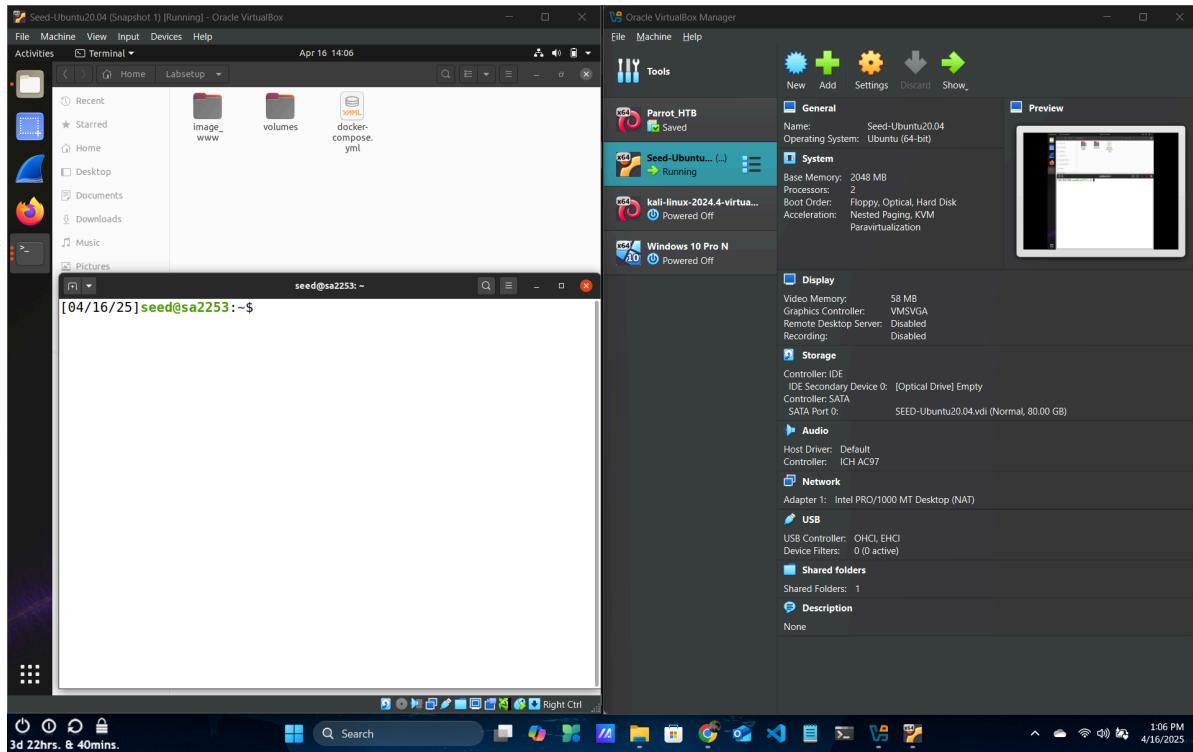


# CSCE 4050/5050 - Project 2 “Public-Key Infrastructure (PKI) Lab”

Group 21: Shajith Vignesh Ananthaneni(11691714) & Taha Al Obaidi(11502216)

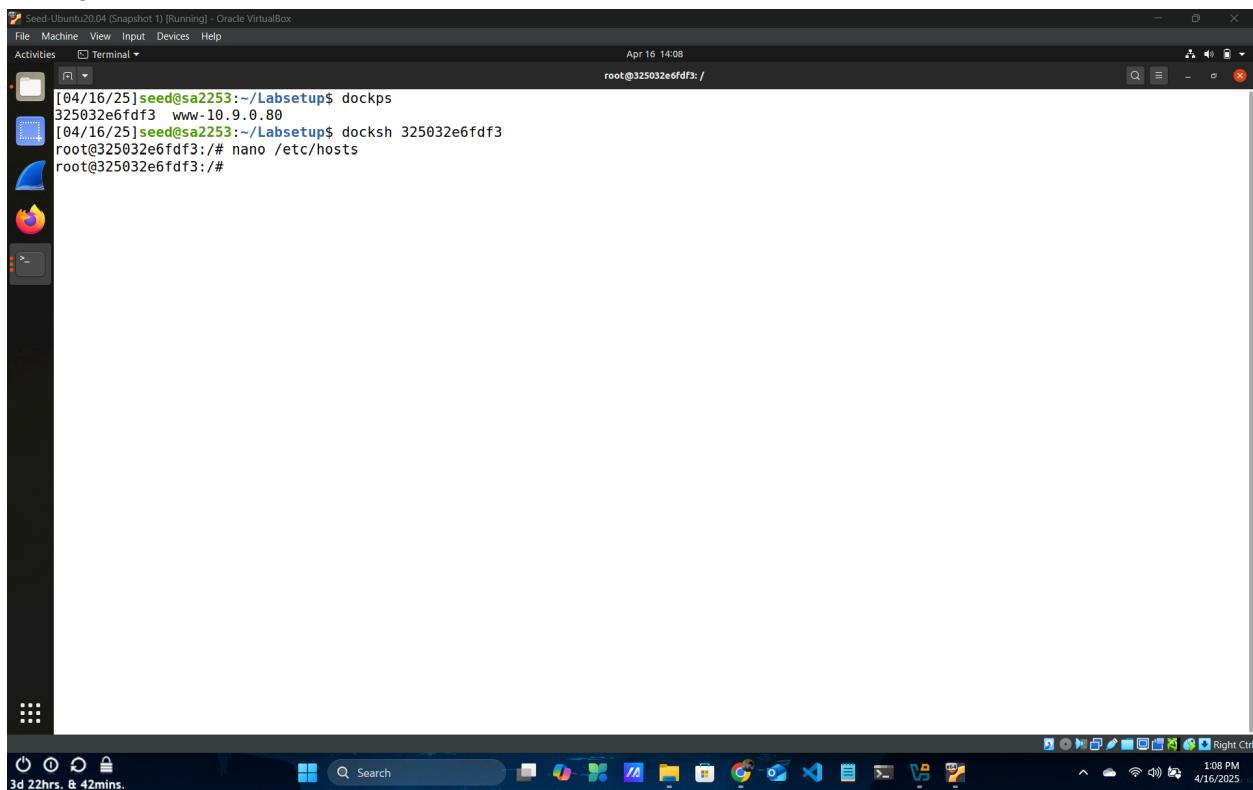
## Lab Setup:



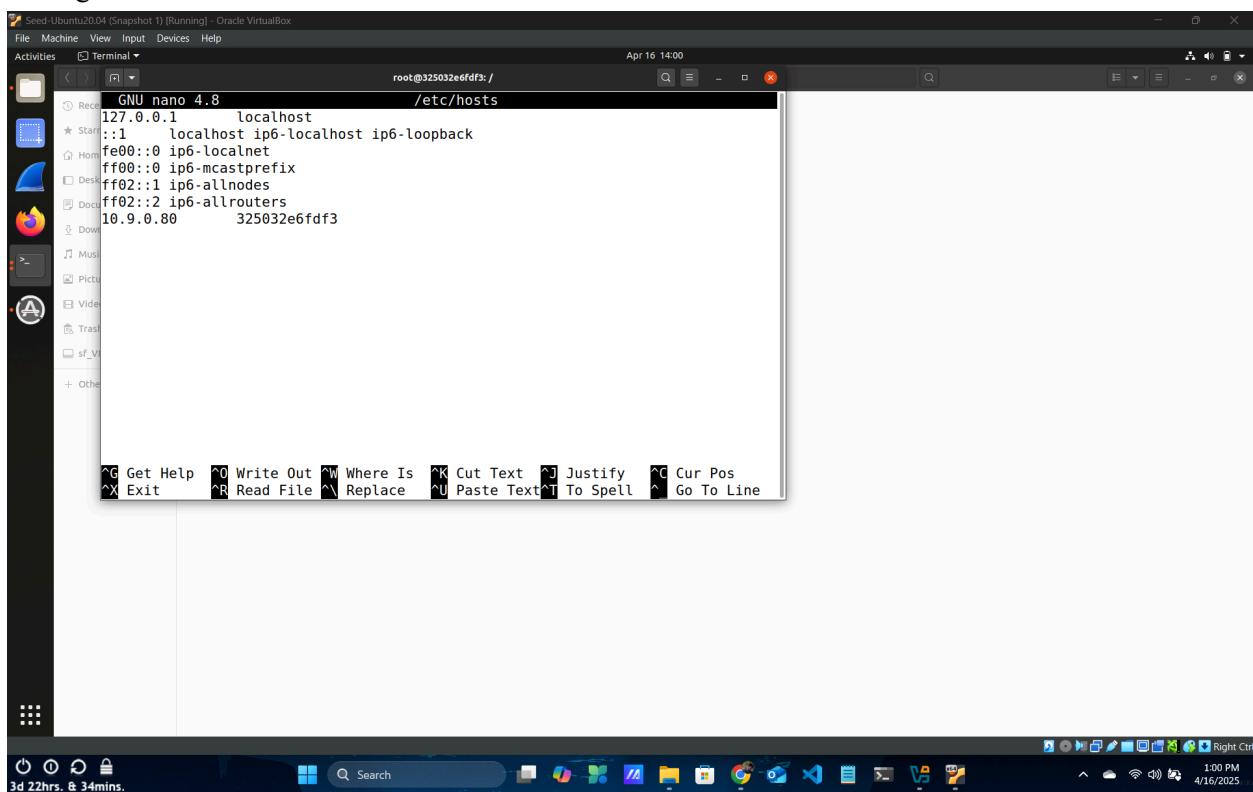
## Building & starting the Docker container

A screenshot of a terminal window within Oracle VM VirtualBox. The terminal output shows the execution of docker-compose commands. It starts with "Building web-server", followed by several "Step 1/7" through "Step 7/7" steps, each involving Docker build operations. After the builds, it shows "Successfully built efc31f2ddd87" and "Successfully tagged seed-image-www-pki:latest". Finally, it runs "docker-compose up", which creates a network, creates a container, and attaches to it. The terminal window is titled "Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox". The host desktop at the bottom has a taskbar with various icons.

## Getting into the shell



## Adding server names



Seed:Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Activities Terminal Apr 16 14:01

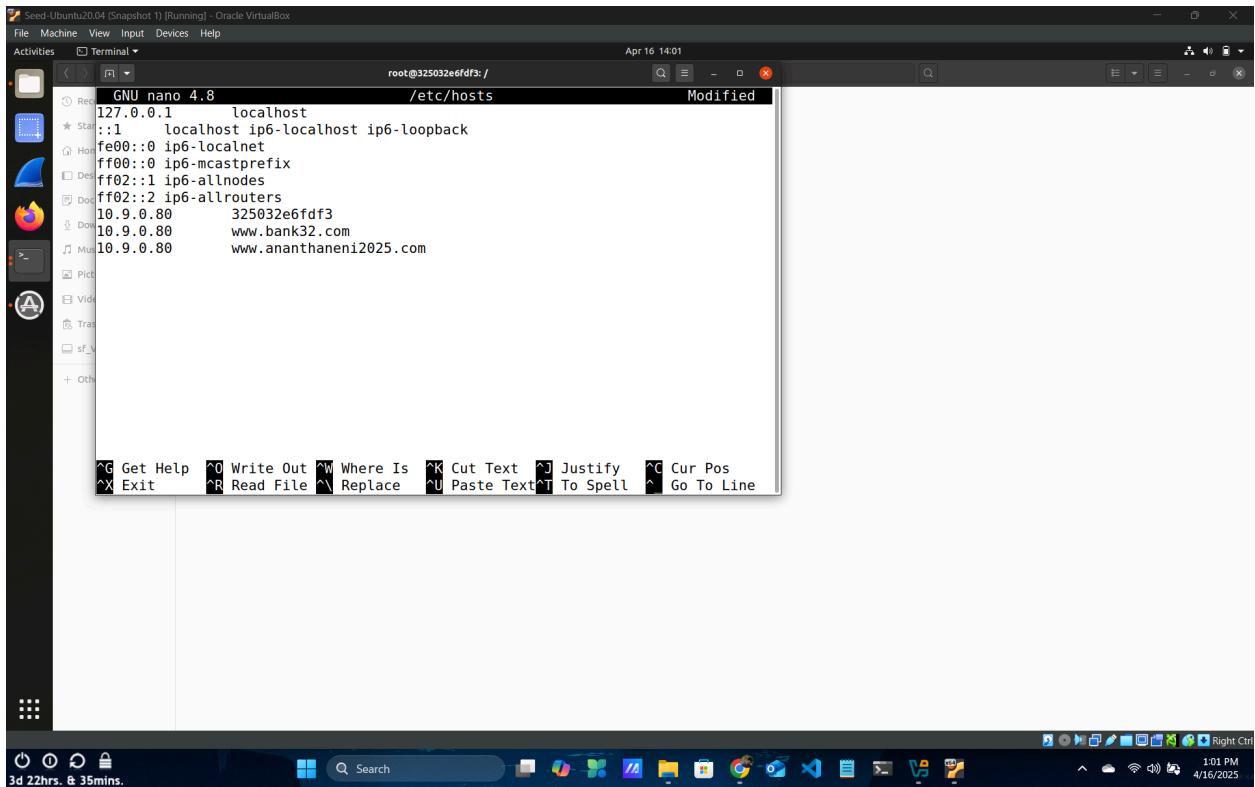
GNU nano 4.8 /etc/hosts Modified

```
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.9.0.80 325032e6fdf3
10.9.0.80 www.bank32.com
10.9.0.80 www.ananthaneni2025.com
```

Get Help Write Out Where Is Cut Text Justify Cur Pos  
Exit Read File Replace Paste Text To Spell Go To Line

10:1 PM 4/16/2025

3d 22hrs. & 35mins.



## Task 1: Becoming a Certificate Authority (CA)

Seed:Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox

File Machine View Input Devices Help

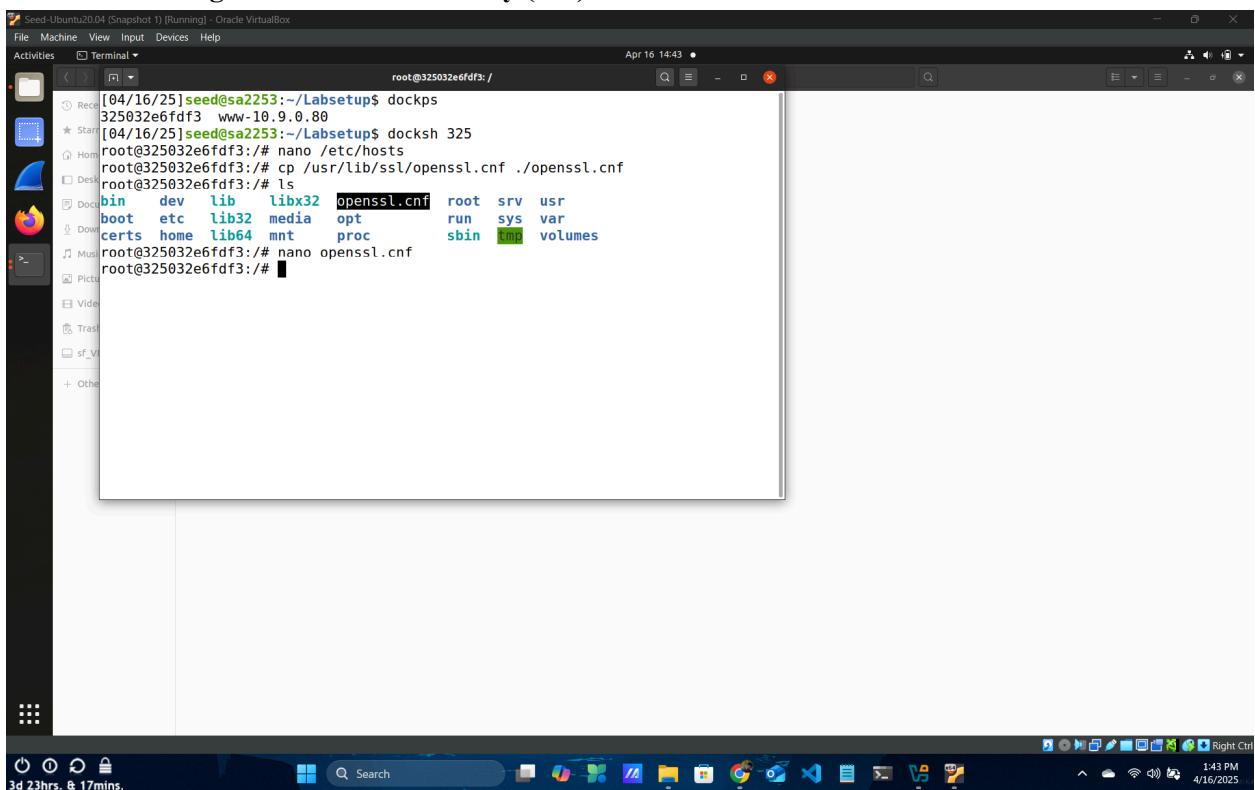
Activities Terminal Apr 16 14:43 •

root@325032e6fdf3:/

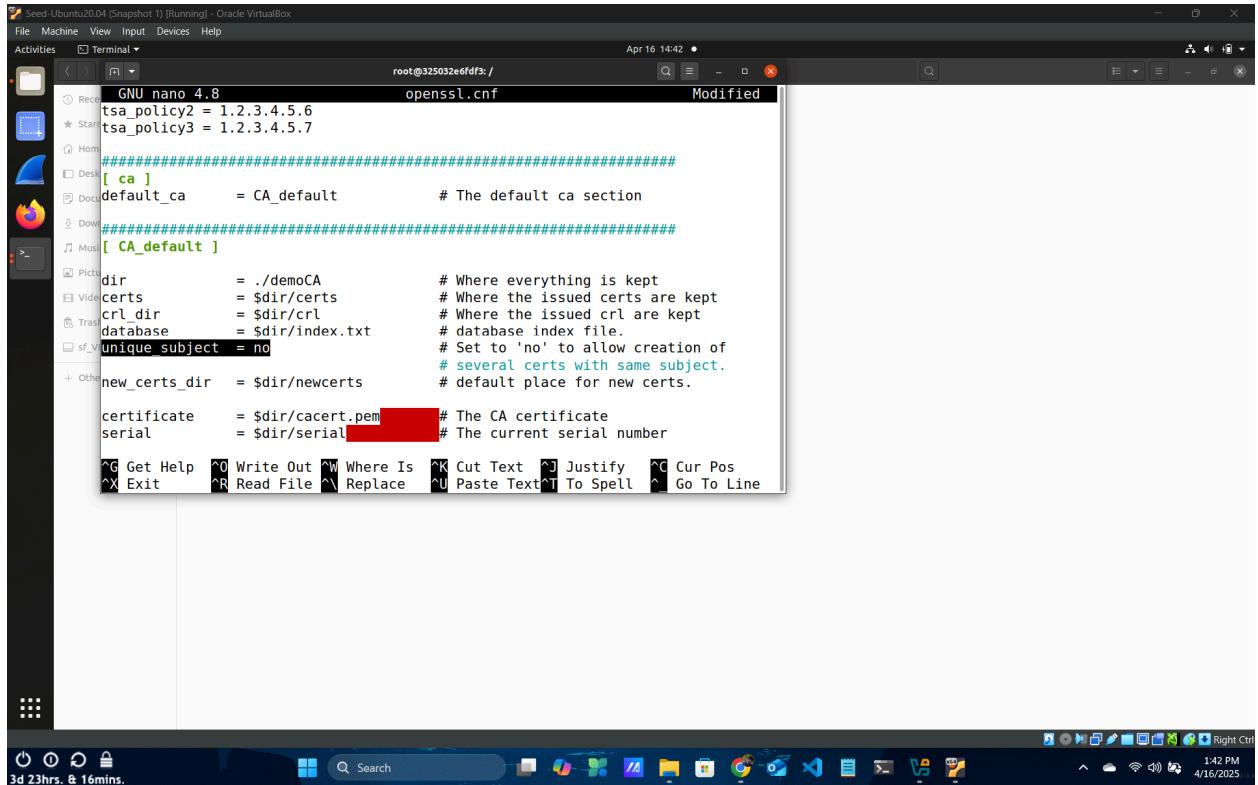
```
[04/16/25]seed@sa2253:~/Labsetup$ dockps
325032e6fdf3 www-10.9.0.80
[04/16/25]seed@sa2253:~/Labsetup$ docksh 325
root@325032e6fdf3:/# nano /etc/hosts
root@325032e6fdf3:/# cp /usr/lib/ssl/openssl.cnf ./openssl.cnf
root@325032e6fdf3:/# ls
bin dev lib libx32 openssl.cnf root srv usr
boot etc lib32 media opt run sys var
certs home lib64 mnt proc sbin tmp volumes
root@325032e6fdf3:/# nano openssl.cnf
root@325032e6fdf3:/#
```

1:43 PM 4/16/2025

3d 23hrs. & 17mins.



## Allowing the creation of certifications with the same subject



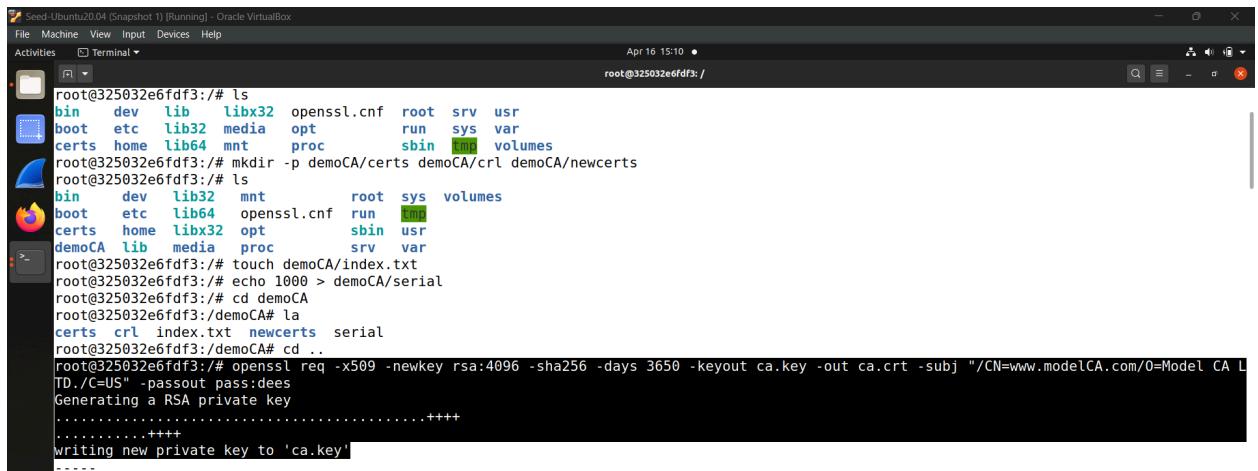
```
root@325032e6fdf3:/home/seed/Desktop/demoCA/openssl.cnf Modified
[ ca ]
default_ca = CA_default      # The default ca section

[ CA_default ]
dir           = ./demoCA          # Where everything is kept
certs         = $dir/certs        # Where the issued certs are kept
crl_dir       = $dir/crl          # Where the issued crl are kept
database     = $dir/index.txt    # database index file.
unique_subject = no             # Set to 'no' to allow creation of
                                # several certs with same subject.
new_certs_dir = $dir/newcerts   # default place for new certs.

certificate  = $dir/cacert.pem   # The CA certificate
serial        = $dir/serial        # The current serial number

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit  ^R Read File  ^V Replace  ^U Paste Text  ^T To Spell  ^L Go To Line
```

## Generating the self-signed certificate for the CA



```
root@325032e6fdf3:/# ls
bin  dev  lib  libx32  openssl.cnf  root  srv  usr
boot etc  lib32 media opt  run  sys  var
certs home lib64 mnt  proc  sbin  tmp  volumes
root@325032e6fdf3:/# mkdir -p demoCA/certs demoCA/crl demoCA/newcerts
root@325032e6fdf3:/# ls
bin  dev  lib32  mnt  root  sys  volumes
boot etc  lib64  openssl.cnf  run  tmp
certs home libx32  opt  sbin  usr
demoCA lib  media  proc  srv  var
root@325032e6fdf3:/# touch demoCA/index.txt
root@325032e6fdf3:/# echo 1000 > demoCA/serial
root@325032e6fdf3:/# cd demoCA
root@325032e6fdf3:/demoCA# la
certs  crl  index.txt  newcerts  serial
root@325032e6fdf3:/demoCA# cd ..
root@325032e6fdf3:/# openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -keyout ca.key -out ca.crt -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" -passout pass:does
Generating a RSA private key
.....+
.....+
writing new private key to 'ca.key'
```

### What part of the certificate indicates this is a CA's certificate?

The CA:TRUE flag under X509v3 Basic Constraints of ca.crt indicates that this certificate belongs to a Certificate Authority (CA)

### What part of the certificate indicates this is a self-signed certificate?

Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US

Subject: CN = www.modelCA.com, O = Model CA LTD., C = US

Since the Issuer and Subject are the same on ca.crt, this certificate is self-signed, i.e., it was signed by the entity that created it

**In the RSA algorithm, we have a public exponent e, a private exponent d, a modulus n, and two secret numbers p and q, such that  $n = pq$ . Please identify the values for these elements in your certificate and key files.**

These values are as follows:

Public exponent e [present in ca.key] = **65537**

Private exponent d [present in ca.key] =

```
00:a9:a1:02:41:fd:d7:7e:ce:d9:8b:e0:25:4c:53:ec:a8:62:dd:c3:35:9b:e7:40:4d:6a:a0:26:a3:04:05:46:1f:d4:c3:73:d9:58:c2:9d:83:c2:8f:71:e7:41:eb:27:89:7a:52:d8:bb:d7:01:a7:3c:66:bc:7a:2d:f6:e0:e1:dc:06:33:fd:e9:22:e9:21:21:03:d0:d4:8c:84:7f:7c:88:8b:c1:7e:63:44:e6:53:2f:e5:25:f9:40:fc:b7:3a:64:ce:dc:da:9c:23:c b:4e:78:11:46:5a:2c:df:26:e9:4b:fd:1b:eb:12:43:84:d9:1b:ab:85:38:41:3a:60:18:83:2d:52:b0:6f:55:45:93:a 7:b4:de:88:c2:75:40:1c:0d:b4:31:c1:e9:36:cd:83:de:e0:33:fa:8d:1c:e0:83:a3:76:02:c7:fc:50:1a:64:eb:81:5 6:f5:29:b6:8b:b2:42:67:dd:50:59:54:d9:b1:a2:d7:43:43:f4:f7:a2:2d:63:72:84:a9:3b:57:b8:2e:0f:95:a8:aa:8 b:52:8a:a2:9c:4a:c7:79:92:28:a7:98:0e:f1:fb:4e:ae:0d:63:5d:a3:24:27:07:99:9b:83:dd:ce:f3:b2:77:70:87:4f :ec:d2:09:c4:20:8c:15:a5:34:6e:7b:37:bb:08:50:c5:76:5e:5b:14:88:f2:bd:72:3b:53:74:27:5c:c0:08:c3:19:9 3:6d:30:d3:0e:a0:94:2c:fe:ea:d4:28:18:6e:e4:94:2e:ee:ee:a3:16:13:eb:9f:22:c3:2c:0f:63:20:a1:e8:6c:20:26 :50:96:d8:0a:3b:6e:62:d2:9b:df:4f:67:2e:14:c8:28:eb:63:1e:2d:47:76:1d:59:ef:b5:b2:ba:bb:31:3a:a1:64:98 :65:e9:e8:27:6a:ff:2d:3e:de:74:7f:30:ab:b3:69:58:3e:5e:a7:df:d7:86:64:b0:ad:9c:97:d8:82:89:bc:47:aa:97: 6a:63:9d:a6:00:0a:cc:3a:34:f2:04:dc:3c:49:df:74:ca:34:a7:f9:82:06:c7:61:43:ff:d7:53:53:1c:dc:78:fe:9e:dd :25:7f:6c:de:b2:eb:2f:65:cf:3d:81:54:58:1b:64:42:02:c5:60:f7:5f:47:04:2c:10:cc:2a:12:84:27:78:58:c5:75: 6c:50:bc:1e:d4:29:91:f6:71:af:1e:87:7e:03:8c:38:1e:ca:0c:25:d1:39:d9:3a:35:b4:7b:40:cb:e5:65:37:7f:9d: 01:e9:c6:8b:df:b9:d6:12:55:fe:c8:85:63:4e:98:f6:30:87:f0:56:3c:95:88:94:25:3f:83:3d:3f:0a:74:92:fd:6d:4 9
```

Modulus n [present in both ca.crt & ca.key] =

```
00:da:ba:fa:99:b7:62:b6:13:45:de:d0:be:a8:a6:bf:07:dc:35:66:c8:e0:77:e6:31:bf:bf:4a:d9:5a:f1:49:b8:70:b 8:d6:3b:ab:8a:8d:18:64:df:f6:71:8a:6b:bf:16:75:73:ad:72:e5:2d:0e:64:03:2a:e7:60:7a:16:a3:b6:ae:ee:6a:b 2:76:10:ea:01:2e:f2:b5:a0:84:11:3b:3a:9d:a2:7e:f1:8e:3e:ab:60:55:0d:62:92:5f:35:59:ef:12:82:45:81:08:3 6:5e:99:88:81:c4:87:d2:48:b9:92:dc:d8:d9:62:10:f3:1f:b3:23:e4:6f:df:21:e6:60:73:eb:0e:51:93:dd:d5:95:7 f:11:7b:f8:9c:60:18:bf:6e:5f:e8:e6:be:b0:b2:a4:4b:98:12:b5:f7:de:19:8f:4d:f1:b2:4a:73:65:47:c4:07:bf:7f:f 9:8e:60:57:b9:ff:6f:bd:f5:15:51:2f:4b:37:f5:98:25:3b:df:18:3f:69:9e:3c:07:45:f6:51:12:9c:31:4d:67:26:83: 33:63:1b:02:80:8d:a5:46:d2:8e:43:c1:a7:95:f3:37:7a:7a:28:40:f7:78:a6:e0:b9:29:ac:a0:7b:85:37:36:91:22: 37:25:97:55:c1:0f:5a:99:54:da:d0:4e:93:63:76:5e:20:2b:52:ee:10:ce:c9:7d:f9:ba:6f:8f:a5:4e:00:2c:3b:b8:d 7:7b:8c:d0:6a:f3:f0:53:bc:24:22:b9:fa:64:43:ce:cd:9a:0c:b3:07:ef:7a:0b:da:00:1f:1d:7a:b4:f6:71:49:b7:ad: 73:cc:33:3d:87:b7:0a:11:de:97:aa:22:26:8d:7b:6b:79:34:e9:89:f8:29:93:c8:8c:81:86:ef:e8:15:95:f4:a6:6b: 9d:0f:56:84:83:fd:ca:8a:d8:78:2a:f9:2c:e0:7b:84:18:a2:72:9e:64:a4:ad:a2:14:5e:7f:1c:b8:6e:fb:52:7d:e3:6 5:76:5f:d4:f8:e0:df:20:60:e6:26:cc:18:35:40:00:e5:5b:c4:fa:d0:65:3d:43:d4:33:2f:10:14:90:92:e2:fb:77 :44:05:22:b9:7a:4f:86:e7:e1:f3:e8:97:a8:a9:c1:91:05:86:24:b9:ec:c6:bf:18:c8:d4:a8:ab:a2:e0:9c:ca:c3:bd:f e:fa:fd:85:e6:9a:b8:7b:c0:16:eb:bc:bc:00:57:29:ee:b8:6b:73:ab:a9:69:af:ec:a3:e6:19:44:1a:6c:62:03:23:85 :49:6b:62:e9:5a:7c:38:2d:ad:60:1d:88:8a:39:f1:60:0a:a5:f8:6d:a2:b0:d0:44:b9:af:7c:59:c0:95:7f:7b
```

Two secret numbers [present in ca.key]

p =

00:f5:6f:18:d1:e5:b4:77:38:4e:1f:45:00:20:78:dc:bc:a6:06:d4:8e:3b:f9:bc:3e:0c:d5:1d:44:15:ac:5b:83:61:32:d9:ef:55:39:d2:4f:57:f4:8b:92:04:af:62:88:82:28:ce:f8:55:ae:b0:1b:5d:0e:e6:cf:09:e7:69:89:df:2e:88:4f:91:f4:28:c3:be:2c:be:d1:0b:a2:92:40:b1:73:38:2d:01:dd:7b:9a:b0:c0:4b:7c:15:bf:4b:88:e3:e1:7b:c8:05:70:a2:a6:e1:f3:4d:ae:fa:75:a6:0f:74:f1:f4:11:3b:1c:e1:d6:40:df:93:ea:a6:7f:d2:ee:b0:4c:11:56:56:50:c0:ce:19:a7:bf:33:ab:89:0a:7d:4e:68:a3:cf:59:38:7b:1f:53:74:27:6c:ba:a0:01:93:d9:03:b7:39:74:d6:c8:16:c9:c0:5f:59:82:96:b1:51:f2:d6:3b:0d:37:23:02:19:7b:9c:74:37:d0:d9:7a:03:2a:b7:1b:33:34:8c:30:9d:80:7e:4f:af:93:2b:4a:9d:f4:46:5b:ed:50:4c:74:65:a9:e9:d7:a2:c2:de:8c:e2:36:c9:e9:ed:8b:76:10:a4:2d:37:86:79:39:71:33:42:24:78:e5:00:85:83:fc:9e:6a:f3:ba:71:6e:95:d8:ad

q =

00:e4:25:95:9d:01:f8:34:d9:88:43:a7:8d:c0:f3:e1:07:98:35:f7:d8:27:bd:fa:15:ad:05:1f:65:79:73:6d:7c:a6:b1:dd:59:ab:05:ae:3e:11:69:81:30:12:06:43:6f:37:32:ff:70:2c:ae:7c:98:f5:de:c4:f7:40:39:40:da:16:f0:0a:21:e7:8b:07:62:6f:c2:df:41:05:08:20:b3:b7:a0:3a:c3:b2:43:9a:c0:9f:8c:47:a0:8f:06:d3:92:3a:0a:a2:cc:2c:85:d6:5d:ba:21:7d:a5:81:8b:30:08:38:16:50:2b:0b:8a:6e:50:f3:09:bd:6e:24:13:2e:74:32:ac:5c:a9:33:50:a2:b6:17:69:72:44:1c:bc:44:7f:f0:64:20:6b:61:9a:40:7e:49:14:7b:81:02:2b:fe:66:67:b0:d2:9d:d6:cc:c9:5e:19:4a:01:5f:df:59:31:d5:a3:5a:a9:d9:37:ff:55:5e:22:f1:87:54:7c:07:e4:e5:fc:28:ae:e2:60:8f:f9:d8:94:10:23:59:82:df:7e:c2:93:05:ae:9a:3b:d9:51:4e:fd:eb:d5:26:82:6b:7f:b6:38:42:8f:12:48:4d:4e:12:5f:4b:30:45:48:29:de:4d:9e:24:d6:31:21:99:2e:9d:0a:77:8f:37:d9:bf:75:c7

Used a simple Python program to convert these hexadecimal strings to integers, calculated & verified  $n = p \times q$

The screenshot shows a Python code editor with the following code:

```
Project 2 > hex to dec.py
```

```
main.py      hex to dec.py      Run      hex to dec
```

```
3
4     # Hex values extracted from the u
5     modulus_hex = "00:da:ba:fa:99:b7:
6     public_exponent = 65537 # Standard
7     private_exponent_hex = "00:a9:a1:
8     prime1_hex = "00:f5:f6:18:d1:e5:b
9     prime2_hex = "00:e4:25:95:9d:01:f
10
11    # Convert hex strings to integers
12    modulus = int(modulus_hex, 16)
13    private_exponent = int(private_exponent_hex, 16)
14    prime1 = int(prime1_hex, 16)
15    prime2 = int(prime2_hex, 16)
16
17    # Compute n from p and q to verify
18    n_from_pq = prime1 * prime2
19
20    print(modulus)
21    print("\n")
22    print(public_exponent)
23    print("\n")
24    print(private_exponent)
25    print("\n")
26    print(prime1)
27    print("\n")
28    print(prime2)
29    print("\n")
30    print(n_from_pq)
31    print("\n")
32    print(modulus == n_from_pq)
```

Output window:

```
True
```

Process finished with exit code 0

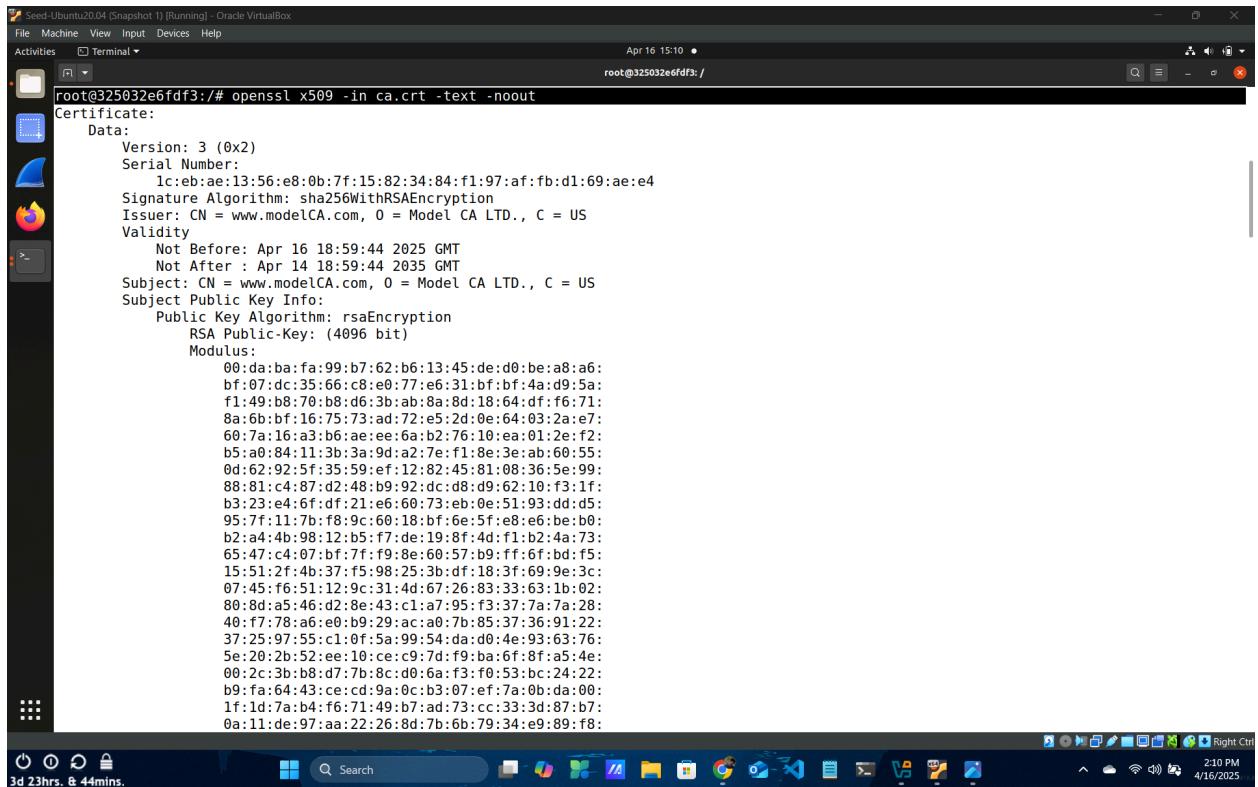
Bottom status bar:

```
32:8 (28 chars, 1 line break) CRLF UTF-8 4 spaces Python 3.11
```

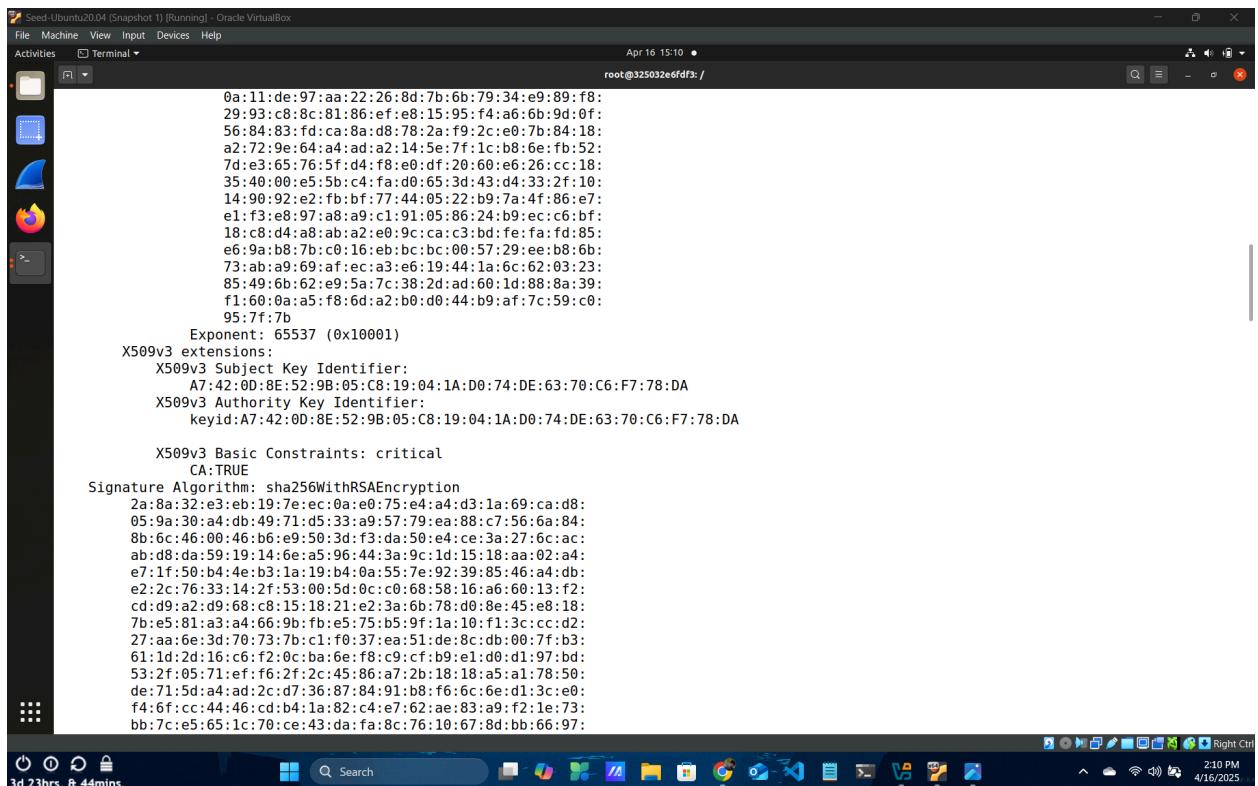
Bottom right corner:

```
4/16/2025
```

## Looking at the decoded content of the X509 certificate



```
Seed-Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:10 •
root@325032e6fdf3:/# openssl x509 -in ca.crt -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
    1c:eb:ae:13:56:e8:0b:7f:15:82:34:84:f1:97:af:fb:d1:69:ae:e4
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
Validity
    Not Before: Apr 16 18:59:44 2025 GMT
    Not After : Apr 14 18:59:44 2035 GMT
Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
            Modulus:
                00:da:ba:fa:99:b7:62:b6:13:45:de:d0:be:a8:a6:
                bf:07:dc:35:66:c8:e0:77:e6:31:bf:bf:4a:d9:5a:
                f1:49:b8:70:8d:63:ab:8a:8d:18:64:df:f6:71:
                8a:6b:bf:16:75:73:ad:72:e5:2d:0e:64:03:2a:e7:
                60:7a:16:a3:b6:ae:ee:6a:b2:76:10:ea:01:2e:f2:
                b5:a0:84:11:3b:3a:9d:a2:e1:8e:3e:ab:60:55:
                0d:62:92:5f:35:59:ef:12:82:45:81:08:36:5e:99:
                88:81:c4:87:d2:48:b9:92:dc:08:d9:62:10:f3:1f:
                b3:23:e4:6f:df:21:e6:60:73:eb:0e:51:93:dd:d5:
                95:7f:11:7b:f8:9c:60:18:bf:6e:5f:e8:e6:be:b0:
                b2:a4:4b:98:12:b5:f7:de:19:8f:4d:f1:b2:4a:73:
                65:47:c4:07:bf:7f:f9:8e:60:57:b9:ff:6f:bd:f5:
                15:51:2f:4b:37:f5:98:25:3b:df:18:3f:69:9e:3c:
                07:45:f6:51:12:9c:31:4d:67:26:83:33:63:1b:02:
                80:8d:a5:46:d2:8e:43:c1:a7:95:f3:37:7a:7a:28:
                40:f7:78:a6:e0:b9:29:ac:a0:7b:85:37:36:91:22:
                37:25:97:55:c1:0f:5a:99:54:da:d0:4e:93:63:76:
                5e:20:2b:52:ee:10:ce:c9:7d:f9:ba:6f:8f:a5:4e:
                00:2c:3b:b8:d7:7b:8c:d0:6a:f3:f0:53:bc:24:22:
                b9:fa:64:43:ce:cd:9a:0c:b3:07:ef:7a:0b:da:00:
                1f:1d:7a:b4:f6:71:49:b7:ad:73:cc:33:3d:87:b7:
                0a:11:de:97:aa:22:26:8d:7b:6b:79:34:e9:89:f8:
```



```
Seed-Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:10 •
root@325032e6fdf3:/#
0a:11:de:97:aa:22:26:8d:7b:6b:79:34:e9:89:f8:
29:93:c8:8c:81:86:ef:e8:15:95:f4:a6:6b:9d:0f:
56:84:83:fd:ca:8a:d8:78:2a:f9:2c:e0:7b:84:18:
a2:72:9e:64:a4:ad:a2:14:5e:7f:1c:b8:6e:fb:52:
7d:e3:65:76:5f:d4:f8:e0:df:20:60:e6:26:cc:18:
35:40:00:e5:5b:cd:fa:d0:65:3d:43:d4:33:2f:10:
14:90:92:e2:fb:bf:77:44:05:22:b9:7a:4f:86:7:
e1:f3:e8:97:8a:a9:c1:91:05:86:24:b9:ec:c6:bf:
18:c8:d4:a8:a2:e0:9c:ca:c3:bd:fe:fa:fd:85:
e6:9a:b8:7b:c0:16:eb:bc:bc:00:57:29:ee:68:6b:
73:ab:a9:69:af:ec:a3:e6:19:44:1a:6c:62:03:23:
85:49:6b:62:e9:5a:7c:38:2d:60:1d:88:8a:39:
f1:60:0a:a5:f8:6d:a2:b0:d0:44:b9:af:7c:59:c0:
95:7f:7b
Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Key Identifier:
        A7:42:0D:8E:52:9B:05:C8:19:04:1A:D0:74:DE:63:70:C6:F7:78:DA
    X509v3 Authority Key Identifier:
        keyid:A7:42:0D:8E:52:9B:05:C8:19:04:1A:D0:74:DE:63:70:C6:F7:78:DA
    X509v3 Basic Constraints: critical
        CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
2a:8a:32:e3:eb:19:7e:ec:0a:e0:75:4e:a4:d3:1a:69:ca:d8:
05:9a:30:a4:db:49:71:d5:33:a9:57:79:ea:88:c7:56:6a:84:
8b:6c:46:00:46:b6:e9:50:3d:f3:da:50:e4:ce:3a:27:6c:ac:
ab:08:da:59:19:14:6e:a5:96:44:3a:9c:1d:15:18:aa:02:a4:
e7:1f:50:b4:4e:b3:1a:19:b4:0a:55:7e:92:39:85:46:a4:db:
e2:2c:76:33:14:2f:53:00:5d:0c:c0:68:58:16:a6:60:13:f2:
cd:d9:a2:d9:68:c8:15:18:21:e2:3a:6b:78:d0:8e:45:e8:18:
7b:e5:81:a3:a4:66:9b:fb:e5:75:b5:9f:1a:10:f1:3c:cc:d2:
27:aa:6e:3d:70:73:7b:c1:f0:37:ea:51:de:8c:db:00:7f:b3:
61:1d:2d:16:c6:f2:0c:ba:6e:f8:c9:cf:b9:e1:d0:d1:97:bd:
53:2f:05:71:ef:f6:2f:2c:45:86:a7:2b:18:18:a5:a1:78:50:
de:71:5d:a4:ad:2c:d7:36:87:84:91:b8:f6:6c:6e:d1:3c:e0:
f4:6f:cc:44:46:cd:b4:1a:82:c4:e7:62:ae:83:a9:f2:1e:73:
bb:7c:e5:65:1c:70:ce:43:da:fa:8c:76:10:67:8d:bb:66:97:
```

```

Seed:Ubuntu:20.04 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:11 •
root@325032e6fdf3:/ 
X509v3 extensions:
    X509v3 Subject Key Identifier:
        A7:42:0D:8E:52:9B:05:C8:19:04:1A:D0:74:DE:63:70:C6:F7:78:DA
    X509v3 Authority Key Identifier:
        keyid:A7:42:0D:8E:52:9B:05:C8:19:04:1A:D0:74:DE:63:70:C6:F7:78:DA

    X509v3 Basic Constraints: critical
        CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
2a:8a:32:e3:eb:19:7e:ec:0a:e0:75:e4:a4:d3:1a:69:ca:d8:
05:9a:30:a4:db:49:71:d5:33:a9:57:79:ea:88:c7:56:6a:84:
8b:6c:46:00:46:b6:e9:50:3d:f3:da:50:e4:ce:3a:27:6c:ac:
ab:08:da:59:19:14:6e:a5:96:44:3a:9c:1d:15:18:aa:02:a4:
e7:1f:50:b4:4e:b3:1a:19:b4:0a:55:e9:23:98:46:a4:db:
e2:2c:7c:33:14:2f:53:00:5d:0c:c0:68:58:16:a6:60:13:f2:
cd:09:a2:d9:68:c8:15:18:21:e2:3a:6b:78:d0:8e:45:e8:18:
7b:e5:81:a3:a4:66:9b:fb:e5:75:b5:9f:1a:10:f1:3c:cc:d2:
27:aa:6e:3d:70:73:b1:f0:37:ea:51:de:8c:db:00:7f:b3:
61:1d:2d:16:c6:f2:0c:ba:6e:f8:c9:cf:b9:e1:d0:d1:97:bd:
53:2f:05:71:ef:f6:2f:2c:45:86:a7:2b:18:18:a5:a1:78:50:
de:71:5d:ad:ad:2c:d0:73:6:87:84:91:b8:f6:6c:6e:d1:3c:ce:0:
f4:6f:cc:44:46:cd:b4:1a:82:c4:e7:62:ae:83:a9:f2:1e:73:
bb:7c:e5:65:1c:70:ce:43:da:fa:c8:76:10:67:8d:bb:66:97:
19:cc:13:2e:c7:17:d8:d6:35:16:81:c3:1e:b0:ea:f7:ba:1b:
1d:28:8c:25:88:29:29:7e:e6:3d:71:a9:ee:ea:12:38:89:f9:
f4:2d:2a:2c:14:2d:c2:fe:14:11:03:86:67:aa:e8:ab:16:76:
63:5a:7c:81:2c:51:ad:9a:a6:a0:f5:c0:1a:ed:42:f8:a7:81:
03:b3:16:58:4f:4d:2b:9a:02:2a:c5:fd:3d:b3:c2:a1:a:80:
8f:f7:66:48:0d:bd:f0:41:4e:13:7f:4d:d4:cc:fe:35:08:27:
a3:c3:0f:4c:2b:9f:3c:88:39:09:a6:37:7c:92:13:ea:f6:7a:
47:07:1b:0e:33:d9:e9:e9:7b:5c:ab:a6:48:c5:3b:42:4f:02:
46:97:d7:bb:48:b4:f5:d6:ab:f2:34:71:e8:6e:c5:e8:a2:dc:
c7:fc:1c:f6:d4:5e:37:95:ed:cf:53:12:41:c3:2e:13:38:f8:
d4:b4:0b:92:33:89:d6:a7:la:b1:fb:a7:8e:72:2b:45:d5:6d:
0d:80:ed:8e:24:a4:cf:a8:7b:12:ab:9d:bb:3a:42:a9:ae:7f:
f2:ab:48:82:89:4a:f3:68:ce:18:42:8f:b7:3d:8f:19:da:a9:
3b:d7:be:04:cd:a8:c7:a7:13:8c:e1:bc:23:da:04:ac:f3:54:
70:e2:8c:27:5c:1a:52:95

```

## Looking at the decoded content of the RSA key

```

Seed:Ubuntu:20.04 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:11 •
root@325032e6fdf3:/ 
root@325032e6fdf3:/# openssl rsa -in ca.key -text -noout -passin pass:dees
RSA Private-Key: (4096 bit, 2 primes)
modulus:
00:da:ba:fa:99:b7:62:b6:13:45:de:0:be:a8:a6:
bf:07:dc:35:66:c8:0:77:e6:31:bf:bf:4a:d9:5a:
f1:49:b8:70:b8:63:ab:a8:8d:18:64:df:f6:71:
8a:6b:bf:16:75:73:ad:72:e5:2d:0e:64:03:2a:e7:
60:7a:16:a3:b6:ae:ee:6a:b2:76:10:ea:01:2e:f2:
b5:a0:84:11:3b:3a:9a:a2:7e:f1:8e:3e:ab:60:55:
0d:62:92:5f:35:59:ef:12:82:45:81:08:36:5e:99:
88:81:c4:87:d2:48:99:92:dc:d8:d9:62:10:f3:1f:
b3:23:c4:6f:df:21:66:60:73:eb:0e:51:93:dd:d5:
95:7f:11:7b:f8:9c:60:18:bf:6e:5f:e8:e6:be:b0:
b2:a4:4b:98:12:b5:f7:de:19:8f:4d:f1:b2:4a:73:
65:47:c4:07:bf:7f:f9:8e:60:57:bf:6f:bd:f5:
15:51:2f:4b:37:f5:98:25:3b:df:18:3f:69:9e:3c:
07:45:f6:51:12:9c:31:4d:67:26:83:33:63:1b:02:
80:8d:a5:46:d2:8e:43:c1:a7:95:f3:37:7a:7a:28:
40:f7:78:a6:e0:b9:29:ac:a0:7b:85:37:36:91:22:
37:25:97:55:c1:0f:5a:99:54:da:d0:0e:93:63:76:
5e:20:2b:52:ee:10:ce:c9:7d:f9:ba:6f:8f:a5:4e:
00:2c:3b:b8:d7:7b:8c:d0:6a:f3:f0:53:bc:24:22:
b9:fa:64:43:ce:cd:9a:0c:b3:07:ef:7a:0b:da:00:
1f:1d:7a:b4:f6:71:49:b7:ad:73:cc:33:3d:87:b7:
0a:11:de:97:aa:22:26:8d:7b:6b:79:34:e9:89:f8:
29:93:c8:8c:81:86:ef:e8:15:95:f4:a6:6b:9d:0f:
56:84:83:fd:ca:8a:08:78:2a:f9:2c:e0:7b:84:18:
a2:72:9e:64:a4:ad:a2:14:5e:7f:1c:b8:6e:fb:52:
7d:e3:65:76:5f:d4:f8:e0:df:20:60:e6:26:cc:18:
35:40:00:e5:5b:c4:fa:d0:65:3d:43:04:33:2f:10:
14:90:92:e2:fb:bf:77:44:05:22:b9:7a:4f:86:e7:
e1:f3:e8:97:a8:a9:c1:91:05:86:24:b9:ec:c6:bf:
18:c8:d4:a8:ab:a2:e0:9c:ca:c3:bd:fe:fa:fd:85:
e6:9a:ba:7b:c0:16:eb:bc:bc:00:57:29:ee:b8:6b:
73:ab:a9:69:af:ec:a3:e6:19:44:1a:6c:62:03:23:
85:49:6b:62:e9:5a:7c:38:2d:ad:60:1d:88:8a:39:
f1:60:0:a5:f8:6d:a2:b0:d0:44:b9:af:7c:59:c0:
95:7f:7b

```

```
Seed-Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:11 •
root@325032e6fd3:/ Search
publicExponent: 65537 (0x10001)
privateExponent:
00:a9:a1:02:41:fd:d7:7e:ce:d9:8b:e0:25:4c:53:
ec:a8:62:dd:c3:35:9b:e7:40:4d:6a:a0:26:a3:04:
05:46:1f:d4:c3:73:d9:58:c2:9d:83:c2:8f:71:e7:
41:eb:27:89:7a:52:d8:bb:d7:01:a7:3c:66:bc:7a:
2d:f6:e0:e1:dc:06:33:fd:e9:22:e9:21:21:03:d0:
d4:8c:84:7f:7c:88:8b:c1:7e:63:44:e6:53:2f:e5:
25:f9:40:fc:b7:3a:64:c1:dc:da:9c:23:cb:4e:78:
11:46:5a:2c:df:26:e9:4b:fd:1b:eb:12:43:84:d9:
1b:ab:85:38:41:3a:60:18:83:2d:52:b0:6f:55:45:
93:a7:b4:de:88:c2:75:40:1c:0d:b4:31:c1:e9:36:
cd:83:de:e0:33:fa:8d:1c:e0:83:a3:76:02:c7:fc:
50:1a:64:eb:81:56:f5:29:b6:8b:b2:42:67:dd:50:
59:54:d9:b1:a2:d7:43:43:f4:f7:a2:2d:63:72:84:
a9:3b:57:b8:2e:0f:95:a8:aa:8b:52:8a:a2:9c:4a:
c7:79:92:28:a7:98:0e:f1:fb:4e:ae:0d:63:5d:a3:
24:27:07:99:9b:83:dc:ce:f3:b2:77:70:87:4f:ec:
d2:09:c4:20:8c:15:a5:34:6e:7b:37:bb:08:50:c5:
76:5e:5b:14:88:f2:bd:72:3b:53:74:27:5c:c0:08:
c3:19:93:6d:30:d3:0e:a0:94:2c:fe:ea:d4:28:18:
6e:4:94:2e:ee:ee:a3:16:13:eb:9f:22:c3:2c:0f:
63:20:a1:e8:6c:20:26:50:96:d8:a0:3b:6e:62:d2:
9b:df:4f:67:2e:14:c8:28:eb:63:1e:2d:47:76:1d:
59:ef:b5:b2:ba:bb:31:3a:a1:64:98:65:e9:e8:27:
6a:ff:2d:3e:de:74:7f:30:ab:b3:69:58:3e:5e:a7:
df:df:78:6:64:b0:ad:9c:97:d8:82:89:bc:47:aa:97:
6a:63:9d:a6:00:0a:cc:3a:34:f2:04:dc:3c:49:df:
74:ca:34:a7:f9:82:06:c7:61:43:ff:d7:53:53:1c:
dc:78:fe:9e:dd:25:7f:6c:de:b2:eb:2f:65:cf:3d:
81:54:58:1b:64:42:02:c5:60:f7:5f:47:04:2c:10:
cc:2a:12:84:27:78:58:c5:75:6c:50:bc:1e:d4:29:
91:f6:71:af:1e:87:7e:03:8c:38:le:ca:0c:25:d1:
39:09:3a:35:b4:7b:40:cb:e5:65:37:7f:9d:01:e9:
c6:8b:df:b9:d6:12:55:fe:c8:85:63:4e:98:f6:30:
87:0:56:3c:95:88:94:25:3f:83:3d:3f:0a:74:92:
fd:6d:49
prime1:
```

```
Seed-Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:12 •
root@325032e6fd3:/ Search
prime1:
00:f5:6f:18:d1:e5:b4:77:38:4e:1f:45:00:20:78:
dc:bc:a6:06:d4:8e:3b:f9:bc:3e:0c:d5:1d:44:15:
ac:5b:83:61:32:d9:ef:55:39:d2:4f:57:f4:8b:92:
04:af:62:88:82:28:ce:f8:55:ae:01:1b:5d:0e:e6:
cf:09:e7:69:89:df:2e:88:4f:91:f4:28:c3:be:2c:
be:d1:0b:a2:92:40:b1:73:38:2d:01:0d:7b:9a:b0:
c0:4b:7c:15:bf:4b:88:e3:e1:7b:c8:05:70:a2:a6:
e1:f3:4d:ae:fa:75:46:0f:74:f1:f4:11:3b:1c:e1:
d6:40:df:93:ea:46:7f:d2:ee:b0:4c:11:56:56:50:
c0:ce:19:a7:bf:33:ab:89:0a:7d:4e:68:a3:cf:59:
38:7b:1f:53:74:27:6c:ba:a0:01:93:09:03:b7:39:
74:06:c8:16:c9:c0:5f:59:82:96:b1:51:f2:d6:3b:
0d:37:23:02:19:7b:9c:74:37:d0:d9:7a:03:2a:b7:
1b:33:34:8c:30:9d:80:7e:4f:af:93:2b:4a:9d:f4:
46:5b:ed:50:4c:74:65:a9:e9:d7:a2:c2:de:8c:e2:
36:c9:ea:ed:8b:76:10:a4:2d:37:86:79:39:71:33:
42:24:78:e5:00:85:83:fc:9e:6a:f3:ba:71:6e:95:
d8:ad
prime2:
00:e4:25:95:9d:01:f8:34:d9:88:43:a7:8d:c0:f3:
e1:07:98:35:f7:d8:27:bd:fa:15:ad:05:1f:65:79:
73:6d:7c:a6:b1:dd:59:ab:05:ae:3e:11:69:81:30:
12:06:43:6f:37:32:ff:70:2c:ae:7c:98:f5:de:c4:
f7:40:39:40:da:16:f0:0a:21:e7:8b:07:62:6f:c2:
dt:41:05:08:20:b3:b7:a0:3a:c3:b2:43:9a:c0:9f:
8c:47:a0:8f:06:d3:92:3a:0a:a2:cc:2c:85:d6:5d:
ba:21:7d:a5:81:8b:30:08:38:16:50:b2:0b:8a:6e:
50:f3:09:bd:6e:24:13:2e:74:32:ac:5c:a9:33:50:
a2:b6:17:69:72:44:1c:bc:44:7f:f0:64:20:6b:61:
9a:40:7e:49:14:7b:81:02:2b:fe:66:67:b0:d2:9d:
d6:cc:c9:5e:19:4a:01:5f:df:59:31:d5:a3:5a:a9:
d9:37:ff:55:5e:22:f1:87:54:7c:07:84:e5:fc:28:
ae:e2:60:8f:f9:d8:94:10:23:59:82:df:7e:c2:93:
05:ae:9a:3b:d9:51:4e:fd:eb:d5:26:82:6b:7f:b6:
38:42:8f:12:48:4d:4e:12:5f:4b:30:45:48:29:de:
4d:9e:24:d6:31:21:99:2e:9d:0a:77:8f:37:d9:bf:
75:c7
```

```

Seed:Ubuntu20.04 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:12 • root@325032e6fdf3:/
exponent1:
00:95:1a:27:13:ec:de:93:c6:ea:fe:e8:26:49:93:
e3:55:df:ef:2a:56:36:6d:63:44:b6:fb:09:a4:81:
78:32:28:40:76:6a:1b:91:c5:0c:d5:12:f4:07:8e:
6f:b6:34:c0:05:82:01:29:e0:b3:bd:5d:02:4d:b9:
3e:72:1f:d9:e7:de:64:20:7f:66:85:d3:f6:06:a4:
9c:4f:d7:27:ae:7e:0a:c9:a8:83:0d:2d:06:98:55:
64:9c:f7:07:27:2d:b6:3d:ea:90:0e:55:ef:b5:80:
78:a8:1c:bb:7e:80:06:9f:71:46:44:25:eb:a9:82:
31:6d:3b:e6:5a:99:47:f2:56:fb:57:5a:f8:fe:7b:
14:86:a0:e3:5d:af:00:38:c2:dc:99:33:cc:c0:7c:
cd:69:4f:00:9e:02:0d:75:db:1a:da:3c:ee:9a:f3:
16:de:1c:b4:6b:60:49:0c:71:df:26:5e:48:8e:89:
55:5f:f7:ae:a0:d8:8d:95:b5:0a:f5:f3:bf:d4:c5:
64:8a:d9:13:89:bd:45:80:76:dc:8d:25:b1:b0:ff:
e3:76:99:57:3c:fb:41:7f:d0:06:20:65:0e:5a:bc:
5a:08:93:7a:b2:4c:c9:93:53:bc:f5:be:d3:7c:c7:
cd:18:e7:31:07:fe:14:ce:f5:56:b8:36:be:0e:96:
8e:09
e7

exponent2:
72:b0:16:1a:dc:6f:9a:99:b3:ef:56:9e:62:dd:f6:
44:6c:16:cd:25:a3:2c:d4:37:eb:47:44:f6:2c:ec:
82:a0:83:e7:ab:bf:34:c2:e1:49:a0:55:2a:35:31:
0a:67:01:d4:7c:d5:7d:dd:68:45:88:5b:29:06:58:
c8:b7:3f:4b:a2:f6:3e:11:b7:24:e3:ac:6f:44:46:
18:98:5f:f2:98:85:79:8d:b0:ec:bf:21:5f:2d:95:
46:38:87:4d:c6:33:9e:eb:d3:d4:d1:98:e2:1f:31:
bf:3e:3b:61:f8:c7:47:8a:72:65:10:8e:77:a3:67:
1c:15:cc:5d:3e:d3:49:a9:ee:03:49:7d:61:27:6a:
f4:20:a6:c8:63:47:12:b9:58:9b:4e:aa:21:70:ea:
2a:fb:90:df:34:0a:b1:3d:ce:60:4a:45:d0:4a:ba:
3d:2e:09:18:ab:64:2f:7e:c6:86:c:f:bf:93:87:08:
84:26:de:12:39:7c:b3:2c:1c:41:97:a6:a9:71:06:
21:14:ab:ab:cc:5c:fa:13:db:1e:78:1d:6f:d0:9a:
ad:a0:28:ef:e0:f8:d5:9a:a5:06:fb:ce:f0:5f:78:
be:b4:cf:5a:fb:49:80:e0:d8:9a:46:69:b5:6a:64:
18:58:aa:37:fe:8c:d3:aa:ec:25:18:20:da:5c:6d:
e7

root@325032e6fdf3:~# ls
bin ca.crt certs dev home lib32 libx32 mnt opt root sbin sys usr volumes
boot ca.key demoCA etc lib lib64 media openssl.cnf proc run srv tmp var
root@325032e6fdf3:~# 

```

2:12 PM  
4/16/2025

The file ca.key contains the CA's private key, while ca.crt contains the public-key certificate

```

Seed:Ubuntu20.04 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:18 • root@325032e6fdf3:/
c8:b7:3f:4b:a2:f6:3e:11:b7:24:e3:ac:6f:44:46:
18:98:5f:f2:98:85:79:8d:b0:ec:bf:21:5f:2d:95:
46:38:87:4d:c6:33:9e:eb:d3:d4:d1:98:e2:1f:31:
bf:3e:3b:61:f8:c7:47:8a:72:65:10:8e:77:a3:67:
1c:15:cc:5d:3e:d3:49:a9:ee:03:49:7d:61:27:6a:
f4:20:a6:c8:63:47:12:b9:58:9b:4e:aa:21:70:ea:
2a:fb:90:df:34:0a:b1:3d:ce:60:4a:45:d0:4a:ba:
3d:2e:09:18:ab:64:2f:7e:c6:86:c:f:bf:93:87:08:
84:26:de:12:39:7c:b3:2c:1c:41:97:a6:a9:71:06:
21:14:ab:ab:cc:5c:fa:13:db:1e:78:1d:6f:d0:9a:
ad:a0:28:ef:e0:f8:d5:9a:a5:06:fb:ce:f0:5f:78:
be:b4:cf:5a:fb:49:80:e0:d8:9a:46:69:b5:6a:64:
18:58:aa:37:fe:8c:d3:aa:ec:25:18:20:da:5c:6d:
e7

coefficient:
00:00:ce:d0:ec:5e:79:9f:eb:88:45:82:9f:32:c8:
e0:69:74:2e:bb:b3:54:ab:c3:30:38:04:95:c9:65:
3b:3d:94:33:15:0d:6b:b7:ae:c1:65:00:eb:25:b3:
12:48:61:5d:0f:98:3e:b2:60:ad:c8:dc:2f:f2:67:
9c:f6:a1:d6:85:55:97:1e:df:d1:47:70:12:2d:f3:
18:42:8b:66:4a:92:b8:c6:4d:78:c7:a4:c0:23:4a:
c2:47:16:43:a3:36:a5:ac:da:87:c9:99:b3:f1:14:
b6:0d:8e:5e:72:d1:a4:03:11:10:32:02:84:da:e9:
f2:c3:0f:09:73:2e:f1:79:e5:d3:0a:8b:36:86:47:
4a:b7:92:29:44:4b:8f:59:d1:5c:9c:93:ca:1b:2b:
ca:51:78:78:1d:7a:c9:d:ff:ee:d0:d3:6c:1c:dc:
09:c6:43:c3:c8:92:b9:16:83:8c:85:ef:aa:b8:da:
07:a2:5d:44:30:e6:ba:ad:30:5e:42:0b:db:be:0e:
c5:c0:19:49:15:9b:79:0f:c6:79:b0:b3:ad:3f:fd:
9c:97:3c:ce:68:ea:33:8d:be:7d:f5:32:6a:54:a0:
24:e0:79:e5:a9:8e:67:c9:8c:60:5a:b7:7d:81:cb:
9f:3a:f4:ba:07:f0:4c:79:82:ee:28:6f:ce:aa:bc:
e9:be
root@325032e6fdf3:~# ls
bin ca.crt certs dev home lib32 libx32 mnt opt root sbin sys usr volumes
boot ca.key demoCA etc lib lib64 media openssl.cnf proc run srv tmp var
root@325032e6fdf3:~# 

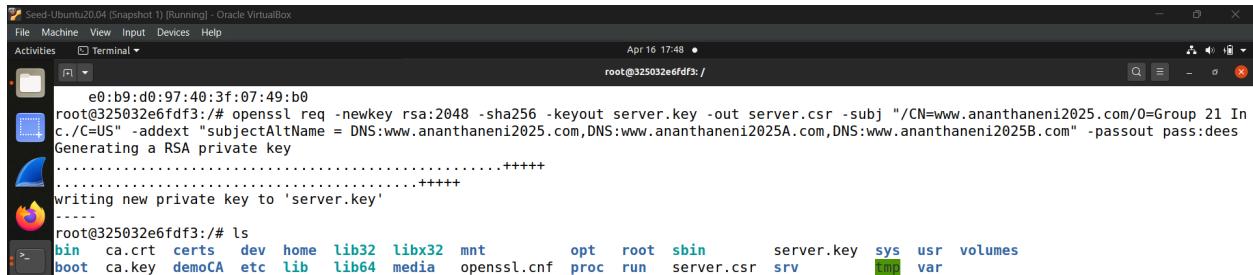
```

2:18 PM  
4/16/2025

### 3.2 Task 2: Generating a Certificate Request for Your Web Server

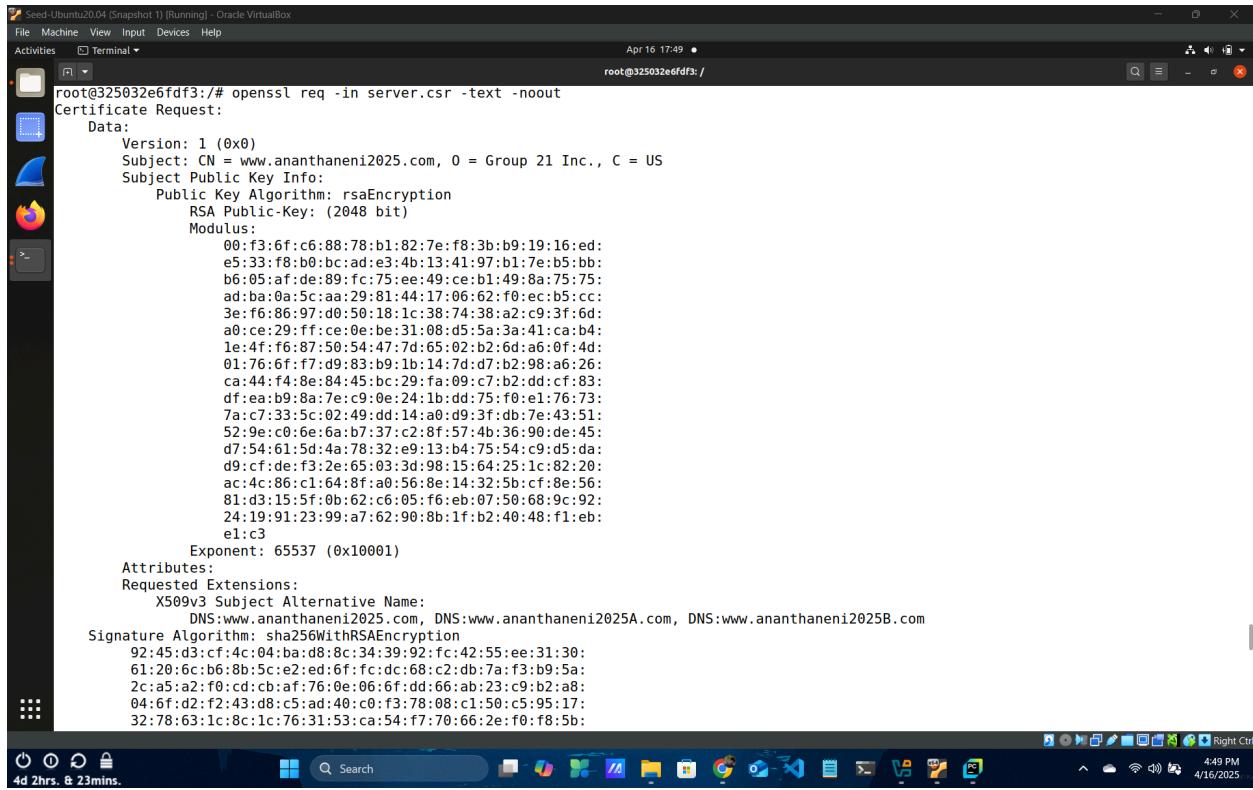
Generating a Certificate Signing Request for our servers ([www.ananthaneni2025.com](http://www.ananthaneni2025.com)) by using SAN extensions to allow a certificate to have multiple names

```
openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/CN=www.ananthaneni2025.com/O=Group 21 Inc./C=US" -addext "subjectAltName = DNS:www.ananthaneni2025.com,DNS:www.ananthaneni2025A.com,DNS:www.ananthaneni2025B.com" -passout pass:dees
```



```
Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:48 •
root@325032e6fdf3:/root
e0:b9:d0:97:40:3f:07:49:b0
root@325032e6fdf3:/# openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/CN=www.ananthaneni2025.com/O=Group 21 Inc./C=US" -addext "subjectAltName = DNS:www.ananthaneni2025.com,DNS:www.ananthaneni2025A.com,DNS:www.ananthaneni2025B.com" -passout pass:dees
Generating an RSA private key
.....+
writing new private key to 'server.key'
-----
root@325032e6fdf3:/# ls
bin ca.crt certs dev home lib32 libx32 mnt opt root sbin server.key sys usr volumes
boot ca.key demoCA etc lib lib64 media openssl.cnf proc run server.csr srv tmp var
```

Looking at the decoded content of the CSR file



```
Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:49 •
root@325032e6fdf3:/root
root@325032e6fdf3:/# openssl req -in server.csr -text -noout
Certificate Request:
Data:
Version: 1 (0x0)
Subject: CN = www.ananthaneni2025.com, O = Group 21 Inc., C = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:f3:6f:c6:88:78:b1:82:7e:f8:3b:b9:19:16:ed:
            e5:33:f8:b0:bc:ad:e3:4b:13:41:97:b1:7e:b5:bb:
            b6:05:af:de:89:fc:75:ee:49:ce:b1:49:8a:75:75:
            ad:ba:0a:5c:aa:29:81:44:17:06:62:f0:ec:b5:c1:
            3e:f6:86:97:00:50:18:1c:38:74:38:a2:c9:3f:6d:
            a0:ce:29:ff:ce:0e:be:31:08:d5:5a:3a:41:ca:b4:
            1e:4f:f6:87:50:54:47:7d:65:02:b2:6d:a6:0f:4d:
            01:76:6f:f7:d9:83:b9:1b:14:7d:d7:b2:98:a6:26:
            ca:44:f4:fe:84:45:bc:29:fa:09:c7:b2:dd:c1:83:
            df:ea:b9:8a:7e:c9:0e:24:1b:dd:75:f0:e1:76:73:
            7a:c7:33:5c:02:49:dd:14:a0:09:3f:db:7e:43:51:
            52:9e:c8:6e:6a:b7:37:c2:8f:57:4b:36:90:de:45:
            d7:54:61:5d:4a:78:32:e9:13:b4:75:54:c9:d5:da:
            d9:c7:de:f3:2e:65:03:3d:98:15:64:25:1c:82:20:
            ac:4c:86:c1:64:8f:a0:56:8e:14:32:5b:cf:8e:56:
            81:d3:15:5f:0b:62:c6:05:f6:eb:07:50:68:9c:92:
            24:19:91:23:99:a7:62:90:8b:1f:b2:40:48:f1:eb:
            e1:c3
        Exponent: 65537 (0x10001)
Attributes:
Requested Extensions:
    X509v3 Subject Alternative Name:
        DNS:www.ananthaneni2025.com, DNS:www.ananthaneni2025A.com, DNS:www.ananthaneni2025B.com
Signature Algorithm: sha256WithRSAEncryption
92:45:d3:cf:4c:04:ba:d8:8c:34:39:92:fc:42:55:ee:31:30:
61:20:6c:b6:8b:5c:e2:ed:6f:fc:dc:68:c2:db:7a:f3:b9:5a:
2c:a5:a2:f0:cd:cb:af:76:0e:06:6f:dd:66:ab:23:c9:b2:a8:
04:6f:d2:f2:43:d8:c5:ad:40:c0:f3:78:08:c1:50:c5:95:17:
32:78:63:1c:8c:1c:76:31:53:ca:54:f7:70:66:2e:f0:f8:5b:
```

```

Seed:Ubuntu20.04 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:49 •
root@325032e6fdf3:/ 
e5:33:t8:00:0c:ad:e3:4b:13:41:9:/:b1:/e:0b:0d:
b6:05:af:de:89:fc:75:ee:49:ce:b1:49:8a:75:75:
ad:ba:0a:5c:aa:29:81:44:17:06:62:f0:ec:b5:cc:
3e:f6:86:97:d0:50:18:1c:38:74:38:a2:c9:3f:6d:
a0:ce:29:ff:ce:0e:be:31:08:05:5a:3a:41:ca:b4:
1e:4f:f6:87:50:54:47:7d:65:02:b2:6d:a6:0f:4d:
01:76:6f:f7:d9:83:b9:1b:14:7d:d7:b2:98:a6:26:
ca:44:f4:8e:84:45:bc:29:fa:09:c7:b2:dd:c1:83:
df:ea:b9:8a:7e:c9:0e:24:1b:dd:75:f0:e1:76:73:
7a:c7:33:5c:02:49:dd:14:a0:09:3f:db:7e:43:51:
52:9e:c0:6e:6a:b7:37:c2:8f:57:4b:36:90:de:45:
d7:54:61:5d:4a:78:32:e9:13:b4:75:54:c9:d5:da:
d9:cf:de:f3:2e:65:03:3d:98:15:64:25:1c:82:20:
ac:4c:86:c1:64:8f:a0:56:8e:14:32:5b:cf:8e:56:
81:d3:15:5f:0b:62:c6:05:f6:eb:07:50:68:9c:92:
24:19:91:23:99:a7:62:90:8b:1f:b2:40:48:f1:eb:
e1:c3
Exponent: 65537 (0x10001)
Attributes:
Requested Extensions:
X509v3 Subject Alternative Name:
DNS:www.ananthaneni2025.com, DNS:www.ananthaneni2025A.com, DNS:www.ananthaneni2025B.com
Signature Algorithm: sha256WithRSAEncryption
92:45:d3:cf:4c:04:ba:d8:8c:34:39:92:fc:42:55:ee:31:30:
61:20:6c:b6:8b:8c:2e:ed:6f:fc:dc:68:c2:db:7a:f3:b9:5a:
2c:a5:a2:f0:cd:cb:af:76:0e:06:f6:dd:66:ab:23:c9:b2:a8:
04:6f:d2:f2:43:d8:5c:ad:40:c0:f3:78:08:c1:5b:c5:95:17:
32:78:63:1c:8c:1c:76:31:53:ca:54:f7:70:66:2e:f0:f8:5b:
d2:be:07:86:aa:94:49:fc:33:11:e4:d2:5f:42:b8:c1:fd:09:
79:38:83:d9:0b:da:27:31:f4:a9:f5:fc:48:e9:e0:4f:33:58:
a2:1f:9c:9b:9e:ad:30:9e:d8:a7:2e:f3:32:f1:8e:3a:10:af:
b0:ce:9b:c3:87:d7:c2:ab:56:7e:2f:b2:bb:e0:0e:a5:b1:20:
fa:30:c6:57:8e:9d:07:5a:c6:7a:88:e2:93:0b:71:69:31:6f:
44:29:23:0f:0e:7a:50:b6:06:c5:ec:b9:fe:2d:65:71:74:5b:
e3:f6:f4:f4:70:80:ea:4e:6f:87:13:8f:1a:51:6e:cb:3f:23:
b5:ed:d9:29:48:56:95:ba:68:3a:93:6b:38:02:60:bd:2d:8e:
c0:4c:78:6d:0a:54:23:f1:fd:5d:a7:0a:d2:7b:23:18:5a:7f:
3e:3d:52:0b

```

## Looking at the decoded content of the private key file

```

Seed:Ubuntu20.04 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:50 •
root@325032e6fdf3:/ 
3e:3d:52:0b
root@325032e6fdf3:/# openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
00:f3:6f:c6:88:78:b1:82:7e:f8:3b:b9:19:16:ed:
e5:33:f8:b0:bc:ad:e3:4b:13:41:97:b1:7e:b5:bb:
b6:05:af:de:89:fc:75:ee:49:ce:b1:49:8a:75:75:
ad:ba:0a:5c:aa:29:81:44:17:06:62:f0:ec:b5:cc:
3e:f6:86:97:d0:50:18:1c:38:74:38:a2:c9:3f:6d:
a0:ce:29:ff:ce:0e:be:31:08:d5:5a:3a:41:ca:b4:
1e:4f:f6:87:50:54:47:7d:65:02:b2:6d:a6:0f:4d:
01:76:6f:f7:d9:83:b9:1b:14:7d:d7:b2:98:a6:26:
ca:44:f4:8e:84:45:bc:29:fa:09:c7:b2:dd:c1:83:
df:ea:b9:8a:7e:c9:0e:24:1b:dd:75:f0:e1:76:73:
7a:c7:33:5c:02:49:dd:14:a0:d9:3f:db:7e:43:51:
52:9e:c0:6e:6a:b7:37:c2:8f:57:4b:36:90:de:45:
d7:54:61:5d:4a:78:32:e9:13:b4:75:54:c9:d5:da:
d9:cf:de:f3:2e:65:03:3d:98:15:64:25:1c:82:20:
ac:4c:86:c1:64:8f:a0:56:8e:14:32:5b:cf:8e:56:
81:d3:15:5f:0b:62:c6:05:f6:eb:07:50:68:9c:92:
24:19:91:23:99:a7:62:90:8b:1f:b2:40:48:f1:eb:
e1:c3
publicExponent: 65537 (0x10001)
privateExponent:
24:2b:f5:aa:0d:95:02:b8:ef:15:a0:b9:53:a8:e1:
a7:c9:4a:29:9f:04:e9:00:e1:7c:32:c9:8b:23:6b:
36:89:1d:5e:0f:7f:4e:7a:f5:15:6e:c1:fe:16:10:
4c:56:81:d2:5e:fc:70:2b:a3:ad:4b:f3:40:48:2b:
0a:e2:90:e8:49:le:6c:03:0f:71:e2:ee:58:58:67:
ce:7a:7b:22:19:1a:b5:9a:84:69:35:c2:d4:e5:d2:
a3:3b:14:7c:21:29:c6:3e:le:la:79:24:75:9d:91:
9c:11:a3:18:54:f4:4a:4b:cf:2f:1f:0:82:df:bc:
aa:66:54:4e:df:35:c8:5e:ae:a5:f6:4e:a2:37:f5:
c7:4a:0e:e0:57:6b:b1:70:ab:5f:da:bd:4a:12:d9:
53:46:f8:42:3f:80:ef:65:ec:d1:86:52:4c:ce:d9:
12:4c:22:d4:f9:0d:f8:0a:de:b5:03:66:87:84:13:
c9:cb:36:5f:e6:53:8b:6c:06:08:d3:67:c9:28:25:

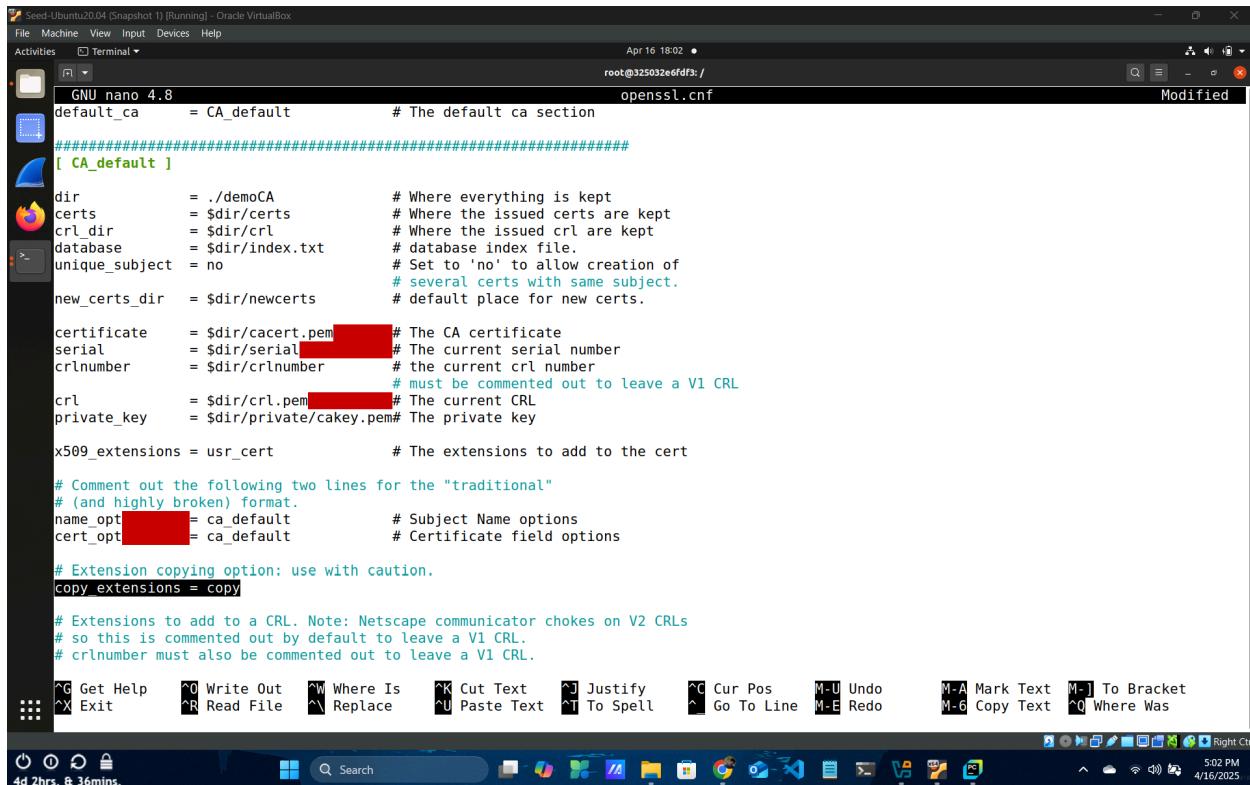
```

```
Seed-Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:51 •
root@325032e6fdf3:/# 
c9:cb:36:5f:eb:53:8b:6c:0b:08:d3:b7:c9:28:25:
ef:2b:5d:0a:22:19:82:79:72:f3:97:40:f5:72:75:
43:ea:55:ca:68:c7:46:8d:20:47:c6:61:ba:41:
3d:f2:0c:03:9d:d0:cc:44:85:1a:1e:9e:1f:6e:b8:
6f:4d:d1:48:a8:e4:40:20:1b:85:0d:bb:be:59:5c:
81
prime1:
00:fe:54:8e:c3:c9:9c:30:bd:e3:72:8e:4e:0e:0d:
48:9a:67:2c:da:26:35:94:92:25:c5:65:26:1e:fb:
58:12:58:d6:a3:d2:12:73:00:aa:0f:91:02:ec:8d:
3f:c6:52:3d:a8:db:01:31:c2:e9:83:94:bc:5a:bf:
62:04:f3:05:30:64:e8:f0:41:89:53:e1:3c:39:6b:
e3:33:77:e3:37:83:22:ac:4c:88:47:88:7e:c6:7:
36:e9:d1:bd:30:08:52:0b:49:fc:f1:4b:ae:21:b4:
25:37:df:97:59:e8:1c:19:11:61:0d:f2:77:1e:c7:
e3:f7:e6:ae:6b:b3:e5:a9:e3
prime2:
00:f5:08:e8:c7:4e:06:99:95:e3:f8:39:80:ba:37:
ca:b9:14:99:4e:38:1a:e5:fe:5d:5c:53:6e:a2:6b:
55:c7:ad:5e:6f:52:97:df:25:89:25:6b:3d:24:
26:02:a5:ef:b7:99:dc:ed:21:30:57:2e:e8:13:a2:
79:dc:ce:fb:d3:c9:97:a9:1d:27:4b:c4:d9:32:03:
43:11:37:1f:56:2d:54:0c:fa:10:33:ce:89:9f:de:
c2:1e:d0:fc:e9:7e:96:57:16:c2:0b:7d:83:d6:ca:
b6:7b:32:23:fe:67:92:12:06:2e:e9:94:9f:c1:fe:
e7:4f:32:a4:31:5d:39:ee:a1
exponent1:
00:94:79:e0:ee:c4:20:7f:04:1c:68:a0:53:49:aa:
a6:f8:1d:0b:be:3f:58:40:68:21:cc:df:84:25:ca:
2e:5c:67:a8:c6:f2:b8:fa:92:84:b5:99:be:cf:42:
96:dc:bc:de:6a:5a:0a:02:b6:fb:84:69:ac:9c:7d:
e6:47:65:68:be:1b:eb:31:77:d1:28:3a:f1:e1:c3:
ee:5b:f9:bd:98:86:e2:13:1c:8a:e2:d7:f8:cb:18:
8b:a2:6d:63:b9:4a:e2:3a:dc:f2:e2:1b:80:89:04:
96:45:cc:2e:9b:ba:39:cd:18:ac:44:6c:2c:c6:b7:
83:8b:12:0c:f9:ab:88:84:69
exponent2:
00:80:6f:26:0b:e9:62:de:37:c9:a0:ff:0a:f1:10:
root@325032e6fdf3:/# 
4d 2hrs. & 25mins. 4:51 PM 4/16/2025
```

```
Seed-Ubuntu20.04 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:51 •
root@325032e6fdf3:/# 
26:02:a5:ef:b7:99:dc:ed:21:30:57:2e:e8:13:a2:
79:dc:ce:fb:d3:c9:97:a9:1d:27:4b:c4:d9:32:03:
43:11:37:1f:56:2d:54:0c:fa:10:33:ce:89:9f:de:
c2:1e:d0:fc:e9:7e:96:57:16:c2:0b:7d:83:d6:ca:
b6:7b:32:23:fe:67:92:12:06:2e:e9:94:9f:c1:fe:
e7:4f:32:a4:31:5d:39:ee:a1
exponent1:
00:94:79:e0:ee:c4:20:7f:04:1c:68:a0:53:49:aa:
a6:f8:1d:0b:be:3f:58:40:68:21:cc:df:84:25:ca:
2e:5c:67:a8:c6:f2:b8:fa:92:84:b5:99:be:cf:42:
96:dc:bc:de:6a:5a:0a:02:b6:fb:84:69:ac:9c:7d:
e6:47:65:68:be:1b:eb:31:77:d1:28:3a:f1:e1:c3:
ee:5b:f9:bd:98:86:e2:13:1c:8a:e2:d7:f8:cb:18:
8b:a2:6d:63:b9:4a:e2:3a:dc:f2:e2:1b:80:89:04:
96:45:cc:2e:9b:ba:39:cd:18:ac:44:6c:2c:c6:b7:
83:8b:12:0c:f9:ab:88:84:69
exponent2:
00:80:6f:26:0b:e9:62:de:37:c9:a0:ff:0a:f1:10:
73:4a:a5:78:61:9e:58:c2:fa:9b:96:dc:08:5e:4b:
a2:53:ba:06:e9:3b:b2:6f:f6:3f:a7:6e:1c:92:94:
92:f3:ca:64:26:b9:18:2a:96:bd:ce:c4:c0:52:22:
54:7b:9f:66:31:b1:35:b4:27:9a:c4:45:2e:8e:df:
54:4d:fe:2e:87:ae:04:a3:34:a3:2f:74:6f:80:83:
72:fe:52:0e:6e:98:b2:56:7d:90:42:13:8c:fa:15:
90:a6:6c:36:9f:8f:4b:e9:f4:a1:bc:3e:f1:a9:ee:
60:f1:8b:1a:b2:e1:29:8f:61
coefficient:
61:7b:f6:8b:4d:10:09:49:15:cc:7e:c8:ce:d6:1b:
5a:c7:b8:0d:cc:f8:2b:b7:ec:3d:cc:06:c0:93:d4:
b8:5f:75:3a:70:22:42:98:fb:1f:ee:0e:f0:f8:60:
9c:4f:3a:34:1b:69:9c:01:60:cc:35:0f:0b:33:31:
53:ef:15:15:75:9e:4d:ad:6d:c8:f2:cb:67:42:6f:
54:ba:ab:b0:f4:2f:bc:4a:59:28:83:76:56:f0:32:
bc:71:94:eb:53:8d:21:29:b8:7f:0f:25:bf:b0:9d:
33:1c:4b:92:7b:07:id:80:54:34:88:72:8d:12:01:
e4:ec:69:43:e9:5f:40:f8
root@325032e6fdf3:/# 
4d 2hrs. & 25mins. 4:51 PM 4/16/2025
```

### 3.3 Task 3: Generating a Certificate for your server

Opened openssl.cnf file in a text editor & uncommented the highlighted line to ensure the Subject Alternative Names (SANs) added by us in the CSR will be included in the final signed certificate



```
root@325032e6fdf3:/root/.nanorc# nano openssl.cnf
root@325032e6fdf3:/root/.nanorc# cat openssl.cnf
# This file can be used to override options in a CA's config file.
# If you do not have access to the CA's config file, you can copy
# its contents here and change the values as needed.
# You can also specify multiple CA config files by listing them
# separated by colons.
# 
# Configuration for a CA
[ CA_default ]
dir      = ./demoCA          # Where everything is kept
certs    = $dir/certs         # Where the issued certs are kept
crl_dir  = $dir/crl           # Where the issued crl are kept
database = $dir/index.txt    # database index file.
unique_subject = no          # Set to 'no' to allow creation of
                             # several certs with same subject.
new_certs_dir = $dir/newcerts # default place for new certs.

certificate = $dir/cacert.pem # The CA certificate
serial     = $dir/serial        # The current serial number
crlnumber  = $dir/crlnumber    # the current crl number
crl       = $dir/crl.pem       # must be commented out to leave a V1 CRL
private_key = $dir/private/cakey.pem# The private key

x509_extensions = usr_cert   # The extensions to add to the cert

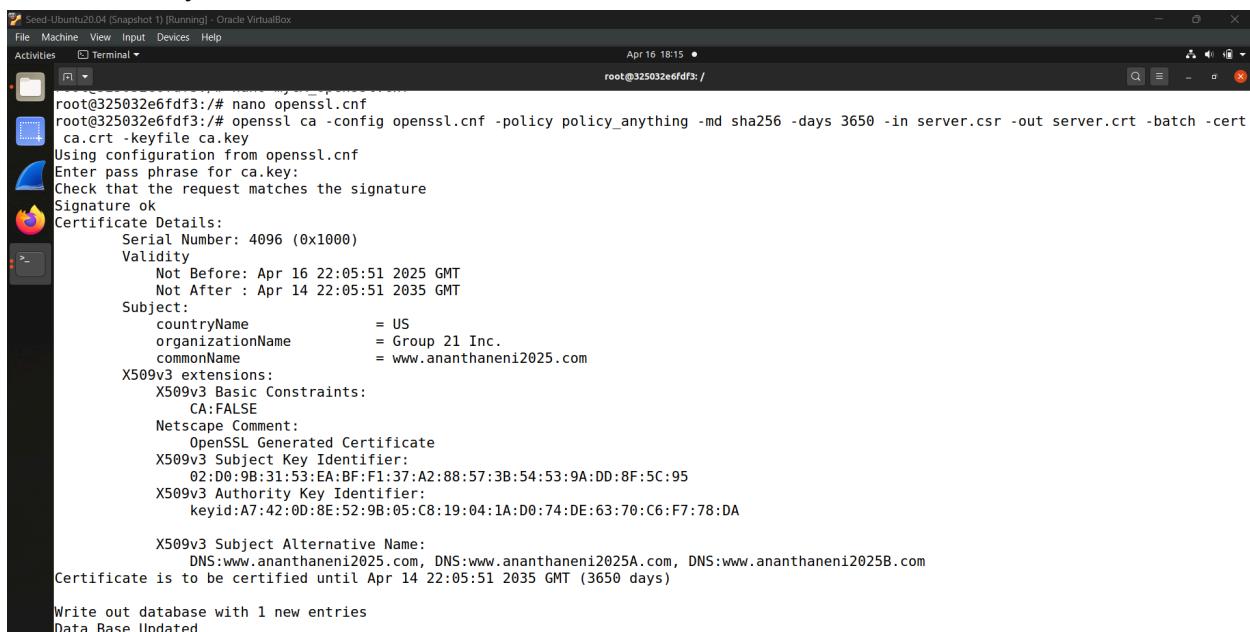
# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt    = ca_default      # Subject Name options
cert_opt    = ca_default      # Certificate field options

# Extension copying option: use with caution.
copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File   ^A Replace   ^U Paste Text ^I To Spell  ^L Go To Line M-E Redo
M-A Mark Text M-J To Bracket M-G Copy Text ^Q Where Was
4d 2hrs. & 36mins. 5:02 PM 4/16/2025
```

Turning our certificate signing request (server.csr) into an X509 certificate (server.crt) by using the CA's ca.crt and ca.key



```
root@325032e6fdf3:/# nano openssl.cnf
root@325032e6fdf3:/# openssl ca -config openssl.cnf -policy policy_anything -md sha256 -days 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4096 (0x1000)
    Validity
        Not Before: Apr 16 22:05:51 2025 GMT
        Not After : Apr 14 22:05:51 2035 GMT
    Subject:
        countryName      = US
        organizationName = Group 21 Inc.
        commonName       = www.ananthaneni2025.com
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            02:D0:9B:31:53:EA:BF:F1:37:A2:88:57:3B:54:53:9A:DD:8F:5C:95
        X509v3 Authority Key Identifier:
            keyid:A7:42:0D:8E:52:9B:05:C8:19:04:1A:D0:74:DE:63:70:C6:F7:78:DA
    X509v3 Subject Alternative Name:
        DNS:www.ananthaneni2025.com, DNS:www.ananthaneni2025A.com, DNS:www.ananthaneni2025B.com
Certificate is to be certified until Apr 14 22:05:51 2035 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

On looking at the decoded content of this certificate, we observed CA:FALSE. This is because we are creating a certificate for a web server, but not for a Certificate Authority, i.e., it should only be used to enable HTTPS and should not be allowed to sign other certificates

```
root@325032e6fdf3:/# openssl x509 -in server.crt -text -noout
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
    Validity
        Not Before: Apr 16 22:05:51 2025 GMT
        Not After : Apr 14 22:05:51 2035 GMT
    Subject: C = US, O = Group 21 Inc., CN = www.ananthaneni2025.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
            Modulus:
                00:f3:6f:c6:88:78:b1:82:7e:f8:3b:b9:19:16:ed:
                e5:33:f8:b0:bc:ad:e3:41:97:b1:7e:b5:bb:
                b6:05:af:de:89:fc:75:ee:49:ce:b1:49:8a:75:75:
                ad:ba:0a:5c:aa:29:81:44:17:06:62:f0:ec:b5:cc:
                3e:f6:86:97:d0:50:18:1c:38:74:38:a2:c9:3f:6d:
                a0:ce:29:ff:ce:0e:be:31:08:d5:a3:41:ca:b4:
                1e:4f:f6:87:50:54:47:7d:65:02:b2:6d:a6:0f:4d:
                01:76:6f:f7:d9:83:b9:1b:14:7d:07:b2:98:a6:26:
                ca:44:f4:8e:84:45:bc:29:fa:09:c7:b2:dd:cf:83:
                df:ea:b9:8a:7e:c9:0e:24:1b:dd:75:f0:e1:76:73:
                7a:c7:33:5c:02:49:dd:14:a0:d9:3f:db:7e:43:51:
                52:9e:c0:6e:6a:b7:37:c2:8f:57:4b:36:90:de:45:
                d7:54:61:5d:4a:78:32:e9:13:b4:75:54:c9:d5:da:
                d9:cf:de:f3:2e:65:03:3d:98:15:64:25:1c:82:20:
                ac:4c:86:c1:64:8f:a0:56:8e:14:32:5b:cf:8e:56:
                81:d3:15:5f:0b:62:c6:05:f6:eb:07:50:68:9c:92:
                24:19:91:23:99:a7:62:90:8b:1f:b2:40:48:f1:eb:
                e1:c3
            Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    Netscape Comment:
```

Here, the alternative names are included successfully

```
root@325032e6fdf3:/#
File Machine View Input Devices Help
Activities Terminal Apr 16 18:17 •
root@325032e6fdf3:/#
openssl x509 -in server.crt -text -noout
-----  

X509v3 Subject Key Identifier:  

02:D8:9B:31:53:EA:BF:F1:37:A2:88:57:3B:54:53:9A:DD:8F:5C:95  

X509v3 Authority Key Identifier:  

keyid:A7:42:0D:8E:52:9B:05:C8:19:04:1A:D0:74:DE:63:70:C6:F7:78:DA  

X509v3 Subject Alternative Name:  

DNS:www.ananthaneni2025.com, DNS:www.ananthaneni2025A.com, DNS:www.ananthaneni2025B.com  

Signature Algorithm: sha256WithRSAEncryption  

5e:36:58:e5:c8:ce:2:85:c7:85:ba:78:3f:59:d1:b5:a2:7e:  

7d:25:06:e1:ac:f1:4f:de:06:c7:fa:51:59:e5:7f:c2:ae:32:  

06:09:c3:d7:08:56:0:8c:78:0a:ee:0b:f5:75:a1:89:b2:7a:  

9a:16:85:25:a9:9b:61:78:d4:75:e3:93:8c:34:b2:c9:28:a0:  

f5:c6:63:2f:4d:2d:72:18:ab:7f:ac:9e:77:a0:25:8c:7f:59:  

ef:59:39:5:e1:f7:55:2a:cb:86:a4:eb:f4:78:62:06:02:79:  

3f:4f:11:69:5b:59:5b:4e:3e:c2:3d:87:20:f0:52:49:86:2e:  

a1:ba:a4:56:e0:69:c5:0f:ea:06:17:d0:db:0b:31:71:26:0b:  

ad:fa:2c:ba:24:f7:30:48:18:f4:8f:18:ee:80:00:b9:dd:98:  

2d:80:3a:50:41:65:ad:3e:0e:10:b2:e2:69:87:02:e3:44:49:  

94:31:45:ea:71:e5:b8:a4:01:c8:5d:24:cb:91:a1:ed:f6:f7:  

db:cb:68:f9:15:b9:39:3e:70:64:f0:d6:35:75:fd:33:70:fd:  

50:6b:80:84:fc:ec:e1:e2:f9:6f:6d:b0:1b:e9:ef:78:fb:  

77:16:2c:b7:1b:0e:05:f8:7e:02:8c:32:bf:aa:6a:d3:7f:c0:  

d1:dd:19:ad:dd:c6:a0:d5:71:33:1c:7d:8:b0:64:d6:67:11:  

9a:56:91:43:ee:fe:29:f7:12:cc:7b:3b:b5:fc:81:9a:fd:  

20:d4:03:81:26:0d:6:a:c6:e9:41:70:96:3f:80:fc:76:7d:81:  

be:cf:62:7f:79:d6:0f:86:db:77:c7:df:b5:b6:0a:4b:1c:bc:  

49:b3:68:c1:bb:e0:84:5b:6e:2:0d:db:01:a4:53:fb:3d:da:  

11:2f:86:16:6d:b3:a4:4:f:69:10:79:84:03:f7:d3:5f:98:c8:  

5c:88:05:6b:97:6c:00:f0:40:e6:f5:36:a3:b2:16:33:b3:2e:  

a0:0e:d1:5d:37:b6:c1:8a:17:1c:82:65:f9:a1:97:29:cc:5f:  

4b:73:3e:46:c2:c1:3f:18:0e:be:00:36:ee:5d:40:fb:77:de:  

bd:d2:c0:88:61:f1:bc:a9:e2:6b:ac:0d:dc:87:05:63:be:  

0d:ad:74:7d:d4:62:a:f:13:0c:86:b1:e2:b3:a9:a3:a1:66:6b:  

2b:67:7b:0b:0b:73:ce:43:e7:ab:56:e1:d0:a2:7e:f0:10:0a:  

3b:25:12:4d:a8:05:69:e7:14:52:79:c4:b4:1f:68:f8:18:66:  

7d:b7:41:7c:01:97:33:06:5a:a2:1e:6a:c7:ff:6e:f5:d2:a7:  

37:f9:be:af:42:54:34:50
```

### 3.4 Task 4: Deploying Certificate in an Apache-Based HTTPS Website

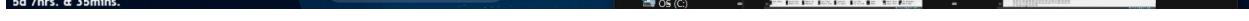
Updated the VirtualHost file located in /etc/apache2/sites-available directory to ensure Apache server to host multiple websites

```
root@325032e6fdf3:/# ls
bin  ca.crt  certs  dev  home  lib32  libx32  mnt  opt  root  sbin  server.csr  srv  var
boot  ca.key  demoCA  etc  lib  lib64  media  openssl.cnf  proc  run  server.crt  server.key  sys  usr  volumes
root@325032e6fdf3:/# cd etc
root@325032e6fdf3:/etc# ls
adduser.conf      debian_version  group-    kernel      lsb-release  nsswitch.conf  rc0.d      security     systemd
alternatives      default        gshadow   ld.so.cache  machine-id  opt          rc1.d      selinux     terminfo
apache2           deluser.conf  gshadow-  ld.so.conf   magic       os-release   rc2.d      services    timezone
apt               dpkg          gss       ld.so.conf.d  magic.mime  pam.conf    rc3.d      shadow     ucf.conf
bash.bashrc       e2scrub.conf host.conf  ldap        mailcap     pam.d       rc4.d      shells     ufw
bindresvport.blacklist environment  hostname  legal      mailcap.order  passwd    rc5.d      skel      update-motd.d
ca-certificates   ethertypes    hosts     libaudt.conf init.d      localtime  mime.types  perl      ssl
ca-certificates.conf fonts        issue     libaudt.conf  libcap     mailcap    rc6.d      subgid    xattr.conf
cron.d            fstab         iproute2  logcheck   mtab       profile    rcS.d      php      rcS.d
cron.daily        gai.conf      issue.net  logrotate.d  nanorc    profile.d  rmt      protocols  rpc      sysctl.conf
debconf.conf      group        issue.net  logrotate.d  networks   protocols  resolv.conf  subuid    sysctl.conf
root@325032e6fdf3:/etc# cd apache2
root@325032e6fdf3:/etc/apache2# ls
apache2.conf  conf-available  envvars  magic  mods-available  ports.conf  sites-available  sites-enabled
root@325032e6fdf3:/etc/apache2# cd sites-available
root@325032e6fdf3:/etc/apache2/sites-available# ls
000-default.conf  bank32_apache_ssl.conf  default-ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available# nano 000-default.conf
root@325032e6fdf3:/etc/apache2/sites-available# nano default-ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available# nano bank32 apache_ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available# cp bank32 apache_ssl.conf ananthaneni2025 apache_ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available# ls
000-default.conf  ananthaneni2025 apache_ssl.conf  bank32 apache_ssl.conf  default-ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf
root@325032e6fdf3:/etc/apache2/sites-available#
```



```
# Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 17 23:01 •
root@074c8fe89635:/etc/apache2/sites-available
GNU nano 4.8
<VirtualHost *:443>
  DocumentRoot /var/www/anthaneni2025
  ServerName www.ananthaneni2025.com
  ServerAlias www.ananthaneni2025A.com
  ServerAlias www.ananthaneni2025B.com
  DirectoryIndex index.html
  SSLEngine On
  SSLCertificateFile /certs/server.crt
  SSLCertificateKeyFile /certs/server.key
</VirtualHost>

# Set the following global entry to suppress an annoying warning message
ServerName localhost
```

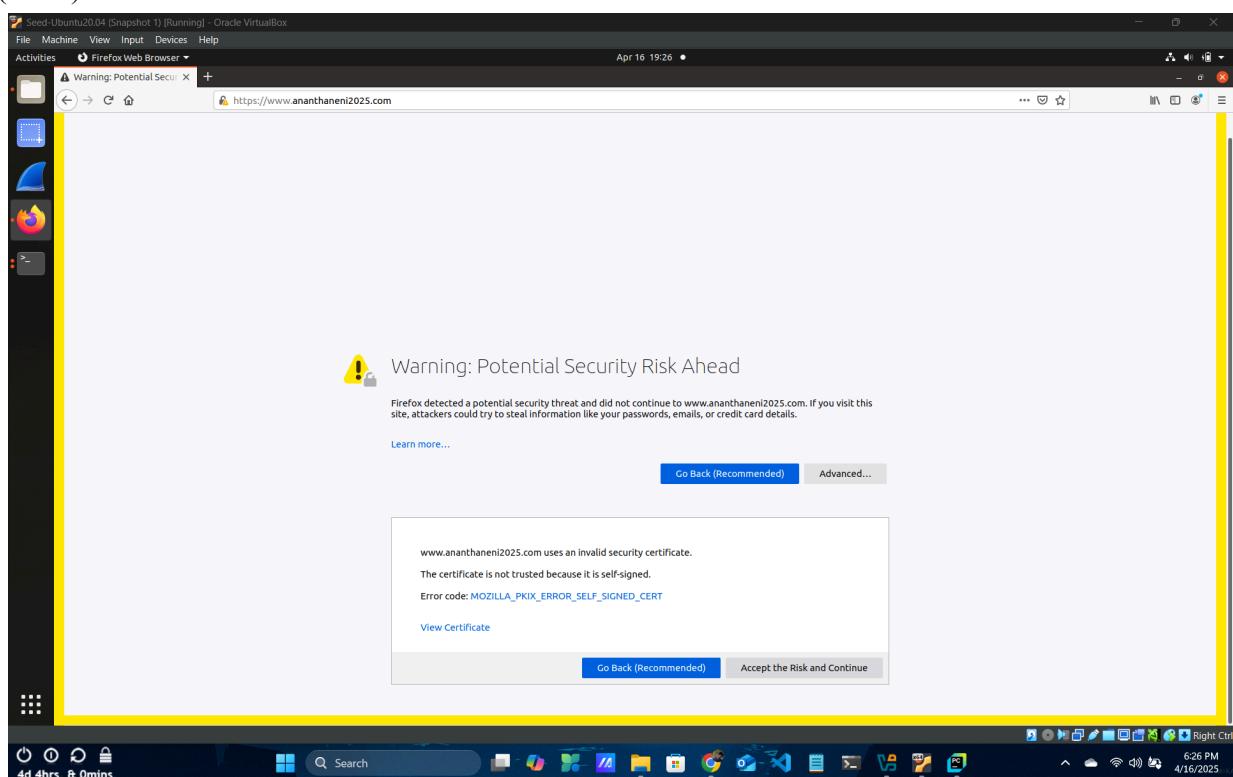


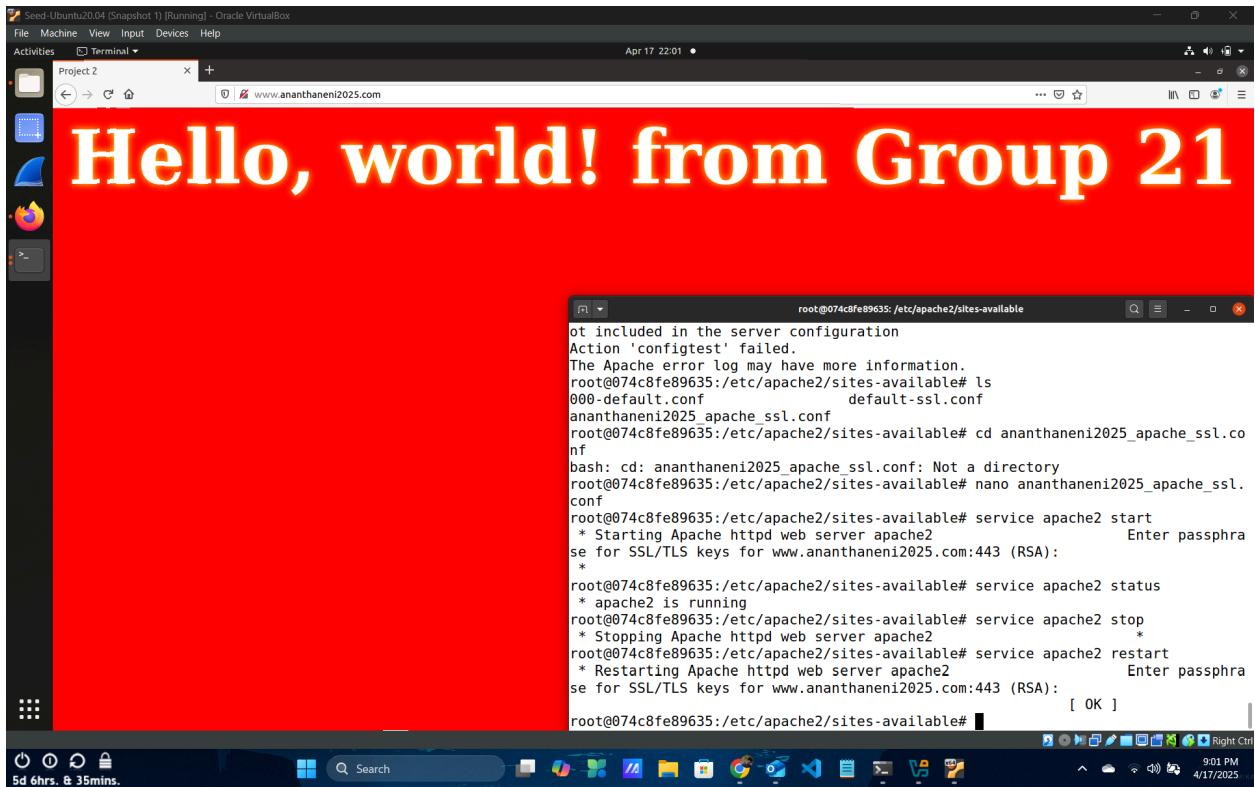
Also, we have made sure the server files are stored in the respective directories, enabled the Apache's ssl module and then enabled our site to make the website work

Restarted the Apache server and pinged our website to confirm the connectivity

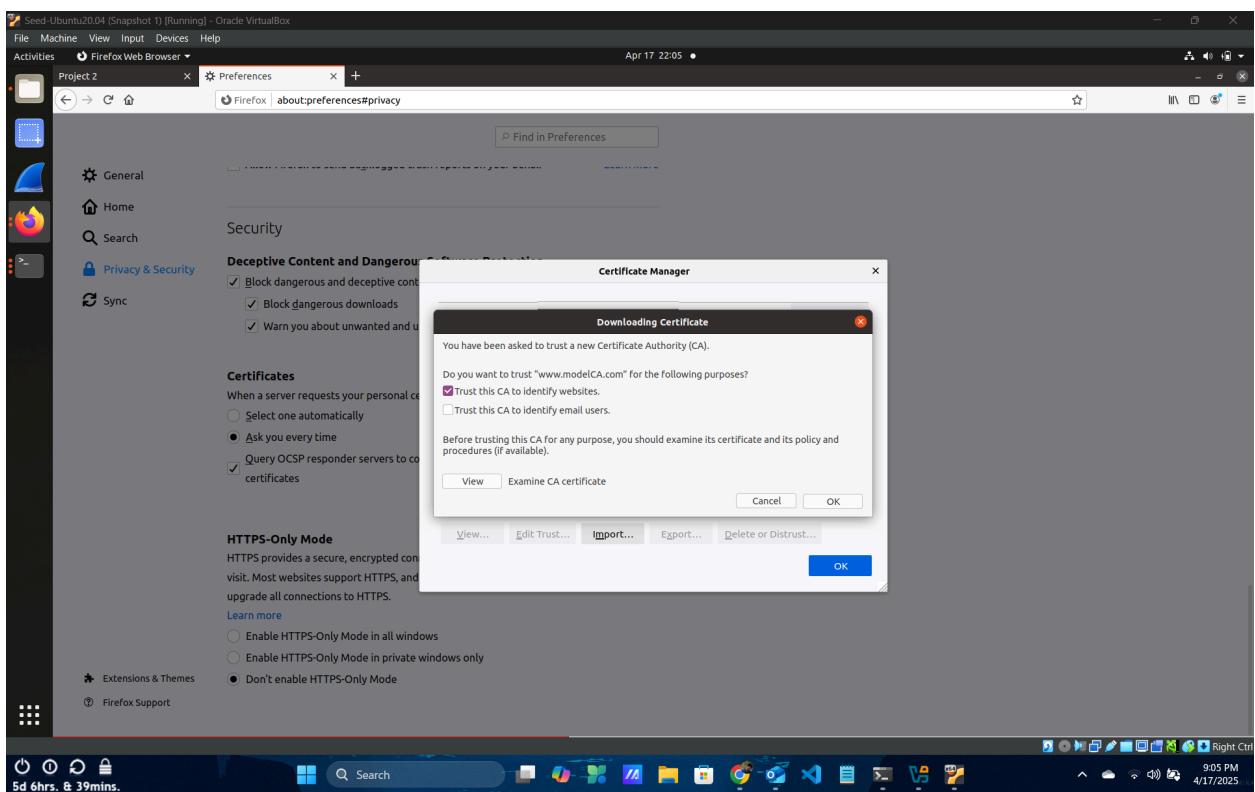
```
root@074c8fe89635:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2                                         Enter passphrase for SSL/TLS keys for www.ananthaneni2025.com:443 (RSA):
 [ OK ]
root@074c8fe89635:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf
root@074c8fe89635:/etc/apache2/sites-available# ping www.ananthaneni2025.com
PING www.ananthaneni2025.com (10.9.0.80) 56(84) bytes of data.
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=3 ttl=64 time=0.045 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=4 ttl=64 time=0.042 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=5 ttl=64 time=0.046 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=6 ttl=64 time=0.042 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=7 ttl=64 time=0.035 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=8 ttl=64 time=0.056 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=9 ttl=64 time=0.047 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=10 ttl=64 time=0.052 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=11 ttl=64 time=0.040 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=12 ttl=64 time=0.043 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=13 ttl=64 time=0.046 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=14 ttl=64 time=0.053 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=15 ttl=64 time=0.035 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=16 ttl=64 time=0.045 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=17 ttl=64 time=0.031 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=18 ttl=64 time=0.033 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=19 ttl=64 time=0.032 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=20 ttl=64 time=0.051 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=21 ttl=64 time=0.038 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=22 ttl=64 time=0.044 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=23 ttl=64 time=0.033 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=24 ttl=64 time=0.053 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=25 ttl=64 time=0.046 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=26 ttl=64 time=0.050 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=27 ttl=64 time=0.042 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=28 ttl=64 time=0.050 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=29 ttl=64 time=0.048 ms
`C
--- www.ananthaneni2025.com ping statistics ---
29 packets transmitted, 29 received, 0% packet loss, time 28658ms
```

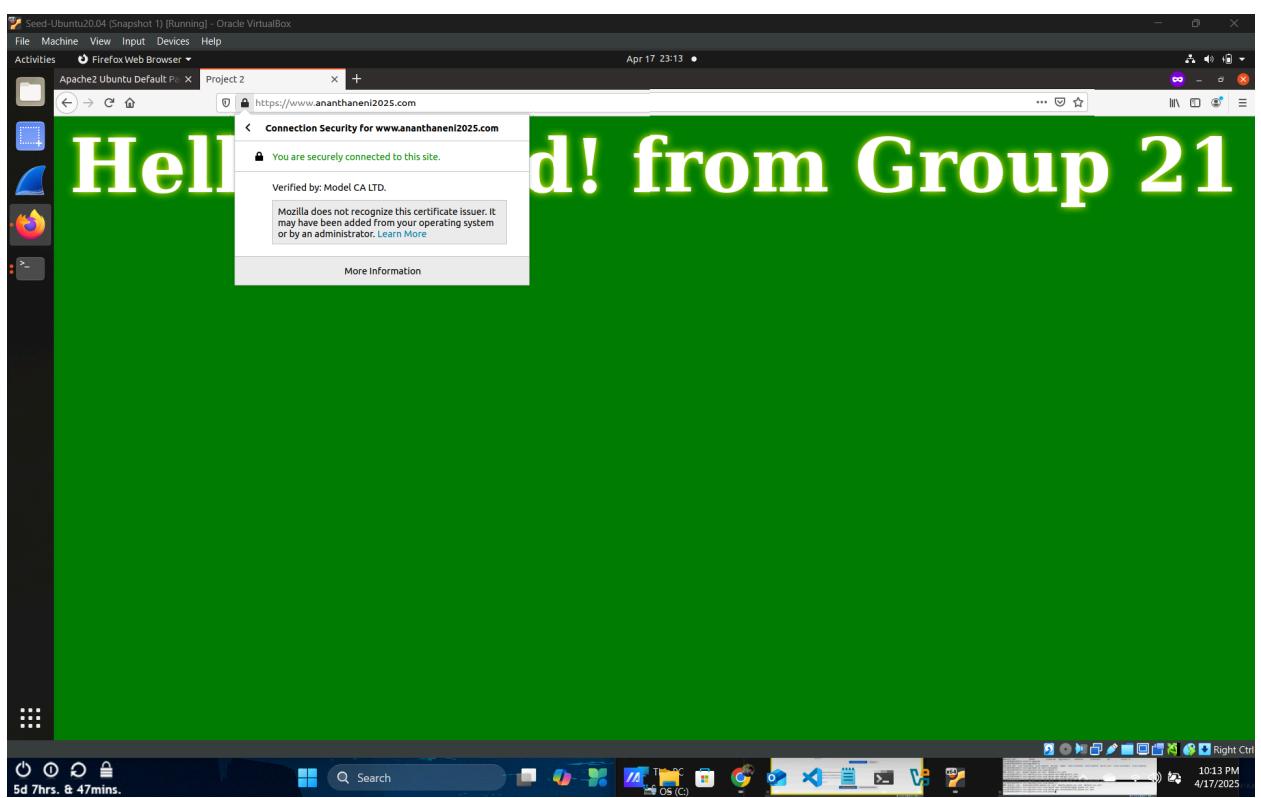
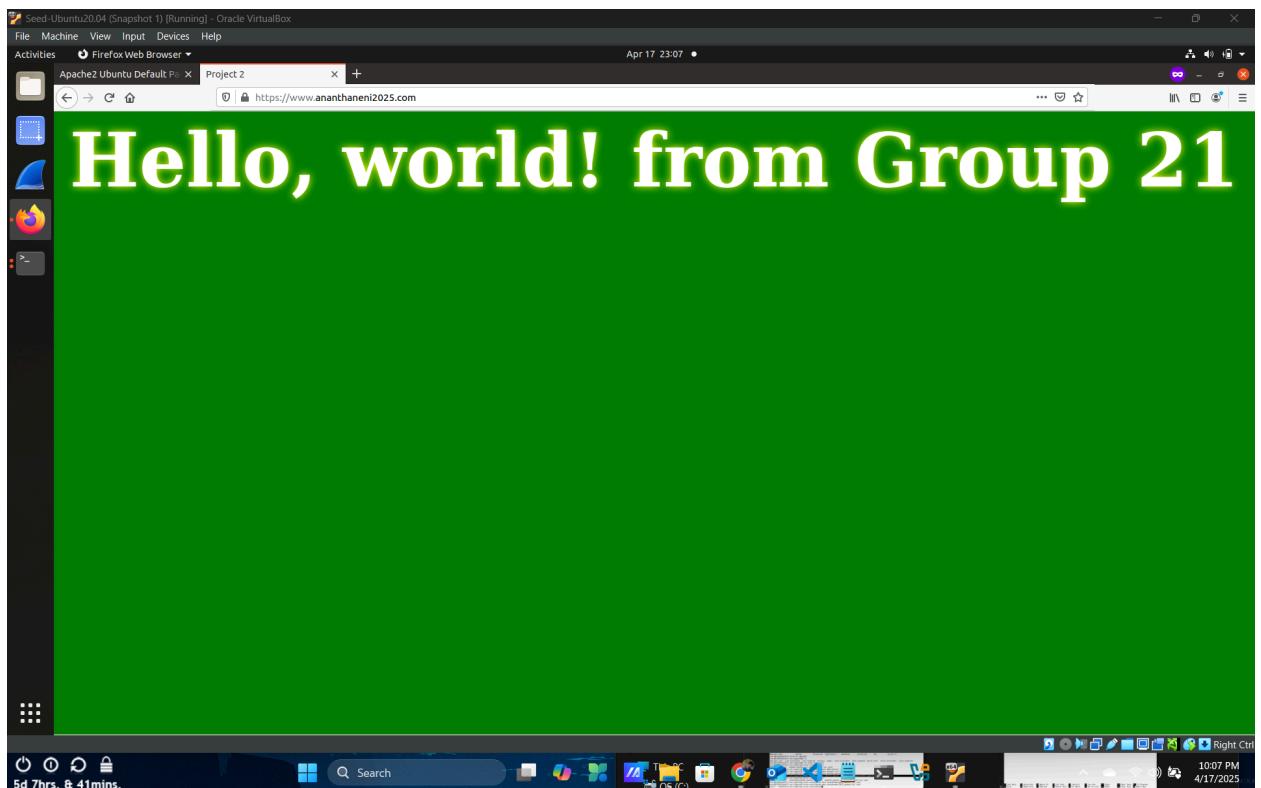
On accessing our website initially, browser said ‘untrusted certificate’ as it doesn’t trust our custom CA (ca.crt)





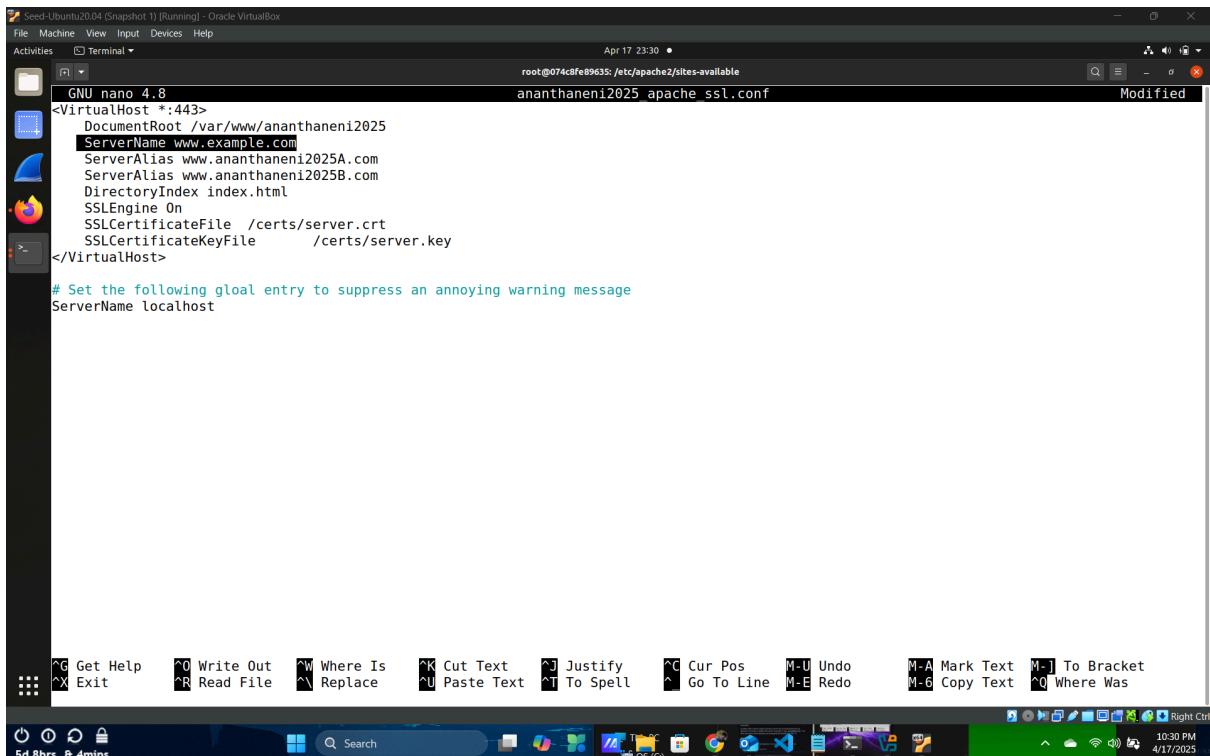
To fix this, we have imported our ca.crt into our browser as a Trusted Authority which made our connection secure





### 3.5 Task 5: Launching a Man-In-The-Middle Attack

Added a new VirtualHost entry for [www.example.com](http://www.example.com) for setting up the malicious website



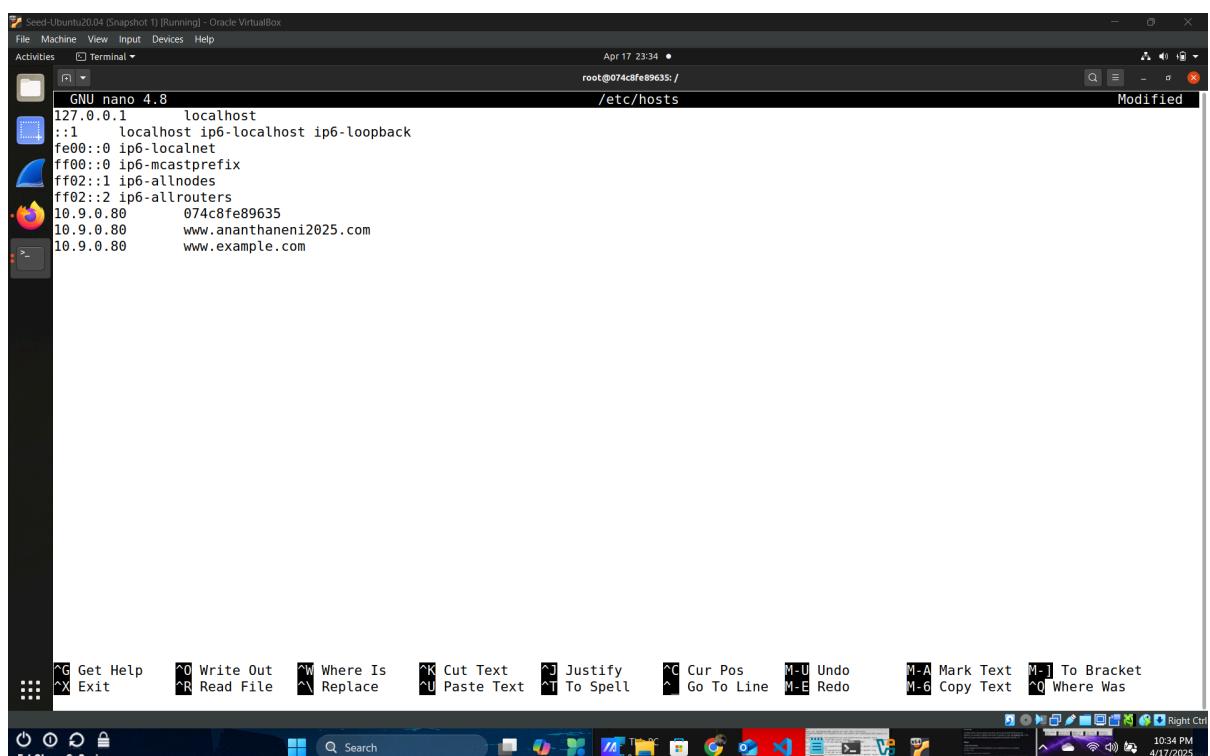
The screenshot shows a terminal window titled "Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox". The command "root@074c8fe89635:/etc/apache2/sites-available" is running. The terminal content is as follows:

```
GNU nano 4.8
<VirtualHost *:443>
    DocumentRoot /var/www/ananthaneni2025
    ServerName www.example.com
    ServerAlias www.ananthaneni2025A.com
    ServerAlias www.ananthaneni2025B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

# Set the following global entry to suppress an annoying warning message
ServerName localhost
```

The terminal has a standard nano editor keymap at the bottom.

Became the man in the middle through simulating DNS Spoofing by editing /etc/hosts file to map the real domain to our malicious web server's IP

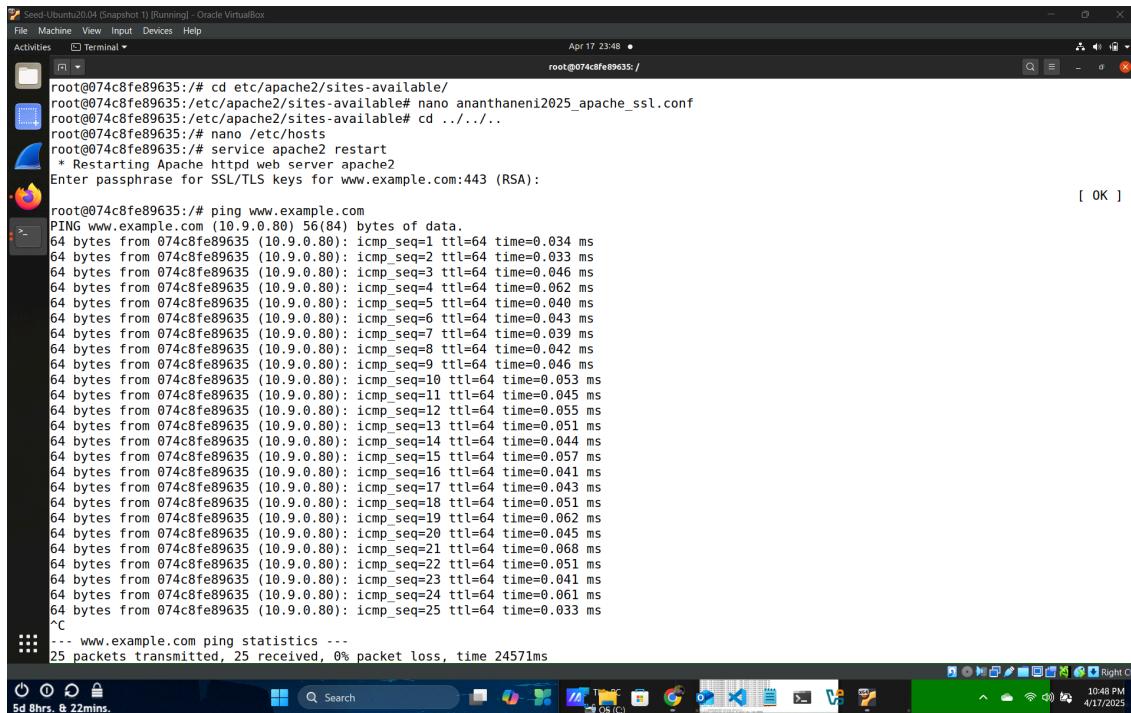


The screenshot shows a terminal window titled "Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox". The command "root@074c8fe89635:/etc/hosts" is running. The terminal content is as follows:

```
GNU nano 4.8
127.0.0.1      localhost
::1      localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.9.0.80      074c8fe89635
10.9.0.80      www.ananthaneni2025.com
10.9.0.80      www.example.com
```

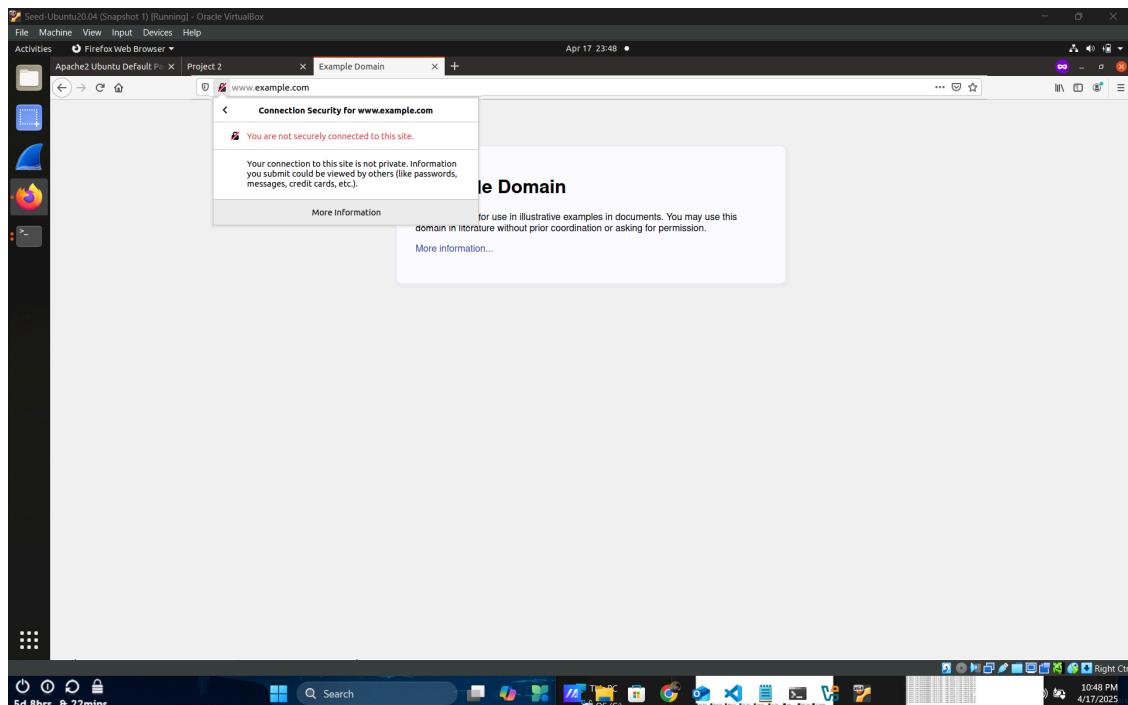
The terminal has a standard nano editor keymap at the bottom.

Restarted the Apache server and pinged the malicious website to confirm the connectivity



```
root@074c8fe89635:~# cd etc/apache2/sites-available/
root@074c8fe89635:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf
root@074c8fe89635:~# nano /etc/hosts
root@074c8fe89635:~# service apache2 restart
 * Restarting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.example.com:443 (RSA):
[ OK ]
root@074c8fe89635:~# ping www.example.com
PING www.example.com (10.9.0.80) 56(84) bytes of data.
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=3 ttl=64 time=0.046 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=4 ttl=64 time=0.062 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=5 ttl=64 time=0.040 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=6 ttl=64 time=0.043 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=7 ttl=64 time=0.039 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=8 ttl=64 time=0.042 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=9 ttl=64 time=0.046 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=10 ttl=64 time=0.053 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=11 ttl=64 time=0.045 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=12 ttl=64 time=0.055 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=13 ttl=64 time=0.051 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=14 ttl=64 time=0.044 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=15 ttl=64 time=0.057 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=16 ttl=64 time=0.041 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=17 ttl=64 time=0.043 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=18 ttl=64 time=0.051 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=19 ttl=64 time=0.062 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=20 ttl=64 time=0.045 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=21 ttl=64 time=0.068 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=22 ttl=64 time=0.051 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=23 ttl=64 time=0.041 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=24 ttl=64 time=0.061 ms
64 bytes from 074c8fe89635 (10.9.0.80): icmp_seq=25 ttl=64 time=0.033 ms
^C
--- www.example.com ping statistics ---
25 packets transmitted, 25 received, 0% packet loss, time 24571ms

```

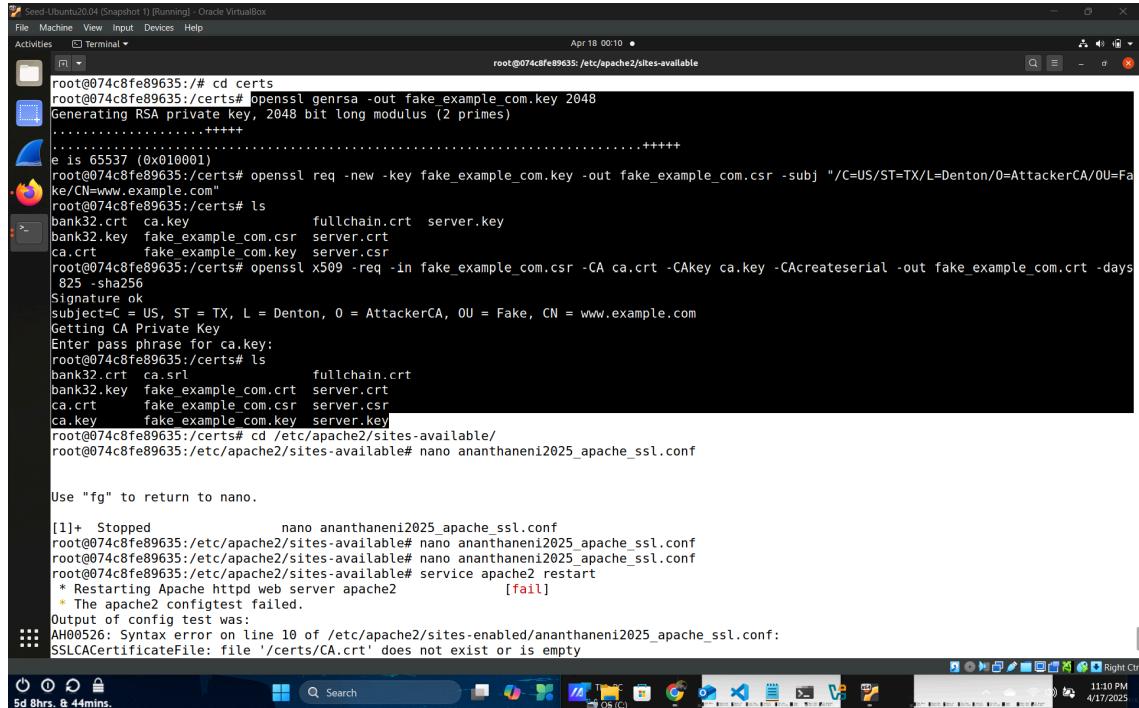


When we tried to visit <https://www.example.com>, the browser showed a security warning indicating that the connection was not private. This is because the fake server's certificate was not issued by a trusted certificate authority (CA) for the real domain. The browser detected that the certificate did not match the domain, preventing a successful MITM attack. This demonstrates how PKI protects users by validating server certificates and preventing attackers from impersonating legitimate websites.

### 3.6 Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

In Task 1, we have already created our own CA. Now, we simulate that this CA has been compromised by generating a certificate for mailicious site ([www.example.com](http://www.example.com))

Generated a key and CSR for this malicious site and used the compromised CA to sign it

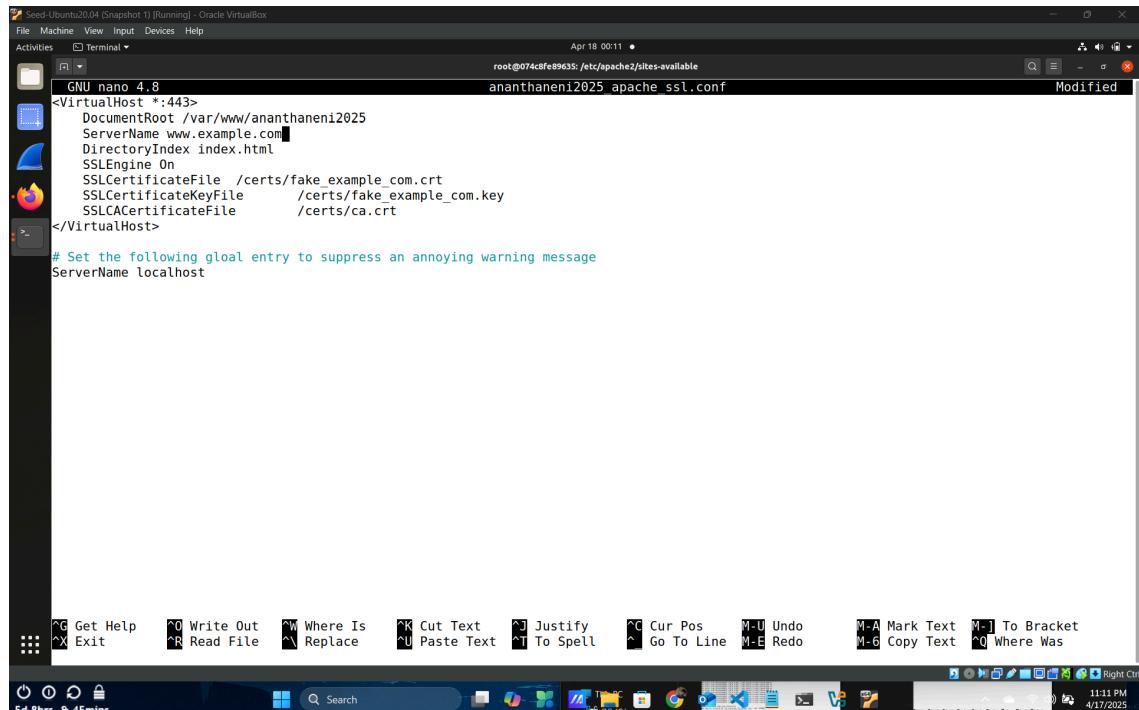


```
root@074c8fe89635:~# cd certs
root@074c8fe89635:certs# openssl genrsa -out fake_example_com.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x10001)
root@074c8fe89635:certs# openssl req -new -key fake_example_com.key -out fake_example_com.csr -subj "/C=US/ST=TX/L=Denton/O=AttackerCA/OU=Fake/CN=www.example.com"
root@074c8fe89635:certs# ls
bank32.crt ca.key fullchain.crt server.key
bank32.key fake_example_com.csr server.crt
ca.crt fake_example_com.key server.csr
root@074c8fe89635:certs# openssl x509 -req -in fake_example_com.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out fake_example_com.crt -days 825 -sha256
Signature ok
subject=C = US, ST = TX, L = Denton, O = AttackerCA, OU = Fake, CN = www.example.com
Getting CA Private Key
Enter pass phrase for ca.key:
root@074c8fe89635:certs# ls
bank32.crt ca.srl fullchain.crt
bank32.key fake_example_com.csr server.crt
ca.crt fake_example_com.key server.csr
ca.key fake_example_com.key server.key
root@074c8fe89635:certs# cd /etc/apache2/sites-available/
root@074c8fe89635:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf

Use "fg" to return to nano.

[1]+ Stopped                  nano ananthaneni2025_apache_ssl.conf
root@074c8fe89635:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf
root@074c8fe89635:/etc/apache2/sites-available# nano ananthaneni2025_apache_ssl.conf
root@074c8fe89635:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2 [fail]
 * The apache configtest failed.
Output of config test was:
AH00526: Syntax error on line 10 of /etc/apache2/sites-enabled/ananthaneni2025_apache_ssl.conf:
SSLCACertificateFile: file '/certs/CA.crt' does not exist or is empty
```

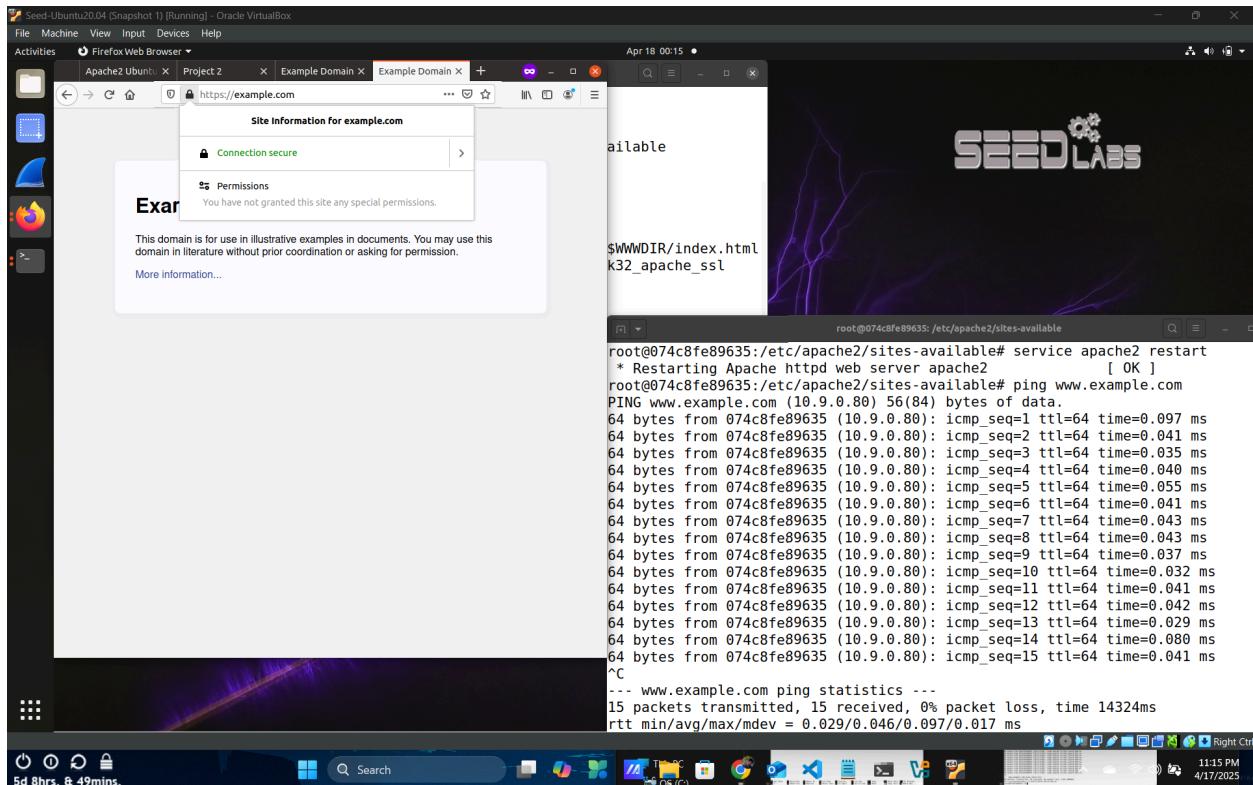
Updated the Apache VirtualHost config to use the new fake cert and key



```
GNU nano 4.8 ananthaneni2025_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/ananthaneni2025
    ServerName www.example.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/fake_example_com.crt
    SSLCertificateKeyFile /certs/fake_example_com.key
    SSLCACertificateFile /certs/ca.crt
</VirtualHost>

# Set the following global entry to suppress an annoying warning message
ServerName localhost
```

On restarting the Apache and visiting the target site (through DNS Hijack again), no browser warning appears (compromised CA certificate is already imported into our browser in previous task) and the fake certificate is trusted.



This demonstrates how an attacker with access to a CA's private key can impersonate any website completely bypassing PKI security mechanisms.

To mitigate Man-In-The-Middle (MITM) attacks caused by a compromised Certificate Authority (CA), several strategies can be employed:

- Certificate Transparency (CT) helps detect rogue certificates by maintaining a public log of all issued certificates
- HSTS (HTTP Strict Transport Security) ensures browsers only use HTTPS connections, preventing downgrade attacks
- OCSP and CRLs enable real-time revocation checks, though they may fail silently
- Certificate pinning (used cautiously) and CAA DNS records can limit which CAs are authorized to issue certificates for a domain

Together, these measures strengthen trust in HTTPS and reduce the impact of compromised CAs.