

# Proj 3 COSC366

## Task 2.1

Vim index.txt -> empty file

Vim serial.txt -> enter "1000"

Vim serial -> enter 1000

Cp /usr/lib/ssl/openssl.cnf .

```
openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
```

create password: crypt

country name code: US

state or province name: Tennessee

locality name: Knoxville

organization name: UTK

organizational unit name: EECS

common name: utkpkilabaustinstrobel.com

email: [utkeecs@gmail.com](mailto:utkeecs@gmail.com)

➔ She didn't say what to name all of this shit

## Task 2.2

```
openssl genrsa -aes128 -out server.key 1024
```

password: crypt

```
openssl rsa -in server.key -text
```

```
Terminal File Edit View Search Terminal Help
65:89:3d:a5
coefficient:
00:89:54:b7:f0:b7:c2:68:e3:22:6a:70:75:39:25:
15:9c:e1:30:0f:b0:1f:8f:39:52:58:49:f5:47:4d:
c0:28:e6:4d:a1:4f:44:19:7d:ae:e6:04:b9:bb:a3:
84:39:bc:51:d6:86:a0:c4:0c:fa:d5:52:9c:6f:ec:
a7:75:1d:cb:87
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDBweNQA8lflQuQXYCH6TyKJKdLjqXiS78gXNivGYhelZ+cjNF6
kBKDQH96jCEoDRC1Mg0YjguiXahYKbGFhEjPTcv7Rf+KNJxwXhZy9fIU2GeVH1DK
9/0UaB1HUpGIr1GRttS9yJ1aHts+LBMuCYWrXgFsIWuU8ebMFeQABarSOQIDAQAB
AoGBAMBI+Zy71UnNMWe400iOGC2ESJ58V3Xn9Cpa06A4d5ReasNDINTATA8DoD9u
96y2oqEfpc17kmI1Dk9IOUumx1VxQXmv09xI0+KefY4GYiBnEt5PgGJeAvbRenS5
QPK+fSvqkLIO4SHL+6vMIk9U+qepeCOUoalV2VDdYyCBdplxAkEA643qX50vOgU3
eHdLqo2IF56vtqZYPVY4N90uxAFG/NLdSwiIhyDuAdz8U1ENST87Lfo0uplq9zmv
t+dQ4qYONQJBANKT00xk2bXwxk7II1jKaLef11HxpBMOJ+XKQ5hosubVZlUSOB/1
I8x8fiQCHIC9GetsX3MGndgbWKpY8FkHhHUCQQDdp8+SZbEZIeu02oNDXKdhwpuK
foGuRkHkn6fwI3lmU26UM3gtPBL7e12dcTnVYUDpBNNzWABF2Wy2217LyIK5AkA2
EqKuilMxmKOCJXiWK1vak0waeb+VORRbuKXE9FXEWtYtUEFjS3LG5s0JeBVTpbuL
LcgQ5IkR3mvVSoNliT2lAkEAiVS38LfCaOMianB10SUVnOEwD7AfjzLSWEn1R03A
K0ZNoU9EGX2u5gS5u60E0bxR1oagxAz61VKcb+yndR3Lhw==
-----END RSA PRIVATE KEY-----
[11/14/2023 14:32] seed@ubuntu:~$
```

password: crypt

openssl req -new -key server.key -out server.csr -config openssl.cnf

country name code: US

state or province name: Tennessee

locality name: Knoxville

organization name: UTK

organizational unit name: EECS

common name: utkpkilabaustinstrobel.com

email: [utkeecs@gmail.com](mailto:utkeecs@gmail.com)

challenge password: snoop

an optional company name: CCI

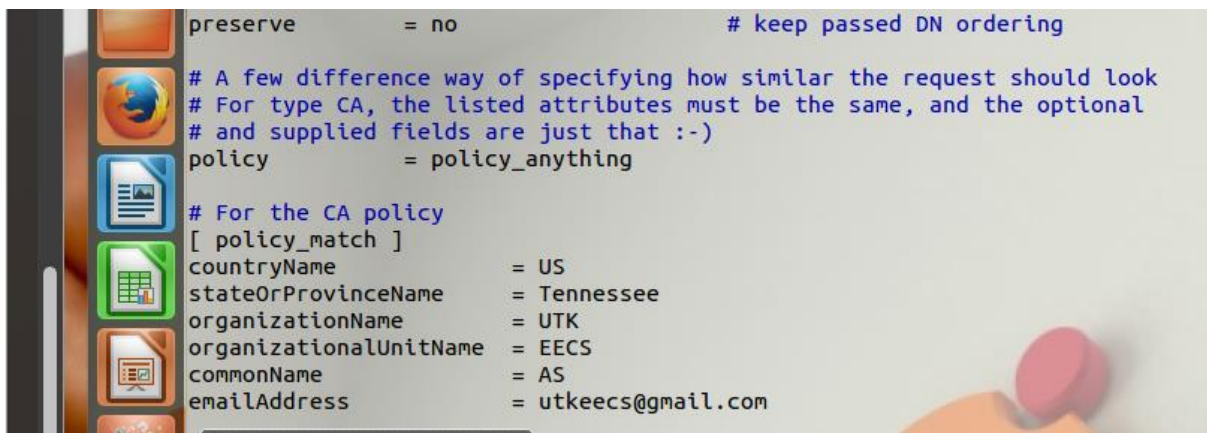
had to do this -> vim openssl.cnf and search for "policy":

If OpenSSL refuses to generate certificates, it is very likely that the names in your requests do not match with those of CA. The matching rules are specified in the configuration file (look at the [polymatch] section). You can change the names of your requests to comply with the policy, or you can change the policy.

The configuration file also includes another policy (called policy anything), which is less restrictive. You can choose that policy by changing the following line:

"policy = policy\_match" change to "policy = policy\_anything".

also changed the specific policy\_match shit -> **DID NOT DO THIS THE SECOND TIME AROUND**



Mkdir demoCA

Cd demoCA

Vim index.txt -> leave it empty

Vim serial -> enter "1000"

Vim serial.txt -> enter "1000"

Mkdir newcerts

Cd newcerts

Vim index.txt -> leave it empty

cd

openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf (WITHOUT THE BACKSLASH)

password: crypt

answer "y" to both questions

## Task 2.3

Sudo vim /etc/hosts

below "127.0.0.1          ubuntu," I put **127.0.0.1          UTKPKILabaustinstrobel.com**

I was somehow able to edit the file by adding this: `!w !sudo tee %` and then answering the subsequent questions (I just pressed "enter") and then doing `!q!` and that somehow worked \*shrugs\*

For some reason, I had to log out (power down the machine) and log back in to actually see my files again – the files I had just created for this project



2023-11-12  
19-24-28.mkv

```
cp server.key server.pem
```

```
cat server.crt >> server.pem
```

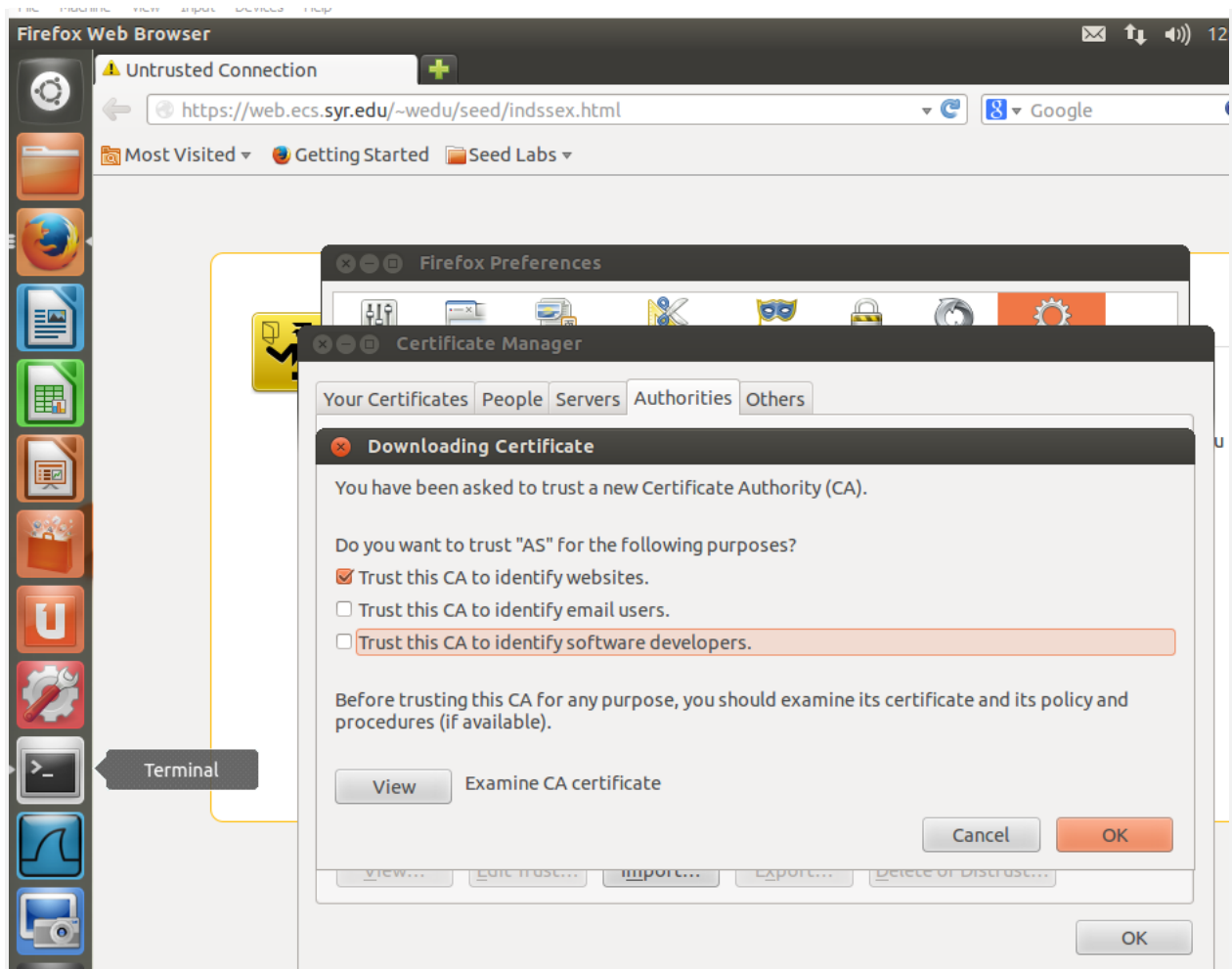
```
openssl s_server -cert server.pem -www
```

➔ I always use "crypt" as mi contraseña

Enter this bad boy into the local Firefox on the VM: [https:// UTKPKILabaustinstrobel.com:4433/](https://UTKPKILabaustinstrobel.com:4433/)

Use Firefox in the VM locally

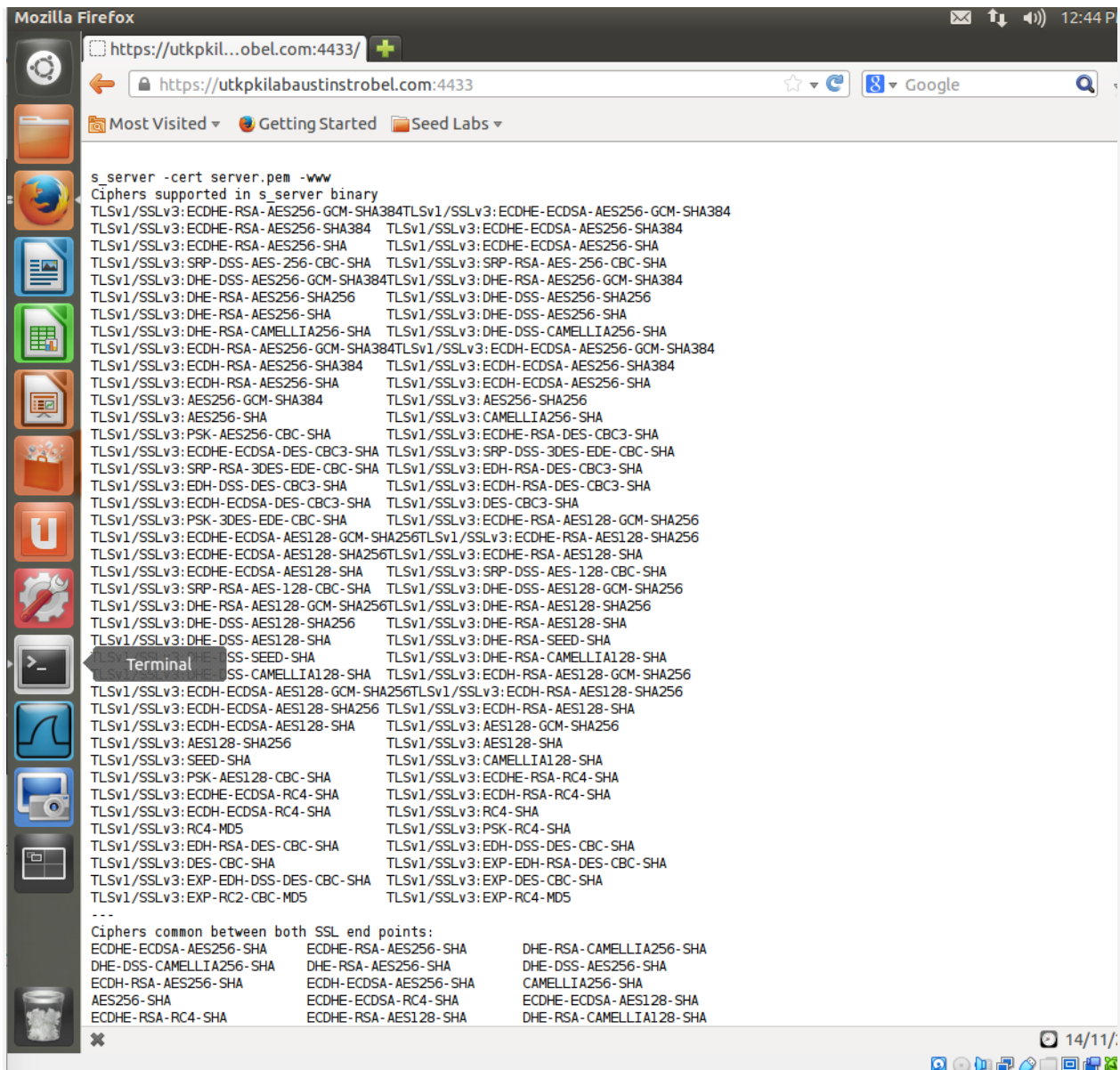
In Firefox, go to Edit -> Preferences -> Advanced -> Certificates -> View Certificates



Make sure the s\_server is running

Go to [utkpkilabaustinstrobel.com:4433](https://utkpkilabaustinstrobel.com:4433)

Just verifying that it actually works:



Now go back to `server.pem` -> `vim server.pem`

Modify a single character (one byte)

I'm going to change this first character from a "w" to a "z":

Original:



Wplb1fn/OQtWzYfODXQ3Cd40HARS7qlRuiVcg+8Y8V50qa+EREKPNGvUntiwYnFC  
A2UQk0CbUmEGpb0WkTPzrqPjCqXgNzHXL497gIuKk74WFfpYPrId003nT2vJ0p3r  
OFG417sDJ3sBeDo4RV+pgXx3fWtq0Bevgfkitc2mIX/wgWdl/mkzcfTfHcpqtXJs  
LWnICsdEj+vWyulI5HdP1nA/le6Eplexe1dvNTXQgepvI+W2yF6RS9nXg5ogWpro  
1i6TBVYAwkDVqg0TXAzo6PXSH1G0y+5enj9l7no01Ao8pCmgk3v1x+hycJZ0i/r2  
0tymeUGs/djoAk0TepAsk6QGaC0ZwvaTv11I7EHPTP/FaMmqmS836+rCKD/a1Dnn  
oQIFrRs303tGtCB82ZR45pur/4nIGt8C6v9h02DITnuGi65VM0muntKYOKAFQaOC  
boJwqjMsVdVhay0/mNV32889rdaLmGhWl8N1UI3Me+uIdm5BcXcXM81DXkJa08/S  
cEXMGGF63rshYIwXG8UefZxJJ+BBIWVtuVrzRRjoIk/0oBa7XLg2Xo2tZ3NIVrhv  
eX3wp1mcb08yR5VavwfMv4dfnZw3NQEbL08IajmyBHeqUILzwG5AfG0MAH6a8KAC  
uwrtGrv36uK/yVepAajVgGp+5aMrJf2bRno6pYQM0bDX2VGUi18wz5kN2TbsE4dE  
qbkcIaHfvuge+rRHvCxL/swudr2SBfdSIgdmQT97LmTBEGNpcl3cdjJwAaw4N38j  
M3DnxtYKQgeyzn7GafVAd37NwTL36MFzgmVUhmWU4rw=

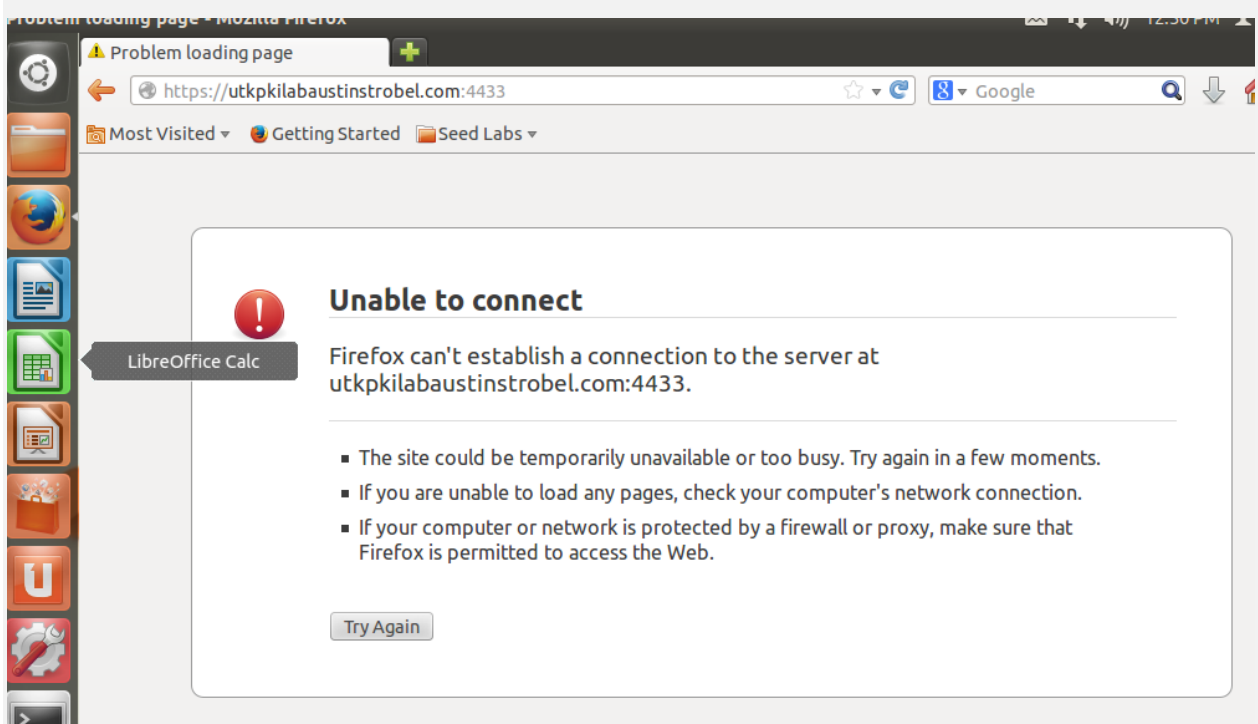
Modified -> this guy will fail:

Wplb1fn/OQtWzYfODXQ3Cd40HARS7qlRuiVcg+8Y8V50qa+EREKPNGvUntiwYnFC  
A2UQk0CbUmEGpb0WkTPzrqPjCqXgNzHXL497gIuKk74WFfpYPrId003nT2vJ0p3r  
OFG417sDJ3sBeDo4RV+pgXx3fWtq0Bevgfkitc2mIX/wgWdl/mkzcfTfHcpqtXJs  
LWnICsdEj+vWyulI5HdP1nA/le6Eplexe1dvNTXQgepvI+W2yF6RS9nXg5ogWpro  
1i6TBVYAwkDVqg0TXAzo6PXSH1G0y+5enj9l7no01Ao8pCmgk3v1x+hycJZ0i/r2  
0tymeUGs/djoAk0TepAsk6QGaC0ZwvaTv11I7EHPTP/FaMmqmS836+rCKD/a1Dnn  
oQIFrRs303tGtCB82ZR45pur/4nIGt8C6v9h02DITnuGi65VM0muntKYOKAFQaOC  
boJwqjMsVdVhay0/mNV32889rdaLmGhWl8N1UI3Me+uIdm5BcXcXM81DXkJa08/S  
cEXMGGF63rshYIwXG8UefZxJJ+BBIWVtuVrzRRjoIk/0oBa7XLg2Xo2tZ3NIVrhv  
eX3wp1mcb08yR5VavwfMv4dfnZw3NQEbL08IajmyBHeqUILzwG5AfG0MAH6a8KAC  
uwrtGrv36uK/yVepAajVgGp+5aMrJf2bRno6pYQM0bDX2VGUi18wz5kN2TbsE4dE  
qbkcIaHfvuge+rRHvCxL/swudr2SBfdSIgdmQT97LmTBEGNpcl3cdjJwAaw4N38j  
M3DnxtYKQgeyzn7GafVAd37NwTL36MFzgmVUhmWU4rw=

Basically now, the server can't get up and running again:

Step 4 #1:

```
[11/14/2023 12:48] seed@ubuntu:~$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
unable to load server certificate private key file
3073738952:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1319:
3073738952:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:381:Type=RSA
3073738952:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:115:
3073738952:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1319:
3073738952:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:381:Type=PKCS8_PRIV_KEY_INFO
3073738952:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1 lib:pem_pkey.c:132:
[11/14/2023 12:48] seed@ubuntu:~$
```

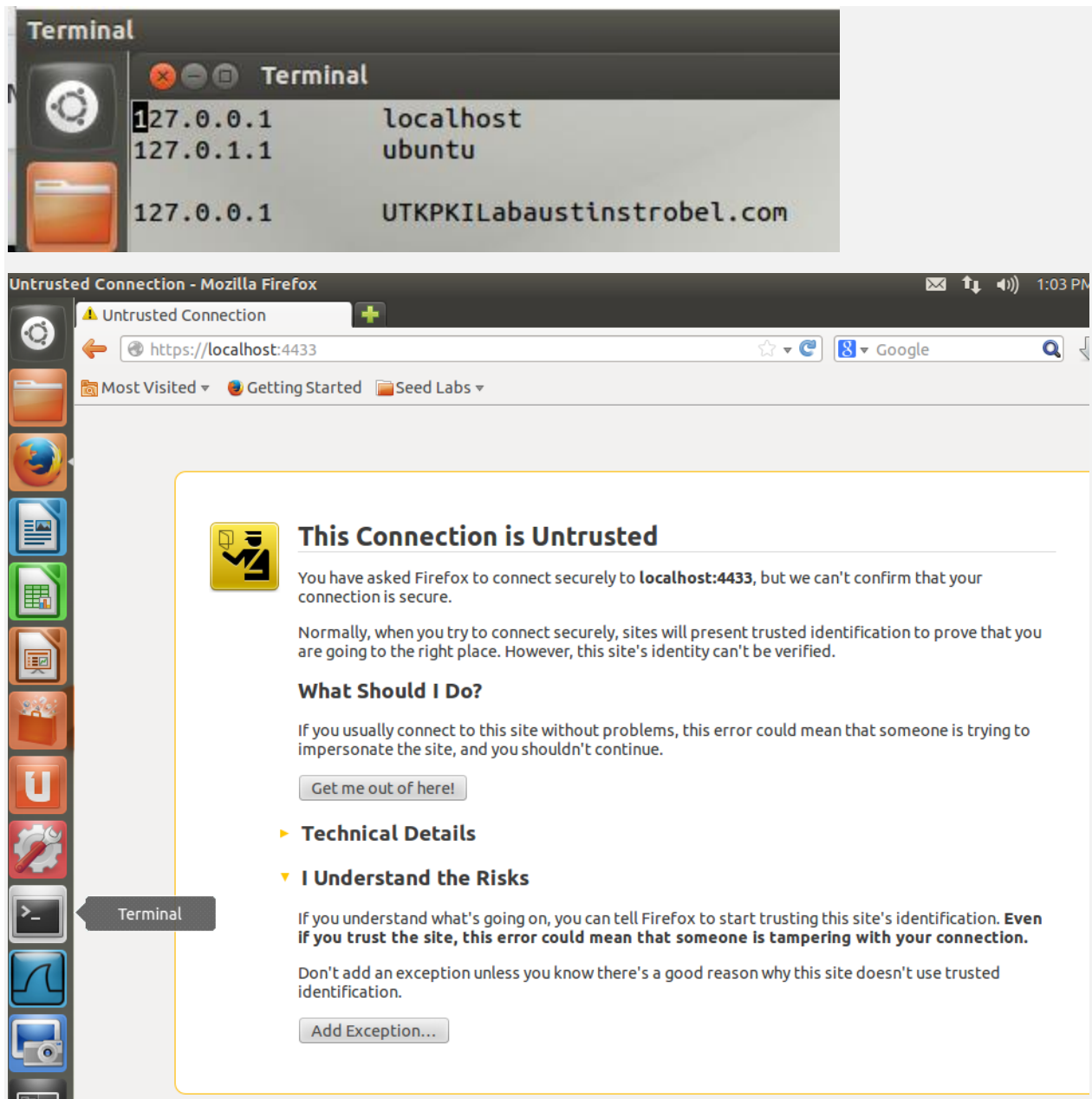


Now change the server.pem file back to how it was with the “w” instead of the “z” -> should run again now

Step 4 #2:

The certificate is only valid for the domain name that I used to create it – utkpkilabaustinstrobel.com. Localhost is a different domain name than utkpkilabaustinstrobel.com and does not share that certificate. However, both localhost and utkpkilabaustinstrobel.com do share the same IP address.

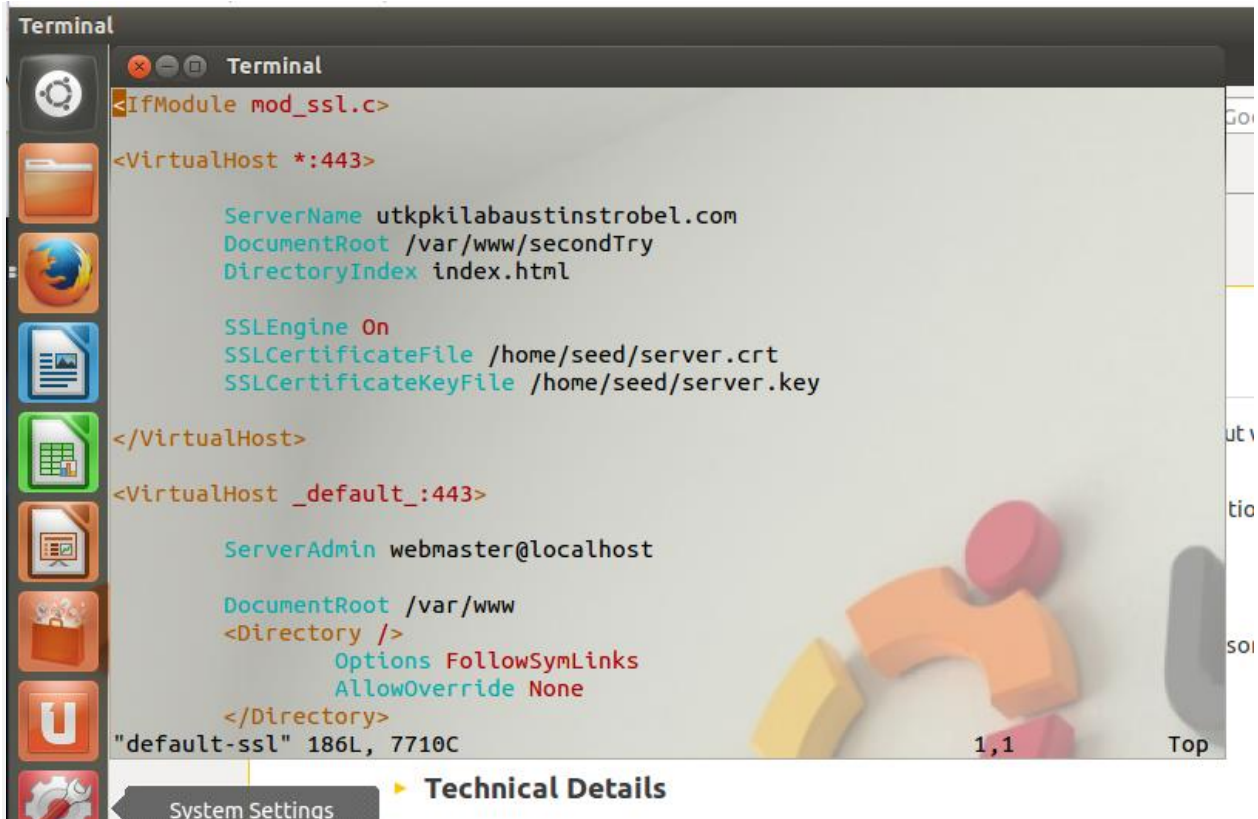




## 2.4 Task 4:

From home directory, cd /etc/apache2/sites-available, then sudo vim default-ssl

➔ Create a new instance of virtual host:



```
Terminal
<IfModule mod_ssl.c>

<VirtualHost *:443>

    ServerName utkpkilabaustinstrobel.com
    DocumentRoot /var/www/secondTry
    DirectoryIndex index.html

    SSLEngine On
    SSLCertificateFile /home/seed/server.crt
    SSLCertificateKeyFile /home/seed/server.key

</VirtualHost>

<VirtualHost _default_:443>

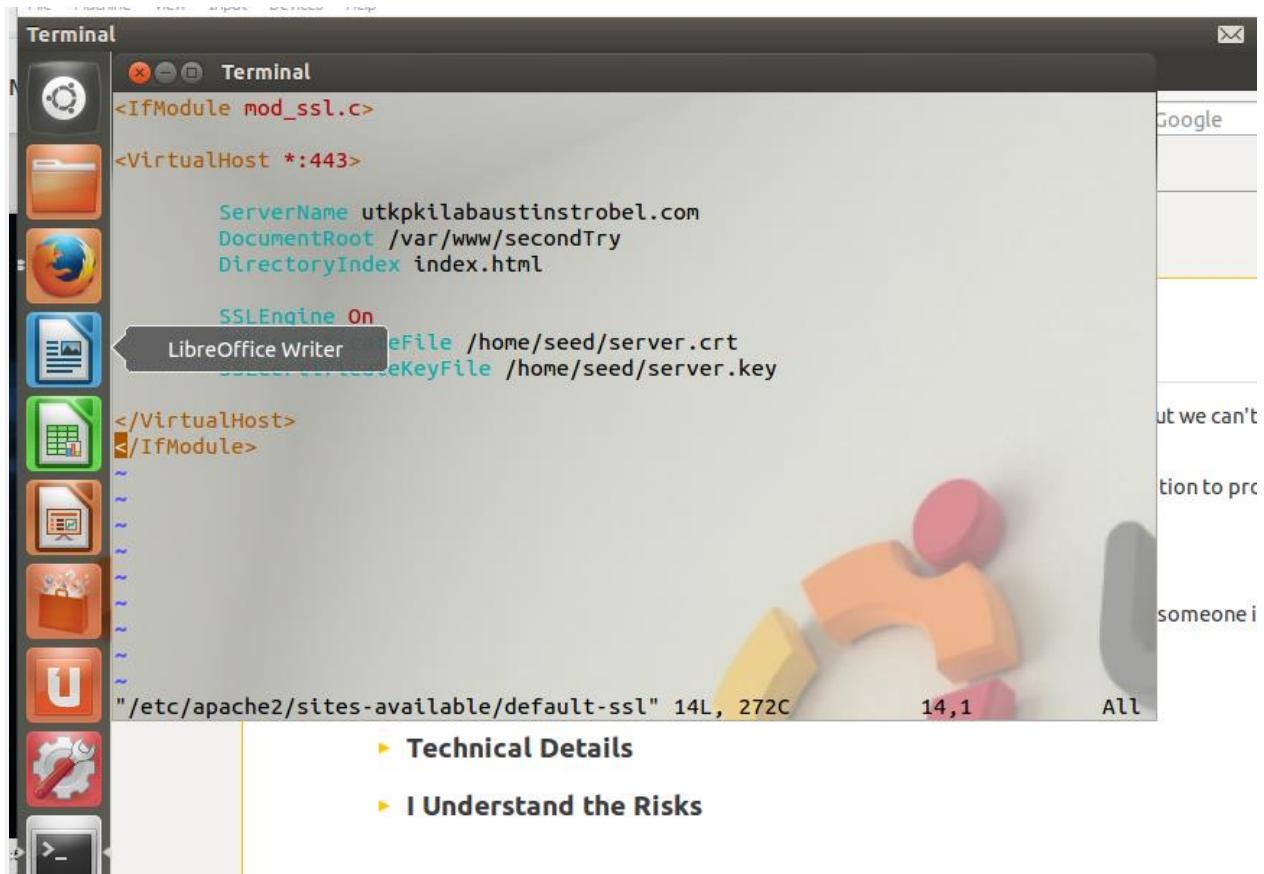
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>

"default-ssl" 186L, 7710C 1,1 Top
```

System Settings Technical Details

➔ Deleted everything past our first instance of virtual host:



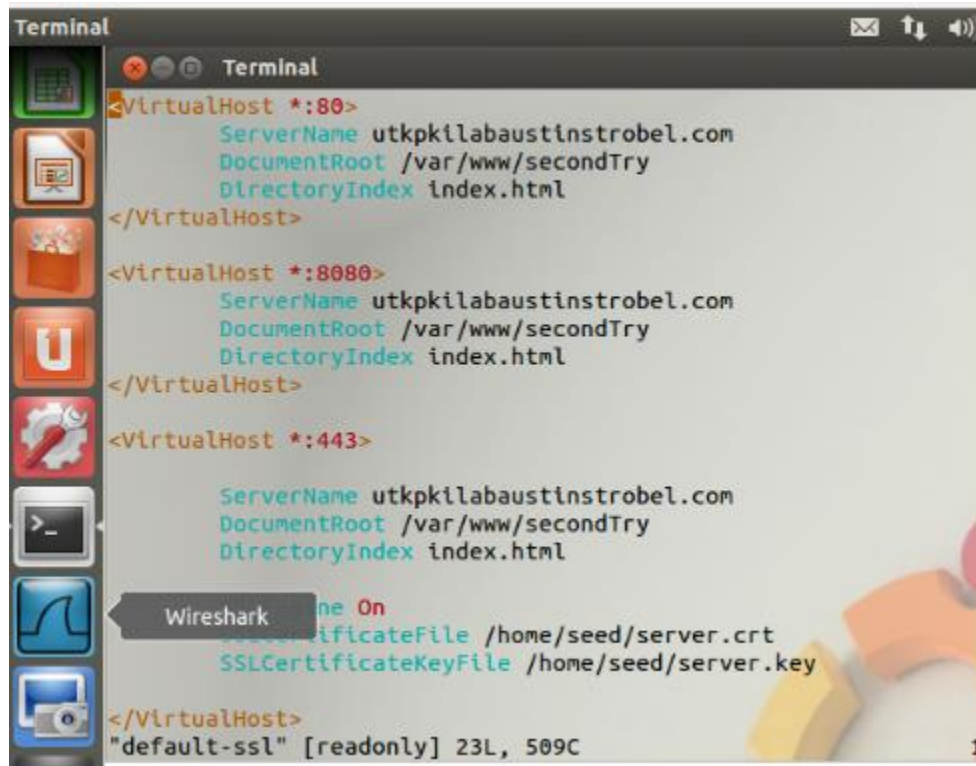
I was somehow able to edit the file by adding this: `":w !sudo tee %"` and then answering the subsequent questions (I just pressed "enter" twice) and then doing `":q!"` and that somehow worked \*shrugs\*

➔ Then type "cd" to get back to your true home directory

Then from the home directory, do `cd /var/www` then `sudo mkdir secondTry`, then `cd secondTry`, `sudo vim index.html`, and then put a few characters in it (doesn't really matter)

```
Sudo cp default-ssl default-ssl.conf
```

> Default-ssl

A terminal window titled "Terminal" with standard window controls (close, maximize, minimize) and system icons (mail, up/down arrows, volume) on the right. The left sidebar shows application icons for a spreadsheet, presentation, folder, terminal, and Wireshark. The terminal content shows the configuration of three VirtualHosts for the domain utkpilabaustinstrobel.com. The first two are for ports 80 and 8080. The third is for port 443 and includes SSL configuration with certificate and key files located at /home/seed/. At the bottom, a status line indicates the configuration is for "default-ssl" and is read-only.

```
Terminal
<VirtualHost *:80>
    ServerName utkpilabaustinstrobel.com
    DocumentRoot /var/www/secondTry
    DirectoryIndex index.html
</VirtualHost>

<VirtualHost *:8080>
    ServerName utkpilabaustinstrobel.com
    DocumentRoot /var/www/secondTry
    DirectoryIndex index.html
</VirtualHost>

<VirtualHost *:443>
    ServerName utkpilabaustinstrobel.com
    DocumentRoot /var/www/secondTry
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /home/seed/server.crt
    SSLCertificateKeyFile /home/seed/server.key
</VirtualHost>
"default-ssl" [readonly] 23L, 509C 1
```

Only kept default-ssl in /etc/apache2/sites-available

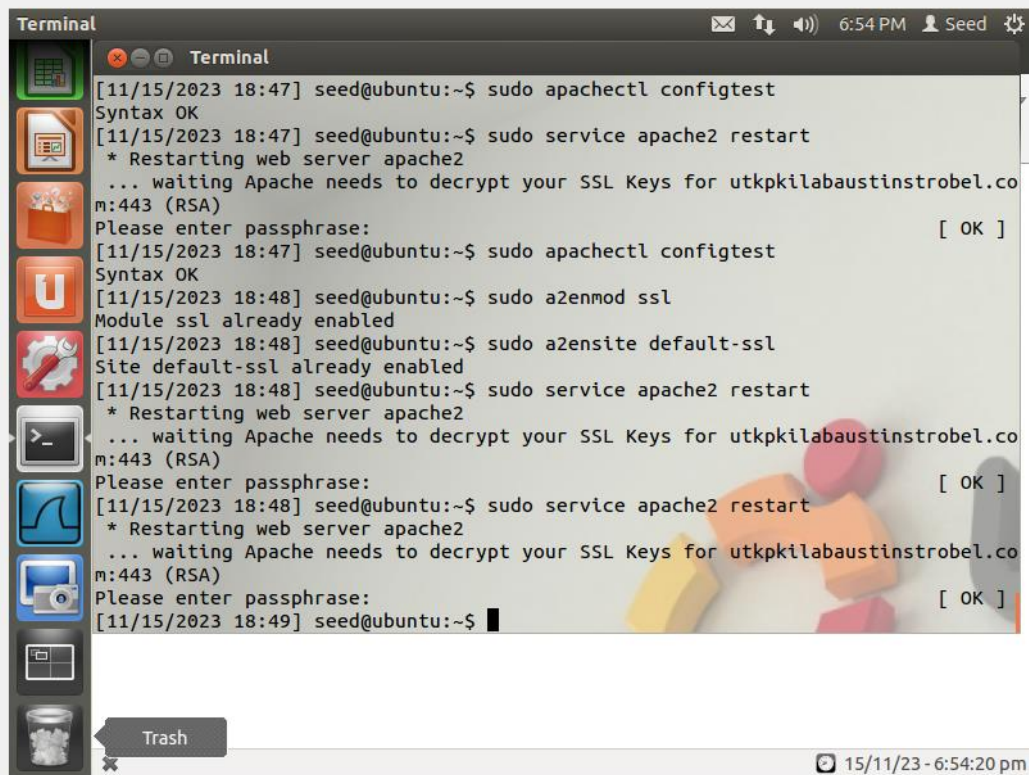


```
sudo apachectl configtest
```

```
// Enable the SSL module  
$ sudo a2enmod ssl
```

```
// Enable the site we have just edited  
$ sudo a2ensite default-ssl
```

```
// Restart Apache  
$ sudo service apache2 restart -> password = crypt
```



The image shows a terminal window titled "Terminal" with a dark background. The window contains the following text:

```
[11/15/2023 18:47] seed@ubuntu:~$ sudo apachectl configtest  
Syntax OK  
[11/15/2023 18:47] seed@ubuntu:~$ sudo service apache2 restart  
* Restarting web server apache2  
... waiting Apache needs to decrypt your SSL Keys for utkpkilabaustinstrobel.co  
m:443 (RSA)  
Please enter passphrase: [ OK ]  
[11/15/2023 18:47] seed@ubuntu:~$ sudo apachectl configtest  
Syntax OK  
[11/15/2023 18:48] seed@ubuntu:~$ sudo a2enmod ssl  
Module ssl already enabled  
[11/15/2023 18:48] seed@ubuntu:~$ sudo a2ensite default-ssl  
Site default-ssl already enabled  
[11/15/2023 18:48] seed@ubuntu:~$ sudo service apache2 restart  
* Restarting web server apache2  
... waiting Apache needs to decrypt your SSL Keys for utkpkilabaustinstrobel.co  
m:443 (RSA)  
Please enter passphrase: [ OK ]  
[11/15/2023 18:48] seed@ubuntu:~$ sudo service apache2 restart  
* Restarting web server apache2  
... waiting Apache needs to decrypt your SSL Keys for utkpkilabaustinstrobel.co  
m:443 (RSA)  
Please enter passphrase: [ OK ]  
[11/15/2023 18:49] seed@ubuntu:~$
```

The terminal window is part of a desktop environment. On the left side, there is a vertical dock with several application icons. At the bottom of the dock, there is a "Trash" icon. The system status bar at the bottom right shows the date and time: "15/11/23 - 6:54:20 pm".

