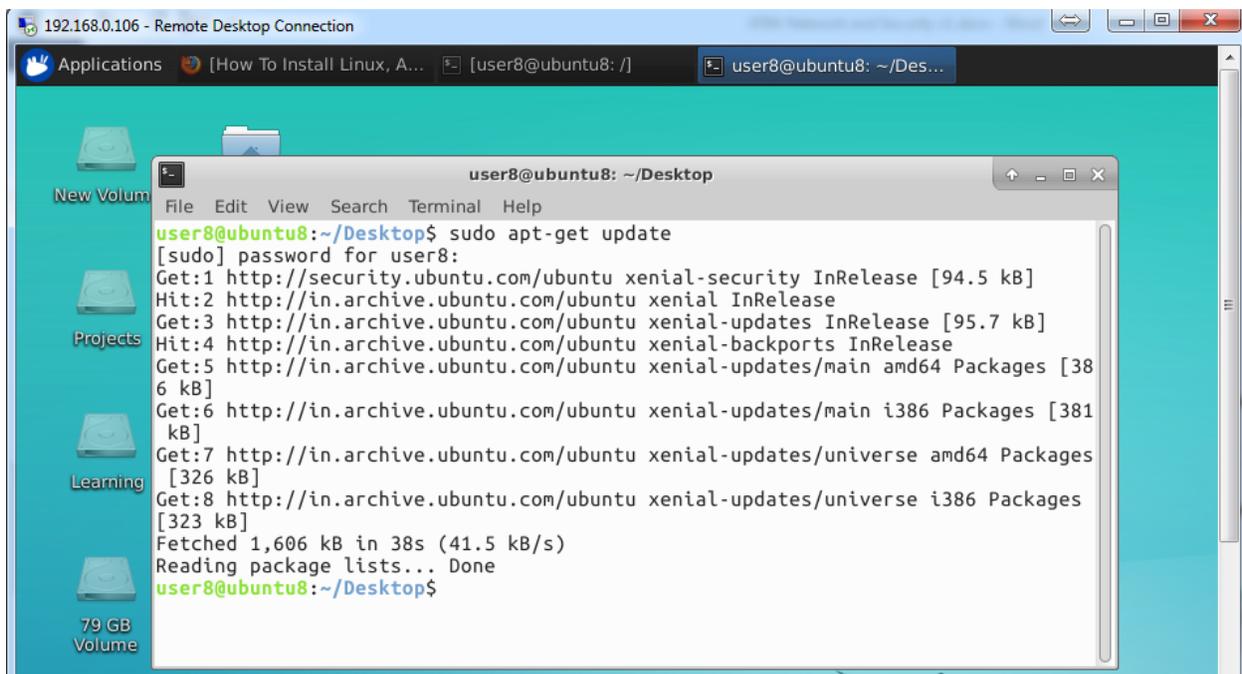


## LAMP Server

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



```
192.168.0.106 - Remote Desktop Connection
Applications [How To Install Linux, A... [user8@ubuntu8: /] user8@ubuntu8: ~/Des...
New Volum
Projects
Learning
79 GB Volume
user8@ubuntu8: ~/Desktop
File Edit View Search Terminal Help
user8@ubuntu8:~/Desktop$ sudo apt-get update
[sudo] password for user8:
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [94.5 kB]
Hit:2 http://in.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu xenial-updates InRelease [95.7 kB]
Hit:4 http://in.archive.ubuntu.com/ubuntu xenial-backports InRelease
Get:5 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [386 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [381 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [326 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [323 kB]
Fetched 1,606 kB in 38s (41.5 kB/s)
Reading package lists... Done
user8@ubuntu8:~/Desktop$
```

#### 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.

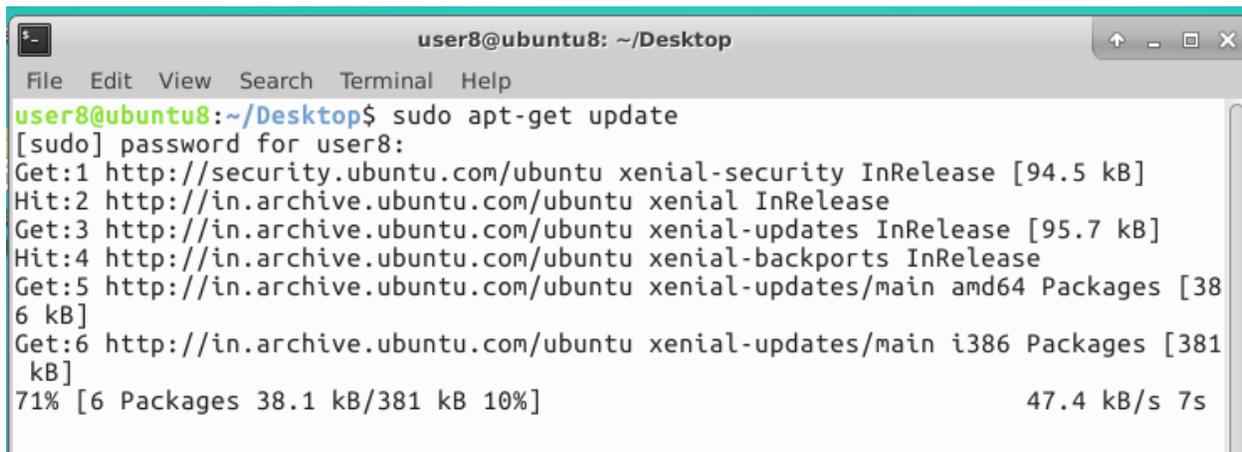
The Apache widely used by Word Press hosting providers.

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,

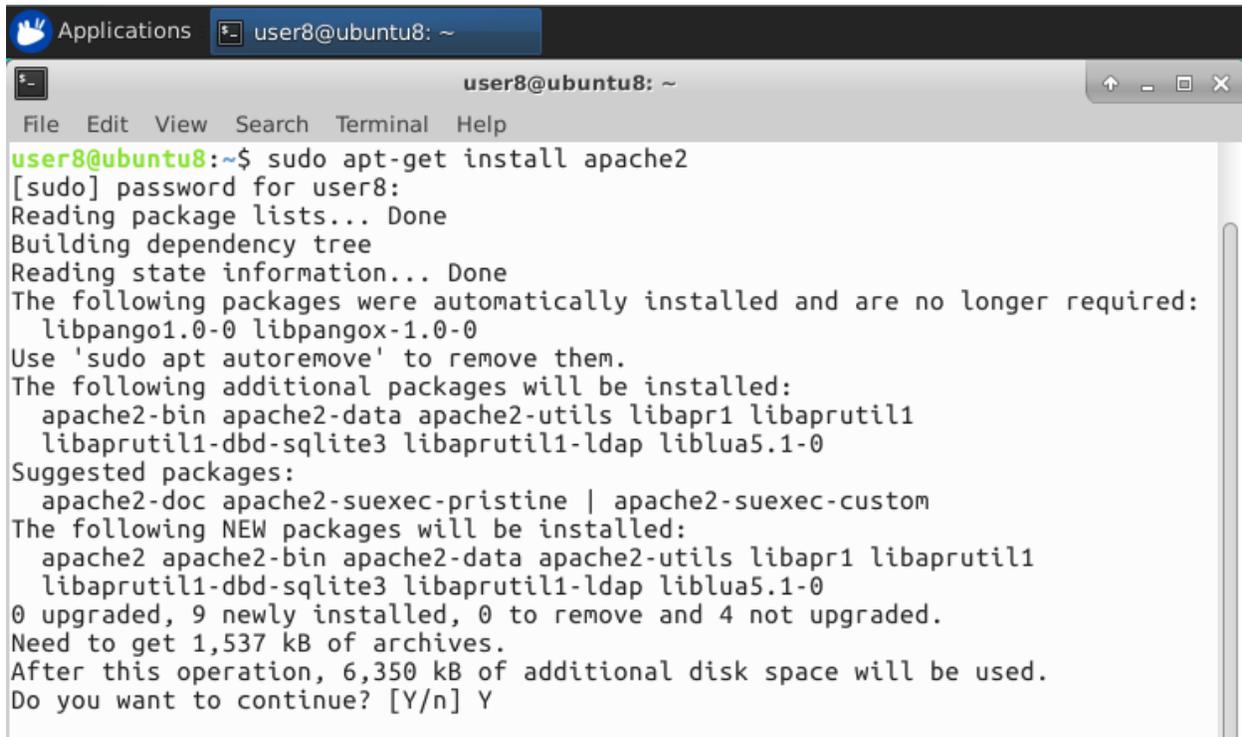
```
sudo apt-get update
```



```
user8@ubuntu8: ~/Desktop
File Edit View Search Terminal Help
user8@ubuntu8:~/Desktop$ sudo apt-get update
[sudo] password for user8:
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [94.5 kB]
Hit:2 http://in.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu xenial-updates InRelease [95.7 kB]
Hit:4 http://in.archive.ubuntu.com/ubuntu xenial-backports InRelease
Get:5 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [38
6 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [381
kB]
71% [6 Packages 38.1 kB/381 kB 10%]                               47.4 kB/s 7s
```

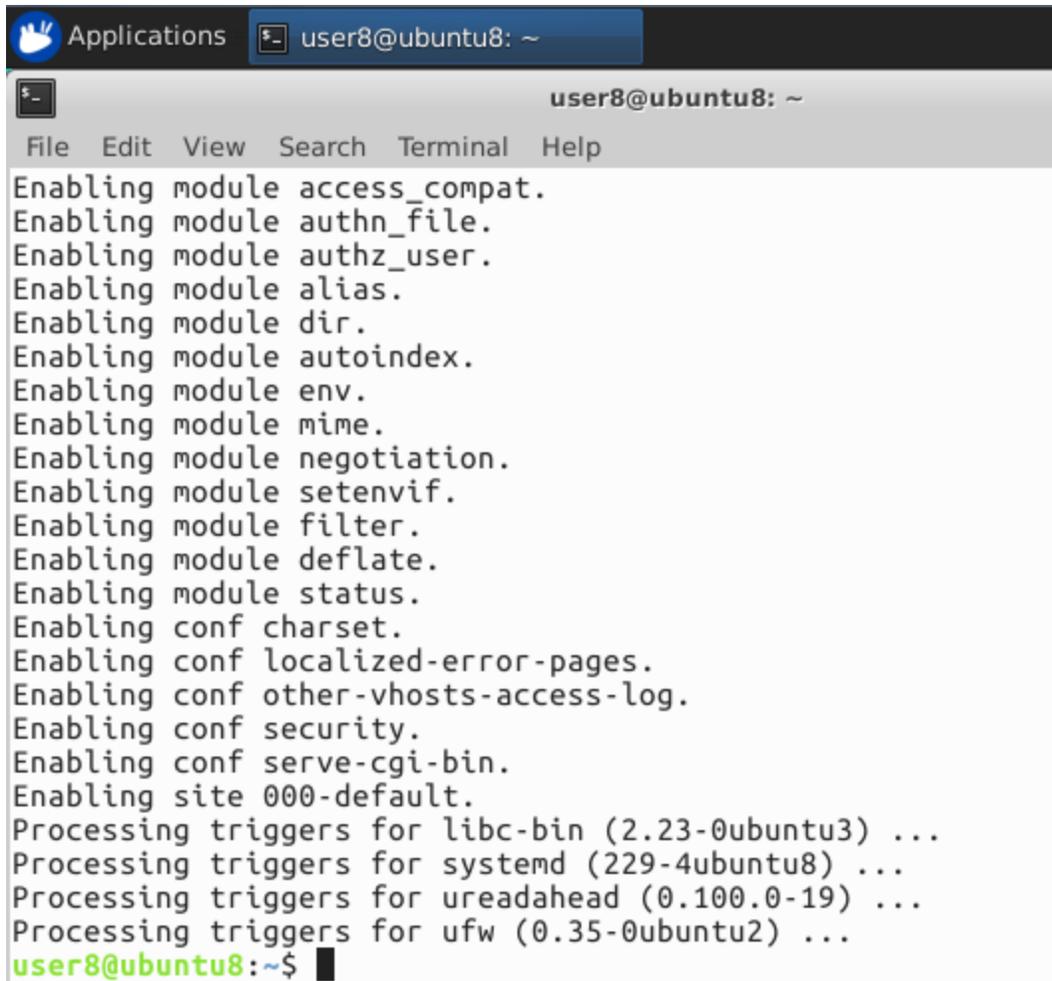
```
sudo apt-get install apache2
```

Got the following, asking for confirmation.



```
user8@ubuntu8: ~  
user8@ubuntu8: ~  
File Edit View Search Terminal Help  
user8@ubuntu8:~$ sudo apt-get install apache2  
[sudo] password for user8:  
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:  
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1  
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0  
Suggested packages:  
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom  
The following NEW packages will be installed:  
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1  
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0  
0 upgraded, 9 newly installed, 0 to remove and 4 not upgraded.  
Need to get 1,537 kB of archives.  
After this operation, 6,350 kB of additional disk space will be used.  
Do you want to continue? [Y/n] Y
```

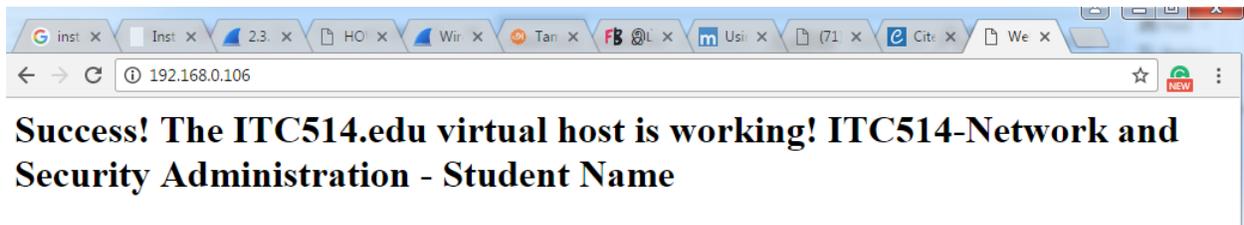
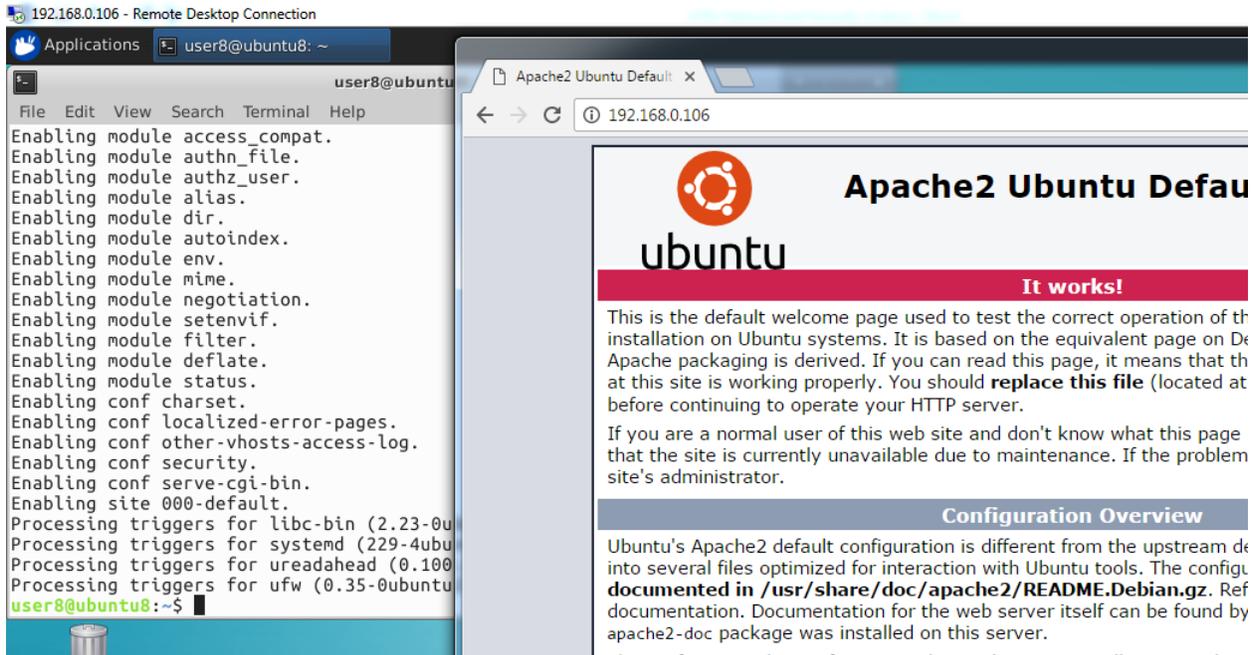
Apache is installed successfully.

A terminal window titled 'user8@ubuntu8: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the following steps for enabling Apache modules and configurations:

```
Enabling module access_compat.  
Enabling module authn_file.  
Enabling module authz_user.  
Enabling module alias.  
Enabling module dir.  
Enabling module autoindex.  
Enabling module env.  
Enabling module mime.  
Enabling module negotiation.  
Enabling module setenvif.  
Enabling module filter.  
Enabling module deflate.  
Enabling module status.  
Enabling conf charset.  
Enabling conf localized-error-pages.  
Enabling conf other-vhosts-access-log.  
Enabling conf security.  
Enabling conf serve-cgi-bin.  
Enabling site 000-default.  
Processing triggers for libc-bin (2.23-0ubuntu3) ...  
Processing triggers for systemd (229-4ubuntu8) ...  
Processing triggers for ureadahead (0.100.0-19) ...  
Processing triggers for ufw (0.35-0ubuntu2) ...  
user8@ubuntu8:~$
```

ears  
☆☆☆☆

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**

```
192.168.0.106 - Remote Desktop Connection
Applications user8@ubuntu8: ~
user8@ubuntu8: ~
File Edit View Search Terminal Help
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:23427224 errors:0 dropped:0 overruns:0 frame:0
TX packets:23427224 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:30119675021 (30.1 GB) TX bytes:30119675021 (30.1 GB)

wlx00e04d04be9c Link encap:Ethernet HWaddr 00:e0:4d:04:be:9c
inet addr:192.168.0.106 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: fe80::a0d9:a95c:1fb:8804/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1131363 errors:0 dropped:0 overruns:0 frame:0
TX packets:2209155 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:102704260 (102.7 MB) TX bytes:3238869045 (3.2 GB)

user8@ubuntu8:~$
```

Apache restarted to implement the changes.

## Installation of MySQL

It is a relational 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
```

 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 displayed 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 webservice**

### **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
```

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.

```

user8@ubuntu8: ~
File Edit View Search Terminal Help
GNU nano 2.5.3 File: /var/www/itc514.edu/public_html/index.html Modified

<html>
  <head>
    <title>Welcome to ITC514.edu</title>
  </head>
  <body>
    <h1>Success! The ITC514.edu virtual host is working!</h1>
  </body>
</html>

```

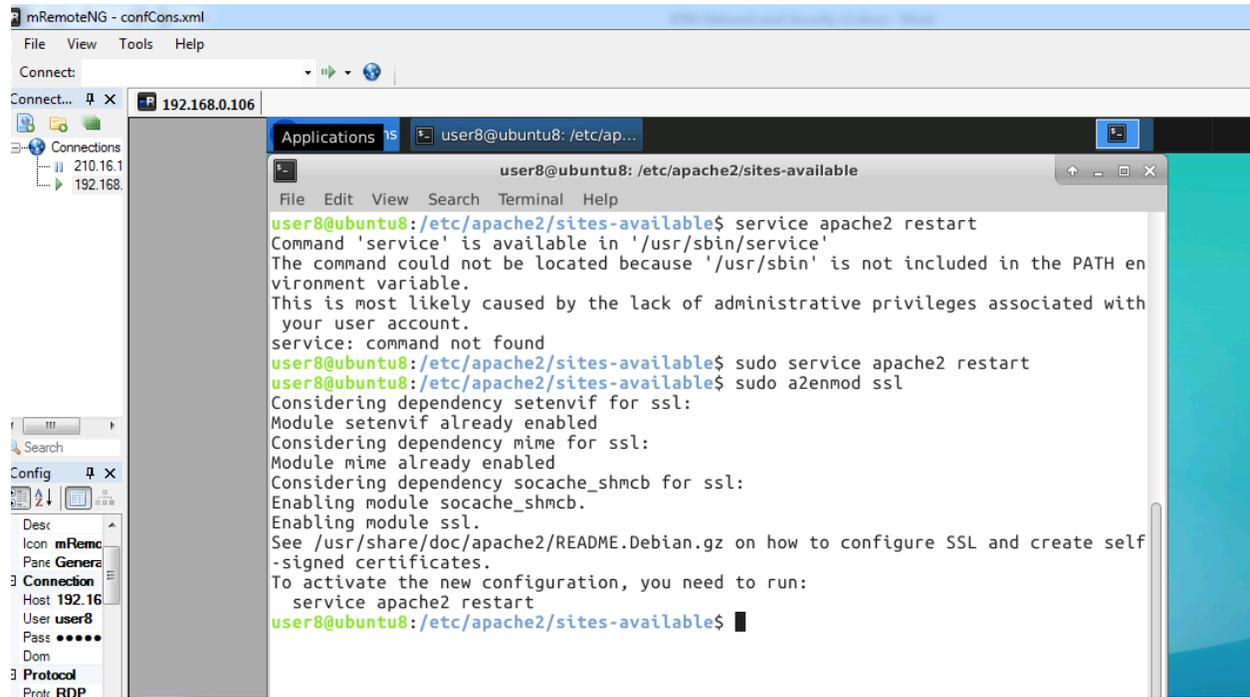
Opened /etc/apache2/sites-available location and changed the itc514.edu.conf file as shown below.

Server Name is itc514.com

ServerAdmin [admin@itc514.edu](mailto:admin@itc514.edu)

DocumentRoot /var/www/itc514.edu/public\_html

## Restarted apache2



The screenshot shows a terminal window within mRemoteNG. The terminal is connected to a host at 192.168.0.106, using user8. The user is in the directory /etc/apache2/sites-available. The terminal output shows the following commands and their results:

```
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$
```

~~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:~$ █
```



```
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
```

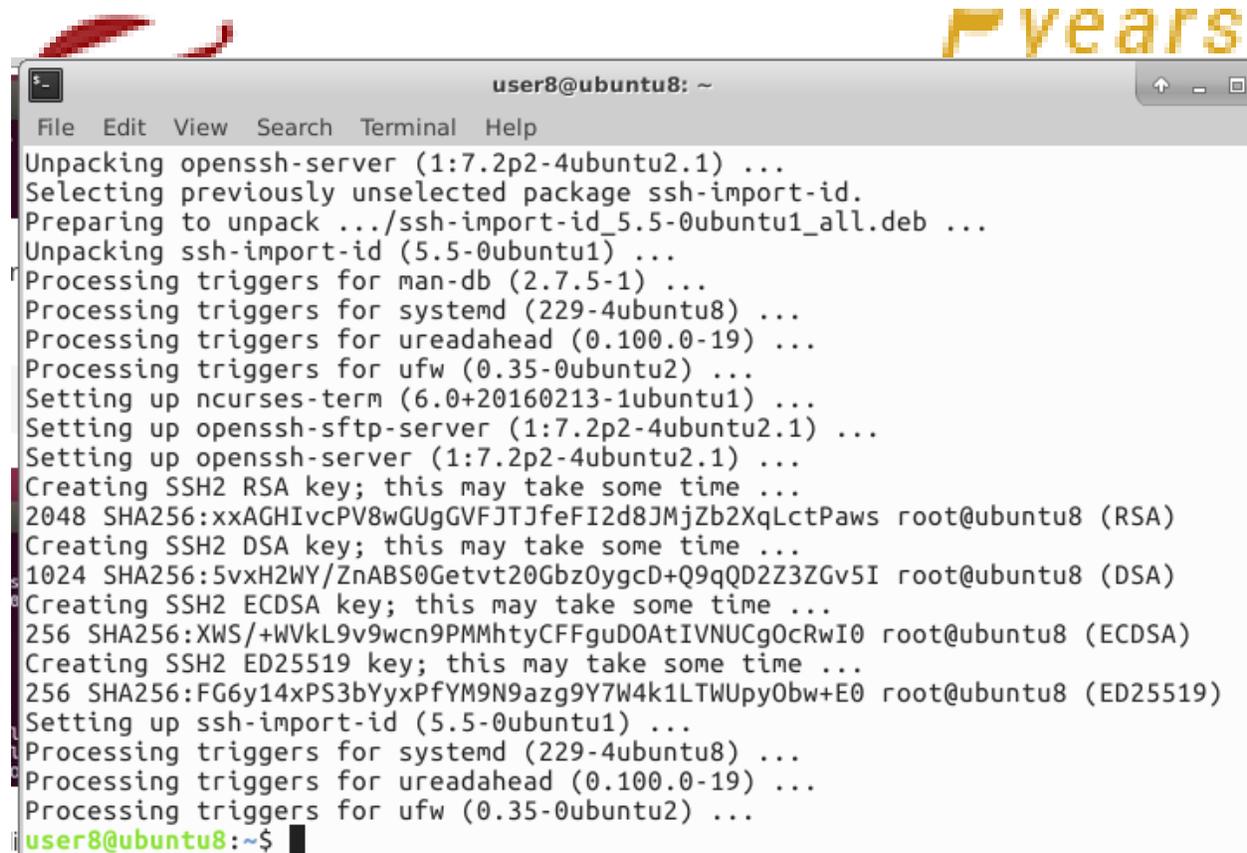
```
mRemoteNG - confCons.xml
File View Tools Help
Connect: 192.168.0.106
Applications user8@ubuntu8: /etc/ap...
user8@ubuntu8:/etc/apache2/sites-available
File Edit View Search Terminal Help
user8@ubuntu8:/etc/apache2/sites-available$ service apache2 restart
Command 'service' is available in '/usr/sbin/service'
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$ █
```

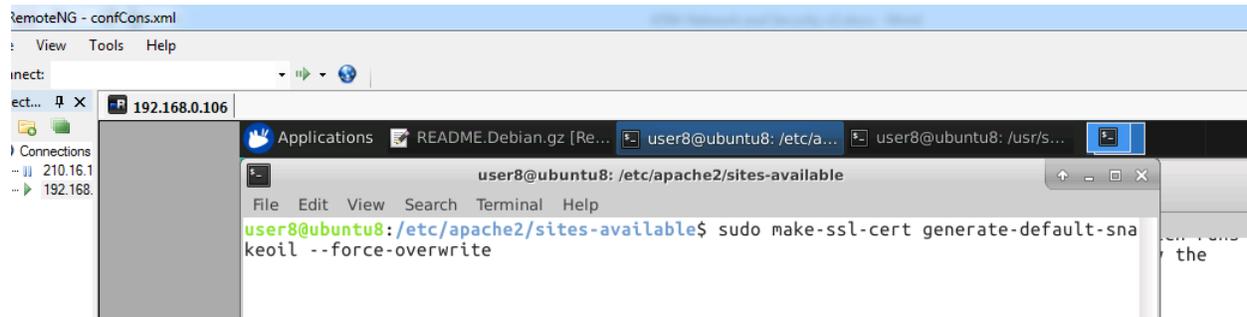
Wanted to run the server from nearby client using putty through SSH2 protocol and hence installed **openssh-server**



```
user8@ubuntu8: ~
File Edit View Search Terminal Help
Unpacking openssh-server (1:7.2p2-4ubuntu2.1) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.5-0ubuntu1_all.deb ...
Unpacking ssh-import-id (5.5-0ubuntu1) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu8) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
Setting up ncurses-term (6.0+20160213-1ubuntu1) ...
Setting up openssh-sftp-server (1:7.2p2-4ubuntu2.1) ...
Setting up openssh-server (1:7.2p2-4ubuntu2.1) ...
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:xxAGHIvcPV8wGUgGVFJTJfeFI2d8JMjZb2XqLctPaws root@ubuntu8 (RSA)
Creating SSH2 DSA key; this may take some time ...
1024 SHA256:5vxH2WY/ZnABS0Getvt20Gbz0ygcD+Q9qQD2Z3ZGv5I root@ubuntu8 (DSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:XWS/+wVkl9v9wcn9PMMhtyCFFguDOAtIVNUCg0cRwI0 root@ubuntu8 (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:FG6y14xPS3bYyxPFYM9N9azg9Y7W4k1LTWUpy0bw+E0 root@ubuntu8 (ED25519)
Setting up ssh-import-id (5.5-0ubuntu1) ...
Processing triggers for systemd (229-4ubuntu8) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
user8@ubuntu8:~$ █
```

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

## Self-Signed SSL Certificate Creation



The screenshot shows a terminal window titled 'remoteNG - confCons.xml'. The terminal prompt is 'user8@ubuntu8: /etc/apache2/sites-available\$'. The command entered is 'sudo make-ssl-cert generate-default-snakeoil --force-overwrite'. The terminal output shows the command being executed successfully.

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
```

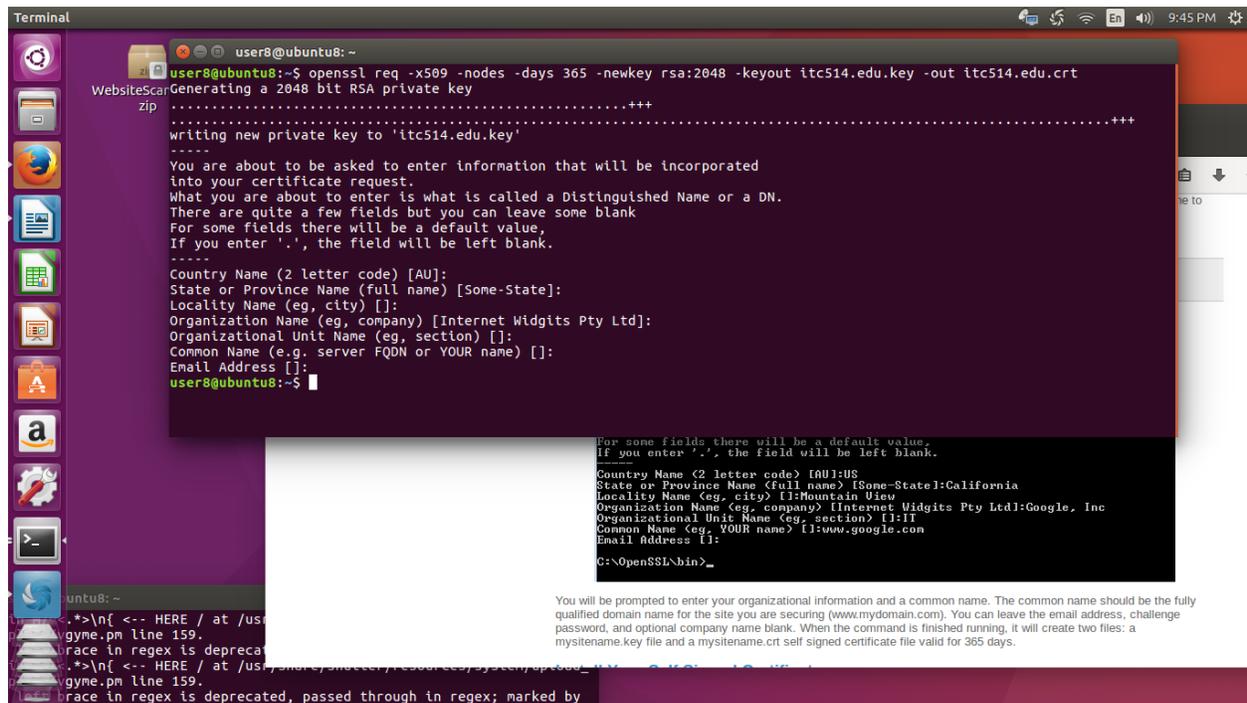
This certificate is valid for 1 year. It is a RSA 2048 strength. Apache key will be stored in /etc/apache2/ssl location and the apache certificate will be stored in /etc/apache2/ssl location. Ensured that both are generated and stored.

```
user8@ubuntu8: ~
File Edit View Search Terminal Help
user8@ubuntu8:~$ openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout mysitename.key -out mysitename.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'mysitename.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
user8@ubuntu8:~$
```

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

```
Applications  README.Debian.gz [Re...  user8@ubuntu8: /etc/a...  user8@ubuntu8: /usr/s...
user8@ubuntu8: /etc/apache2/sites-enabled
File Edit View Search Terminal Help
user8@ubuntu8:/etc/apache2/sites-enabled$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/itc514.edu.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
user8@ubuntu8:/etc/apache2/sites-enabled$ █
```

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



```
user8@ubuntu8:~$ openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout itc514.edu.key -out itc514.edu.crt
Generating a 2048 bit RSA private key
.....+++
writing new private key to 'itc514.edu.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
user8@ubuntu8:~$
```

## 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.

```
user8@ubuntu8: ~
File Edit View Search Terminal Help
GNU nano 2.5.3 File: /etc/apache2/sites-available/default-ssl.conf

<IfModule mod_ssl.c>

<VirtualHost 192.168.0.106:443>
DocumentRoot /var/www/itc514.edu
ServerName itc514.edu
SSLEngine on
SSLCertificateFile /etc/ssl/crt/itc514.edu.crt
SSLCertificateKeyFile /etc/ssl/crt/itc514.edu.key
</VirtualHost>

<VirtualHost _default_:443>
ServerAdmin webmaster@localhost
File Name to Write: /etc/apache2/sites-available/default-ssl.conf
^G Get Help      M-D DOS Format  M-A Append     M-B Backup File
^C Cancel        M-M Mac Format  M-P Prepend    ^T To Files
```

### SSL Virtual Host Activation

Enabled Virtual host of SSL by typing:

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

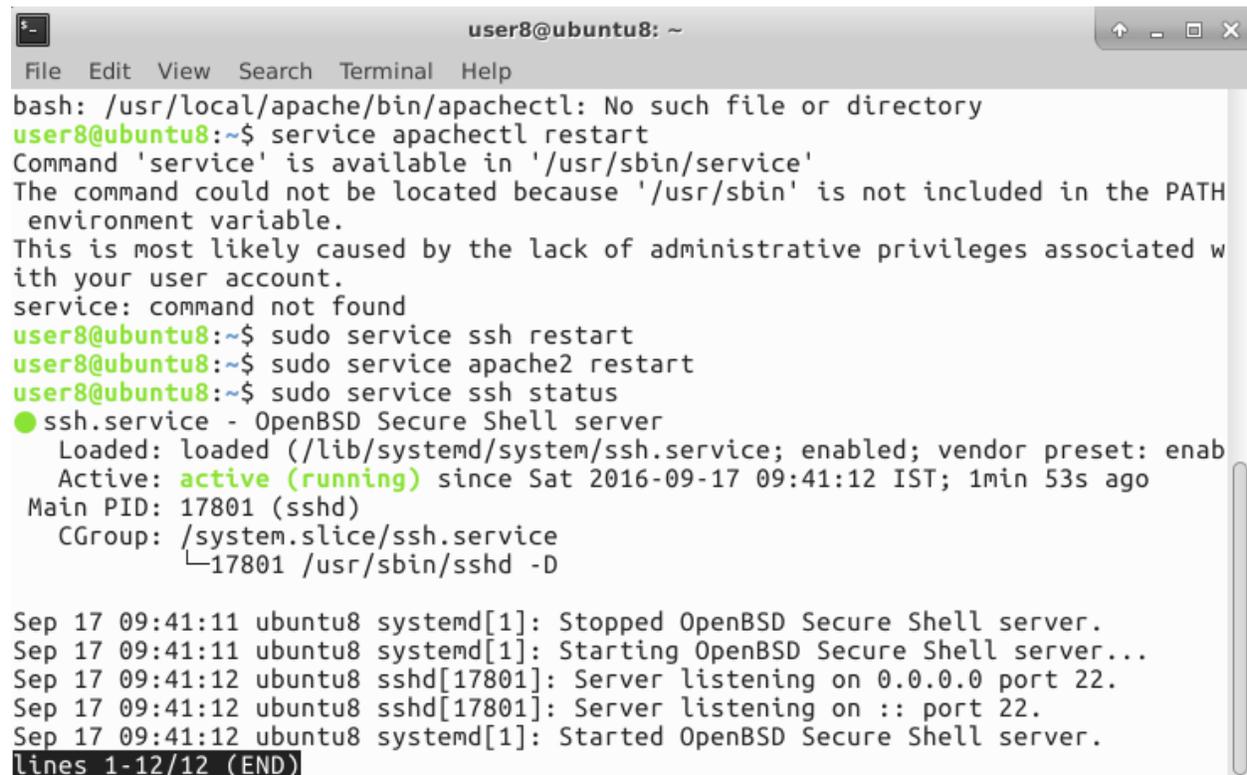
```
Applications  README.Debian.gz [Re...  user8@ubuntu8: /etc/a...  user8@ubuntu8: /usr/s...
user8@ubuntu8: /etc/apache2/sites-available
File Edit View Search Terminal Help
user8@ubuntu8:/etc/apache2/sites-available$ ls
000-default.conf  default-ssl.conf  default-ssl.conf.save  itc514.edu.conf
user8@ubuntu8:/etc/apache2/sites-available$ sudo nano default-ssl.conf
user8@ubuntu8:/etc/apache2/sites-available$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
user8@ubuntu8:/etc/apache2/sites-available$
```

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.



```
user8@ubuntu8: ~
File Edit View Search Terminal Help
bash: /usr/local/apache/bin/apachectl: No such file or directory
user8@ubuntu8:~$ service apachectl 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 w
ith your user account.
service: command not found
user8@ubuntu8:~$ sudo service ssh restart
user8@ubuntu8:~$ sudo service apache2 restart
user8@ubuntu8:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Sat 2016-09-17 09:41:12 IST; 1min 53s ago
   Main PID: 17801 (sshd)
   CGroup: /system.slice/ssh.service
           └─17801 /usr/sbin/sshd -D

Sep 17 09:41:11 ubuntu8 systemd[1]: Stopped OpenBSD Secure Shell server.
Sep 17 09:41:11 ubuntu8 systemd[1]: Starting OpenBSD Secure Shell server...
Sep 17 09:41:12 ubuntu8 sshd[17801]: Server listening on 0.0.0.0 port 22.
Sep 17 09:41:12 ubuntu8 sshd[17801]: Server listening on :: port 22.
Sep 17 09:41:12 ubuntu8 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

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

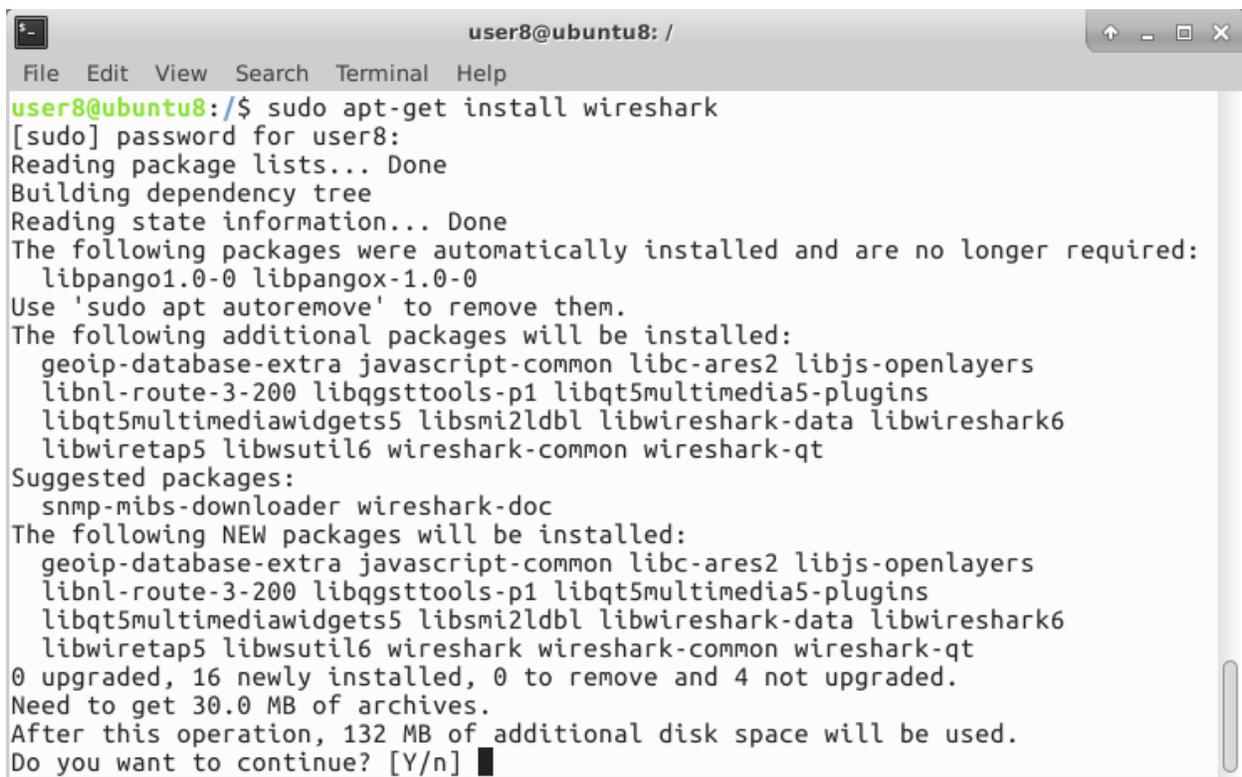
To Test our Setup by using Public IP address or Server Domain name by entering the Protocol as follows:

<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.



```
user8@ubuntu8: /
File Edit View Search Terminal Help
user8@ubuntu8:/$ sudo apt-get install wireshark
[sudo] password for user8:
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:
 geoip-database-extra javascript-common libc-ares2 libjs-openlayers
 libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
 libqt5multimediamediawidgets5 libsmi2ldbl libwireshark-data libwireshark6
 libwiretap5 libwsutil6 wireshark-common wireshark-qt
Suggested packages:
 snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
 geoip-database-extra javascript-common libc-ares2 libjs-openlayers
 libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
 libqt5multimediamediawidgets5 libsmi2ldbl libwireshark-data libwireshark6
 libwiretap5 libwsutil6 wireshark wireshark-common wireshark-qt
0 upgraded, 16 newly installed, 0 to remove and 4 not upgraded.
Need to get 30.0 MB of archives.
After this operation, 132 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Ran the Wireshark from sudo mode.

Started capturing from server side.

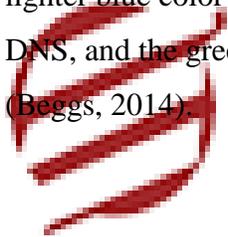
Tried FTP, TELNET, PING and HTTP / HTTPS

Captured the packet.

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 libpcap 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.p  
capng

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 screenshot displays a Wireshark network traffic capture for a file named 'ScanWebsite.pcapng'. The interface shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 1) is a COTP PDU (0) EOT from 192.168.0.150 to 192.168.0.106. Below the packet list, the packet details pane shows the structure of the COTP PDU, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and TPMT. The packet bytes pane shows the raw hexadecimal and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.150	192.168.0.106	COTP	103	0 [0] TPDU (0) EOT
2	0.200737205	192.168.0.150	192.168.0.106	TCP	54	1154 → 3389 [ACK] Seq=1 Ack=50 Win=64944 Len=0
3	6.778833424	192.168.0.106	192.168.0.150	COTP	103	DT TPDU (0) EOT
4	6.883066428	192.168.0.104	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x7b724171
5	6.989992867	192.168.0.150	192.168.0.106	TCP	54	1154 → 3389 [ACK] Seq=1 Ack=99 Win=64932 Len=0
6	12.778047894	192.168.0.106	192.168.0.150	COTP	103	DT TPDU (0) EOT
7	12.979642251	192.168.0.150	192.168.0.106	TCP	54	1154 → 3389 [ACK] Seq=1 Ack=148 Win=64920 Len=0
8	26.835662512	192.168.0.106	192.168.0.150	COTP	778	DT TPDU (0) EOT
9	27.042034449	192.168.0.150	192.168.0.106	TCP	54	1154 → 3389 [ACK] Seq=1 Ack=872 Win=64739 Len=0
10	31.547951847	00:76:01:02:0a:6b	Internet_04:be:9c	ARP	42	Who has 192.168.0.106? Tell 192.168.0.150
11	31.547978228	Internet_04:be:9c	00:76:01:02:0a:6b	ARP	42	192.168.0.106 is at 00:e0:4d:04:be:9c
12	38.709979325	Internet_04:c6:81	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.105
13	62.500956165	192.168.0.150	192.168.0.106	COTP	110	DT TPDU (0) EOT
14	62.581018018	192.168.0.106	192.168.0.150	TCP	54	3389 → 1154 [ACK] Seq=872 Ack=57 Win=1619 Len=0
15	62.582371646	192.168.0.150	192.168.0.106	COTP	110	DT TPDU (0) EOT
16	62.582459741	192.168.0.106	192.168.0.150	TCP	54	3389 → 1154 [ACK] Seq=872 Ack=113 Win=1619 Len=0
17	62.614022345	192.168.0.106	192.168.0.150	TCP	1514	[TCP segment of a reassembled PDU]

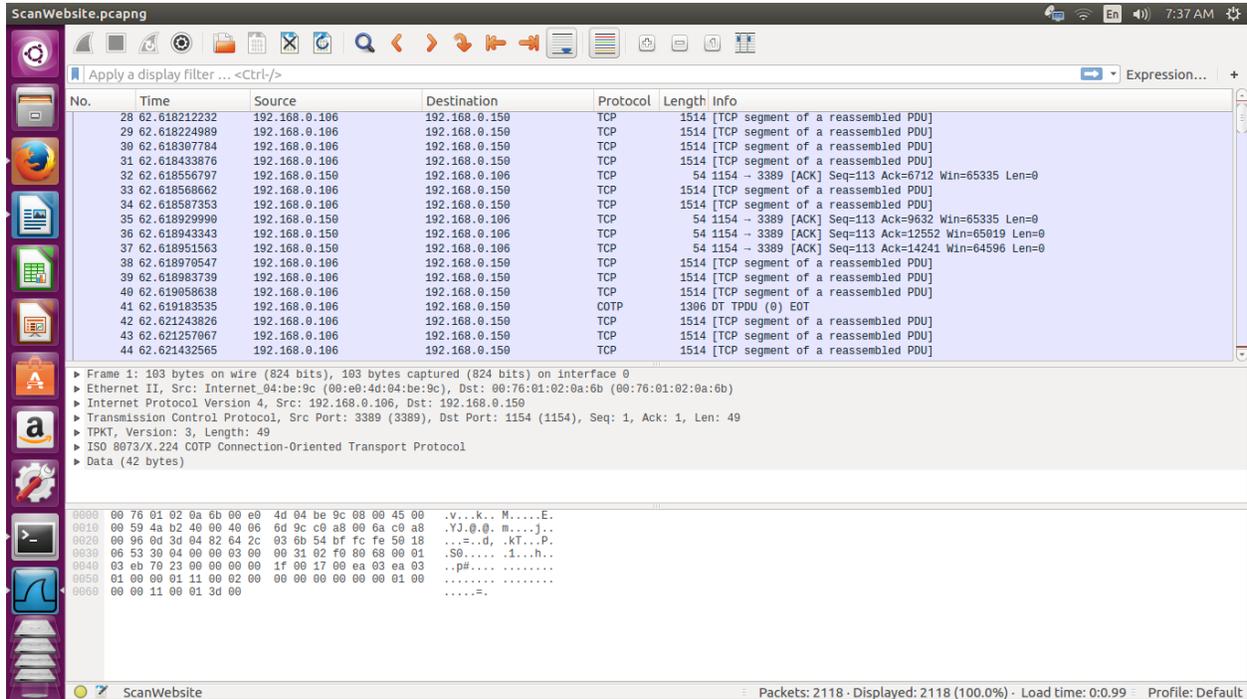
Packet details for Frame 1:

- Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
- Ethernet II, Src: Internet\_04:be:9c (00:e0:4d:04:be:9c), Dst: 00:76:01:02:0a:6b (00:76:01:02:0a:6b)
- Internet Protocol Version 4, Src: 192.168.0.150, Dst: 192.168.0.106
- Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 1154 (1154), Seq: 1, Ack: 1, Len: 49
- TPMT, Version: 3, Length: 49
- ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
- Data (42 bytes)

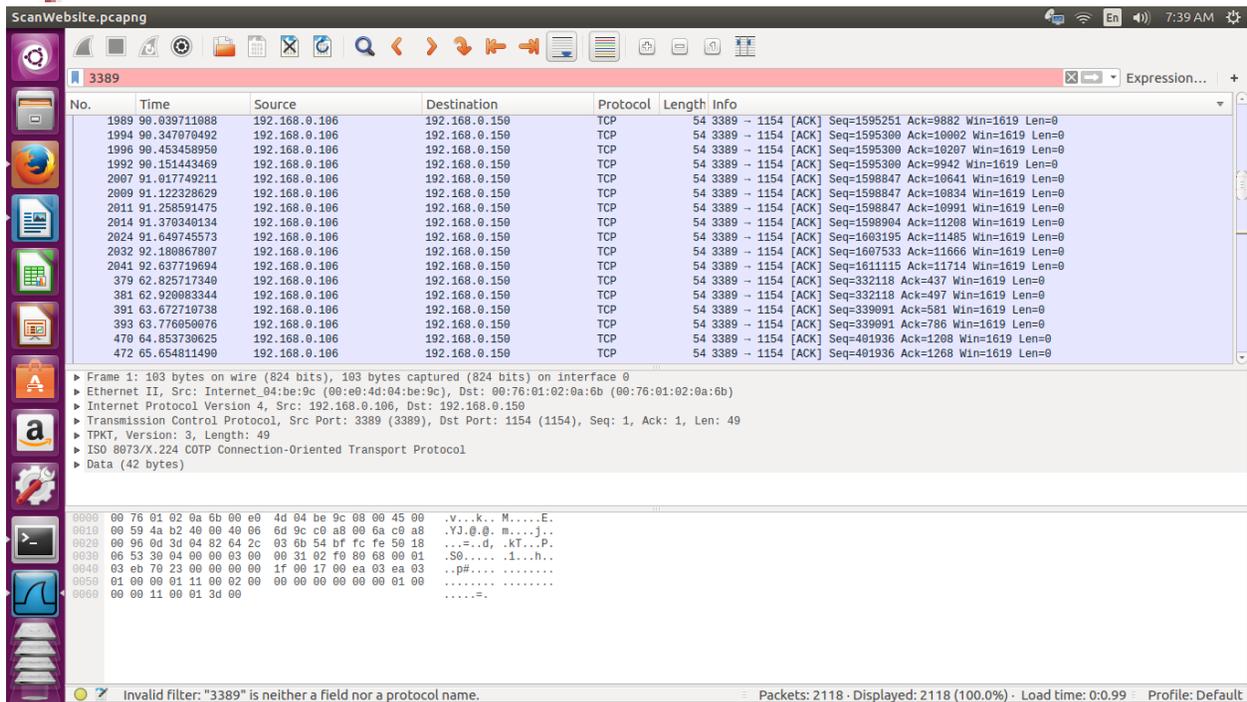
Packet bytes:

```
0000 00 76 01 02 0a 6b 00 e0 4d 04 be 9c 00 00 45 00 .v...k..M....E.
0010 00 59 4a b2 40 00 40 06 6d 9c c9 a8 00 6a c9 a8 .Yl@.0.m....j.
0020 00 96 0d 3d 04 82 64 2c 03 0b 54 bf fc fe 50 18 ...=.d,.kT...P.
0030 06 53 30 04 00 00 03 00 00 31 02 f0 00 68 00 01 .S0....i...h...
0040 03 eb 79 23 00 00 00 00 1f 00 17 00 ea 03 ea 03 .pR.....
0050 01 00 00 01 11 00 02 00 00 00 00 00 00 01 00 .....
0060 00 00 11 00 01 3d 00 .....=.
```

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 image shows a Wireshark capture of network traffic. The main pane displays a list of packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. A red arrow points to packet 1, which is a COTP (Connection-Oriented Transport Protocol) packet from 192.168.0.106 to 192.168.0.150. The packet details pane shows the following structure:

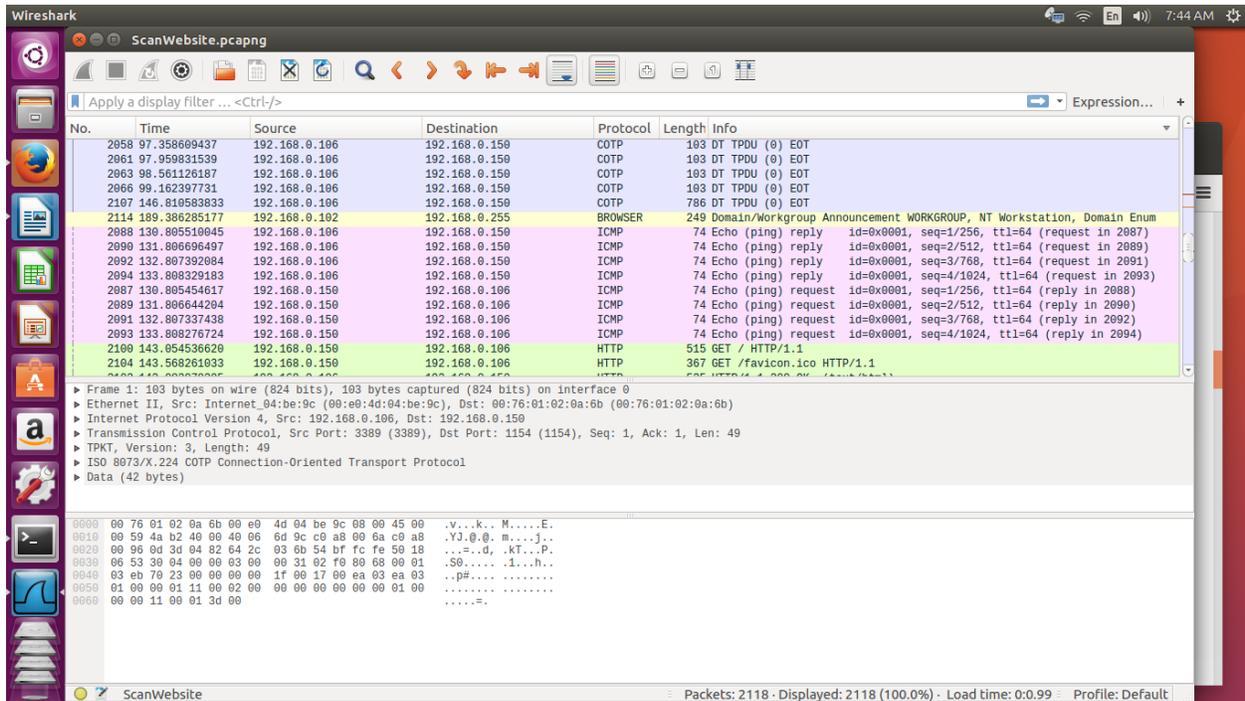
- Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
- Ethernet II, Src: Internet\_04:be:9c (08:e0:4d:04:be:9c), Dst: 00:76:01:02:0a:6b (00:76:01:02:0a:6b)
- Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.150
- Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 1154 (1154), Seq: 1, Ack: 1, Len: 49
- TPKT, Version: 3, Length: 49
- ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
- Data (42 bytes)

The packet bytes pane shows the raw data in hexadecimal and ASCII format:

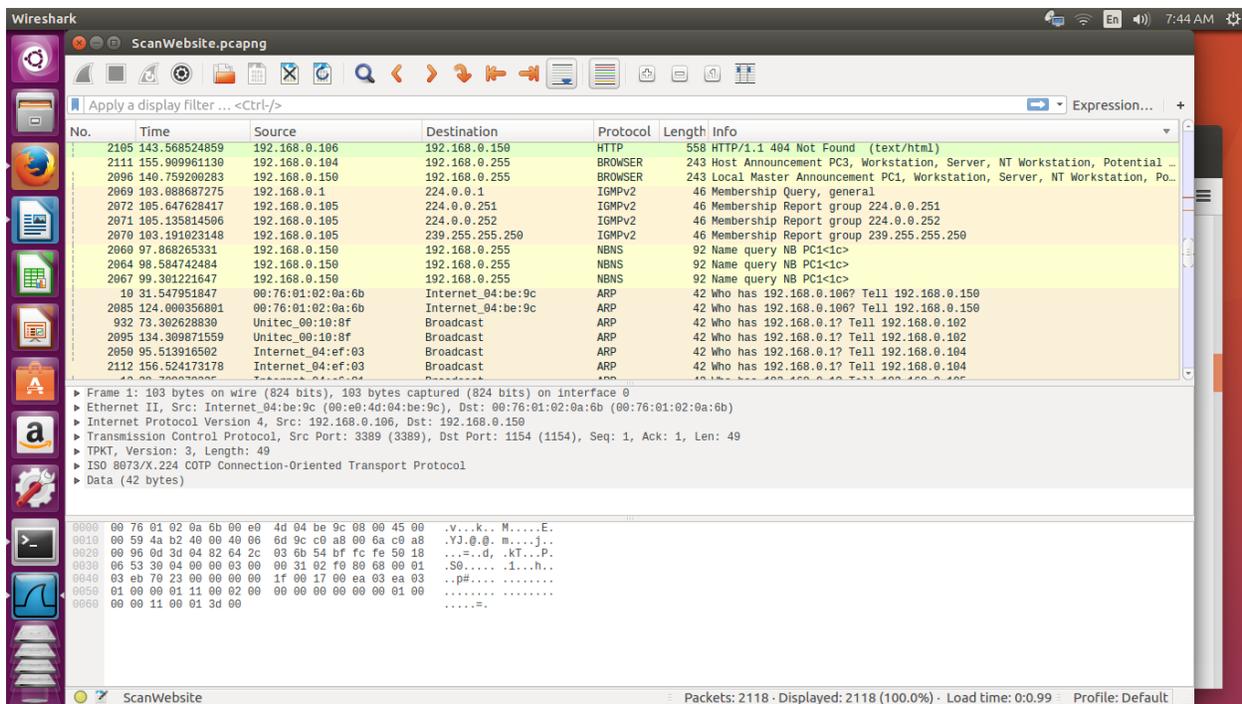
```

0000 00 76 01 02 0a 6b 00 e0 4d 04 be 9c 08 00 45 00  .v...k..M....E.
0010 00 59 4a b2 40 00 40 06 6d 9c c0 a8 00 6a c0 a8  .YJ.@.@.m....j..
0020 00 96 0d 3d 04 02 04 2c 03 00 54 bf fc fe 50 18  .:..d, .kt...P.
0030 06 53 30 04 00 00 03 00 00 31 02 f0 00 68 00 01  .S0.....1...h..
0040 03 eb 70 23 00 00 00 00 1f 00 17 00 ea 03 ea 03  ..pR.....
0050 01 00 00 01 11 00 02 00 00 00 00 00 00 01 00  .....
0060 00 00 11 00 01 3d 00  .....=.
```

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.

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

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

Keveith, 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](https://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallWinInstall.html) [Accessed 17 Sep. 2016].



**EssayCorp** 5 years ★★★★★