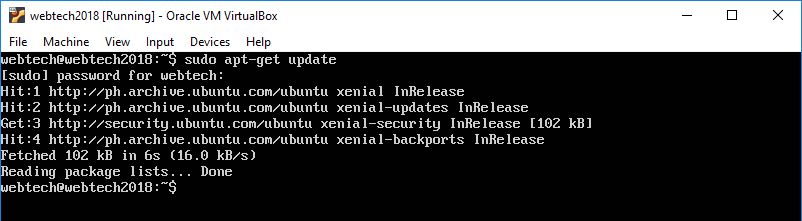
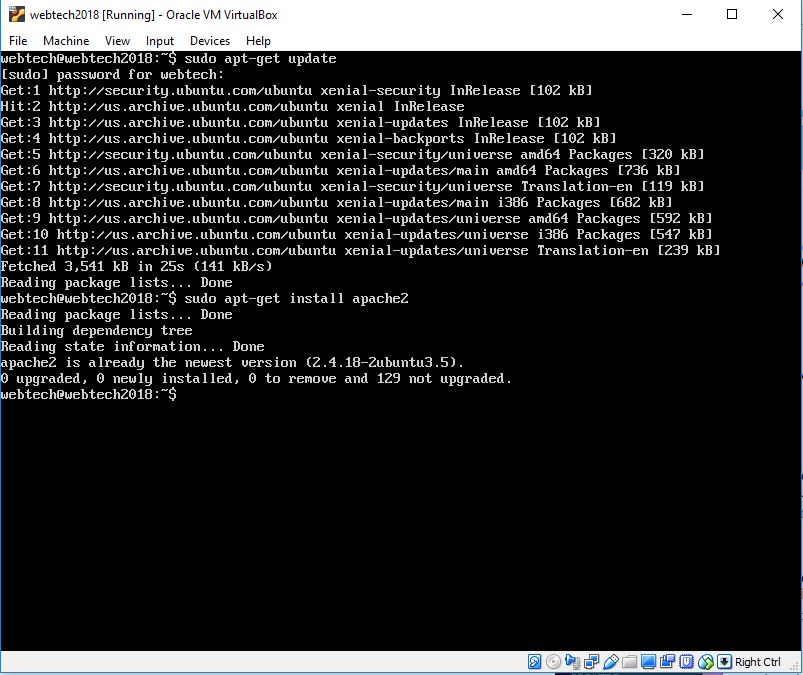
VIRTUAL HOSTS: [**www.group6a.org**](http://www.group6a.org) **|** [**www.group6b.org**](http://www.group6b.org)**|** [**www.grou6c.org**](http://www.grou6c.org)

* Log in to ubuntu server using the username: webtech, and password: 2018. After logging in enter the following commands to update the ubuntu system, and to install apache2.
* **sudo apt-get update**



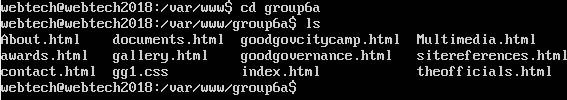
* **sudo apt-get install apache2**



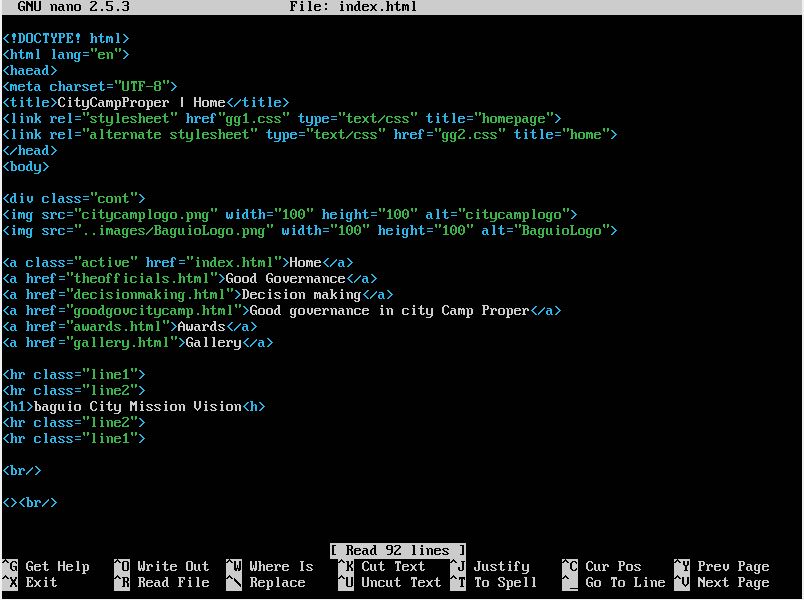
* Go to **cd /var/www** and create a folder that will represent the domain name, [www.group6a.org](http://www.group6a.org), [www.group6b.org](http://www.group6b.org), [www.group6c.org](http://www.group6c.org), webtech1.negotiage.org, webtech1.access.org, webtech1.ssi.org, and webtech1.secure.org.
* **sudo mkdir group6a**
* **sudo mkdir group6b**
* **sudo mkdir group6c**
* **sudo mkdir webtech1negotiage**
* **sudo mkdir webtech1access**
* **sudo mkdir webtech1ssi**
* **sudo mkdir webtech1secure**
* Check if the folders are created, type **ls** and it will show you the folders that were created inside the /var/www directory.



* For the folders group6a, group6b, and group6c each will contain the contents of the three advocacy websites, css and html files. Below is an example contents of group6a.



* To create or edit an html or css files, type the command,
* **sudo nano index.html**
* When done editing press **ctrl + x** to exit the file and press **y** to save, **n** otherwise.

****

* **sudo nano gg1.css**

****

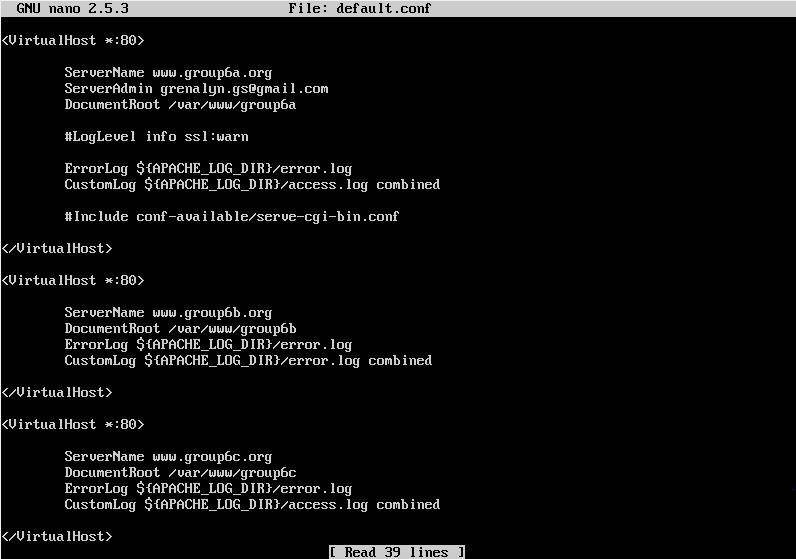
* For the configuration of the virtual hosts go to **cd /etc/apache2**. Type **ls** to see the contents residing in this directory.
* **mods-enabled** contain modules that are functioning inside the apache2 like deflate, expires, rewrite and the like that you can enable or disable.
* **sudo a2ensite deflate** (*to enable the deflate module.*)
* **sudo a2dissite deflate** (t*o disable the deflate module*)

****

* **sites-available** whenever you want to configure a virtual host, go to this folder. Enter **sudo nano <filename>.conf** to create a configuration file. The created default.conf will hold the codes for the configuration of the virtual hosts [www.group6a.org](http://www.group6a.org), [www.group6b.org](http://www.group6b.org), [www.group6c.org](http://www.group6c.org).

****

* This are the codes inside default.conf**.** For each virtual host the code must start with **<VirtualHost \*:80>**. Followed by the server name, for instance group6a will have the server name www.group6a.org, server alias can also be added but make sure that it won’t have the same name as the server name. Server alias can be named to group6a.org. Add the server admin email, followed by DocumentRoot. The document root will be the location of the created folder for group6a. That folder is under **/var/www**. Add the **ErrorLog ${APACHE\_LOG\_DIR}/error.log** and **CustomLog ${APACHE\_LOG\_DIR}/access.log** and finally include **</VirtualHost>** to finish the code. Save and exit virtual host.

****

**VIRTUAL HOST:** webtech1.negotiage.org

* After saving the virtual host you will have to enable the sites and reload them.
* **sudo a2ensite default.conf**
* **sudo service apache2 restart**
* Create a configuration file for group6a in the /etc/apache2/sites-available.
* **Sudo nano wgroup6a.conf**
* Configure the file to enable compression of the content. The compression will be limited to html and css files only. The client must be able to cache png, jpg and gif files for up to 24 hours.



VIRTUAL HOST: **webtech1.negotiage.org**

* Go to webtech1negotiage directory. Inside this folder create dummy files named content.html and context.txt.
* **cd /var/www/webtech1negotiage**
* **sudo nano content.html**





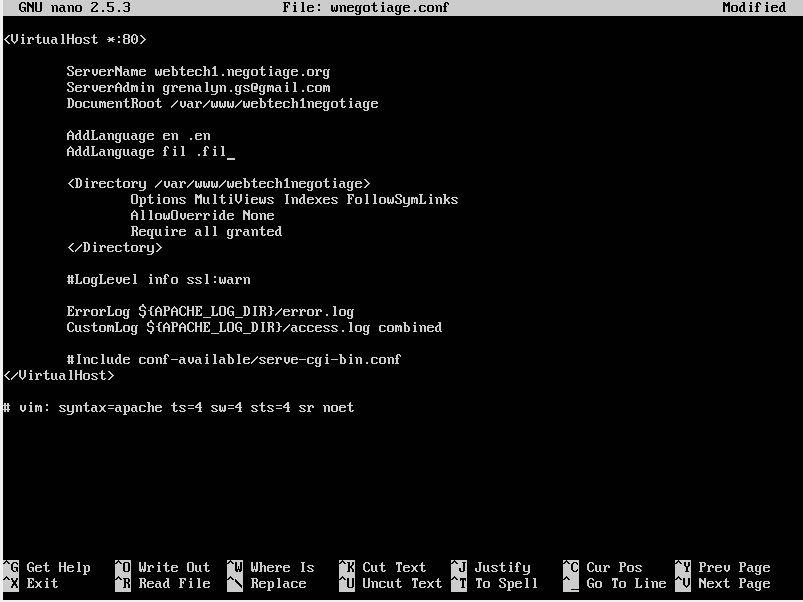
* **sudo nano context.html**
* Create another dummy files named language.html.en and language.html.fil
* **sudo nano language.html.en**



* **sudo nano language.html.fil**



* In the **/etc/apache2/sites-available** directory create a configuration file for webtech1negotiage. Save and exit. Enable the file **sudo a2ensite wnegotiage.conf**

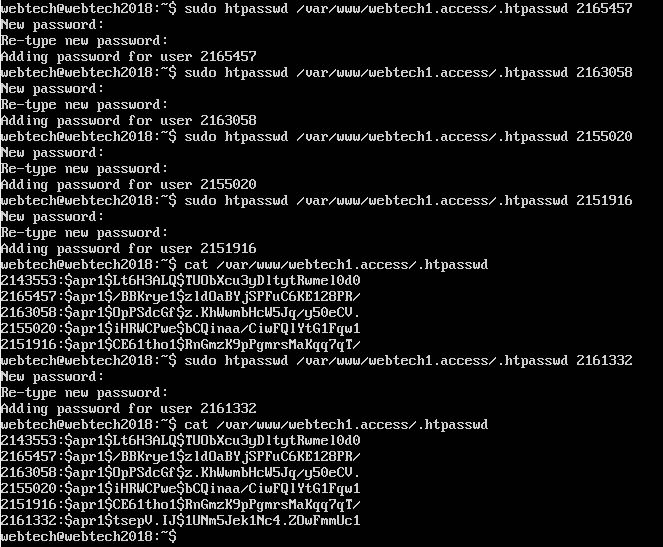


VIRTUAL HOST: **webtech1.access.org**

* Create a file named index.html in the document root webtech1access.
* Configure the virtual host that will only allow requests from host with .\*edu or \*.org. Only GET, HEAD, and POST will be allowed. And POST requests will only be allowed for valid and authorized users. The ID Number of each member of the group will serve as their user credentials.
* In /etc/apache2/sites-available create a configuration file named access.conf. The configuration file will look like this.



* Save the file and don’t forget to enable it before restarting.
* Type the command bellow to create htpasswd in/var/www/webtech1.access. Only place -c for the first user only, when you add another user neglect the -c on the command.



VIRTUAL HOST: **webtech1.ssi.org**

* Configure the file for webtech1.ssi.org to enable server-side includes on these virtual host.
* Create a configuration file named wssi.conf inside sites-available. This is what the configuration file for webtech.ssi.org looks like. The end of Options there must include, Include. XBitHack is also turned on.



VIRTUAL HOST: **webtech1.secure.org**

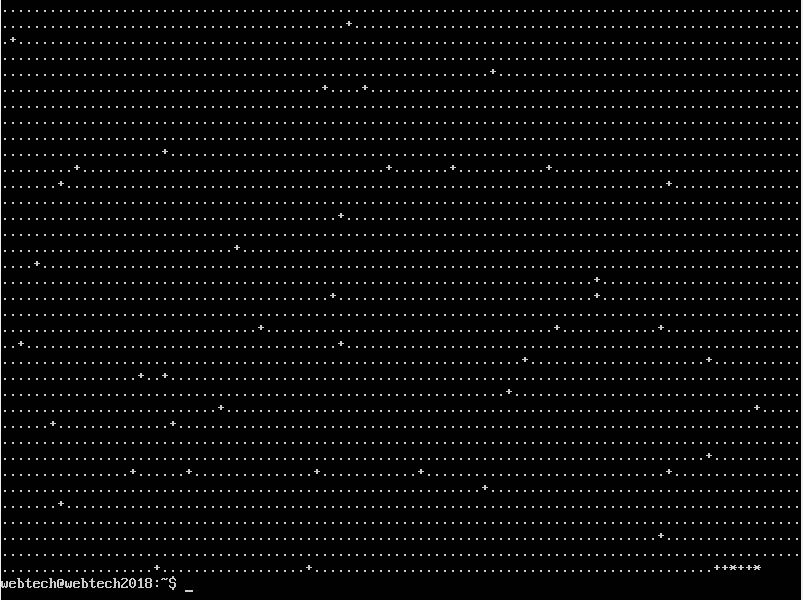
* Create index.html file in the folder webtech1secure. In sites-available, create wsecure.conf. This is the code inside wsecure.conf file.



* The commands below were used for the configuration of the webtech1.secure.org.
* Enter the command below to create selfsigned key and certificate. You’re your password then press enter key.



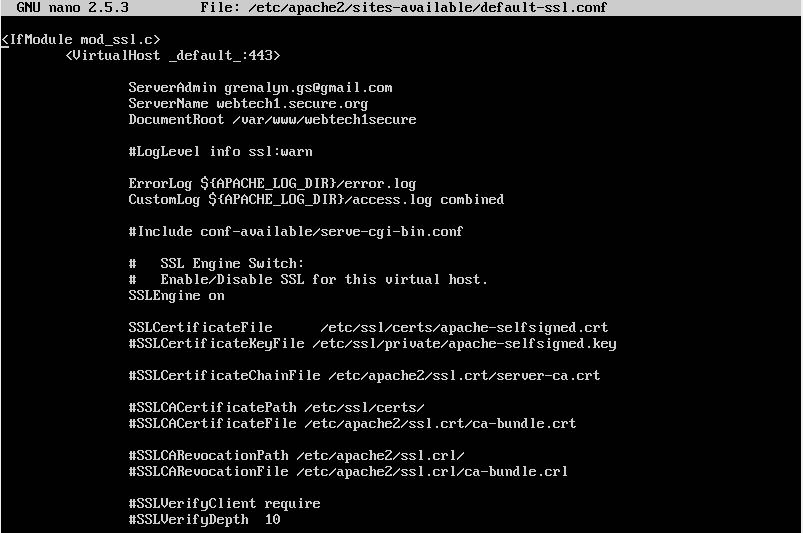
* After typing **sudo openssl shparam -out /etc/ss/certs/dhparam.certs** it will generate something like this a strong DH group.

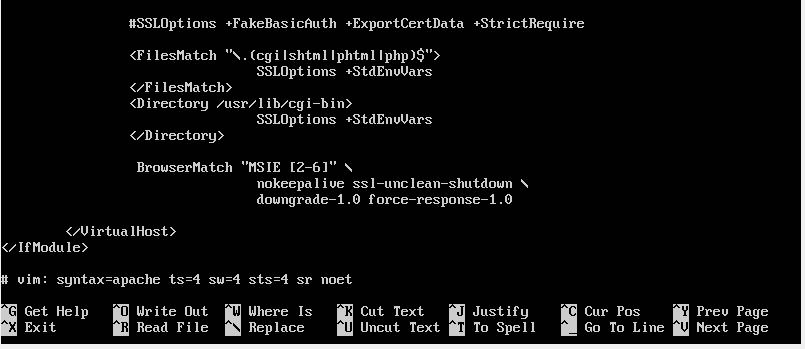


* **sudo nano /etc/apache2/conf-available/ssl-params.conf**, enter the following codes.



* Modify the default apache SSL virtual host file.
* **sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak**
* Now that the default ssl configuration file has been modified, type the following code to make some adjustments.
* **sudo nano /etc/apache2/sites-available/default-ssl.conf**





* **sudo nano /etc/apache2/sites-available/000-default.conf**



* To allow SSL traffic there will be an adjustment need too be done in the enabled ufw firewall.
* **sudo ufw app list**
* HTTPS traffic: Allow Apache Full
* **sudo ufw allow ‘Apache Full’**
* **sudo ufw delete allow ‘Apache’**
* Some settings in SSL snippet needs to enable mod\_ssl and mod\_headers.
* **sudo a2enmod ssl**
* **sudo a2enmod headers**
* enable SSL Virtual Host
* **sudo a2ensite default-ssl.conf**
* enable ssl-params.conf file
* **sudo a2enconf ssl-params**
* to check if there are any syntax error, type
* **sudo apachectl configtest**
* restart the service

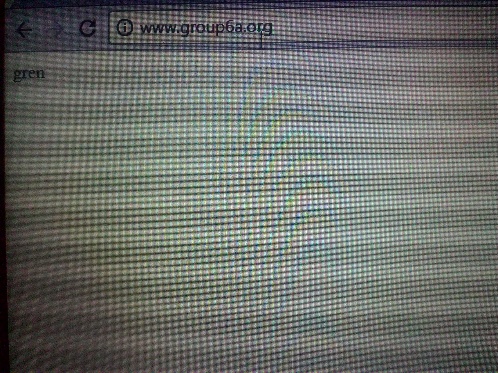
**- sudo systemctl restart apache2**

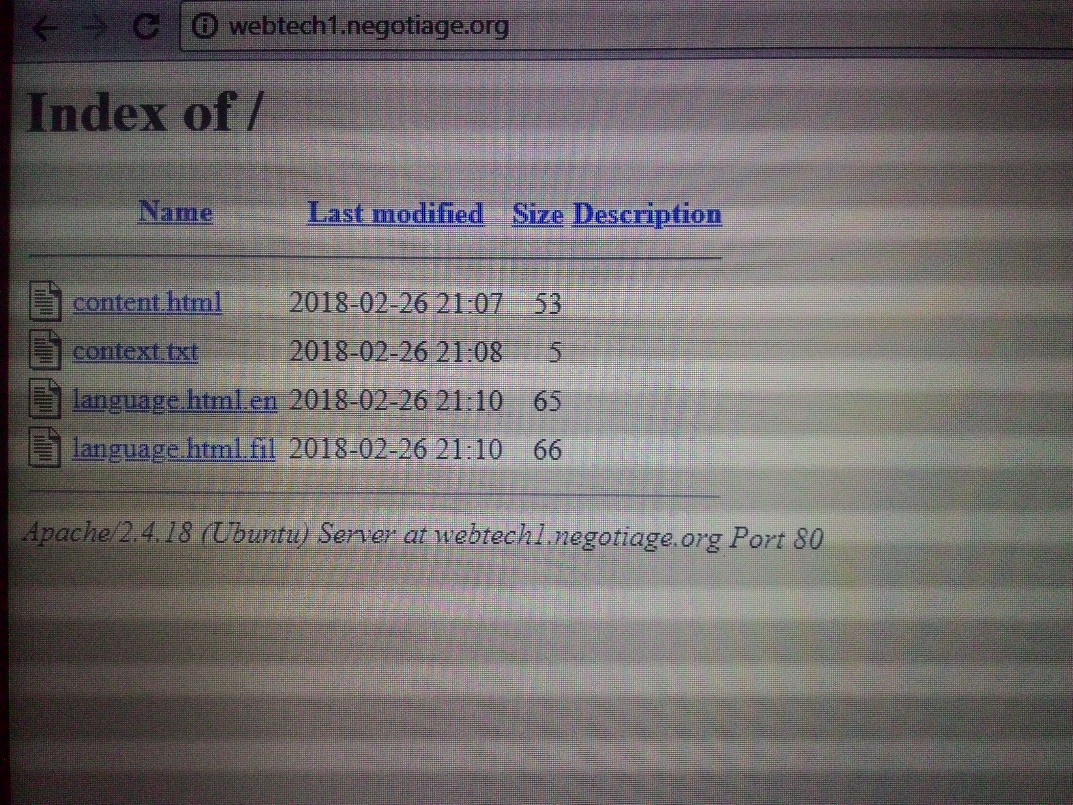
* Disable 000-default.conf located in the sites-available by typing the command **sudo a2dissite 000-default.conf**
* Disable default-ssl.conf.bak
* You can see all the enabled configuration files for the virtual hosts inside **sites-enabled** foler.

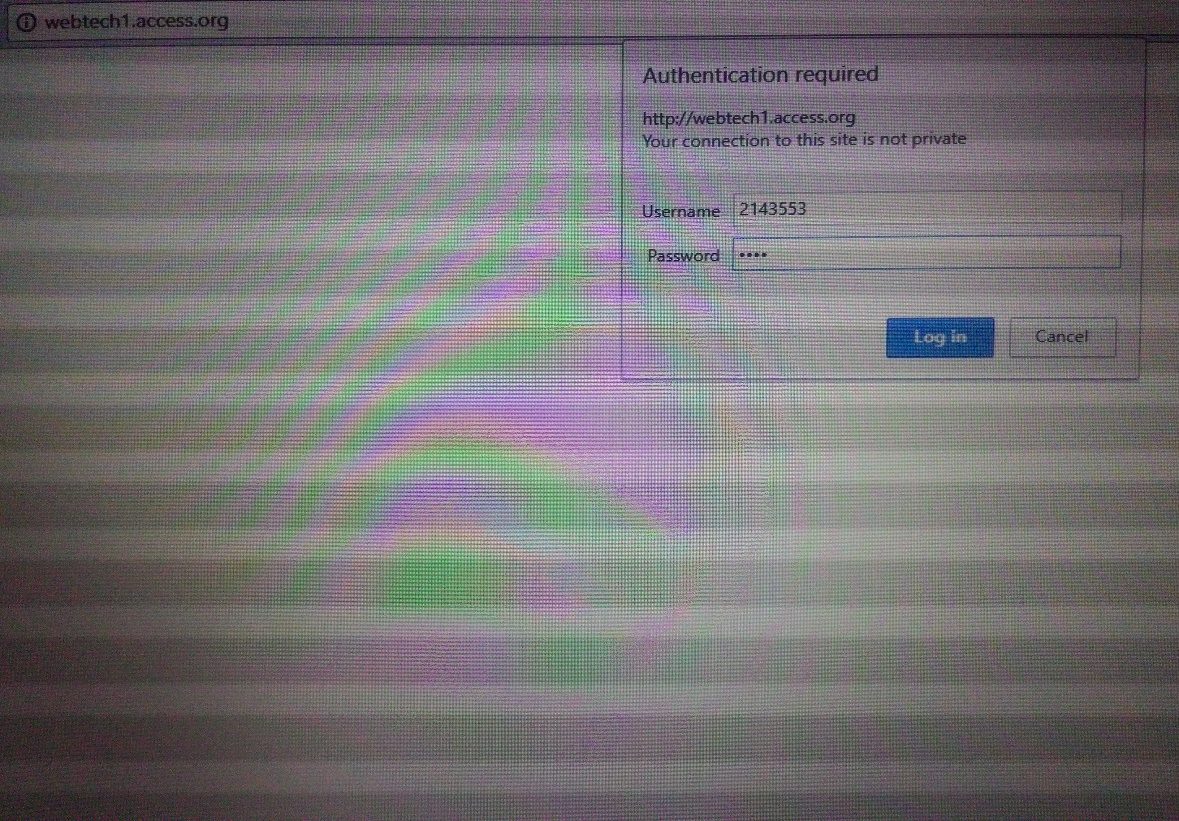
===================================================

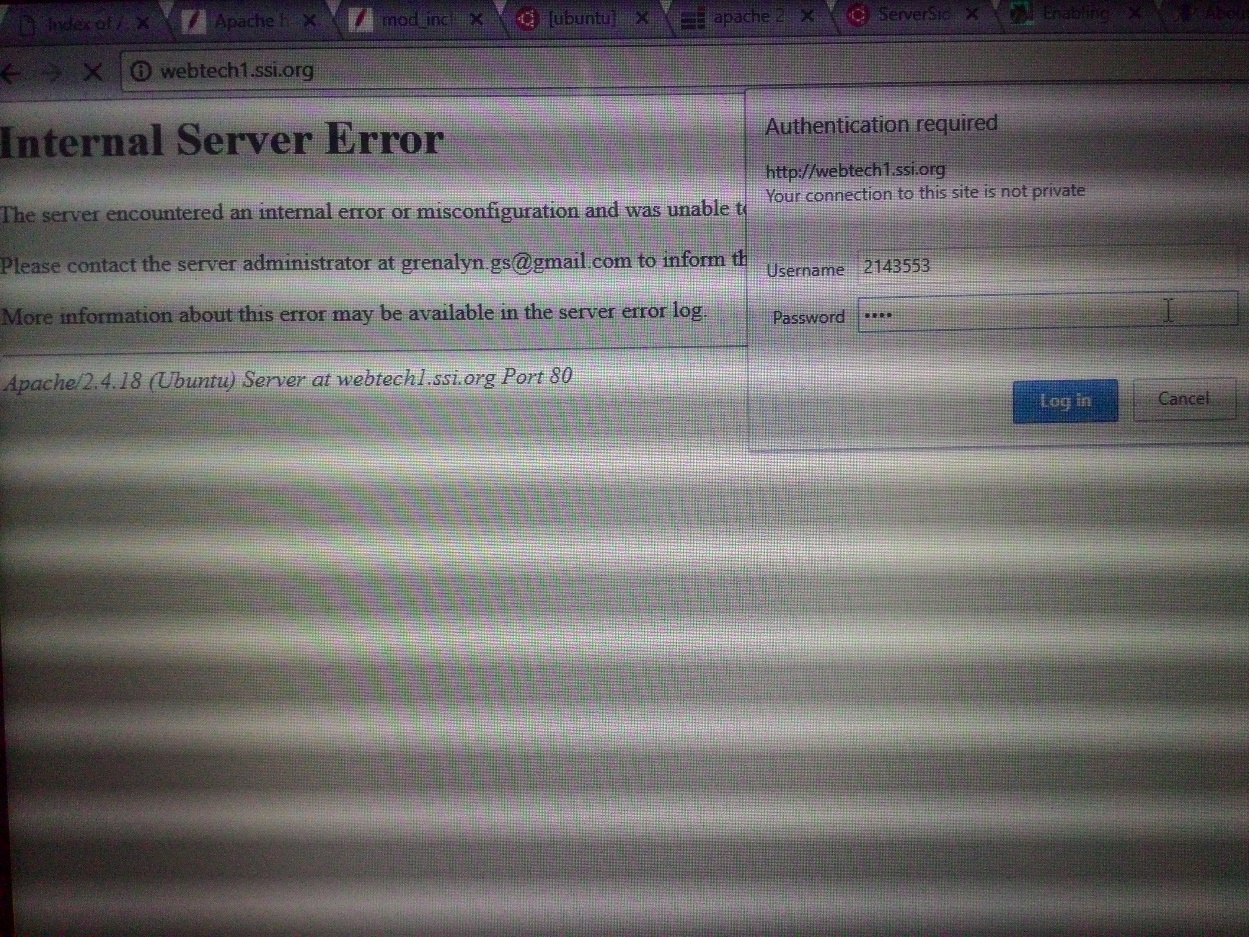
IMAGES FOR EACH SITE ADDRESS THAT WAS ACCESSED. (kaso di ko na ulit maaccess problema ko nagiiba yung ip address sa ubuntu…)

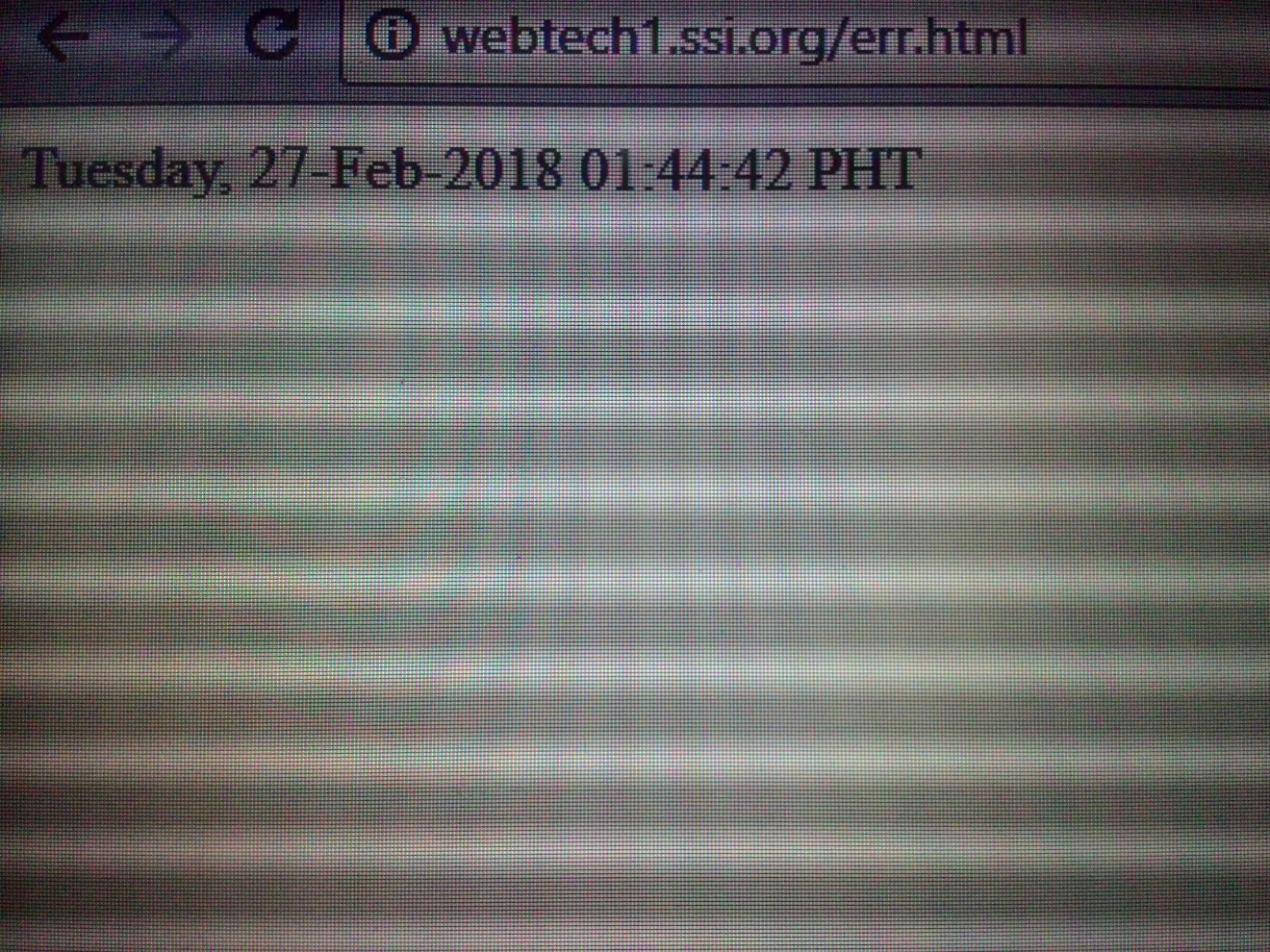












* Edit the hosts file in your host terminal using any text editor. For this example we used Notepad++. Make sure that you run it as administrator. Go to **/windows/system32/drivers/etc** inside this directory is a file named host where you will add the IP address and the site address (www.<ServverName>.org) declared in the default.conf file.

