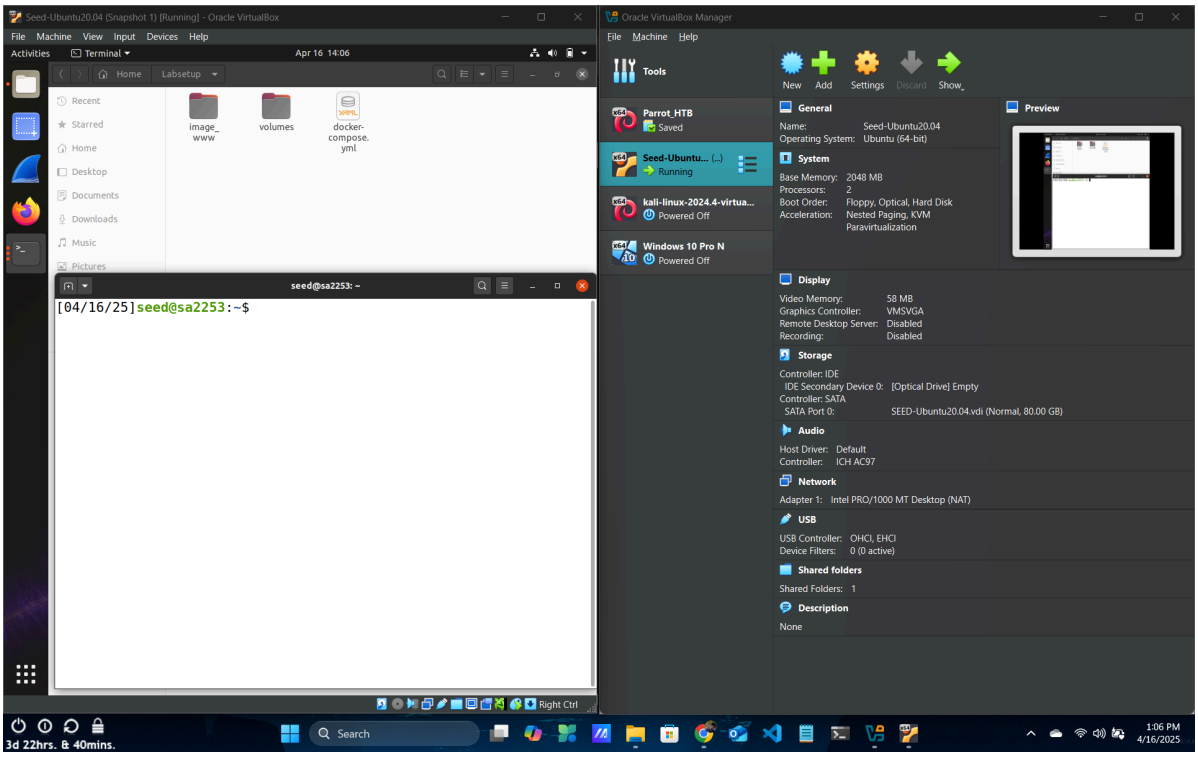
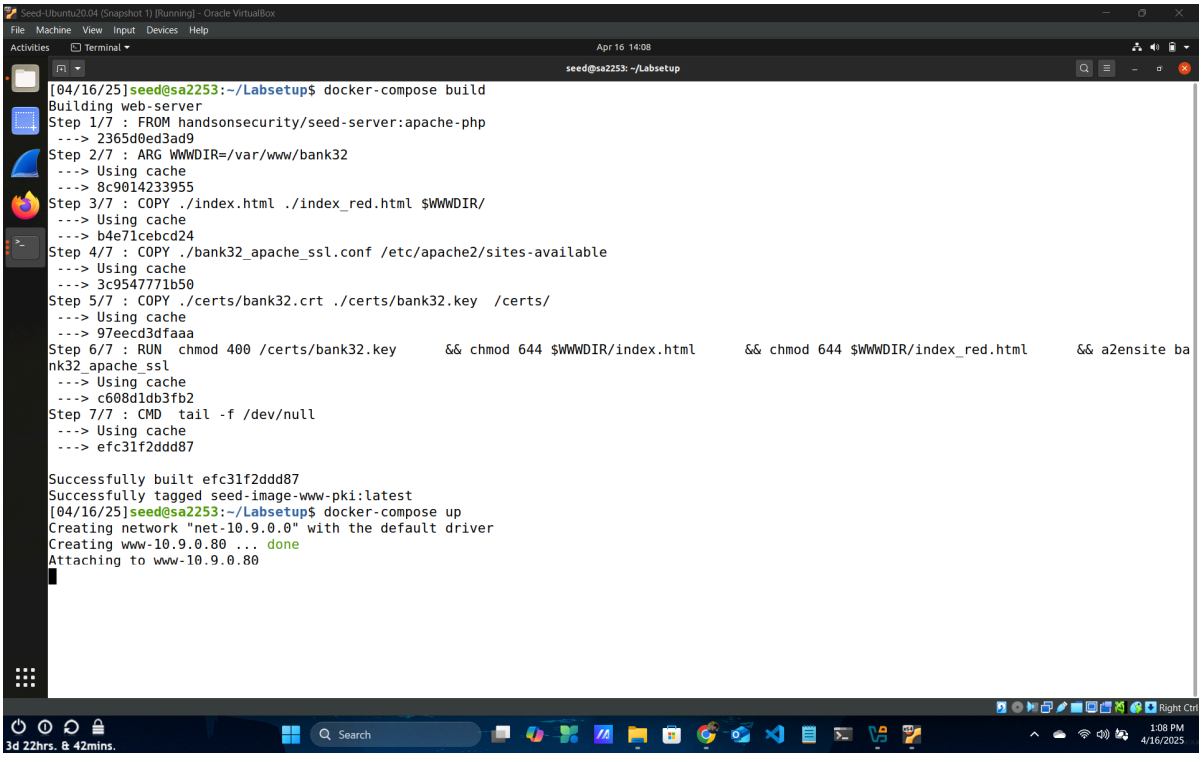
CSCE 4050/5050 - Project 2 “Public-Key Infrastructure (PKI) Lab”

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

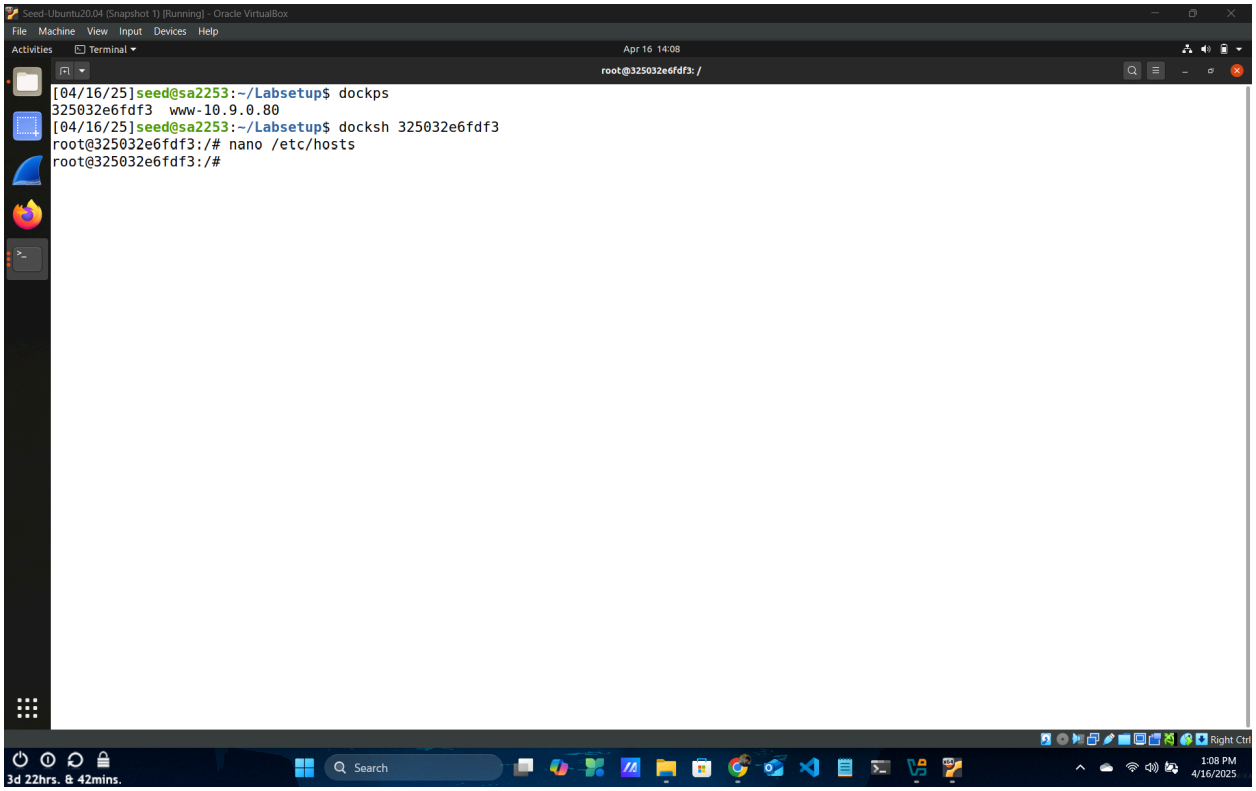
Lab Setup:



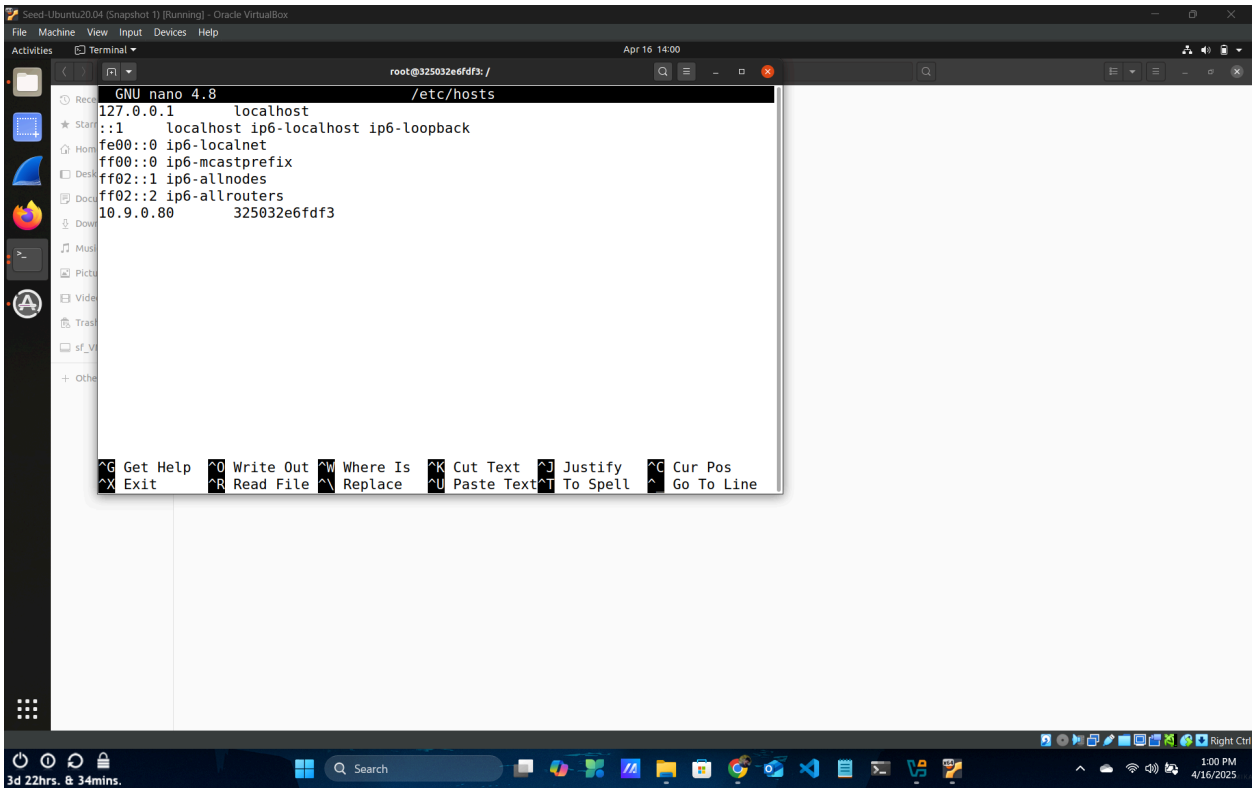
Building & starting the Docker container

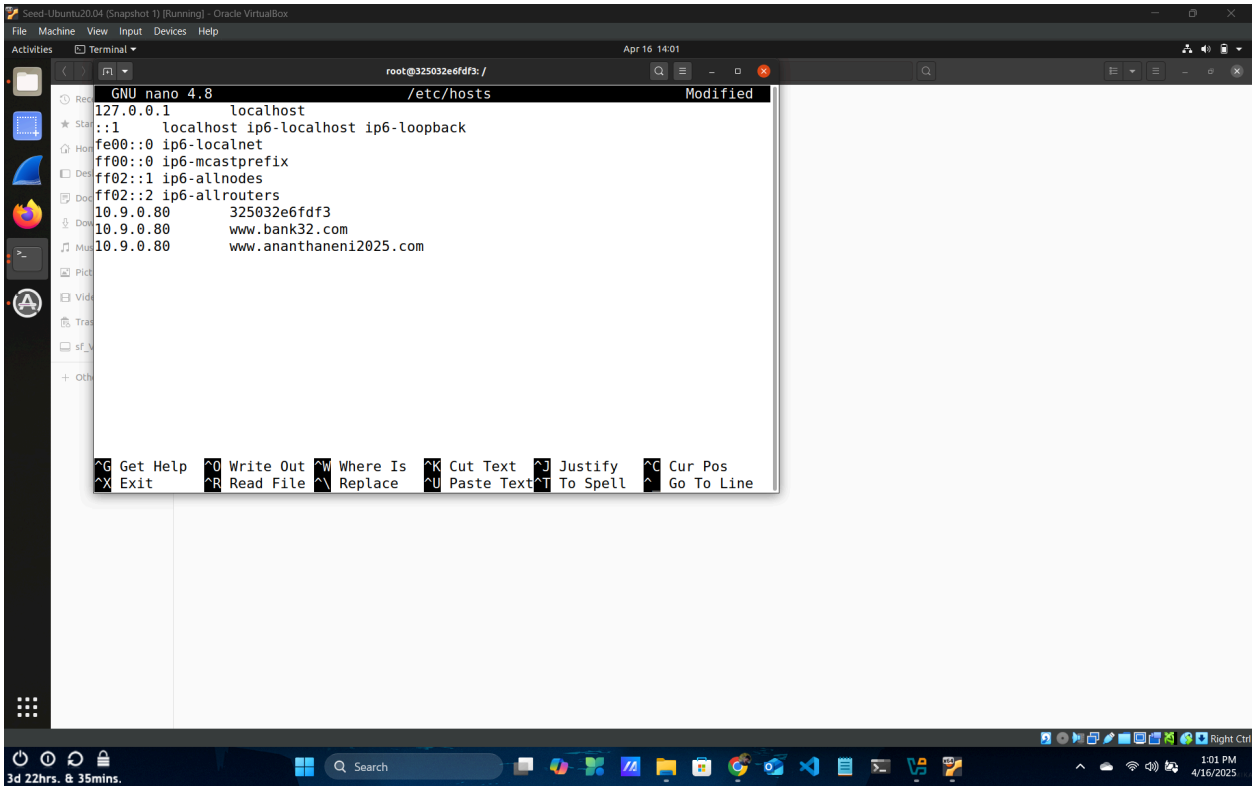


Getting into the shell

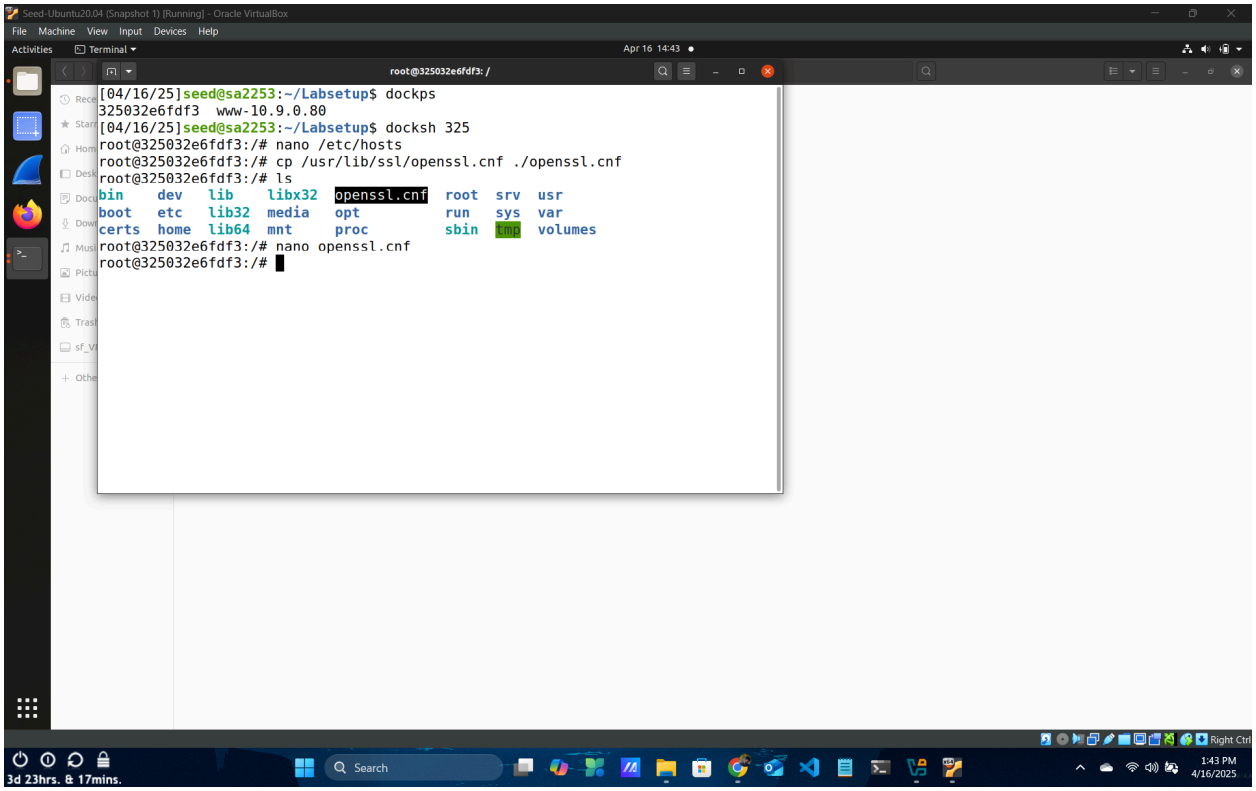


Adding server names

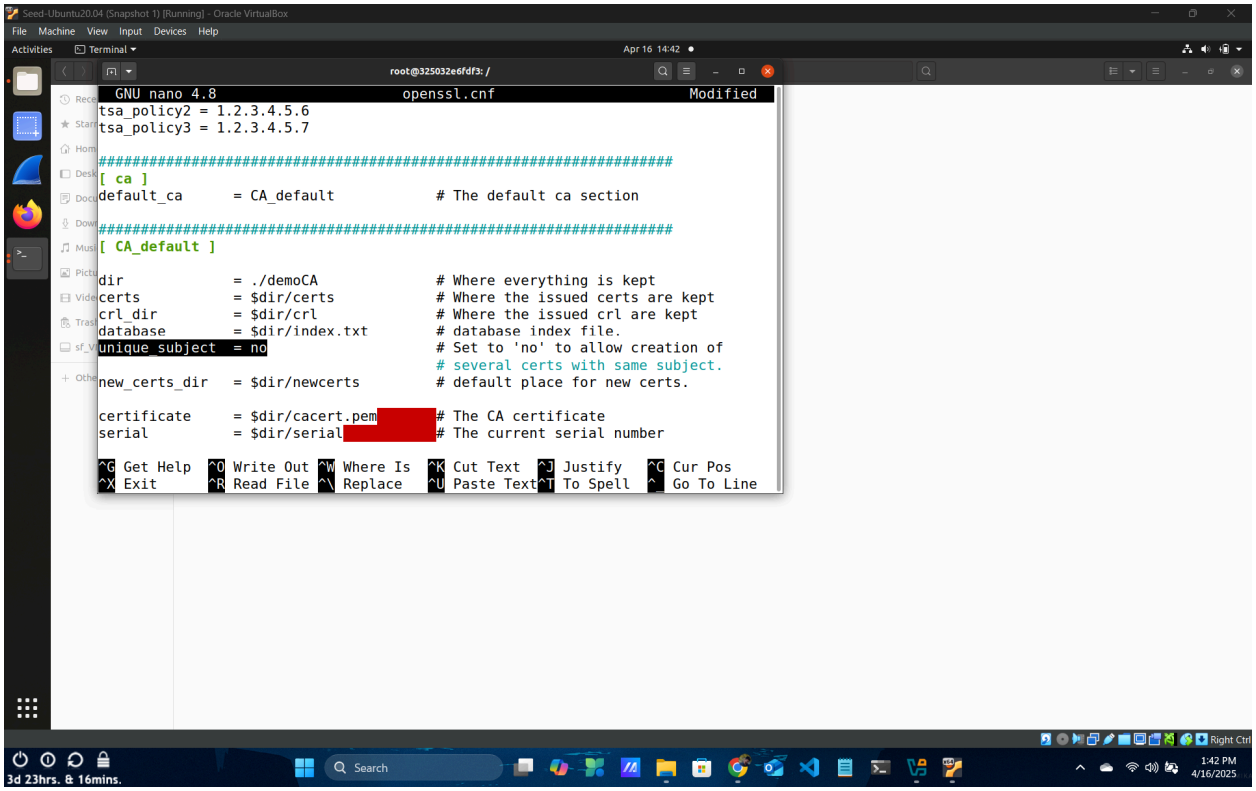




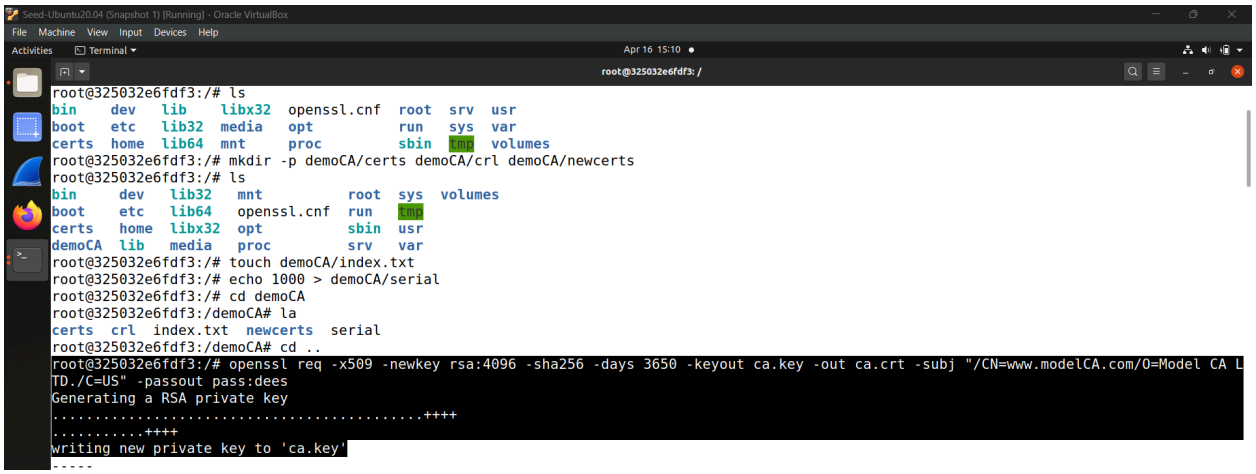
Task 1: Becoming a Certificate Authority (CA)



Allowing the creation of certifications with the same subject



Generating the self-signed certificate for the CA



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: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: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]

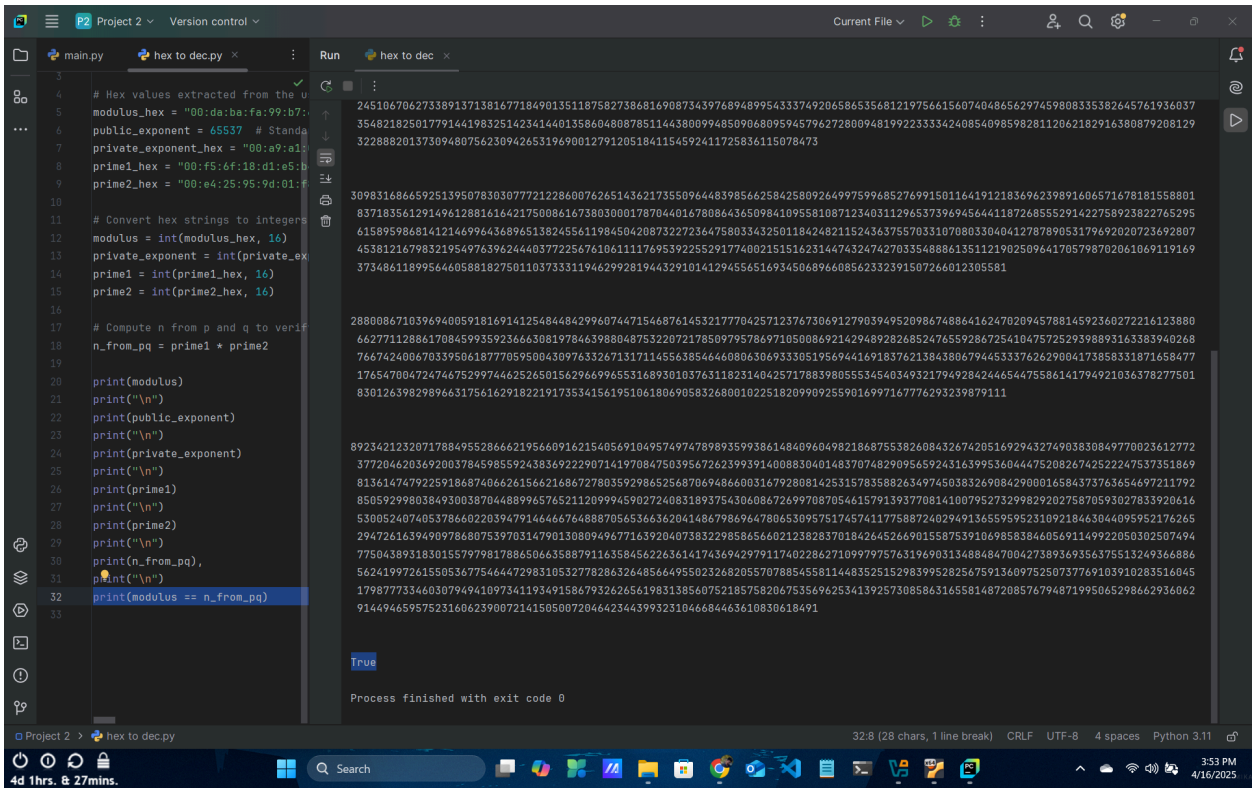
p =

```
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
```

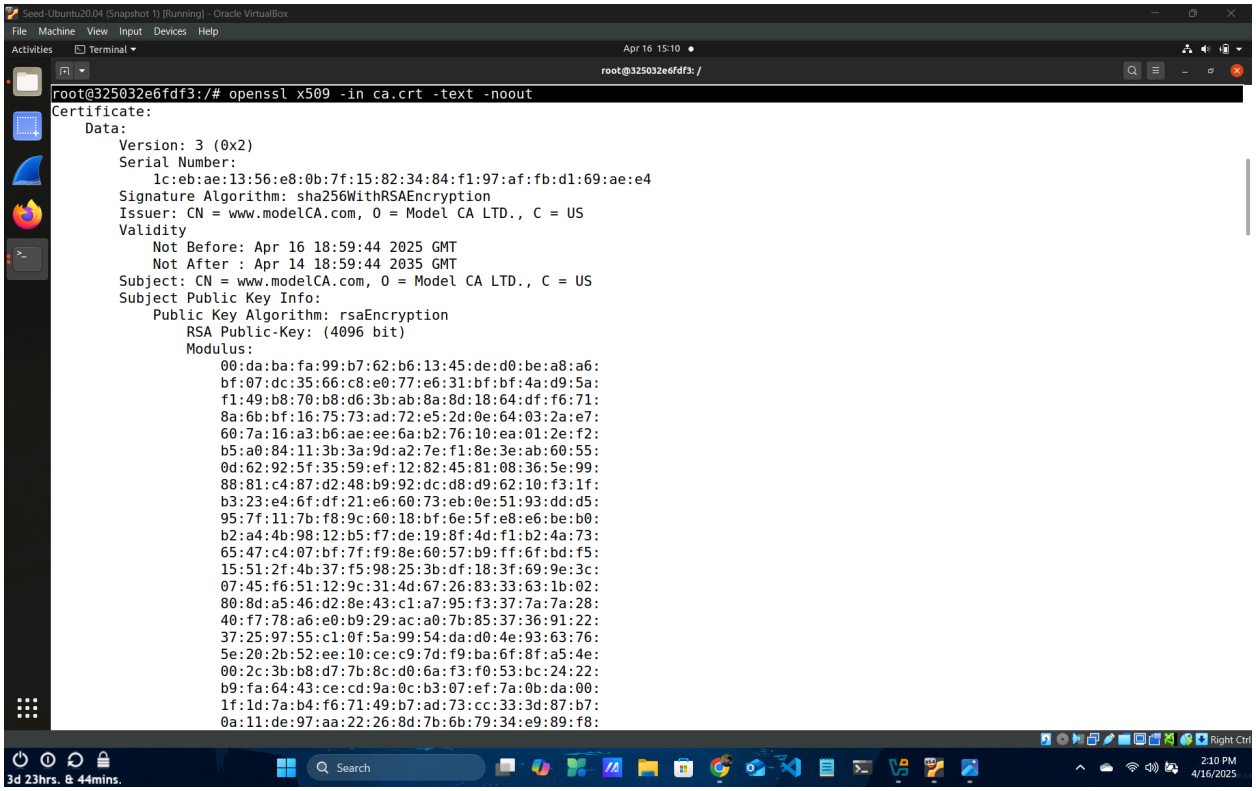
q =

```
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:2
1: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:b
6:17:69:72:44:1c: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:19:4
a: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
```

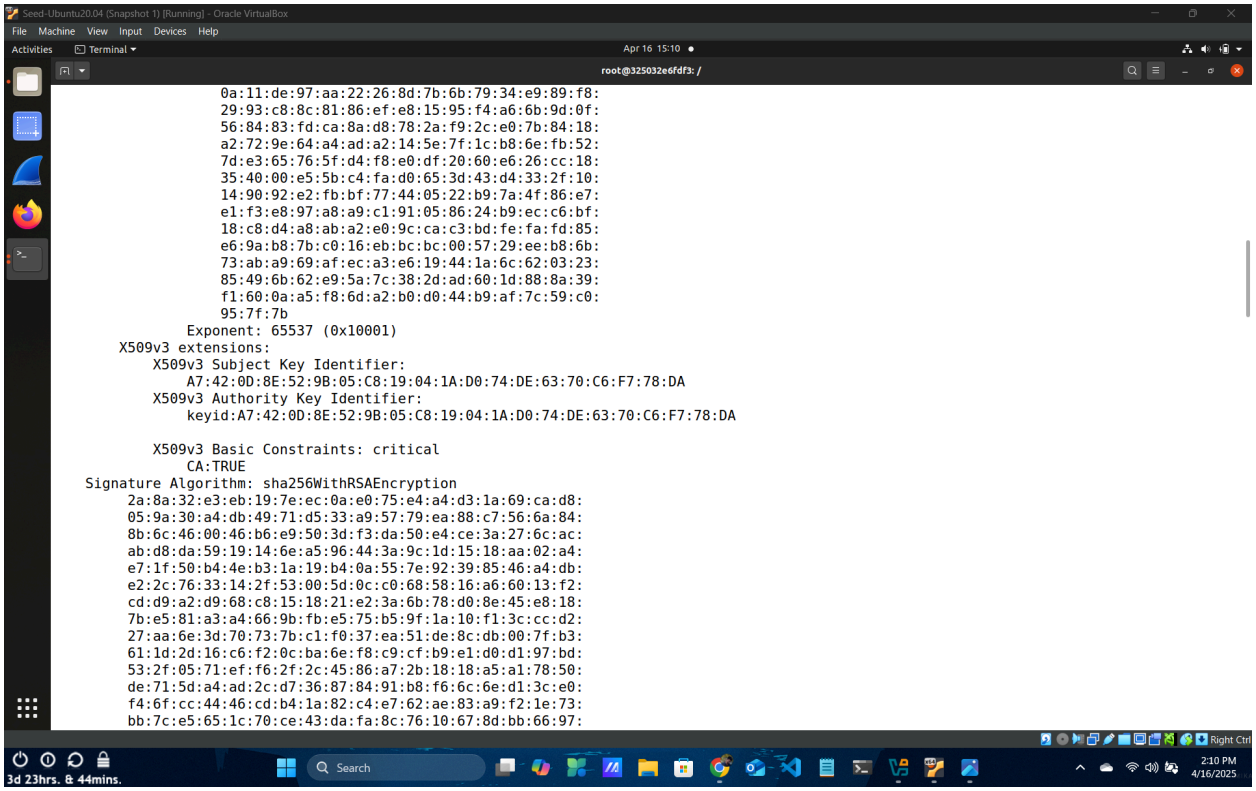
Used a simple Python program to convert these hexadecimal strings to integers, calculated & verified n = p x q



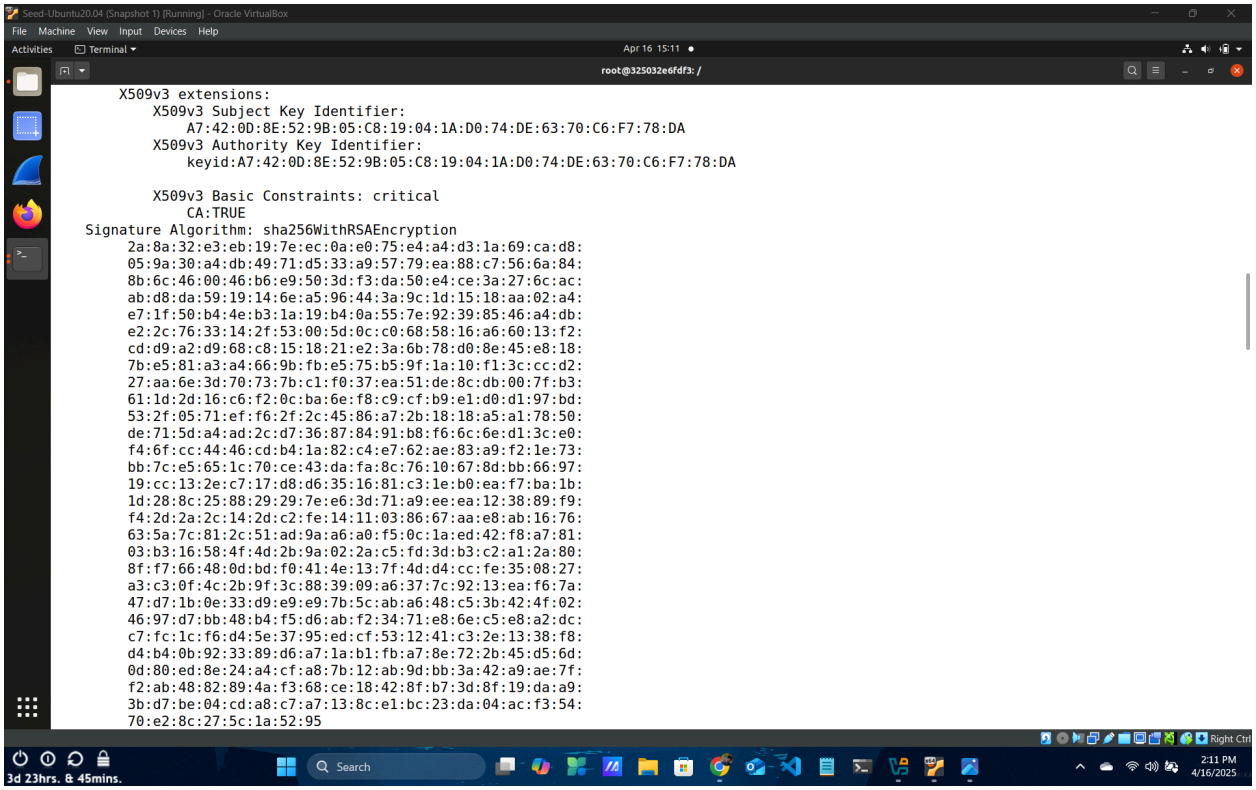
Looking at the decoded content of the X509 certificate



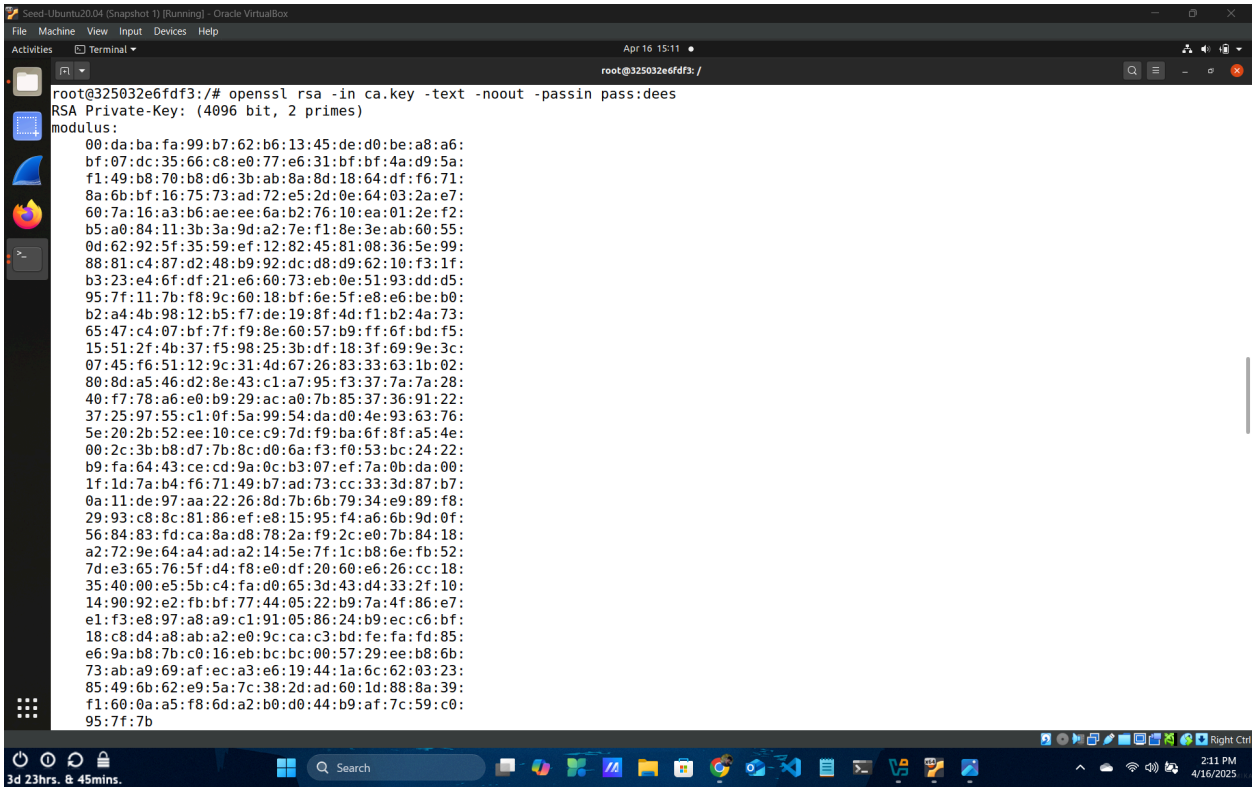
```
root@325032e6fdf3:/# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1c:eb:ae:13:56:e8:0b:7f:15:82:34:84:f1:97:af:fb:d1:69:ae:e4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model 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:b8: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:b2:76:10: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:12:82:45:81:08:36:5e: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:
                    95:7f: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:
```

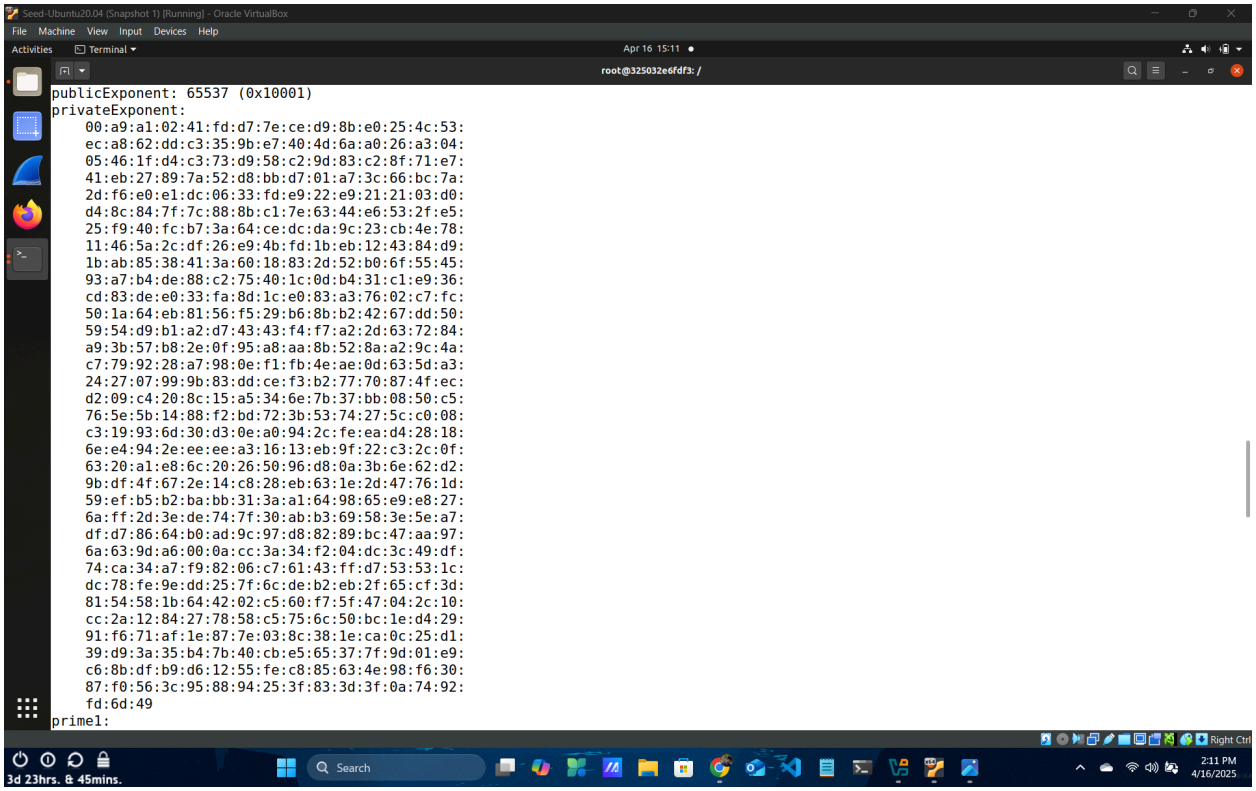


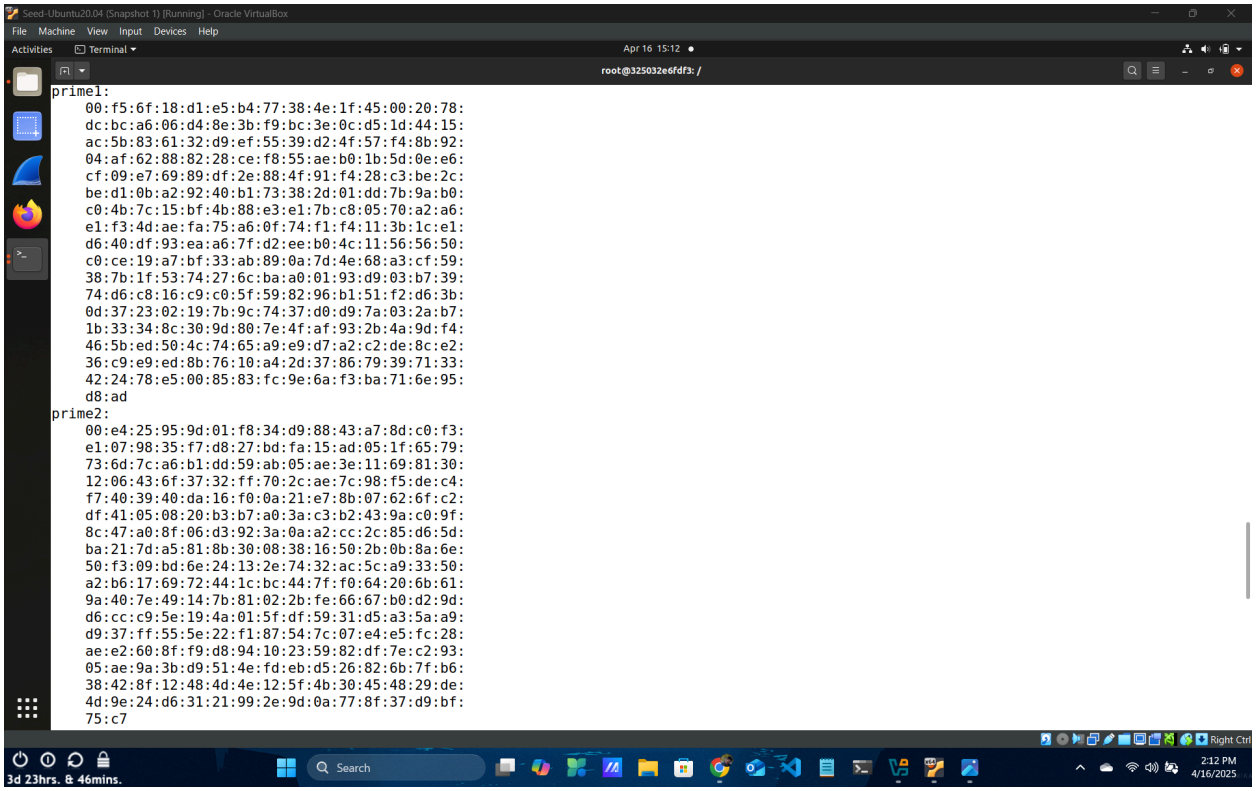
```
                    0a:11:de:97:aa:22:26:8d:7b:6b:79:34:e9:89:f8:
                    29:93:c8:8c:81:86:ef:e8:15:95:f4:a6:6b:9d:0f:
                    56:84:83:fd:ca:8a:d8:78:2a:f9:2c:e0:7b:84:18:
                    a2:72:9e:64:a4:ad:a2:14:5e:7f:1c:b8:6e:fb:52:
                    7d:e3:65:76:5f:d4:f8:e0:df:20:60:e6:26:cc:18:
                    35:40:00:e5:5b:c4:fa:d0:65:3d:43:d4:33:2f: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: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
                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: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:d8: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:
```

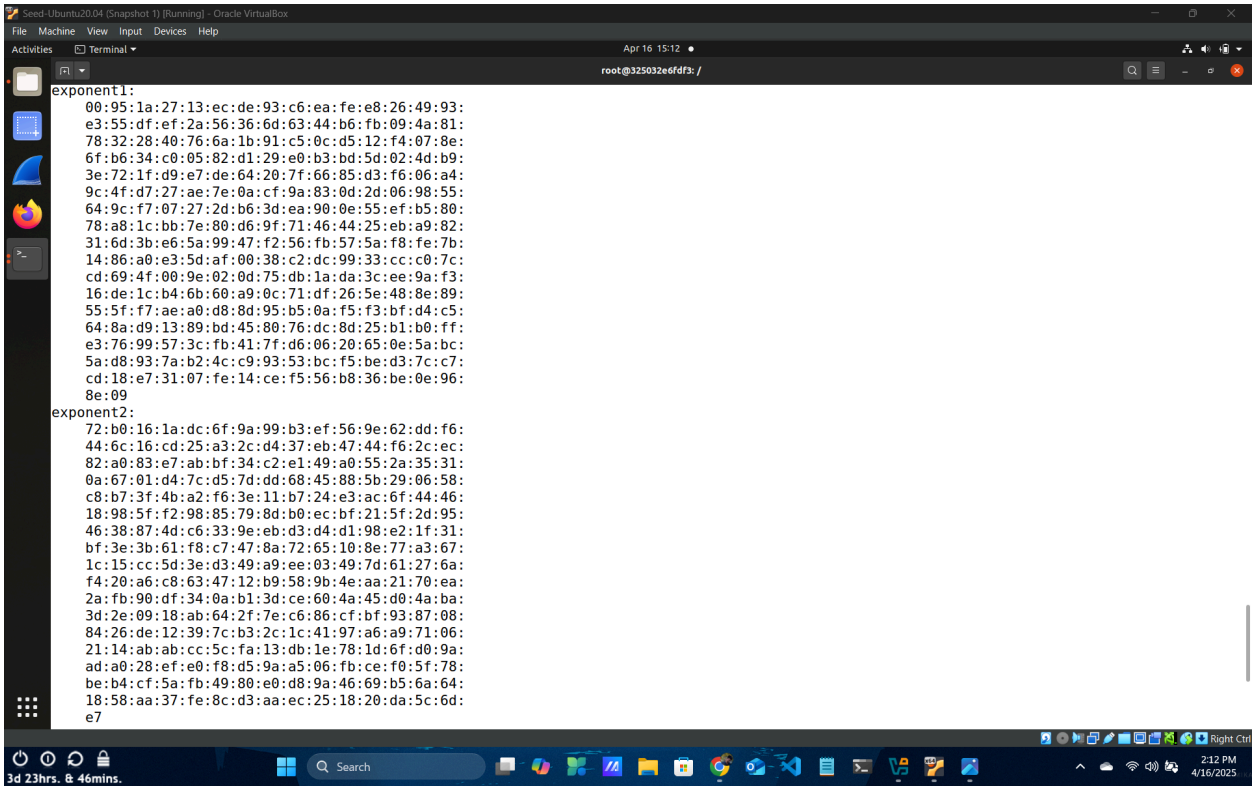


Looking at the decoded content of the RSA key

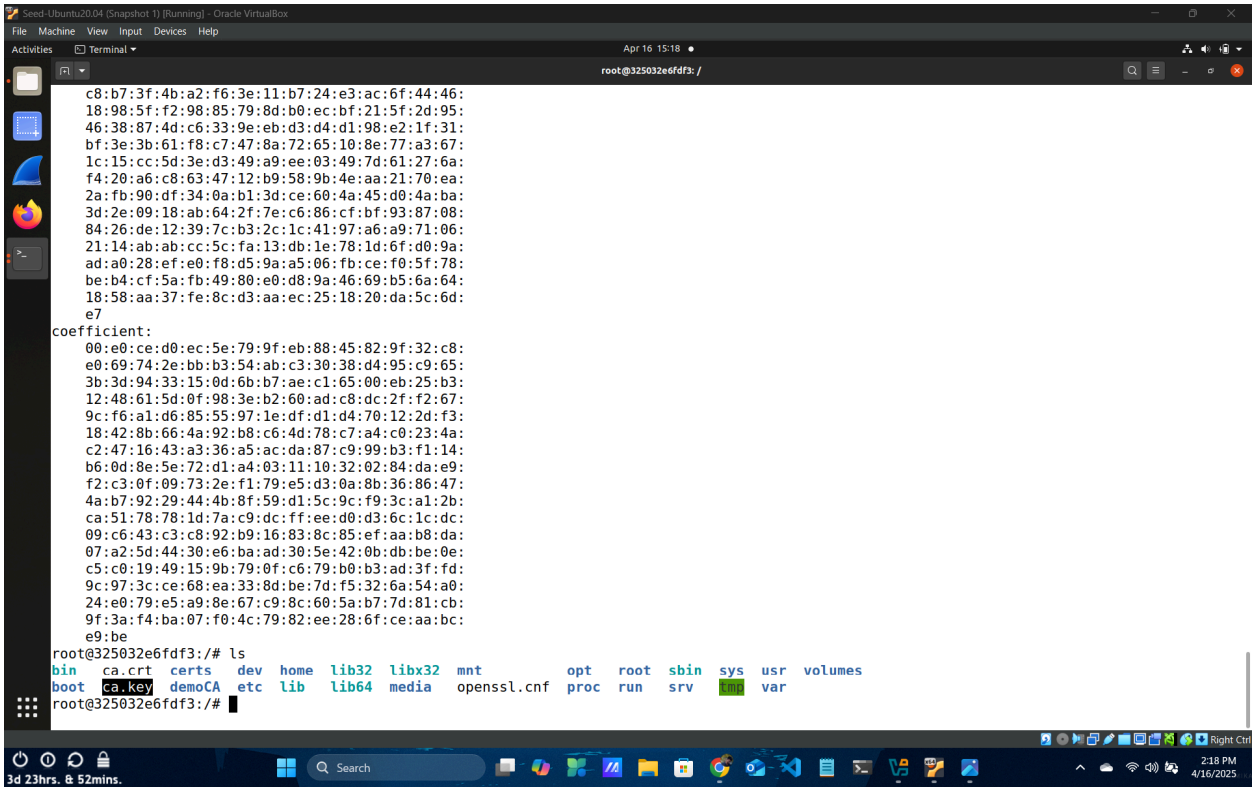



Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:11
root@325032e6fdf3: /
publicExponent: 65537 (0x10001)
privateExponent:
00:a9:a1:02:41:fd:d7:7e:ce:d9:8b:e0:25:4c:53:
ec:a8:62:dd:c3:35:9b:e7:40:4d:6a:a0:26:a3:04:
05:46:1f:d4:c3:73:d9:58:c2:9d:83:c2:8f:71:e7:
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:ce: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: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:
c3:19:93:6d: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:49
prime1:
Right Ctrl
3d 23hrs. & 45mins.
Search
2:11 PM
4/16/2025


Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 15:12
root@325032e6fdf3: /
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: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
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:
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
Right Ctrl
3d 23hrs. & 46mins.
Search
2:12 PM
4/16/2025



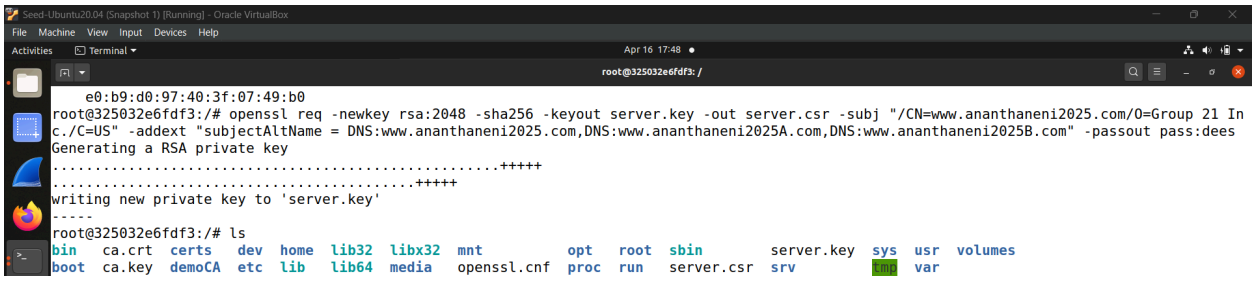
The file ca.key contains the CA's private key, while ca.crt contains the public-key certificate



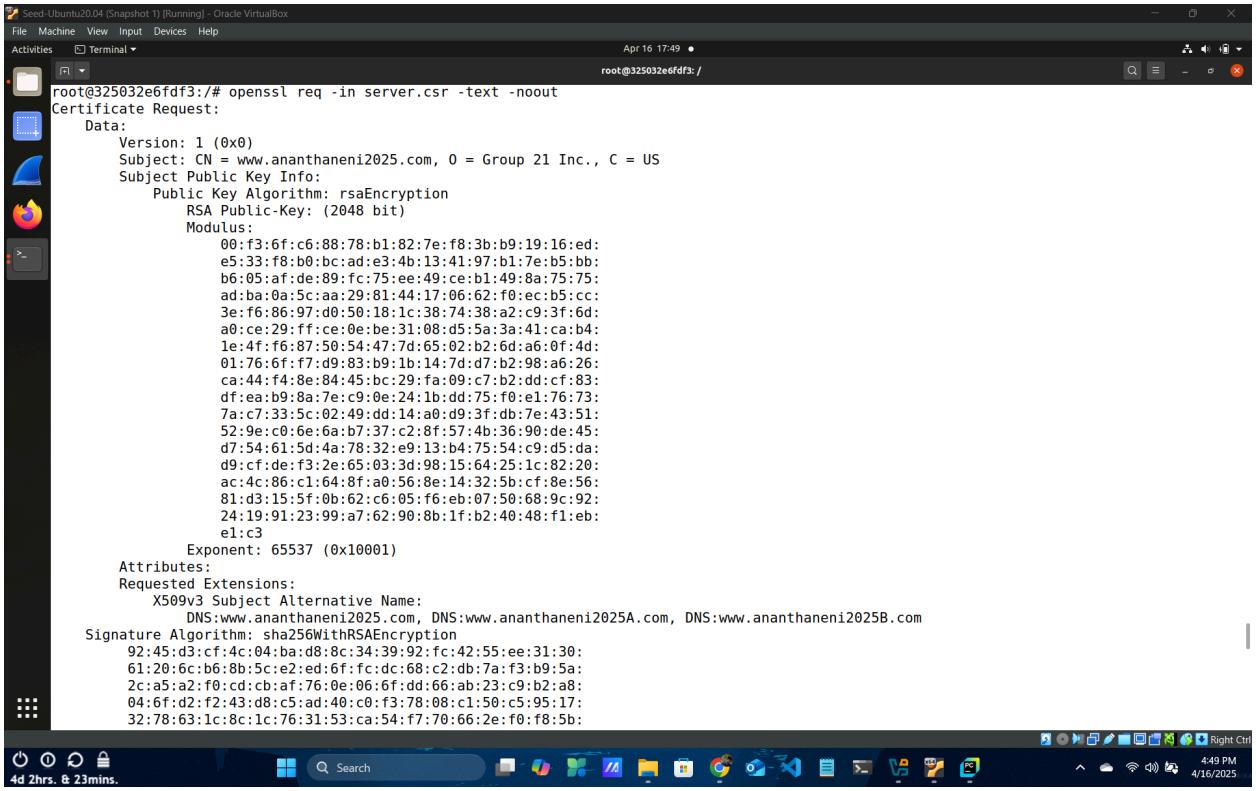
3.2 Task 2: Generating a Certificate Request for Your Web Server

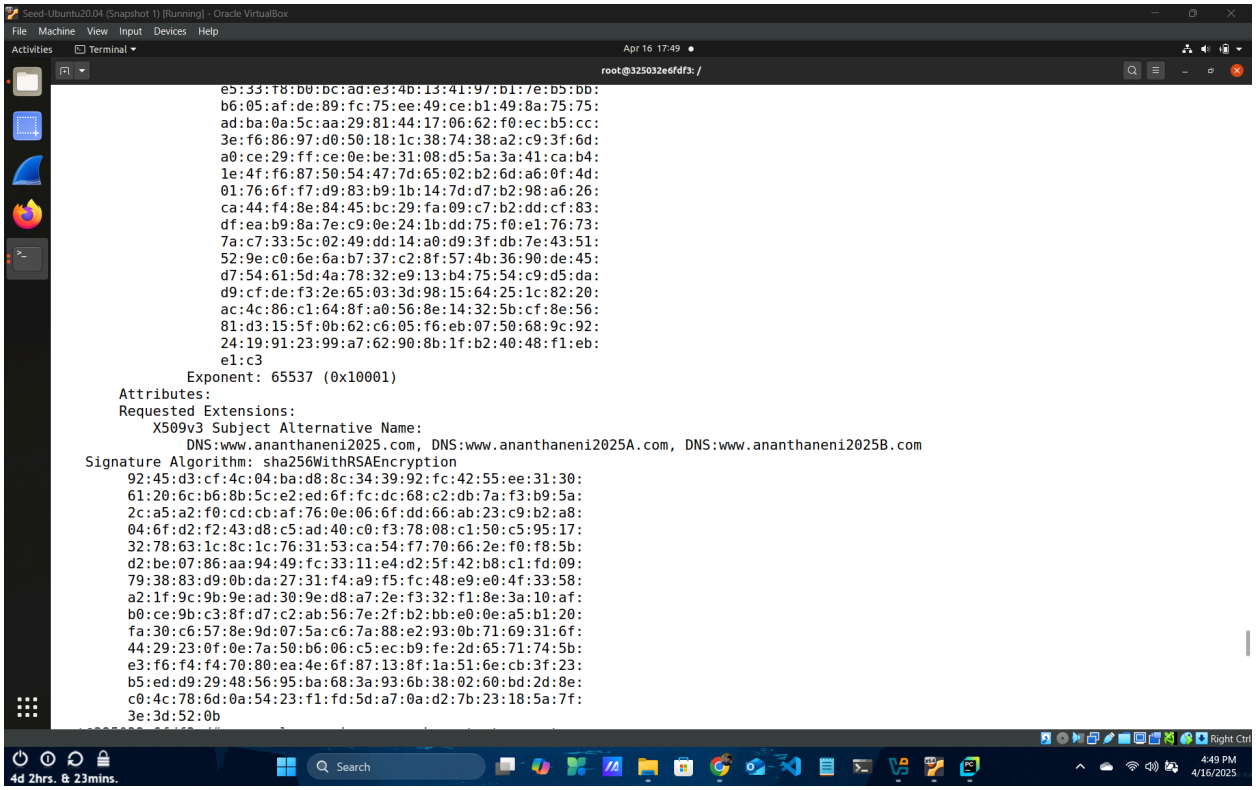
Generating a Certificate Signing Request for our servers (www.ananthaneni2025.com) by using SAN extensions to allow a certificate to have multiple names

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

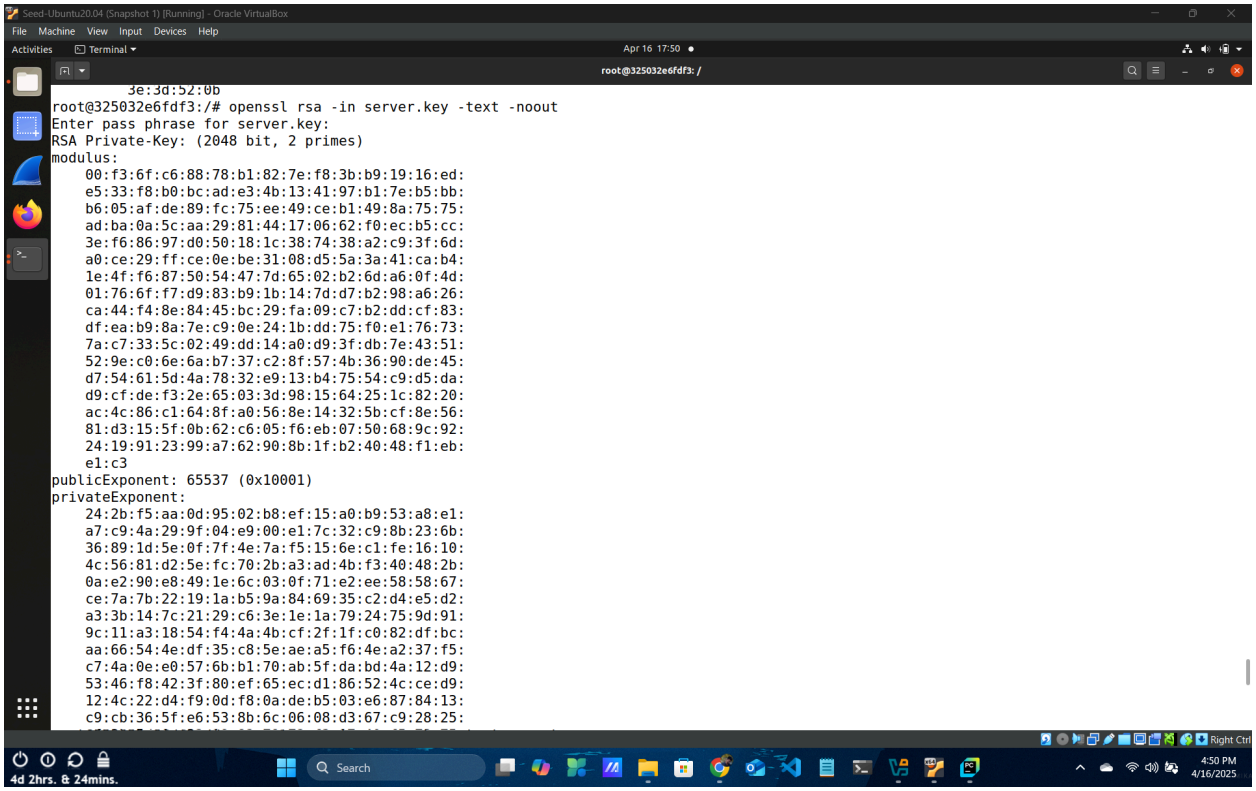


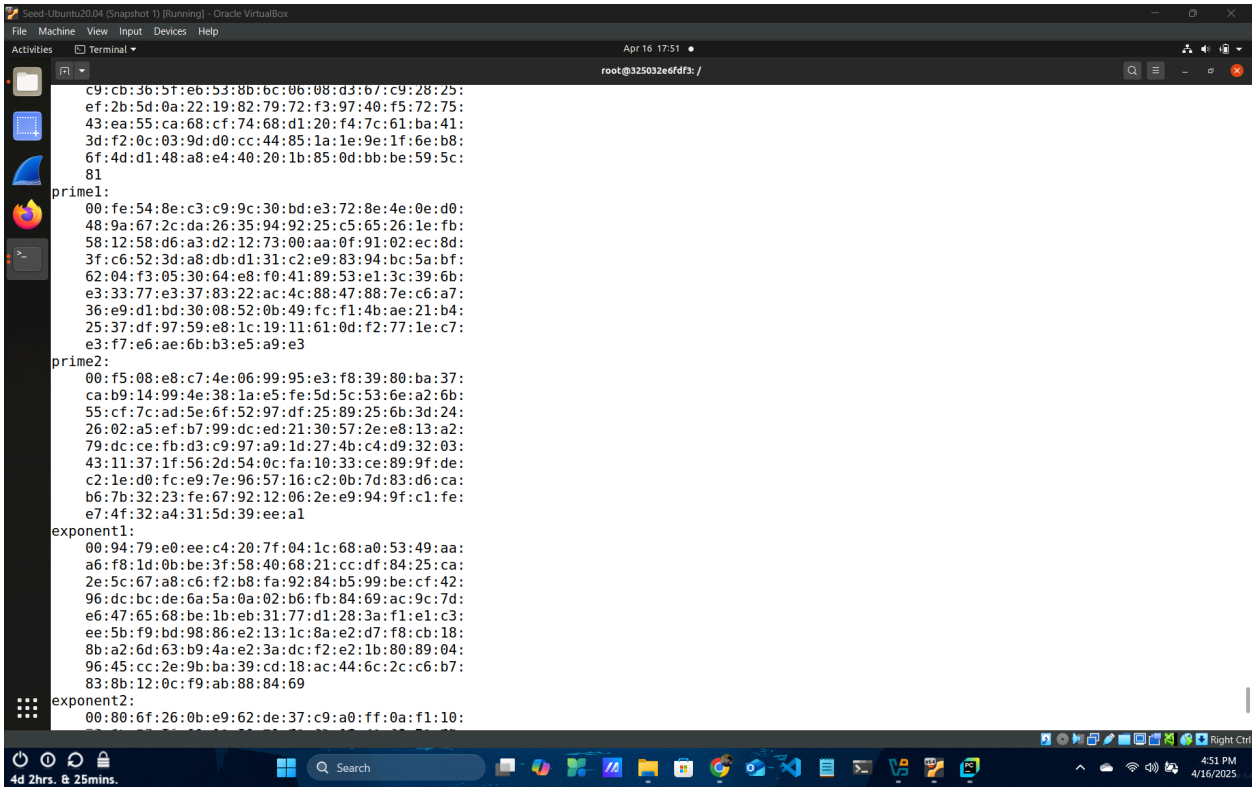
Looking at the decoded content of the CSR file

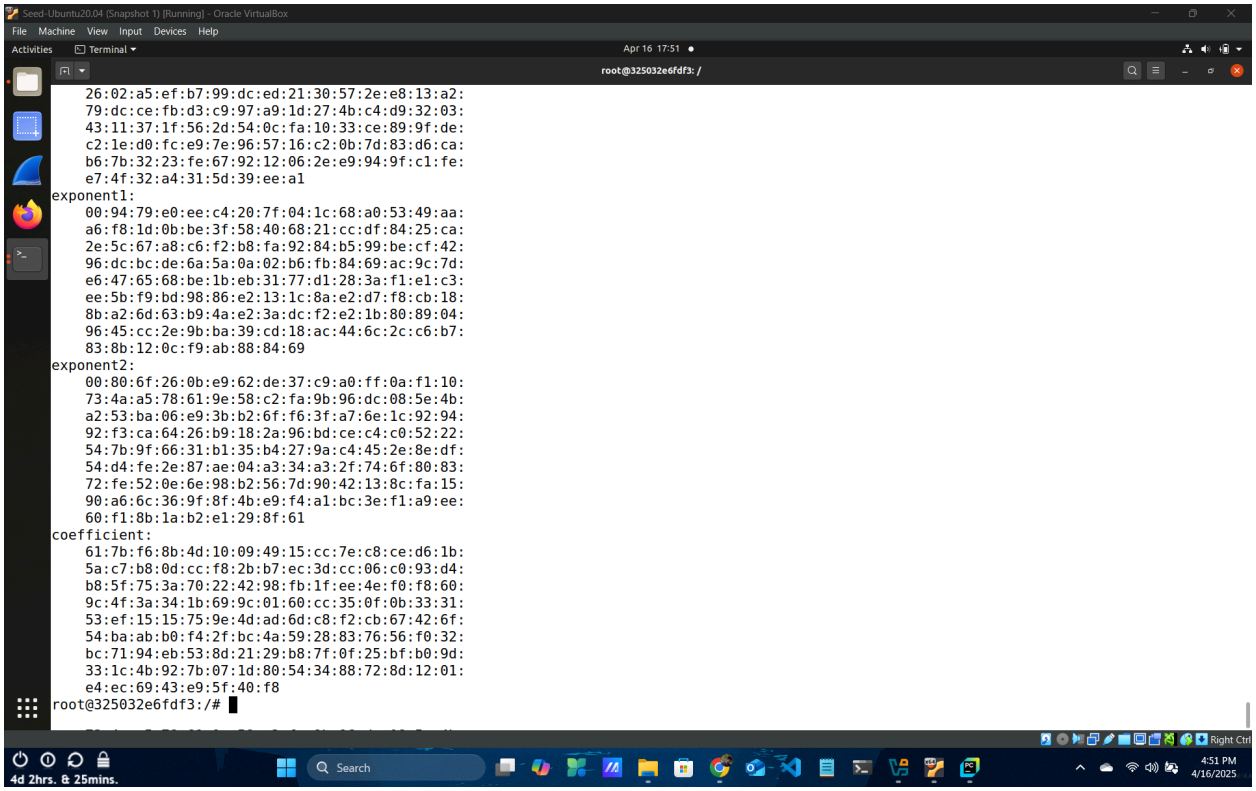




Looking at the decoded content of the private key file

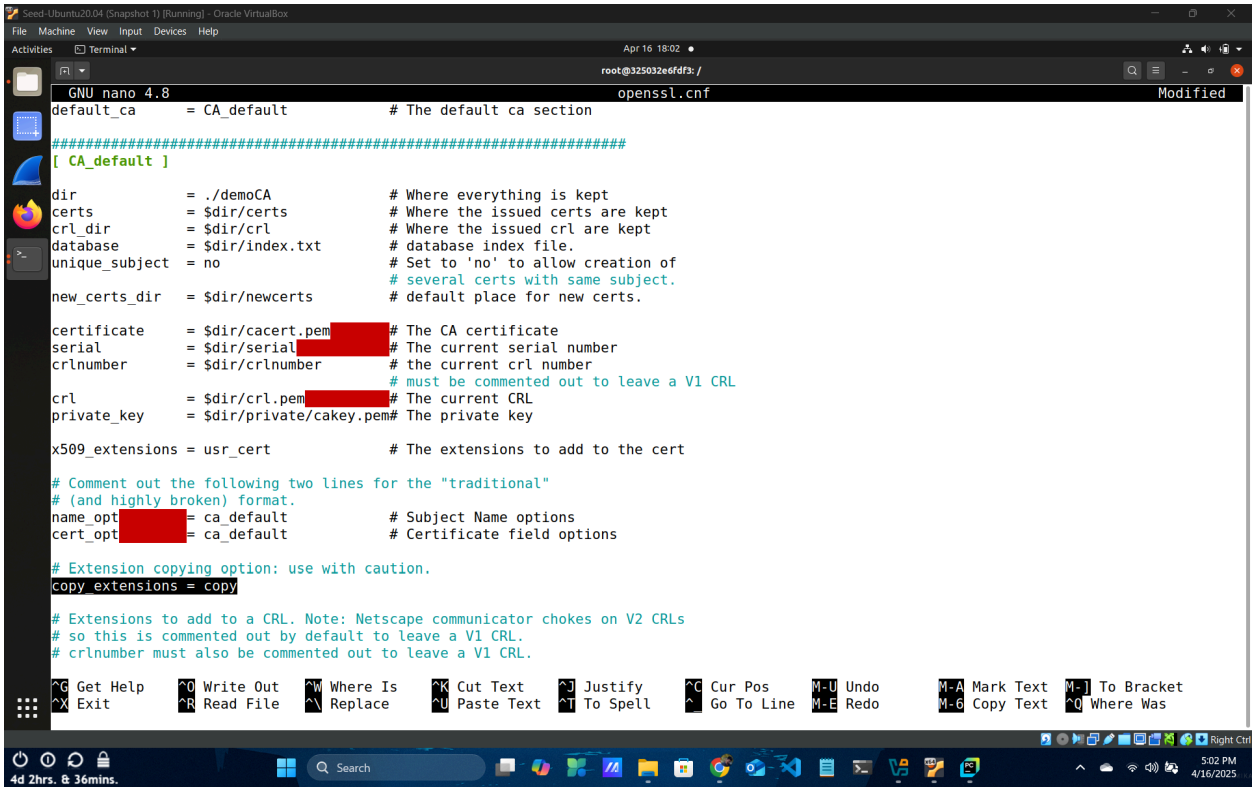



Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:51
root@325032e6fdf3: /
c9:cb:36:5f:e6:53:8b:6c:0b:08:d3:67:c9:28:25:
ef:2b:5d:0a:22:19:82:79:72:f3:97:40:f5:72:75:
43:ea:55:ca:68:cf:74:68:d1:20:f4:7c:61:ba:41:
3d:f2:0c:03:9d:d0:cc:44:85:1a:1e:9e:1f:6e:b8:
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:d0:
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:d1:31: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:a7:
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:cf:7c: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:
Right Ctrl
4d 2hrs. & 25mins.
Search
4:51 PM
4/16/2025

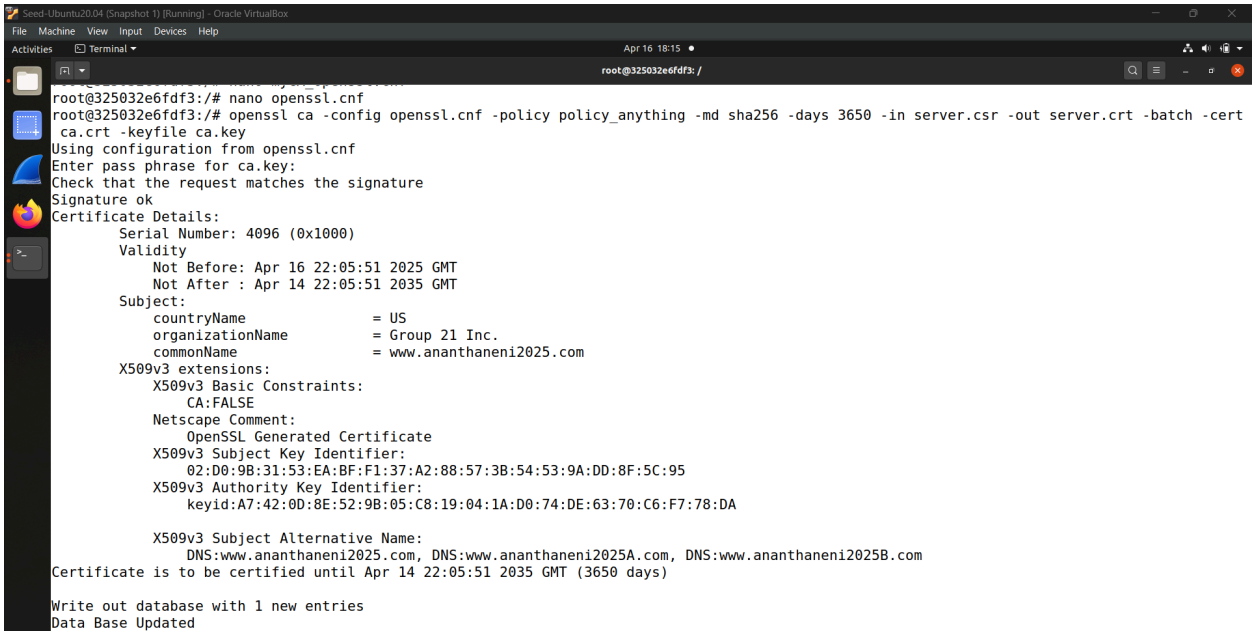

Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 16 17:51
root@325032e6fdf3: /
26:02:a5:ef:b7:99:dc:ed:21:30:57:2e:e8:13:a2:
79:dc:ce:fb:d3:c9:97:a9:1d:27:4b:c4:d9:32:03:
43:11:37:1f:56:2d:54:0c:fa:10:33:ce:89:9f:de:
c2:1e:d0:fc:e9:7e:96:57:16:c2:0b:7d:83:d6:ca:
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:d4: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:4e: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:07:1d:80:54:34:88:72:8d:12:01:
e4:ec:69:43:e9:5f:40:f8
root@325032e6fdf3:/#
Right Ctrl
4d 2hrs. & 25mins.
Search
4:51 PM
4/16/2025

3.3 Task 3: Generating a Certificate for your server

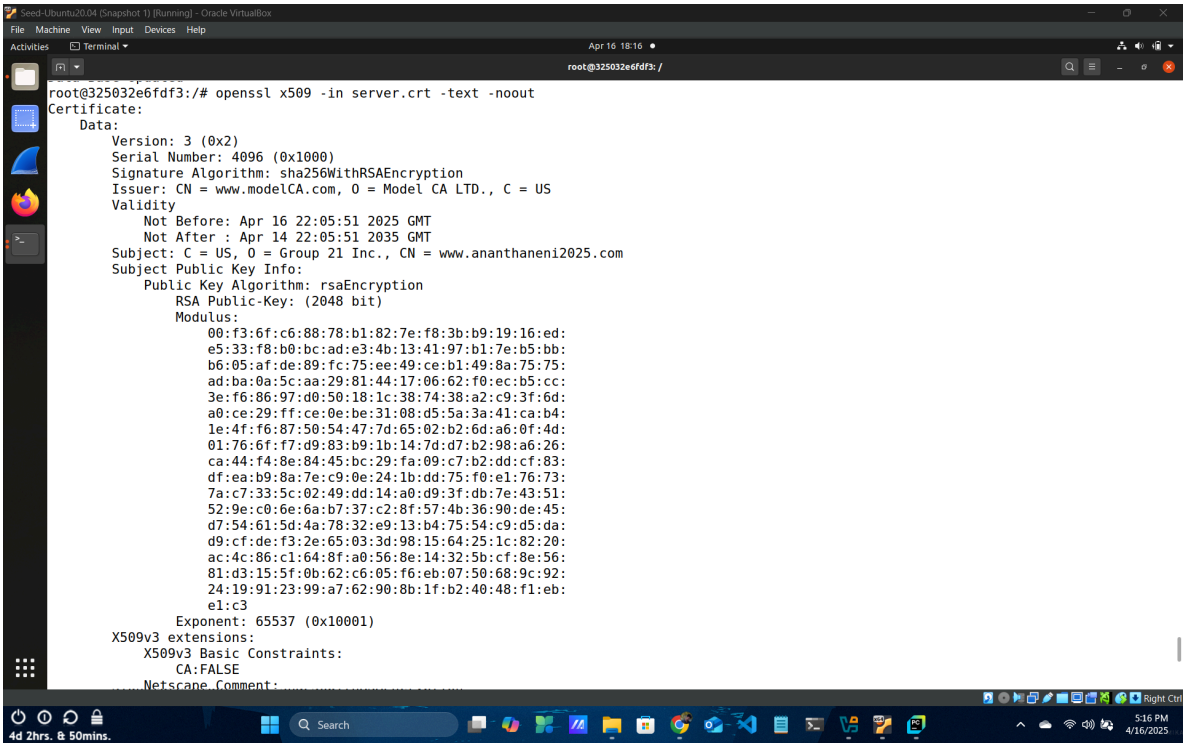
Opened openssl.cnf file in a text editor & uncommented the highlighted line to ensure the Subject Alternative Names (SANs) added by us in the CSR will be included in the final signed certificate



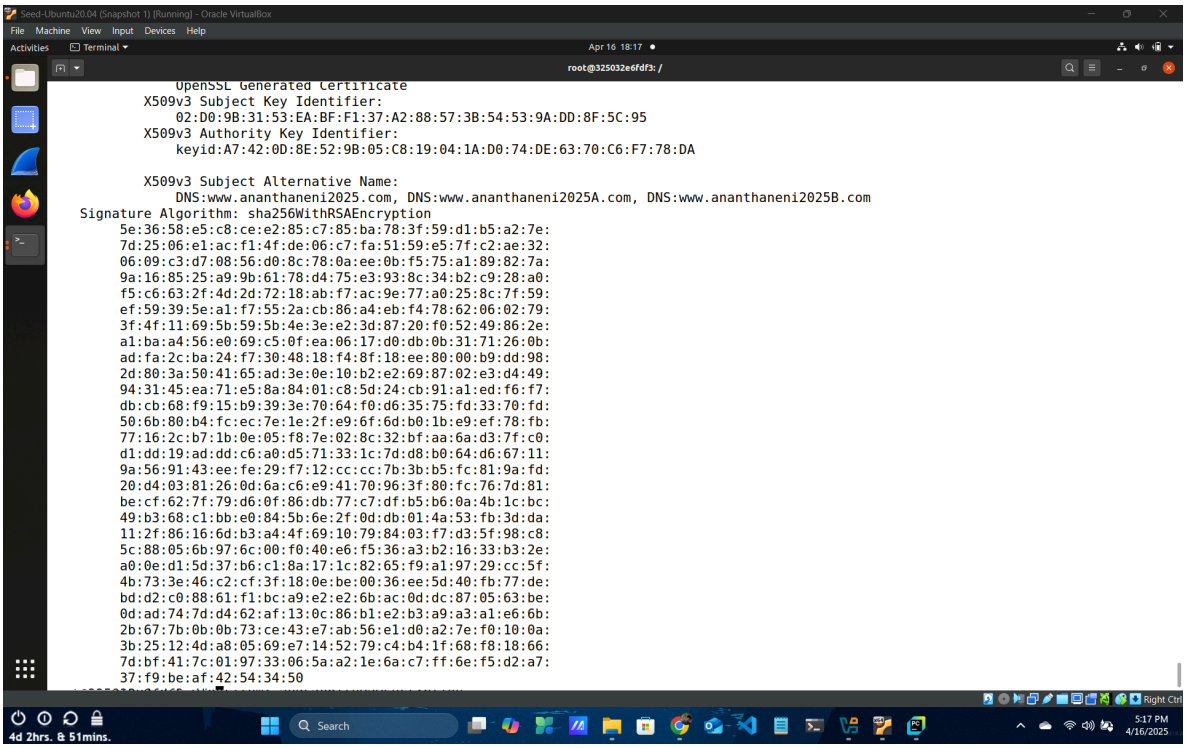
Turning our certificate signing request (server.csr) into an X509 certificate (server.crt) by using the CA's ca.crt and ca.key



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

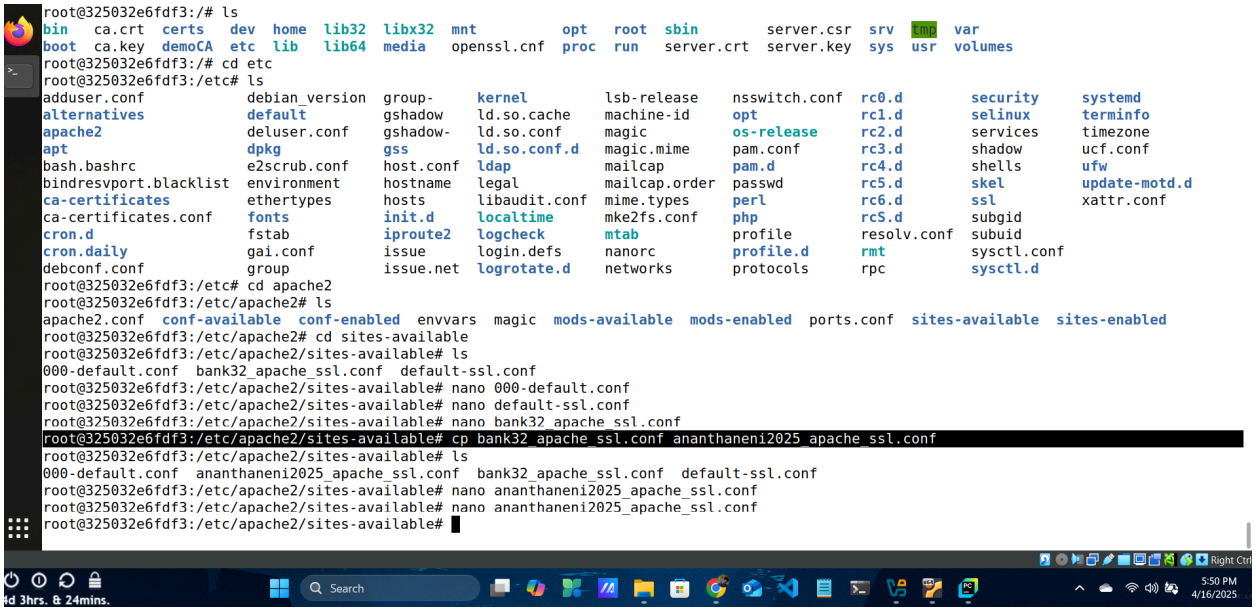


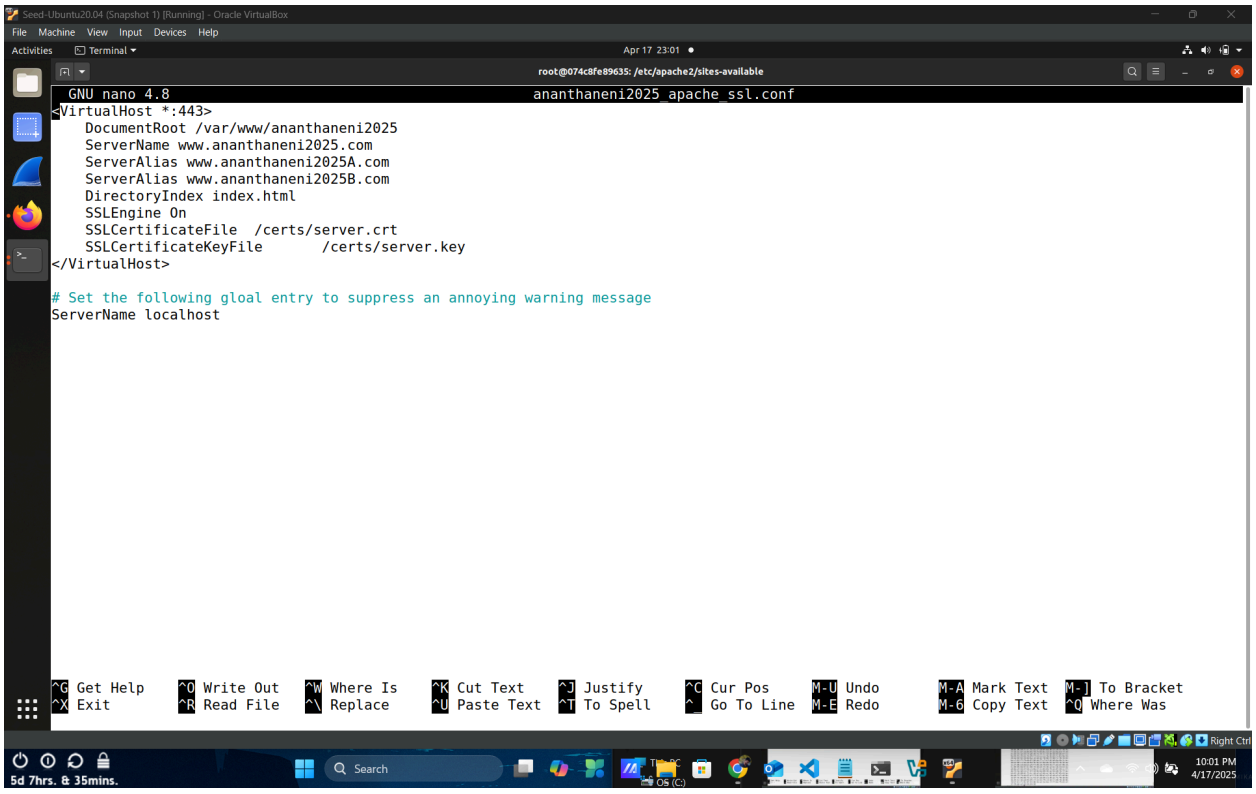
Here, the alternative names are included successfully



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

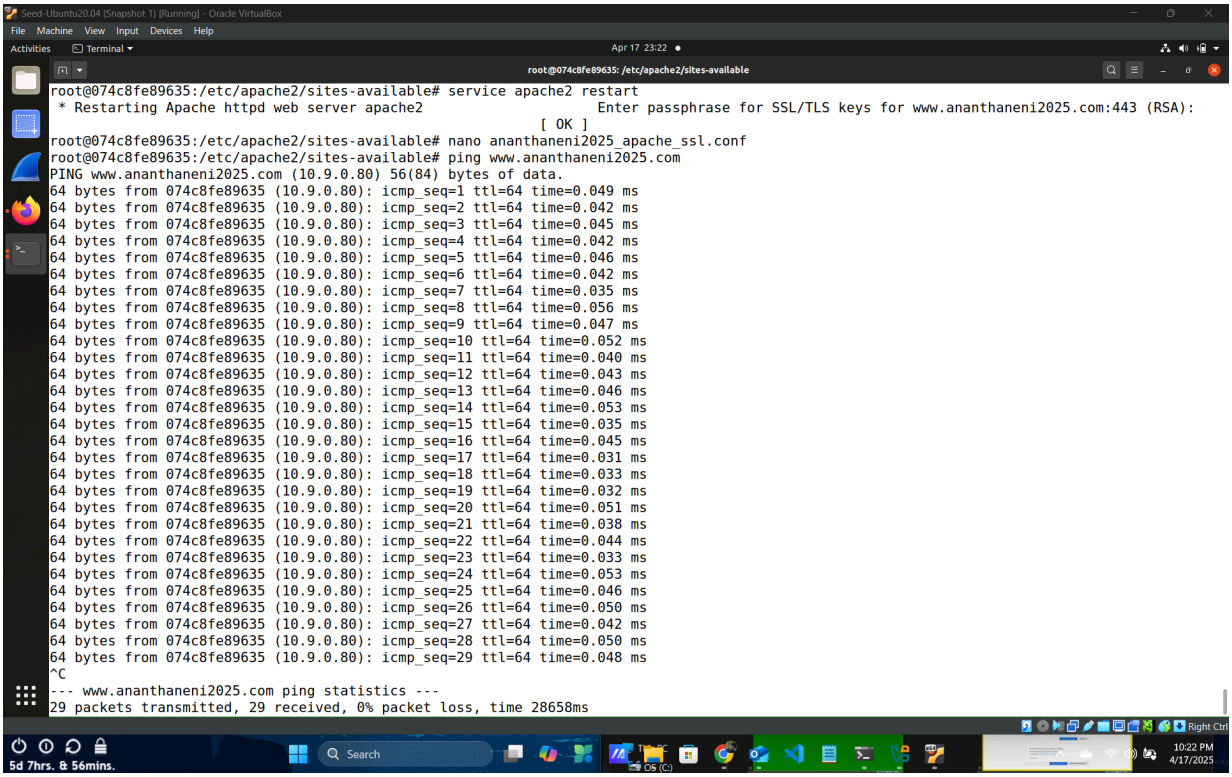
Updated the VirtualHost file located in /etc/apache2/sites-available directory to ensure Apache server to host mutliple websites



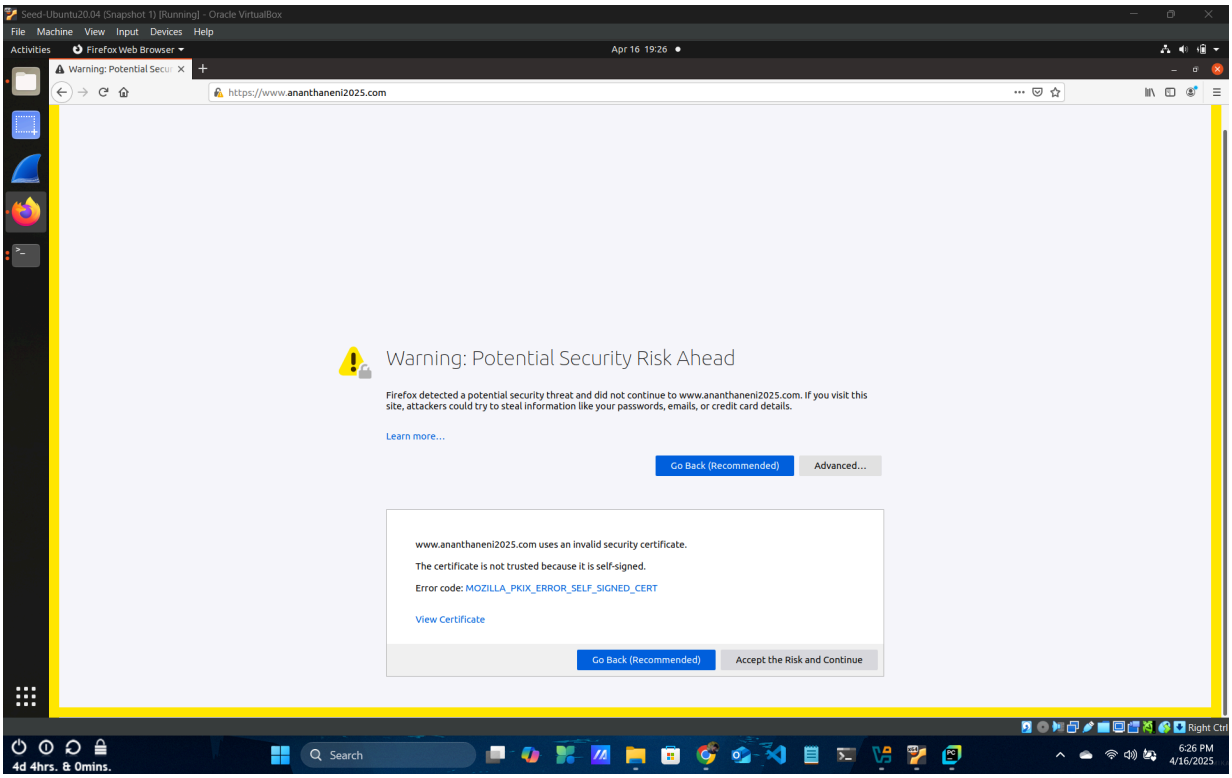


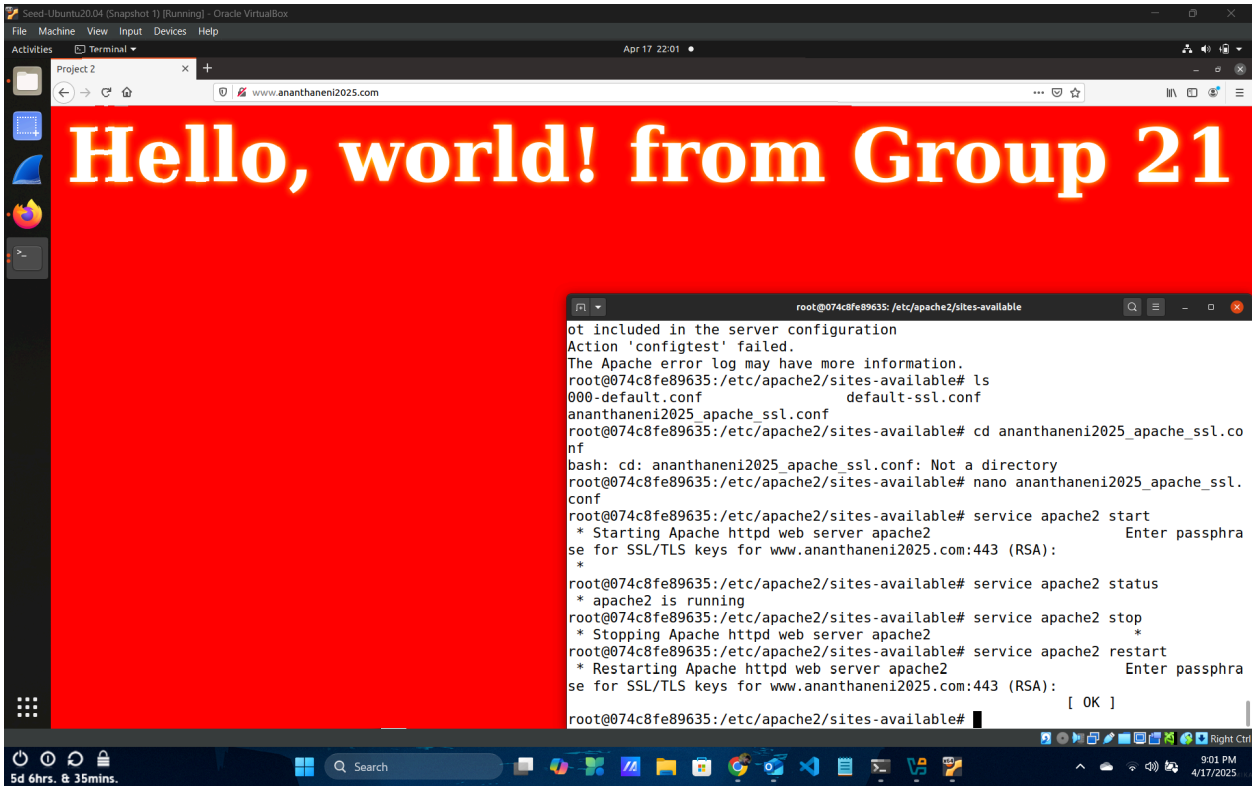
Also, we have made sure the server files are stored in the respective directories, enabled the Apache's ssl module and then enabled our site to make the website work

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

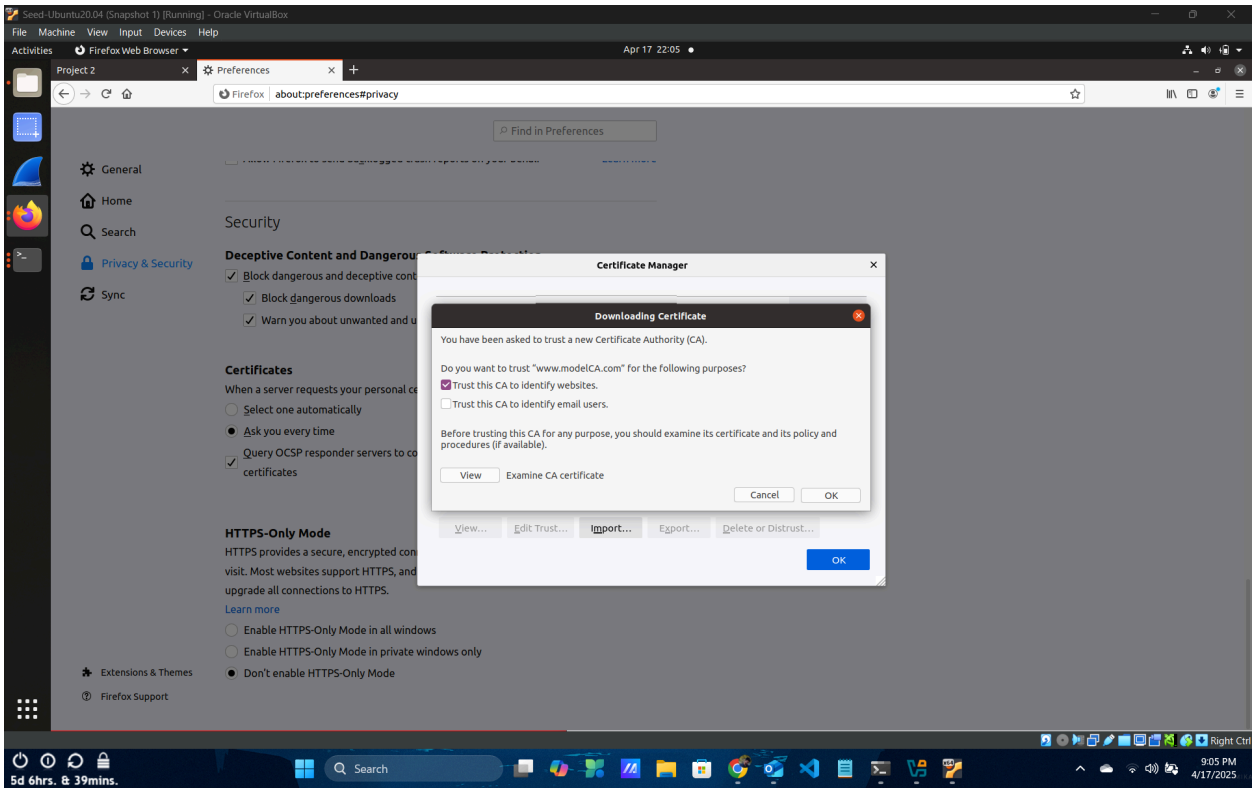


On accessing our website initially, browser said ‘untrusted certificate’ as it doesn’t trust our custom CA (ca.crt)

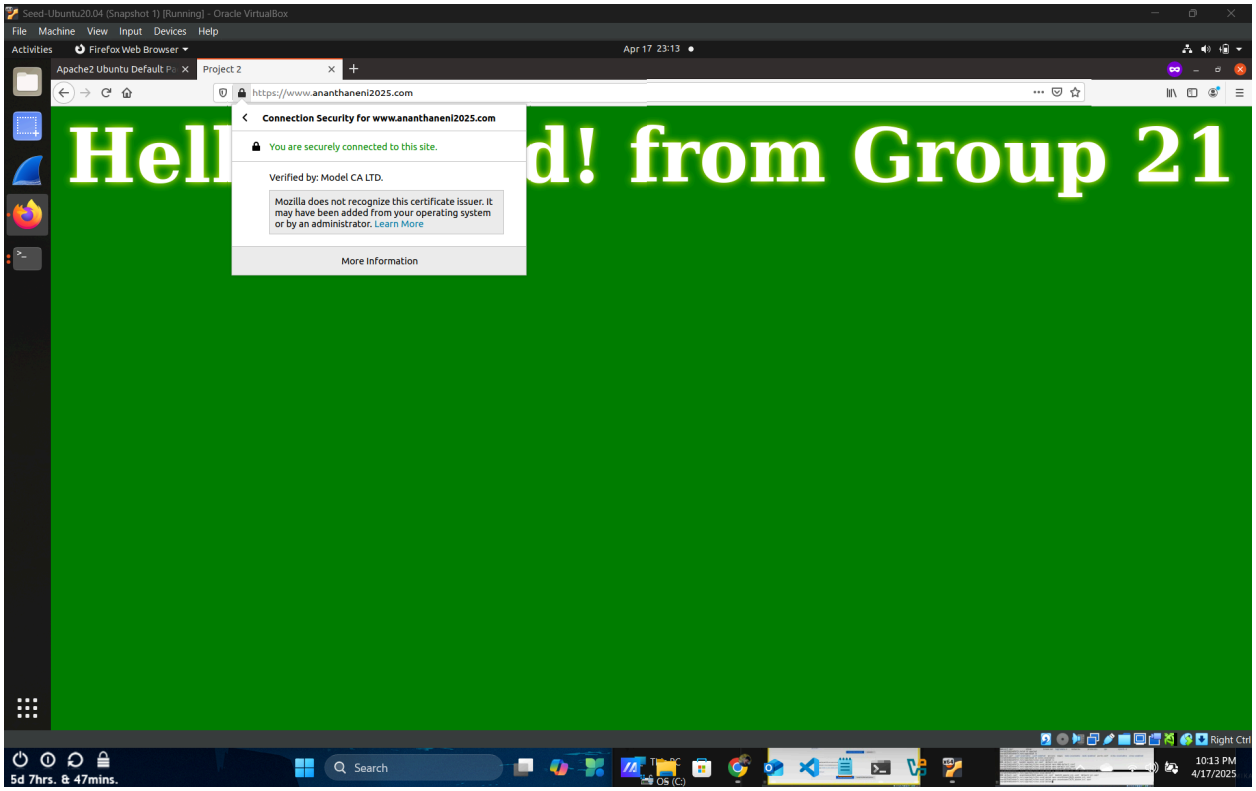




To fix this, we have imported our ca.crt into our browser as a Trusted Authority which made our connection secure

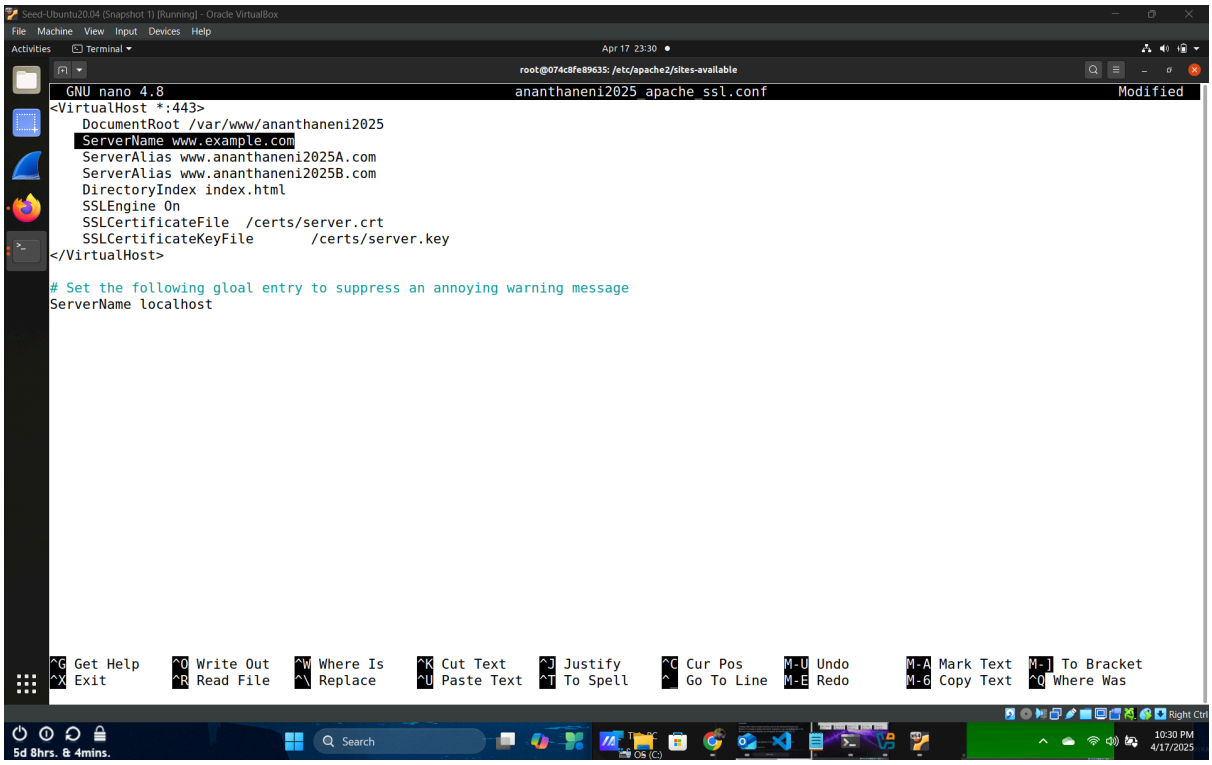



Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Apr 17 23:07
Apache2 Ubuntu Default Pa
Project 2
https://www.ananthaneni2025.com
Hello, world! from Group 21
5d 7hrs. & 41mins.
Search
10:07 PM
4/17/2025

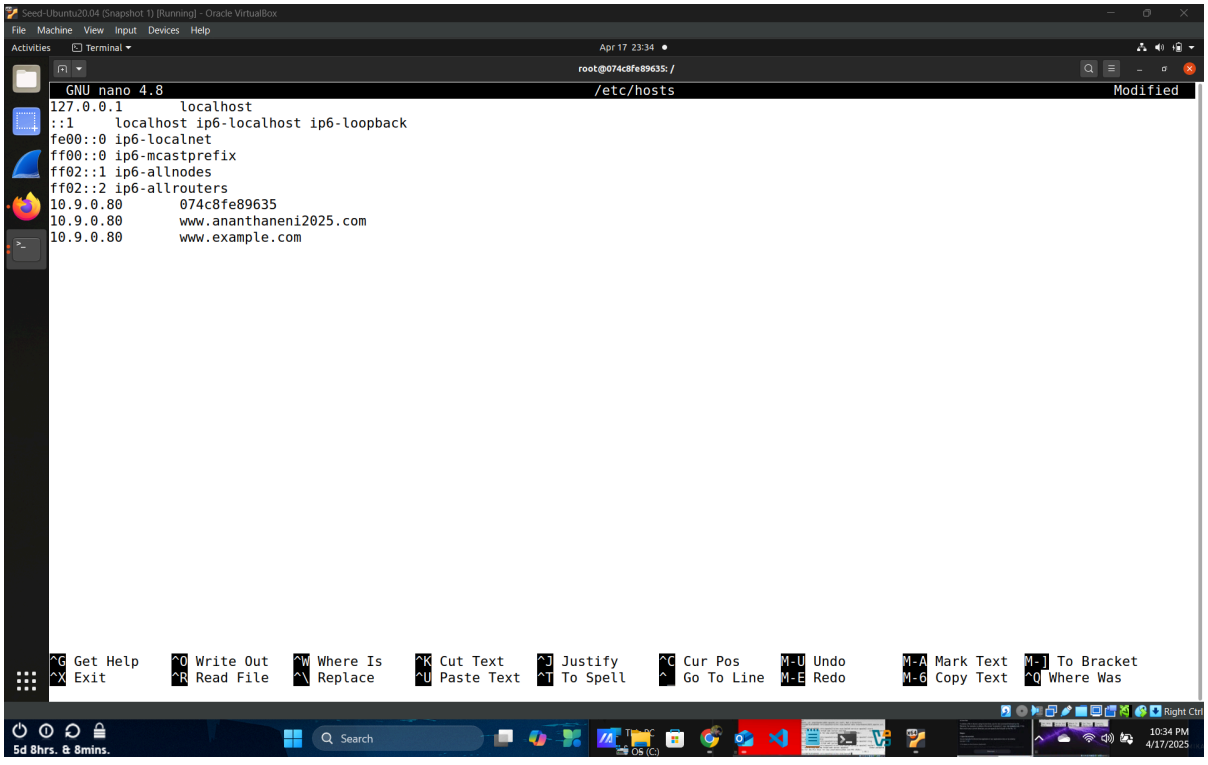

Seed-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Apr 17 23:13
Apache2 Ubuntu Default Pa
Project 2
https://www.ananthaneni2025.com
Connection Security for www.ananthaneni2025.com
You are securely connected to this site.
Verified by: Model CA LTD.
Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More
More Information
Hell
d! from Group 21
5d 7hrs. & 47mins.
Search
10:13 PM
4/17/2025

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

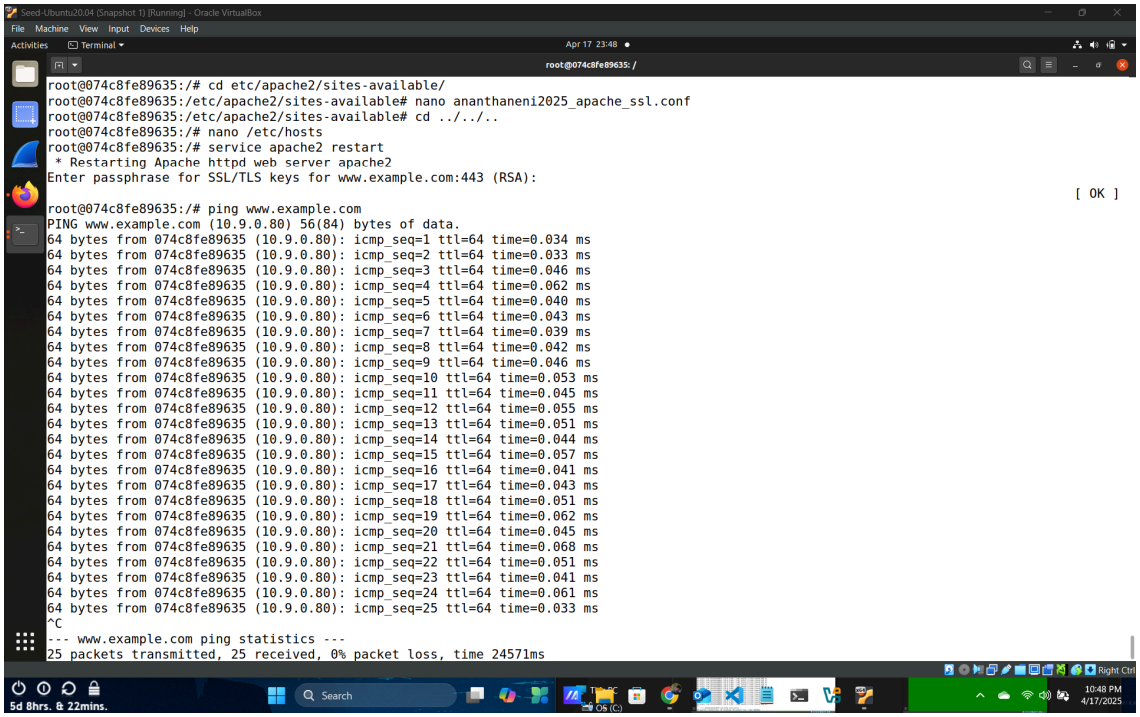
Added a new VirtualHost entry for www.example.com for setting up the malicious website

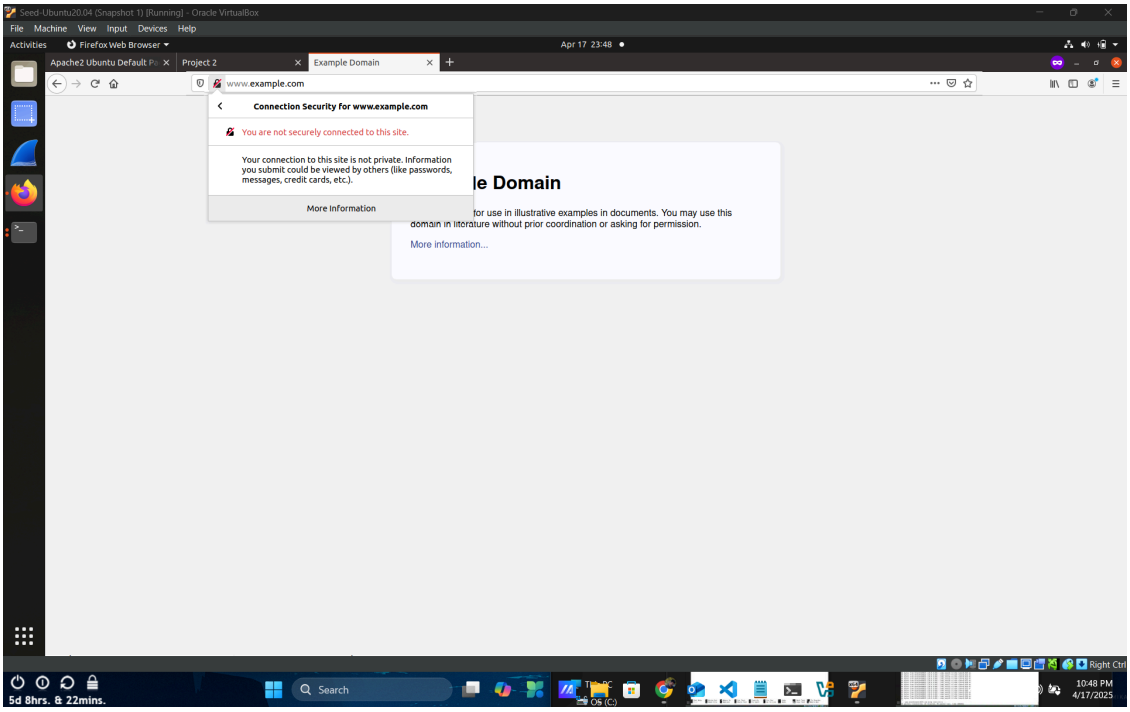


Became the man in the middle through simulating DNS Spoofing by editing /etc/hosts file to map the real domain to our malicious web server's IP



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



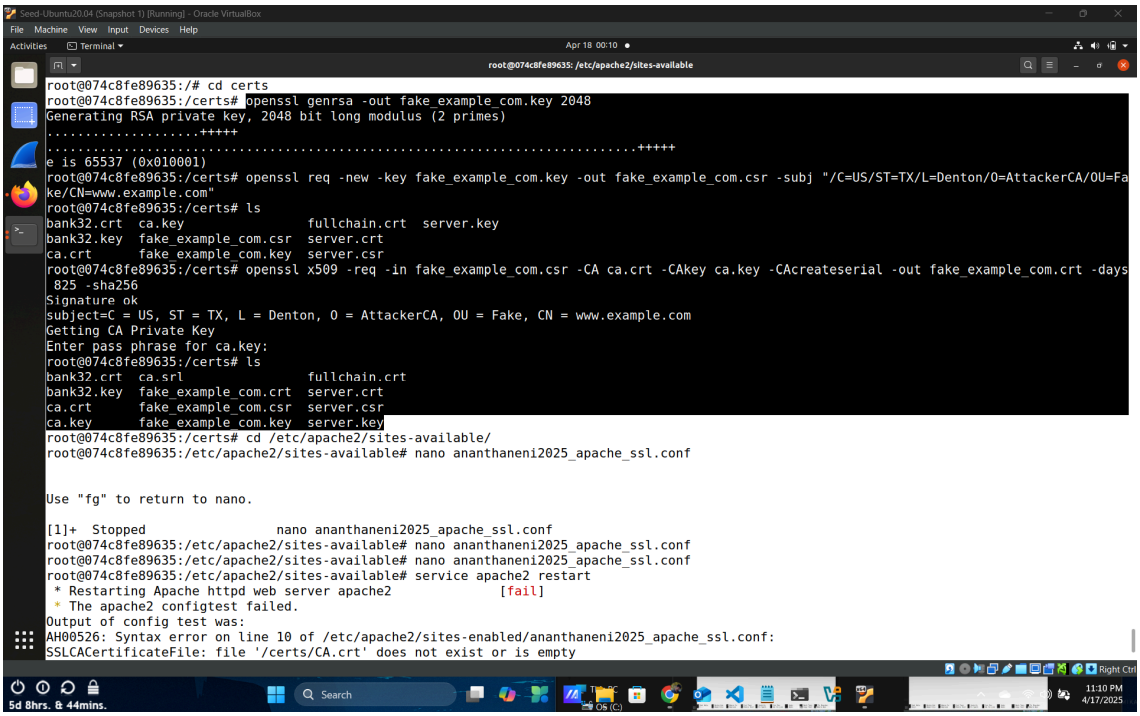


When we tried to visit https://www.example.com, the browser showed a security warning indicating that the connection was not private. This is because the fake server's certificate was not issued by a trusted certificate authority (CA) for the real domain. The browser detected that the certificate did 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.

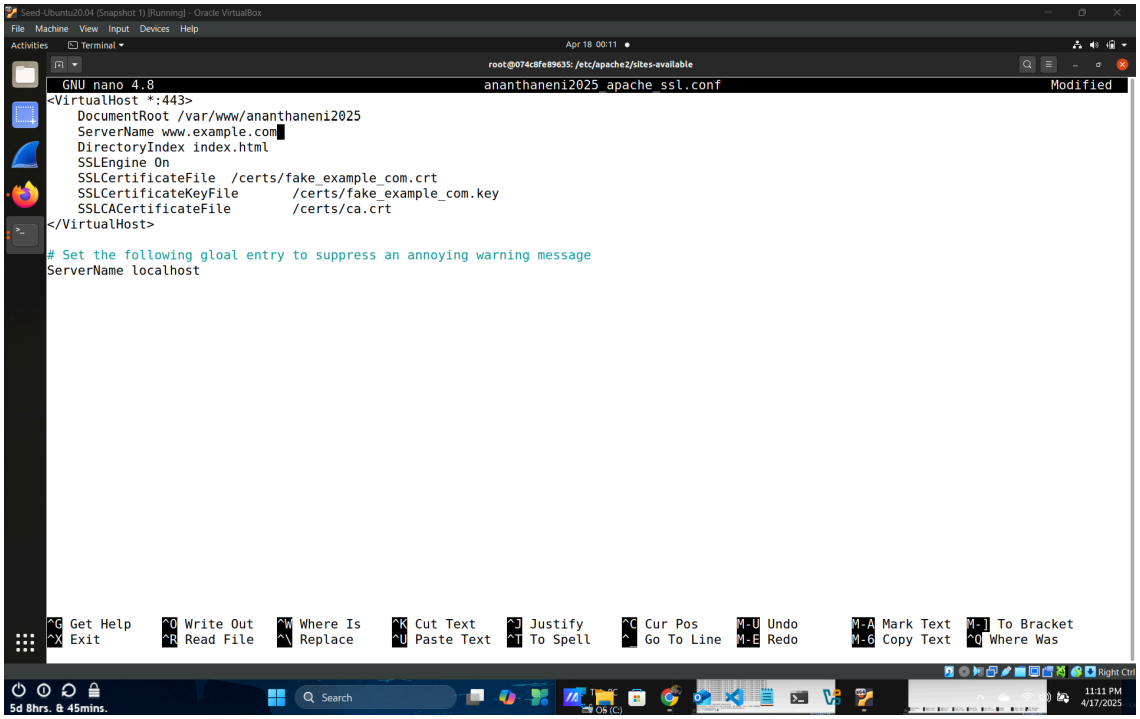
3.6 Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

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

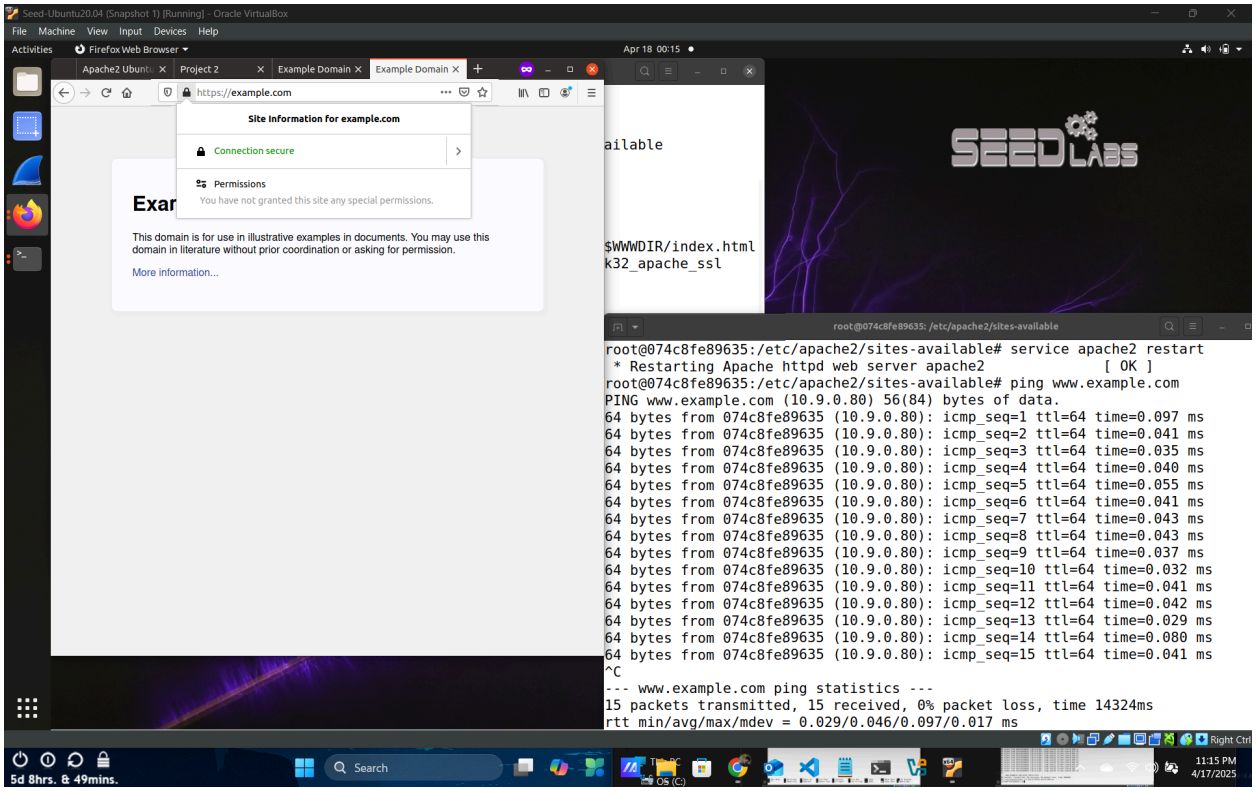
Generated a key and CSR for this malicious site and used the compromised CA to sign it



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



On restarting the Apache and visting the target site(through DNS Hijack again), no browser warning appears (compromised CA ceritificate 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.