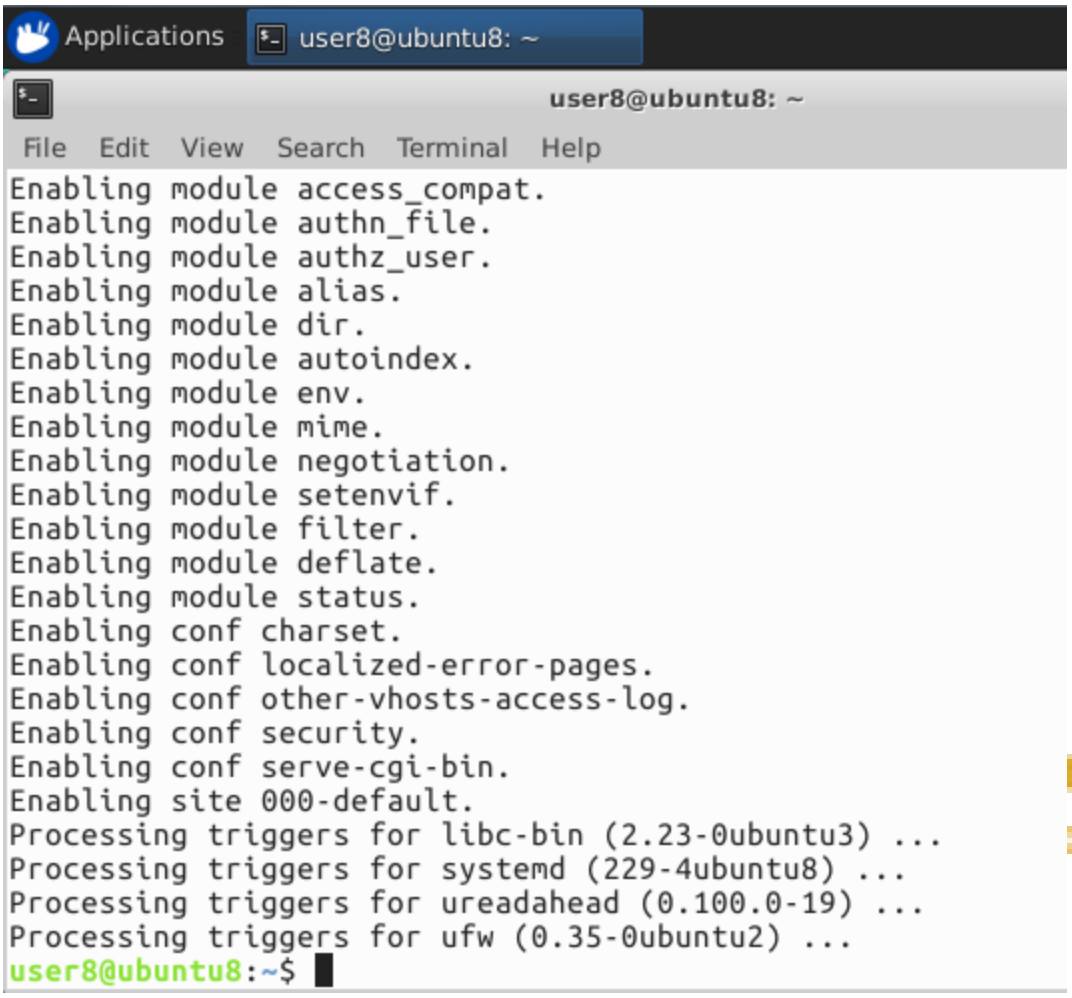


```
sudo apt-get install apache2
```

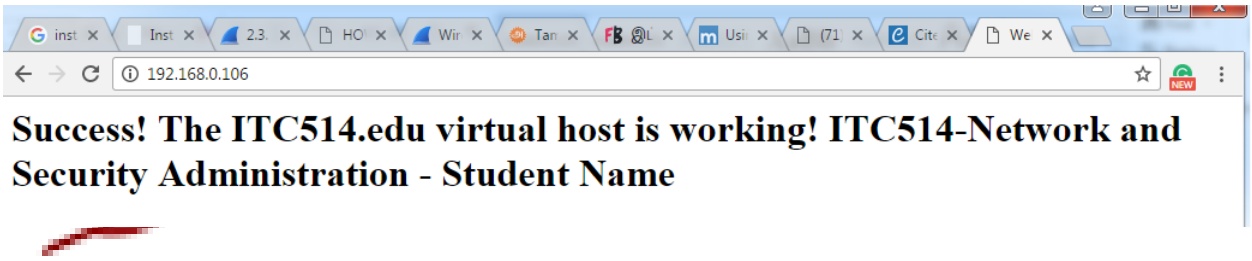
Got the following, asking for confirmation.



Apache is installed successfully.



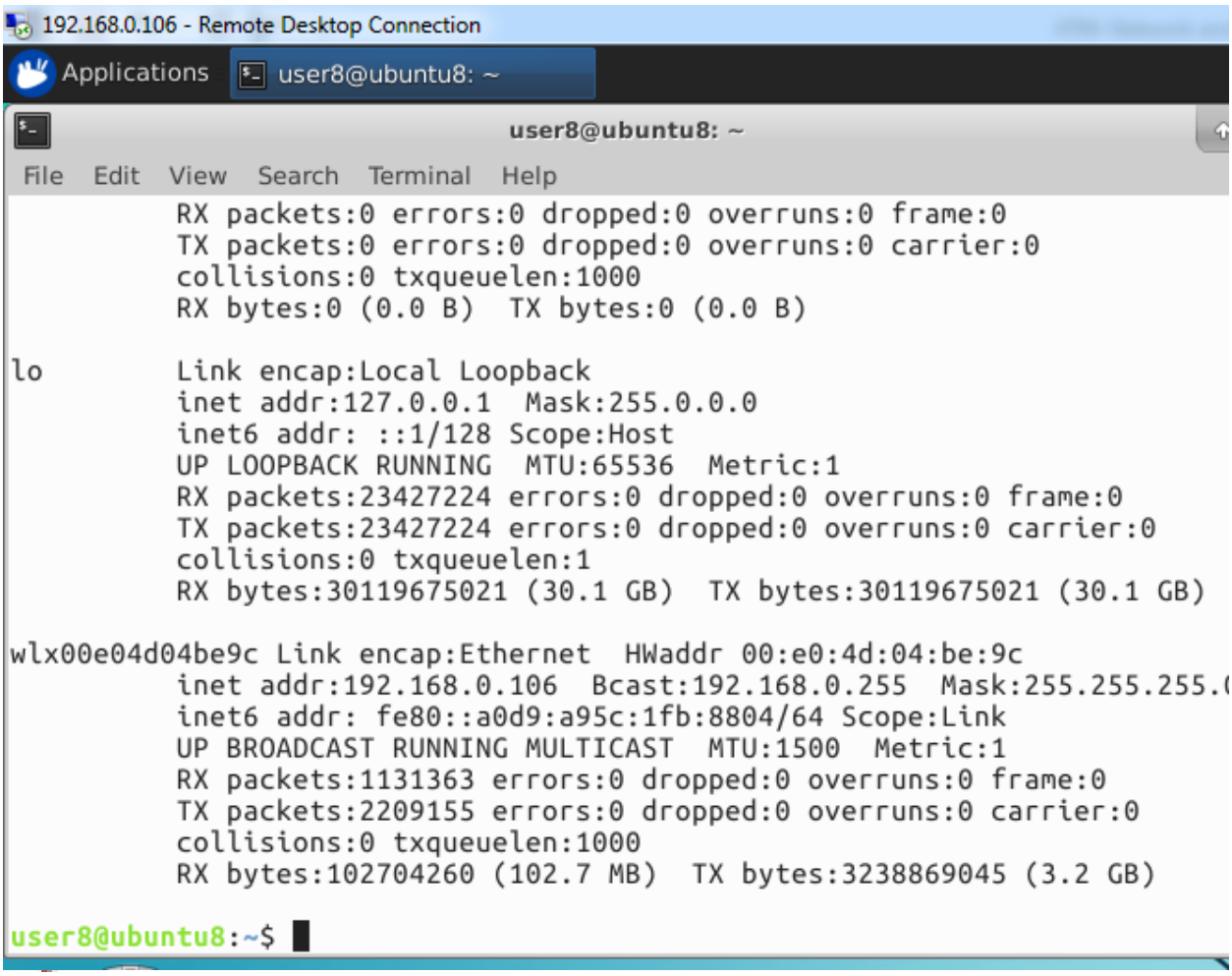
For checking the apache is installed or not, give servers IP address in the browser (http://192.168.0.106).It will display the command (Works) on the page.



Servers IP address

Using this below command users can acknowledge the servers IP address

sudo ifconfig



Apache restarted to implment the changes.

Installation of MySQL

It is a rational database Management System in which information's are stored as Tables. it is used for web development application. It is owned by Oracle corp.it is running as the back-end database in some popular websites like Wikipedia, Google and Facebook. It has the following features, Cross platform support,triggers,cursors,information schemas' support, Built-in Replication support, Query catching. MySQL dump used as a logical backup tool with community and enterprise editions.

MySQL Workbench is used as the official integrated environment of MySQL. By using MySQL we can do the operations such as creation, deletion, update and Modifications in the database. It is a fast, easy to use RDBMS used for big and small businesses. It is developed, marketed and supported by MySQL .It is released under an open source license so we can use it by free of cost. It uses slandered form of SQL data language. It can be used in many operating systems and languages such as PHP, PERL, C, C++, JAVA, etc. It works well even with large database. It can be customized by programmers to fit for their own specific environment. It supports Novell cluster Services. It supports several development interfaces such as JDBC, ODBC, PHP, and PERL. It is scalable, so we can increase the theoretical limitation of data. This system is mainly used to organize and retrieve the data. It is a more powerful DB system. For an installation of MySQL, open the terminal. Type the below commands in the terminal screen. The commands are,

```
sudo apt-get install mysql-server libapache2-mod-auth-mysql php5-mysql
```

EssayCorp

Root password will be asked by the MySQL while installing the program. If the users not giving the password after some time set the password in MySQL shell.

After installation of MySQL run this command in the terminal screen

```
sudo mysql_install_db
```

To finish the MySQL running give this command script

```
sudo /usr/bin/mysql_secure_installation
```

To setup the current root password

Enter current password for root (enter for none):

OK, successfully used password, moving on...

If users want to change this password, give N and go to the other steps

End of the process MySQL will be reloaded and implement the new thing changes.

Finished the installation process.

Installation of PHP

PHP is an acronym of Hypertext Pre-processor, which is open source scripting language embedded in HTML. It is widely used for managing the dynamic content, e-commerce sites and session tracking. It is a free download scripting language which is integrated with MySQL, Oracle, Informix and etc. It also supports many protocols like IMAP, LDAP, and POP3.It also supports many protocols like IMAP, LDAP and POP3.

For an installation of apache, open the terminal. Type the below commands in the terminal screen.

The commands are,

```
sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt
```

After giving yes command PHP installed by itself.

Adding PHP to the directory index, which is very useful.

sudo nano /etc/apache2/mods-enabled/dir.conf

In index file add the index.php. It shows like this

<IfModule mod_dir.c>

DirectoryIndex index.php index.html index.cgi index.pl index.php index.xhtml index.htm

</IfModule>

Modules in PHP:

In virtual server add modules and libraries. After that see the available libraries list

apt-cache search php5-

List of possible modules displyed by the terminal screen

php5-cgi - server-side, HTML-embedded scripting language (CGI binary)

php5-cli - command-line interpreter for the php5 scripting language

php5-common - Common files for packages built from the php5 source

php5-curl - CURL module for php5

php5-dbg - Debug symbols for PHP5

php5-dev - Files for PHP5 module development

php5-gd - GD module for php5

php5-gmp - GMP module for php5

php5-ldap - LDAP module for php5

php5-mysql - MySQL module for php5

php5-odbc - ODBC module for php5

php5-pgsql - PostgreSQL module for php5

php5-pspell - pspell module for php5

php5-recode - recode module for php5

php5-snmp - SNMP module for php5

php5-sqlite - SQLite module for php5

php5-tidy - tidy module for php5

php5-xmlrpc - XML-RPC module for php5

php5-xsl - XSL module for php5

php5-adodb - Extension optimising the ADOdb database abstraction library

php5-auth-pam - A PHP5 extension for PAM authentication

For installing the module type use this below command

sudo apt-get install name of the module

Congrats! Users successfully installed the LAMP on the droplet.

To see the PHP ON USERS SERVER

To create a new document or file give the below command

sudo nano /var/www/info.php

Also, add the below lines

```
<?php
phpinfo();
?>
```

Save and click exit.

After this restart the apache for taking the new changes.

```
sudo service apache2 restart
```

After finishing it, visit the PHP info page, which is http://192.168.0.106/info.php.

Task-2: Enabling SSL in webserver

SSL Certificate

Transport layer Security (TLS), Secure Socket Layer (SSL) are protocols which is used to create encrypted wrapper and normal traffic in a protected way. They are used to validate and identify the domains and servers through internet by certificate authority of the genuine server.

Create a sample domain with a sample website.

Domain name assumed is itc514.edu

Create the directory structure

```
sudo mkdir –p /var/www/itc514.edu/public_html
```

EssayCorp

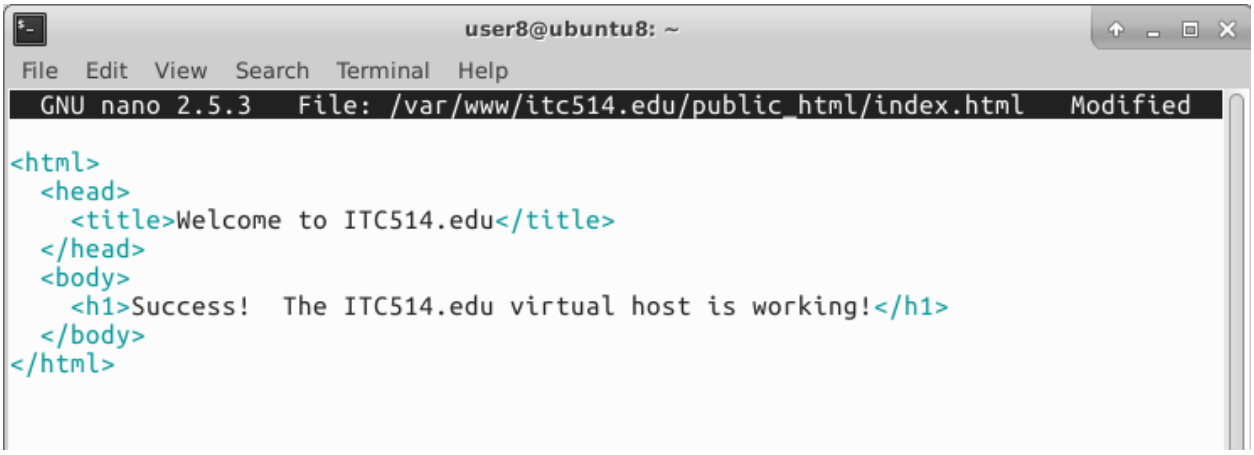
Required permissions granted

```
Sudo chown –R $USER:$USER  /var/www/itc514.edu/public_html
```

The index file is located in /var/www/itc514.edu/public_html

In the above address itc514.edu is created by me.

Changed the index file and added ITC514.edu key word. Checked the html page in local browser and ensured that HTML page is working fine. Moved the index.html file to the default location of the itc514.edu domain.

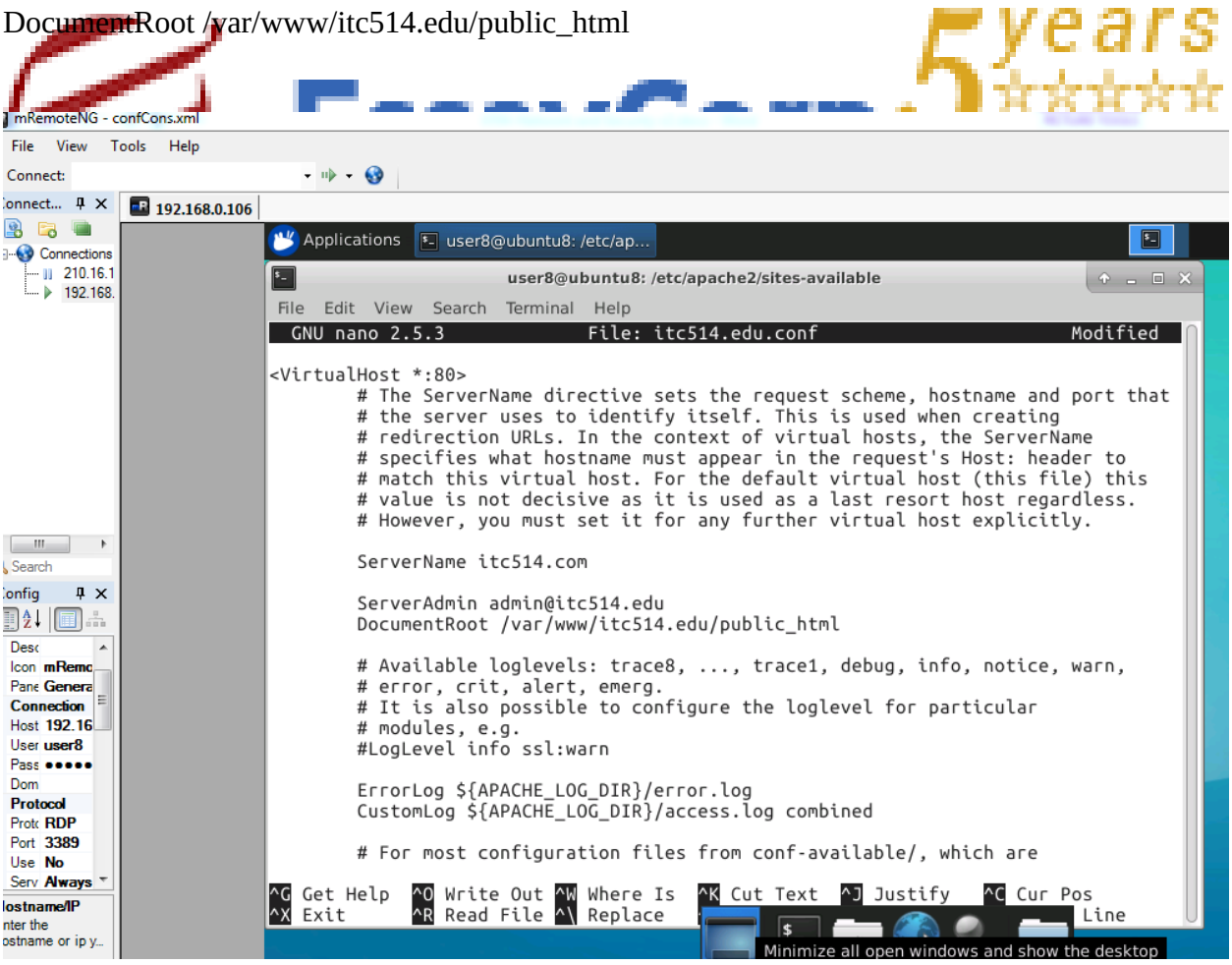


Opened /etc/apache2/sites-available location and changed the itc514.edu.conf file as shown below.

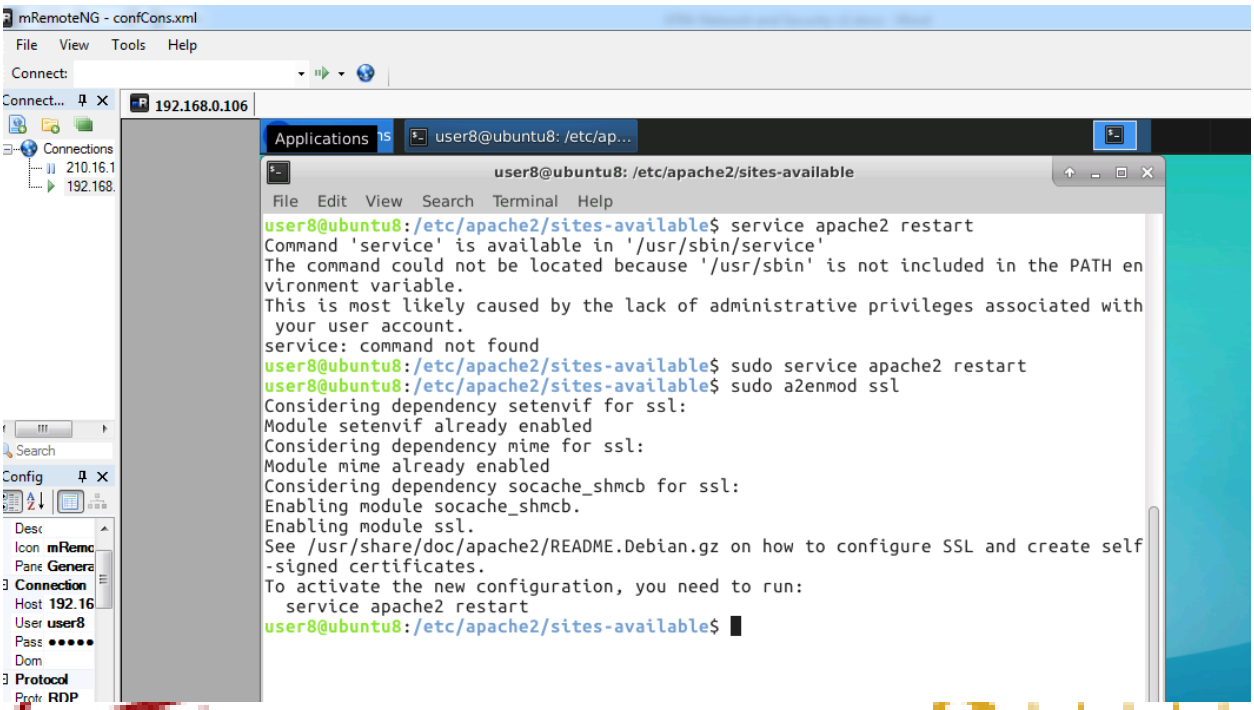
Server Name is itc514.com

ServerAdmin admin@itc514.edu

DocumentRoot /var/www/itc514.edu/public_html



Restarted apache2



EssayCorp

Installed MySQL and PHP too. Later I can test my website with any of the web application if necessary.

```
user8@ubuntu8: ~
File  Edit  View  Search  Terminal  Help
Package php5-mysql is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

E: Unable to locate package libapache2-mod-auth-mysql
E: Package 'php5-mysql' has no installation candidate
user8@ubuntu8:~$ sudo systemctl restart apache2
user8@ubuntu8:~$ sudo mkdir -p /var/www/example.com/public_html
user8@ubuntu8:~$ sudo mkdir -p /var/www/example.com/public_html
user8@ubuntu8:~$ sudo mkdir -p /var/www/itc514.edu/public_html
user8@ubuntu8:~$ sudo chown -R $USER:$USER /var/www/itc514.edu/public_html
user8@ubuntu8:~$ sudo chmod -R 755 /var/www
user8@ubuntu8:~$ nano /var/www/itc514.edu/public_html/index.html
user8@ubuntu8:~$ sudo cp /etc/apache2/sites-available/000-default.conf /etc/apac
he2/sites-available/itc514.edu.conf
user8@ubuntu8:~$ nano /etc/apache2/sites-available/itc514.edu.conf
user8@ubuntu8:~$ sudo nano /etc/apache2/sites-available/itc514.edu.conf
[sudo] password for user8:
user8@ubuntu8:~$ sudo a2ensite itc514.edu.conf
Enabling site itc514.edu.
To activate the new configuration, you need to run:
  service apache2 reload
user8@ubuntu8:~$ sudo service apache2 reload
user8@ubuntu8:~$
```

EssayCorp


```
user8@ubuntu8: ~
File  Edit  View  Search  Terminal  Help
Package php5-mysql is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

E: Unable to locate package libapache2-mod-auth-mysql
E: Package 'php5-mysql' has no installation candidate
user8@ubuntu8:~$ sudo systemctl restart apache2
user8@ubuntu8:~$ sudo mkdir -p /var/www/example.com/public_html
user8@ubuntu8:~$ sudo mkdir -p /var/www/example.com/public_html
user8@ubuntu8:~$ sudo mkdir -p /var/www/itc514.edu/public_html
user8@ubuntu8:~$ sudo chown -R $USER:$USER /var/www/itc514.edu/public_html
user8@ubuntu8:~$ sudo chmod -R 755 /var/www
user8@ubuntu8:~$ nano /var/www/itc514.edu/public_html/index.html
user8@ubuntu8:~$ sudo cp /etc/apache2/sites-available/000-default.conf /etc/apac
he2/sites-available/itc514.edu.conf
user8@ubuntu8:~$ nano /etc/apache2/sites-available/itc514.edu.conf
user8@ubuntu8:~$ sudo nano /etc/apache2/sites-available/itc514.edu.conf
[sudo] password for user8:
user8@ubuntu8:~$ sudo a2ensite itc514.edu.conf
Enabling site itc514.edu.
To activate the new configuration, you need to run:
  service apache2 reload
user8@ubuntu8:~$ sudo service apache2 reload
user8@ubuntu8:~$
```

Restarted apache service. Tested the website from a client with IP 192.168.0.106 and got the following page.

The above page proved that apache, web page creation, web page location all are fine and working.

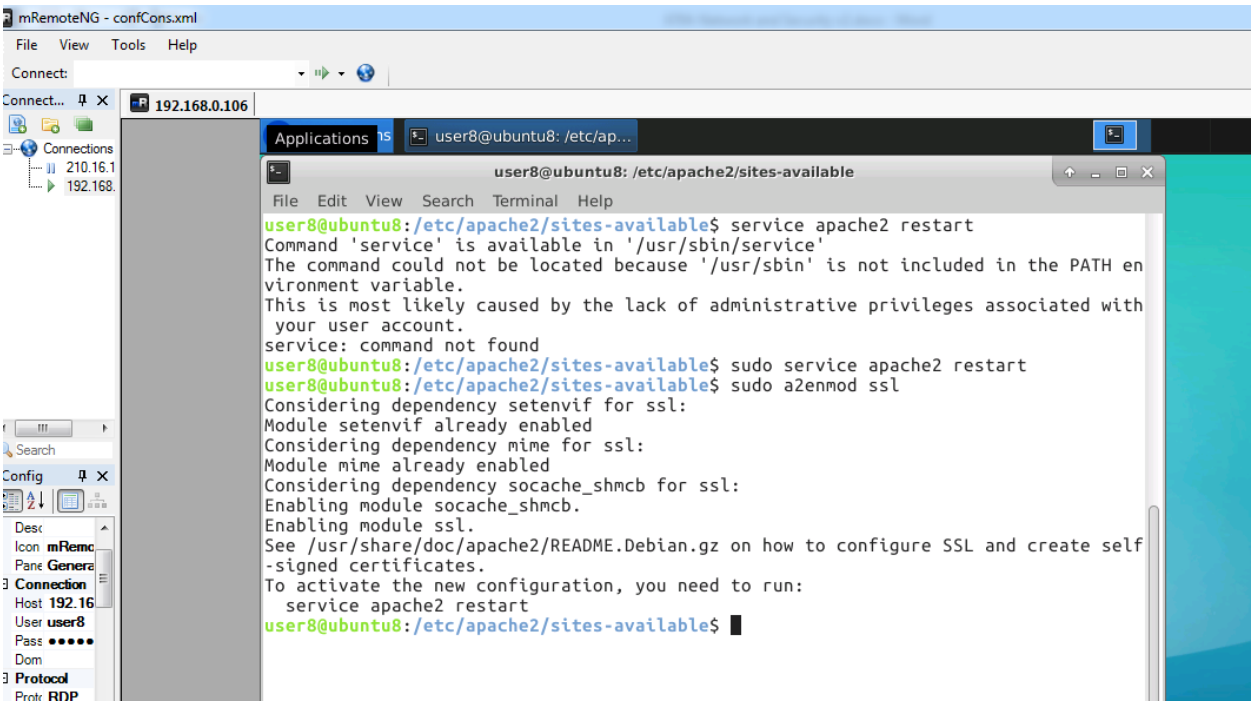
SSL Module Activation

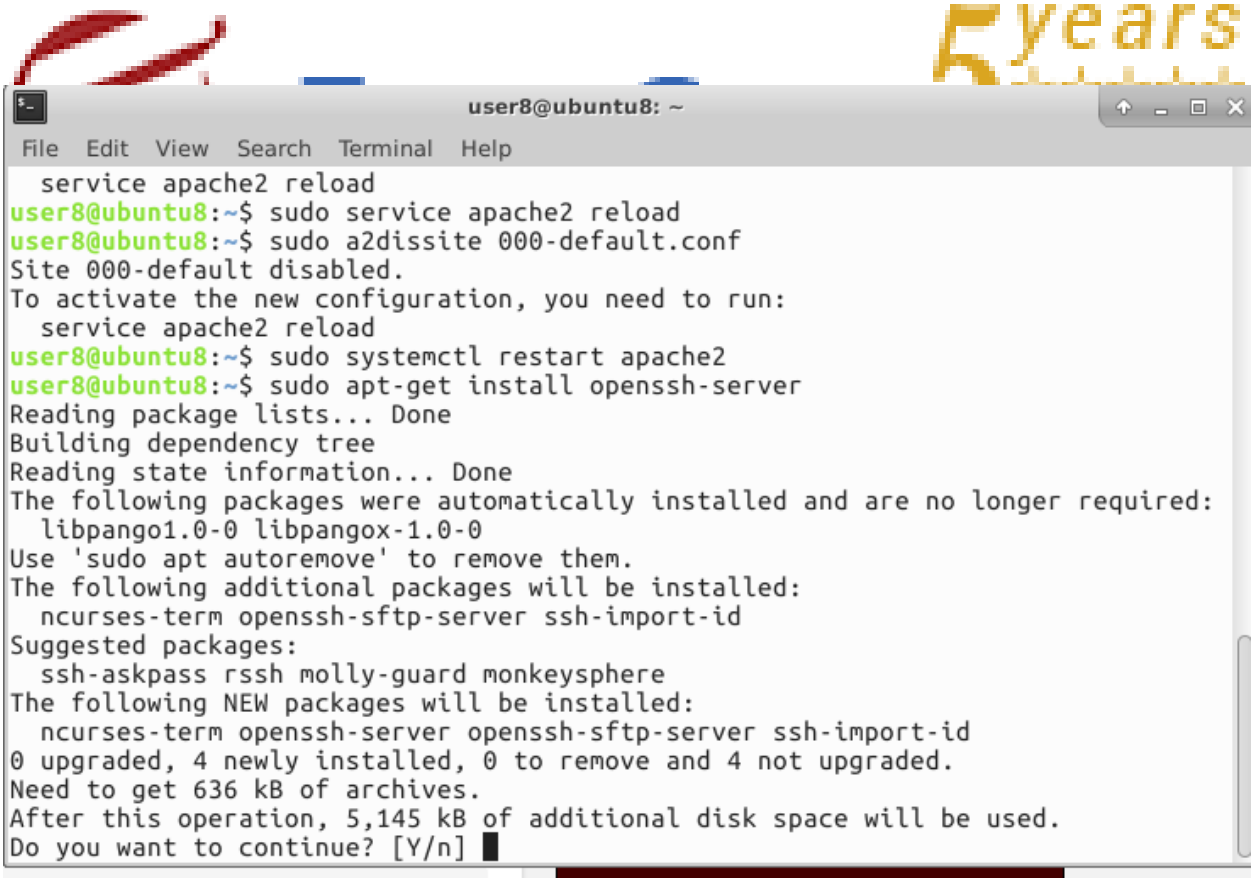
Enable Ubuntu 16.04 Apache Package by using the following commands to get the advantages of SSL system (Katz and Yung, 2007). Restarted apache2 service once and enabled SSL with the following command.

```
sudo a2enmod ssl
```

Restart the web server by using following commands to get the features of SSL.

```
sudo service apache2 restart
```


mRemoteNG - confCons.xml
File View Tools Help
Connect:
192.168.0.106
Applications
user8@ubuntu8: /etc/ap...
user8@ubuntu8: /etc/apache2/sites-available
File Edit View Search Terminal Help
user8@ubuntu8:/etc/apache2/sites-available$ service apache2 restart
Command 'service' is available in '/usr/sbin/service'
The command could not be located because '/usr/sbin' is not included in the PATH environment variable.
This is most likely caused by the lack of administrative privileges associated with your user account.
service: command not found
user8@ubuntu8:/etc/apache2/sites-available$ sudo service apache2 restart
user8@ubuntu8:/etc/apache2/sites-available$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
service apache2 restart
user8@ubuntu8:/etc/apache2/sites-available$

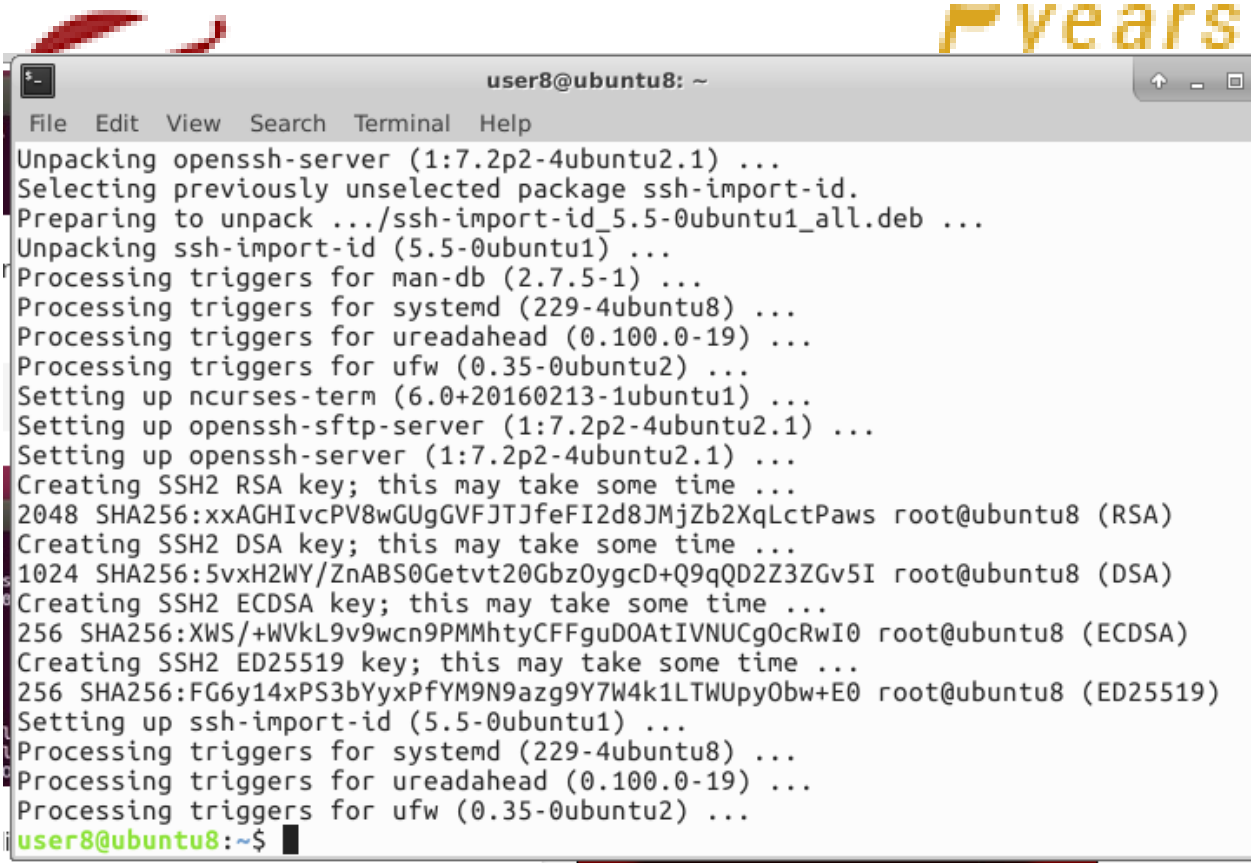

user8@ubuntu8: ~
File Edit View Search Terminal Help
service apache2 reload
user8@ubuntu8:~$ sudo service apache2 reload
user8@ubuntu8:~$ sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
service apache2 reload
user8@ubuntu8:~$ sudo systemctl restart apache2
user8@ubuntu8:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
libpango1.0-0 libpangox-1.0-0
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
ssh-askpass rssh molly-guard monkeysphere
The following NEW packages will be installed:
ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 4 not upgraded.
Need to get 636 kB of archives.
After this operation, 5,145 kB of additional disk space will be used.
Do you want to continue? [Y/n]

Enabled firewall to allow SSH from the server with the command

Sudo ufw allow in “Apache Full”

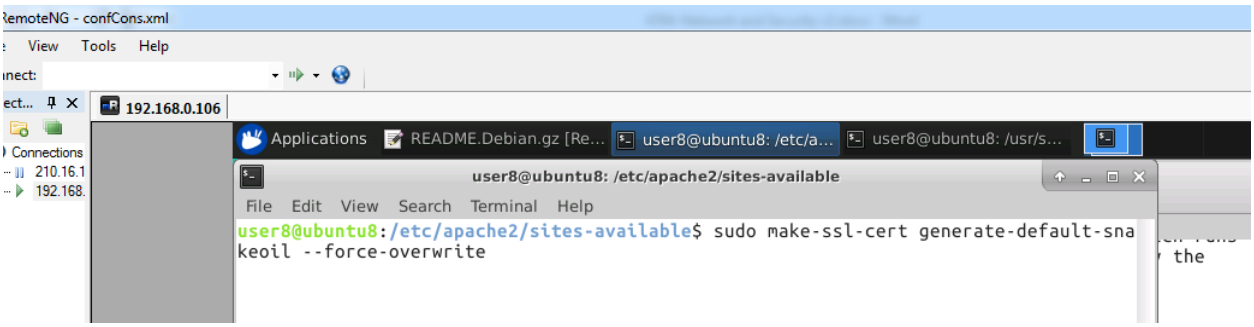
```
user8@ubuntu8:/etc$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
  OpenSSH
user8@ubuntu8:/etc$ sudo ufw allow in "Apache Full"
Rules updated
Rules updated (v6)
user8@ubuntu8:/etc$
```

Wanted to run the server from nearby client using putty through SSH2 protocol and hence installed **openssh-server**



Created a self-signed SSL certificate with the help of the make-ssl-cert command. It is created successfully.

Self-Signed SSL Certificate Creation



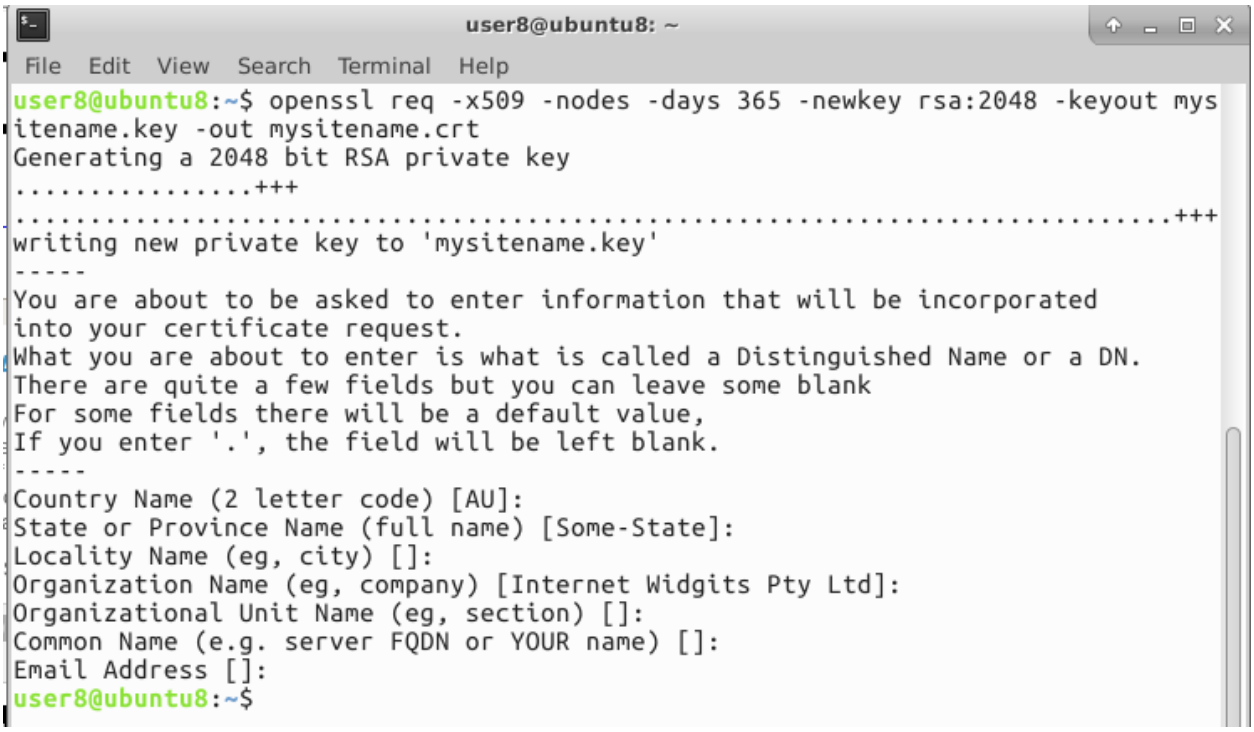
To Store our certificate files in Apache, create a subdirectory by using the following Command.

```
sudo mkdir /etc/apache2/ssl
```

Create a location by using following commands, To Store our Certificate and Keys.

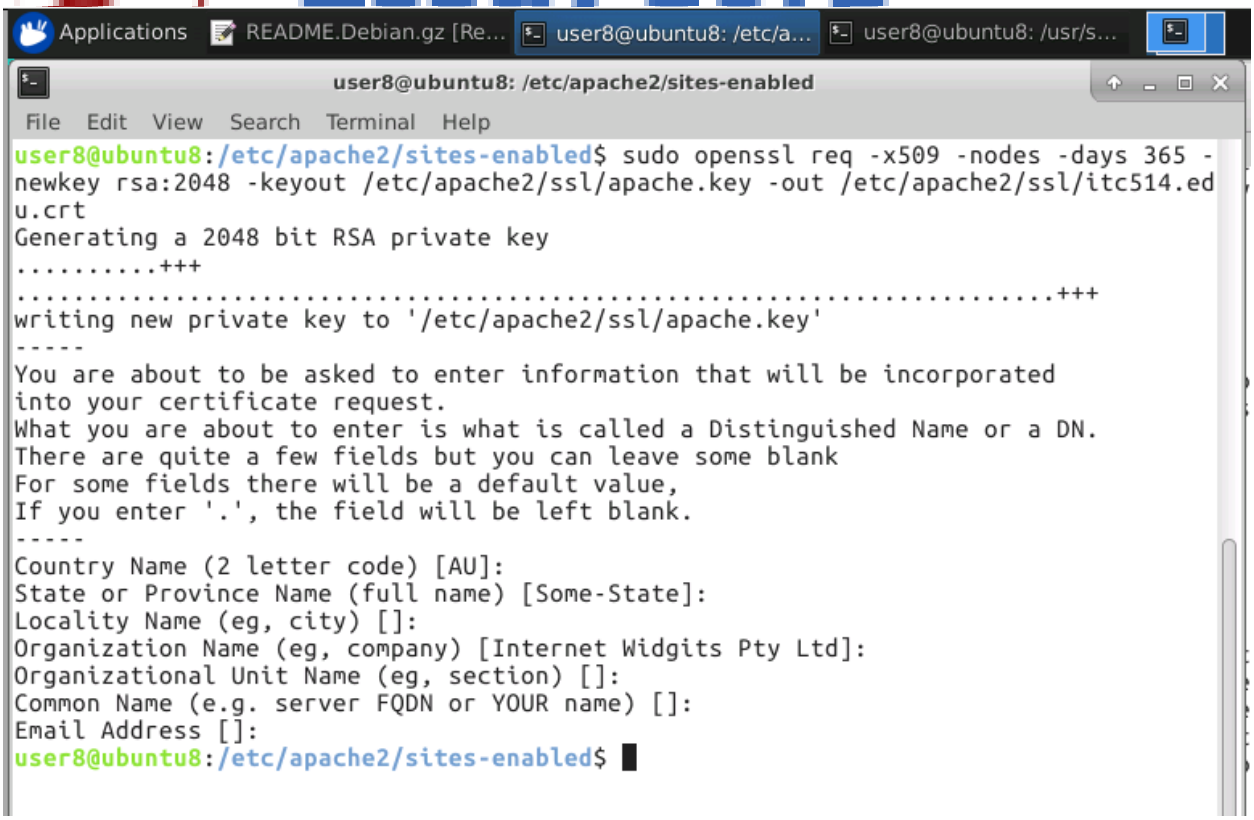
```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
```

This certificate is valid for 1 year. It is a RSA 2048 strength. Apache key will be stored in /etc/apache2/ssl location and the apache certificate will be stored in /etc/apache2/ssl location. Ensured that both are generated and stored.

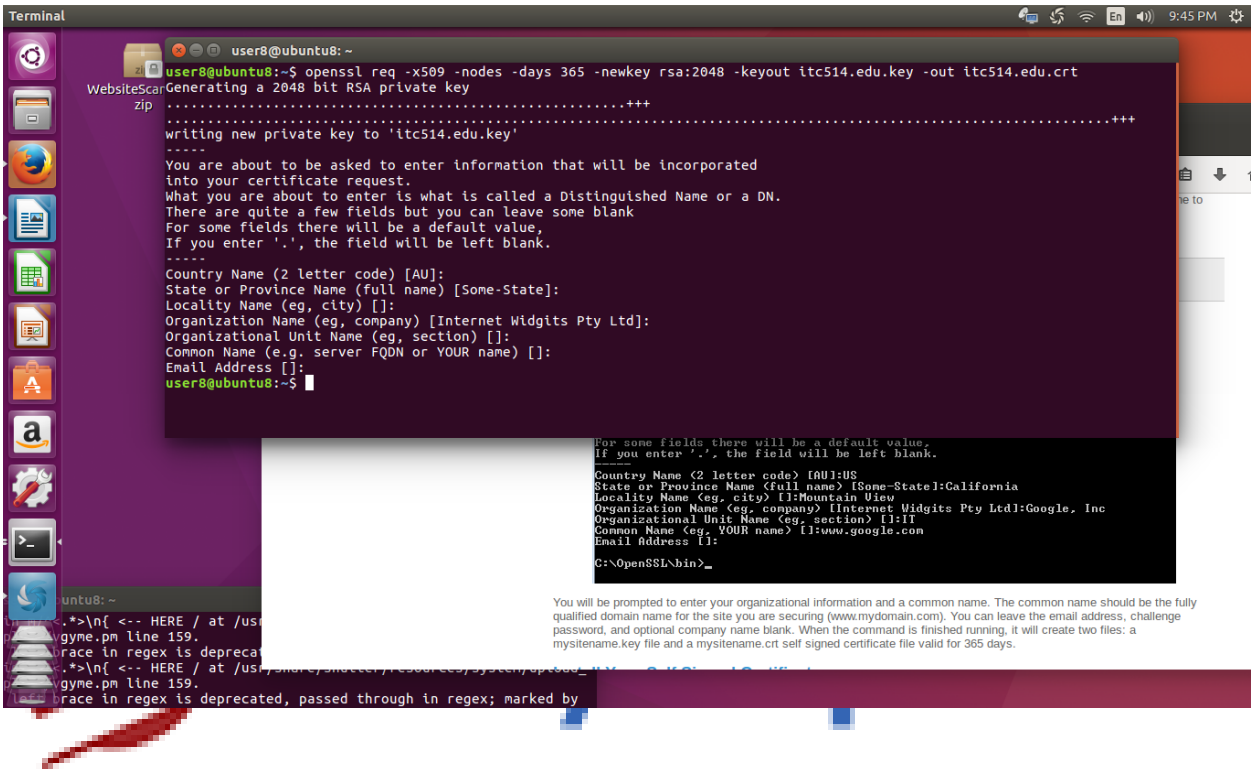


The above key creation is a sample key and sample certificate only. The key and certificate for itc514.edu is created below. The below screen is done in the target SSL webserver (192.168.0.106).

EssayCorp 5 years



The following command is run from the client through remote desktop connection. The server is configured with remote desktop allow permission. Now both key and certificate are created for itc514.edu



Configuration of Apache

Configure Apache to use files of our key and certificate in virtual host file.

To get the default configuration of SSL by typing following commands

sudo nano /etc/apache2/sites-available/default-ssl.conf

The Files looks as follows, when the commands are removed,

<IfModule mod_ssl.c>

<VirtualHost _default_:443>

ServerAdmin webmaster@localhost

DocumentRoot /var/www/html

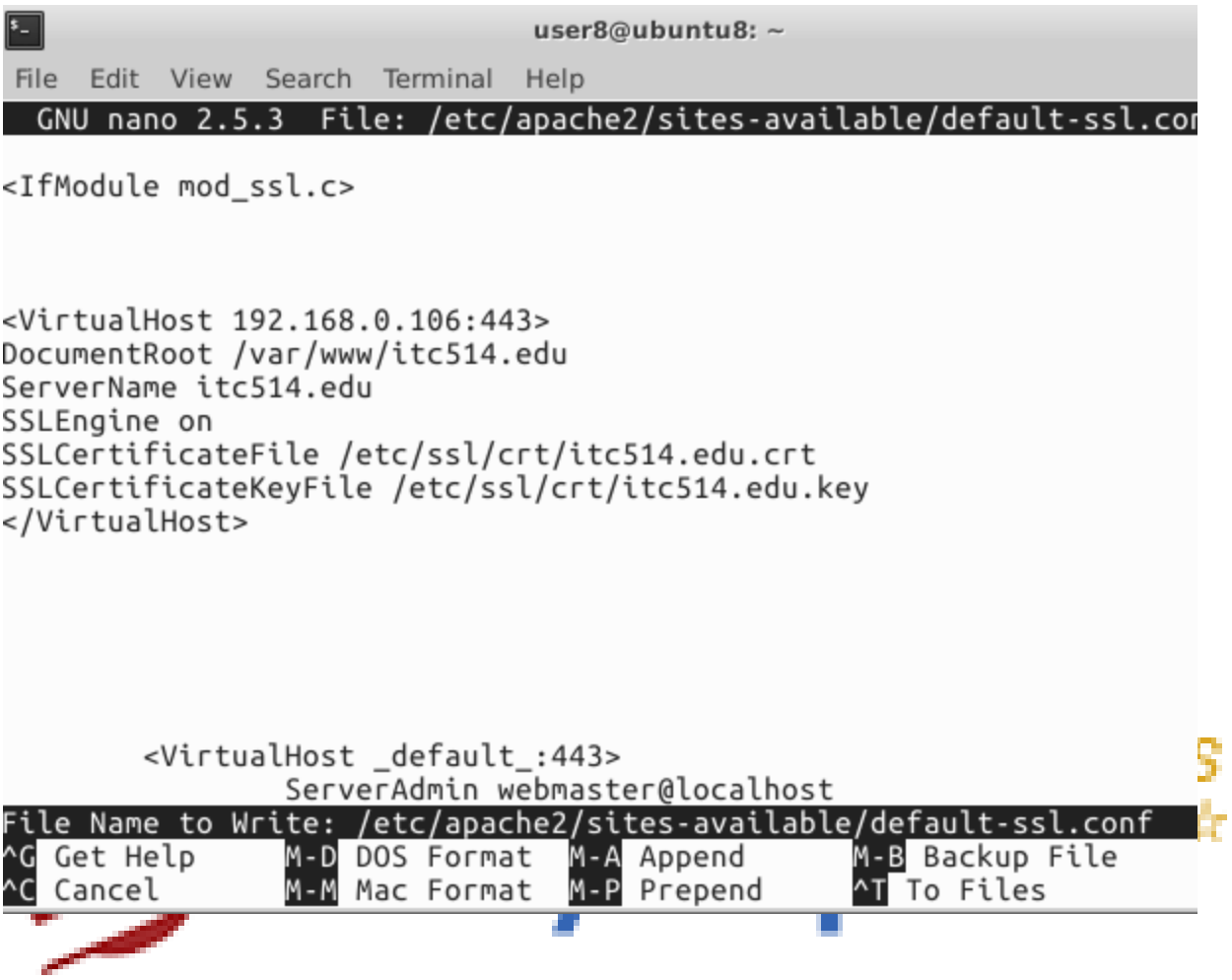
ErrorLog ${APACHE_LOG_DIR}/error.log

```
CustomLog ${APACHE_LOG_DIR}/access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
<FilesMatch "\.(cgi|shtml|phtml|php)$">
SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
SSLOptions +StdEnvVars
</Directory>
BrowserMatch "MSIE [2-6]" \
nokeepalive ssl-unclean-shutdown \
downgrade-1.0 force-response-1.0
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
</IfModule>
```

EssayCorp 5 years

The file default-ssl.conf is configured for the SSL site hosted at 192.168.0.106 and the operating port is 443.

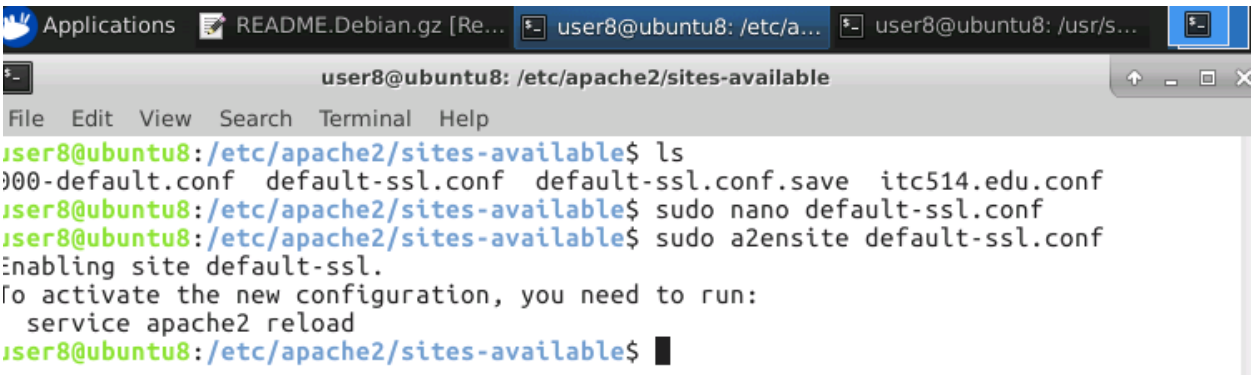
Initially the certificate file location and key location are configured wrongly to test the SSL setup.



SSL Virtual Host Activation

Enabled Virtual host of SSL by typing:

```
sudo a2ensite default-ssl.conf
```

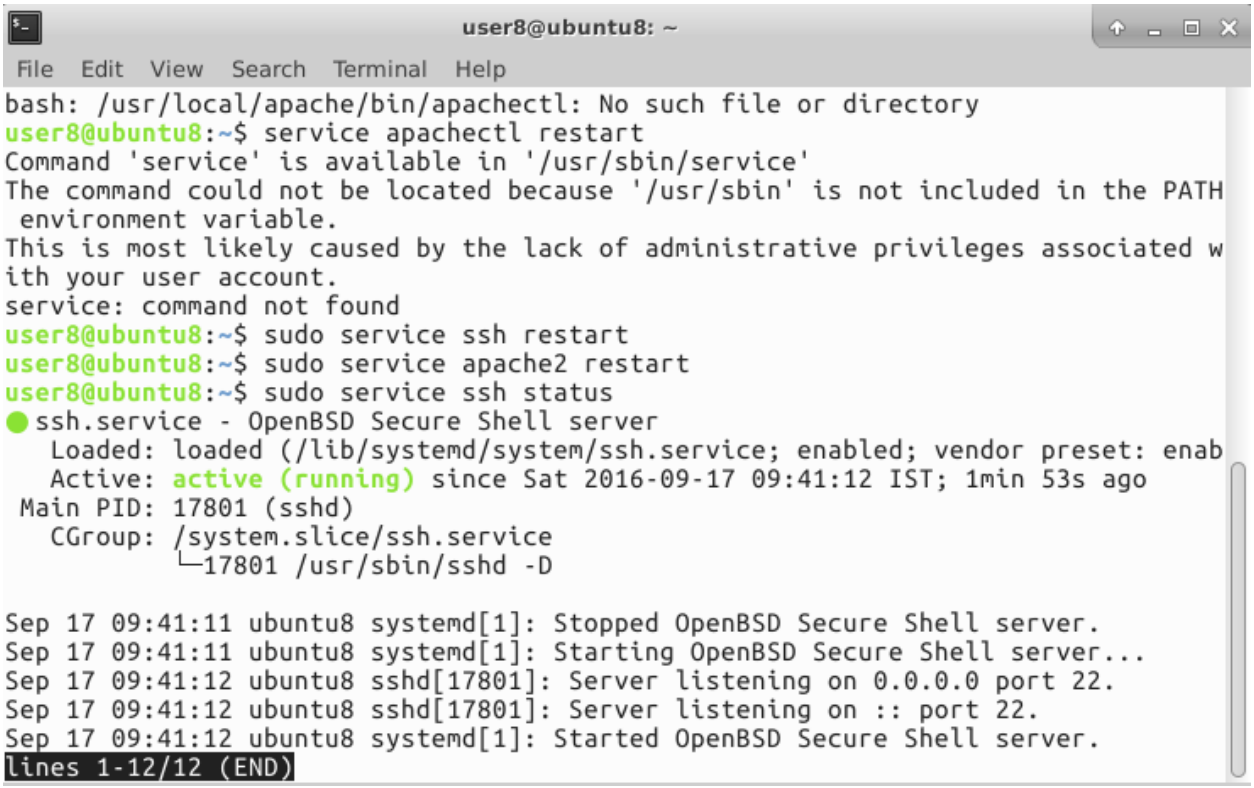


To load the new virtual host file, restart Apache by typing:

```
sudo service apache2 restart
```

This will enable our new virtual host to get the encrypted contents of our SSL Certificate.

Got various errors.



Then moved the cert file and key file to the actual location /etc/ssl and now the apache re-configuration went successfully.

Testing of our Setup

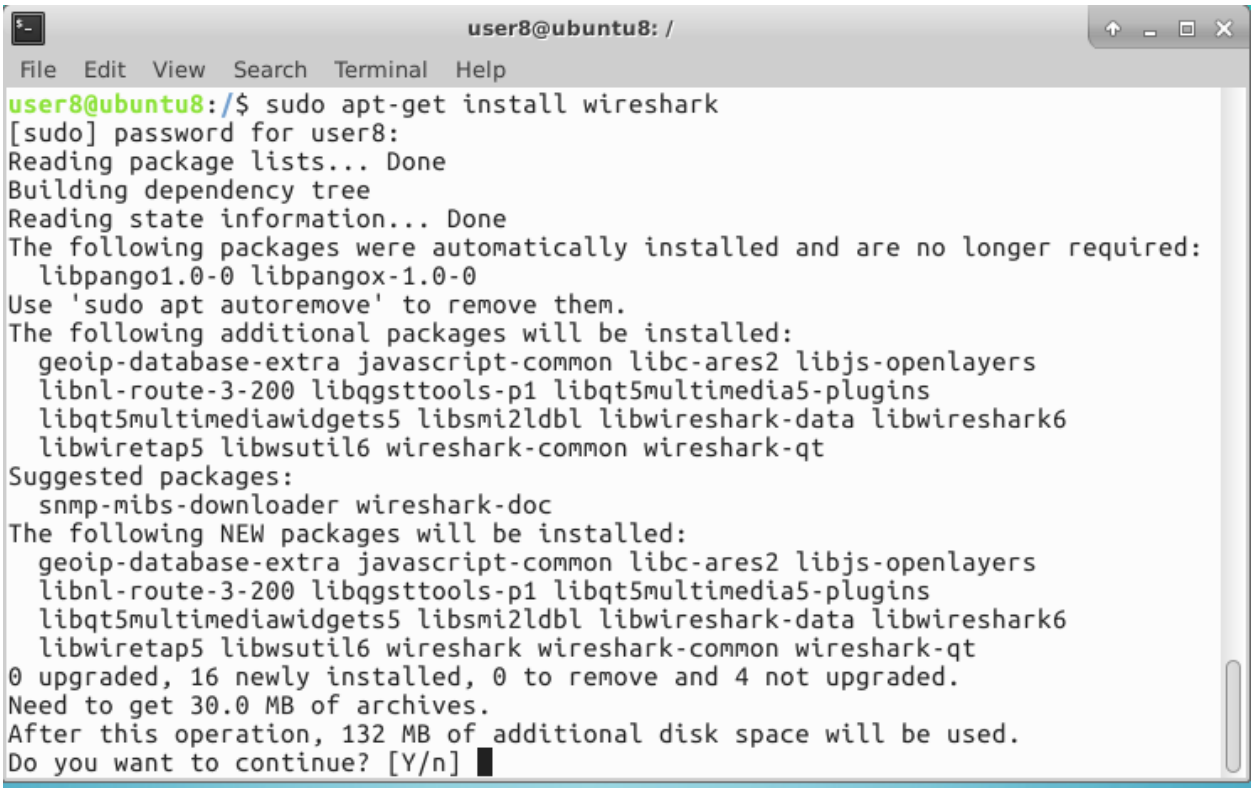
To Test our Setup by using Public IP address or Server Domain name by entering the Protocol as follows:

https://192.168.0.106

The trusted certificates authorities are not signed in so the browser cannot verify our identity so we will get a warning message. So you have to click the "Proceed anyway" option in our browser. Now we can take the content in Document Root and we will get encrypted traffic.

3. TRAFFIC ANALYSIS USING WIRESHARK

Installed Wireshark in both windows ("2.3.Installing Wireshark under Windows", 2016) client machine and Ubuntu server machine.



Ran the Wireshark from sudo mode.

Started capturing from server side.

Tried FTP, TELNET, PING and HTTP / HTTPS

Captured the pocket.

The PCAPPNG file is attached (Allen, Heriyanto and Ali, 2014)

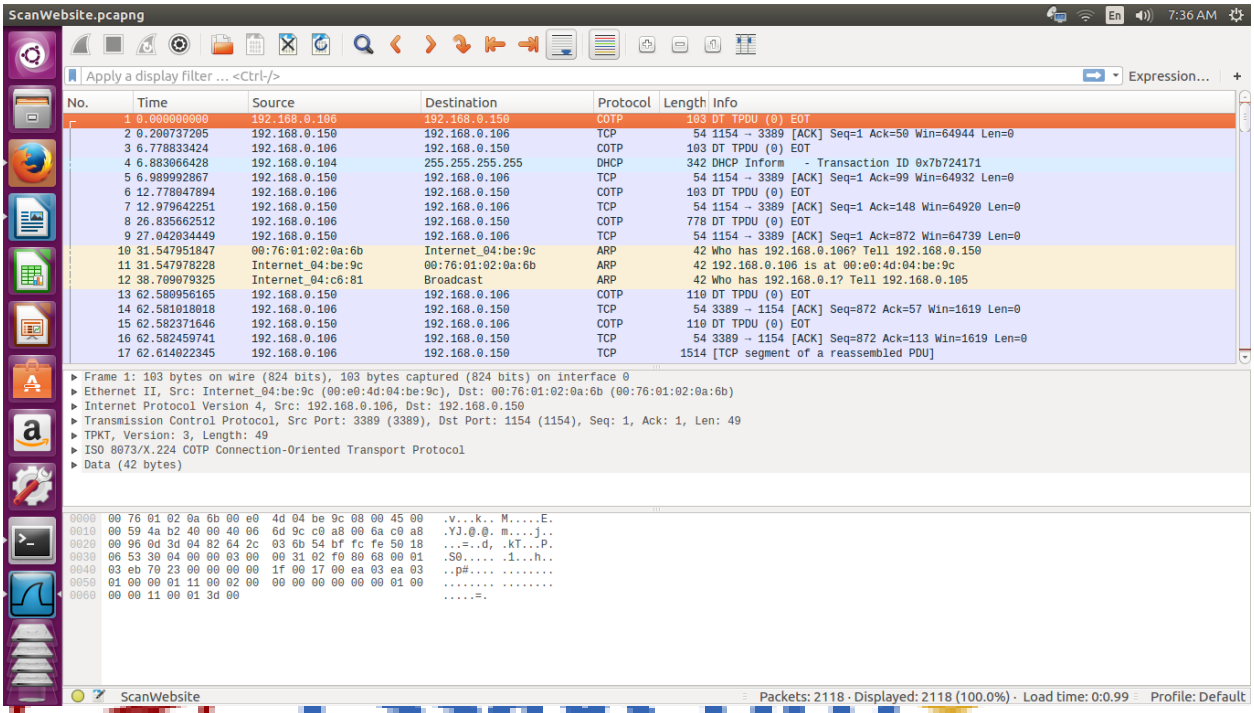
The PCAP file clearly shows the data transfers.

Wireshark is mainly used to monitor network traffic. It is used to watch the network in microscopic level. It will monitor network traffic directly from network card. It is a popular and powerful network analyzer mainly for windows, Mac, Linux. It is a tool used to monitor the data passing through a network interface. Frames are the series of data which is inspected by Wireshark it includes packets. Wireshark provides import packets from text files. It is used to analyze the flow of packets while troubleshooting the wireless LAN. It offers the tools to diagnose the problems. It uses WinPcap or lip cap to capture network traffic (Kudithipudi.org, 2009). WinPcap does not support wireless network cards, so Wi-Fi traffic monitoring on windows is not possible. Wireshark monitor mode for windows is not supported by default. Mostly the capturing is limited by WinPcap and not by Wireshark. Wi-Fi network traffic captured in promiscuous mode. It does not have Graphical User Interface (GUI). It is also available in the standard software distribution systems. It uses colors to identify the traffic, lighter blue color indicates the traffic in UDP SNMP, the Dark blue color indicates the traffic in DNS, and the green color indicates the HTTP traffic. It also uses complex color coding scheme (Beggs, 2014).

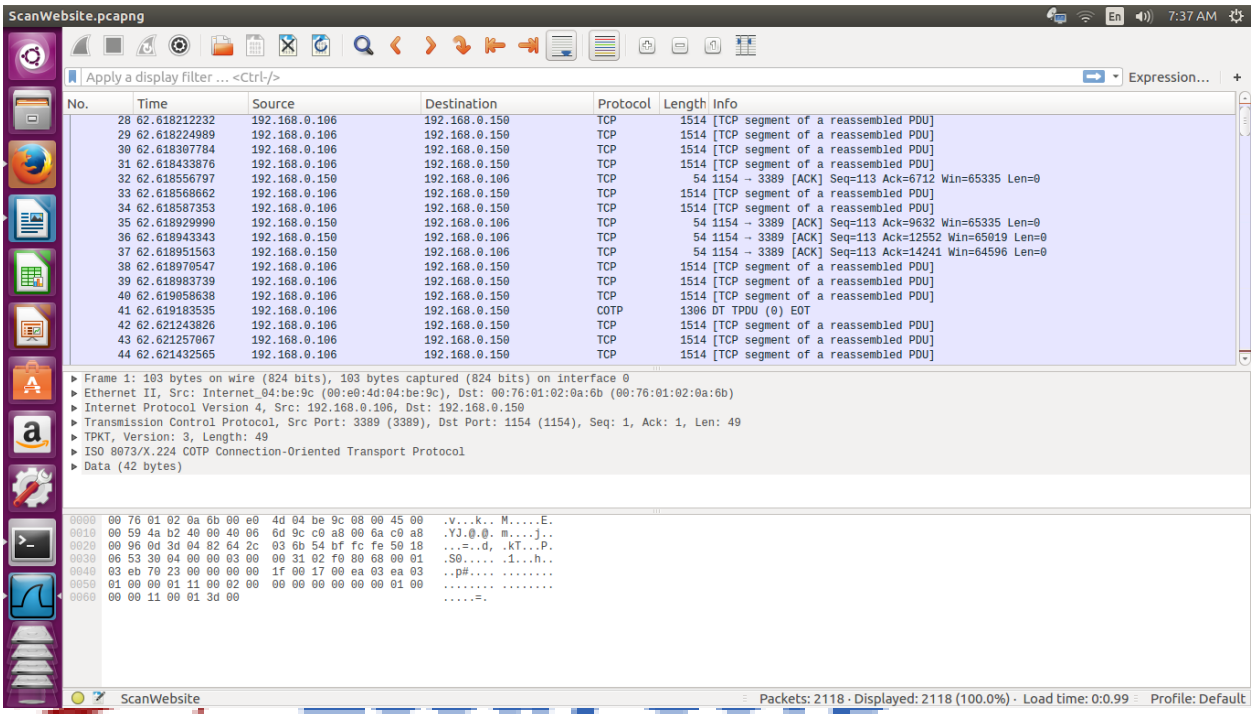
EssayCorp 5 years

WebsiteScanning.pcapng

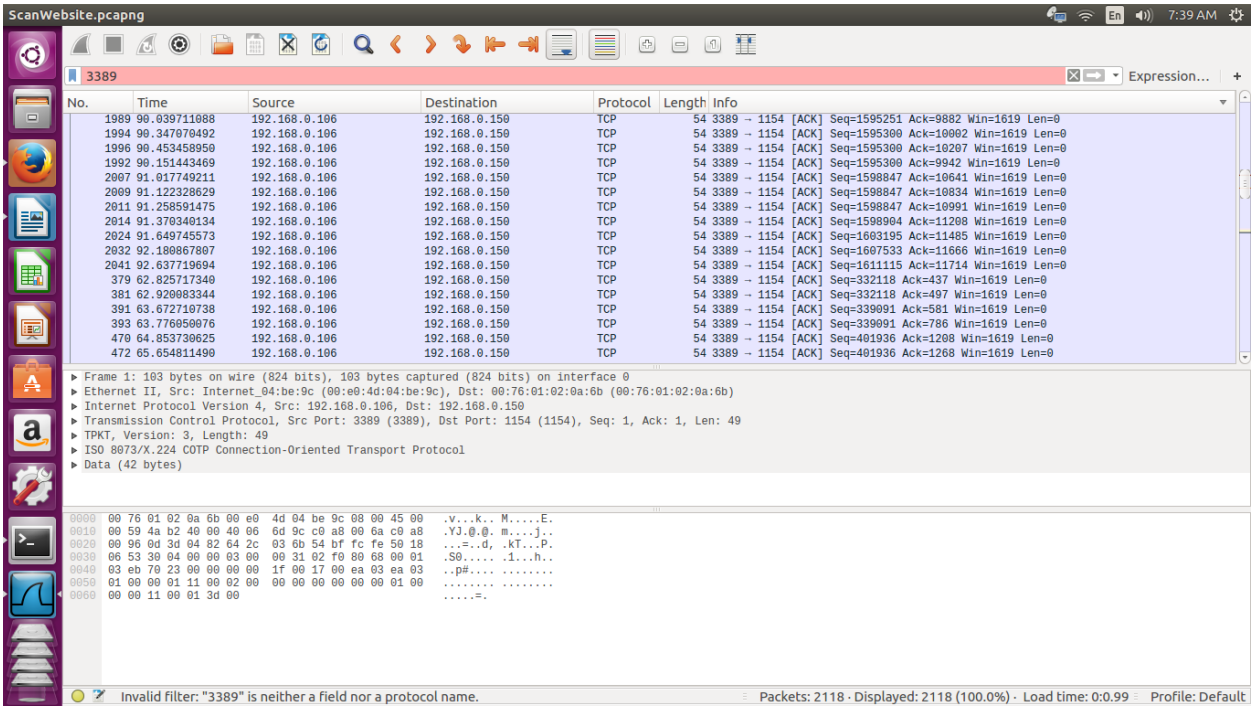
Some of the screenshots are shown and explained below. The following screenshot shows the connection between the Ubuntu server (192.168.0.106) and the client 192.168.0.150.



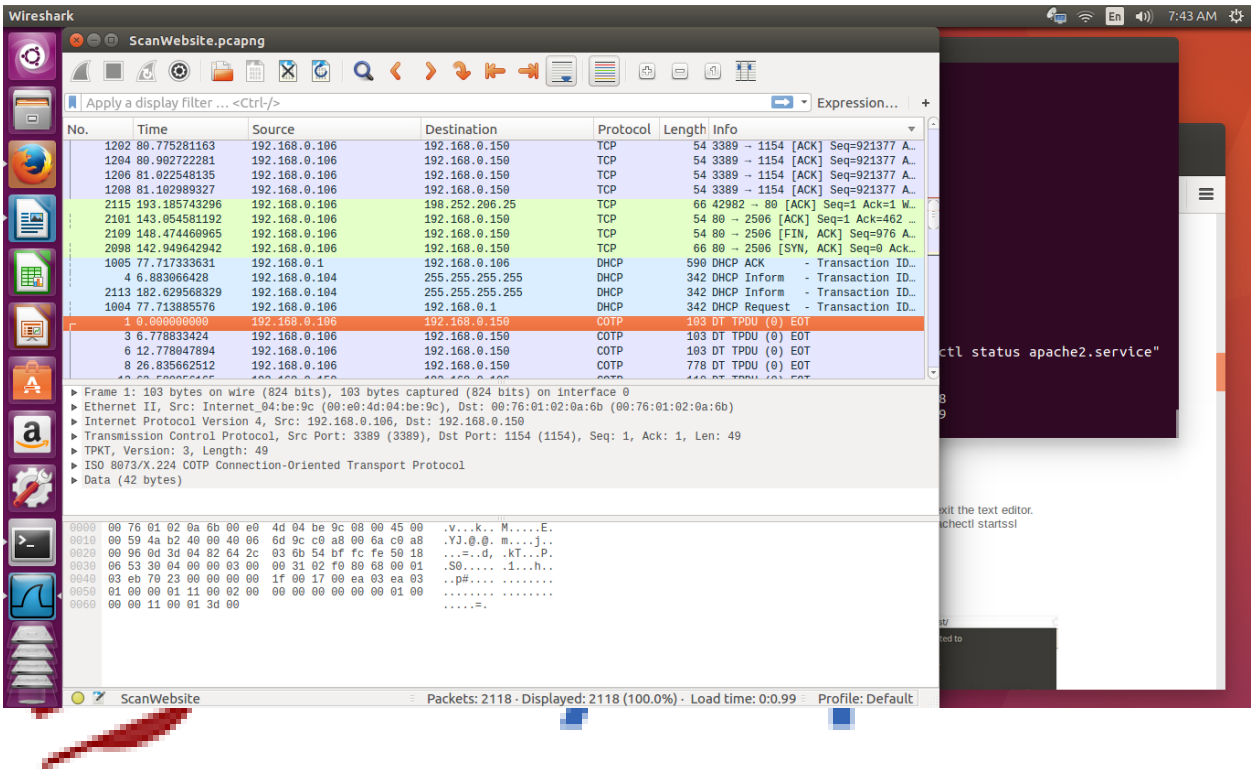
The following screenshot shows the remote desktop connection establishment through port number 3389 between the client and the server. The remote desktop service is running in the port 3389.



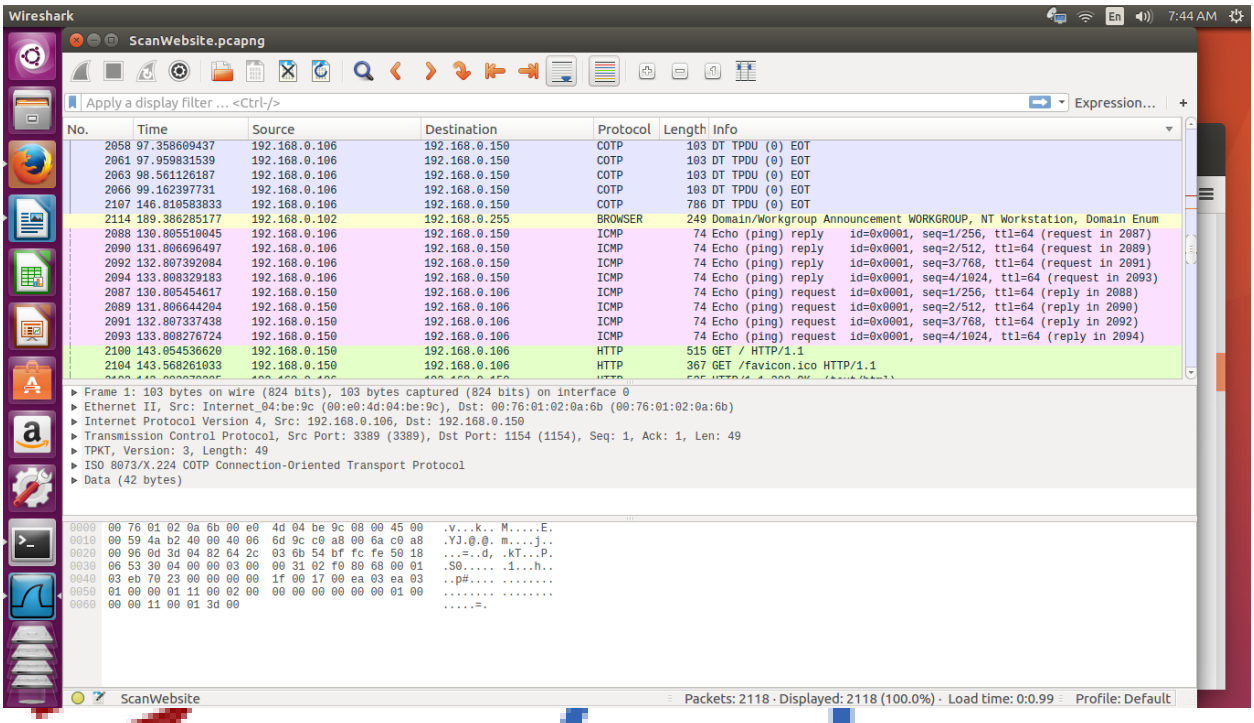
RDP connection is active through port number 3389



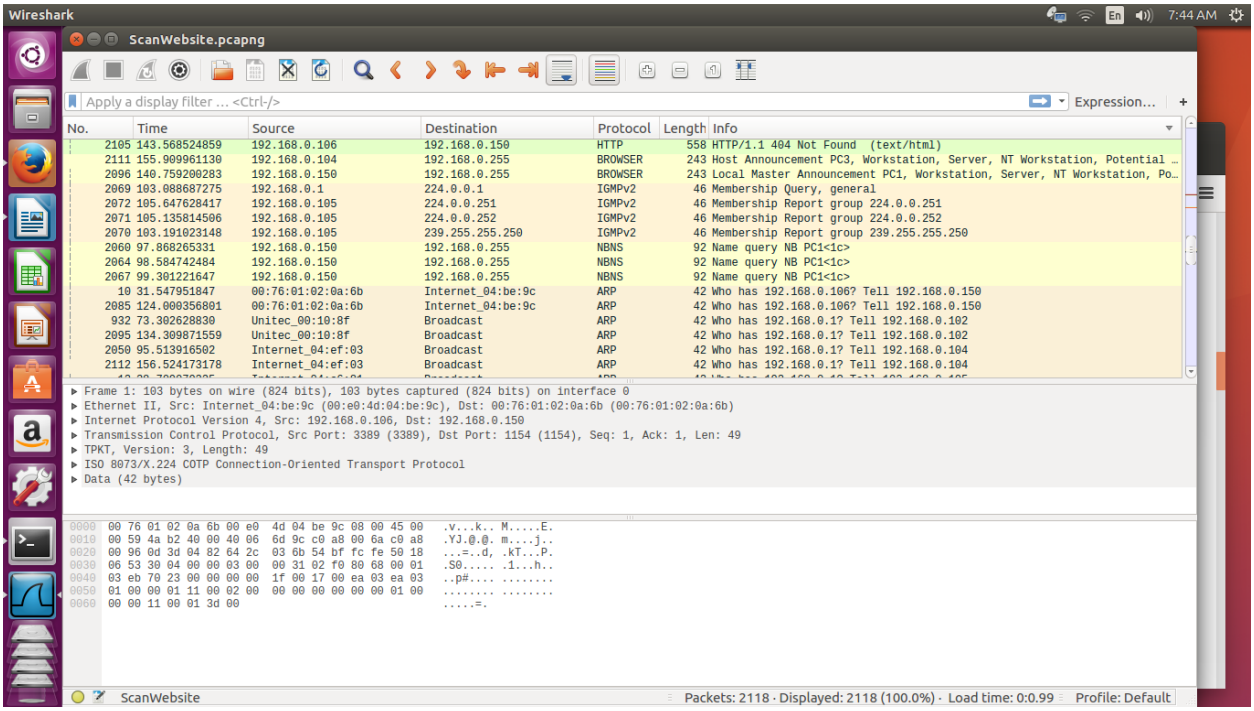
HTTP connection established through port number 80. The webserver is serving the web page from the IP 192.168.0.106 and the client requested in IP 192.168.0.150. The time stamp is marked. The source IP is shown. The Destination IP is shown. The protocol is TCP. The application port is 80. Hand shake procedure happened.



The client gave PING request to the server and the server responded. TTL is shown. The webserver is serving the PING RESPONSE from the IP 192.168.0.106 and the client requested it from IP 192.168.0.150. The time stamp is marked. The source IP is shown. The Destination IP is shown. The protocol is ICMP. The application port is 80. Packet length info is shown.



Name query is shown below. The following screenshot shows many details about the transactions that happens between the client and the server.



References

Allen, L., Heriyanto, T. and Ali, S. (2014). *Kali Linux - Assuring Security by Penetration Testing*. Birmingham, UK: Packt Pub.

Beggs, R. (2014). *Mastering Kali Linux for advanced penetration testing*. Birmingham, UK: Packt Pub.

Kaeo, M. (1999). *Designing network security*. Indianapolis, IN: Cisco Press.

Katz, J. and Yung, M. (2007). *Applied cryptography and network security*. Berlin: Springer.

Keveth, O., Saint-Andre, D. and Saint-Andre, D. (2013). *Using Wireshark on Ubuntu - Make Tech Easier*. [online] Make Tech Easier. Available at: https://www.maketecheasier.com/using-wireshark-ubuntu/ [Accessed 17 Sep. 2016].

Kudithipudi.org. (2009). *HOW TO : Install Wireshark on Windows 7 | Kudithipudi.Org*. [online] Available at: http://kudithipudi.org/2009/07/17/how-to-install-wireshark-on-window-7/ [Accessed 17 Sep. 2016].

Pritchett, W. and De Smet, D. (2013). *Kali Linux cookbook*. Birmingham, UK: Packt Pub.

Raggi, E. (2010). *Beginning Ubuntu Linux*. [Place of publication not identified]: Apress.

Stallings, W. (2000). *Network security essentials*. Upper Saddle River, NJ: Prentice Hall.

Wireshark.org. (2016). *2.3.Installing Wireshark under Windows*. [online] Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallWinInstall.html [Accessed 17 Sep. 2016].