EAST WEST UNIVERSITY

Fall -2024

CSE-487

Mini Project 1

Project Title: "**Securing a networked system with Public Key Infrastructure"**

Submitted By (Group – 5) :

Student Name	Student ID
Md Ripon Al Mamun	2021-2-60-083
S.M. Nazmul Hasan	2021-2-60-040
Taslima Akter Sathi	2021-1-60-114
Md. Shakil Hossain	2020-2-60-148

Project Supervisor:

Dr. Md. Hasanul Ferdaus

Assistant Professor,

Department of Computer Science and Engineering

Date of Submission: 11-01-2025

Recorded Presentation

(Google Drive Link student mail address:)

Table of Contents

Problem Statement

We have to secure a networked system with Public Key Infrastructure by implementing Transport Layer Security on HTTP for the https:// connection.

Requirements:

* Configuration of Certification Authority AcmeCA with AcmeRootCA as the RootCA.

* Configuration of the Web Server with Apache2 on a Linux Host.

* DNSconfiguration for www.verysecureserver.com

* Firewall configuration to allow necessary ports (53, 80, 443) only

* CSR Configuration and Generation for the www.verysecureserver.com

* Transferring the CSR to AcmeCA

* Certification process (Verification and Certificate Generation from CSR)

* Transferring the certificate from AcmeCA to www.verysecureserver.com

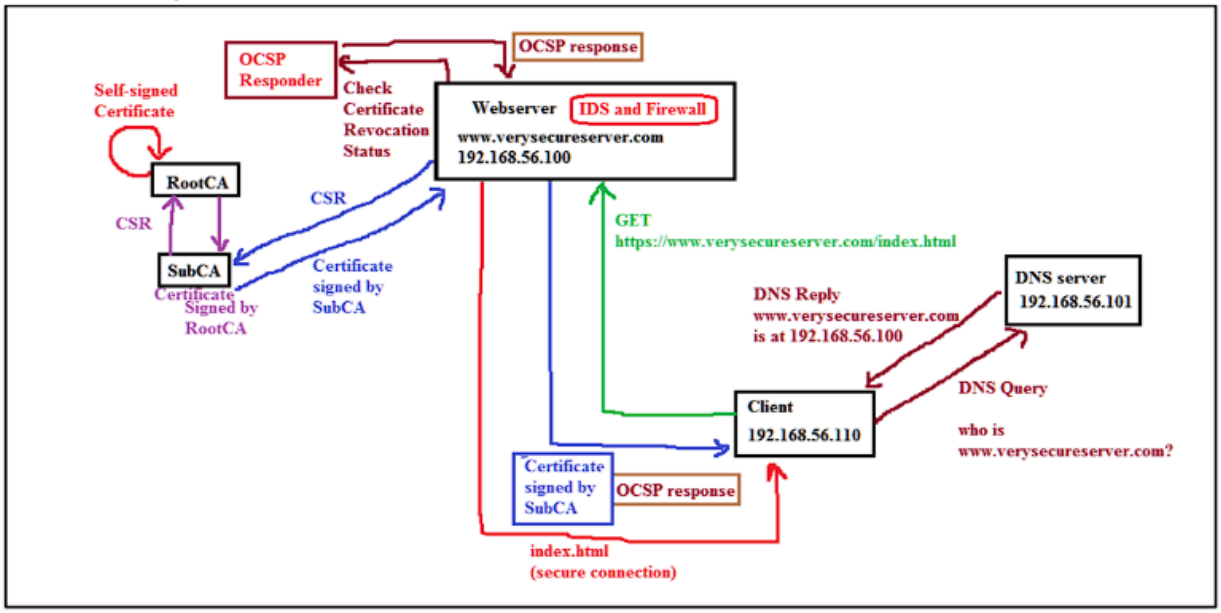
* Installation of the signed the SSL certificate in the server of www.verysecureserver.com

* Making the system trust Acme-RootCA

* Implementation of a simple file uploading page in the server.

* Verifying the security of the connection by inspection (the padlock icon)

Network Setup:



Necessary Elements:

- Oracle VM VirtualBox
- Linux Ubuntu 18.04
- Firefox version 59.0.2 (64-bit)
- XAMPP

Create Virtual Machines In Windows 11

We need to create a virtual machine to work with our project.

- Download linux ubuntu-18.04-desktop-amd64

[Ubuntu 18.04.6 LTS (Bionic Beaver)]

- Download and install VMware Workstation 16 Player
- Extract ubuntu-18.04-desktop-amd64 from zip file
- In the VM Click on new=>Give the VM a name, Folder Directory and insert the necessary iso file
- Start the VM and give Username = Lazy Boy, Password=rasel, Hostname = Lazy Boy

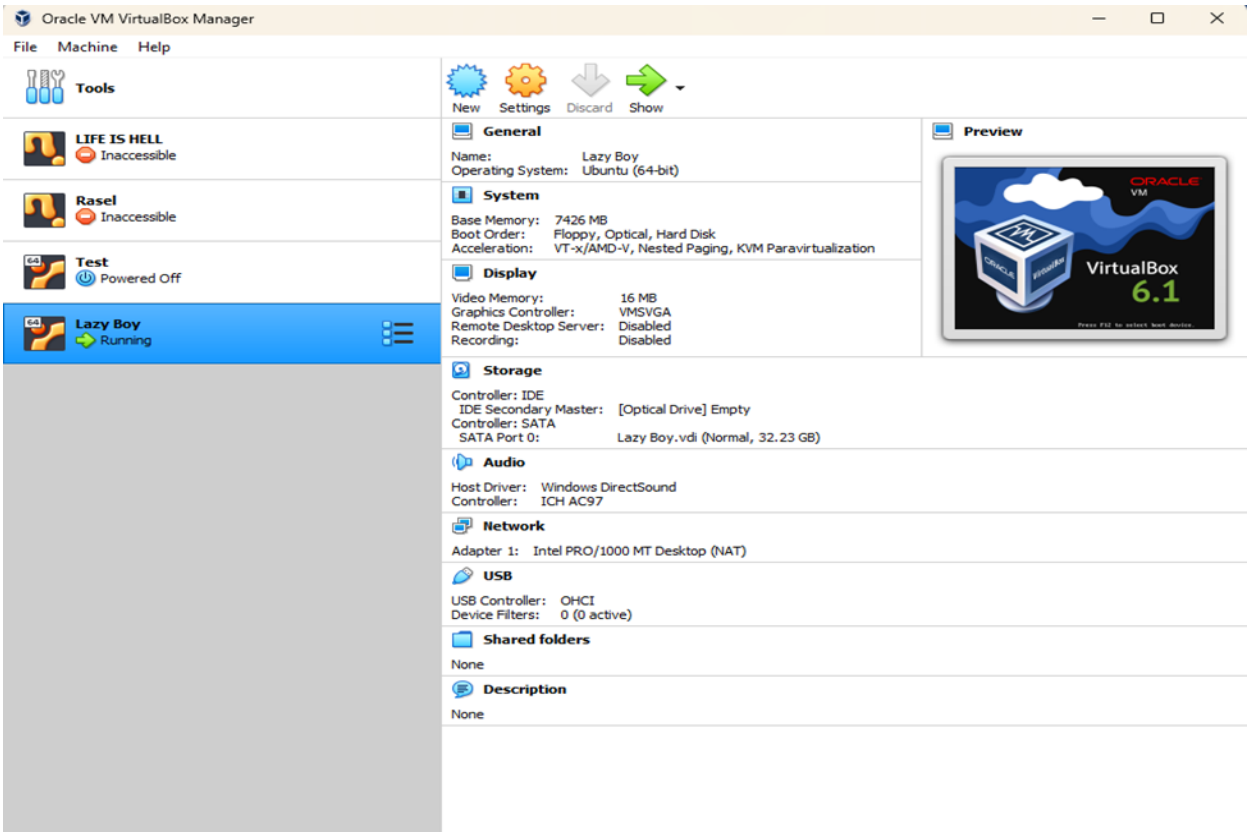
● Open the terminal and go to root user Su Password: ubuntu and check if sudo is in the sudoers file fix the situation if it is not there then add it there

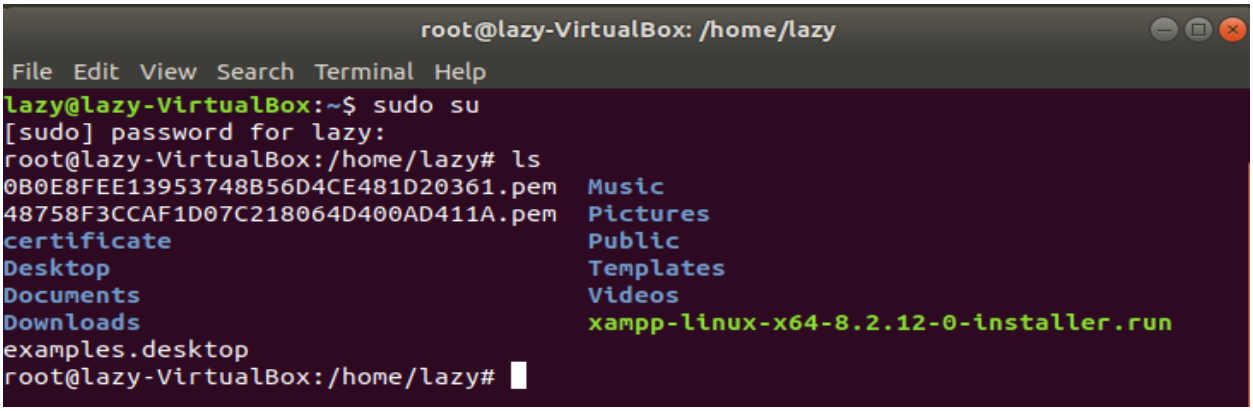
Web Server Configuration (Web Server VM)

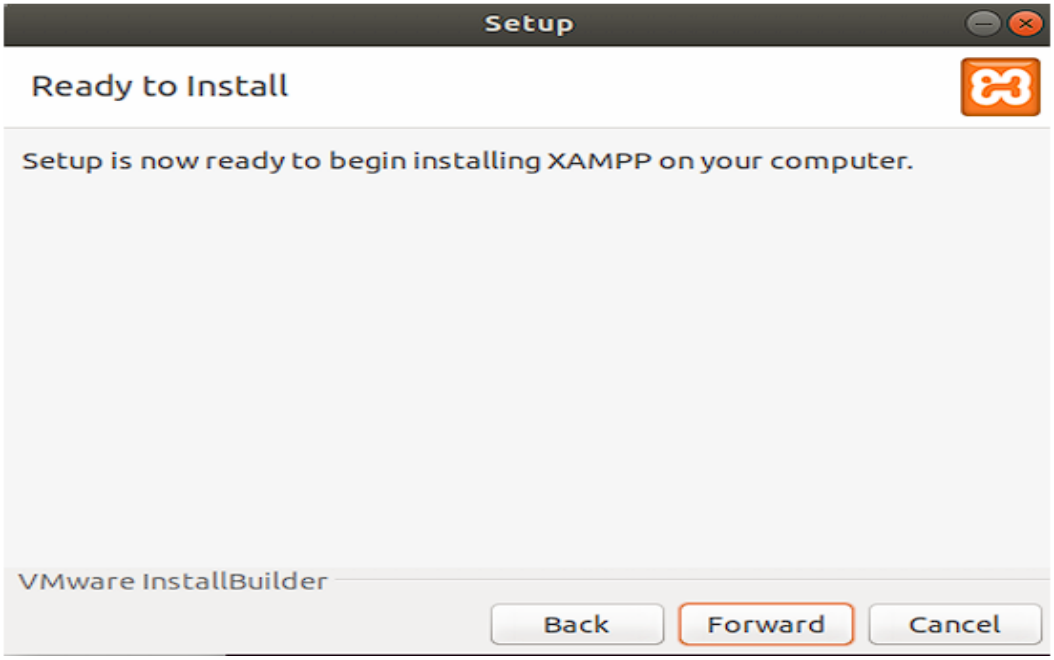
We will have to install some LAMP distribution and turn the VM into a webserver. We will use Xampp to make things easy.

1. Download xampp from Firefox

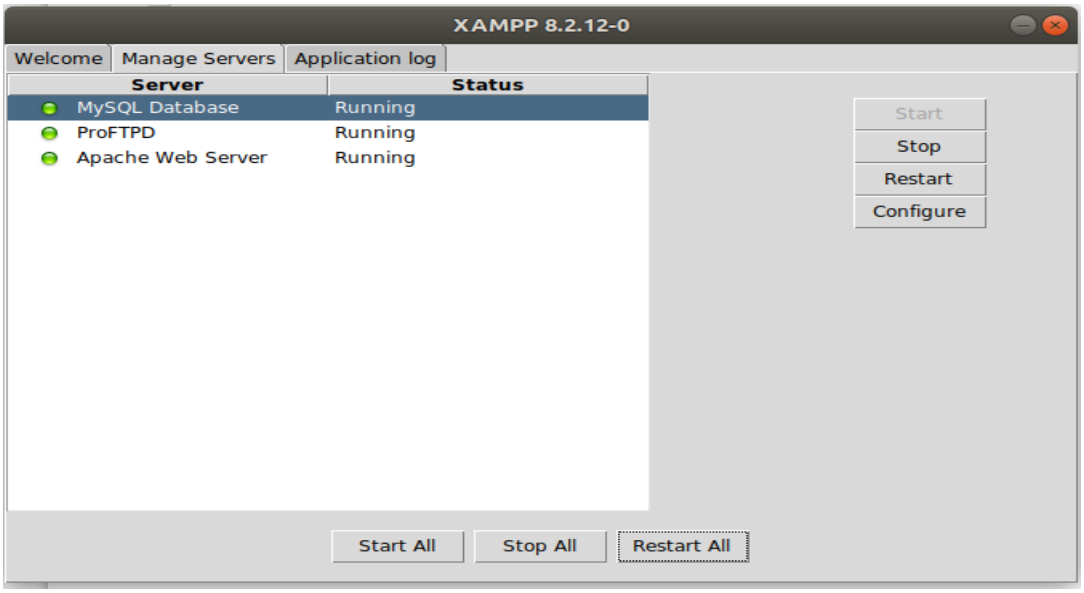
2. Make necessary preparation for installation






Setup
Ready to Install
Setup is now ready to begin installing XAMPP on your computer.
VMware InstallBuilder
Back
Forward
Cancel


Setup
Completing the XAMPP Setup Wizard
Setup has finished installing XAMPP on your computer.
Launch XAMPP
Back
Finish
Cancel



This is to check whether xampp server is working or not.

Creating CA, Sub-CA and Generating SSL Certificates

i) Preparing environment

su -

Giving the password : rasel

And then preparing all the directories

Changing the root of ca and sub ca private folder

---

chmod-v 700 ca/{root-ca,sub-ca,server}/private

Creating file index in both root ca and sub ca

---

touch ca/{root-ca,sub-ca}/index

writing serial number of root ca

---

openssl rand-hex 16 > ca/root-ca/serial

writing serial number of sub ca

---

openssl rand-hex 16 > ca/sub-ca/serial

Generating private key for root ca, sub ca and server

Public key for rootCA Public key for rootCA

---

openssl genrsa-aes256-out root-ca/private/ca.key 4096

Public key for subCA

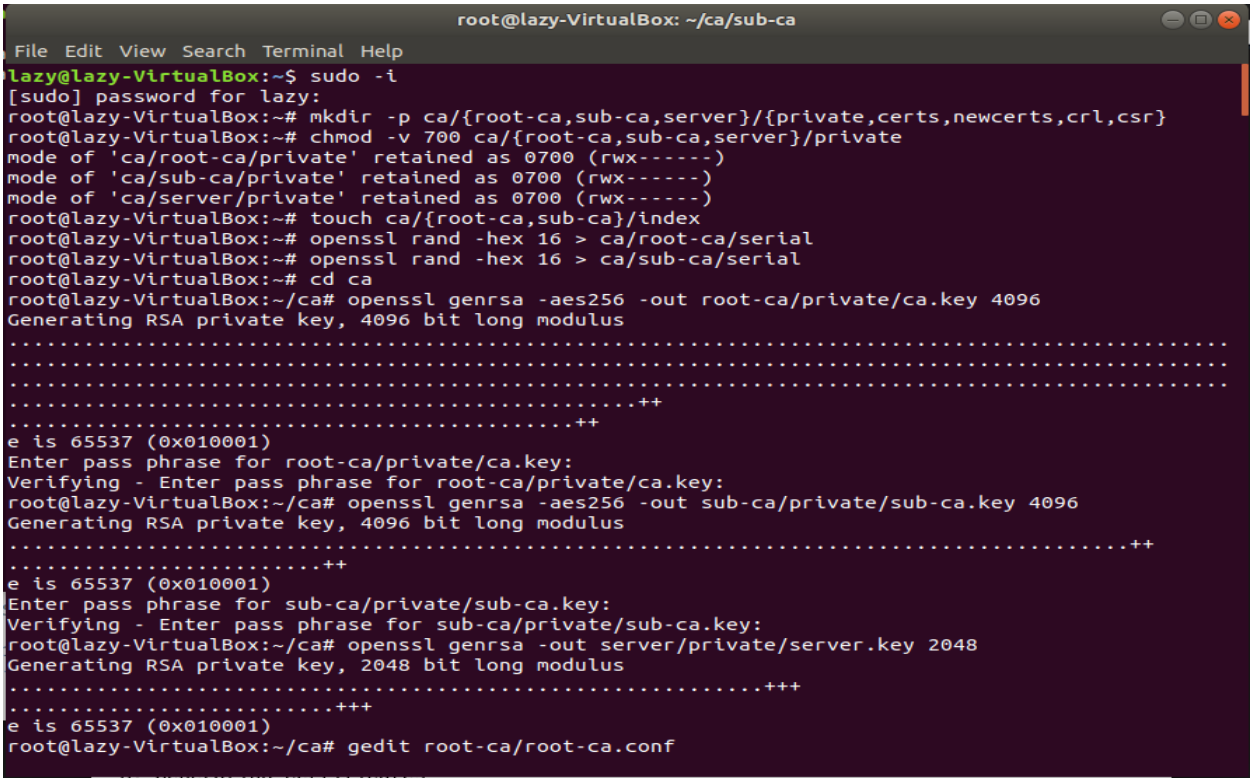
---

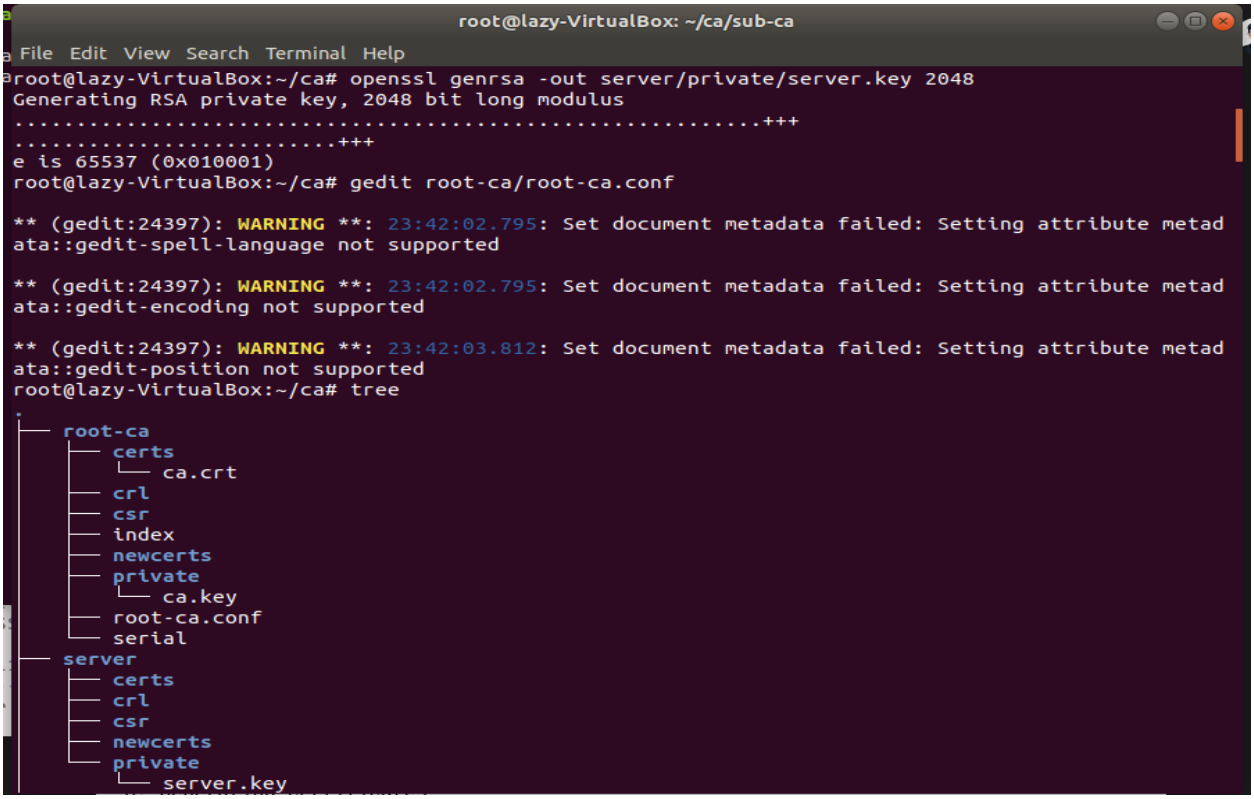
openssl genrsa-aes256-out sub-ca/private/sub-ca.key 4096

Public key for server

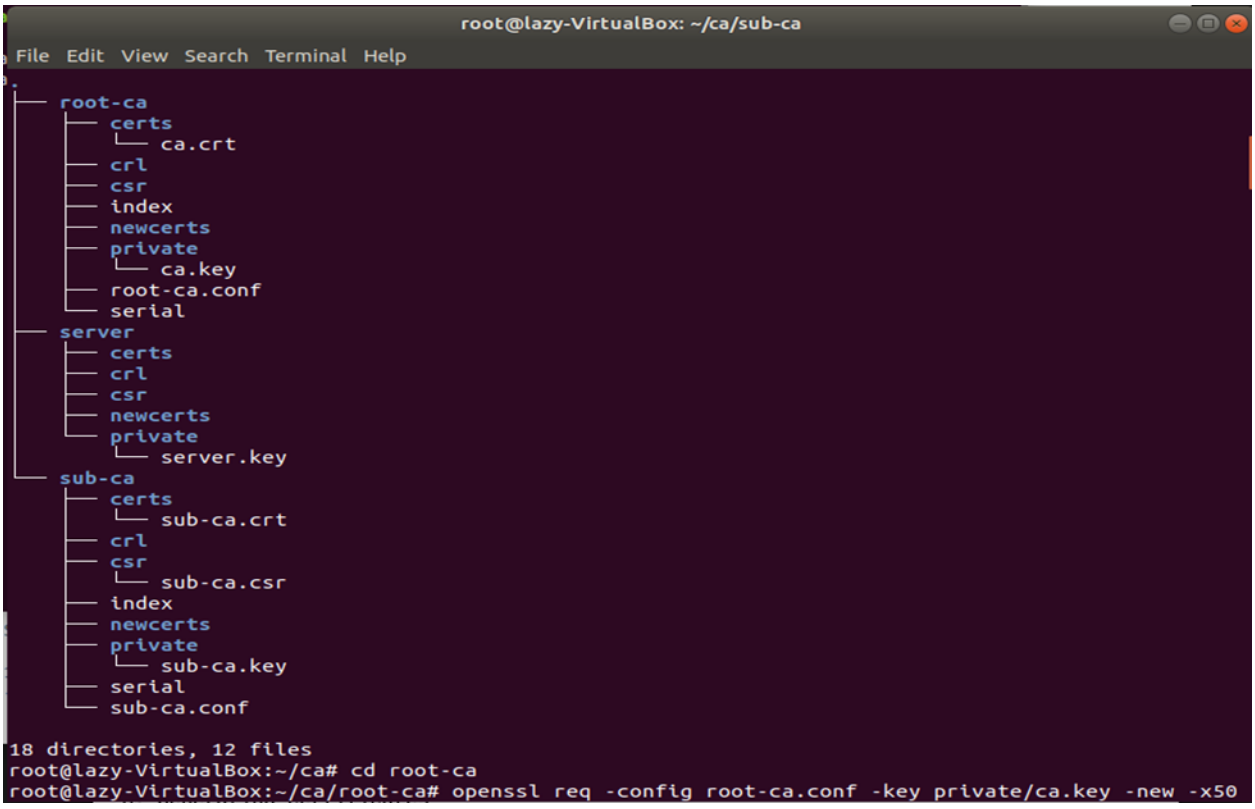
---

openssl genrsa-out server/private/server.key 2048





Verifying the changes via the directories



Create file named root-ca.conf and paste the following code

[ca]

[ca]

```
#/root/ca/root-ca/root-ca.conf
#see man ca
default_ca    = CA_default
[CA_default]
dir     = /root/ca/root-ca
certs     =  $dir/certs
crl_dir    = $dir/crl
new_certs_dir   = $dir/newcerts
database   = $dir/index
serial    = $dir/serial
RANDFILE   = $dir/private/.rand
private_key   = $dir/private/ca.key
certificate   = $dir/certs/ca.crt
crlnumber   = $dir/crlnumber
crl    =  $dir/crl/ca.crl
crl_extensions   = crl_ext
default_crl_days    = 30
default_md   = sha256
name_opt   = ca_default
cert_opt   = ca_default
default_days   = 365
preserve   = no
policy    = policy_strict
[ policy_strict ]
countryName   = supplied
stateOrProvinceName  =  supplied
organizationName  = match
organizationalUnitName  =  optional
commonName   =  supplied
emailAddress   =  optional
[ policy_loose ]
countryName   = optional
stateOrProvinceName  = optional
localityName   = optional
organizationName  = optional
organizationalUnitName   = optional
commonName   = supplied
emailAddress   = optional
[ req ]
# Options for the req tool, man req.
default_bits   = 2048
```

```
distinguished_name  = req_distinguished_name
string_mask   = utf8only
default_md   =  sha256
# Extension to add when the -x509 option is used.
x509_extensions   = v3_ca
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
stateOrProvinceName           = State or Province Name
localityName                = Locality Name
0.organizationName            = Organization Name
organizationalUnitName         = Organizational Unit Name
commonName                  = Common Name
emailAddress                = Email Address
countryName_default  = BD
stateOrProvinceName_default = Dhaka
localityName_default = Rampura
0.organizationName_default = EWU
organizationalUnitName_default = Cyber-Security
commonName_default = Cybergroup5
emailAddress_default = cybergroup5@gmail.com
[ v3_ca ]
# Extensions to apply when createing root ca
# Extensions for a typical CA, man x509v3_config
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer
basicConstraints  = critical, CA:true
keyUsage   =  critical, digitalSignature, cRLSign, keyCertSign
[ v3_intermediate_ca ]
# Extensions to apply when creating intermediate or sub-ca
# Extensions for a typical intermediate CA, same man as above
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer
#pathlen:0 ensures no more sub-ca can be created below an intermediate
basicConstraints  = critical, CA:true, pathlen:0
keyUsage   = critical, digitalSignature, cRLSign, keyCertSign
[ server_cert ]
# Extensions for server certificates
basicConstraints  = CA:FALSE
nsCertType   = server
nsComment   =  "OpenSSL Generated Server Certificate"
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid,issuer:always
keyUsage   =  critical, digitalSignature, keyEncipherment
extendedKeyUsage  = serverAuth
```

● Generating root ca certificate

● Ensuring that the certificate has been created properly

Moving inside root-ca

---

cd root-ca Generating root ca certificate

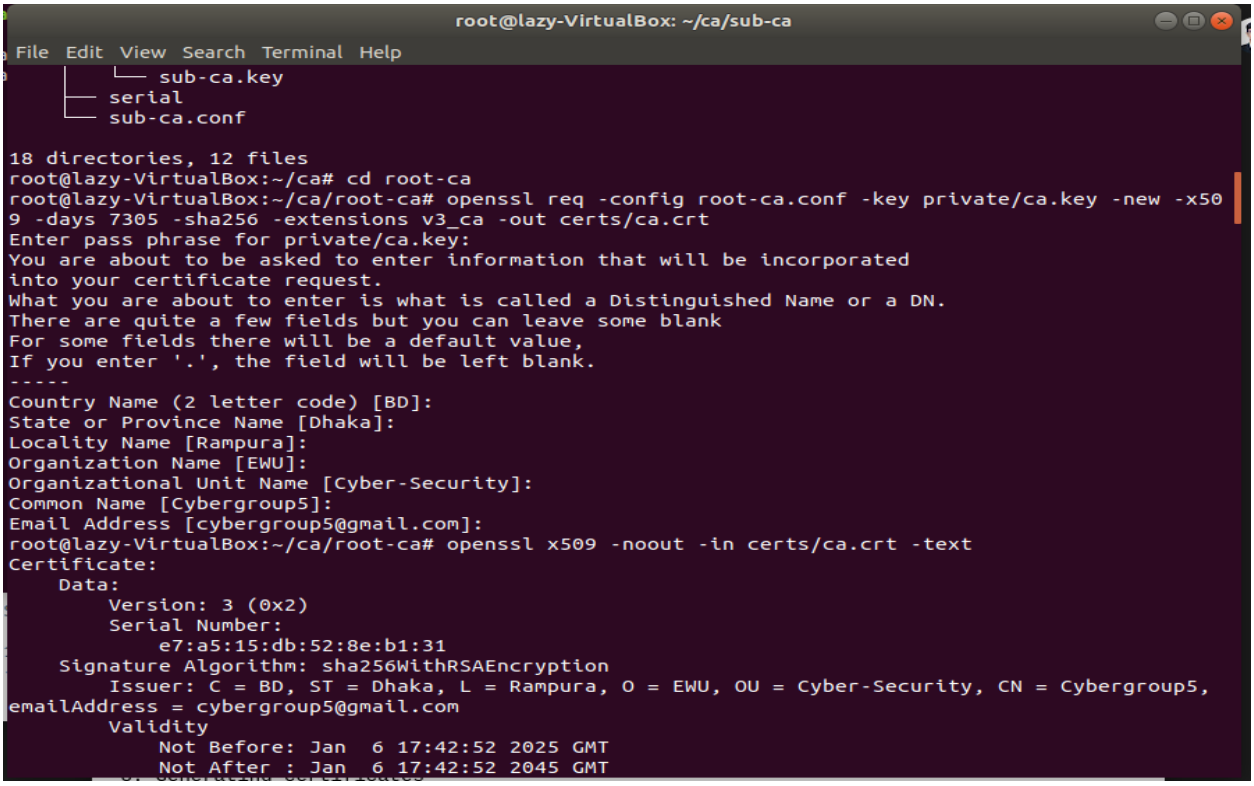
---

openssl req-config root-ca.conf-key private/ca.key-new-x509-days 7305-sha256-extensions v3_ca-out certs/ca.crt

Ensuring that the certificate has been created properly

---

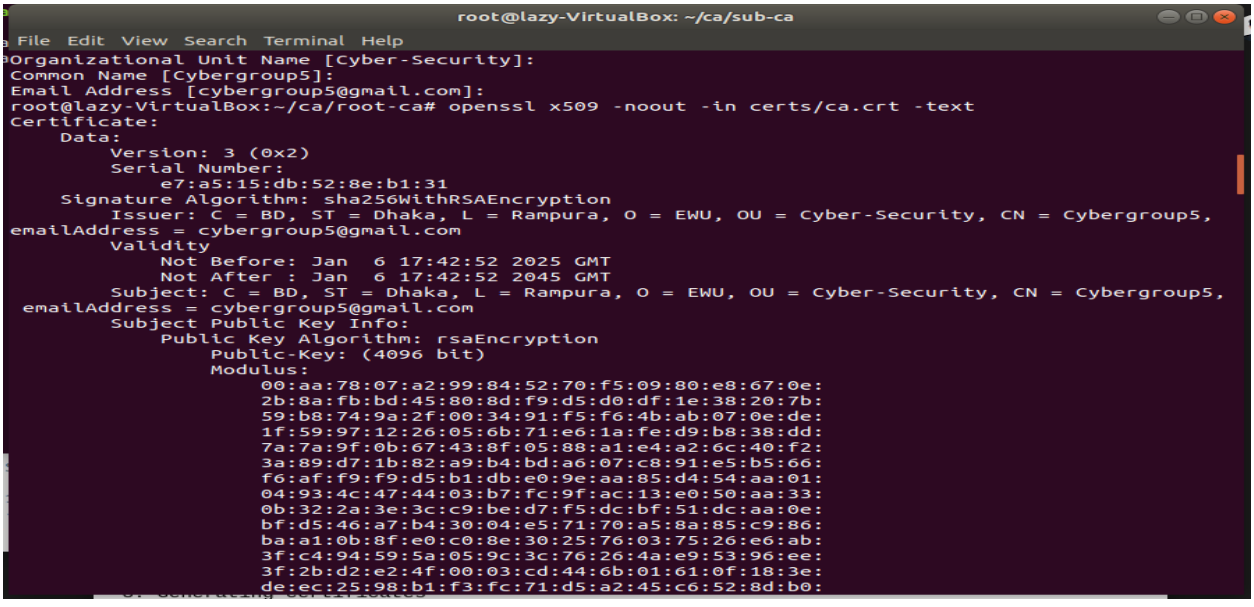
openssl x509-noout-in certs/ca.crt-text

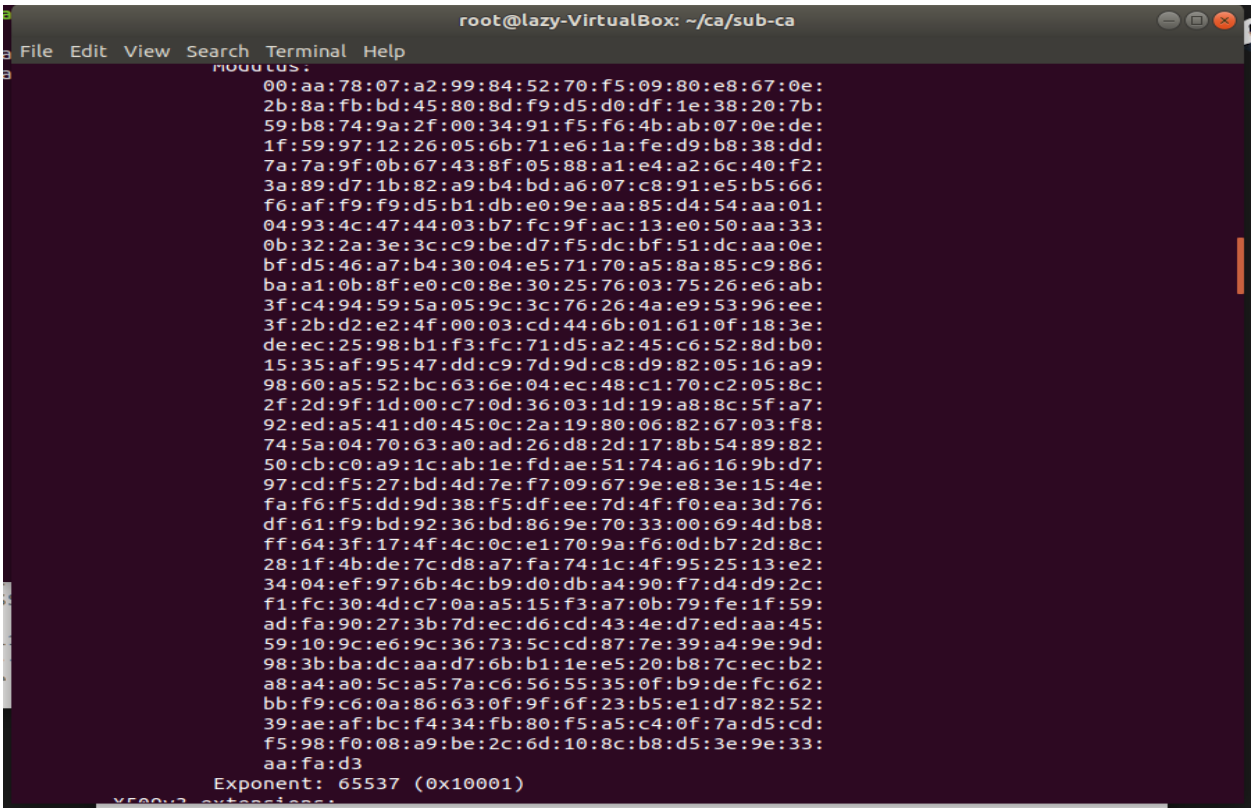


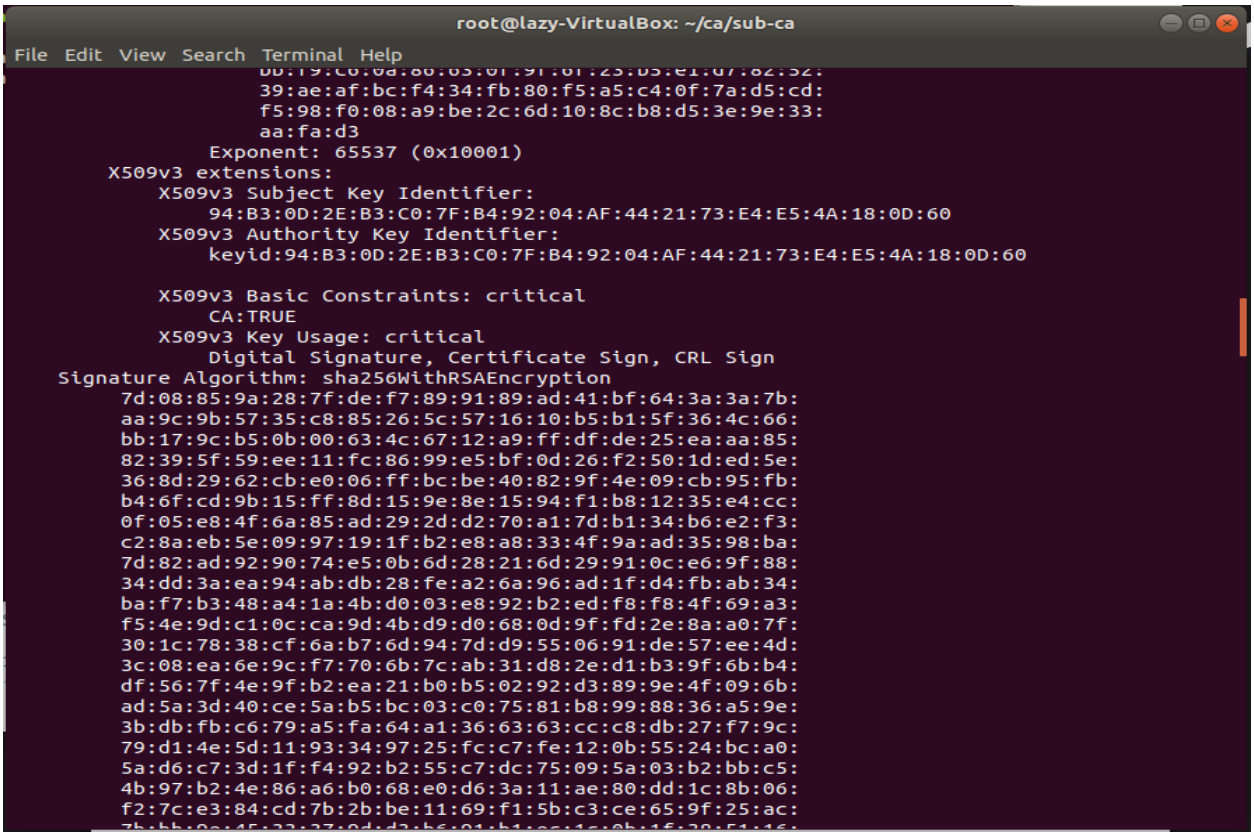
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:aa:78:07:a2:99:84:52:70:f5:09:80:e8:67:0e:

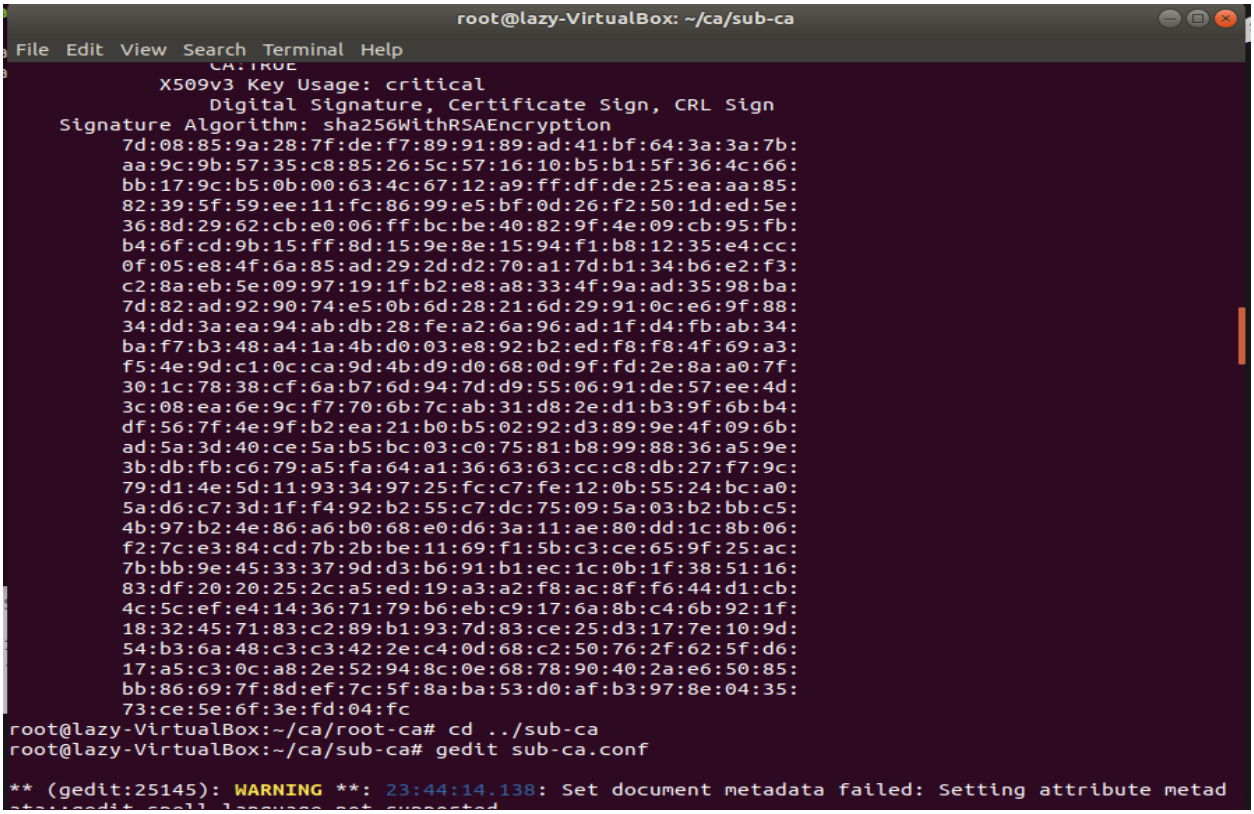
```
            2b:8a:fb:bd:45:80:8d:f9:d5:d0:df:1e:38:20:7b:
            59:b8:74:9a:2f:00:34:91:f5:f6:4b:ab:07:0e:de:
            1f:59:97:12:26:05:6b:71:e6:1a:fe:d9:b8:38:dd:
            7a:7a:9f:0b:67:43:8f:05:88:a1:e4:a2:6c:40:f2:
            3a:89:d7:1b:82:a9:b4:bd:a6:07:c8:91:e5:b5:66:
            f6:af:f9:f9:d5:b1:db:e0:9e:aa:85:d4:54:aa:01:
            04:93:4c:47:44:03:b7:fc:9f:ac:13:e0:50:aa:33:
            0b:32:2a:3e:3c:c9:be:d7:f5:dc:bf:51:dc:aa:0e:
            bf:d5:46:a7:b4:30:04:e5:71:70:a5:8a:85:c9:86:
            ba:a1:0b:8f:e0:c0:8e:30:25:76:03:75:26:e6:ab:
            3f:c4:94:59:5a:05:9c:3c:76:26:4a:e9:53:96:ee:
            3f:2b:d2:e2:4f:00:03:cd:44:6b:01:61:0f:18:3e:
            de:ec:25:98:b1:f3:fc:71:d5:a2:45:c6:52:8d:b0:
            15:35:af:95:47:dd:c9:7d:9d:c8:d9:82:05:16:a9:
            98:60:a5:52:bc:63:6e:04:ec:48:c1:70:c2:05:8c:
            2f:2d:9f:1d:00:c7:0d:36:03:1d:19:a8:8c:5f:a7:
            92:ed:a5:41:d0:45:0c:2a:19:80:06:82:67:03:f8:
            74:5a:04:70:63:a0:ad:26:d8:2d:17:8b:54:89:82:
            50:cb:c0:a9:1c:ab:1e:fd:ae:51:74:a6:16:9b:d7:
            97:cd:f5:27:bd:4d:7e:f7:09:67:9e:e8:3e:15:4e:
            fa:f6:f5:dd:9d:38:f5:df:ee:7d:4f:f0:ea:3d:76:
            df:61:f9:bd:92:36:bd:86:9e:70:33:00:69:4d:b8:
            ff:64:3f:17:4f:4c:0c:e1:70:9a:f6:0d:b7:2d:8c:
            28:1f:4b:de:7c:d8:a7:fa:74:1c:4f:95:25:13:e2:
            34:04:ef:97:6b:4c:b9:d0:db:a4:90:f7:d4:d9:2c:
            f1:fc:30:4d:c7:0a:a5:15:f3:a7:0b:79:fe:1f:59:
            ad:fa:90:27:3b:7d:ec:d6:cd:43:4e:d7:ed:aa:45:
            59:10:9c:e6:9c:36:73:5c:cd:87:7e:39:a4:9e:9d:
            98:3b:ba:dc:aa:d7:6b:b1:1e:e5:20:b8:7c:ec:b2:
            a8:a4:a0:5c:a5:7a:c6:56:55:35:0f:b9:de:fc:62:
            bb:f9:c6:0a:86:63:0f:9f:6f:23:b5:e1:d7:82:52:
            39:ae:af:bc:f4:34:fb:80:f5:a5:c4:0f:7a:d5:cd:
            f5:98:f0:08:a9:be:2c:6d:10:8c:b8:d5:3e:9e:33:
            aa:fa:d3
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60
        X509v3 Authority Key Identifier:
            keyid:94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60

        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
```

7d:08:85:9a:28:7f:de:f7:89:91:89:ad:41:bf:64:3a:3a:7b:
aa:9c:9b:57:35:c8:85:26:5c:57:16:10:b5:b1:5f:36:4c:66:
bb:17:9c:b5:0b:00:63:4c:67:12:a9:ff:df:de:25:ea:aa:85:
82:39:5f:59:ee:11:fc:86:99:e5:bf:0d:26:f2:50:1d:ed:5e:
36:8d:29:62:cb:e0:06:ff:bc:be:40:82:9f:4e:09:cb:95:fb:
b4:6f:cd:9b:15:ff:8d:15:9e:8e:15:94:f1:b8:12:35:e4:cc:
0f:05:e8:4f:6a:85:ad:29:2d:d2:70:a1:7d:b1:34:b6:e2:f3:
c2:8a:eb:5e:09:97:19:1f:b2:e8:a8:33:4f:9a:ad:35:98:ba:
7d:82:ad:92:90:74:e5:0b:6d:28:21:6d:29:91:0c:e6:9f:88:
34:dd:3a:ea:94:ab:db:28:fe:a2:6a:96:ad:1f:d4:fb:ab:34:
ba:f7:b3:48:a4:1a:4b:d0:03:e8:92:b2:ed:f8:f8:4f:69:a3:
f5:4e:9d:c1:0c:ca:9d:4b:d9:d0:68:0d:9f:fd:2e:8a:a0:7f:
30:1c:78:38:cf:6a:b7:6d:94:7d:d9:55:06:91:de:57:ee:4d:
3c:08:ea:6e:9c:f7:70:6b:7c:ab:31:d8:2e:d1:b3:9f:6b:b4:
df:56:7f:4e:9f:b2:ea:21:b0:b5:02:92:d3:89:9e:4f:09:6b:
ad:5a:3d:40:ce:5a:b5:bc:03:c0:75:81:b8:99:88:36:a5:9e:
3b:db:fb:c6:79:a5:fa:64:a1:36:63:63:cc:c8:db:27:f7:9c:
79:d1:4e:5d:11:93:34:97:25:fc:c7:fe:12:0b:55:24:bc:a0:
5a:d6:c7:3d:1f:f4:92:b2:55:c7:dc:75:09:5a:03:b2:bb:c5:
4b:97:b2:4e:86:a6:b0:68:e0:d6:3a:11:ae:80:dd:1c:8b:06:
f2:7c:e3:84:cd:7b:2b:be:11:69:f1:5b:c3:ce:65:9f:25:ac:
7b:bb:9e:45:33:37:9d:d3:b6:91:b1:ec:1c:0b:1f:38:51:16:
83:df:20:20:25:2c:a5:ed:19:a3:a2:f8:ac:8f:f6:44:d1:cb:
4c:5c:ef:e4:14:36:71:79:b6:eb:c9:17:6a:8b:c4:6b:92:1f:
18:32:45:71:83:c2:89:b1:93:7d:83:ce:25:d3:17:7e:10:9d:
54:b3:6a:48:c3:c3:42:2e:c4:0d:68:c2:50:76:2f:62:5f:d6:
17:a5:c3:0c:a8:2e:52:94:8c:0e:68:78:90:40:2a:e6:50:85:
bb:86:69:7f:8d:ef:7c:5f:8a:ba:53:d0:af:b3:97:8e:04:35:
73:ce:5e:6f:3e:fd:04:fc




root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
Modulus:
00:aa:78:07:a2:99:84:52:70:f5:09:80:e8:67:0e:
2b:8a:fb:bd:45:80:8d:f9:d5:d0:df:1e:38:20:7b:
59:b8:74:9a:2f:00:34:91:f5:f6:4b:ab:07:0e:de:
1f:59:97:12:26:05:6b:71:e6:1a:fe:d9:b8:38:dd:
7a:7a:9f:0b:67:43:8f:05:88:a1:e4:a2:6c:40:f2:
3a:89:d7:1b:82:a9:b4:bd:a6:07:c8:91:e5:b5:66:
f6:af:f9:f9:d5:b1:db:e0:9e:aa:85:d4:54:aa:01:
04:93:4c:47:44:03:b7:fc:9f:ac:13:e0:50:aa:33:
0b:32:2a:3e:3c:c9:be:d7:f5:dc:bf:51:dc:aa:0e:
bf:d5:46:a7:b4:30:04:e5:71:70:a5:8a:85:c9:86:
ba:a1:0b:8f:e0:c0:8e:30:25:76:03:75:26:e6:ab:
3f:c4:94:59:5a:05:9c:3c:76:26:4a:e9:53:96:ee:
3f:2b:d2:e2:4f:00:03:cd:44:6b:01:61:0f:18:3e:
de:ec:25:98:b1:f3:fc:71:d5:a2:45:c6:52:8d:b0:
15:35:af:95:47:dd:c9:7d:9d:c8:d9:82:05:16:a9:
98:60:a5:52:bc:63:6e:04:ec:48:c1:70:c2:05:8c:
2f:2d:9f:1d:00:c7:0d:36:03:1d:19:a8:8c:5f:a7:
92:ed:a5:41:d0:45:0c:2a:19:80:06:82:67:03:f8:
74:5a:04:70:63:a0:ad:26:d8:2d:17:8b:54:89:82:
50:cb:c0:a9:1c:ab:1e:fd:ae:51:74:a6:16:9b:d7:
97:cd:f5:27:bd:4d:7e:ef:7:09:67:9e:e8:3e:15:4e:
fa:f6:f5:dd:9d:38:f5:df:ee:7d:4f:f0:ea:3d:76:
df:61:f9:bd:92:36:bd:86:9e:70:33:00:69:4d:b8:
ff:64:3f:17:4f:4c:0c:e1:70:9a:f6:0d:b7:2d:8c:
28:1f:4b:de:7c:d8:a7:fa:74:1c:4f:95:25:13:e2:
34:04:ef:97:6b:4c:b9:d0:db:a4:90:f7:d4:d9:2c:
f1:fc:30:4d:c7:0a:a5:15:f3:a7:0b:79:fe:1f:59:
ad:fa:90:27:3b:7d:ec:d6:cd:43:4e:d7:ed:aa:45:
59:10:9c:e6:9c:36:73:5c:cd:87:7e:39:a4:9e:9d:
98:3b:ba:dc:aa:d7:6b:b1:1e:e5:20:b8:7c:ec:b2:
a8:a4:a0:5c:a5:7a:c6:56:55:35:0f:b9:de:fc:62:
bb:f9:c6:0a:86:63:0f:9f:6f:23:b5:e1:d7:82:52:
39:ae:af:bc:f4:34:fb:80:f5:a5:c4:0f:7a:d5:cd:
f5:98:f0:08:a9:be:2c:6d:10:8c:b8:d5:3e:9e:33:
aa:fa:d3
Exponent: 65537 (0x10001)


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
39:ae:af:bc:f4:34:fb:80:f5:a5:c4:0f:7a:d5:cd:
f5:98:f0:08:a9:be:2c:6d:10:8c:b8:d5:3e:9e:33:
aa:fa:d3
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60
X509v3 Authority Key Identifier:
keyid:94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
7d:08:85:9a:28:7f:de:f7:89:91:89:ad:41:bf:64:3a:3a:7b:
aa:9c:9b:57:35:c8:85:26:5c:57:16:10:b5:b1:5f:36:4c:66:
bb:17:9c:b5:0b:00:63:4c:67:12:a9:ff:df:de:25:ea:aa:85:
82:39:5f:59:ee:11:fc:86:99:e5:bf:0d:26:f2:50:1d:ed:5e:
36:8d:29:62:cb:e0:06:ff:bc:be:40:82:9f:4e:09:cb:95:fb:
b4:6f:cd:9b:15:ff:8d:15:9e:8e:15:94:f1:b8:12:35:e4:cc:
0f:05:e8:4f:6a:85:ad:29:2d:d2:70:a1:7d:b1:34:b6:e2:f3:
c2:8a:eb:5e:09:97:19:1f:b2:e8:a8:33:4f:9a:ad:35:98:ba:
7d:82:ad:92:90:74:e5:0b:6d:28:21:6d:29:91:0c:e6:9f:88:
34:dd:3a:ea:94:ab:db:28:fe:a2:6a:96:ad:1f:d4:fb:ab:34:
ba:f7:b3:48:a4:1a:4b:d0:03:e8:92:b2:ed:f8:f8:4f:69:a3:
f5:4e:9d:c1:0c:ca:9d:4b:d9:d0:68:0d:9f:fd:2e:8a:a0:7f:
30:1c:78:38:cf:6a:b7:6d:94:7d:d9:55:06:91:de:57:ee:4d:
3c:08:ea:6e:9c:f7:70:6b:7c:ab:31:d8:2e:d1:b3:9f:6b:b4:
df:56:7f:4e:9f:b2:ea:21:b0:b5:02:92:d3:89:9e:4f:09:6b:
ad:5a:3d:40:ce:5a:b5:bc:03:c0:75:81:b8:99:88:36:a5:9e:
3b:db:fb:c6:79:a5:fa:64:a1:36:63:63:cc:c8:db:27:f7:9c:
79:d1:4e:5d:11:93:34:97:25:fc:c7:fe:12:0b:55:24:bc:a0:
5a:d6:c7:3d:1f:f4:92:b2:55:c7:dc:75:09:5a:03:b2:bb:c5:
4b:97:b2:4e:86:a6:b0:68:e0:d6:3a:11:ae:80:dd:1c:8b:06:
f2:7c:e3:84:cd:7b:2b:be:11:69:f1:5b:c3:ce:65:9f:25:ac:



Moving a step back and then to sub-ca

---

cd ../sub-ca

Sub-CA

Creating sub-ca.config

---

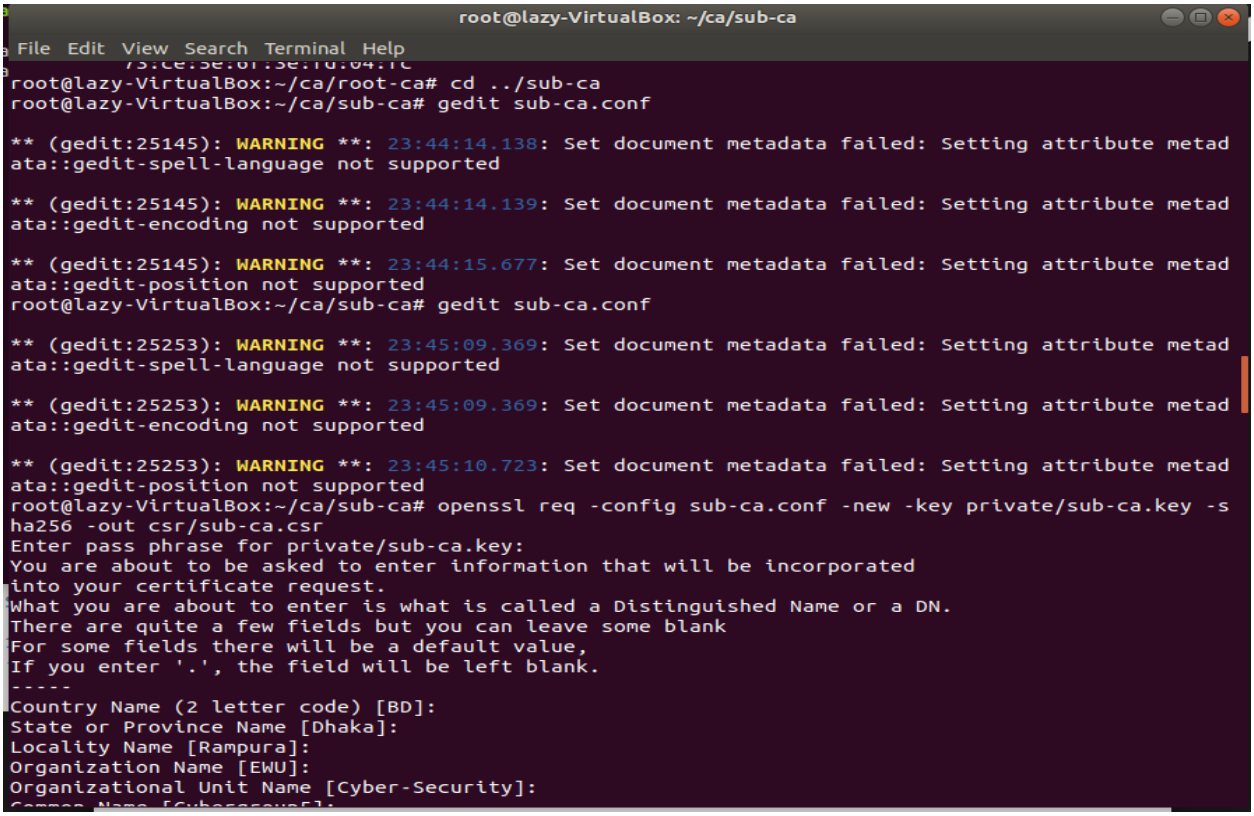
gedit sub-ca.conf

Inserting the code into sub-ca.config file

[ca]
#/root/ca/sub-ca/sub-ca.conf
#see man ca
default_ca = CA_default
[CA_default]
dir = /root/ca/sub-ca
certs = $dir/certs
crl_dir = $dir/crl
new_certs_dir = $dir/newcerts
database = $dir/index

```
serial    = $dir/serial
RANDFILE   = $dir/private/.rand
private_key   = $dir/private/sub-ca.key
certificate   = $dir/certs/sub-ca.crt
crlnumber   = $dir/crlnumber
crl    =  $dir/crl/ca.crl
crl_extensions   = crl_ext
default_crl_days    = 30
default_md   = sha256
name_opt   = ca_default
cert_opt   = ca_default
default_days   = 365
preserve   = no
policy    = policy_loose
[ policy_strict ]
countryName   = supplied
stateOrProvinceName  =  supplied
organizationName  = match
organizationalUnitName  =  optional
commonName   =  supplied
emailAddress   =  optional
[ policy_loose ]
countryName   = optional
stateOrProvinceName  = optional
localityName   = optional
organizationName  = optional
organizationalUnitName   = optional
commonName   = supplied
emailAddress   = optional
[ req ]
# Options for the req tool, man req.
default_bits   = 2048
distinguished_name  = req_distinguished_name
string_mask   = utf8only
default_md   =  sha256
# Extension to add when the -x509 option is used.
x509_extensions   = v3_ca
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
stateOrProvinceName           = State or Province Name
localityName                = Locality Name
0.organizationName            = Organization Name
organizationalUnitName         = Organizational Unit Name
commonName                  = Common Name
emailAddress                = Email Address
countryName_default  = BD
```

```
stateOrProvinceName_default = Dhaka
localityName_default = Rampura
0.organizationName_default = EWU
organizationalUnitName_default = Cyber-Security
commonName_default = Cybergroup5
emailAddress_default = cybergroup5@gmail.com
[ v3_ca ]
# Extensions to apply when createing root ca
# Extensions for a typical CA, man x509v3_config
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer
basicConstraints  = critical, CA:true
keyUsage   =  critical, digitalSignature, cRLSign, keyCertSign
[ v3_intermediate_ca ]
# Extensions to apply when creating intermediate or sub-ca
# Extensions for a typical intermediate CA, same man as above
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer
#pathlen:0 ensures no more sub-ca can be created below an intermediate
basicConstraints  = critical, CA:true, pathlen:0
keyUsage   = critical, digitalSignature, cRLSign, keyCertSign
[ server_cert ]
# Extensions for server certificates
basicConstraints  = CA:FALSE
nsCertType   = server
nsComment   =  "OpenSSL Generated Server Certificate"
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid,issuer:always
keyUsage   =  critical, digitalSignature, keyEncipherment
extendedKeyUsage  = serverAuth
```



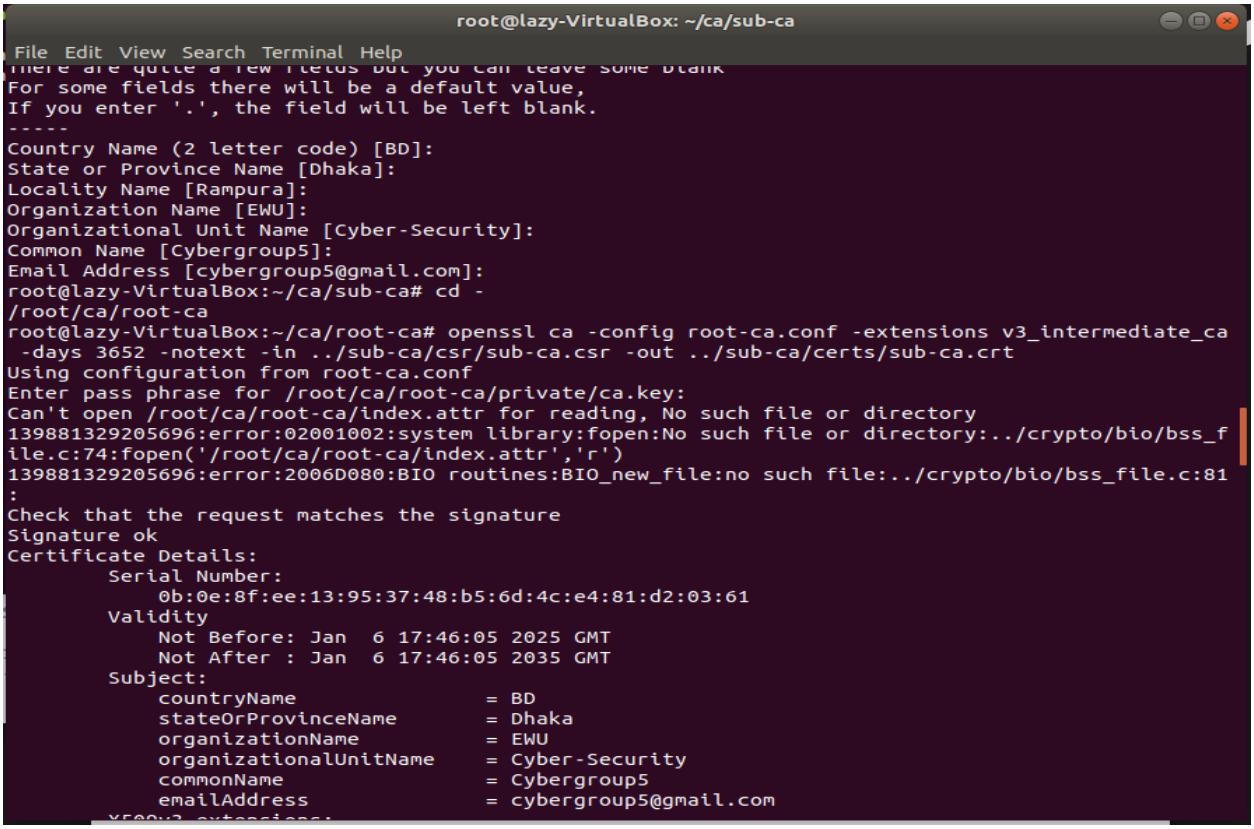
● Generating sub-ca certificate

● Ensuring that the certificate has been created properly

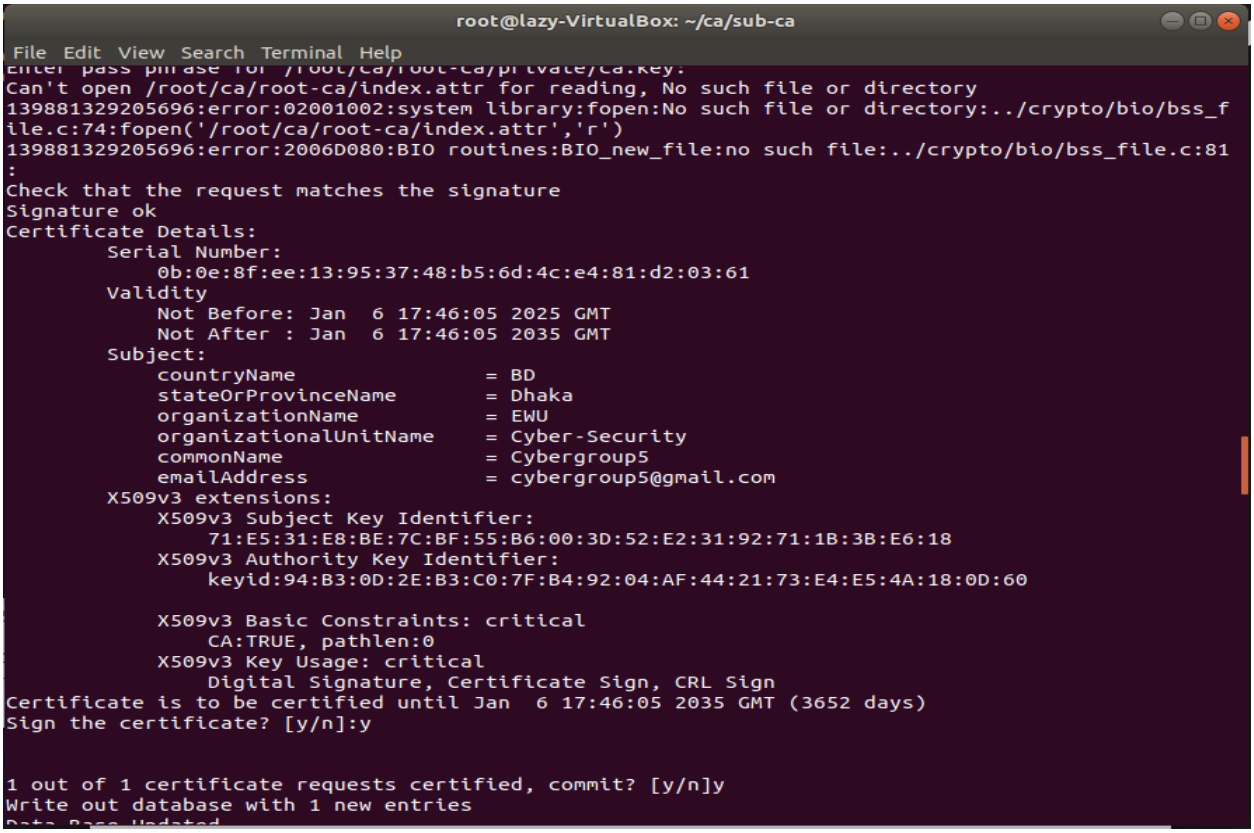
Signing the request of sub ca by root ca

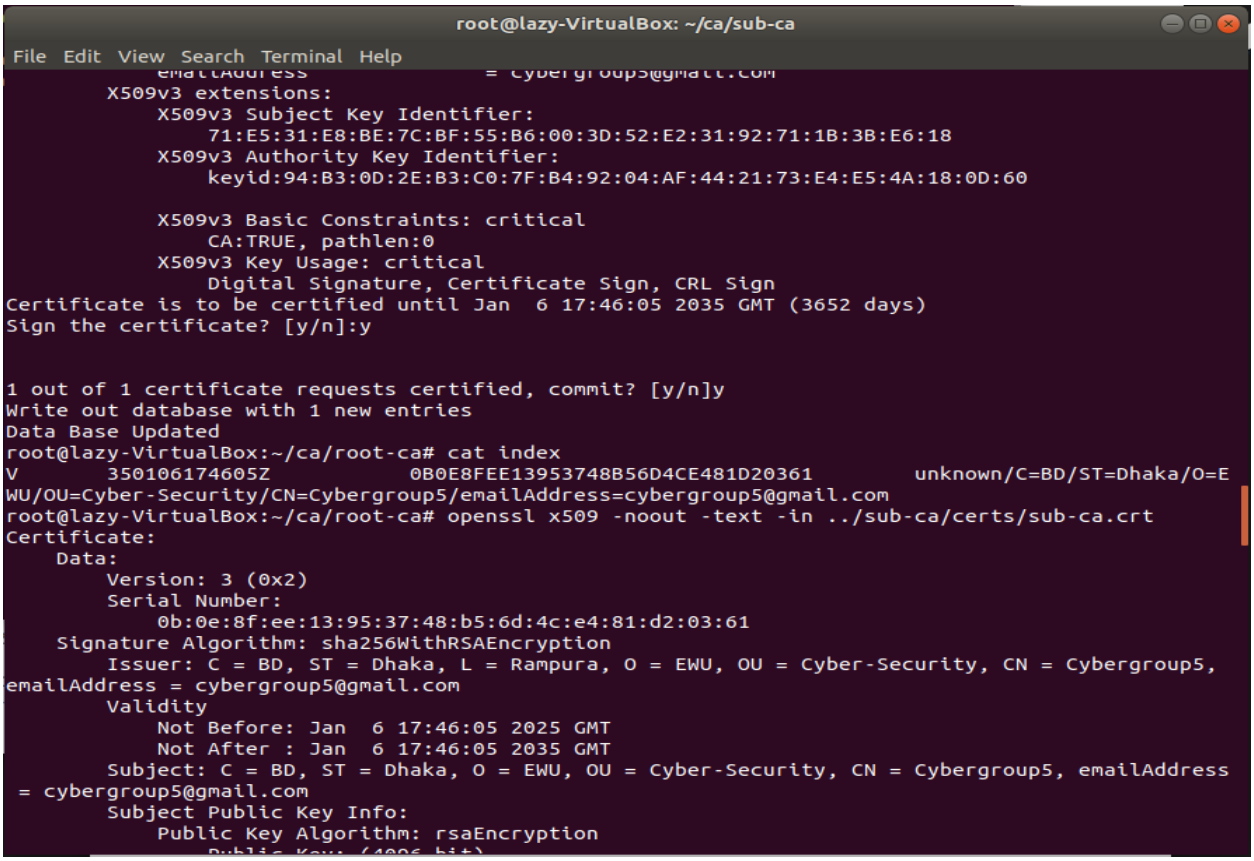
---

openssl ca-config root-ca.conf-extensions v3_intermediate_ca-days 3652-notext-in ../sub-ca/csr/sub-ca.csr-out ../sub-ca/certs/sub-ca.crt


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
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) [BD]:
State or Province Name [Dhaka]:
Locality Name [Rampura]:
Organization Name [EWU]:
Organizational Unit Name [Cyber-Security]:
Common Name [Cybergroup5]:
Email Address [cybergroup5@gmail.com]:
root@lazy-VirtualBox:~/ca/sub-ca# cd -
/root/ca/root-ca
root@lazy-VirtualBox:~/ca/root-ca# openssl ca -config root-ca.conf -extensions v3_intermediate_ca
-days 3652 -notext -in ../sub-ca/csr/sub-ca.csr -out ../sub-ca/certs/sub-ca.crt
Using configuration from root-ca.conf
Enter pass phrase for /root/ca/root-ca/private/ca.key:
Can't open /root/ca/root-ca/index.attr for reading, No such file or directory
139881329205696:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_f
ile.c:74:fopen('/root/ca/root-ca/index.attr','r')
139881329205696:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81
:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number:
0b:0e:8f:ee:13:95:37:48:b5:6d:4c:e4:81:d2:03:61
Validity
Not Before: Jan 6 17:46:05 2025 GMT
Not After : Jan 6 17:46:05 2035 GMT
Subject:
countryName = BD
stateOrProvinceName = Dhaka
organizationName = EWU
organizationalUnitName = Cyber-Security
commonName = Cybergroup5
emailAddress = cybergroup5@gmail.com


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
Enter pass phrase for /root/ca/root-ca/private/ca.key:
Can't open /root/ca/root-ca/index.attr for reading, No such file or directory
139881329205696:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_f
ile.c:74:fopen('/root/ca/root-ca/index.attr','r')
139881329205696:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81
:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number:
0b:0e:8f:ee:13:95:37:48:b5:6d:4c:e4:81:d2:03:61
Validity
Not Before: Jan 6 17:46:05 2025 GMT
Not After : Jan 6 17:46:05 2035 GMT
Subject:
countryName = BD
stateOrProvinceName = Dhaka
organizationName = EWU
organizationalUnitName = Cyber-Security
commonName = Cybergroup5
emailAddress = cybergroup5@gmail.com
X509v3 extensions:
X509v3 Subject Key Identifier:
71:E5:31:E8:BE:7C:BF:55:B6:00:3D:52:E2:31:92:71:1B:3B:E6:18
X509v3 Authority Key Identifier:
keyid:94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Jan 6 17:46:05 2035 GMT (3652 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries



Public Key Algorithm: rsaEncryption

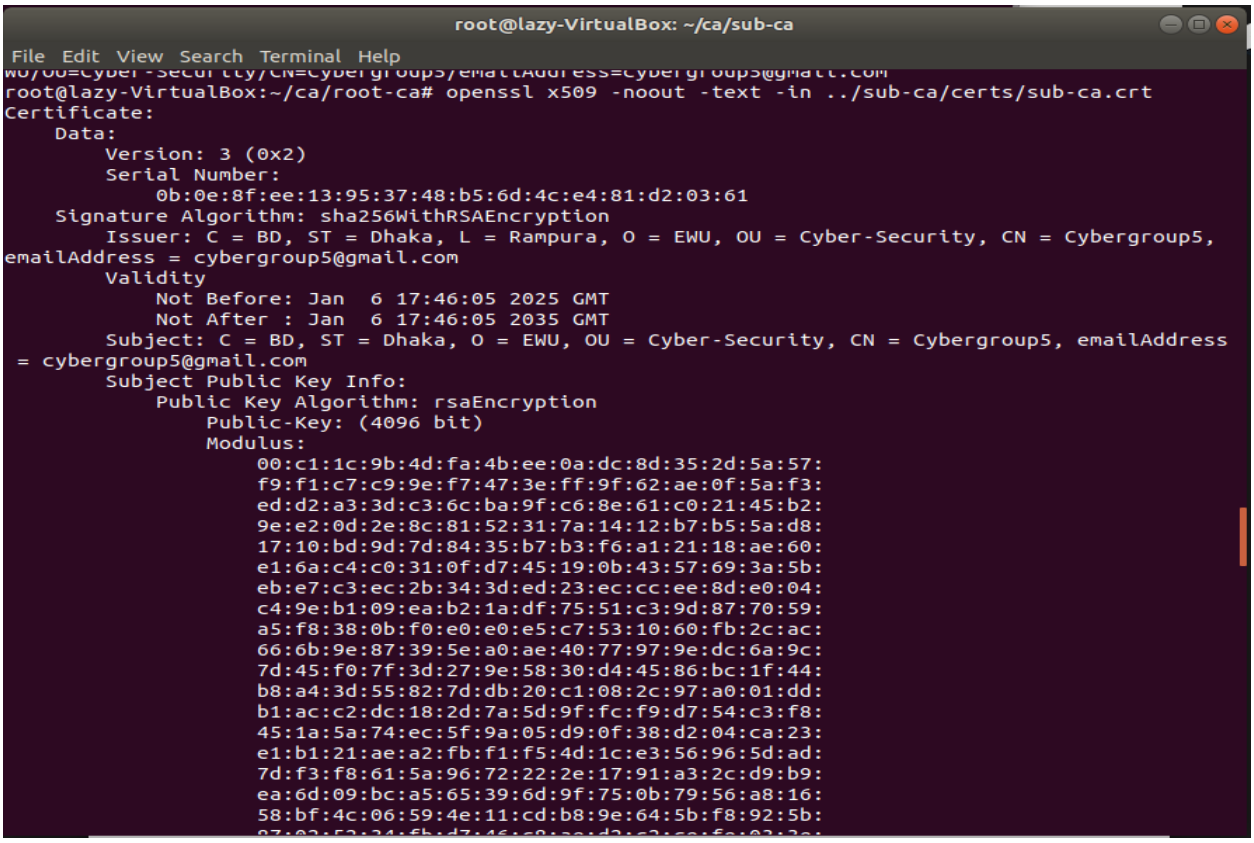
Public-Key: (4096 bit)

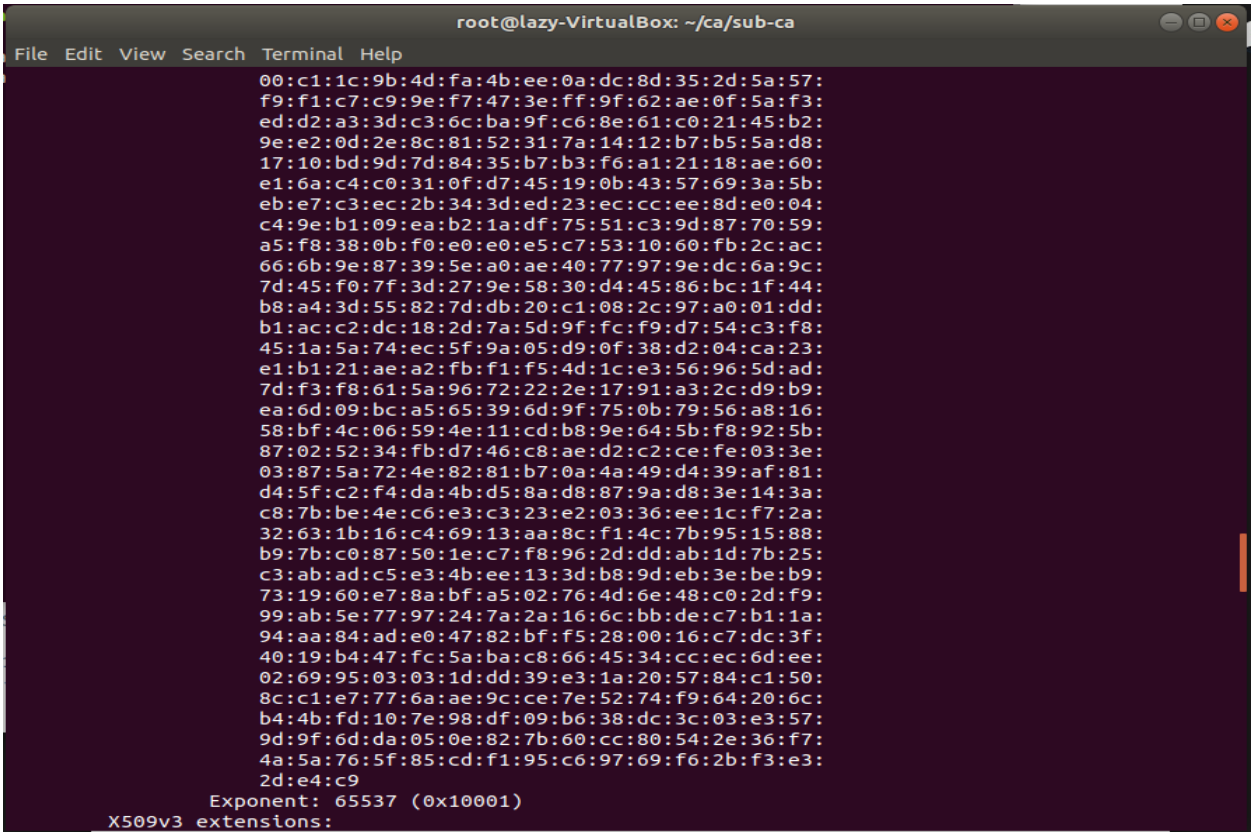
Modulus:

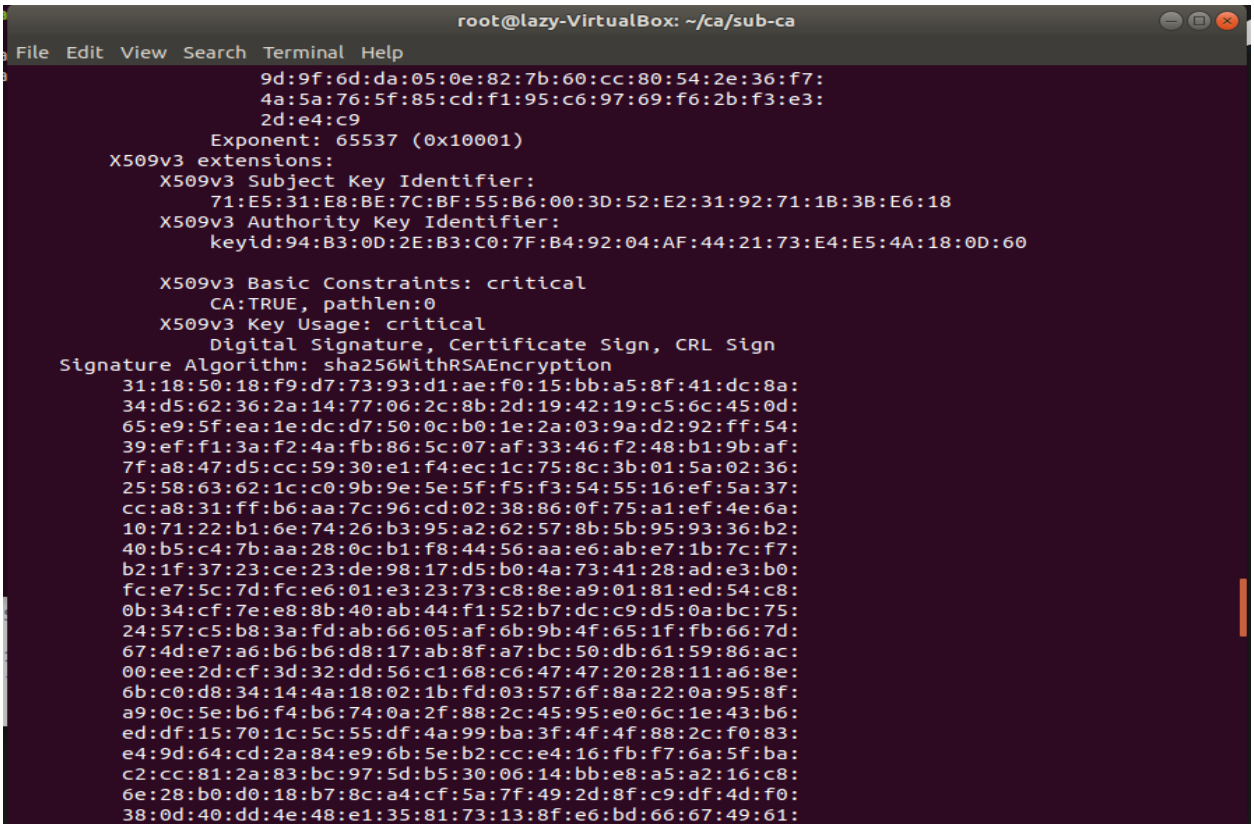
00:c1:1c:9b:4d:fa:4b:ee:0a:dc:8d:35:2d:5a:57:
f9:f1:c7:c9:9e:f7:47:3e:ff:9f:62:ae:0f:5a:f3:
ed:d2:a3:3d:c3:6c:ba:9f:c6:8e:61:c0:21:45:b2:
9e:e2:0d:2e:8c:81:52:31:7a:14:12:b7:b5:5a:d8:
17:10:bd:9d:7d:84:35:b7:b3:f6:a1:21:18:ae:60:
e1:6a:c4:c0:31:0f:d7:45:19:0b:43:57:69:3a:5b:
eb:e7:c3:ec:2b:34:3d:ed:23:ec:cc:ee:8d:e0:04:
c4:9e:b1:09:ea:b2:1a:df:75:51:c3:9d:87:70:59:
a5:f8:38:0b:f0:e0:e0:e5:c7:53:10:60:fb:2c:ac:
66:6b:9e:87:39:5e:a0:ae:40:77:97:9e:dc:6a:9c:
7d:45:f0:7f:3d:27:9e:58:30:d4:45:86:bc:1f:44:
b8:a4:3d:55:82:7d:db:20:c1:08:2c:97:a0:01:dd:
b1:ac:c2:dc:18:2d:7a:5d:9f:fc:f9:d7:54:c3:f8:
45:1a:5a:74:ec:5f:9a:05:d9:0f:38:d2:04:ca:23:
e1:b1:21:ae:a2:fb:f1:f5:4d:1c:e3:56:96:5d:ad:
7d:f3:f8:61:5a:96:72:22:2e:17:91:a3:2c:d9:b9:
ea:6d:09:bc:a5:65:39:6d:9f:75:0b:79:56:a8:16:
58:bf:4c:06:59:4e:11:cd:b8:9e:64:5b:f8:92:5b:
87:02:52:34:fb:d7:46:c8:ae:d2:c2:ce:fe:03:3e:
03:87:5a:72:4e:82:81:b7:0a:4a:49:d4:39:af:81:

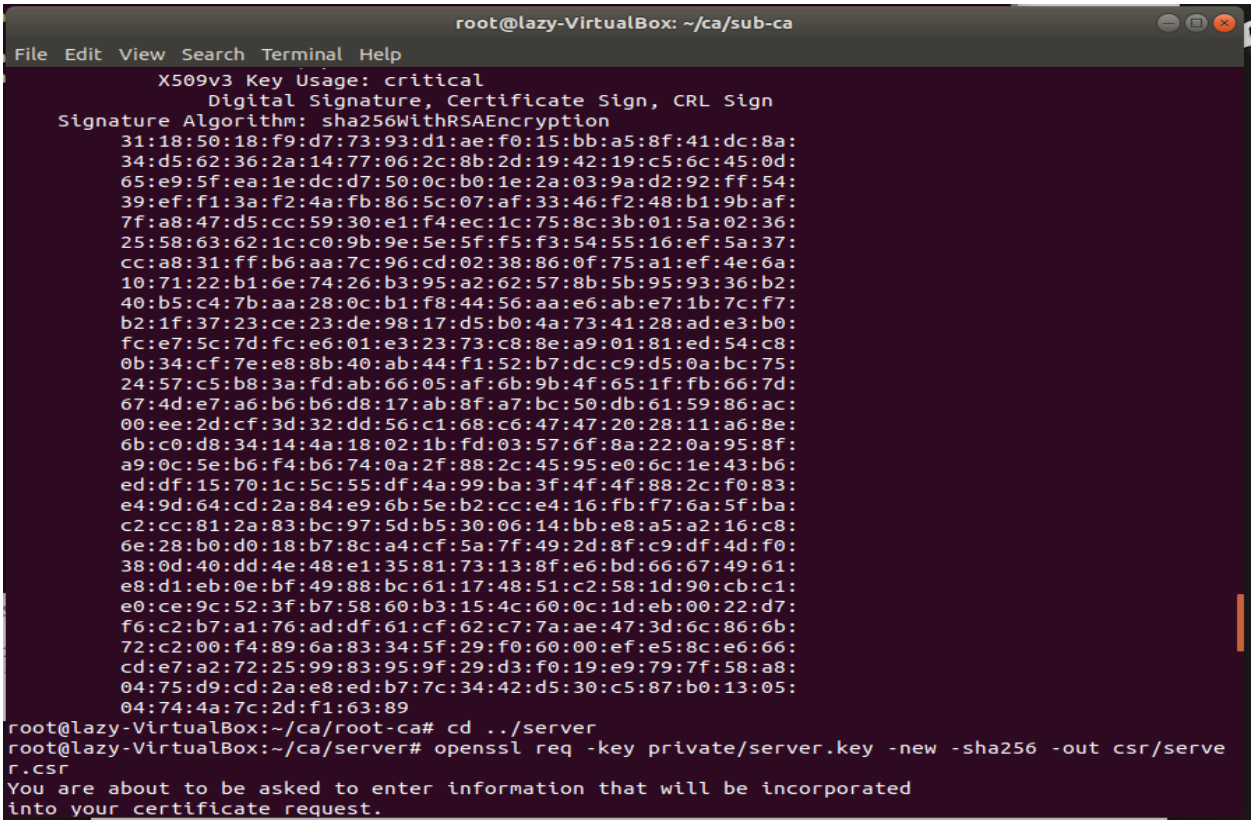
```
                d4:5f:c2:f4:da:4b:d5:8a:d8:87:9a:d8:3e:14:3a:
                c8:7b:be:4e:c6:e3:c3:23:e2:03:36:ee:1c:f7:2a:
                32:63:1b:16:c4:69:13:aa:8c:f1:4c:7b:95:15:88:
                b9:7b:c0:87:50:1e:c7:f8:96:2d:dd:ab:1d:7b:25:
                c3:ab:ad:c5:e3:4b:ee:13:3d:b8:9d:eb:3e:be:b9:
                73:19:60:e7:8a:bf:a5:02:76:4d:6e:48:c0:2d:f9:
                99:ab:5e:77:97:24:7a:2a:16:6c:bb:de:c7:b1:1a:
                94:aa:84:ad:e0:47:82:bf:f5:28:00:16:c7:dc:3f:
                40:19:b4:47:fc:5a:ba:c8:66:45:34:cc:ec:6d:ee:
                02:69:95:03:03:1d:dd:39:e3:1a:20:57:84:c1:50:
                8c:c1:e7:77:6a:ae:9c:ce:7e:52:74:f9:64:20:6c:
                b4:4b:fd:10:7e:98:df:09:b6:38:dc:3c:03:e3:57:
                9d:9f:6d:da:05:0e:82:7b:60:cc:80:54:2e:36:f7:
                4a:5a:76:5f:85:cd:f1:95:c6:97:69:f6:2b:f3:e3:
                2d:e4:c9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                71:E5:31:E8:BE:7C:BF:55:B6:00:3D:52:E2:31:92:71:1B:3B:E6:18
            X509v3 Authority Key Identifier:
                keyid:94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
        31:18:50:18:f9:d7:73:93:d1:ae:f0:15:bb:a5:8f:41:dc:8a:
        34:d5:62:36:2a:14:77:06:2c:8b:2d:19:42:19:c5:6c:45:0d:
        65:e9:5f:ea:1e:dc:d7:50:0c:b0:1e:2a:03:9a:d2:92:ff:54:
        39:ef:f1:3a:f2:4a:fb:86:5c:07:af:33:46:f2:48:b1:9b:af:
        7f:a8:47:d5:cc:59:30:e1:f4:ec:1c:75:8c:3b:01:5a:02:36:
        25:58:63:62:1c:c0:9b:9e:5e:5f:f5:f3:54:55:16:ef:5a:37:
        cc:a8:31:ff:b6:aa:7c:96:cd:02:38:86:0f:75:a1:ef:4e:6a:
        10:71:22:b1:6e:74:26:b3:95:a2:62:57:8b:5b:95:93:36:b2:
        40:b5:c4:7b:aa:28:0c:b1:f8:44:56:aa:e6:ab:e7:1b:7c:f7:
        b2:1f:37:23:ce:23:de:98:17:d5:b0:4a:73:41:28:ad:e3:b0:
        fc:e7:5c:7d:fc:e6:01:e3:23:73:c8:8e:a9:01:81:ed:54:c8:
        0b:34:cf:7e:e8:8b:40:ab:44:f1:52:b7:dc:c9:d5:0a:bc:75:
        24:57:c5:b8:3a:fd:ab:66:05:af:6b:9b:4f:65:1f:fb:66:7d:
        67:4d:e7:a6:b6:b6:d8:17:ab:8f:a7:bc:50:db:61:59:86:ac:
        00:ee:2d:cf:3d:32:dd:56:c1:68:c6:47:47:20:28:11:a6:8e:
        6b:c0:d8:34:14:4a:18:02:1b:fd:03:57:6f:8a:22:0a:95:8f:
        a9:0c:5e:b6:f4:b6:74:0a:2f:88:2c:45:95:e0:6c:1e:43:b6:
        ed:df:15:70:1c:5c:55:df:4a:99:ba:3f:4f:4f:88:2c:f0:83:
        e4:9d:64:cd:2a:84:e9:6b:5e:b2:cc:e4:16:fb:f7:6a:5f:ba:
```

c2:cc:81:2a:83:bc:97:5d:b5:30:06:14:bb:e8:a5:a2:16:c8:
6e:28:b0:d0:18:b7:8c:a4:cf:5a:7f:49:2d:8f:c9:df:4d:f0:
38:0d:40:dd:4e:48:e1:35:81:73:13:8f:e6:bd:66:67:49:61:
e8:d1:eb:0e:bf:49:88:bc:61:17:48:51:c2:58:1d:90:cb:c1:
e0:ce:9c:52:3f:b7:58:60:b3:15:4c:60:0c:1d:eb:00:22:d7:
f6:c2:b7:a1:76:ad:df:61:cf:62:c7:7a:ae:47:3d:6c:86:6b:
72:c2:00:f4:89:6a:83:34:5f:29:f0:60:00:ef:e5:8c:e6:66:
cd:e7:a2:72:25:99:83:95:9f:29:d3:f0:19:e9:79:7f:58:a8:
04:75:d9:cd:2a:e8:ed:b7:7c:34:42:d5:30:c5:87:b0:13:05:
04:74:4a:7c:2d:f1:63:89




root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
00:c1:1c:9b:4d:fa:4b:ee:0a:dc:8d:35:2d:5a:57:
f9:f1:c7:c9:9e:f7:47:3e:ff:9f:62:ae:0f:5a:f3:
ed:d2:a3:3d:c3:6c:ba:9f:c6:8e:61:c0:21:45:b2:
9e:e2:0d:2e:8c:81:52:31:7a:14:12:b7:b5:5a:d8:
17:10:bd:9d:7d:84:35:b7:b3:f6:a1:21:18:ae:60:
e1:6a:c4:c0:31:0f:d7:45:19:0b:43:57:69:3a:5b:
eb:e7:c3:ec:2b:34:3d:ed:23:ec:cc:ee:8d:e0:04:
c4:9e:b1:09:ea:b2:1a:df:75:51:c3:9d:87:70:59:
a5:f8:38:0b:f0:e0:e0:e5:c7:53:10:60:fb:2c:ac:
66:6b:9e:87:39:5e:a0:ae:40:77:97:9e:dc:6a:9c:
7d:45:f0:7f:3d:27:9e:58:30:d4:45:86:bc:1f:44:
b8:a4:3d:55:82:7d:db:20:c1:08:2c:97:a0:01:dd:
b1:ac:c2:dc:18:2d:7a:5d:9f:fc:f9:d7:54:c3:f8:
45:1a:5a:74:ec:5f:9a:05:d9:0f:38:d2:04:ca:23:
e1:b1:21:ae:a2:fb:f1:f5:4d:1c:e3:56:96:5d:ad:
7d:f3:f8:61:5a:96:72:22:2e:17:91:a3:2c:d9:b9:
ea:6d:09:bc:a5:65:39:6d:9f:75:0b:79:56:a8:16:
58:bf:4c:06:59:4e:11:cd:b8:9e:64:5b:f8:92:5b:
87:02:52:34:fb:d7:46:c8:ae:d2:c2:ce:fe:03:3e:
03:87:5a:72:4e:82:81:b7:0a:4a:49:d4:39:af:81:
d4:5f:c2:f4:da:4b:d5:8a:d8:87:9a:d8:3e:14:3a:
c8:7b:be:4e:c6:e3:c3:23:e2:03:36:ee:1c:f7:2a:
32:63:1b:16:c4:69:13:aa:8c:f1:4c:7b:95:15:88:
b9:7b:c0:87:50:1e:c7:f8:96:2d:dd:ab:1d:7b:25:
c3:ab:ad:c5:e3:4b:ee:13:3d:b8:9d:eb:3e:be:b9:
73:19:60:e7:8a:bf:a5:02:76:4d:6e:48:c0:2d:f9:
99:ab:5e:77:97:24:7a:2a:16:6c:bb:de:c7:b1:1a:
94:aa:84:ad:e0:47:82:bf:f5:28:00:16:c7:dc:3f:
40:19:b4:47:fc:5a:ba:c8:66:45:34:cc:ec:6d:ee:
02:69:95:03:03:1d:dd:39:e3:1a:20:57:84:c1:50:
8c:c1:e7:77:6a:ae:9c:ce:7e:52:74:f9:64:20:6c:
b4:4b:fd:10:7e:98:df:09:b6:38:dc:3c:03:e3:57:
9d:9f:6d:da:05:0e:82:7b:60:cc:80:54:2e:36:f7:
4a:5a:76:5f:85:cd:f1:95:c6:97:69:f6:2b:f3:e3:
2d:e4:c9
Exponent: 65537 (0x10001)
X509v3 extensions:


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
9d:9f:6d:da:05:0e:82:7b:60:cc:80:54:2e:36:f7:
4a:5a:76:5f:85:cd:f1:95:c6:97:69:f6:2b:f3:e3:
2d:e4:c9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
71:E5:31:E8:BE:7C:BF:55:B6:00:3D:52:E2:31:92:71:1B:3B:E6:18
X509v3 Authority Key Identifier:
keyid:94:B3:0D:2E:B3:C0:7F:B4:92:04:AF:44:21:73:E4:E5:4A:18:0D:60
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
31:18:50:18:f9:d7:73:93:d1:ae:f0:15:bb:a5:8f:41:dc:8a:
34:d5:62:36:2a:14:77:06:2c:8b:2d:19:42:19:c5:6c:45:0d:
65:e9:5f:ea:1e:dc:d7:50:0c:b0:1e:2a:03:9a:d2:92:ff:54:
39:ef:f1:3a:f2:4a:fb:86:5c:07:af:33:46:f2:48:b1:9b:af:
7f:a8:47:d5:cc:59:30:e1:f4:ec:1c:75:8c:3b:01:5a:02:36:
25:58:63:62:1c:c0:9b:9e:5e:5f:f5:f3:54:55:16:ef:5a:37:
cc:a8:31:ff:b6:aa:7c:96:cd:02:38:86:0f:75:a1:ef:4e:6a:
10:71:22:b1:6e:74:26:b3:95:a2:62:57:8b:5b:95:93:36:b2:
40:b5:c4:7b:aa:28:0c:b1:f8:44:56:aa:e6:ab:e7:1b:7c:f7:
b2:1f:37:23:ce:23:de:98:17:d5:b0:4a:73:41:28:ad:e3:b0:
fc:e7:5c:7d:fc:e6:01:e3:23:73:c8:8e:a9:01:81:ed:54:c8:
0b:34:cf:7e:e8:8b:40:ab:44:f1:52:b7:dc:c9:d5:0a:bc:75:
24:57:c5:b8:3a:fd:ab:66:05:af:6b:9b:4f:65:1f:fb:66:7d:
67:4d:e7:a6:b6:b6:d8:17:ab:8f:a7:bc:50:db:61:59:86:ac:
00:ee:2d:cf:3d:32:dd:56:c1:68:c6:47:47:20:28:11:a6:8e:
6b:c0:d8:34:14:4a:18:02:1b:fd:03:57:6f:8a:22:0a:95:8f:
a9:0c:5e:b6:f4:b6:74:0a:2f:88:2c:45:95:e0:6c:1e:43:b6:
ed:df:15:70:1c:5c:55:df:4a:99:ba:3f:4f:4f:88:2c:f0:83:
e4:9d:64:cd:2a:84:e9:6b:5e:b2:cc:e4:16:fb:f7:6a:5f:ba:
c2:cc:81:2a:83:bc:97:5d:b5:30:06:14:bb:e8:a5:a2:16:c8:
6e:28:b0:d0:18:b7:8c:a4:cf:5a:7f:49:2d:8f:c9:df:4d:f0:
38:0d:40:dd:4e:48:e1:35:81:73:13:8f:e6:bd:66:67:49:61:



● Movingtoserver

● Generating certificate signing request from server

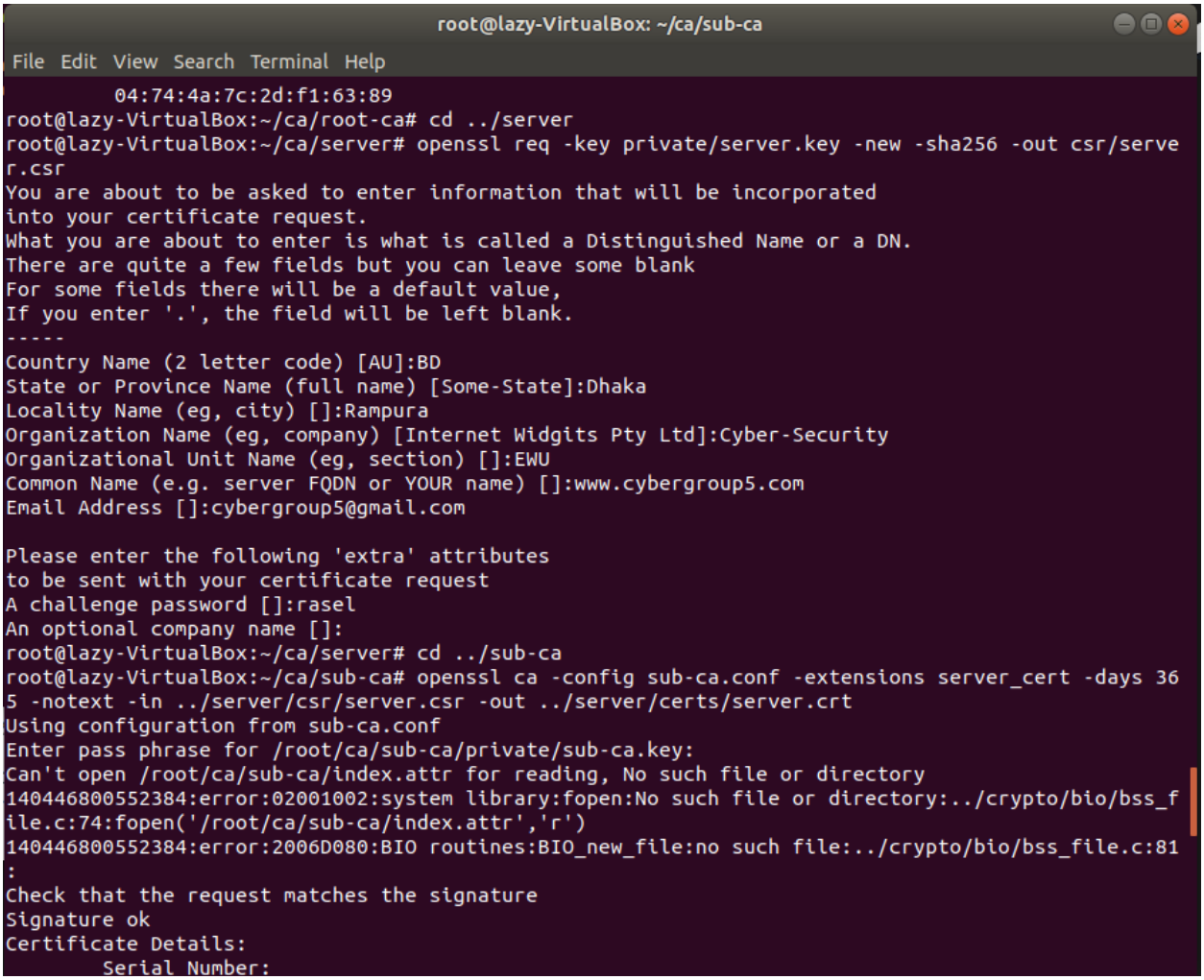
---

openssl req-key private/server.key-new-sha256-out csr/ server.csr

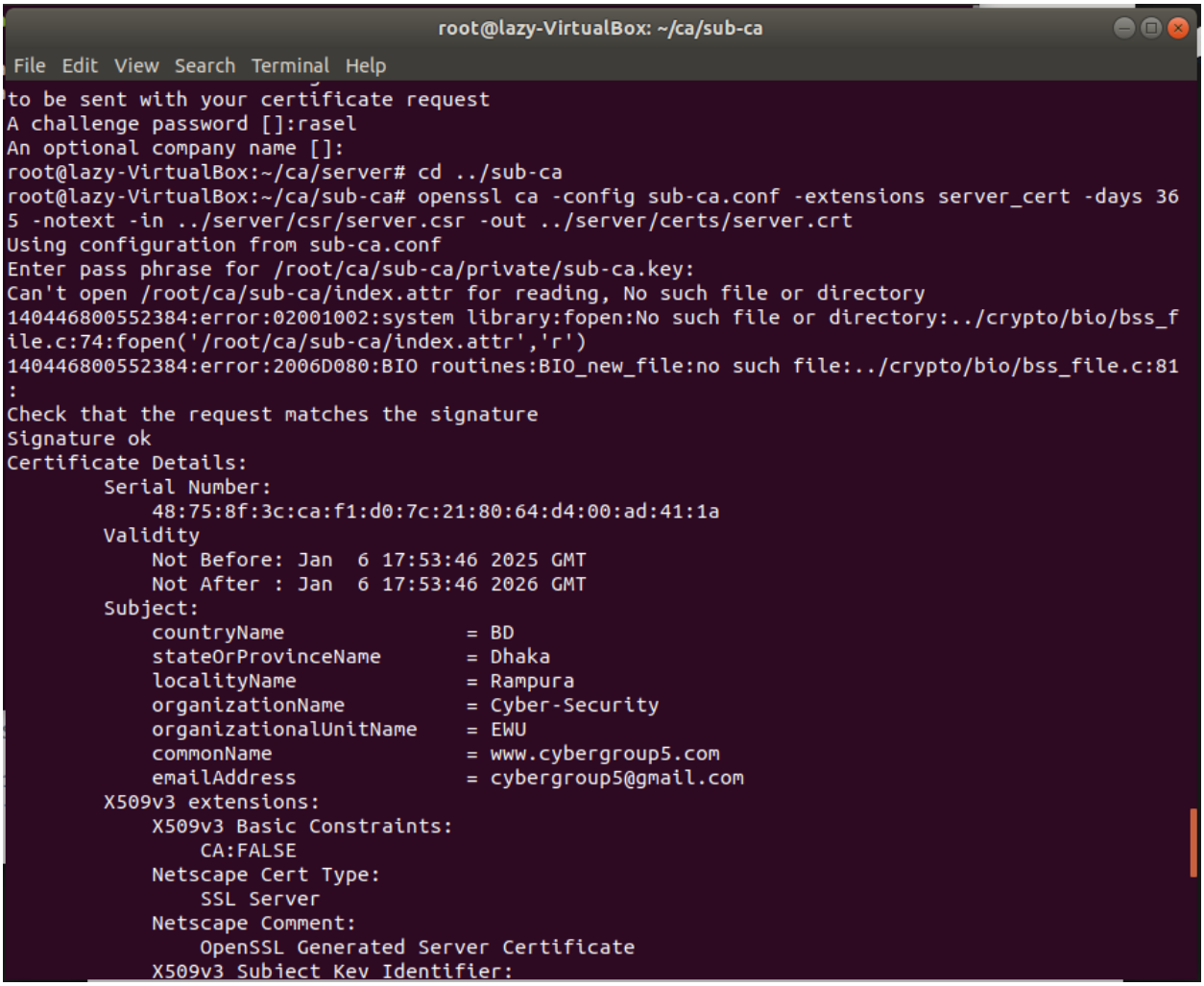
Sub ca signing certificate request of server

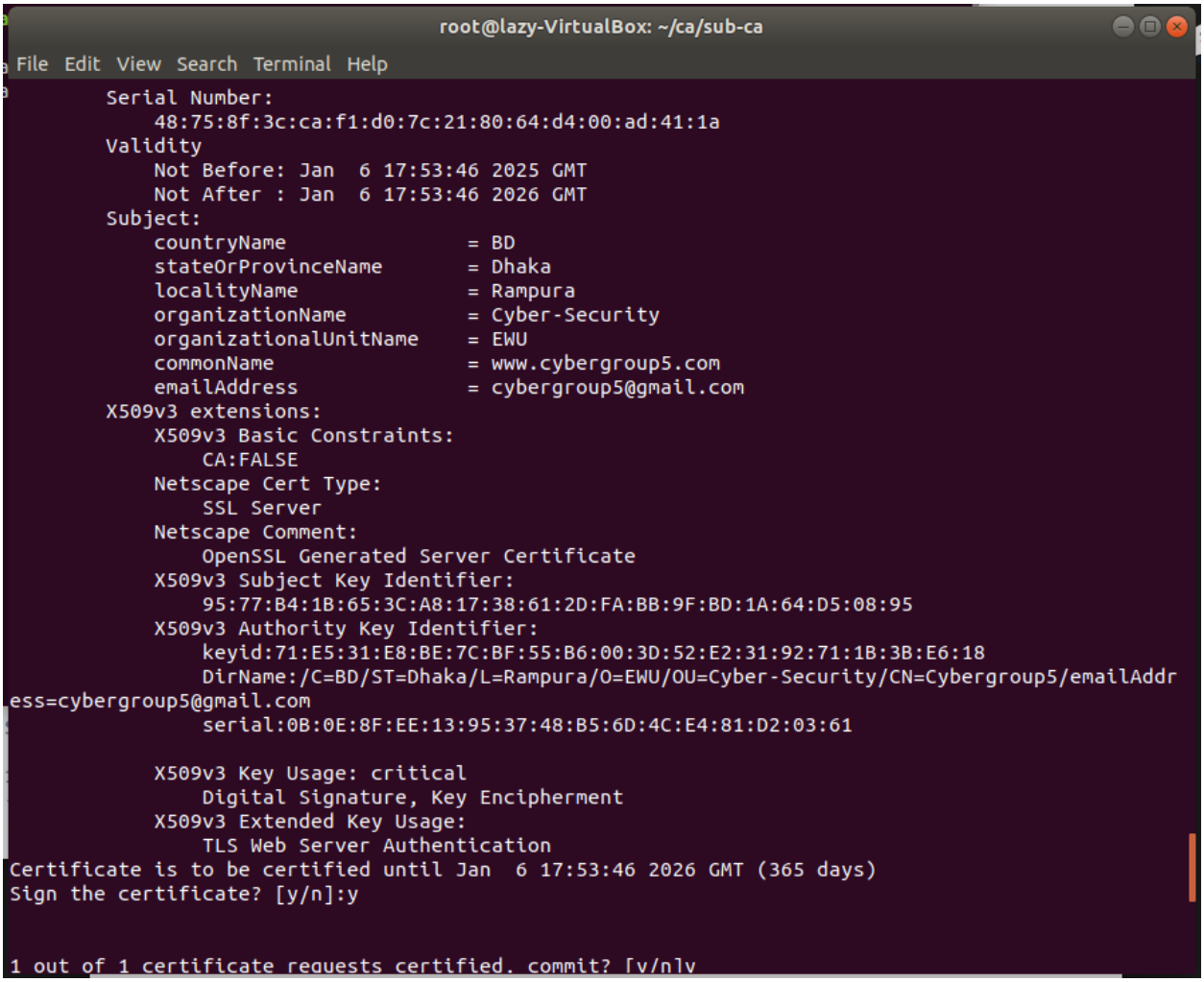
---

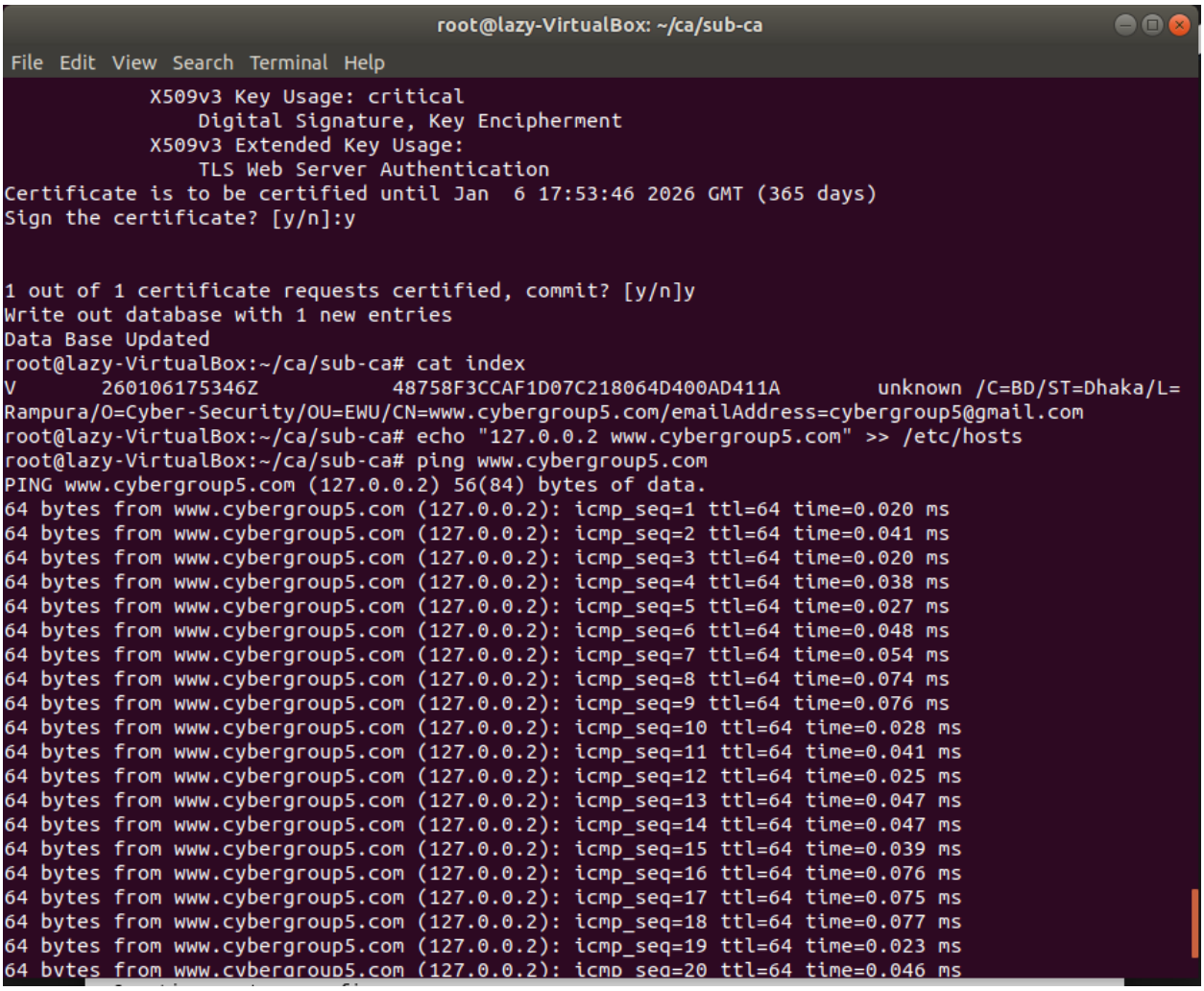
openssl ca-config sub-ca.conf-extensions server_cert-days 365-notext-in ../server/csr/server.csr-out ../server/certs/server.cr


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
04:74:4a:7c:2d:f1:63:89
root@lazy-VirtualBox:~/ca/root-ca# cd ../server
root@lazy-VirtualBox:~/ca/server# openssl req -key private/server.key -new -sha256 -out csr/server.csr
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]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Rampura
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cyber-Security
Organizational Unit Name (eg, section) []:EWU
Common Name (e.g. server FQDN or YOUR name) []:www.cybergroup5.com
Email Address []:cybergroup5@gmail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:rasel
An optional company name []:
root@lazy-VirtualBox:~/ca/server# cd ../sub-ca
root@lazy-VirtualBox:~/ca/sub-ca# openssl ca -config sub-ca.conf -extensions server_cert -days 365 -notext -in ../server/csr/server.csr -out ../server/certs/server.crt
Using configuration from sub-ca.conf
Enter pass phrase for /root/ca/sub-ca/private/sub-ca.key:
Can't open /root/ca/sub-ca/index.attr for reading, No such file or directory
140446800552384:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:74:fopen('/root/ca/sub-ca/index.attr','r')
140446800552384:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number:


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
to be sent with your certificate request
A challenge password []:rasel
An optional company name []:
root@lazy-VirtualBox:~/ca/server# cd ../sub-ca
root@lazy-VirtualBox:~/ca/sub-ca# openssl ca -config sub-ca.conf -extensions server_cert -days 36
5 -notext -in ../server/csr/server.csr -out ../server/certs/server.crt
Using configuration from sub-ca.conf
Enter pass phrase for /root/ca/sub-ca/private/sub-ca.key:
Can't open /root/ca/sub-ca/index.attr for reading, No such file or directory
140446800552384:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_f
ile.c:74:fopen('/root/ca/sub-ca/index.attr','r')
140446800552384:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81
:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number:
48:75:8f:3c:ca:f1:d0:7c:21:80:64:d4:00:ad:41:1a
Validity
Not Before: Jan 6 17:53:46 2025 GMT
Not After : Jan 6 17:53:46 2026 GMT
Subject:
countryName = BD
stateOrProvinceName = Dhaka
localityName = Rampura
organizationName = Cyber-Security
organizationalUnitName = EWU
commonName = www.cybergroup5.com
emailAddress = cybergroup5@gmail.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Cert Type:
SSL Server
Netscape Comment:
OpenSSL Generated Server Certificate
X509v3 Subject Key Identifier:


root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
Serial Number:
48:75:8f:3c:ca:f1:d0:7c:21:80:64:d4:00:ad:41:1a
Validity
Not Before: Jan 6 17:53:46 2025 GMT
Not After : Jan 6 17:53:46 2026 GMT
Subject:
countryName = BD
stateOrProvinceName = Dhaka
localityName = Rampura
organizationName = Cyber-Security
organizationalUnitName = EWU
commonName = www.cybergroup5.com
emailAddress = cybergroup5@gmail.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Cert Type:
SSL Server
Netscape Comment:
OpenSSL Generated Server Certificate
X509v3 Subject Key Identifier:
95:77:B4:1B:65:3C:A8:17:38:61:2D:FA:BB:9F:BD:1A:64:D5:08:95
X509v3 Authority Key Identifier:
keyid:71:E5:31:E8:BE:7C:BF:55:B6:00:3D:52:E2:31:92:71:1B:3B:E6:18
DirName:/C=BD/ST=Dhaka/L=Rampura/O=EWU/OU=Cyber-Security/CN=Cybergroup5/emailAddr
ess=cybergroup5@gmail.com
serial:0B:0E:8F:EE:13:95:37:48:B5:6D:4C:E4:81:D2:03:61
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
Certificate is to be certified until Jan 6 17:53:46 2026 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y



To see details

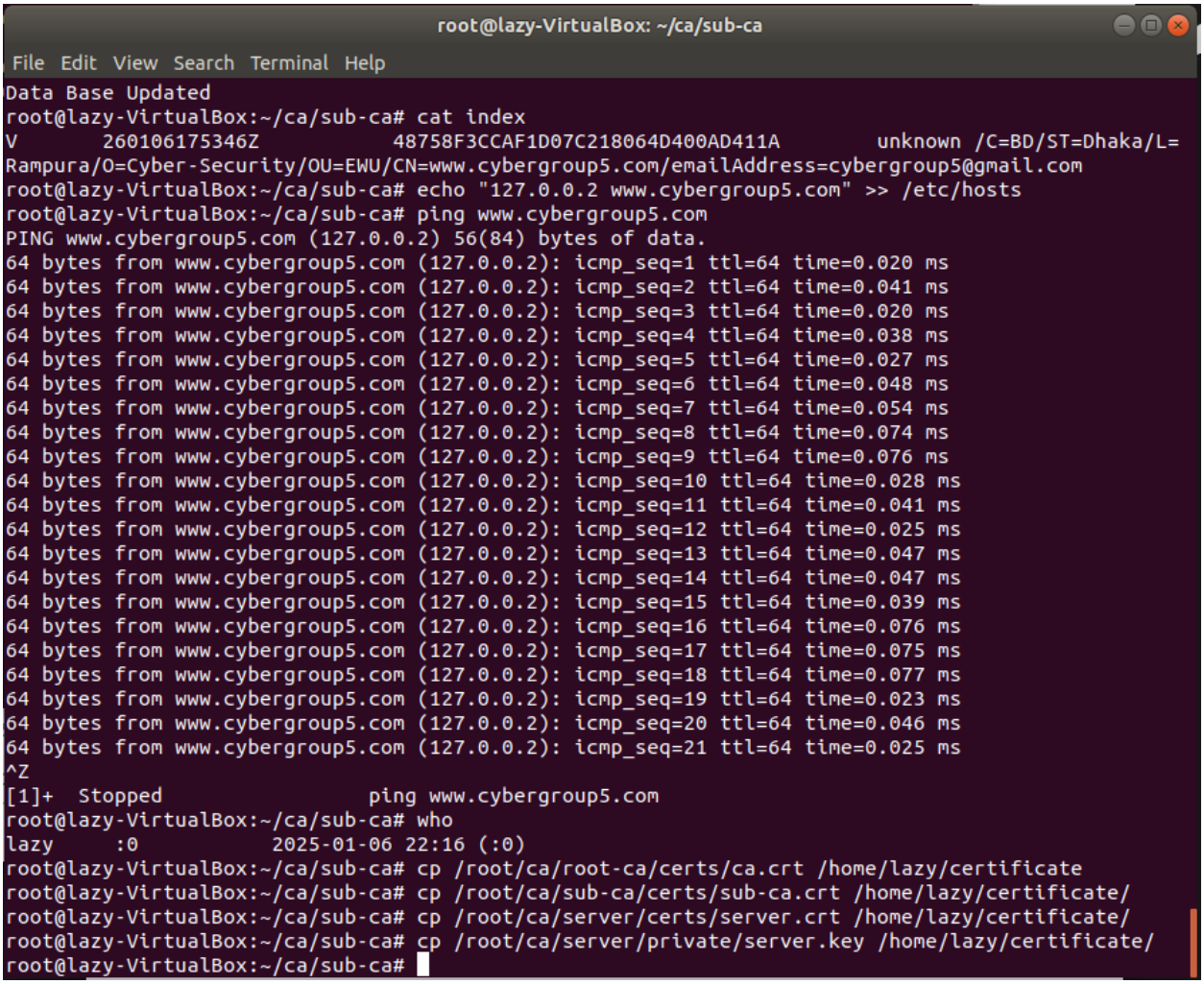
---

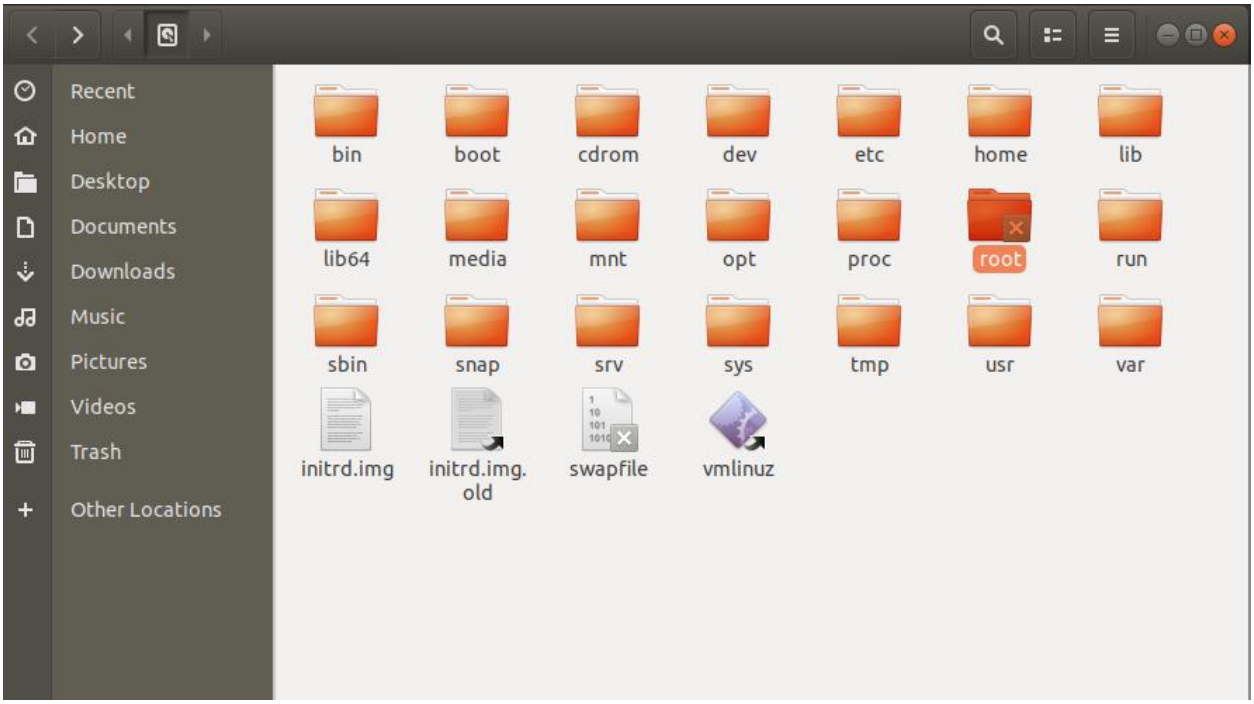
cat index

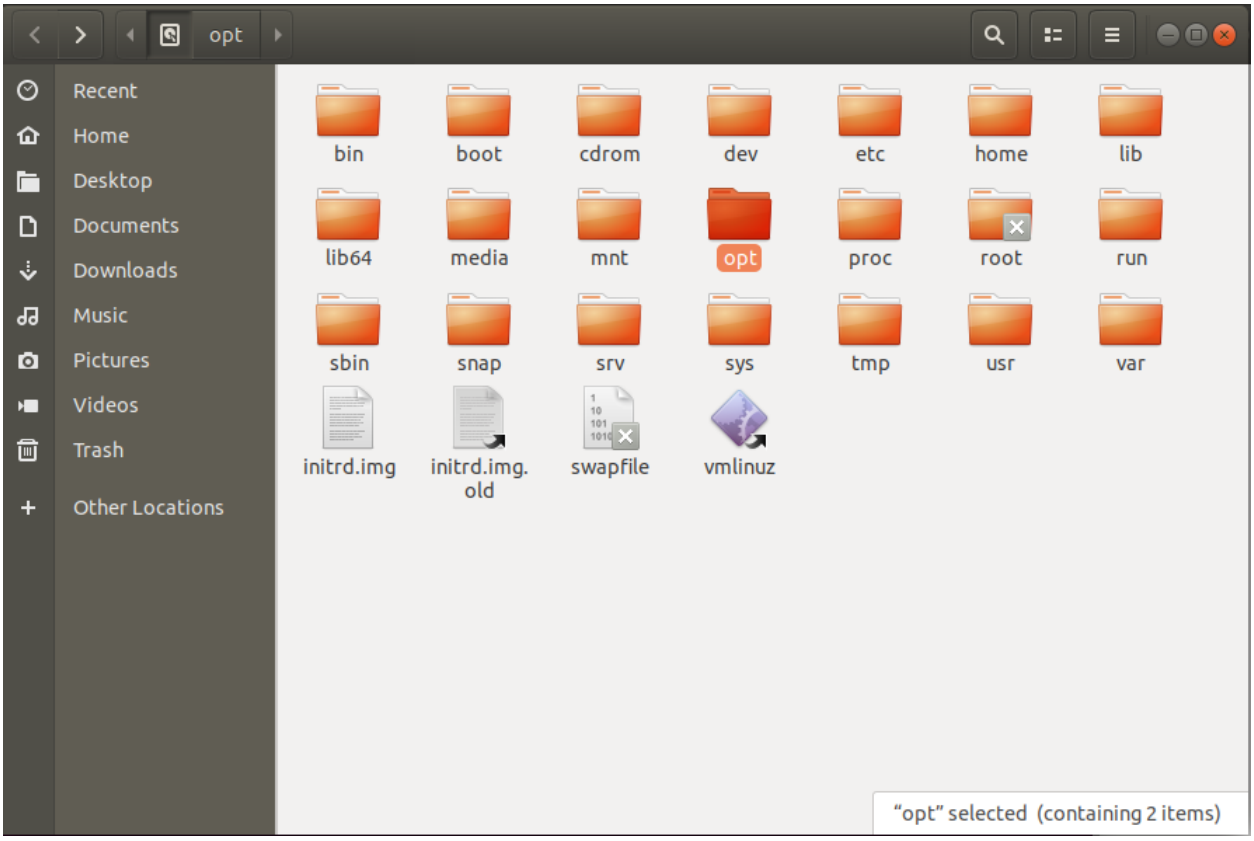
Verifying via the ping command

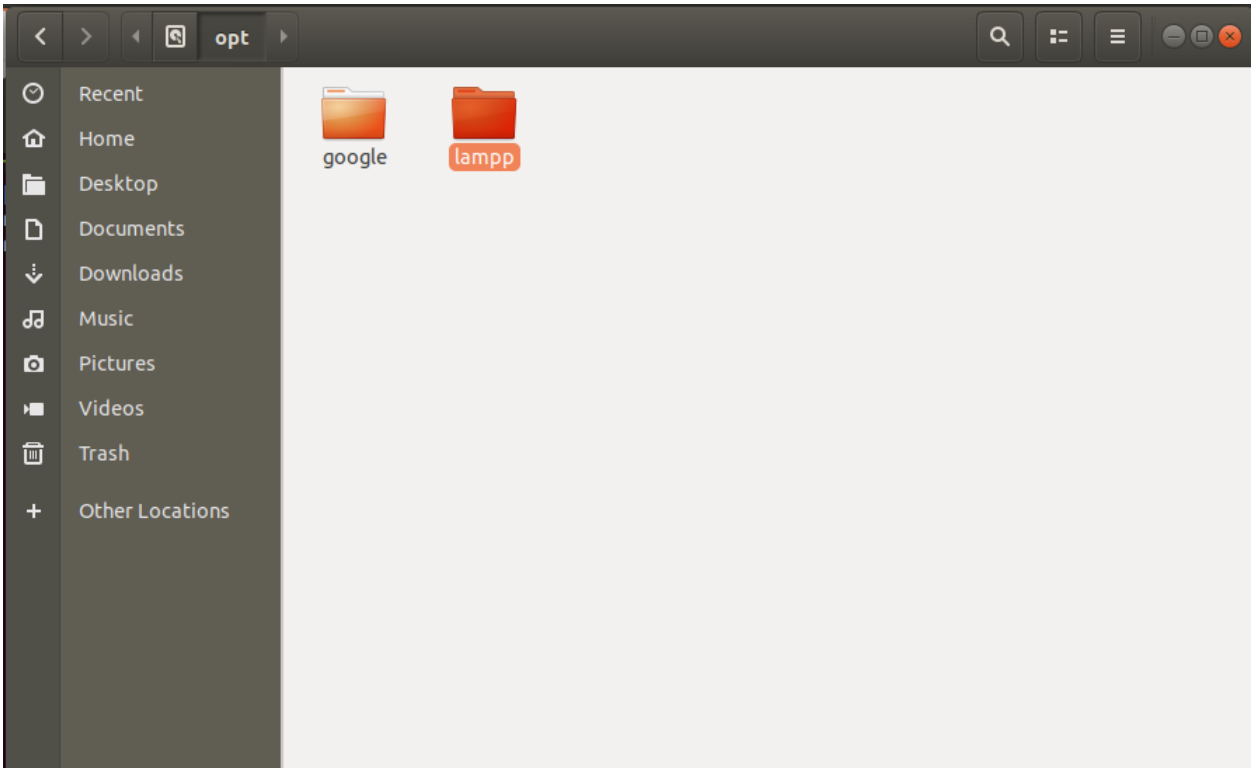
---

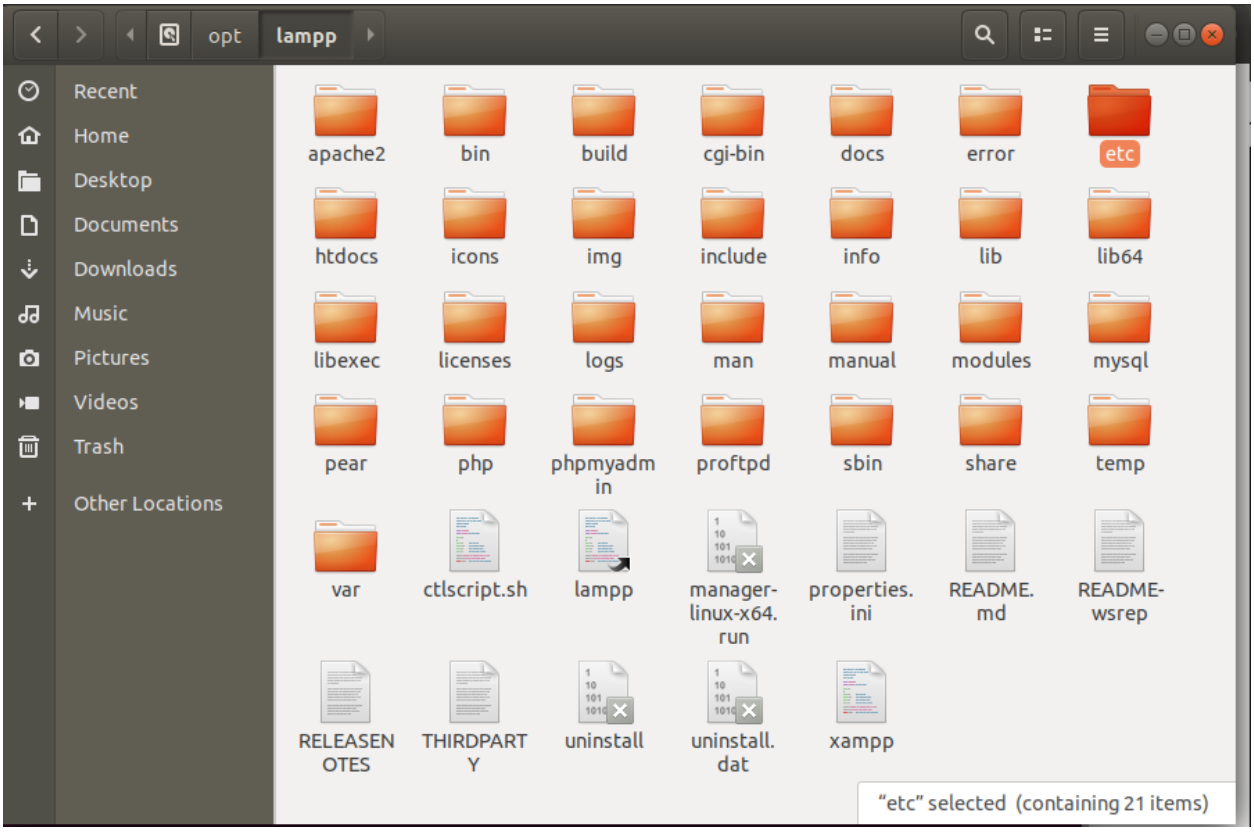
www.cybergroup5.com

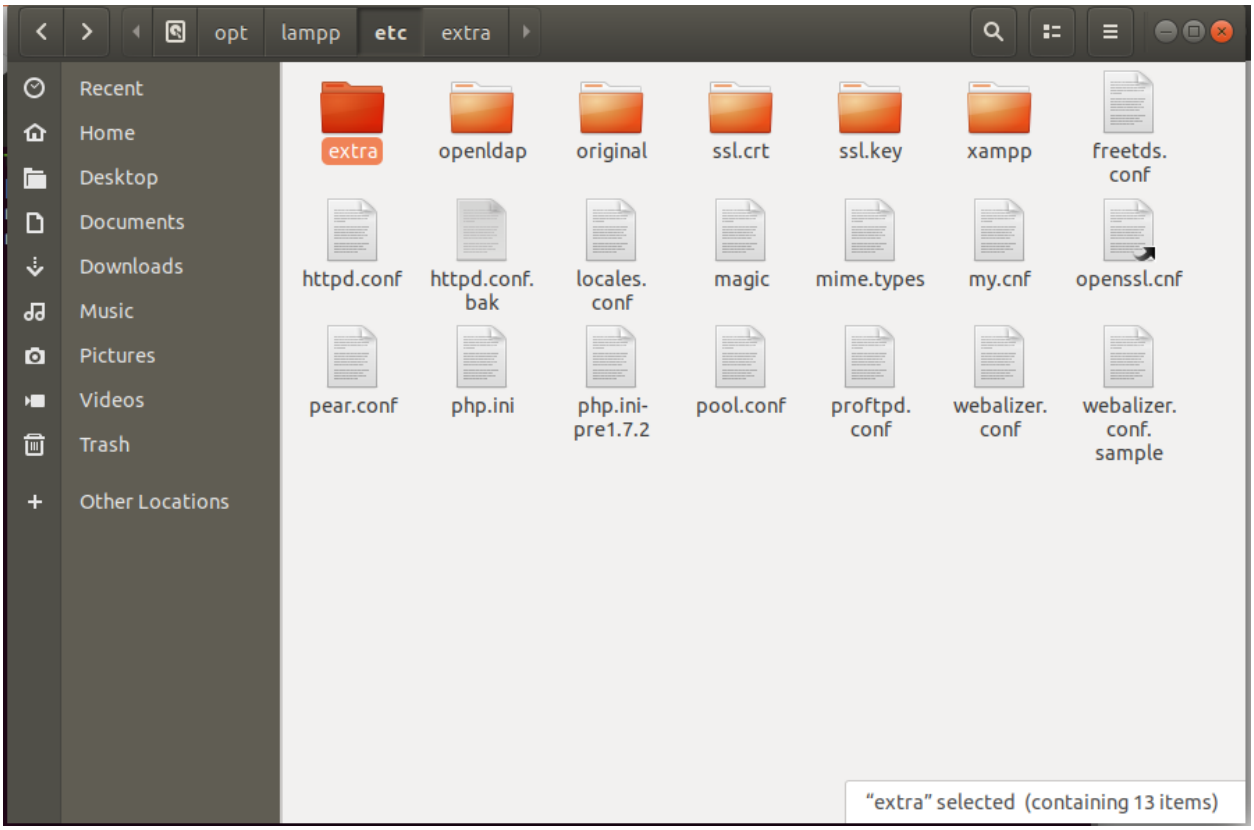

root@lazy-VirtualBox: ~/ca/sub-ca
File Edit View Search Terminal Help
Data Base Updated
root@lazy-VirtualBox:~/ca/sub-ca# cat index
V 260106175346Z 48758F3CCAF1D07C218064D400AD411A unknown /C=BD/ST=Dhaka/L=
Rampura/O=Cyber-Security/OU=EWU/CN=www.cybergroup5.com/emailAddress=cybergroup5@gmail.com
root@lazy-VirtualBox:~/ca/sub-ca# echo "127.0.0.2 www.cybergroup5.com" >> /etc/hosts
root@lazy-VirtualBox:~/ca/sub-ca# ping www.cybergroup5.com
PING www.cybergroup5.com (127.0.0.2) 56(84) bytes of data.
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=3 ttl=64 time=0.020 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=5 ttl=64 time=0.027 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=7 ttl=64 time=0.054 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=8 ttl=64 time=0.074 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=9 ttl=64 time=0.076 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=10 ttl=64 time=0.028 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=11 ttl=64 time=0.041 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=12 ttl=64 time=0.025 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=13 ttl=64 time=0.047 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=14 ttl=64 time=0.047 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=15 ttl=64 time=0.039 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=16 ttl=64 time=0.076 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=17 ttl=64 time=0.075 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=18 ttl=64 time=0.077 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=19 ttl=64 time=0.023 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=20 ttl=64 time=0.046 ms
64 bytes from www.cybergroup5.com (127.0.0.2): icmp_seq=21 ttl=64 time=0.025 ms
^Z
[1]+ Stopped ping www.cybergroup5.com
root@lazy-VirtualBox:~/ca/sub-ca# who
lazy :0 2025-01-06 22:16 (:0)
root@lazy-VirtualBox:~/ca/sub-ca# cp /root/ca/root-ca/certs/ca.crt /home/lazy/certificate
root@lazy-VirtualBox:~/ca/sub-ca# cp /root/ca/sub-ca/certs/sub-ca.crt /home/lazy/certificate/
root@lazy-VirtualBox:~/ca/sub-ca# cp /root/ca/server/certs/server.crt /home/lazy/certificate/
root@lazy-VirtualBox:~/ca/sub-ca# cp /root/ca/server/private/server.key /home/lazy/certificate/
root@lazy-VirtualBox:~/ca/sub-ca#

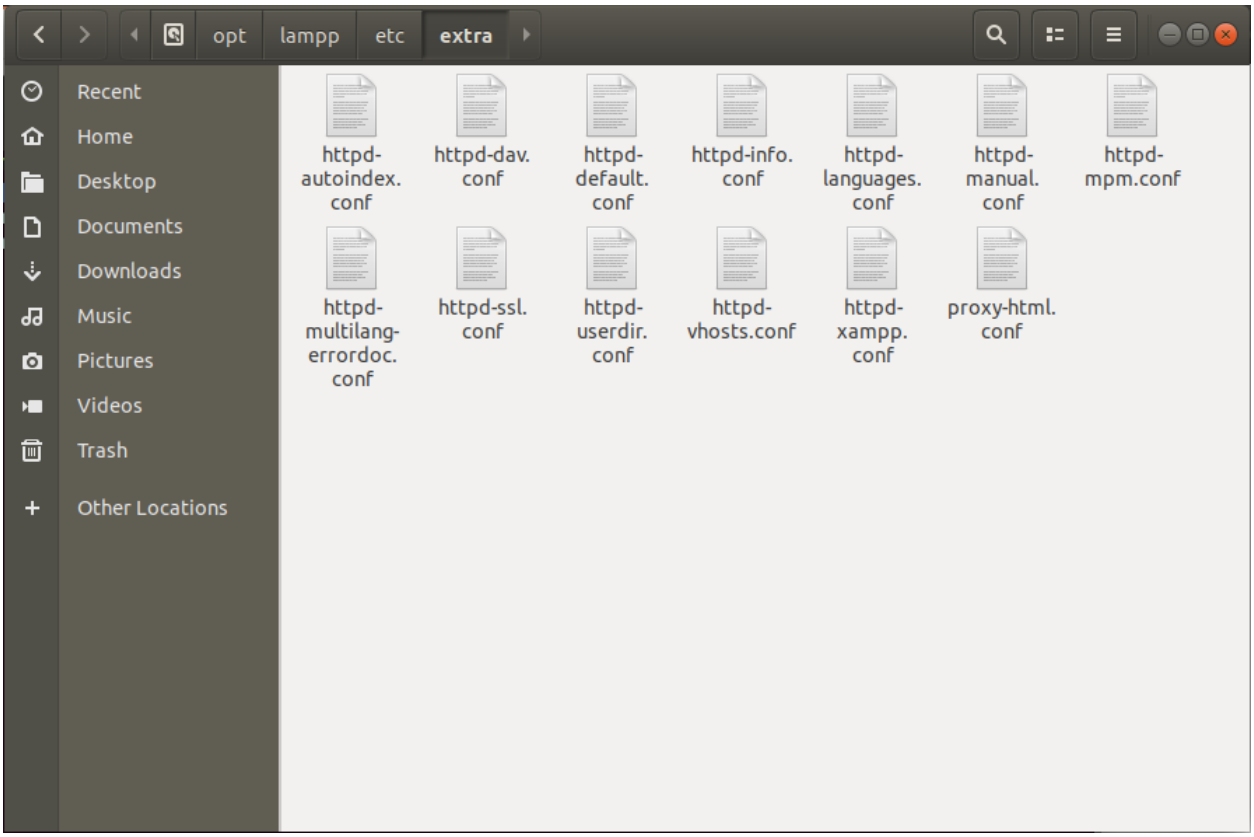

Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
bin
boot
cdrom
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
initrd.img
initrd.img.old
swapfile
vmlinuz

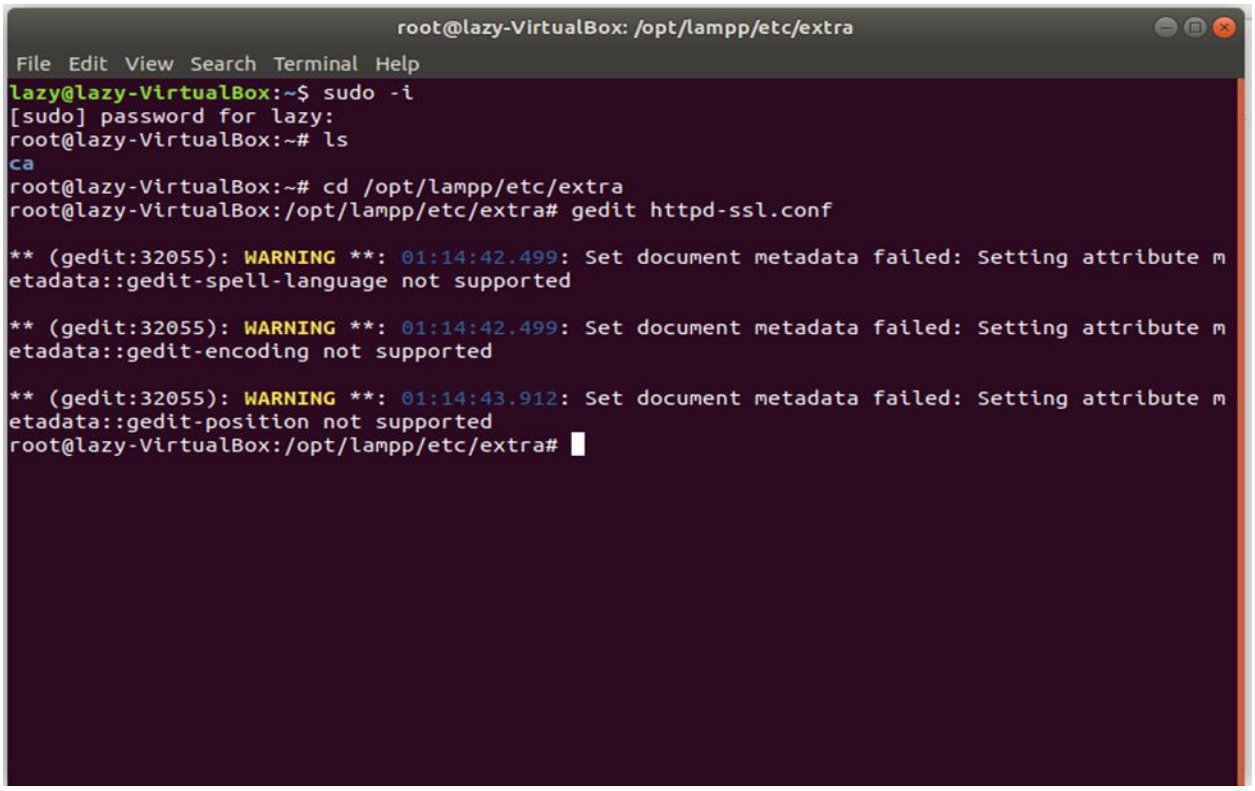

opt
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
bin
boot
cdrom
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
initrd.img
initrd.img.old
swapfile
vmlinuz
"opt" selected (containing 2 items)


opt
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
google
lampp


opt
lampp
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
apache2
bin
build
cgi-bin
docs
error
etc
htdocs
icons
img
include
info
lib
lib64
libexec
licenses
logs
man
manual
modules
mysql
pear
php
phpmyadmin
proftpd
sbin
share
temp
var
ctlscript.sh
lampp
manager-linux-x64.run
properties.ini
README.md
README-wsrep
RELEASENOTES
THIRDPARTY
uninstall
uninstall.dat
xampp
"etc" selected (containing 21 items)


opt
lampp
etc
extra
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
extra
openldap
original
ssl.crt
ssl.key
xampp
freetds.conf
httpd.conf
httpd.conf.bak
locales.conf
magic
mime.types
my.cnf
openssl.cnf
pear.conf
php.ini
php.ini-pre1.7.2
pool.conf
proftpd.conf
webalizer.conf
webalizer.conf.sample
"extra" selected (containing 13 items)


opt
lampp
etc
extra
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
httpd-autoindex.conf
httpd-dav.conf
httpd-default.conf
httpd-info.conf
httpd-languages.conf
httpd-manual.conf
httpd-mpm.conf
httpd-multilang-errordoc.conf
httpd-ssl.conf
httpd-userdir.conf
httpd-vhosts.conf
httpd-xampp.conf
proxy-html.conf



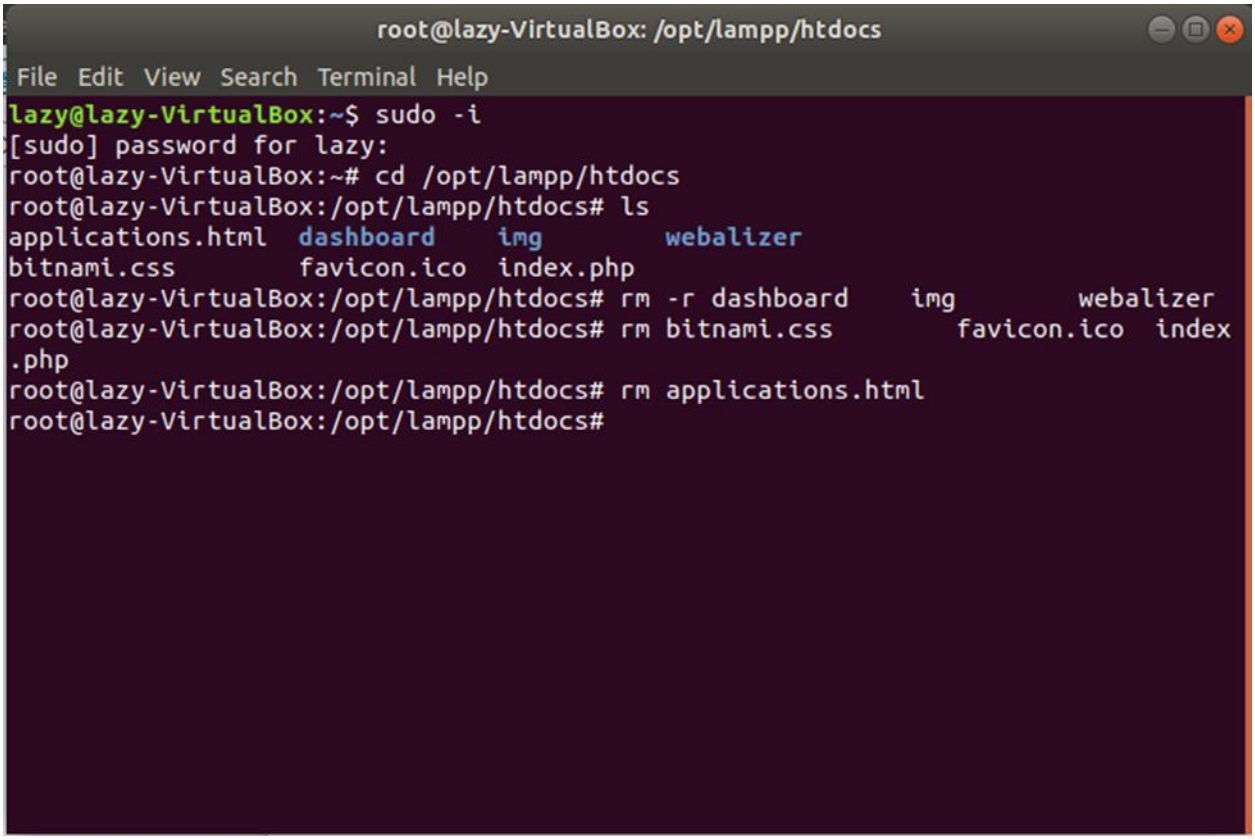
Editing the httpd-ssl.conf file

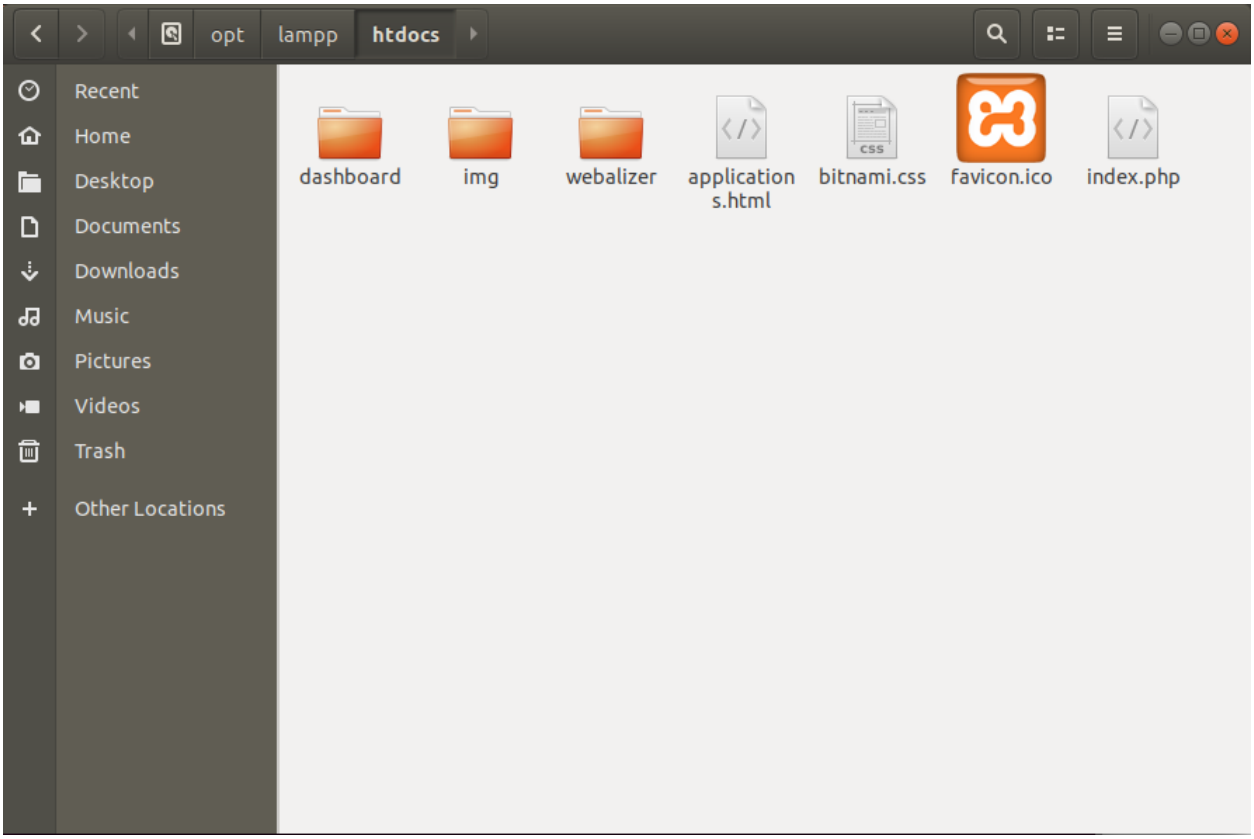
```
#   Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
#   require an ECC certificate which can also be configured in
#   parallel. Below is line 106
SSLCertificateFile "/home/group5/certificate/server.crt"
#SSLCertificateFile "/opt/lampp/etc/server-dsa.crt"
#SSLCertificateFile "/opt/lampp/etc/server-ecc.crt"

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
```

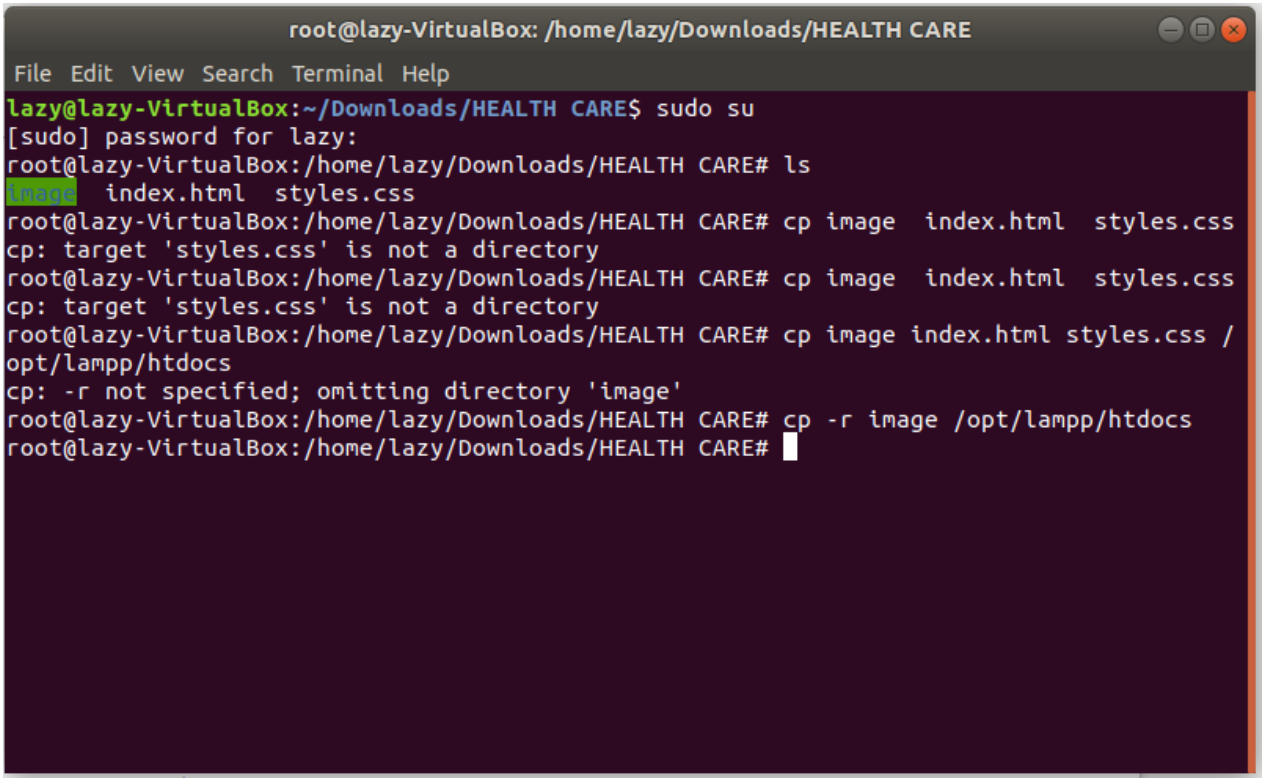
```
#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#   ECC keys, when in use, can also be configured in parallel  below is line 116
SSLCertificateKeyFile "/home/group5/certificate/server.key"
#SSLCertificateKeyFile "/opt/lampp/etc/server-dsa.key"
#SSLCertificateKeyFile "/opt/lampp/etc/server-ecc.key"
```

```
#SSLCertificateChainFile "/opt/lampp/etc/server-ca.crt"

#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#   Note: Inside SSLCACertificatePath you need hash symlinks
#         to point to the certificate files. Use the provided
#         Makefile to update the hash symlinks after changes.Below is line 136
SSLCACertificatePath "/home/group5/certificate"
#SSLCACertificateFile "/opt/lampp/etc/ssl.crt/ca-bundle.crt"

#   Certificate Revocation Lists (CRL):
#   Set the CA revocation path where to find CA CRLs for client
#   authentication or alternatively one huge file containing all
#   of them (file must be PEM encoded).
```

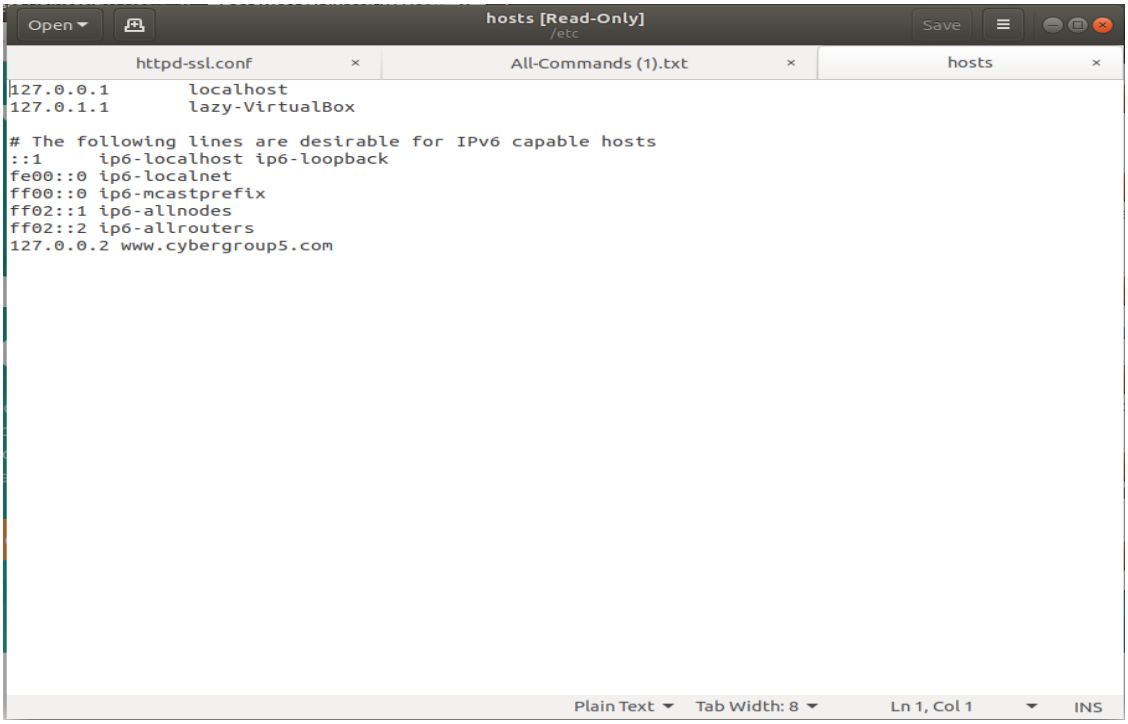
Here, Other files in ST Dogs have been deleted here and html ,CSS ,image files have been added.

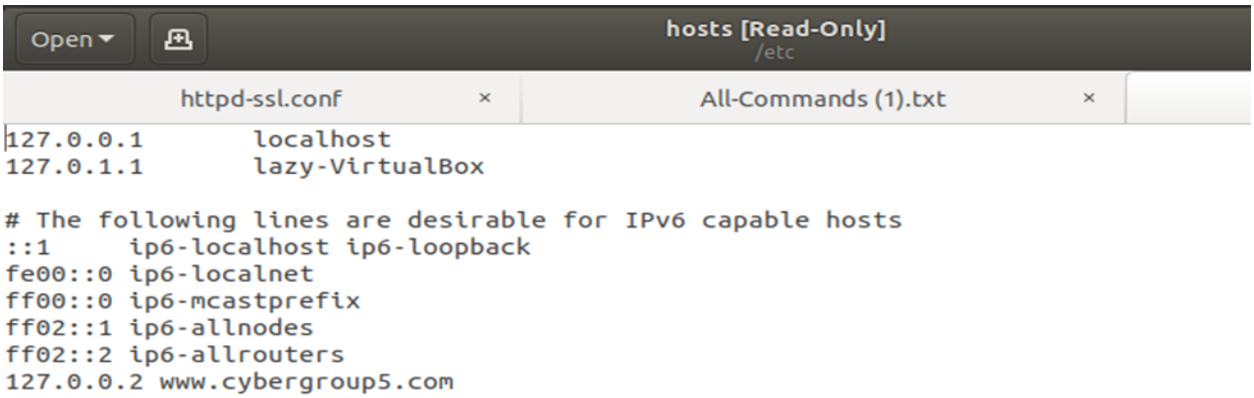



opt
lampp
htdocs
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
dashboard
img
webalizer
applications.html
bitnami.css
favicon.ico
index.php

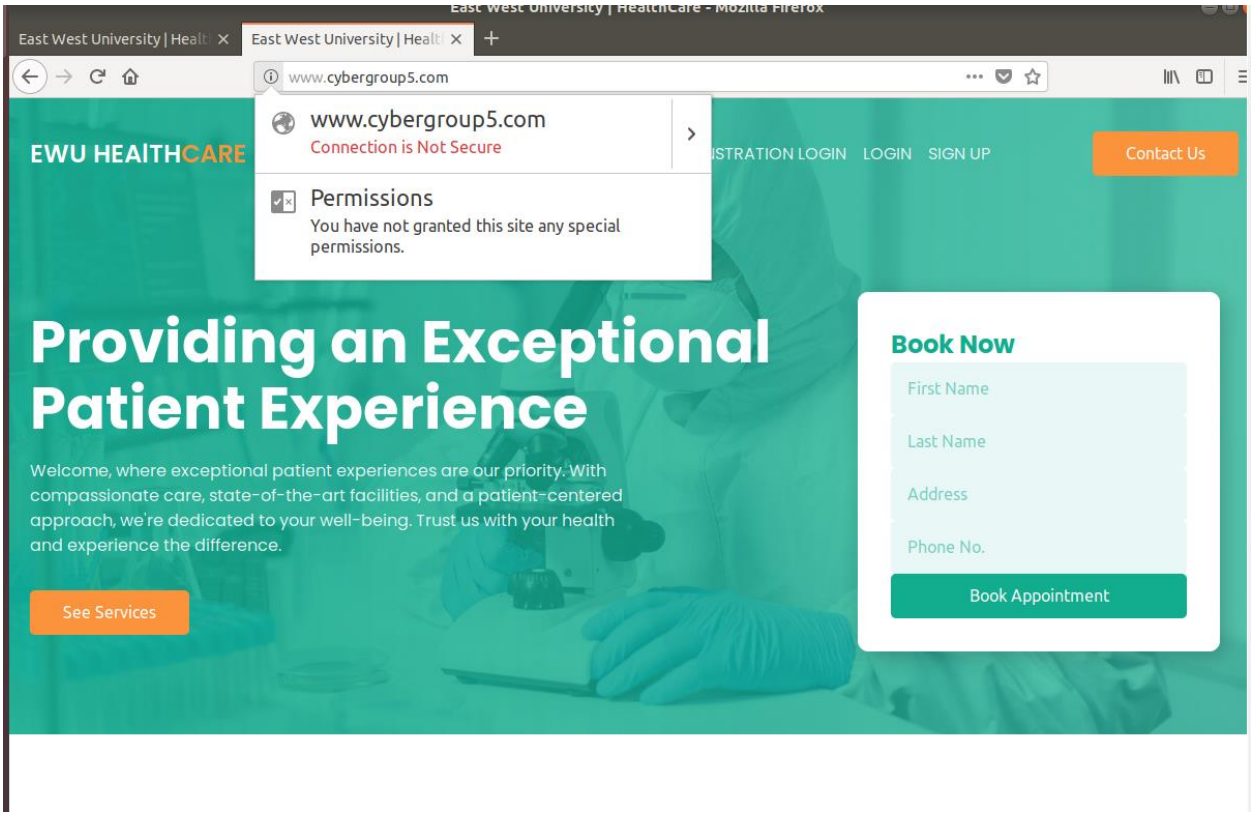

root@lazy-VirtualBox: /home/lazy/Downloads/HEALTH CARE
File Edit View Search Terminal Help
lazy@lazy-VirtualBox:~/Downloads/HEALTH CARE$ sudo su
[sudo] password for lazy:
root@lazy-VirtualBox:/home/lazy/Downloads/HEALTH CARE# ls
image index.html styles.css
root@lazy-VirtualBox:/home/lazy/Downloads/HEALTH CARE# cp image index.html styles.css
cp: target 'styles.css' is not a directory
root@lazy-VirtualBox:/home/lazy/Downloads/HEALTH CARE# cp image index.html styles.css
cp: target 'styles.css' is not a directory
root@lazy-VirtualBox:/home/lazy/Downloads/HEALTH CARE# cp image index.html styles.css /
opt/lampp/htdocs
cp: -r not specified; omitting directory 'image'
root@lazy-VirtualBox:/home/lazy/Downloads/HEALTH CARE# cp -r image /opt/lampp/htdocs
root@lazy-VirtualBox:/home/lazy/Downloads/HEALTH CARE#

This file is in read-only mode and has been modified for editing.

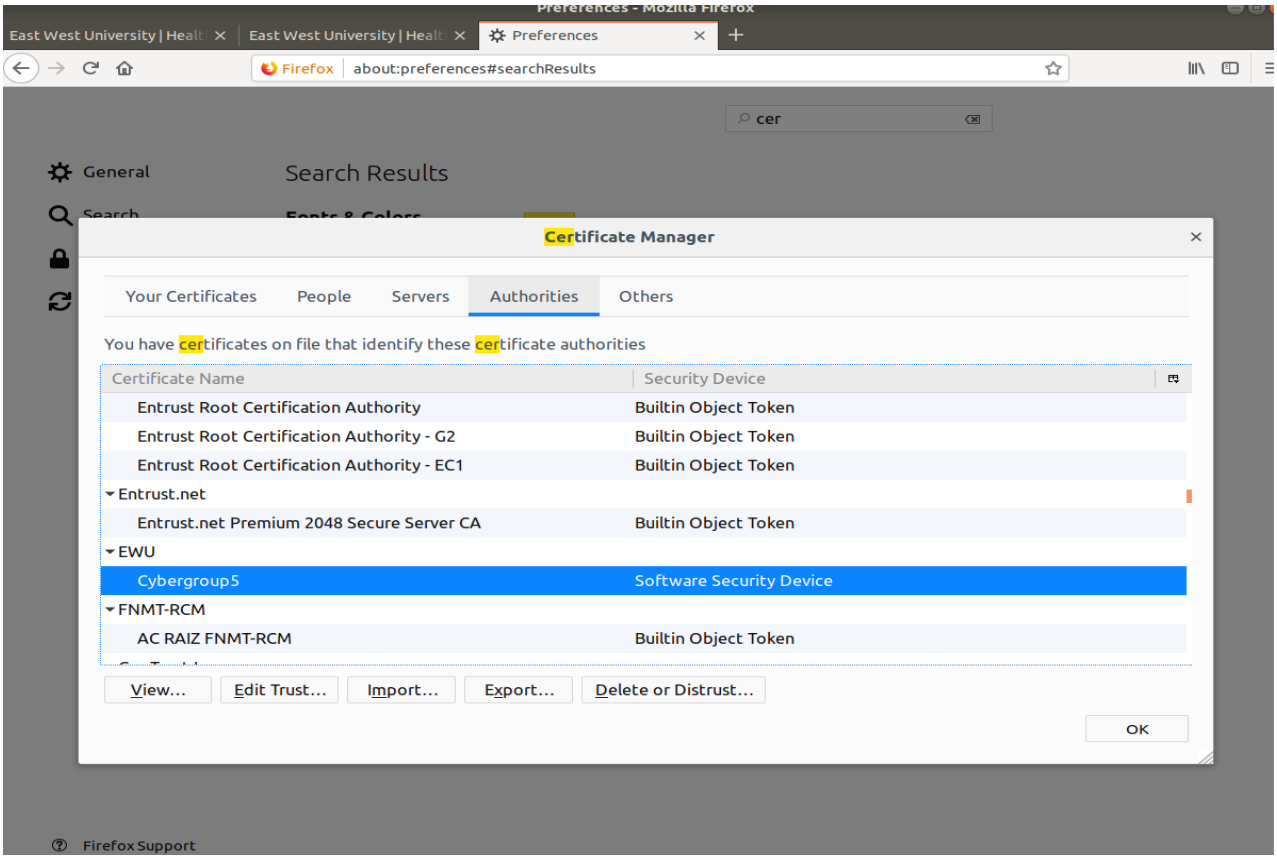


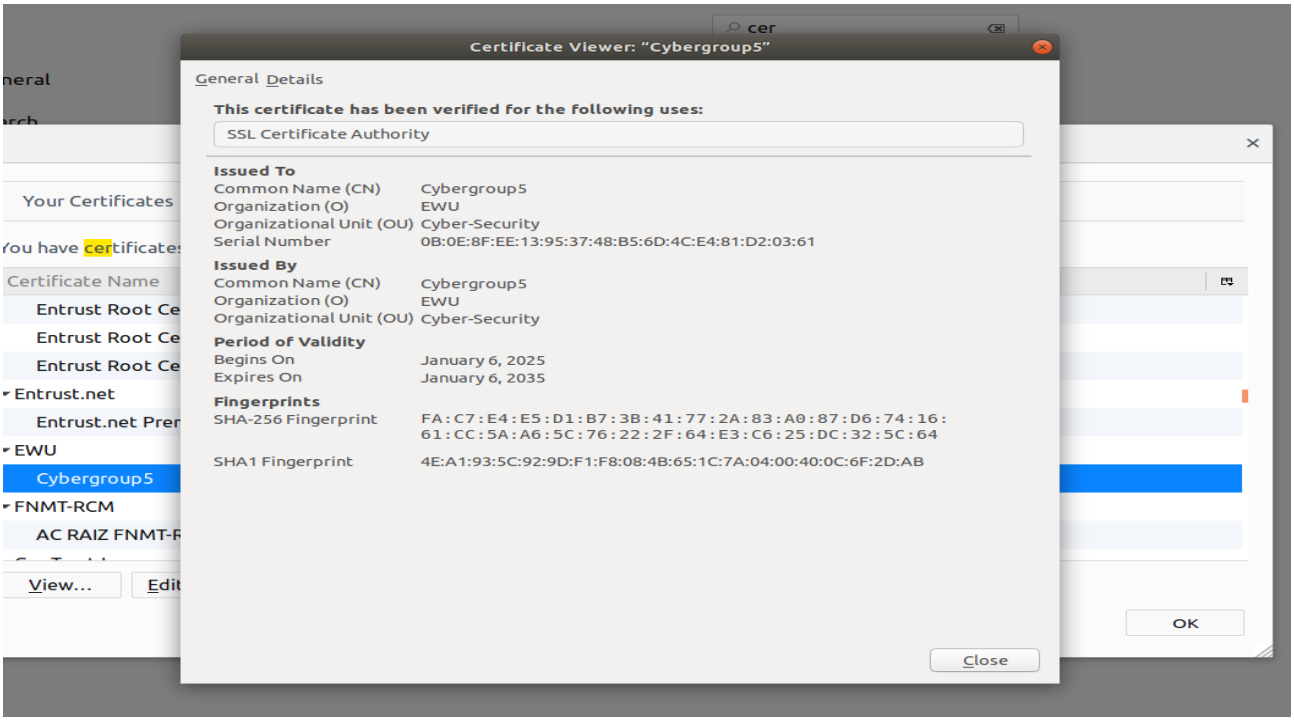


Primarily, www.verysecureserver.com is not secure Before inserting all the certificates

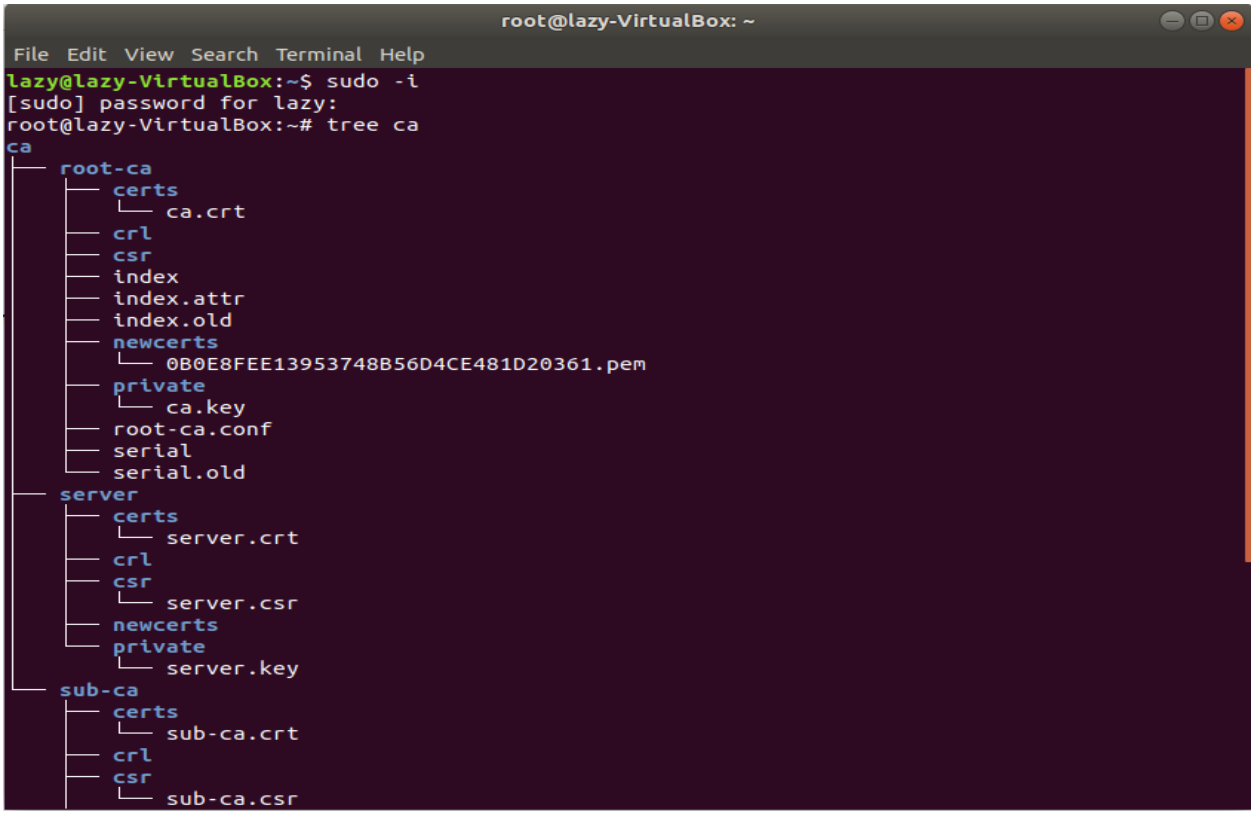


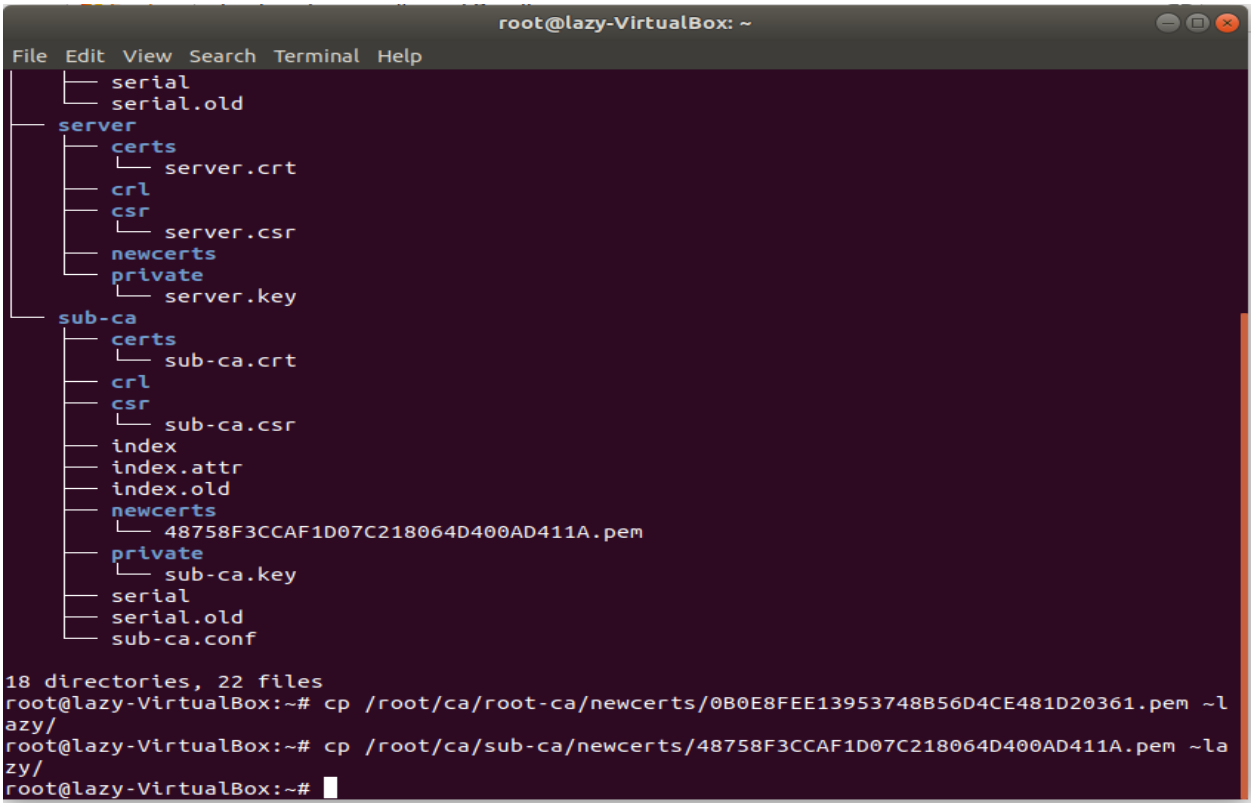
#Importing all necessary certificates



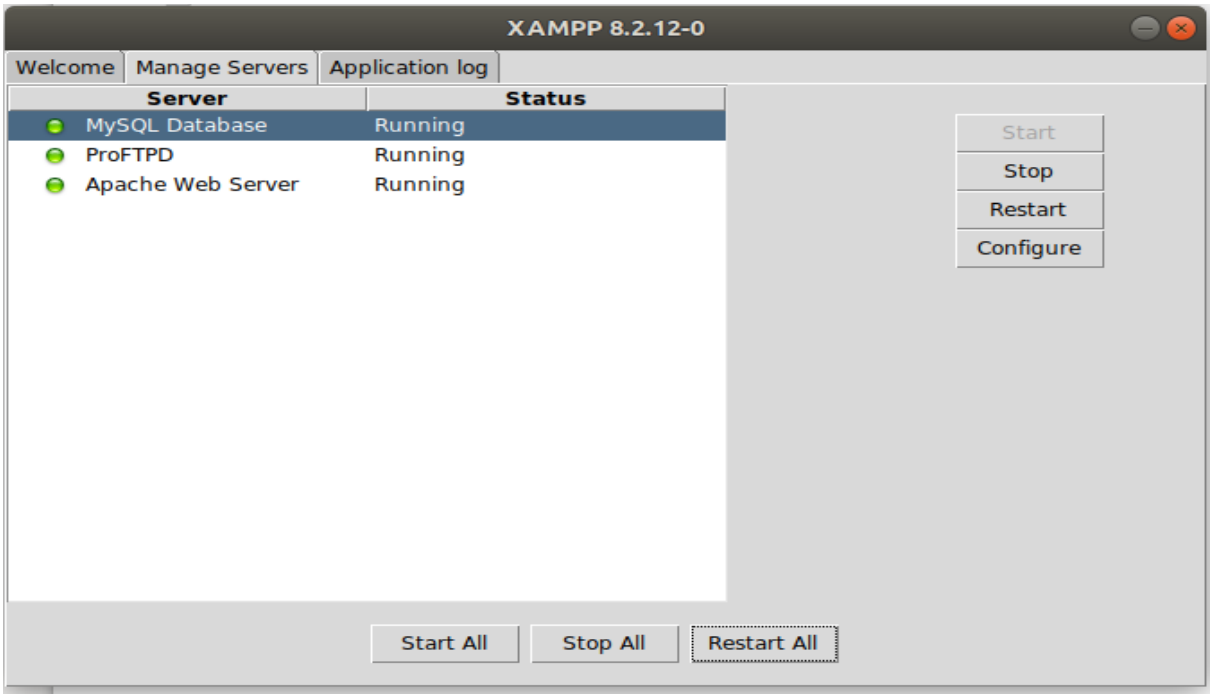


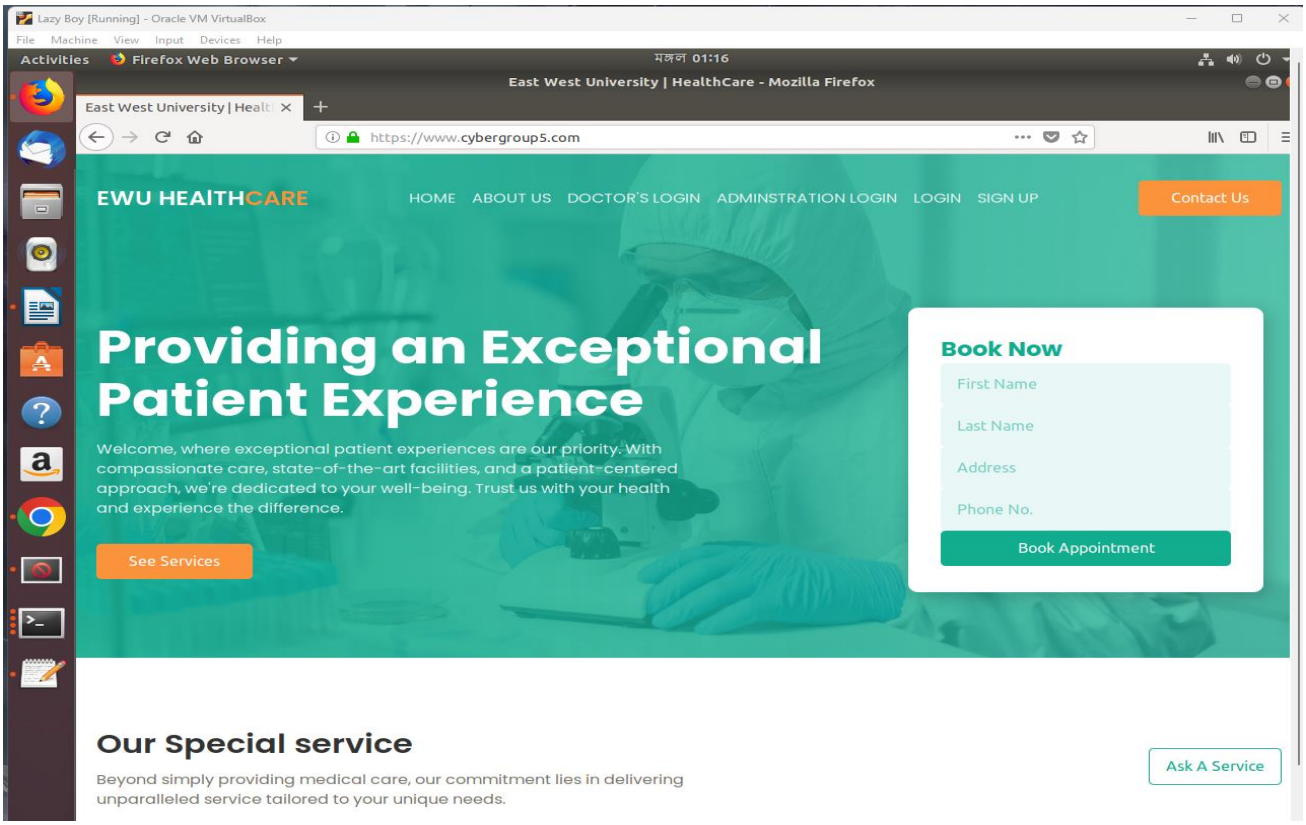
Later, two pem files are placed in a folder called certificates.



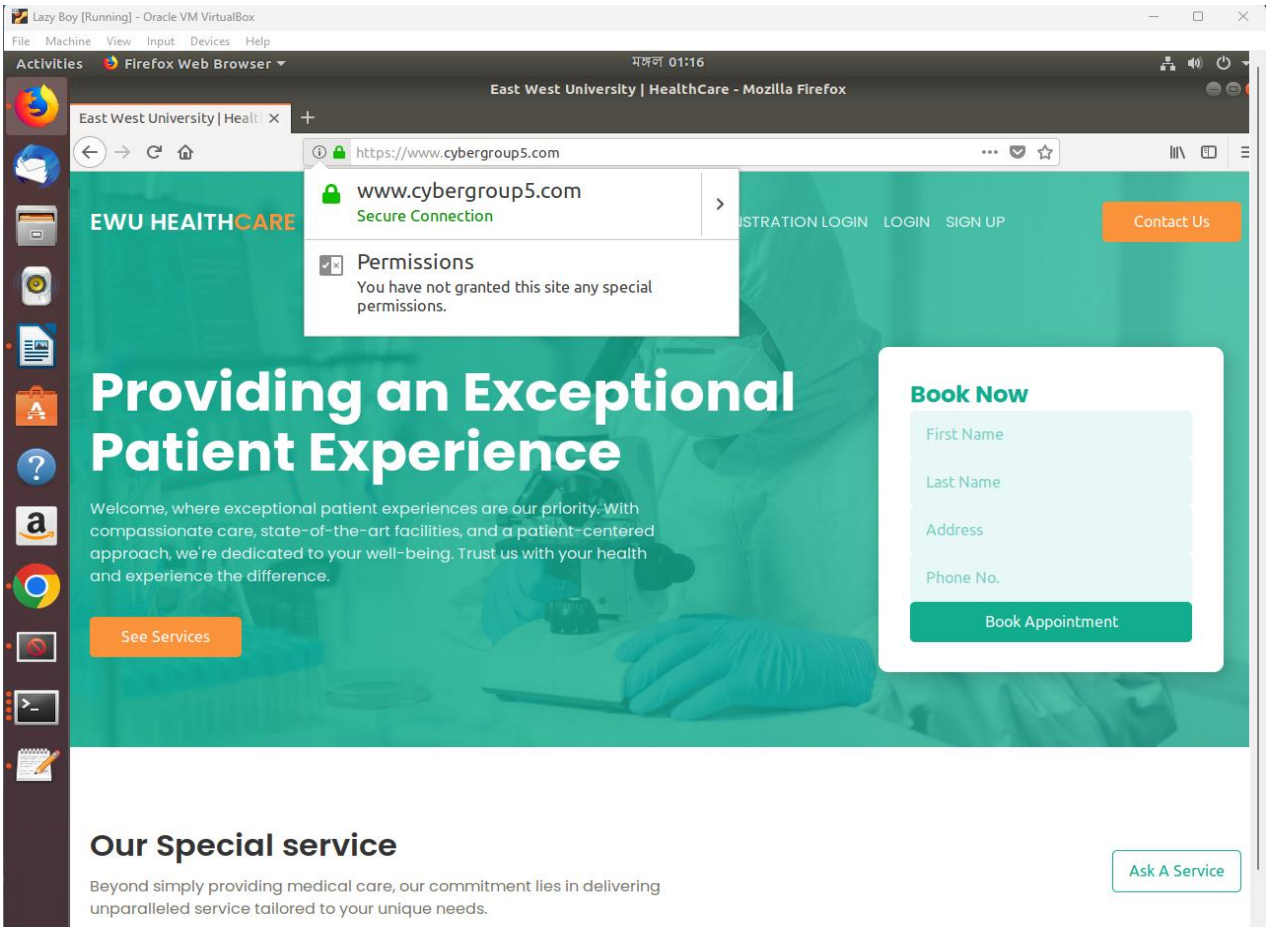


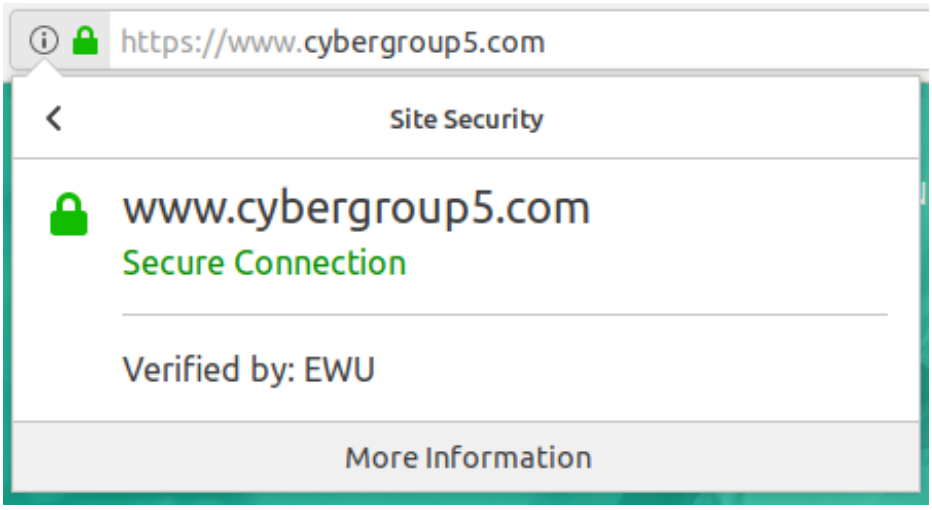
The website was run by restarting the xampp file again.





Finally, we were able to secure our website and bring the lock.





Conclusion:

The protocols TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are used to create encrypted and authorized connections between computers connected to a network. Our task involved using Public Key Infrastructure to implement Transport Layer Security (TLS) on HTTP for https:// connections in order to secure a networked system in this case (https://www.verysecureserver.com) At last, a secure website with a certificate from a reliable issuer has been achieved. We have utilized RSA for our public key. The SHA-256 hash value is displayed in the certificate. Lastly, it is demonstrated that a secured website has been created.