

Ref:

[https://wiki.openssl.org/index.php/Simple\\_TLS\\_Server](https://wiki.openssl.org/index.php/Simple_TLS_Server)

<https://www.cs.cmu.edu/~srini/15-441/F02/Projects/lab01/reference/part1.pdf>

Certificates generated from the commands given below:

Generating CA:

```
openssl req \  
-x509 \  
-nodes \  
-days 3650 \  
-newkey rsa:4096 \  
-keyout CA/ca_key.pem \  
-out CA/ca_cert.pem \  
-subj "/C=IN/ST=Delhi/L=Delhi/O=Certifying Authority/CN=root.ca.com"
```

Generating server keys:

```
openssl genrsa -out Server/server_key.pem 4096  
openssl req -new \  
-key Server/server_key.pem \  
-out Server/server.csr \  
-subj "/C=IN/ST=Delhi/L=Delhi/O=IIITD/CN=127.0.0.1:7777"
```

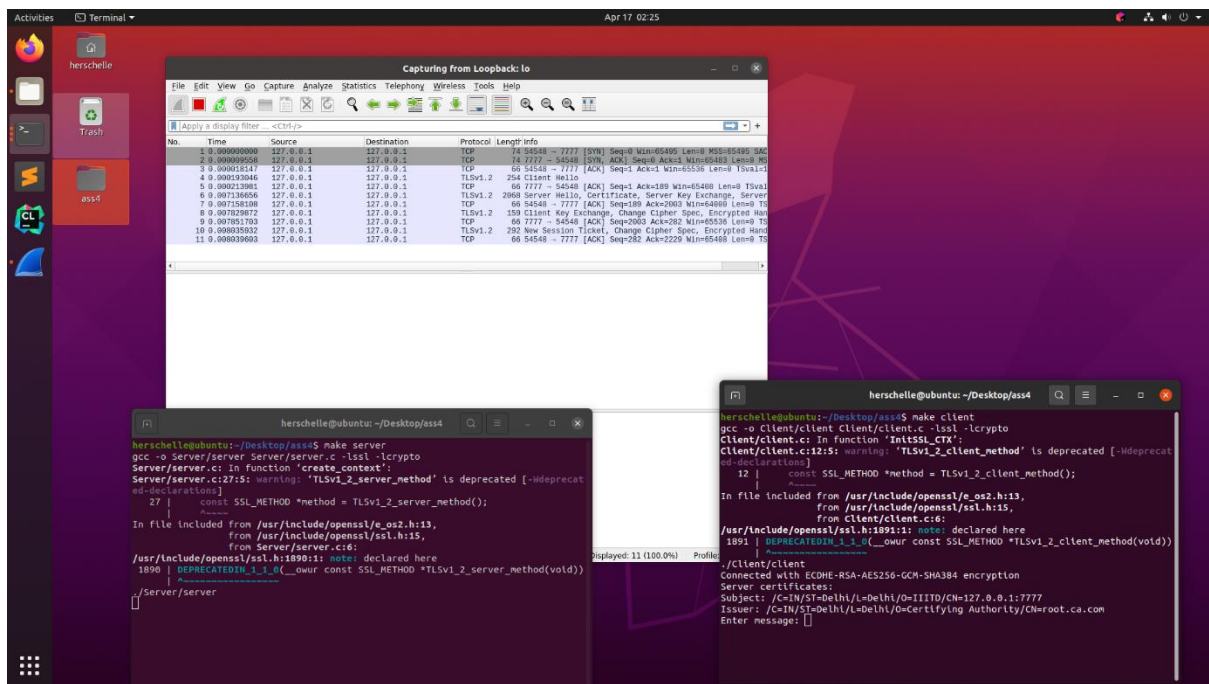
Generating and signing server's certificate with CA:

```
openssl x509 -req -days 1460 -in Server/server.csr \  
-CA CA/ca_cert.pem -CAkey CA/ca_key.pem \  
-CAcreateserial -out Server/server_cert.pem
```

Run Wireshark and start capturing packets on loopback interface.

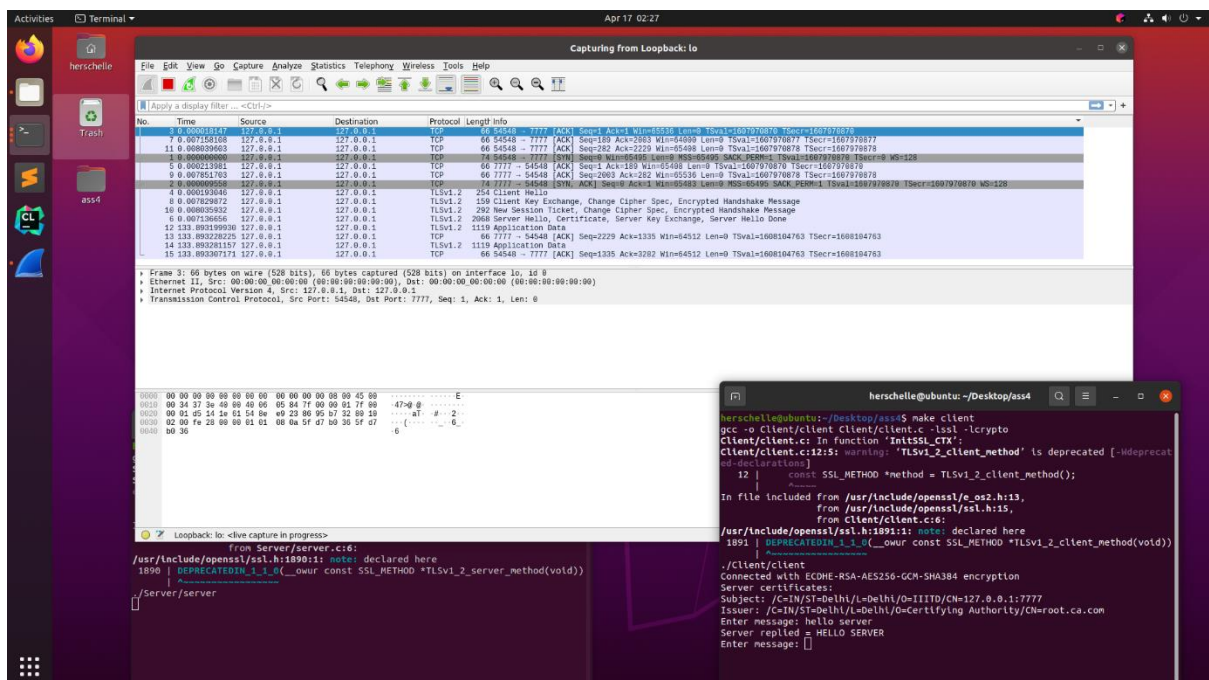
Open 2 terminals, on one type "make server" and "make client" on other.

TLS handshake and key exchange can be seen below.



Now we can enter message and server sends it back in all caps. Send “exit” to close the connection.

These captured packets .pcap file is submitted along with the code.



Finally, we can test if the code is actually verifying the certificate by commenting the shown line in the image below or giving wrong path of the CA file. We receive error code 20 which is unable to obtain certificate. We can also give some other certificate in which case we receive error code 20 which means first server certificate verification failed.

Activities Terminal Apr 17 02:30

~/Desktop/ass4/Client/client.c - Sublime Text (UNREGISTERED)

```
64 }
65 }
66
67 int main() {
68     SSL_load_error_strings();
69     SSL_CTX *ctx = InitSSL_CTX();
70     SSL *ssl = SSL_new(ctx);
71
72     const int sfd = OpenConnection("localhost", "7777");
73     SSL_set_fd(ssl, sfd);
74
75     SSL_CTX_set_verify(ctx, SSL_VERIFY_NONE, NULL);
76     // SSL_CTX_load_verify_locations(ctx, "CA/ca_cert.pem", NULL);
77
78     SSL_connect(ssl);
79
80     printf("Connected with %s encryption\n", SSL_get_cipher(ssl));
81
82     herschelle@ubuntu: ~/Desktop/ass4
83
84 herschelle@ubuntu:~/Desktop/ass4$ make server
85 gcc -o Server/server Server/server.c -lssl -lcrypto
86 Server/server.c: In function 'create_context':
87 Server/server.c:27:15: warning: 'TLSv1_2_server_method' is deprecated [-Wdeprecated-declarations]
88     const SSL_METHOD *method = TLSv1_2_server_method();
89                               ^
In file included from /usr/include/openssl/e_os2.h:13,
                  from /usr/include/openssl/ssl.h:15,
                  from Server/server.c:6:
/usr/include/openssl/ssl.h:1890:1: note: declared here
1890 | DEPRECATEDIN_1_1_0(owur const SSL_METHOD *TLSv1_2_server_method(void))
      | ^
./Server/server
herschelle@ubuntu:~/Desktop/ass4$
```

herschelle@ubuntu:~/Desktop/ass4

```
herschelle@ubuntu:~/Desktop/ass4$ make client
gcc -o Client/client Client/client.c -lssl -lcrypto
Client/client.c: In function 'InitSSL_CTX':
Client/client.c:12:5: warning: 'TLSv1_2_client_method' is deprecated [-Wdeprecated-declarations]
12 |     const SSL_METHOD *method = TLSv1_2_client_method();
    |     ^
In file included from /usr/include/openssl/e_os2.h:13,
                  from /usr/include/openssl/ssl.h:15,
                  from Client/client.c:6:
/usr/include/openssl/ssl.h:1891:1: note: declared here
1891 | DEPRECATEDIN_1_1_0(owur const SSL_METHOD *TLSv1_2_client_method(void))
      | ^
./Client/client
Connected with ECDHE-RSA-AES256-GCM-SHA384 encryption
Server certificates:
Subject: /C=IN/ST=Delhi/L=Delhi/O=IIITD/CN=127.0.0.1:7777
Issuer: /C=IN/ST=Delhi/L=Delhi/O=Certifying Authority/CN=root.ca.com
Certificate verification error, code = 20
Closing the connection.
herschelle@ubuntu:~/Desktop/ass4$
```

Activities Sublime Text Apr 17 02:38

~/Desktop/ass4/Client/client.c - Sublime Text (UNREGISTERED)

```
70 SSL *ssl = SSL_new(ctx);
71
72 const int sfd = OpenConnection("localhost", "7777");
73 SSL_set_fd(ssl, sfd);
74
75 SSL_CTX_set_verify(ctx, SSL_VERIFY_NONE, NULL);
76 SSL_CTX_load_verify_locations(ctx, "CA/ca_cert.pem", NULL);
77
78 SSL_connect(ssl);
79
80 printf("Connected with %s encryption\n", SSL_get_cipher(ssl));
81
82 DisplayCerts(ssl);
83
84 unsigned int verify = SSL_get_verify_result(ssl);
85 if (verify != X509_V_OK) {
86     printf("Certificate verification error, code = %d\n", verify);
87     printf("Closing the connection.\n");
88     SSL_write(ssl, "exit", 4);
89     return 0;
90 }
91
92 while (1) {
93     char input[1024];
94     printf("Enter message: ");
```