Security Engineering
Lab 4

Siddharth Sharma 2014108
Pankaj Kumar Anuragi 2014073

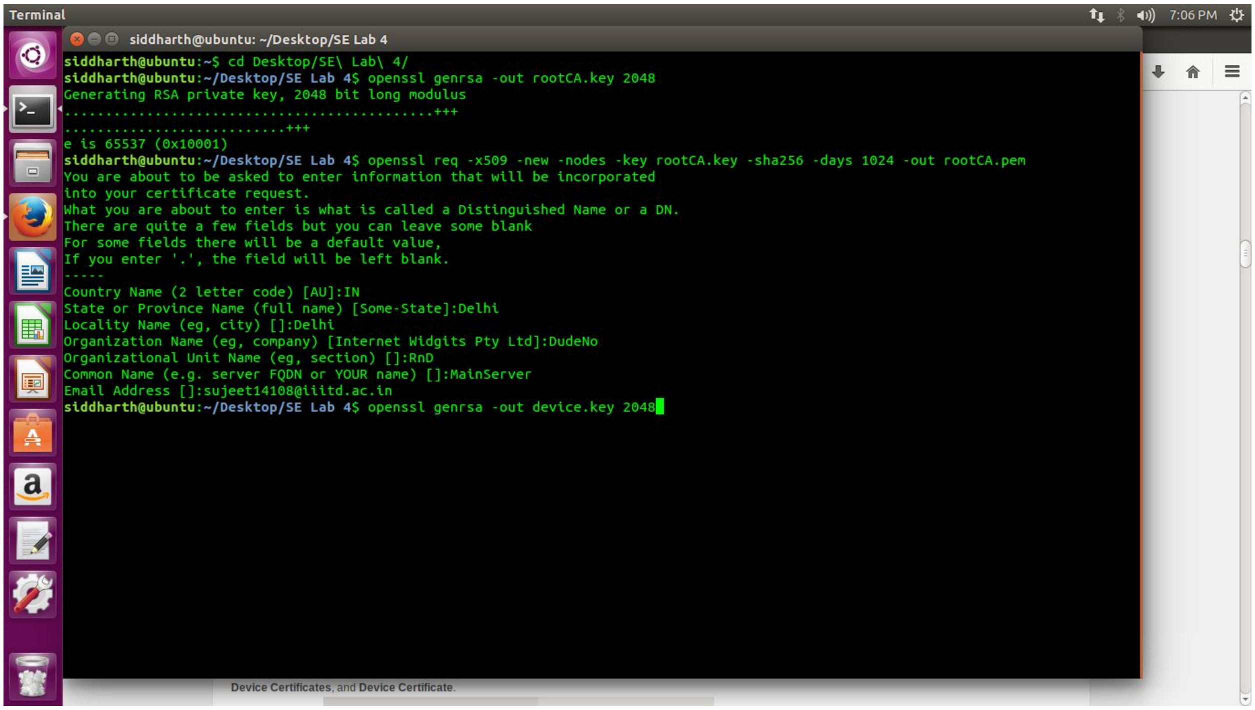
Part 1 :
Generating Root Key and Certificate

Key

- openssl genrsa -out rootCA.key 2048

Generate Self-signed Certificate

- openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem


Terminal
7:06 PM
siddharth@ubuntu: ~/Desktop/SE Lab 4
Device Certificates, and Device Certificate.

```
siddharth@ubuntu:~$ cd Desktop/SE\ Lab\ 4/
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl genrsa -out rootCA.key 2048
Generating RSA private key, 2048 bit long modulus
.............................................+++
...........................+++
e is 65537 (0x10001)
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Delhi
Locality Name (eg, city) []:Delhi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DudeNo
Organizational Unit Name (eg, section) []:RnD
Common Name (e.g. server FQDN or YOUR name) []:MainServer
Email Address []:sujeet14108@iiitd.ac.in
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl genrsa -out device.key 2048
```

Generating Server Public Key, Private Key and Certificate

Private key

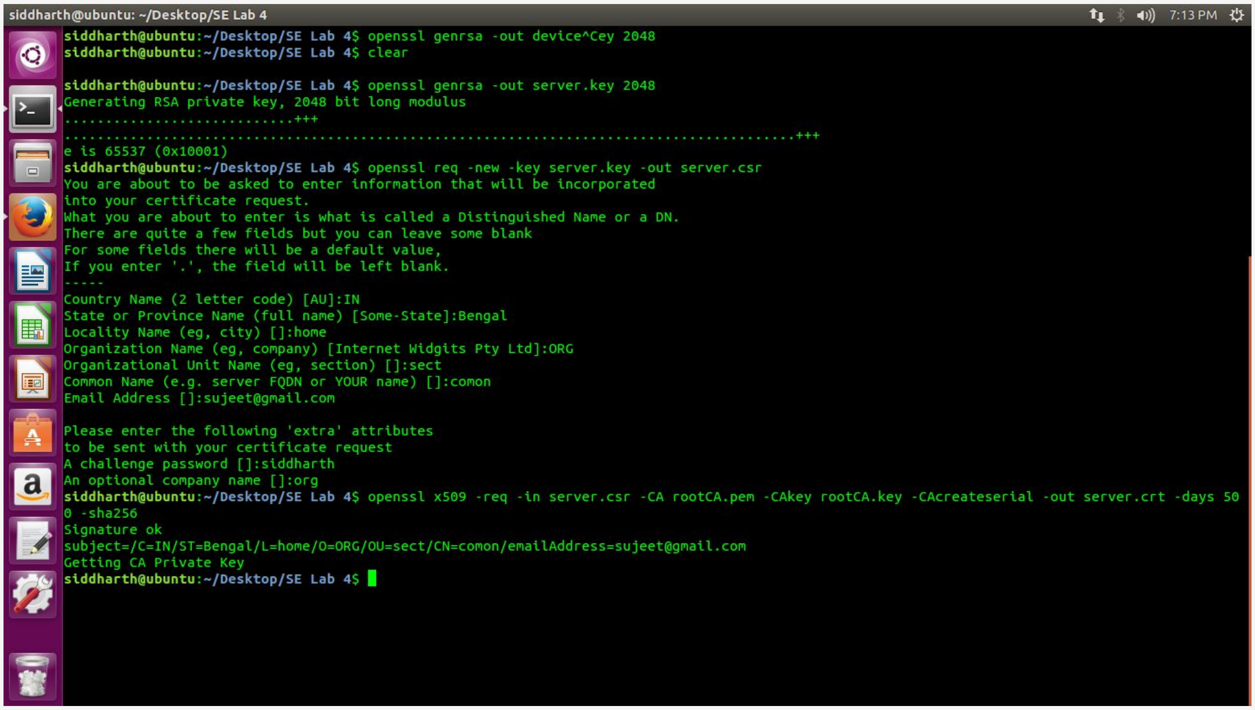
- openssl genrsa -out server.key 2048

Public key

- openssl req -new -key server.key -out server.csr

Generate Self-signed Certificate (Validity : 500 days)

- openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out server.crt -days 500 -sha256



```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl genrsa -out device^Cey 2048
siddharth@ubuntu:~/Desktop/SE Lab 4$ clear

siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus
............................+++
.........................................................................................+++
e is 65537 (0x10001)
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Bengal
Locality Name (eg, city) []:home
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ORG
Organizational Unit Name (eg, section) []:sect
Common Name (e.g. server FQDN or YOUR name) []:comon
Email Address []:sujeet@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:siddharth
An optional company name []:org
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out server.crt -days 50
0 -sha256
Signature ok
subject=/C=IN/ST=Bengal/L=home/O=ORG/OU=sect/CN=comon/emailAddress=sujeet@gmail.com
Getting CA Private Key
siddharth@ubuntu:~/Desktop/SE Lab 4$ 
```

Generating Server Public Key, Private Key and Certificate

Private key

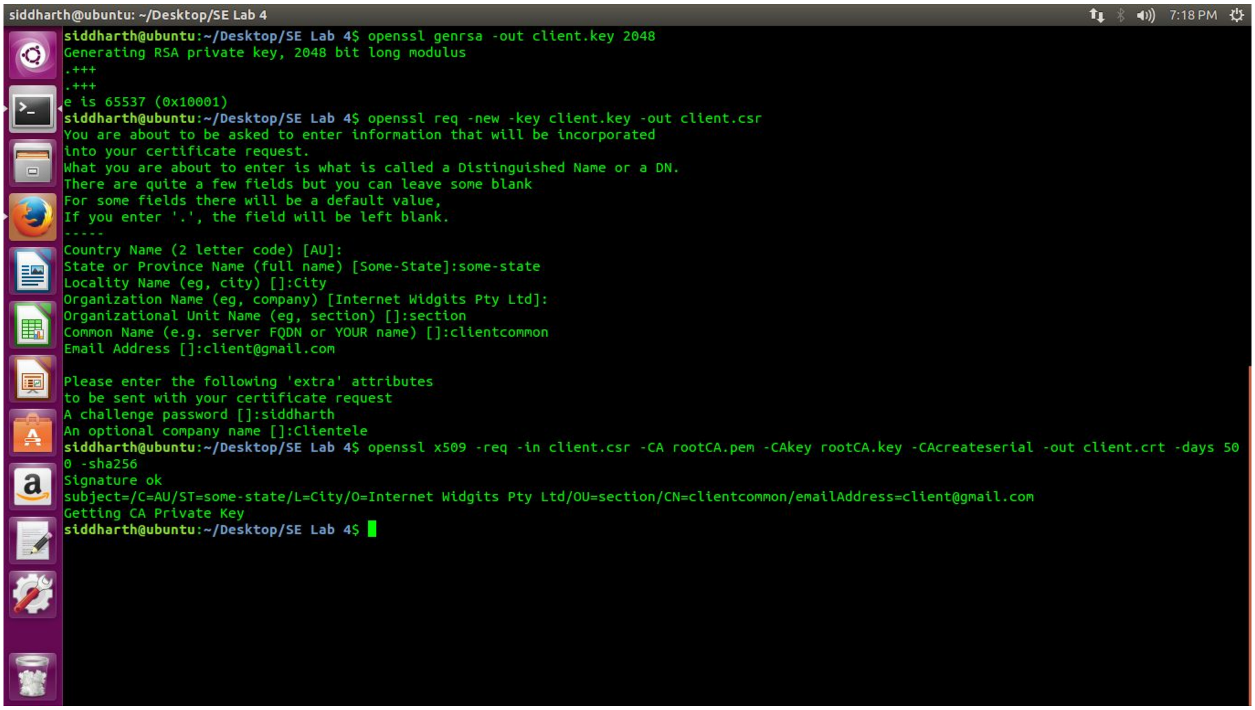
- openssl genrsa -out client.key 2048

Public key

- openssl req -new -key client.key -out client.csr

Generate Self-signed Certificate (Validity : 500 days)

- openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out client.crt -days 500 -sha256



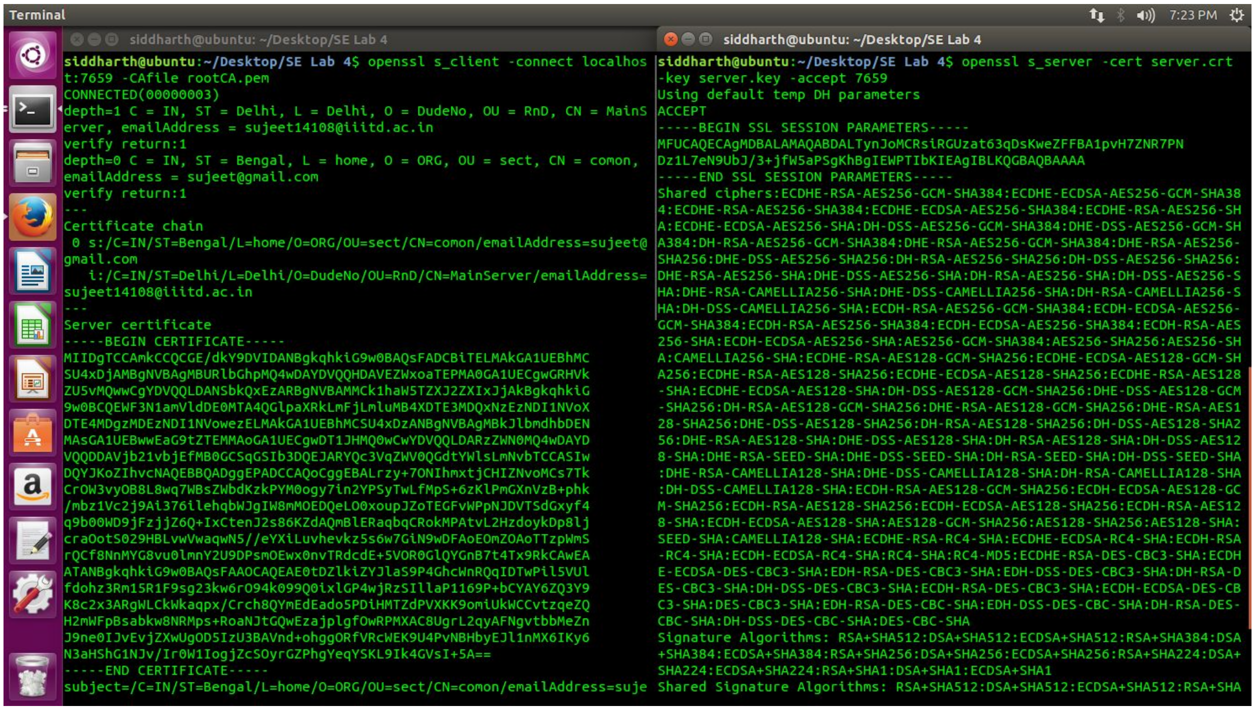
```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl genrsa -out client.key 2048
Generating RSA private key, 2048 bit long modulus
.+++
.+++
e is 65537 (0x10001)
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl req -new -key client.key -out client.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:some-state
Locality Name (eg, city) []:City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:section
Common Name (e.g. server FQDN or YOUR name) []:clientcommon
Email Address []:client@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:siddharth
An optional company name []:Clientele
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out client.crt -days 50
0 -sha256
Signature ok
subject=/C=AU/ST=some-state/L=City/O=Internet Widgits Pty Ltd/OU=section/CN=clientcommon/emailAddress=client@gmail.com
Getting CA Private Key
siddharth@ubuntu:~/Desktop/SE Lab 4$ 
```

Part 2 :

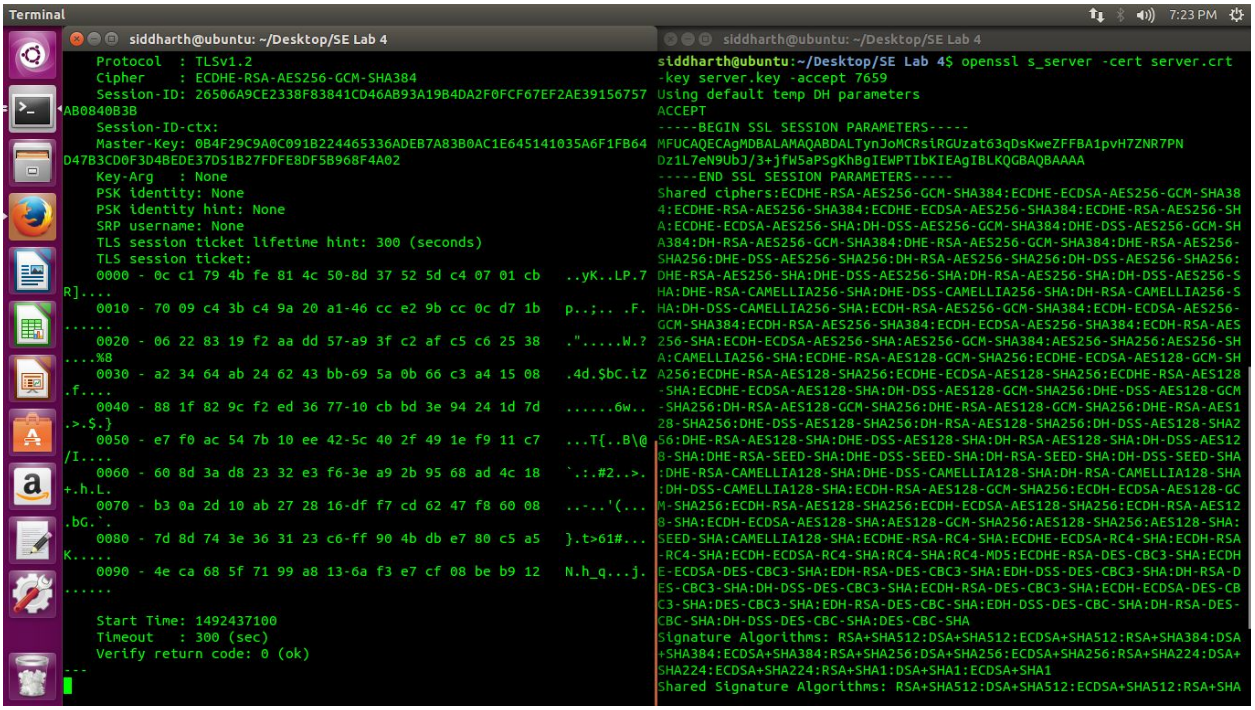
Start the Server : openssl s_server -cert server.crt -key server.key -accept 7658

Send a request from the client : openssl s_client -connect localhost:7658 -CAfile rootCA.pem


Terminal
7:23 PM
siddharth@ubuntu: ~/Desktop/SE Lab 4
siddharth@ubuntu: ~/Desktop/SE Lab 4

```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl s_client -connect localhos
t:7659 -CAfile rootCA.pem
CONNECTED(00000003)
depth=1 C = IN, ST = Delhi, L = Delhi, O = DudeNo, OU = RnD, CN = MainS
erver, emailAddress = sujeet14108@iiitd.ac.in
verify return:1
depth=0 C = IN, ST = Bengal, L = home, O = ORG, OU = sect, CN = comon,
emailAddress = sujeet@gmail.com
verify return:1
---
Certificate chain
 0 s:/C=IN/ST=Bengal/L=home/O=ORG/OU=sect/CN=comon/emailAddress=sujeet@
gmail.com
   i:/C=IN/ST=Delhi/L=Delhi/O=DudeNo/OU=RnD/CN=MainServer/emailAddress=
sujeet14108@iiitd.ac.in
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDgTCCAmkCCQCGE/dkY9DVIDANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMC
SU4xDjAMBgNVBAgMBURlbGhpMQ4wDAYDVQQHDAVEZWxoaTEPMA0GA1UECgwGRHVk
ZU5vMQwwCgYDVQQLDANSbkQxEzARBgNVBAMMCk1haW5TZXJ2ZXIxJjAkBgkqhkiG
9w0BCQEWF3N1amVldDE0MTA4QGlpaXRkLmFjLmluMB4XDTE3MDQxNzEzNDI1NVoX
DTE4MDgzMDEzNDI1NVowezELMAkGA1UEBhMCSU4xDzANBgNVBAgMBkJlbmdhbDEN
MAsGA1UEBwwEaG9tZTEMMAoGA1UECgwDT1JHMQ0wCwYDVQQLDARzZWN0MQ4wDAYD
VQQDDAVjb21vbjEfMB0GCSqGSIb3DQEJARYQc3VqZWV0QGdtYWlsLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALrzy+7ONIhmxtjCHIZNvoMCs7Tk
CrOW3vyOB8L8wq7WBsZWbdKzkPYM0ogy7in2YPSyTwLfMpS+6zKlPmGXnVzB+phk
/mbz1Vc2j9Ai376ilehqbWJgIW8mMOEDQeLO0xoupJZoTEGFvWPpNJDVTSdGxyf4
q9b00WD9jFzjjZ6Q+IxCtenJ2s86KZdAQmBlERaqbqCRokMPAtvL2HzdoykDp8lj
craOotS029HBLvwVwaqwN5//eYXiLuvhevkz5s6w7GiN9wDFAoEOmZOAoTTzpWmS
rQCf8NnMYG8vu0lmnY2U9DPsmOEwx0nvTRdcdE+5VOR0GlQYGnB7t4Tx9RkCAwEA
ATANBgkqhkiG9w0BAQsFAAOCAQEAE0tDZlkiZYJlaS9P4GhcWnRQqIDTwPil5VUl
fdohz3Rm15R1F9sg23kw6rO94k099Q0ixlGP4wjRzSIllaP1169P+bCYAY6ZQ3Y9
K8c2x3ARgWLCkWkaqpx/Crch8QYmEdEado5PDiHMTZdPVXKK9omiUkWCCvtzqeZQ
H2mWFpBsabkw8NRMps+RoaNJtGQwEzajplgfOwRPMXAC8UgrL2qyAFNgvtbbMeZn
J9ne0IJvEvjZXwUgOD5IzU3BAVnd+ohggORfVRcWEK9U4PvNBHbyEJl1nMX6IKy6
N3aHShG1NJv/Ir0W1IogjZcSOyrGZPhgYeqYSKL9Ik4GVsI+5A==
-----END CERTIFICATE-----
subject=/C=IN/ST=Bengal/L=home/O=ORG/OU=sect/CN=comon/emailAddress=suje
```

```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl s_server -cert server.crt
-key server.key -accept 7659
Using default temp DH parameters
ACCEPT
-----BEGIN SSL SESSION PARAMETERS-----
MFUCAQECAgMDBALAMAQABDALTynJoMCRsiRGUzat63qDsKweZFFBA1pvH7ZNR7PN
Dz1L7eN9UbJ/3+jfW5aPSgKhBgIEWPTIbKIEAgIBLKQGBAQBAAAA
-----END SSL SESSION PARAMETERS-----
Shared ciphers:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA38
4:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SH
A:ECDHE-ECDSA-AES256-SHA:DH-DSS-AES256-GCM-SHA384:DHE-DSS-AES256-GCM-SH
A384:DH-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
SHA256:DHE-DSS-AES256-SHA256:DH-RSA-AES256-SHA256:DH-DSS-AES256-SHA256:
DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DH-RSA-AES256-SHA:DH-DSS-AES256-S
HA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:DH-RSA-CAMELLIA256-S
HA:DH-DSS-CAMELLIA256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-
GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES
256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SH
A:CAMELLIA256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SH
A256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128
-SHA:ECDHE-ECDSA-AES128-SHA:DH-DSS-AES128-GCM-SHA256:DHE-DSS-AES128-GCM
-SHA256:DH-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES1
28-SHA256:DHE-DSS-AES128-SHA256:DH-RSA-AES128-SHA256:DH-DSS-AES128-SHA2
56:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DH-RSA-AES128-SHA:DH-DSS-AES12
8-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DH-RSA-SEED-SHA:DH-DSS-SEED-SHA
:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:DH-RSA-CAMELLIA128-SHA
:DH-DSS-CAMELLIA128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GC
M-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES12
8-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:
SEED-SHA:CAMELLIA128-SHA:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:ECDH-RSA
-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:ECDHE-RSA-DES-CBC3-SHA:ECDH
E-ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DH-RSA-D
ES-CBC3-SHA:DH-DSS-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:ECDH-ECDSA-DES-CB
C3-SHA:DES-CBC3-SHA:EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:DH-RSA-DES-
CBC-SHA:DH-DSS-DES-CBC-SHA:DES-CBC-SHA
Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA384:DSA
+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:ECDSA+SHA256:RSA+SHA224:DSA+
SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
Shared Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA
```


Terminal
7:23 PM
siddharth@ubuntu: ~/Desktop/SE Lab 4
siddharth@ubuntu: ~/Desktop/SE Lab 4

```
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 26506A9CE2338F83841CD46AB93A19B4DA2F0FCF67EF2AE39156757
AB0840B3B
    Session-ID-ctx:
    Master-Key: 0B4F29C9A0C091B224465336ADEB7A83B0AC1E645141035A6F1FB64
D47B3CD0F3D4BEDE37D51B27FDFE8DF5B968F4A02
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 0c c1 79 4b fe 81 4c 50-8d 37 52 5d c4 07 01 cb   ..yK..LP.7
R]....
    0010 - 70 09 c4 3b c4 9a 20 a1-46 cc e2 9b cc 0c d7 1b   p..;.. .F.
......
    0020 - 06 22 83 19 f2 aa dd 57-a9 3f c2 af c5 c6 25 38   .".....W.?
....%8
    0030 - a2 34 64 ab 24 62 43 bb-69 5a 0b 66 c3 a4 15 08   .4d.$bC.iZ
.f....
    0040 - 88 1f 82 9c f2 ed 36 77-10 cb bd 3e 94 24 1d 7d   ......6w..
.>.$.}
    0050 - e7 f0 ac 54 7b 10 ee 42-5c 40 2f 49 1e f9 11 c7   ...T{..B\@
/I....
    0060 - 60 8d 3a d8 23 32 e3 f6-3e a9 2b 95 68 ad 4c 18   `.:.#2..>.
+.h.L.
    0070 - b3 0a 2d 10 ab 27 28 16-df f7 cd 62 47 f8 60 08   ..-..'(...
.bG.`.
    0080 - 7d 8d 74 3e 36 31 23 c6-ff 90 4b db e7 80 c5 a5   }.t>61#...
K.....
    0090 - 4e ca 68 5f 71 99 a8 13-6a f3 e7 cf 08 be b9 12   N.h_q...j.
......

    Start Time: 1492437100
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

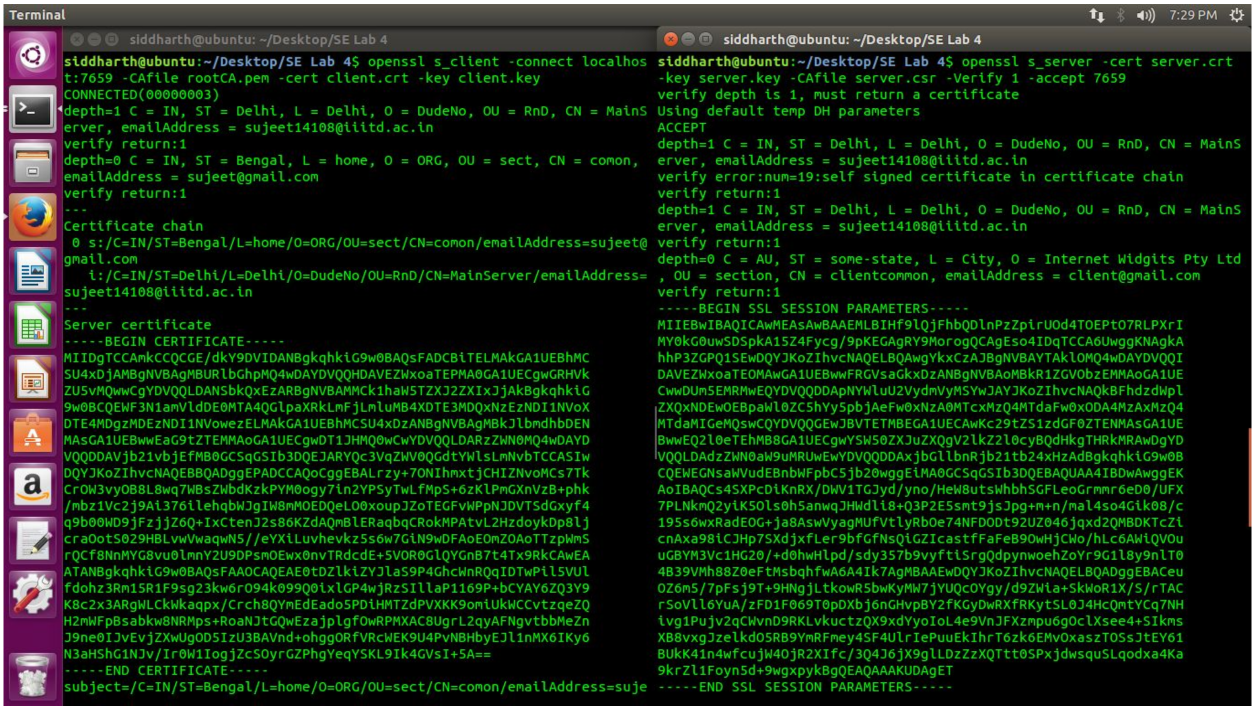
```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl s_server -cert server.crt
-key server.key -accept 7659
Using default temp DH parameters
ACCEPT
-----BEGIN SSL SESSION PARAMETERS-----
MFUCAQECAgMDBALAMAQABDALTynJoMCRsiRGUzat63qDsKweZFFBA1pvH7ZNR7PN
Dz1L7eN9UbJ/3+jfW5aPSgKhBgIEWPTIbKIEAgIBLKQGBAQBAAAA
-----END SSL SESSION PARAMETERS-----
Shared ciphers:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA38
4:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SH
A:ECDHE-ECDSA-AES256-SHA:DH-DSS-AES256-GCM-SHA384:DHE-DSS-AES256-GCM-SH
A384:DH-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
SHA256:DHE-DSS-AES256-SHA256:DH-RSA-AES256-SHA256:DH-DSS-AES256-SHA256:
DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DH-RSA-AES256-SHA:DH-DSS-AES256-S
HA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:DH-RSA-CAMELLIA256-S
HA:DH-DSS-CAMELLIA256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-
GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES
256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SH
A:CAMELLIA256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SH
A256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128
-SHA:ECDHE-ECDSA-AES128-SHA:DH-DSS-AES128-GCM-SHA256:DHE-DSS-AES128-GCM
-SHA256:DH-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES1
28-SHA256:DHE-DSS-AES128-SHA256:DH-RSA-AES128-SHA256:DH-DSS-AES128-SHA2
56:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DH-RSA-AES128-SHA:DH-DSS-AES12
8-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DH-RSA-SEED-SHA:DH-DSS-SEED-SHA
:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:DH-RSA-CAMELLIA128-SHA
:DH-DSS-CAMELLIA128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GC
M-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES12
8-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:
SEED-SHA:CAMELLIA128-SHA:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:ECDH-RSA
-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:ECDHE-RSA-DES-CBC3-SHA:ECDH
E-ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DH-RSA-D
ES-CBC3-SHA:DH-DSS-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:ECDH-ECDSA-DES-CB
C3-SHA:DES-CBC3-SHA:EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:DH-RSA-DES-
CBC-SHA:DH-DSS-DES-CBC-SHA:DES-CBC-SHA
Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA384:DSA
+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:ECDSA+SHA256:RSA+SHA224:DSA+
SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
Shared Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA
```

Part 3 :

Run server in verification mode. Option -Verify ensures that the client has to send their certificate.

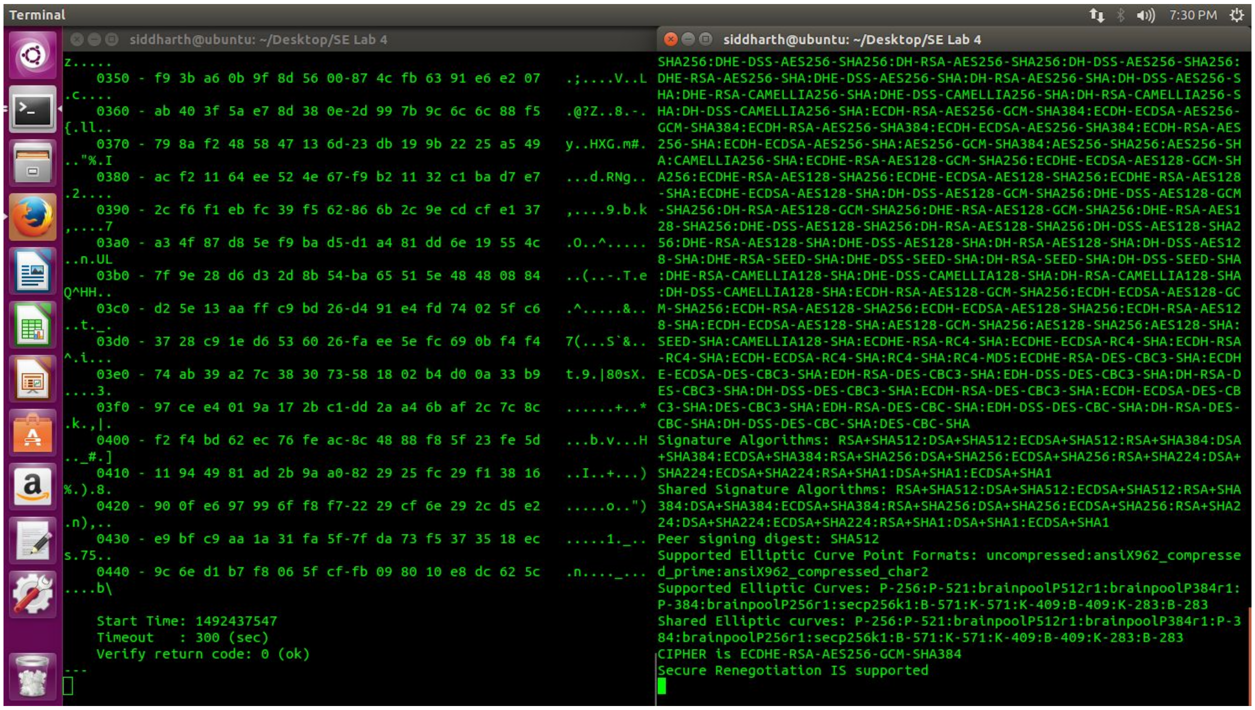
Server : openssl s_server -cert server.crt -CAfile server.csr -key server.key -Verify 1 -accept 7659

Client : openssl s_client -connect localhost:7659 -CAfile rootCA.pem -cert client.crt -key client.key


Terminal
7:29 PM
siddharth@ubuntu: ~/Desktop/SE Lab 4
siddharth@ubuntu: ~/Desktop/SE Lab 4

```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl s_client -connect localhos
t:7659 -CAfile rootCA.pem -cert client.crt -key client.key
CONNECTED(00000003)
depth=1 C = IN, ST = Delhi, L = Delhi, O = DudeNo, OU = RnD, CN = MainS
erver, emailAddress = sujeet14108@iiitd.ac.in
verify return:1
depth=0 C = IN, ST = Bengal, L = home, O = ORG, OU = sect, CN = comon,
emailAddress = sujeet@gmail.com
verify return:1
---
Certificate chain
 0 s:/C=IN/ST=Bengal/L=home/O=ORG/OU=sect/CN=comon/emailAddress=sujeet@
gmail.com
   i:/C=IN/ST=Delhi/L=Delhi/O=DudeNo/OU=RnD/CN=MainServer/emailAddress=
sujeet14108@iiitd.ac.in
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDgTCCAmkCCQCGE/dkY9DVIDANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMC
SU4xDjAMBgNVBAgMBURlbGhpMQ4wDAYDVQQHDAVEZWxoaTEPMA0GA1UECgwGRHVk
ZU5vMQwwCgYDVQQLDANSbkQxEzARBgNVBAMMCk1haW5TZXJ2ZXIxJjAkBgkqhkiG
9w0BCQEWF3N1amVldDE0MTA4QGlpaXRkLmFjLmluMB4XDTE3MDQxNzEzNDI1NVoX
DTE4MDgzMDEzNDI1NVowezELMAkGA1UEBhMCSU4xDzANBgNVBAgMBkJlbmdhbDEN
MAsGA1UEBwwEaG9tZTEMMAoGA1UECgwDT1JHMQ0wCwYDVQQLDARzZWN0MQ4wDAYD
VQQDDAVjb21vbjEfMB0GCSqGSIb3DQEJARYQc3VqZWV0QGdtYWlsLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALrzy+7ONIhmxtjCHIZNvoMCs7Tk
CrOW3vyOB8L8wq7WBsZWbdKzkPYM0ogy7in2YPSyTwLfMpS+6zKlPmGXnVzB+phk
/mbz1Vc2j9Ai376ilehqbWJgIW8mMOEDQeLO0xoupJZoTEGFvWPpNJDVTSdGxyf4
q9b00WD9jFzjjZ6Q+IxCtenJ2s86KZdAQmBlERaqbqCRokMPAtvL2HzdoykDp8lj
craOotS029HBLvwVwaqwN5//eYXiLuvhevkz5s6w7GiN9wDFAoEOmZOAoTTzpWmS
rQCf8NnMYG8vu0lmnY2U9DPsmOEwx0nvTRdcdE+5VOR0GlQYGnB7t4Tx9RkCAwEA
ATANBgkqhkiG9w0BAQsFAAOCAQEAE0tDZlkiZYJlaS9P4GhcWnRQqIDTwPil5VUl
fdohz3Rm15R1F9sg23kw6rO94k099Q0ixlGP4wjRzSIllaP1169P+bCYAY6ZQ3Y9
K8c2x3ARgWLCkWkaqpx/Crch8QYmEdEado5PDiHMTZdPVXKK9omiUkWCCvtzqeZQ
H2mWFpBsabkw8NRMps+RoaNJtGQwEzajplgfOwRPMXAC8UgrL2qyAFNgvtbbMeZn
J9ne0IJvEvjZXwUgOD5IzU3BAVnd+ohggORfVRcWEK9U4PvNBHbyEJl1nMX6IKy6
N3aHShG1NJv/Ir0W1IogjZcSOyrGZPhgYeqYSKL9Ik4GVsI+5A==
-----END CERTIFICATE-----
subject=/C=IN/ST=Bengal/L=home/O=ORG/OU=sect/CN=comon/emailAddress=suje
```

```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl s_server -cert server.crt
-key server.key -CAfile server.csr -Verify 1 -accept 7659
verify depth is 1, must return a certificate
Using default temp DH parameters
ACCEPT
depth=1 C = IN, ST = Delhi, L = Delhi, O = DudeNo, OU = RnD, CN = MainS
erver, emailAddress = sujeet14108@iiitd.ac.in
verify error:num=19:self signed certificate in certificate chain
verify return:1
depth=1 C = IN, ST = Delhi, L = Delhi, O = DudeNo, OU = RnD, CN = MainS
erver, emailAddress = sujeet14108@iiitd.ac.in
verify return:1
depth=0 C = AU, ST = some-state, L = City, O = Internet Widgits Pty Ltd
, OU = section, CN = clientcommon, emailAddress = client@gmail.com
verify return:1
-----BEGIN SSL SESSION PARAMETERS-----
MIIEBwIBAQICAwMEAsAwBAAEMLBIHf9lQjFhbQDlnPzZpirUOd4TOEPtO7RLPXrI
MY0kG0uwSDSpkA15Z4Fycg/9pKEGAgRY9MorogQCAgEso4IDqTCCA6UwggKNAgkA
hhP3ZGPQ1SEwDQYJKoZIhvcNAQELBQAwgYkxCzAJBgNVBAYTAklOMQ4wDAYDVQQI
DAVEZWxoaTEOMAwGA1UEBwwFRGVsaGkxDzANBgNVBAoMBkR1ZGVObzEMMAoGA1UE
CwwDUm5EMRMwEQYDVQQDDApNYWluU2VydmVyMSYwJAYJKoZIhvcNAQkBFhdzdWpl
ZXQxNDEwOEBpaWl0ZC5hYy5pbjAeFw0xNzA0MTcxMzQ4MTdaFw0xODA4MzAxMzQ4
MTdaMIGeMQswCQYDVQQGEwJBVTETMBEGA1UECAwKc29tZS1zdGF0ZTENMAsGA1UE
BwwEQ2l0eTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYD
VQQLDAdzZWN0aW9uMRUwEwYDVQQDDAxjbGllbnRjb21tb24xHzAdBgkqhkiG9w0B
CQEWEGNsaWVudEBnbWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCs4SXPcDiKnRX/DWV1TGJyd/yno/HeW8utsWhbhSGFLeoGrmmr6eD0/UFX
7PLNkmQ2yiK5Ols0h5anwqJHWdli8+Q3P2E5smt9jsJpg+m+n/mal4so4Gik08/c
195s6wxRadEOG+ja8AswVyagMUfVtlyRbOe74NFDODt92UZ046jqxd2QMBDKTcZi
cnAxa98iCJHp7SXdjxfLer9bfGfNsQiGZIcastfFaFeB9OwHjCWo/hLc6AWiQVOu
uGBYM3Vc1HG20/+d0hwHlpd/sdy357b9vyftiSrgQdpynwoehZoYr9G1l8y9nlT0
4B39VMh88Z0eFtMsbqhfwA6A4Ik7AgMBAAEwDQYJKoZIhvcNAQELBQADggEBACeu
OZ6m5/7pFsj9T+9HNgjLtkowR5bwKyMW7jYUQcOYgy/d9ZWia+SkWoR1X/S/rTAC
rSoVll6YuA/zFD1F069T0pDXbj6nGHvpBY2fKGyDwRXfRKytSL0J4HcQmtYCq7NH
ivg1Pujv2qCWvnD9RKLvkuctzQX9xdYyoIoL4e9VnJFXzmpu6gOclXsee4+SIkms
XB8vxgJzelkdO5RB9YmRFmey4SF4UlrIePuuEkIhrT6zk6EMvOxaszTOSsJtEY61
BUkK41n4wfcujW4OjR2XIfc/3Q4J6jX9glLDzZzXQTtt0SPxjdwsquSLqodxa4Ka
9krZl1Foyn5d+9wgxpykBgQEAQAAAKUDAgET
-----END SSL SESSION PARAMETERS-----
```


Terminal
7:30 PM
siddharth@ubuntu: ~/Desktop/SE Lab 4
siddharth@ubuntu: ~/Desktop/SE Lab 4

```
z.....
    0350 - f9 3b a6 0b 9f 8d 56 00-87 4c fb 63 91 e6 e2 07   .;....V..L
.c....
    0360 - ab 40 3f 5a e7 8d 38 0e-2d 99 7b 9c 6c 6c 88 f5   .@?Z..8.-.
{.ll..
    0370 - 79 8a f2 48 58 47 13 6d-23 db 19 9b 22 25 a5 49   y..HXG.m#.
.."%.I
    0380 - ac f2 11 64 ee 52 4e 67-f9 b2 11 32 c1 ba d7 e7   ...d.RNg..
.2....
    0390 - 2c f6 f1 eb fc 39 f5 62-86 6b 2c 9e cd cf e1 37   ,....9.b.k
,....7
    03a0 - a3 4f 87 d8 5e f9 ba d5-d1 a4 81 dd 6e 19 55 4c   .O..^.....
..n.UL
    03b0 - 7f 9e 28 d6 d3 2d 8b 54-ba 65 51 5e 48 48 08 84   ..(..-.T.e
Q^HH..
    03c0 - d2 5e 13 aa ff c9 bd 26-d4 91 e4 fd 74 02 5f c6   .^.....&..
..t._.
    03d0 - 37 28 c9 1e d6 53 60 26-fa ee 5e fc 69 0b f4 f4   7(...S`&..
^.i...
    03e0 - 74 ab 39 a2 7c 38 30 73-58 18 02 b4 d0 0a 33 b9   t.9.|80sX.
....3.
    03f0 - 97 ce e4 01 9a 17 2b c1-dd 2a a4 6b af 2c 7c 8c   ......+..*
.k.,|.
    0400 - f2 f4 bd 62 ec 76 fe ac-8c 48 88 f8 5f 23 fe 5d   ...b.v...H
.._#.]
    0410 - 11 94 49 81 ad 2b 9a a0-82 29 25 fc 29 f1 38 16   ..I..+...)
%.).8.
    0420 - 90 0f e6 97 99 6f f8 f7-22 29 cf 6e 29 2c d5 e2   .....o..")
.n),..
    0430 - e9 bf c9 aa 1a 31 fa 5f-7f da 73 f5 37 35 18 ec   .....1._..
s.75..
    0440 - 9c 6e d1 b7 f8 06 5f cf-fb 09 80 10 e8 dc 62 5c   .n...._...
....b\

    Start Time: 1492437547
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

```
SHA256:DHE-DSS-AES256-SHA256:DH-RSA-AES256-SHA256:DH-DSS-AES256-SHA256:
DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DH-RSA-AES256-SHA:DH-DSS-AES256-S
HA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:DH-RSA-CAMELLIA256-S
HA:DH-DSS-CAMELLIA256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-
GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES
256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SH
A:CAMELLIA256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SH
A256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128
-SHA:ECDHE-ECDSA-AES128-SHA:DH-DSS-AES128-GCM-SHA256:DHE-DSS-AES128-GCM
-SHA256:DH-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES1
28-SHA256:DHE-DSS-AES128-SHA256:DH-RSA-AES128-SHA256:DH-DSS-AES128-SHA2
56:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DH-RSA-AES128-SHA:DH-DSS-AES12
8-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DH-RSA-SEED-SHA:DH-DSS-SEED-SHA
:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:DH-RSA-CAMELLIA128-SHA
:DH-DSS-CAMELLIA128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GC
M-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES12
8-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:
SEED-SHA:CAMELLIA128-SHA:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:ECDH-RSA
-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:ECDHE-RSA-DES-CBC3-SHA:ECDH
E-ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DH-RSA-D
ES-CBC3-SHA:DH-DSS-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:ECDH-ECDSA-DES-CB
C3-SHA:DES-CBC3-SHA:EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:DH-RSA-DES-
CBC-SHA:DH-DSS-DES-CBC-SHA:DES-CBC-SHA
Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA384:DSA
+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:ECDSA+SHA256:RSA+SHA224:DSA+
SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
Shared Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA
384:DSA+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:ECDSA+SHA256:RSA+SHA2
24:DSA+SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
Peer signing digest: SHA512
Supported Elliptic Curve Point Formats: uncompressed:ansiX962_compresse
d_prime:ansiX962_compressed_char2
Supported Elliptic Curves: P-256:P-521:brainpoolP512r1:brainpoolP384r1:
P-384:brainpoolP256r1:secp256k1:B-571:K-571:K-409:B-409:K-283:B-283
Shared Elliptic curves: P-256:P-521:brainpoolP512r1:brainpoolP384r1:P-3
84:brainpoolP256r1:secp256k1:B-571:K-571:K-409:B-409:K-283:B-283
CIPHER is ECDHE-RSA-AES256-GCM-SHA384
Secure Renegotiation IS supported
```

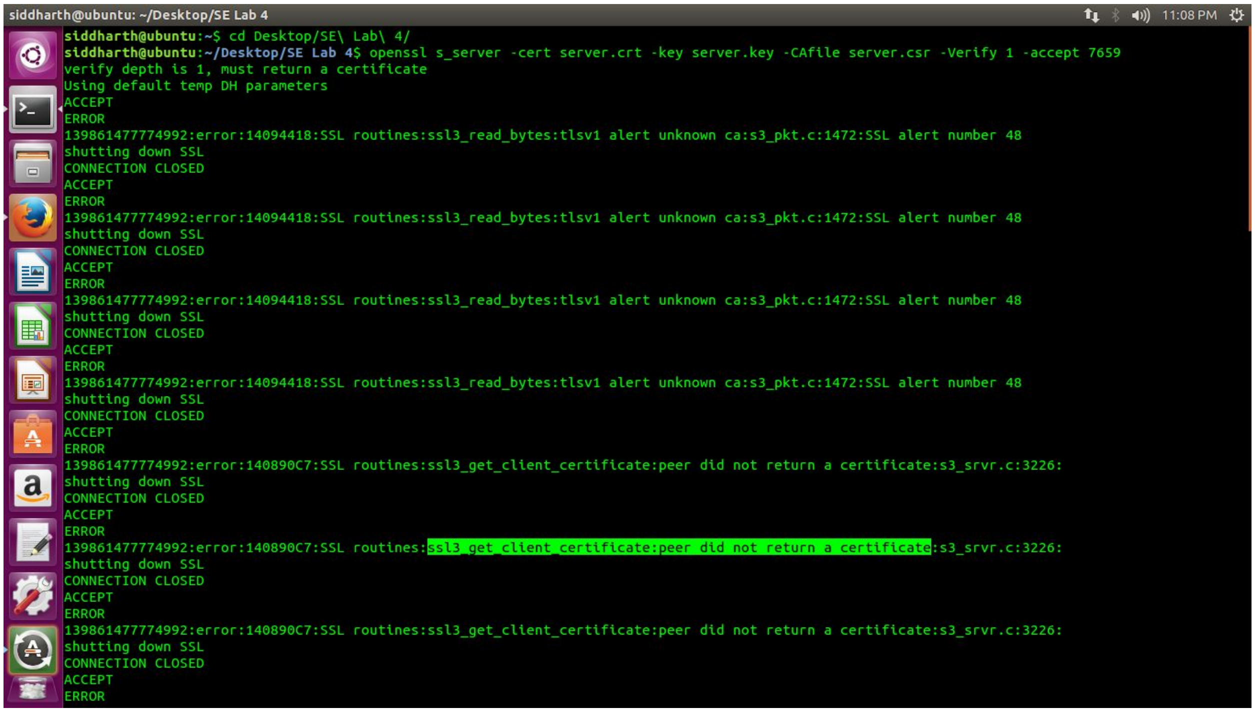
Part 4 :

- Import the Root certificate into Firefox

- Start the server with -www option to send a status message back to the client when it connects through the browser

openssl s_server -www -cert server.crt -key server.key -accept 7659

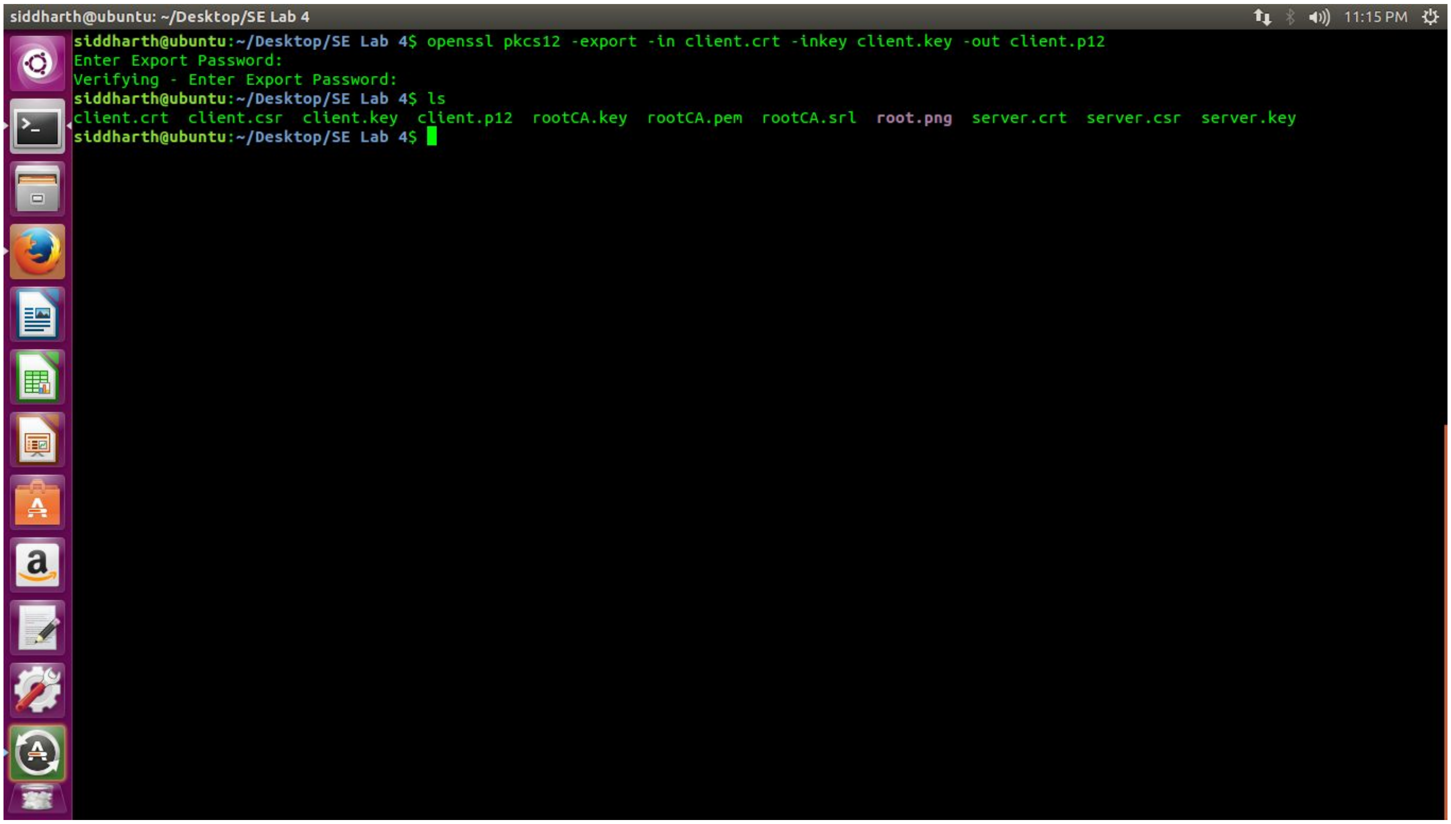
Connect to https://localhost:7659/ through the browser on which the certificate has been imported/installed.



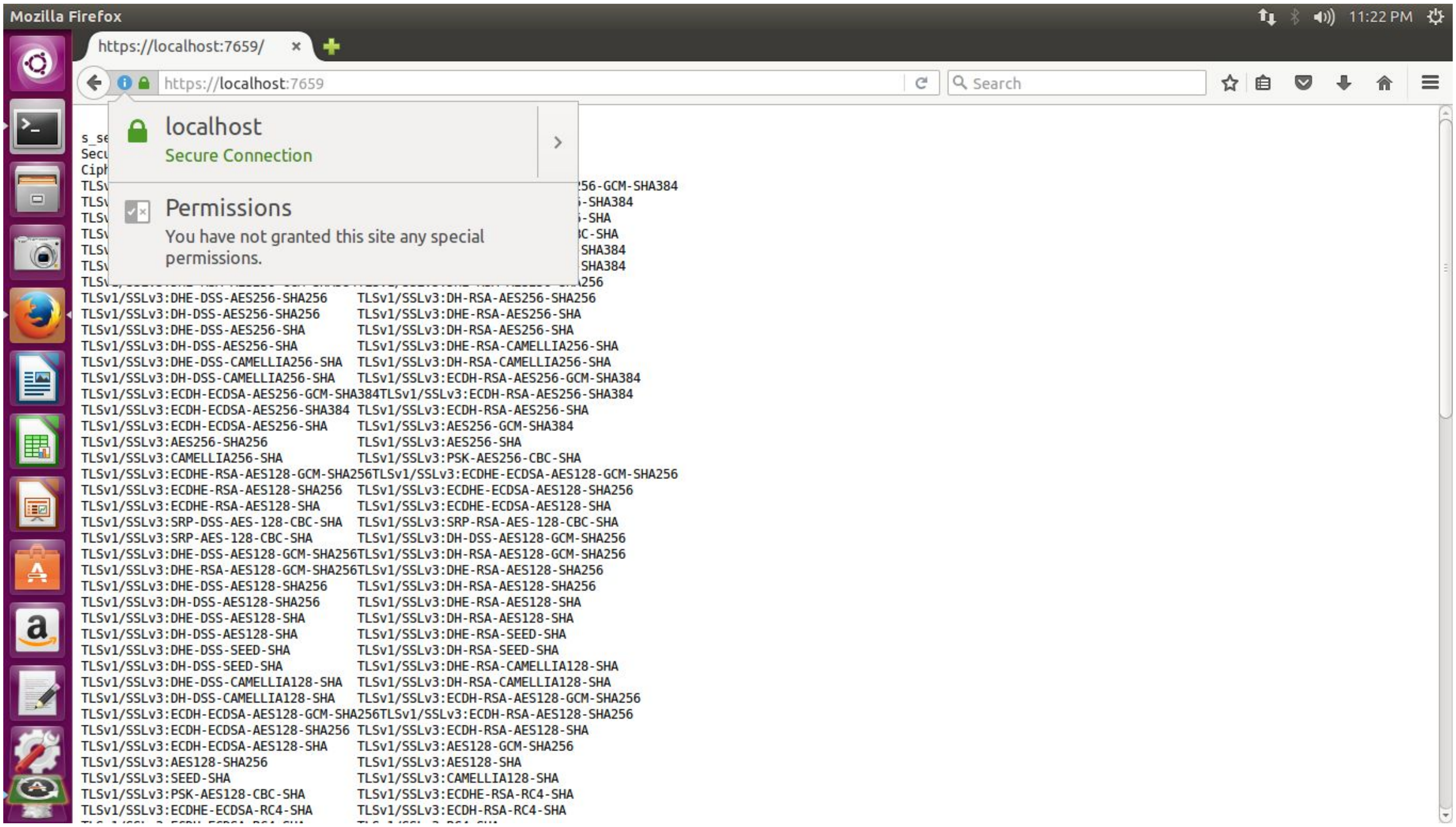
```
siddharth@ubuntu:~$ cd Desktop/SE\ Lab\ 4/
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl s_server -cert server.crt -key server.key -CAfile server.csr -Verify 1 -accept 7659
verify depth is 1, must return a certificate
Using default temp DH parameters
ACCEPT
ERROR
139861477774992:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:s3_pkt.c:1472:SSL alert number 48
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
139861477774992:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:s3_pkt.c:1472:SSL alert number 48
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
139861477774992:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:s3_pkt.c:1472:SSL alert number 48
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
139861477774992:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:s3_pkt.c:1472:SSL alert number 48
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
139861477774992:error:140890C7:SSL routines:ssl3_get_client_certificate:peer did not return a certificate:s3_srvr.c:3226:
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
139861477774992:error:140890C7:SSL routines:ssl3_get_client_certificate:peer did not return a certificate:s3_srvr.c:3226:
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
139861477774992:error:140890C7:SSL routines:ssl3_get_client_certificate:peer did not return a certificate:s3_srvr.c:3226:
shutting down SSL
CONNECTION CLOSED
ACCEPT
ERROR
```

The above screenshot displays the output when the www option isn’t used.

Combine the client certificate and the private key into a p12 format which can then be installed in the browser:



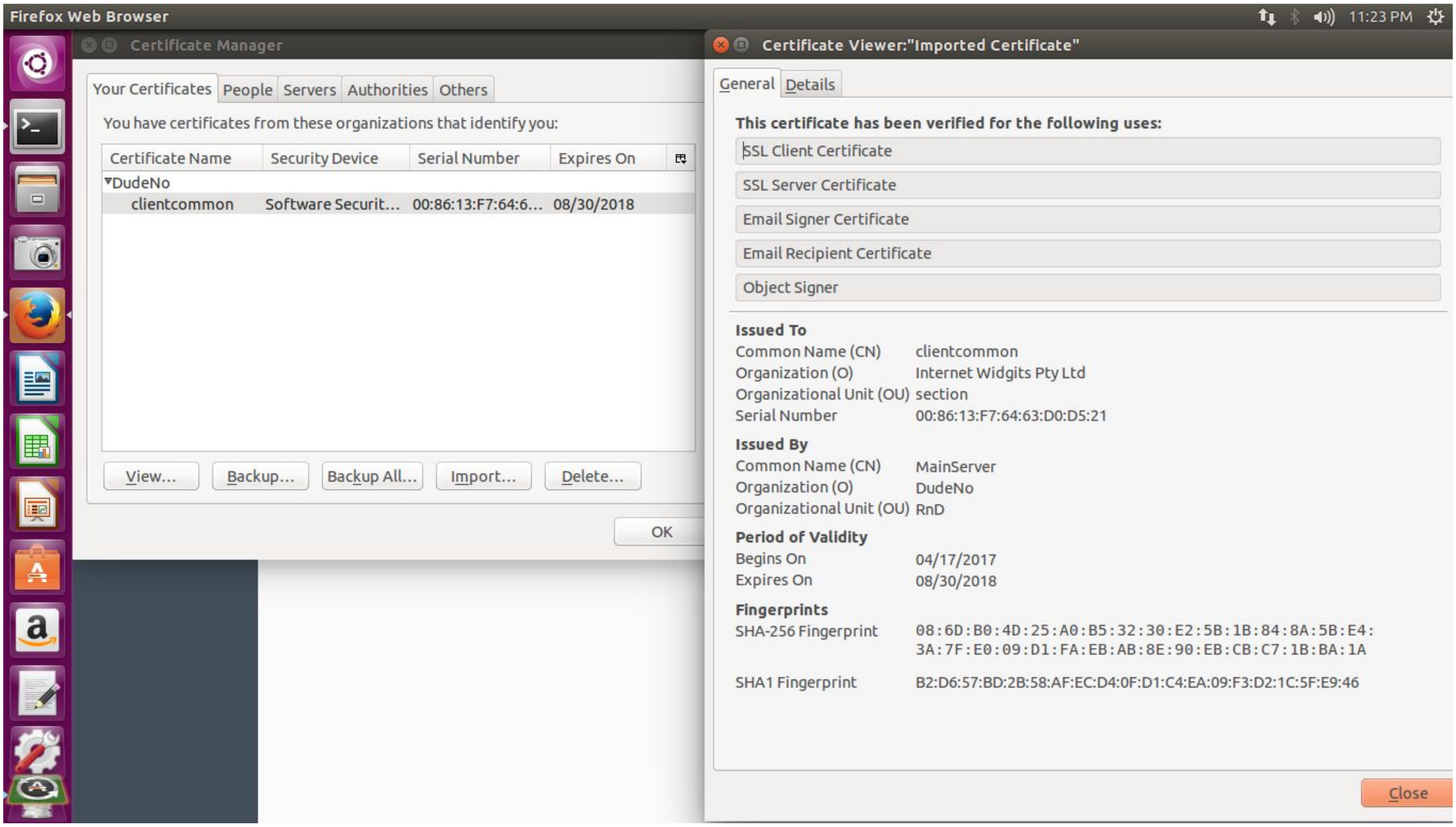
```
siddharth@ubuntu:~/Desktop/SE Lab 4$ openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12
Enter Export Password:
Verifying - Enter Export Password:
siddharth@ubuntu:~/Desktop/SE Lab 4$ ls
client.crt  client.csr  client.key  client.p12  rootCA.key  rootCA.pem  rootCA.srl  root.png  server.crt  server.csr  server.key
siddharth@ubuntu:~/Desktop/SE Lab 4$ 
```



localhost
Secure Connection

Permissions
You have not granted this site any special permissions.

```
s_se
Secu
Ciph
TLSv                                                   256-GCM-SHA384
TLSv                                                   -SHA384
TLSv                                                   -SHA
TLSv                                                   3C-SHA
TLSv                                                   SHA384
TLSv                                                   SHA384
TLSv                                                   256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256     TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256      TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA        TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA         TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA    TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA     TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256             TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA           TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256   TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA      TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA   TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA       TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256     TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256      TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA        TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA         TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA          TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA           TLSv1/SSLv3:DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA    TLSv1/SSLv3:ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA     TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256             TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                  TLSv1/SSLv3:CAMELLIA128-SHA
TLSv1/SSLv3:PSK-AES128-CBC-SHA        TLSv1/SSLv3:ECDHE-RSA-RC4-SHA
TLSv1/SSLv3:ECDHE-ECDSA-RC4-SHA       TLSv1/SSLv3:ECDH-RSA-RC4-SHA
```



You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
▾DudeNo			
clientcommon	Software Securit...	00:86:13:F7:64:6...	08/30/2018

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Email Signer Certificate

Email Recipient Certificate

Object Signer

Issued To

Common Name (CN)	clientcommon
Organization (O)	Internet Widgits Pty Ltd
Organizational Unit (OU)	section
Serial Number	00:86:13:F7:64:63:D0:D5:21

Issued By

Common Name (CN)	MainServer
Organization (O)	DudeNo
Organizational Unit (OU)	RnD

Period of Validity

Begins On	04/17/2017
Expires On	08/30/2018

Fingerprints

SHA-256 Fingerprint	08:6D:B0:4D:25:A0:B5:32:30:E2:5B:1B:84:8A:5B:E4: 3A:7F:E0:09:D1:FA:EB:AB:8E:90:EB:CB:C7:1B:BA:1A
SHA1 Fingerprint	B2:D6:57:BD:2B:58:AF:EC:D4:0F:D1:C4:EA:09:F3:D2:1C:5F:E9:46

--------------O--------------O--------------O--------------------