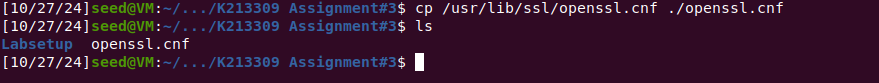
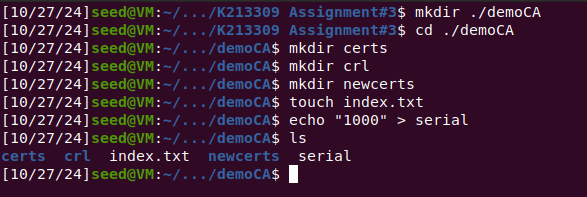
# Task#1

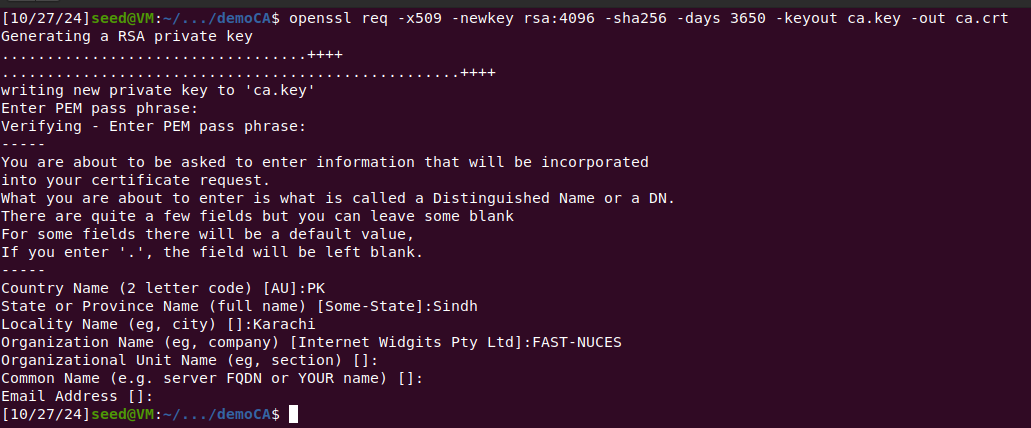
Following the steps given in the manual, we first need to copy the openssl.conf file since we need to make changes to this file and use OpenSSL to create certificates.



Next, we need to create several sub-directories, and the [CA default] section of the configuration file shows the default setting that we need to prepare.

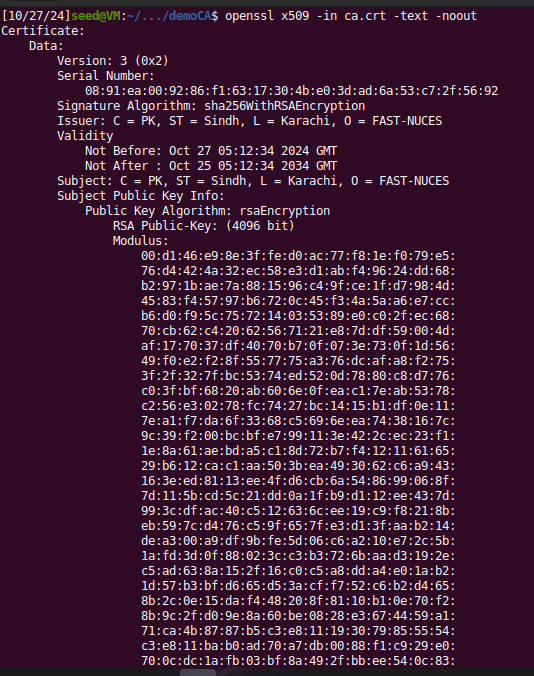


Now that we have setup the configuration file openssl.cnf, we can create and issue certificates. We can now run the following command as given in the manual to generate the self-signed certificate for the CA:



The password is set to 12345.

Now we can use the following commands to look at the decoded content of the X509 certificate and the RSA key.



The full file is given below:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

08:91:ea:00:92:86:f1:63:17:30:4b:e0:3d:ad:6a:53:c7:2f:56:92

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = PK, ST = Sindh, L = Karachi, O = FAST-NUCES

Validity

Not Before: Oct 27 05:12:34 2024 GMT

Not After : Oct 25 05:12:34 2034 GMT

Subject: C = PK, ST = Sindh, L = Karachi, O = FAST-NUCES

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (4096 bit)

Modulus:

00:d1:46:e9:8e:3f:fe:d0:ac:77:f8:1e:f0:79:e5:

76:d4:42:4a:32:ec:58:e3:d1:ab:f4:96:24:dd:68:

b2:97:1b:ae:7a:88:15:96:c4:9f:ce:1f:d7:98:4d:

45:83:f4:57:97:b6:72:0c:45:f3:4a:5a:a6:e7:cc:

b6:d0:f9:5c:75:72:14:03:53:89:e0:c0:2f:ec:68:

70:cb:62:c4:20:62:56:71:21:e8:7d:df:59:00:4d:

af:17:70:37:df:40:70:b7:0f:07:3e:73:0f:1d:56:

49:f0:e2:f2:8f:55:77:75:a3:76:dc:af:a8:f2:75:

3f:2f:32:7f:bc:53:74:ed:52:0d:78:80:c8:d7:76:

c0:3f:bf:68:20:ab:60:6e:0f:ea:c1:7e:ab:53:78:

c2:56:e3:02:78:fc:74:27:bc:14:15:b1:df:0e:11:

7e:a1:f7:da:6f:33:68:c5:69:6e:ea:74:38:16:7c:

9c:39:f2:00:bc:bf:e7:99:11:3e:42:2c:ec:23:f1:

1e:8a:61:ae:bd:a5:c1:8d:72:b7:f4:12:11:61:65:

29:b6:12:ca:c1:aa:50:3b:ea:49:30:62:c6:a9:43:

16:3e:ed:81:13:ee:4f:d6:cb:6a:54:86:99:06:8f:

7d:11:5b:cd:5c:21:dd:0a:1f:b9:d1:12:ee:43:7d:

99:3c:df:ac:40:c5:12:63:6c:ee:19:c9:f8:21:8b:

eb:59:7c:d4:76:c5:9f:65:7f:e3:d1:3f:aa:b2:14:

de:a3:00:a9:df:9b:fe:5d:06:c6:a2:10:e7:2c:5b:

1a:fd:3d:0f:88:02:3c:c3:b3:72:6b:aa:d3:19:2e:

c5:ad:63:8a:15:2f:16:c0:c5:a8:dd:a4:e0:1a:b2:

1d:57:b3:bf:d6:65:d5:3a:cf:f7:52:c6:b2:d4:65:

8b:2c:0e:15:da:f4:48:20:8f:81:10:b1:0e:70:f2:

8b:9c:2f:d0:9e:8a:60:be:08:28:e3:67:44:59:a1:

71:ca:4b:87:87:b5:c3:e8:11:19:30:79:85:55:54:

c3:e8:11:ba:b0:ad:70:a7:db:00:88:f1:c9:29:e0:

70:0c:dc:1a:fb:03:bf:8a:49:2f:bb:ee:54:0c:83:

24:dd:fc:54:48:df:21:cc:52:07:61:94:f3:05:41:

32:78:6e:db:fc:06:19:8d:ca:35:06:ad:ce:76:ba:

30:60:27:49:b9:5e:1f:3d:c3:76:17:e1:40:23:80:

bd:cf:73:49:4d:9c:3e:99:c1:c7:8d:31:34:1e:0d:

c1:b0:c7:2a:de:52:d8:0d:90:51:ef:bd:a6:ff:07:

32:35:66:b4:55:22:87:c8:72:4d:9a:64:b6:ab:f1:

f1:8f:61

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

7B:4D:E4:71:E8:0D:E9:BB:B0:F6:AC:F3:19:80:D9:12:70:52:F7:7E

X509v3 Authority Key Identifier:

keyid:7B:4D:E4:71:E8:0D:E9:BB:B0:F6:AC:F3:19:80:D9:12:70:52:F7:7E

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha256WithRSAEncryption

cd:ad:b1:c2:0f:78:79:59:11:cb:09:ee:26:2b:80:64:6e:27:

2c:f0:48:00:7c:37:d3:22:cd:67:44:f4:4e:cb:32:5e:89:a1:

59:a7:29:a1:ba:31:ab:cc:b8:25:46:73:73:5b:95:05:87:37:

71:65:28:81:d6:15:50:a4:da:da:ec:23:64:17:f3:9c:62:49:

05:c0:18:d0:4a:92:c5:dd:74:30:80:41:7c:12:0a:91:5c:e9:

1f:2b:43:e4:78:34:a8:92:0a:b2:e8:fa:5c:78:fc:9e:c4:e0:

a9:d2:de:99:72:07:58:ae:58:11:be:5f:ac:9d:38:9d:fb:c1:

59:1a:2c:7b:f9:97:36:b3:ad:c6:c3:8c:7d:3c:ec:b3:91:6e:

b2:42:5f:68:79:7f:1f:34:91:47:4c:3b:2f:cf:35:c1:ed:07:

06:a8:75:fe:86:26:73:ae:2c:35:ea:a8:11:db:2b:f4:48:af:

f6:60:6a:92:04:c3:66:54:61:85:38:fb:2b:40:61:e1:7b:1f:

59:d0:36:1f:0d:10:5c:8f:4b:52:6c:0c:99:8c:25:89:6a:de:

49:94:b3:63:c2:1a:6c:24:cc:8f:2a:a4:55:bd:81:2f:5c:6c:

ac:d8:30:f8:ec:19:e0:dd:62:e3:6b:79:c7:80:5e:6e:bc:60:

f8:56:e8:48:c5:60:48:ba:41:f6:06:5c:2b:6d:75:05:22:48:

8e:22:7a:1b:12:58:80:5b:90:7b:52:65:4d:3c:d9:34:46:7c:

27:1b:63:d1:27:ad:30:15:37:d2:6e:43:55:c0:da:29:5f:be:

3a:74:63:3d:09:ad:4a:84:80:8d:f7:74:9b:d4:7a:19:a3:6d:

64:f3:21:98:12:00:df:c0:2e:46:81:d7:0b:fa:42:de:28:ab:

43:11:31:3f:d7:9f:33:e1:5e:7a:e1:1c:5f:2e:62:ee:5a:d1:

a0:7d:48:95:13:a4:bb:30:03:db:c1:3d:87:97:70:6a:08:81:

08:8c:e7:b1:ab:a9:db:25:48:1c:0b:55:84:38:71:5b:96:bc:

e3:0c:60:6c:4b:10:82:7e:a6:b5:6f:ef:fe:33:6d:d0:db:b7:

a7:1e:2e:50:5a:6b:16:52:ff:78:0b:12:ea:0d:6b:0b:2b:8f:

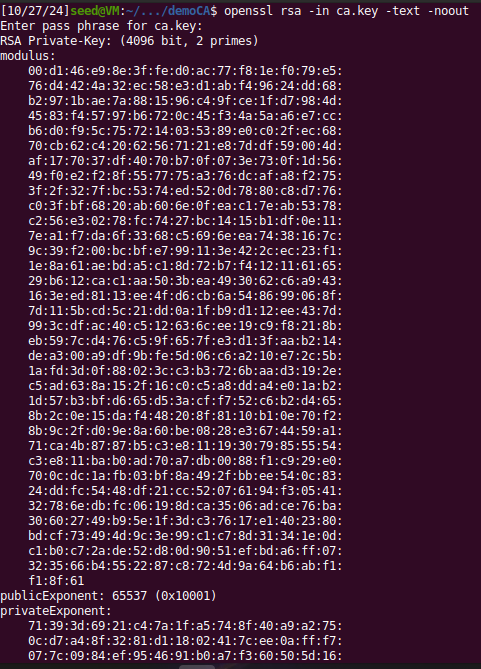
bf:0d:c1:d9:d2:a4:76:51:6e:27:5c:8b:b6:3f:20:00:48:c7:

26:03:a1:a7:a3:b6:52:30:b1:c5:f3:24:c6:cb:91:95:6f:37:

17:7d:84:46:9a:43:53:1e:04:69:b3:d6:cb:e7:21:46:94:a8:

f5:a5:15:d7:3b:21:b1:6b:9c:32:ed:a8:9d:fe:a2:1e:e9:d6:

fa:de:34:b2:7a:d6:63:32



The full file is given below:

RSA Private-Key: (4096 bit, 2 primes)

modulus:

00:d1:46:e9:8e:3f:fe:d0:ac:77:f8:1e:f0:79:e5:

76:d4:42:4a:32:ec:58:e3:d1:ab:f4:96:24:dd:68:

b2:97:1b:ae:7a:88:15:96:c4:9f:ce:1f:d7:98:4d:

45:83:f4:57:97:b6:72:0c:45:f3:4a:5a:a6:e7:cc:

b6:d0:f9:5c:75:72:14:03:53:89:e0:c0:2f:ec:68:

70:cb:62:c4:20:62:56:71:21:e8:7d:df:59:00:4d:

af:17:70:37:df:40:70:b7:0f:07:3e:73:0f:1d:56:

49:f0:e2:f2:8f:55:77:75:a3:76:dc:af:a8:f2:75:

3f:2f:32:7f:bc:53:74:ed:52:0d:78:80:c8:d7:76:

c0:3f:bf:68:20:ab:60:6e:0f:ea:c1:7e:ab:53:78:

c2:56:e3:02:78:fc:74:27:bc:14:15:b1:df:0e:11:

7e:a1:f7:da:6f:33:68:c5:69:6e:ea:74:38:16:7c:

9c:39:f2:00:bc:bf:e7:99:11:3e:42:2c:ec:23:f1:

1e:8a:61:ae:bd:a5:c1:8d:72:b7:f4:12:11:61:65:

29:b6:12:ca:c1:aa:50:3b:ea:49:30:62:c6:a9:43:

16:3e:ed:81:13:ee:4f:d6:cb:6a:54:86:99:06:8f:

7d:11:5b:cd:5c:21:dd:0a:1f:b9:d1:12:ee:43:7d:

99:3c:df:ac:40:c5:12:63:6c:ee:19:c9:f8:21:8b:

eb:59:7c:d4:76:c5:9f:65:7f:e3:d1:3f:aa:b2:14:

de:a3:00:a9:df:9b:fe:5d:06:c6:a2:10:e7:2c:5b:

1a:fd:3d:0f:88:02:3c:c3:b3:72:6b:aa:d3:19:2e:

c5:ad:63:8a:15:2f:16:c0:c5:a8:dd:a4:e0:1a:b2:

1d:57:b3:bf:d6:65:d5:3a:cf:f7:52:c6:b2:d4:65:

8b:2c:0e:15:da:f4:48:20:8f:81:10:b1:0e:70:f2:

8b:9c:2f:d0:9e:8a:60:be:08:28:e3:67:44:59:a1:

71:ca:4b:87:87:b5:c3:e8:11:19:30:79:85:55:54:

c3:e8:11:ba:b0:ad:70:a7:db:00:88:f1:c9:29:e0:

70:0c:dc:1a:fb:03:bf:8a:49:2f:bb:ee:54:0c:83:

24:dd:fc:54:48:df:21:cc:52:07:61:94:f3:05:41:

32:78:6e:db:fc:06:19:8d:ca:35:06:ad:ce:76:ba:

30:60:27:49:b9:5e:1f:3d:c3:76:17:e1:40:23:80:

bd:cf:73:49:4d:9c:3e:99:c1:c7:8d:31:34:1e:0d:

c1:b0:c7:2a:de:52:d8:0d:90:51:ef:bd:a6:ff:07:

32:35:66:b4:55:22:87:c8:72:4d:9a:64:b6:ab:f1:

f1:8f:61

publicExponent: 65537 (0x10001)

privateExponent:

71:39:3d:69:21:c4:7a:1f:a5:74:8f:40:a9:a2:75:

0c:d7:a4:8f:32:81:d1:18:02:41:7c:ee:0a:ff:f7:

07:7c:09:84:ef:95:46:91:b0:a7:f3:60:50:5d:16:

0c:13:29:44:c2:87:a7:8e:3c:d7:70:7e:36:90:f2:

23:d3:95:ab:51:01:f4:de:c0:8c:e1:4d:cc:48:a1:

25:d8:94:a5:b4:ae:71:dc:d7:8d:2a:46:5b:bc:ab:

cb:31:82:78:fd:c3:3d:b7:1a:c3:35:ba:ea:b3:61:

a3:bb:15:62:68:ea:0d:b2:57:bf:84:26:12:af:4e:

74:f9:8c:54:56:8e:bf:4b:12:50:ac:d4:7c:86:19:

f3:23:5a:71:ba:66:9c:85:6e:0c:2b:bd:03:97:25:

05:9f:22:1a:54:f3:7e:ff:e9:99:e7:36:f7:c4:8d:

4f:91:ea:13:19:ac:48:8a:07:61:3f:69:8c:f8:f4:

09:01:9e:56:80:39:0b:fe:61:41:aa:4e:44:0f:d2:

e7:29:7c:41:cc:a9:10:1f:0d:d9:35:e1:43:61:59:

14:d1:cb:f2:c5:73:4d:47:2f:3b:c7:65:15:f4:5e:

d7:c2:e5:7f:e4:02:3c:02:a7:cf:7d:56:d3:4e:d4:

6a:8c:d1:69:54:44:e3:92:50:95:05:f9:f4:77:c2:

6c:4b:57:95:cc:72:18:c3:25:f4:bc:d1:14:d2:a4:

a6:a1:7b:53:b3:94:b0:0d:b5:2f:38:95:a7:52:56:

5e:5e:44:7b:88:7d:d6:32:81:93:1e:fa:4f:a6:9b:

d5:4c:ad:98:35:6d:b6:ea:64:81:4f:e7:10:fe:fd:

33:72:da:45:14:a6:05:b8:37:c0:2f:ea:75:f9:e5:

2a:c8:21:1e:8f:6e:b9:34:e8:0a:ac:29:5d:c9:f8:

cf:8e:3c:51:63:66:c3:0e:45:ac:10:02:30:91:3f:

b5:a1:ce:ef:84:eb:0f:4c:5d:c9:cc:f1:fc:61:03:

5c:66:85:f0:7a:ec:28:76:94:b2:5d:b6:a9:59:ab:

70:c5:5b:09:b4:35:6d:68:58:23:50:49:f5:c4:a1:

85:47:7f:05:2e:e4:2e:a1:c5:ad:61:d3:5e:42:cd:

07:dc:ce:73:e2:3f:c8:d6:64:6f:61:78:00:36:b5:

e8:14:45:47:59:a8:77:ba:c3:30:01:2d:46:23:3a:

4c:49:a5:2f:8a:d6:95:8a:d4:a0:15:d4:de:82:d5:

a4:59:dd:70:42:39:70:ff:7a:94:ae:d9:b7:22:bb:

0a:ba:e5:83:60:89:70:f6:3e:1c:d3:a4:06:9a:c1:

4c:bc:0d:d4:08:e8:b8:b3:3a:bb:b5:aa:8c:6f:f1:

ec:95

prime1:

00:ea:d8:8c:06:b6:55:89:c3:3e:b6:ff:8a:0b:d6:

dc:37:57:3c:44:bf:c6:0b:9f:f8:cf:49:88:8d:f5:

69:2c:89:f6:1e:99:36:62:8c:c0:5f:9e:10:df:37:

b2:04:03:46:95:49:8b:a7:4d:69:30:da:18:ae:5b:

fa:87:b8:87:6c:e0:78:f4:0f:78:b5:fa:a0:f8:c7:

94:6c:61:ad:71:45:c9:5b:ad:33:ce:07:7d:85:c4:

c0:4b:82:dd:5e:1d:d9:7c:d5:c8:91:ae:57:8e:6d:

87:27:10:a0:34:31:ff:7c:d2:29:67:88:f9:98:ad:

33:e1:02:3d:86:d8:b0:68:26:09:0b:2b:77:dd:5b:

f2:ec:6e:c1:f7:e2:d0:3c:f7:cc:e8:5a:ba:96:d3:

36:8c:e9:ac:7a:e6:a4:cc:dc:1d:2c:e5:2a:4f:f7:

54:ea:a7:70:df:41:4c:2c:fd:61:b1:47:02:4d:d9:

be:f8:ea:71:8c:eb:8d:57:a0:3a:4d:91:df:70:71:

82:25:f9:6a:b4:df:0b:ea:76:64:46:87:b0:5f:e5:

a7:50:1e:70:6c:21:61:d9:88:3c:02:a8:c1:bf:db:

42:dc:43:7b:13:9d:bc:ed:24:c2:2f:1a:72:4f:f4:

95:d4:16:79:45:19:df:7e:91:ef:04:ba:fa:c6:af:

a9:2b

prime2:

00:e4:20:c1:ca:39:0a:fb:b0:48:4c:d3:8a:92:3d:

fe:c6:9e:91:b8:ca:2a:e9:bf:52:98:96:b4:dd:b8:

30:8f:8c:d0:1e:6f:51:a7:e7:19:81:a6:eb:6f:71:

bc:f6:96:a2:99:7d:aa:db:fb:ea:5d:aa:df:fb:76:

4f:12:0a:fb:72:17:3f:0b:71:4a:98:d4:43:85:50:

54:16:a4:02:35:6f:f3:bc:1e:a1:73:31:50:73:fd:

8a:bb:cb:a6:13:28:2c:5d:a8:78:81:94:86:d9:bc:

9b:0a:85:a1:bb:db:9c:8c:a5:1c:ef:cc:85:33:f0:

31:86:43:c4:a4:96:02:e2:30:5d:9d:42:5e:e7:88:

ce:33:d1:43:95:fc:ba:e0:47:f0:e4:37:ab:a6:5a:

04:3e:31:cc:d0:2f:81:01:4b:9e:87:34:9e:12:16:

21:6d:4b:7b:ee:9b:ec:9c:12:cd:6a:38:a8:e0:32:

bf:ab:2c:91:37:a1:69:2d:ef:17:f0:1d:76:95:c3:

0e:ed:a8:4b:d4:a9:ed:d6:df:fc:13:58:78:bb:b0:

dd:38:07:0f:1f:bd:c6:82:a0:f1:e9:1e:fe:d8:60:

f1:43:b7:29:ca:2d:a2:0f:4d:87:c3:f4:de:af:a9:

0f:91:27:75:0b:f1:42:5f:4e:e2:cc:d2:b0:59:7c:

0b:a3

exponent1:

00:8a:62:54:10:d8:7c:8b:13:2b:ef:75:a1:08:dc:

f1:23:03:1a:96:80:52:d9:22:c8:e0:8c:ba:14:bc:

99:df:0e:e4:a2:9f:31:b6:dc:ad:b7:2a:53:52:d5:

64:e6:8c:6f:99:24:9f:50:54:83:39:b0:2a:7f:03:

e0:1a:fd:97:7f:86:be:7f:42:66:a5:05:2c:b9:ac:

11:3f:d4:46:f9:ca:5f:9e:cf:ef:08:e6:cd:06:78:

2b:bf:d3:3b:52:6c:50:6e:09:23:89:04:ac:bf:56:

b7:1f:43:e2:c3:1e:fb:27:b8:47:81:a4:eb:3f:16:

40:cd:c4:1e:31:49:9a:99:a4:60:0b:de:ef:60:d6:

ff:cc:66:6f:91:fc:6b:2c:a1:f0:72:b2:93:e4:b0:

4d:22:b7:c7:55:1c:77:db:e7:90:a1:95:e0:5b:02:

a9:5d:24:91:94:5c:cb:e0:6e:e6:94:29:fd:a7:96:

39:bc:3f:99:ed:aa:17:bd:9c:c2:fe:56:88:cd:9f:

75:4b:9f:2f:4b:a9:6b:42:1b:c5:76:f2:19:f2:48:

47:51:24:be:a6:58:fd:69:cb:a7:61:01:c4:39:a3:

a0:40:5e:db:35:71:eb:93:e9:e7:2b:0e:70:71:c0:

f4:50:e7:75:4a:4c:b6:af:c4:9a:8d:b5:08:74:ef:

a9:c5

exponent2:

6b:99:23:ae:3c:ef:78:3c:f2:2d:02:4d:c6:a2:65:

0b:cb:78:d1:de:d1:14:c4:ff:b1:26:cc:12:13:b1:

1b:d3:ff:c9:8b:19:c9:86:cf:d9:fe:1f:e7:c5:8e:

aa:03:ec:97:56:d5:82:c2:b4:0d:0f:ee:6b:0d:a7:

47:cc:54:42:c0:c2:24:a4:7f:d9:cb:ac:39:31:e5:

27:74:9d:f2:14:66:b2:a1:03:e7:70:28:11:3d:51:

f5:37:9d:92:45:8d:7f:73:59:bb:4c:91:ba:1b:22:

49:79:34:0a:86:0f:b5:aa:9f:16:5f:b1:a8:08:af:

63:33:8d:89:4f:93:f6:99:77:5e:18:12:e9:43:f6:

76:2c:4a:a3:70:bb:b7:d3:56:c4:5d:99:a1:71:ad:

b4:a4:0a:85:5b:12:8e:c8:da:f1:cc:98:8d:d1:50:

5c:db:90:8d:bf:8f:7f:21:c3:2f:49:a0:25:76:ea:

3e:53:5b:ff:10:2b:aa:d5:ad:c5:bc:2f:d5:7d:56:

0a:34:29:e8:19:6a:2b:c2:23:84:00:63:99:ab:56:

fb:f9:20:62:09:41:9b:15:4c:64:77:11:1e:7f:c2:

eb:fc:75:42:7d:f9:85:1c:3d:5f:e8:9c:2b:e0:22:

8e:85:3c:c8:b0:37:6c:fa:a9:30:90:63:4b:21:9d:

df

coefficient:

00:9a:a1:43:b0:4c:9b:73:b3:52:6f:f5:69:f5:a4:

6e:5c:8d:23:1a:83:3f:ed:df:87:cc:aa:0e:b7:32:

a7:39:4f:d7:d9:ca:3a:09:fa:45:93:53:78:cc:15:

b4:ea:fe:cf:f3:3c:ab:16:77:17:3c:a1:49:0b:36:

ad:b8:e8:09:c9:64:b9:f4:7b:7c:73:06:92:14:6f:

47:5c:ca:8a:12:1b:92:21:95:81:46:9a:da:76:7f:

d5:e1:32:4c:59:64:7c:fa:8f:b5:ac:13:1a:17:dd:

0a:7e:6f:a0:0c:1b:92:28:a1:b4:86:76:b9:c0:50:

b7:3f:ef:64:0e:11:c4:3f:ea:35:c0:2f:77:38:e8:

88:f4:0f:c3:78:a8:ab:58:4a:9e:03:e0:f9:27:a4:

58:35:15:c8:d3:7e:9b:76:dc:d3:8b:ab:0d:a1:e2:

c7:b6:25:de:47:cf:fd:bf:ea:d6:75:62:b8:94:0c:

49:88:d7:b5:e7:83:f5:be:23:c8:8e:b1:db:d4:8a:

2b:10:7d:0b:78:49:c1:e4:e5:e5:8d:4c:ef:46:35:

7c:26:78:1a:d9:28:fe:db:38:17:24:b1:f5:f9:0e:

d3:99:6a:8c:4b:9d:20:3f:83:cd:df:c5:71:af:8b:

61:46:3d:4b:1b:14:bc:80:7e:65:f3:b6:fe:8e:b2:

59:64

The part of the certificate that indicates this is a CA's certificate is the X509v3 Basic Constraints extension. Specifically, the following line:

X509v3 Basic Constraints: critical CA:TRUE

The part of the certificate that indicates it is self-signed can be inferred from two pieces of information:

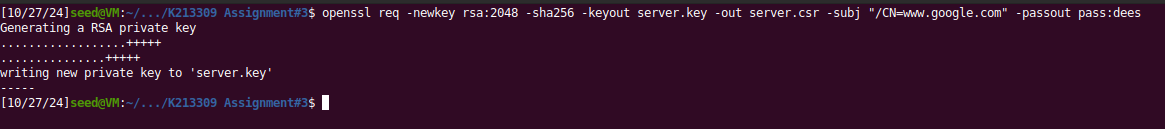
Issuer: C = PK, ST = Sindh, L = Karachi, O = FAST-NUCES

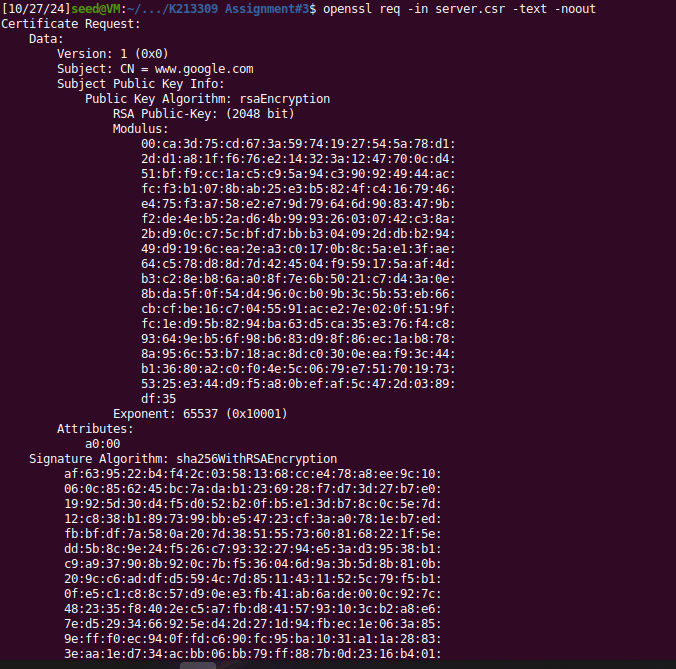
Subject: C = PK, ST = Sindh, L = Karachi, O = FAST-NUCES

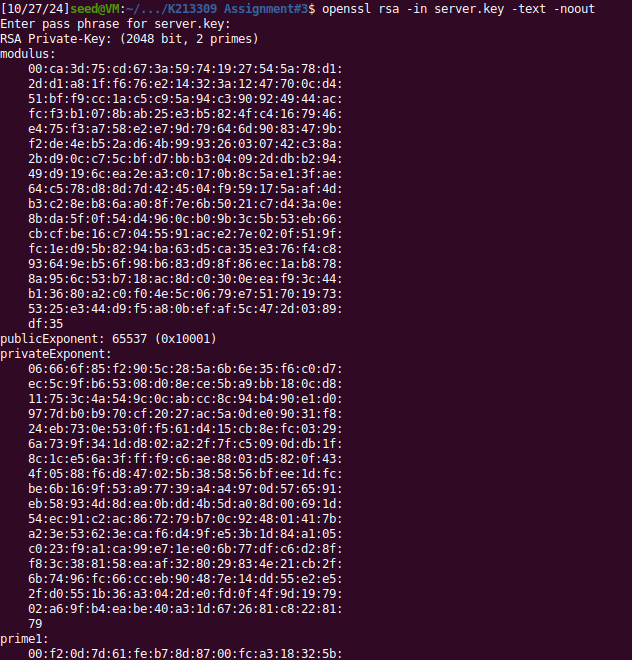
Both the Issuer and Subject fields are identical, indicating that the certificate is self-signed.

# Task#2

In this task, we will generate a certificate request for a web server. The command is given in the manual and the webserver we picked was google.com.

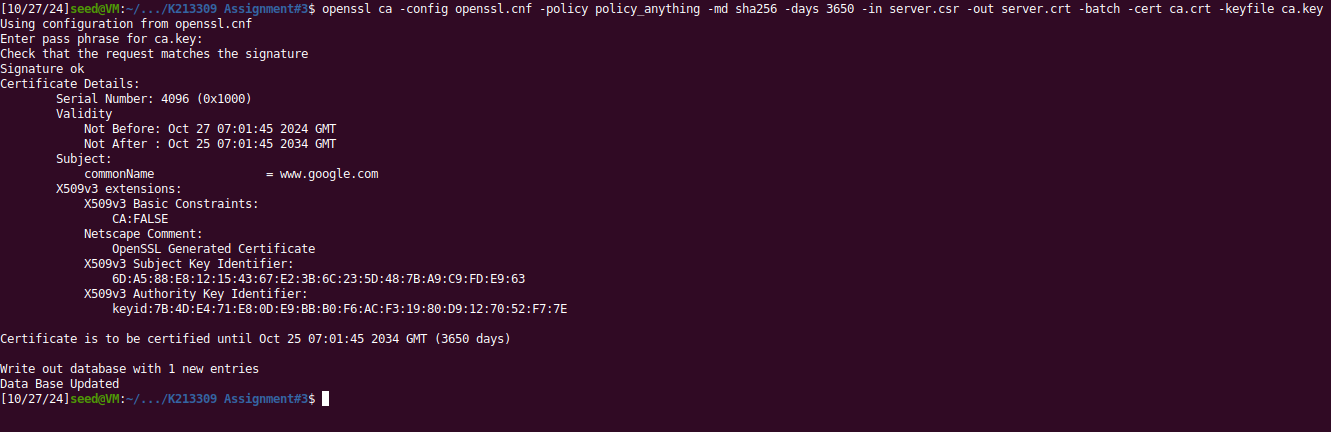




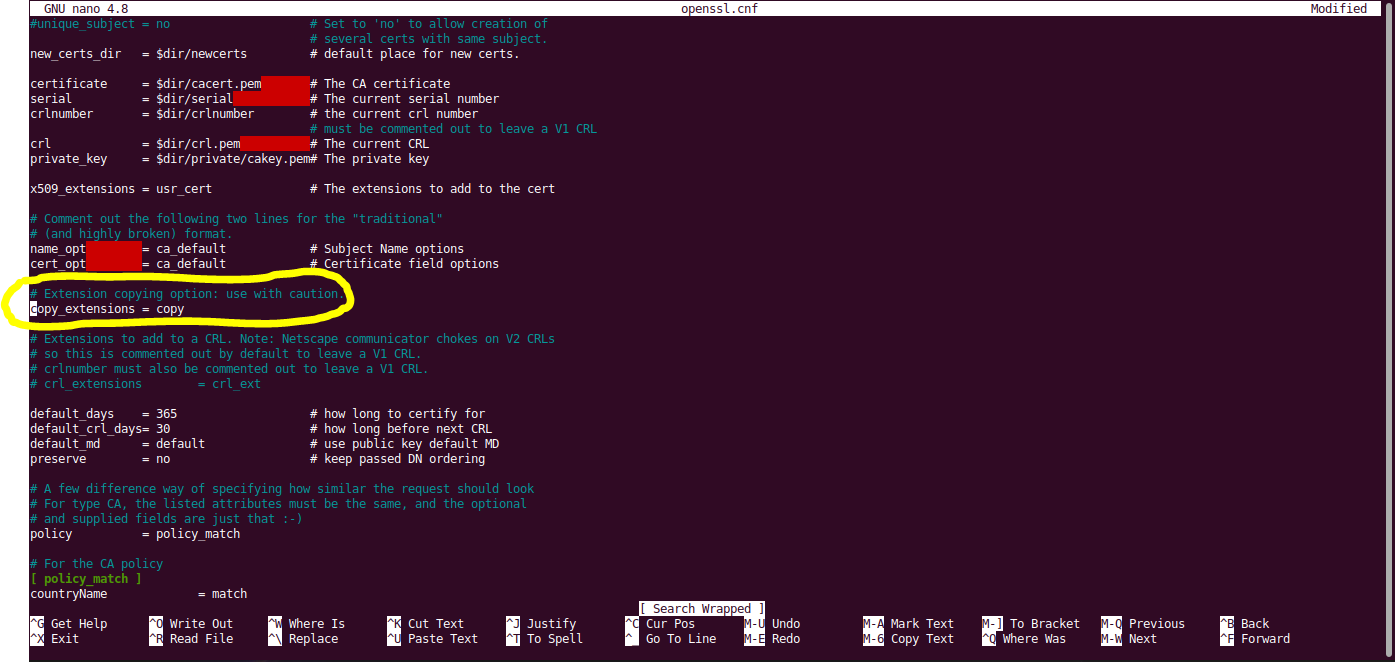


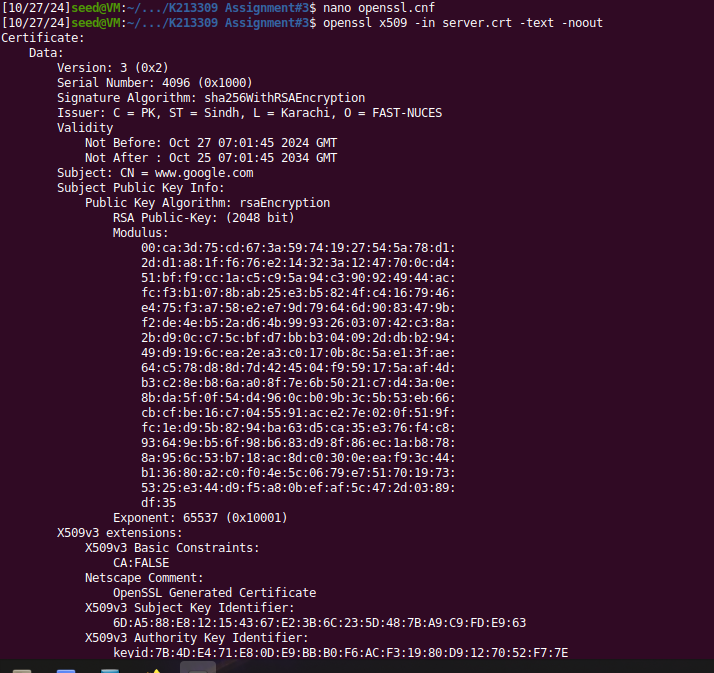
# Task#3

In this task, we will generate a certificate request for a server. we will use our own trusted CA to generate certificates. The following command turns the certificate signing request (server.csr) into an X509 certificate (server.crt), using the CA’s ca.crt and ca.key:



Further following the steps in manual:

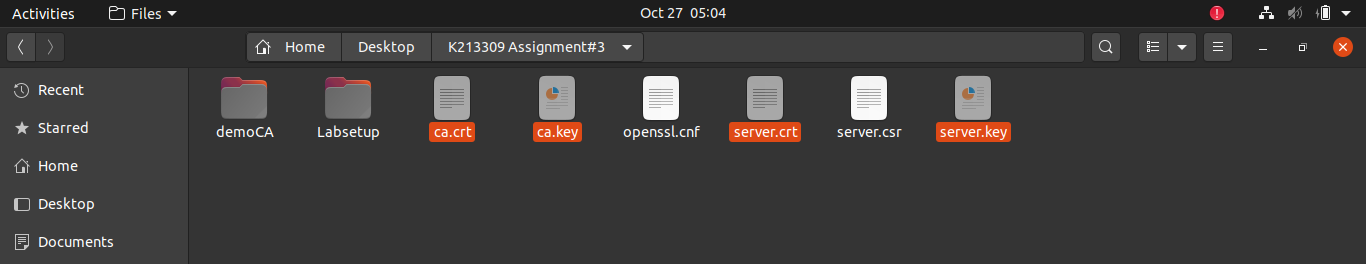


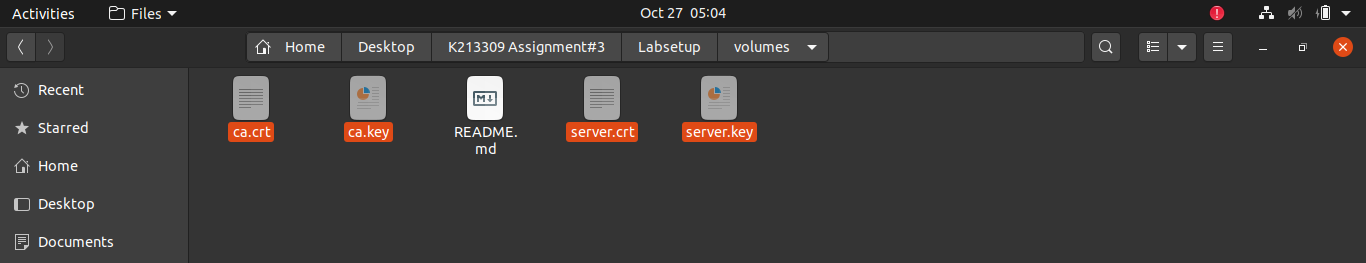


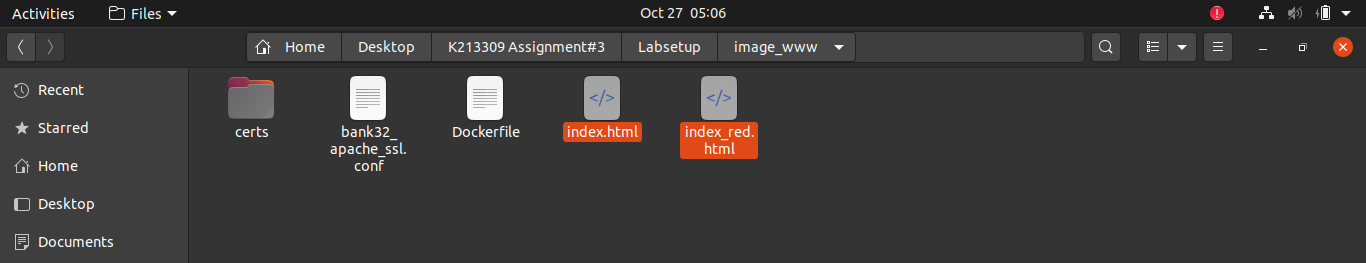
# Task#4

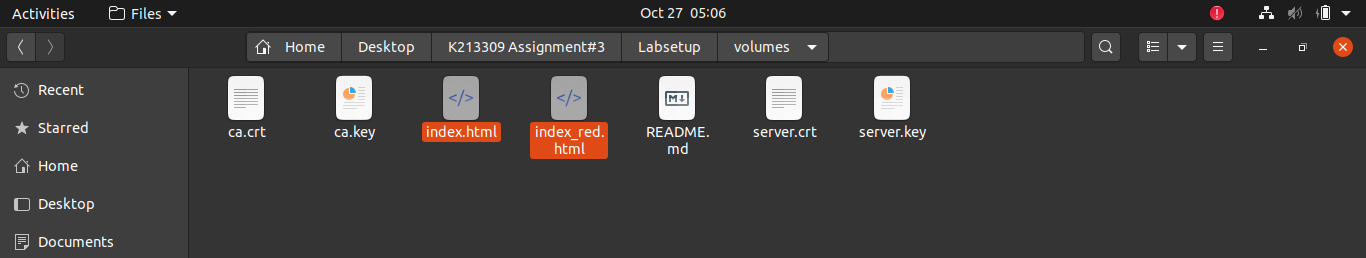
In this task, we will deploy a certificate in an Apache-based HTTPS website.

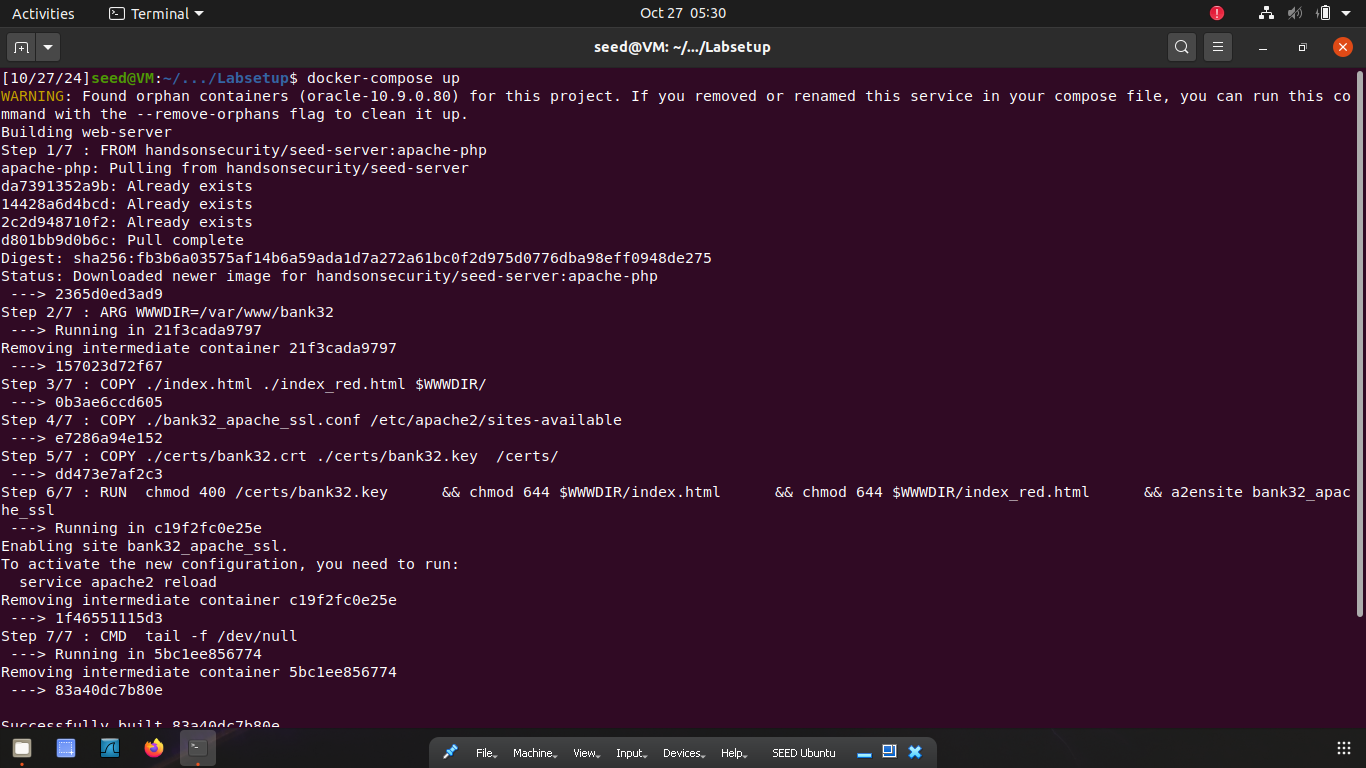
Firstly, we will need to copy the relevant files into the volumes folder so that the docker-compose can copy them over to the container.

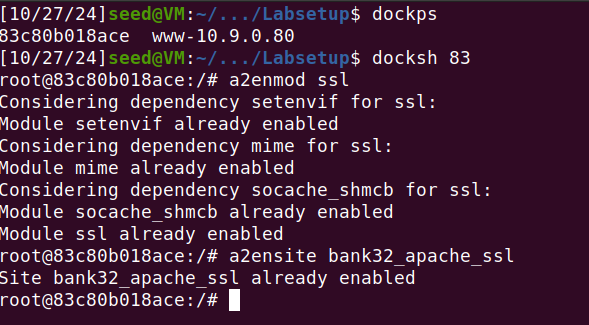




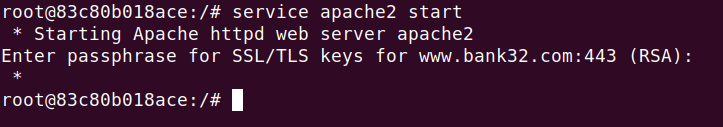




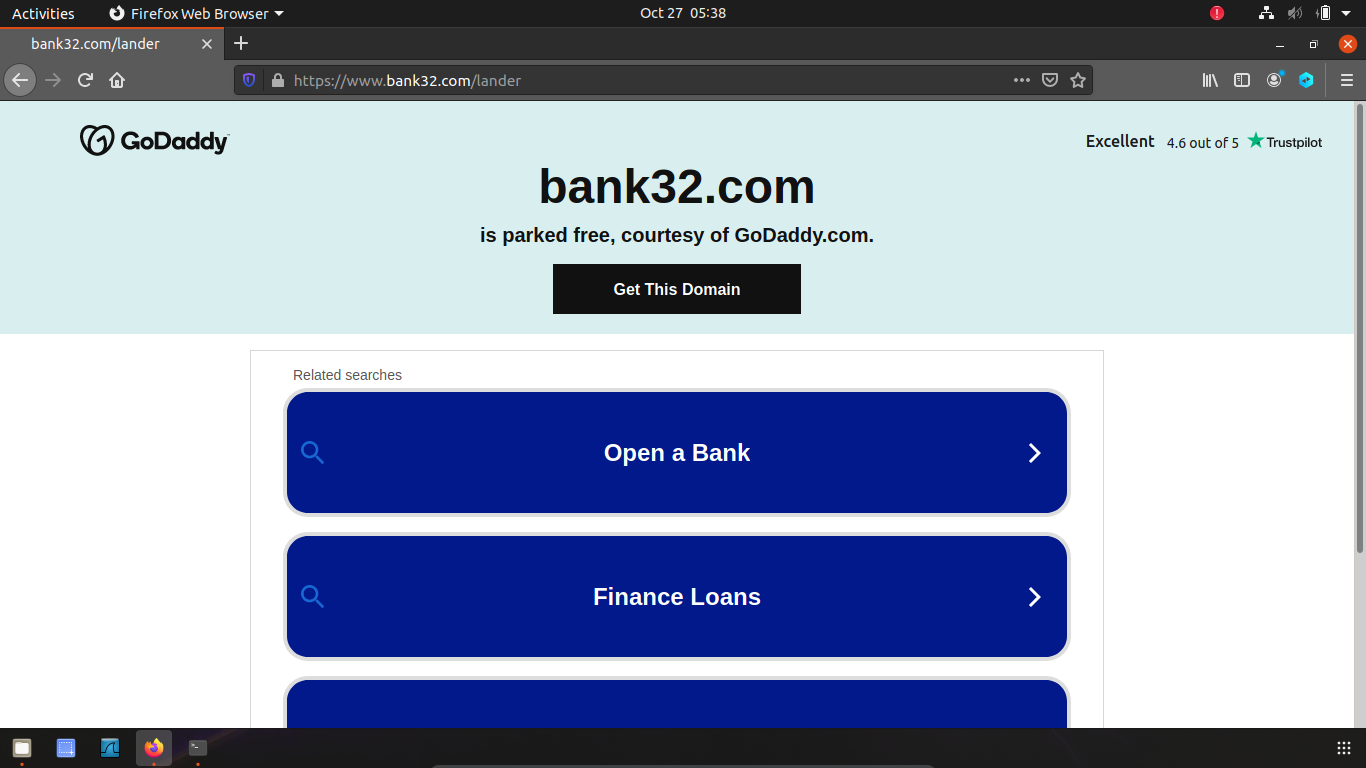
Now we compose our docker file and use it.



Then we follow the steps given in the manual.



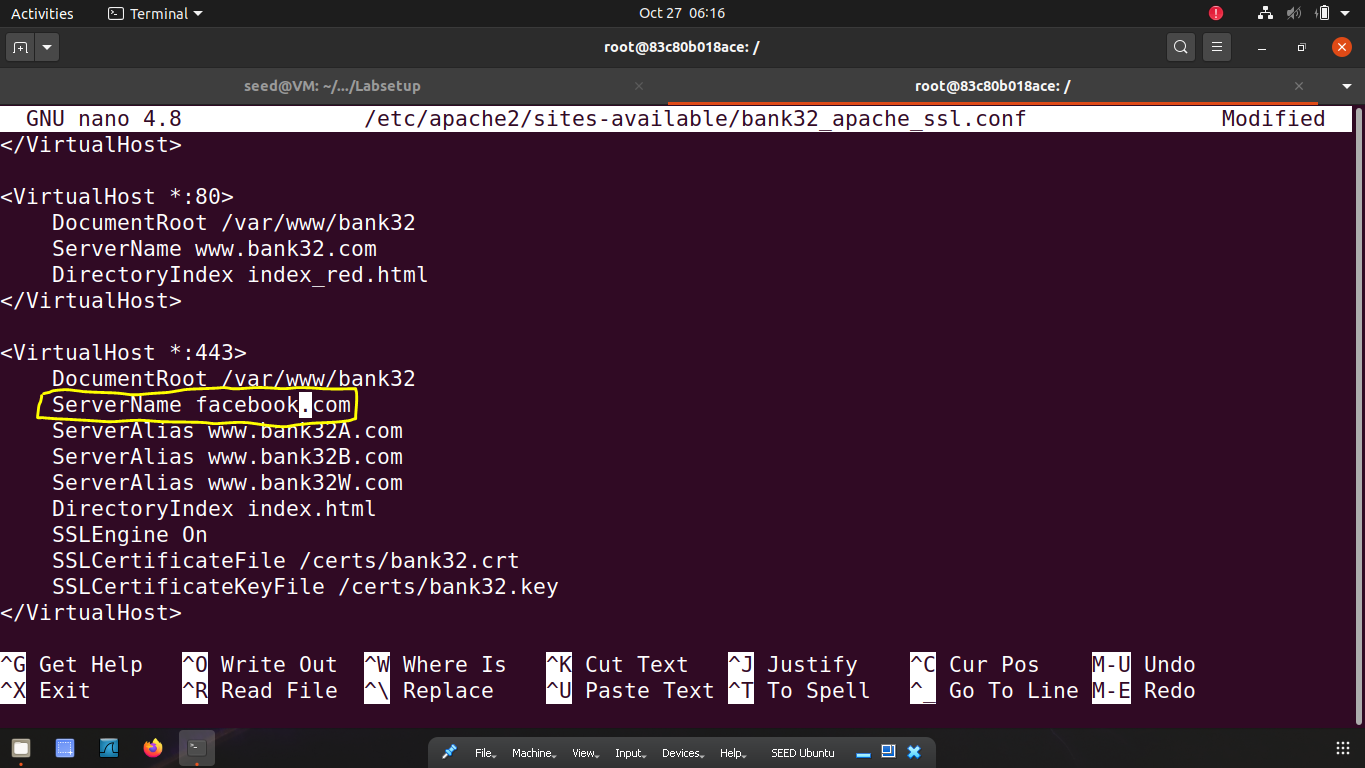
Finaly, we can access the website **ONLY USING HTTPS**.

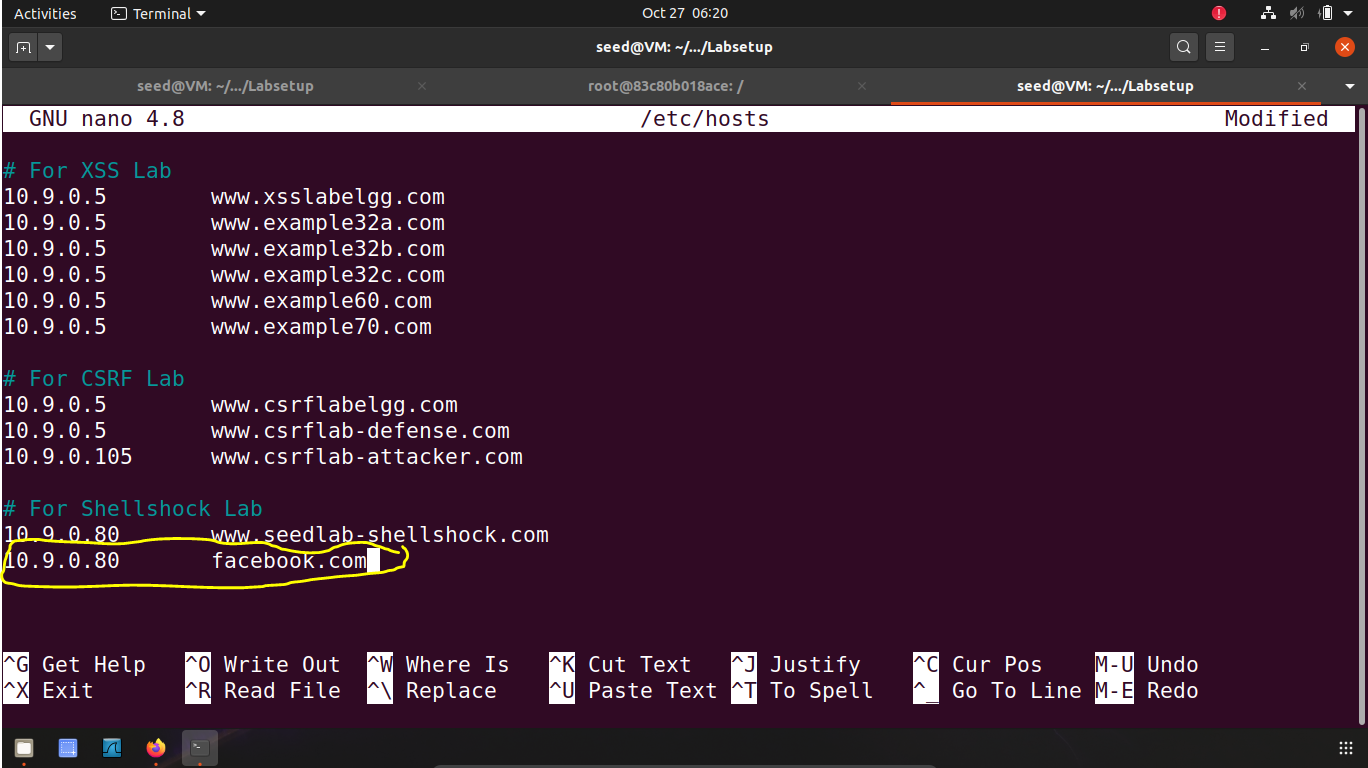


# Task#5

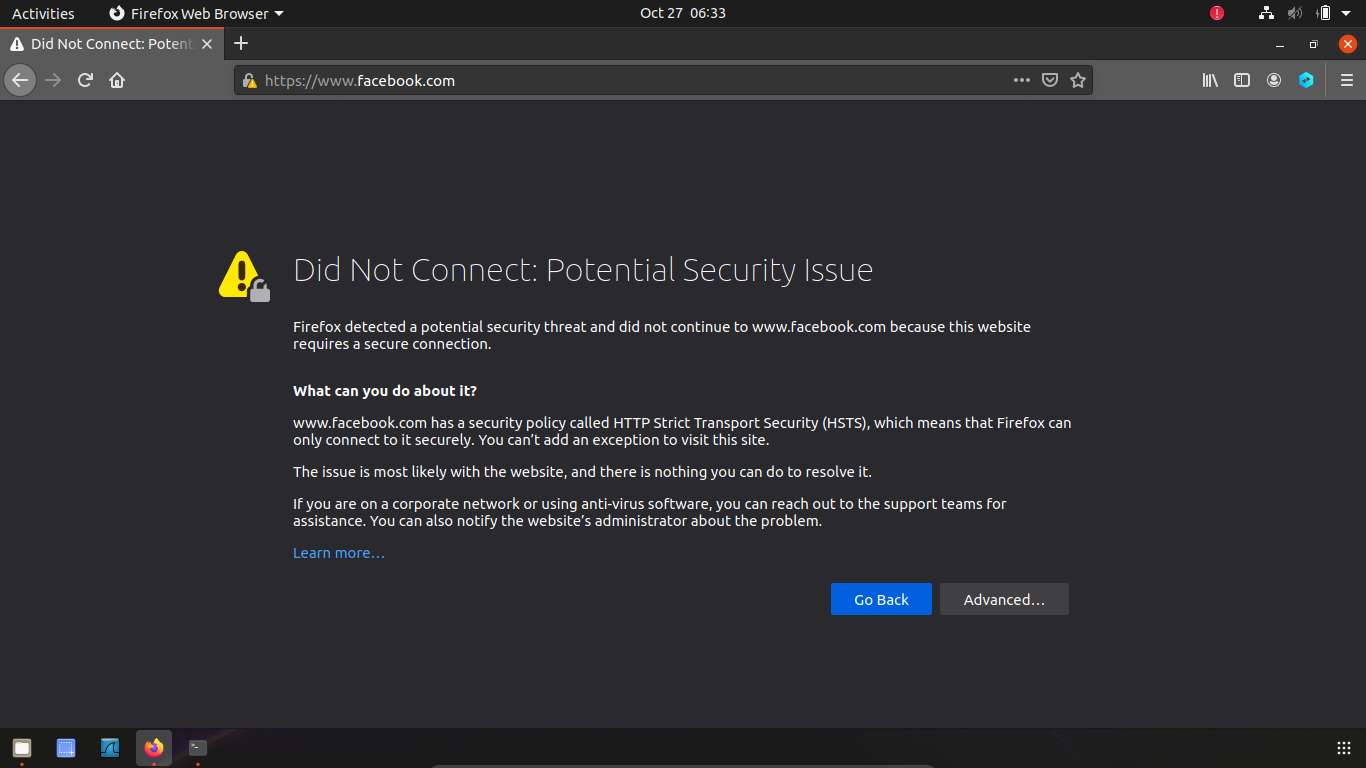
In this task, we will show how PKI can defeat Man-In-The-Middle (MITM) attacks. We will be using facebook.com as an example.

We will first add facebook.com in the apache server.



Next we will modify the /etc/hosts file and add facebook. 

The final result being that our browser doesn’t let us access facebook because it found a different certificate than ours.



# Task#6

Once we use the server.key file to get to crt file we can try to access the facebook page.



As you can see the facebook page is redirected elsewhere.

