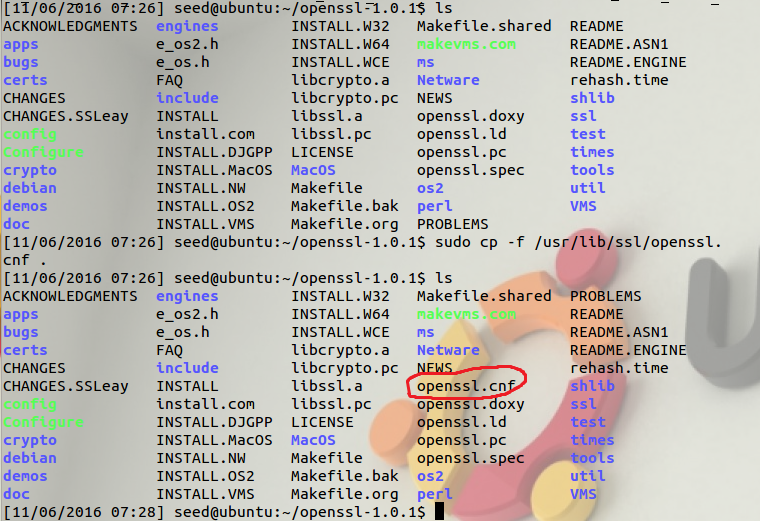
**2 Lab Environment**

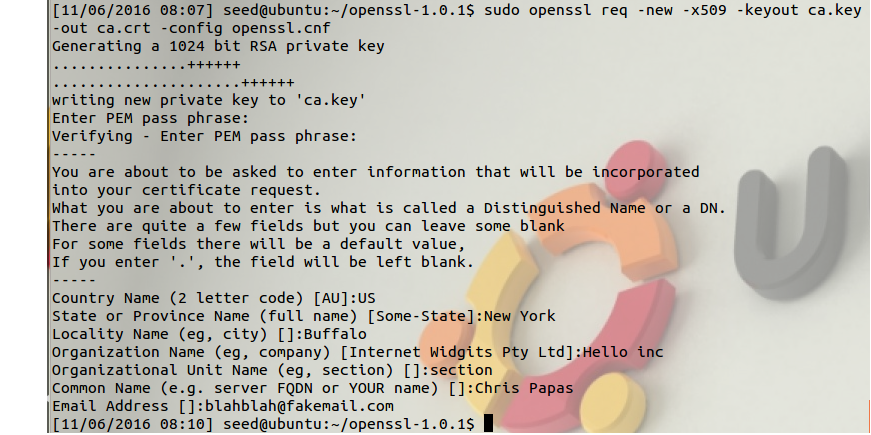
1. **Download VirtualBox**
2. **Download from provided link , SEEDUbuntu12.04.zip and unzip it once downloaded**
3. **Open image with VirtualBox**

**3 Lab Tasks**

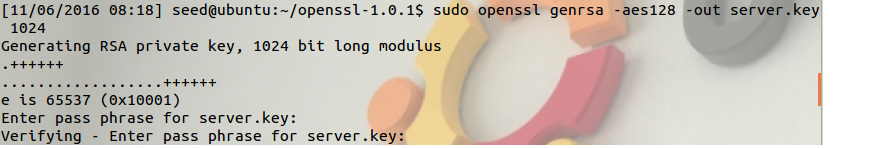
1. **Go to** /home/seed/openssl-1.0.1 and execute these commands
   1. sudo ./config
   2. sudo make
   3. sudo make test
   4. sudo make install
2. **copy the openssl.cnf file from /usr/lib/ssl/ by executing this command**
   1. **sudo cp -f /usr/lib/ssl/openssl.cnf . (we use sudo to increase our privileges)**

****

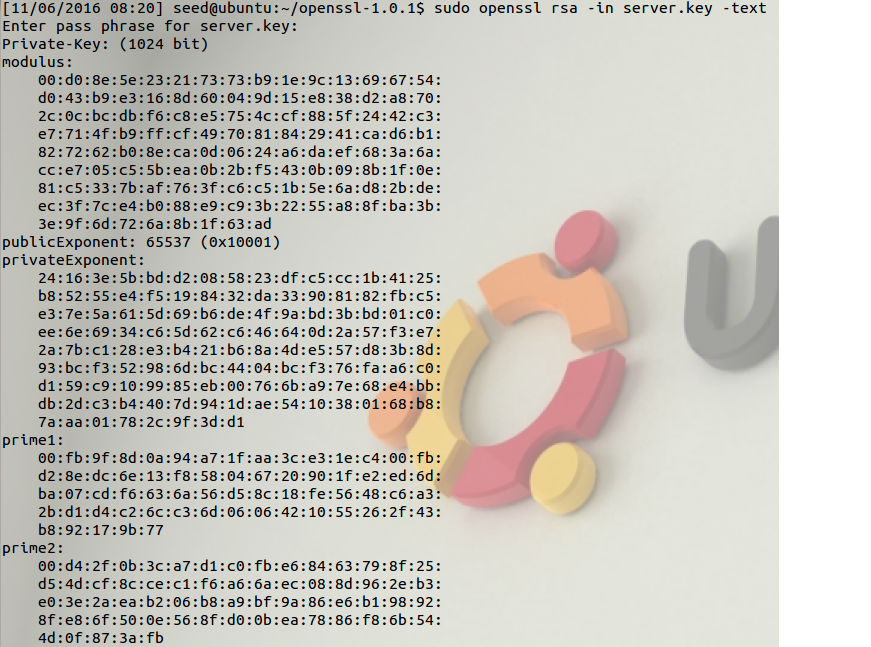
1. **execute these commands to create the necessary directories and files**
   1. **sudo mkdir demoCA**
   2. **cd demoCA**
   3. **sudo mkdir certs**
   4. **sudo mkdir crl**
   5. **sudo mkdir newcerts**
   6. **sudo emacs index.txt (leave it empty and save it)**
   7. **sudo emacs serial (put number 1000 in there and save it)**
2. **execute this command sudo** openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf and do the following:
   1. **enter PEM pass phrase (write it down)**
   2. **enter country name**
   3. **enter locality name**
   4. **enter organization name**
   5. **enter organizational unit**
   6. **enter common name**
   7. **enter email address**

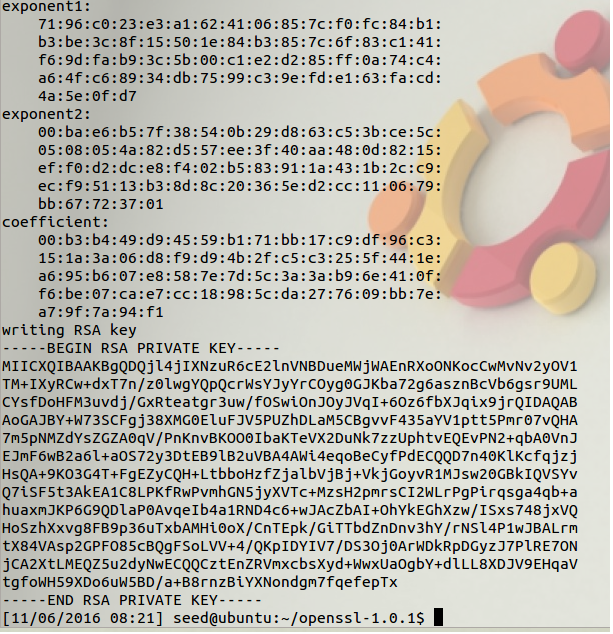
****

1. **execute this command sudo** openssl genrsa -aes128 -out server.key 1024 and do the following:
   1. **enter a pass phrase for server.key (write it down)**
   2. **verify it**

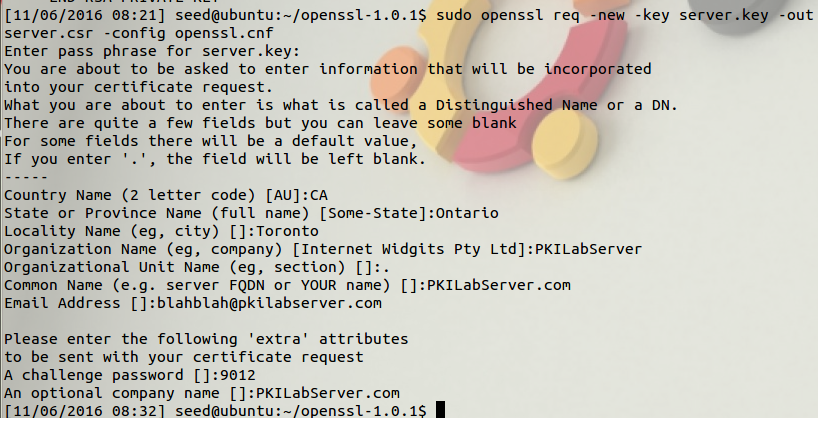
****

1. **to view the key execute this command(optional):**
   1. sudo openssl rsa -in server.key -text

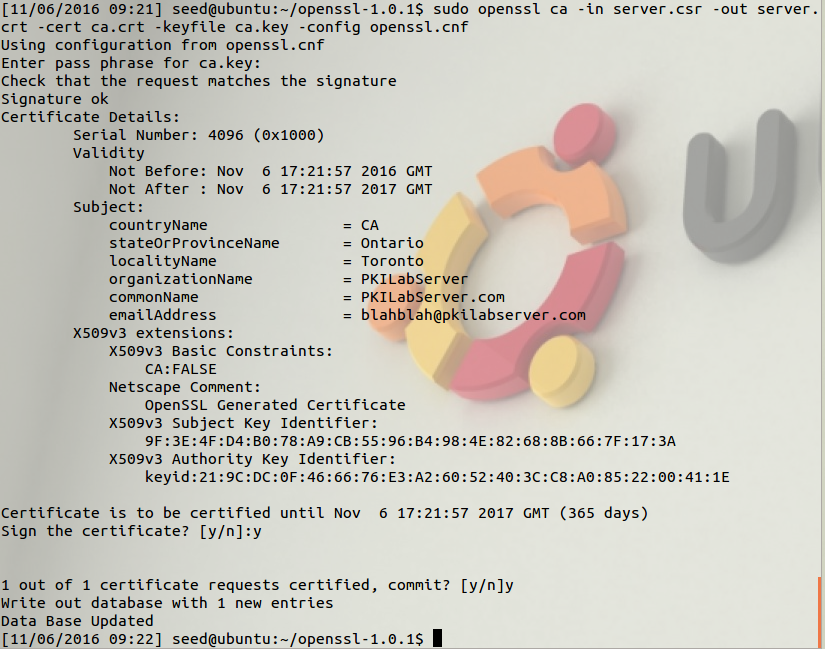
****

****

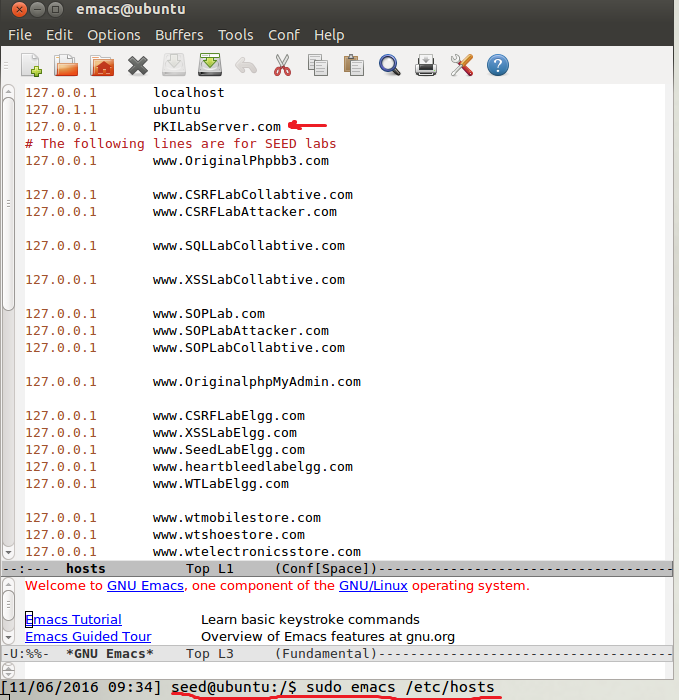
1. execute this command sudo openssl req -new -key server.key -out server.csr -config openssl.cnf and fill in what is needed , take note of passwords

****

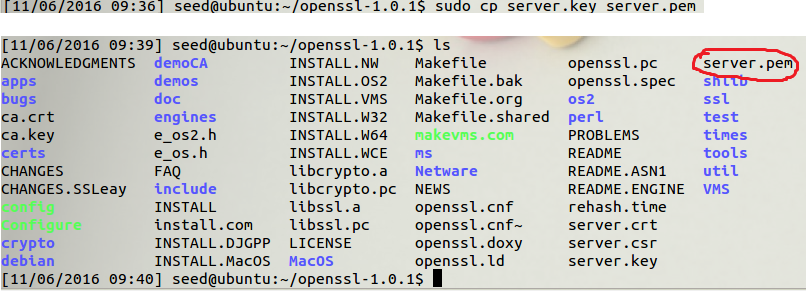
1. **sudo emacs openssl.cnf and look for** "policy = policy\_match" and change to "policy = policy\_anything", save it
2. **execute this command sudo** openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf , fillin what is needed and say yes to everything

****

1. **go to /etc/hosts and sudo emacs hosts ,add this line** 127.0.0.1 PKILabServer.com and save

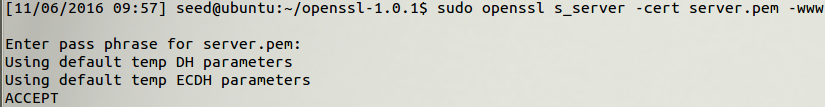
****

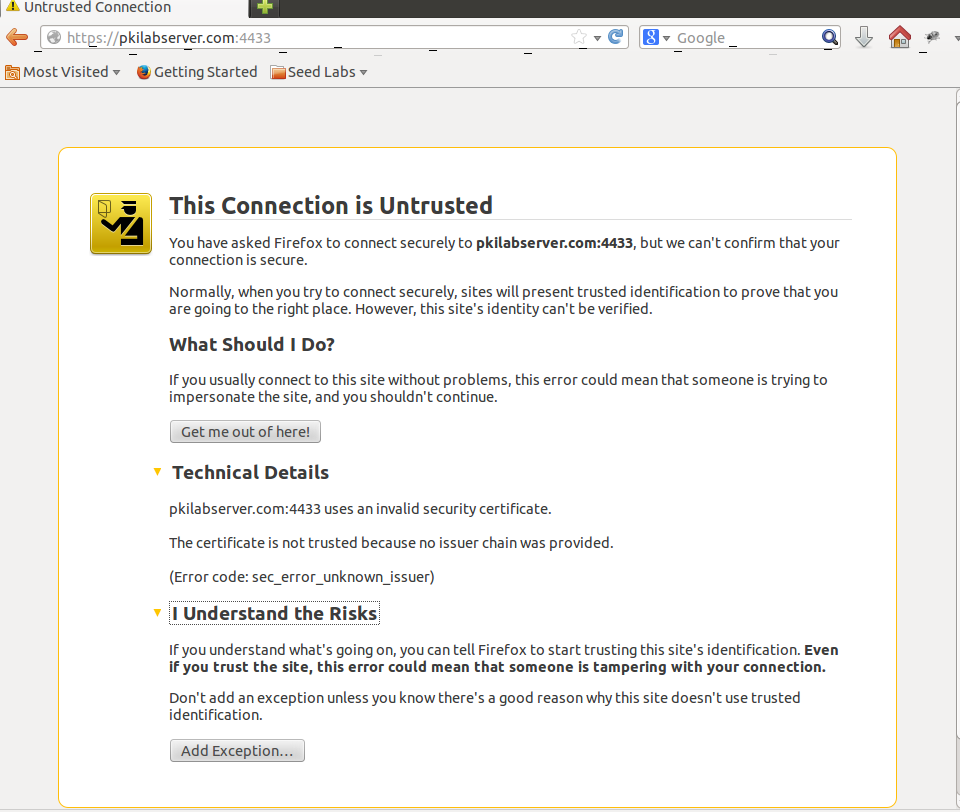
1. **go back to** /home/seed/openssl-1.0.1 and do the following
   1. **sudo cp server.key server.pem**

****

* 1. **sudo gedit server.crt and copy all the contents**
  2. **into server.pem by executing first sudo gedit server.pem and pasting them at the end of the file, then save**

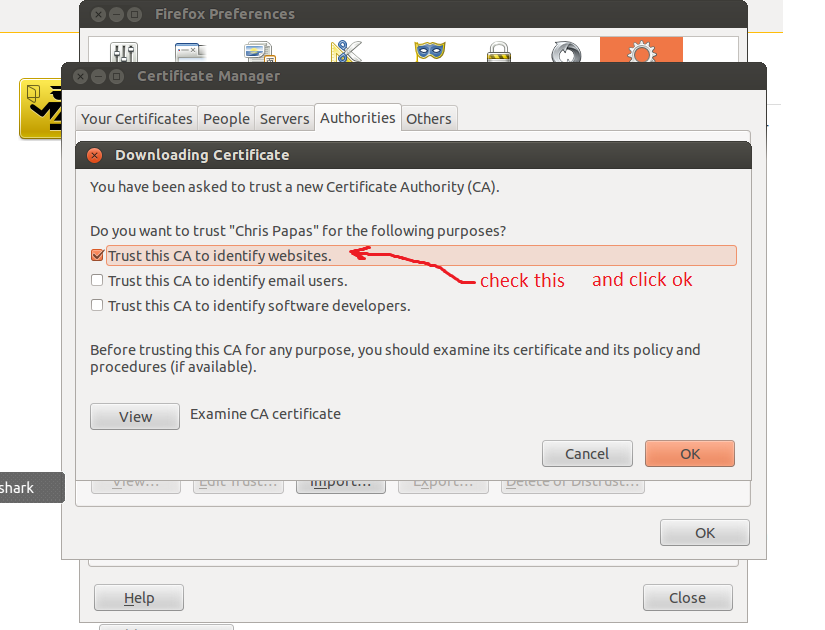
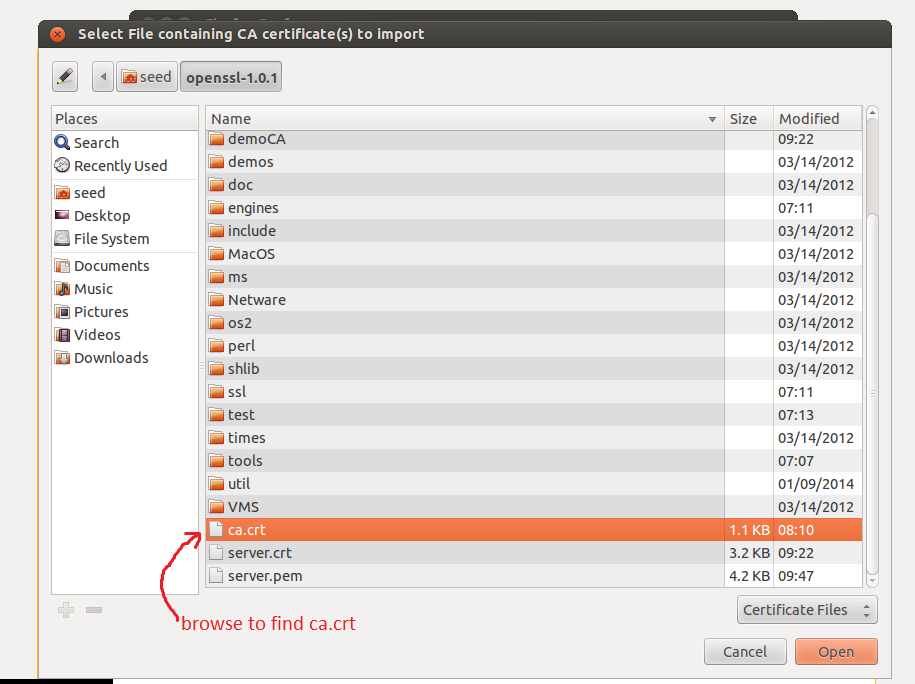
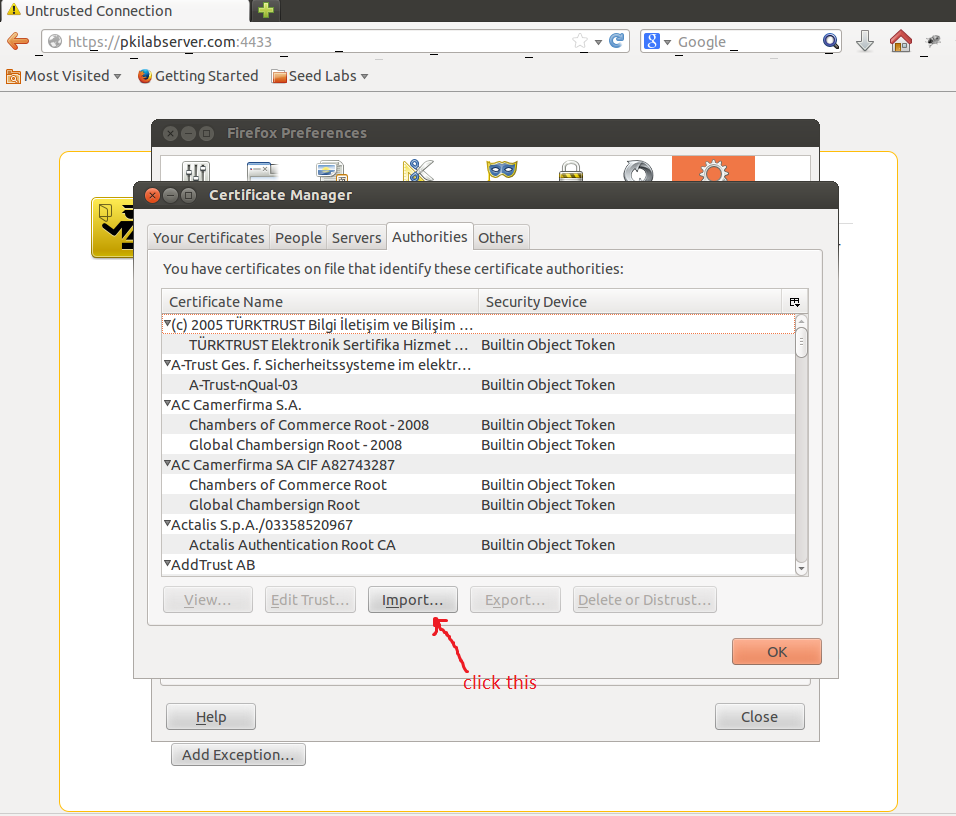
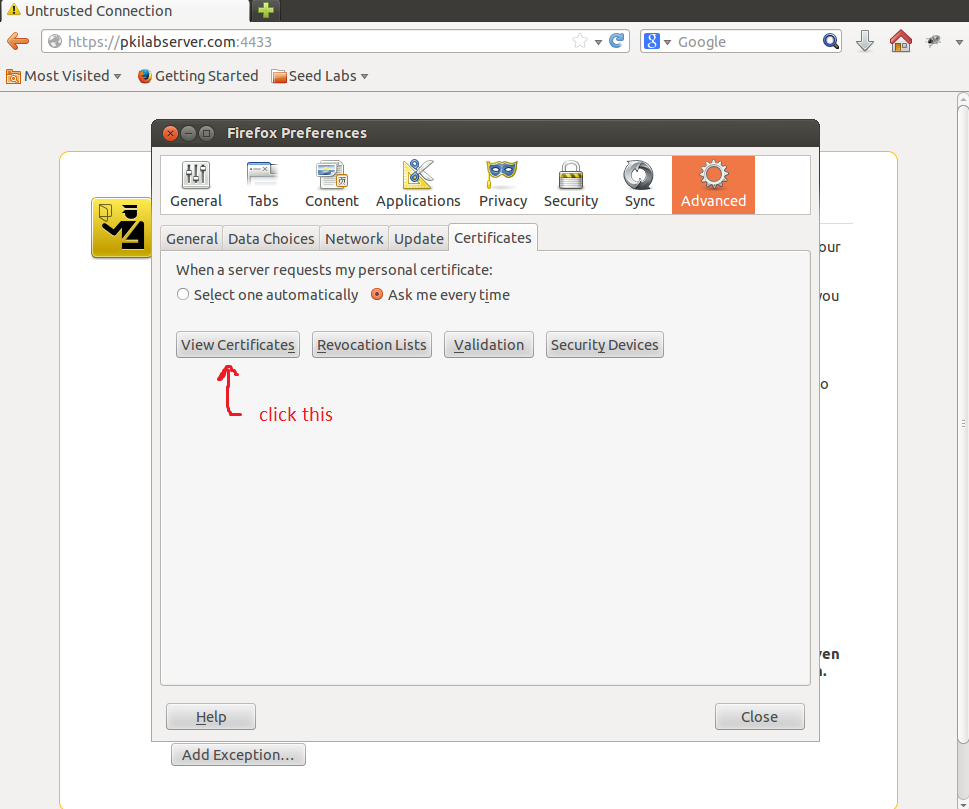
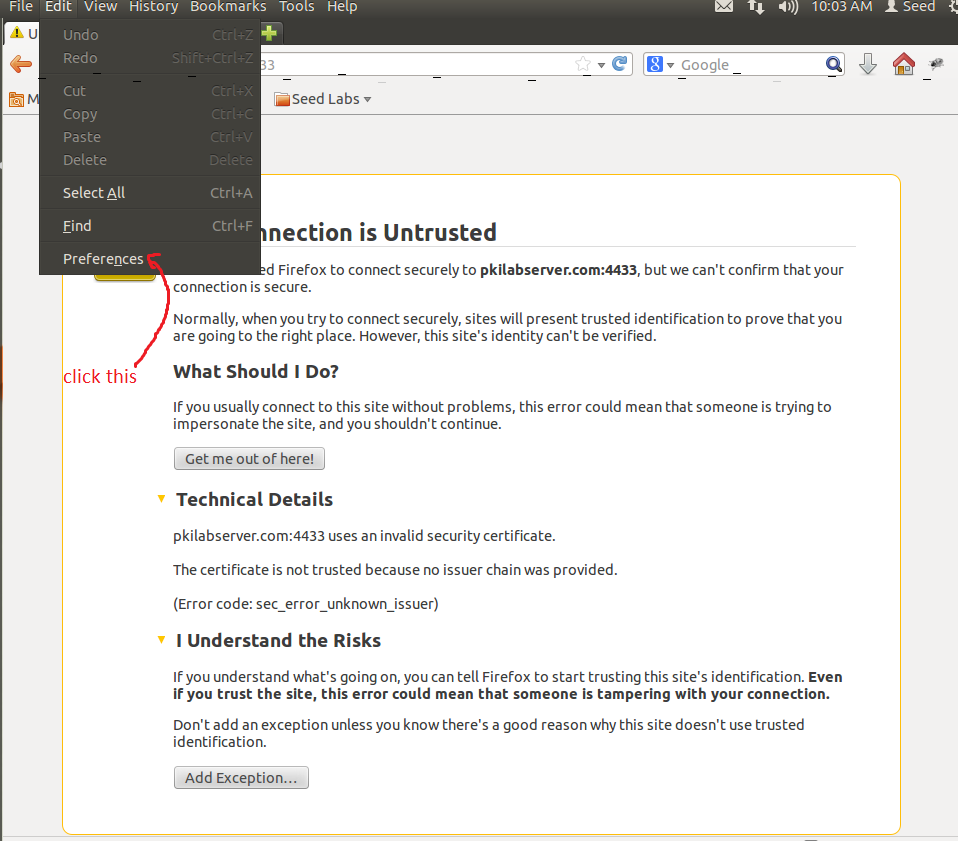
1. **execute command sudo** openssl s\_server -cert server.pem -www
   1. enter the server.key pass phrase
   2. while it says ACCEPT go to firefox and search for <https://PKILabServer.com:4433>,

****

****

* 1. **then ctrl-C**

1. **To load ca.crt into firefox go to** Edit -> Preference -> Advanced -> View Certificates in firefox and you will see a list of certificates that are already accepted by Firefox. From here, we can “import” our own certificate. Please import ca.crt, and select the following option: “Trust this CA to identify web sites”

****