TASK 1: Certificates

Commands for Creating a root CA certificate (V3 X.509 certificate, self-signed using 512-bit ECC Private Key of the root)

We have generated the subject name: NTS Root R1, V3 X.509 certificate, self-signed using 512-bit ECC Private Key of the root .

Command: openssl ecparam -out ec-cakey.pem -name brainpoolP512t1 -genkey

```
mahanth@mahanth-HP-Laptop-15s-dr1xxx: ~/SecureChat/Assignment/Alice/certificates Q = —

mahanth@mahanth-HP-Laptop-15s-dr1xxx: ~/SecureChat/Assignment/Alice/certificates$ cat ec-cakey.pem
-----BEGIN EC PARAMETERS-----
BgkrJAMDAggBAQ4=
-----BND EC PARAMETERS-----
MIHAAGEBBECpoVYaSW03v360SDMWQ6FGysHLwT30GVLC70Vjn2mBcZHNGUF/mYhq
yZj5LniyuJ3rTPP76kkQKvgyrsogoh+joAsGCSskAwMCCAEBDqGBhQOBggAEPtFI
x+mYVLOe7t2cCgA2pKZ8sRngPLqVDbZJ6ouxan1Mrcahr4Rz3Rd4ungCPfV7nUFF
OUEIvNChDVEw2PFHfxrq5q3TGrbPVJ7VOeG90+KY5YKBN55t6y3GWY+J67E7Yzv/
rPjvvLy8rd19eAbotf6U3dDEnk9zPEfeC3yGdm4=
-----END EC PRIVATE KEY-----
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$
```

```
Command: openssl req -new -key ec-cakey.pem -out rootCA.csr
```

```
Command: openssl x509 -req -in rootCA.csr -signkey ec-cakey.pem -out rootCA.crt -days 3650 -sha256 -extfile Extensions_CA.ext
```

The extensions had the CA true indicating that it can sign the other certificates.

```
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$ cat Extensions_CA.ext
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints = CA:TRUE
keyUsage = critical,keyCertSign,cRLSign
mahanth@mahanth=HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$ cat Extensions ext
```

```
ent/Alice/certificates$ cat rootCA.crt
   ----BEGIN CERTIFICATE---
MIIDszCCAxegAwIBAgIUdTFWaHQ7qrKUrAf3Uj3+6iFS3qkwCgYIKoZIzj0EAwIw
gYwxCzAJBgnVBAYTAklOMQswCQYDVQQIDAJUUZEMMAoGA1UEBwwDSFlEMRQwEgYD
VQQKDAtOVFMgUm9vdCBSMTEMMAoGA1UECwwDTlRTMRQwEgYDVQQDDAtOVFMgUm9v
dCBSMTEOMCYGCSqGSIb3DQEJARYZY3MyMm10ZWNOMTEwMTVAaWl0aCShYy5pbjAe
  -w0yMzAzMjUxMjAzMjNaFw0zMzAzMjIxMjAzMjNaMIGMMQswCQYDVQQGEwJJTjEL
 MAKGA1UECAWCVFMxDDAKBgNVBAcMA0hZRDEUMBIGA1UECgwLTlRTIFJvb3QgUjEx
DDAKBgNVBAsMA05UUZEUMBIGA1UEAwwLTlRTIFJvb3QgUjExKDAmBgkqhkiG9w0B
CQEWGWNZMjJtdGVjaDExMDE1QGlpdGguYWMuaW4wgZswFAYHKoZIzj0CAQYJKyQD
AwIIAQEOA4GCAAQ+0UjH6ZhUs57u3ZwKADakpnyxGeA8upUNtknqi7FqfUytxqGv
hHPdF3i6eAI99XudQUU5QQi80KENUTDY8Ud/GurmrdMats9UntU54b3T4pjlgoE3
 nm3rLcZZj4nrsTtj0/+s+0+8vLyt3X14Bui1/pTd0MSeT3M8R94LfIZ2bq0CARAw
hm3rtcz2j4nr3rtj0/+5+0+8VLyt3x148btt1p10dm3e13m8k94Lr1z2bqUcAkkaw
ggeMM1HMBgNVHSMEgcQwgcGAEGLxGw+2zrlHqbJVxDtK9r0XDh41oYGSpIGPMIGM
MQswCQYDVQQGEwJJTjELMAkGA1UECAwcVFMxDDAKBgNVBAcMA0hZRDEUMBIGA1UE
CgwLTlRTIFJvb3QgUjExDDAKBgNVBASMA05UUZEUMBIGA1UEAwwLTlRTIFJvb3Qg
UjExKDAmBgkqhkiG9w0BCQEWGWNZMjJtdGVjaDExMDE1QGlpdGguYWMuaW6CFHUX
 Vmh006qylKwH91I9/uohUt6pMAwGA1UdEwQFMAMBAf8wDgYDVR0PAQH/BAQDAgEG
MB0GA1UdDgQWBBRi8RsPts65R6myVcQ7Svazlw4eCDAKBggqhkj0PQQDAgDBiQAw
gYUCQQCjNNHvpZu3jjJWxE2pcb8PfrYSYVMYAQlJWy1Lr9D/3hpPFYh01CkH7yfn
 RwcVtLIBOM+/j047nVySwe63R6ZYAkB+RMhkVkne3RgqyUm6v05mCXupoDJZUu/K
eoYJw0ULSBgS5h7QAQLZTwULH8LYG88q2lm4UxYh4gCBrVU5hjzS
   ---END CERTIFICATE---
     anth@mahanth-HP-Laptop-15s-dr1xxx:~
```

Commands to generate the intermediate certificate signed by rootCA

```
Command: openssl req -newkey rsa:2048 -nodes -keyout intermediate_key.pem -days 365 -out inter.csr
```

```
Command: openssl x509 -req -CA rootCA.crt -days 365 -in inter.csr -CAkey ec-cakey.pem -CAcreateserial -out inter.crt -extfile Extensions_CA.ext
```

```
- END CERTIFICATE.
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$ cat inter.crt
 ----BEGIN CERTIFICATE----
MIIENDCCA5igAwIBAgIUCELwgnWa1cYJLHXBkV66SNk4d6AwCgYIKoZIzj0EAwIw
gYwxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJUUzEMMAoGA1UEBwwDSFlEMRQwEgYD
VQQKDAtOVFMgUm9vdCBSMTEMMAoGA1UECwwDTlRTMRQwEgYDVQQDDAtoVFMgUm9v
dCBSMTEoMCYGCSqGSIb3DQEJARYZY3MyMm10ZWNoMTEwMTVAaWl0aC5hYy5pbjAe
Fw0yMzAzMjUxMjI3MjhaFw0yNDAzMjQxMjI3MjhaMIGFMQswCQYDVQQGEwJJTjEL
MAKGA1UECAWCVFMxDDAKBgNVBAcMA0hZRDEMMAoGA1UECgwDTlRTMQ4wDAYDVQQL
DAVJTlRFUjETMBEGA1UEAwwKTlRTIENBIDFSMzEoMCYGCSqGSIb3DQEJARYZY3My
Mm10ZWNoMTEwMTVAaWl0aC5hYy5pbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAPdvCG0HCEo4y2JvwWeb5pKQiXxWuyFmfjI/8rw+02f9qikb/hY2X6l0
RxgIh93bSIfbHeTySgHnzXUlyHRtB0ULub/iRZWf1bi6By2ZyUMF+WMWWPWWU3ym
cC+tNrjD9JWwoxB9WzYJ7mcUjPFHCtF60800BIV+6j8zQr8dbDBulmDLLb0DrHyU
abCNXTq6Ur7SzwJesNICHJ0oSrSp3oU/h9l0+TDagXCEQ9V6ROS7Umlm/FdjW036
9HVkXZ44RcOHJQvoRsEaAdkH1fXjTBLjI2ulxlN3QQIaQy1VM3vVV8Lm3+G7NP68
vxsldFyUMWB2+RUqws4RQu3XVvLlBrMCAwEAAaOCARAwggEMMIHMBgNVHSMEgcQw
gcGAFGĹxGw+2zrlHqbJVxDtK9rOXDh4IoYGSpIGPMIGMMQswCQYDVQQGEwJJTjEL
MAKGA1UECAwCVFMxDDAKBgNVBAcMA0hZRDEUMBIGA1UECgwLTlRTIFJvb3QgUjEx
DDAKBgNVBAsMA05UUzEUMBIGA1UEAwwLTlRTIFJvb3QgUjExKDAmBgkqhkiG9w0B
CQEWGWNzMjJtdGVjaDExMDE1QGlpdGguYWMuaW6CFHUxVmh006qylKwH91I9/uoh
Ut6pMAwGA1UdEwQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBQuB8Qn
tQE98LndGZ8vm0hF6ialYzTAKBggqhkjOPQQDAgOBiQAwgYUCQQCdxgP17IBtAQ5k
aY7DeiGCbLFuON7ekgsS++Q8xXsXe830xuRR73t1UMTZ65InlsqH1RSQr3FaklGl
nKYkb6oQAkAv31ruT/n1RQ0fW+K0n22yIIhHB+6EOCStteUKdPrmMr8ABJmN7ckM
lLCFRVyj9Bf7Dk54abDeyzV0I2jwyijZ
    --END CERTIFICATE--
 mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/Secur
```

Commands to generate Alice certificates

We have changed the key size to 2048 bits since there was an error with a 1024 bits key saying that it is small.

Command: openssl req -newkey rsa:2048 -nodes -keyout alice.key -days 365 -out alice.csr -subj="/C=US/O=NTS/OU=CA/CN=Alice1.com"

Command: openssl x509 -req -CA inter_2.crt -days 365 -in alice.csr -CAkey intermediate_key.pem -CAcreateserial -out alice_2.crt -extfile Extensions.ext

mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates\$ cat Extensions.ext
authorityKeyIdentifier = keyid,issuer
basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation,keyEncipherment,dataEncipherment
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates\$

```
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$ cat alice.crt
 ----BEGIN CERTIFICATE----
MIIDqzCCApOgAwIBAgIUaHSTS0a6X8gKaXFB+WQvLvcq4GswDQYJKoZIhvcNAQEL
BQAwgYUxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJUUzEMMAoGA1UEBwwDSFlEMQww
CgYDVQQKDANOVFMxDjAMBgNVBAsMBUlOVEVSMRMwEQYDVQQDDApOVFMgQ0EgMVIz
MSgwJgYJKoZIhvcNAQkBFhljczIybXRlY2gxMTAxNUBpaXRoLmFjLmluMB4XDTIz
MDMyNTEyMjg1M1oXDTI0MDMyNDEyMjg1M1owPTELMAkGA1UEBhMCVVMxDDAKBgNV
BAOMA05UUzELMAkGA1UECwwCQ0ExEzARBqNVBAMMCkFsaWNlMS5jb20wqqEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCX5lPHCrSs7cUAGKCT+zgJz4ZTIKVn
ildqh/nQJFyywJi0EdR+w+Z87WB4RaEVi7xF6IRVeRtCvXVuDErqYN7Y0W0DlMkZ
4otffDUHbtzZKQdSm/sLpX9op0DmOknOpOIbrtqpULUAewUPxlQK7JA7ZVrJMacs
Akxs+esG0/gvJcPeFAHHDmKmd2t+KJHiK5XzxueXsoduxG1RT+vqLbQUiQ+6USls
4XHg+NTTOrlEylyd054oQSl2mv4npHiV0TtYKeR9aLVig4E7UDfLBuBvGMfZW+5B
vvo3R4SE0l5GsztSqdwXeihGDnah0x1QtKth5ciHUw/mX0bRsJQh7MuDAgMBAAGj
WjBYMB8GA1UdIwQYMBaAFC4HxCdAT3wud0Zny+bSEXqJqVjNMAkGA1UdEwQCMAAw
CwYDVR0PBAQDAgTwMB0GA1UdDgQWBBTaFdPX9rGbQfzU79j17pAwlbKldDANBgkq
hkiG9w0BAQsFAAOCAQEAreG9bPiF9T8PsQ/TfipePocXdoV/f940T9jwJNXlYd5g
ojD/Yx4Fc4ulZYFRvOKgI270dCw82I51i9MCXIgrPizNPhKIDwtC2Z4+QZ9Yrphr
vg0PoB1jV+o2DHRdvkMdmUxRY6q+iUienLOI1V0wfOv+D6KeiBbeXi89HjOK8ZZ1
EHLp26DAQymsg0rC1uXIaYQVx+/Qr2UI1Mjw6Bq/bJIccmV6pxTo3VegkY5YuG8x
IVBTFwDm15Lj5lt80G0BIFzjo6L03TKiyrlwL5nHFgemYg5iI2mZKlI6jZiU5Y3o
3nE3iV5KPQAxuui845nfBAggwWEpfJxvB0wBzYb71g==
 ----END CERTIFICATE----
 mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$
```

Commands to generate bob certificate

Command: openssl ecparam -genkey -name prime256v1 -out bob.key

Command: openss1 req -new -key bob.key -out Bob.csr -subj="/C=US/O=NTS/OU=CA/CN=Bob1.com"

Command: openss1 x509 -req -CA inter_2.crt -days 365 -in Bob.csr -CAkey

intermediate key.pem -CAcreateserial -out bob.crt -extfile Extensions.ext

```
nahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates$ cat bob.crt
----BEGIN CERTIFICATE---
MIIC3jCCAcagAwIBAgIUJ08njewbyie+ut0pvT0TyLmu6LUwDQYJKoZIhvcNAQEL
BQAwgYUxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJUUzEMMAoGA1UEBwwDSFlEMQww
CgYDVQQKDANOVFMxDjAMBgNVBAsMBUlOVEVSMRMwEQYDVQQDDApOVFMgQ0EgMVIz
MSgwJgYJKoZIhvcNAQkBFhljczIybXRlY2gxMTAxNUBpaXRoLmFjLmluMB4XDTIz
MDMyNTEyMjk0M1oXDTI0MDMyNDEyMjk0M1owOzELMAkGA1UEBhMCVVMxDDAKBgNV
BAOMA05UUZELMAkGA1UECwwCQ0ExETAPBgNVBAMMCEJvYjEuY29tMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAEV5mgRZ//TwlIRcyKR9b5XdqaCi7UQ42kNTi2hSKU
jNJRzSGCEQWP5KWWzVOLhaTvMS3XdnyAa/KxPUCNP+qY5aNaMFgwHwYDVR0jBBgw
FoAULgfEJ0BPfC53RmfL5tIReompWM0wCQYDVR0TBAIwADALBgNVHQ8EBAMCBPAw
HQYDVR0OBBYEFKY0hdtDN2jdgjBA5HbD8zvMtOPxMA0GCSqGSIb3DQEBCwUAA4IB
AQAfi/Qq4u0k8LAuiUa3V6Gyae4UuvEJ330hYb0cMjg9gQ9W3skz3zutWuw72e5u
1pLeeY/hRGVQaus6cPdiSzlFY5PcrWU/f4pZleDo7/GrPrltFPzsIi+qNqdP1kk4
NrCBdEEjodSRSBfxeay5zUkrH3CrvDIg0bqci/s9NNJ8CNNMWld2qdZ7Em8OWUoM
oIY8XGv5acDQ0NP7LYk/LJHU9BIJcKQM+Q5MKpTxzCagZT1Vlw09VP6bX96/KjDO
S8NuAhlsQ83Z/MFwL8uEiCqY7QD0f/+nFa/Mt3dntqIU0iVS5DRAp/RYmxta67tL
8p4tkV3Q0WXUZobAoUu9vHBa
 ----END CERTIFICATE----
 mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/Secure
```

VERIFICATION OF ALL THE CERTIFICATES:

Using a shell script we have combined both the intermediate and root certificates into pem file which we named it as CAfile.pem. Which is used later for verification purposes.

Shell script to combine the certificates

```
for i in inter_2.crt rootCA_2.crt; do
   openssl x509 -in $i -text >> CAfile.pem
done
```

mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates\$ openssl verify -verbose -CAfile rootCA.crt inter.crt
inter.crt: OK
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/certificates\$

mahanth@mahanth-HP-Laptop-15s-drixxx:~/SecureChat/Assignment/Alice/new_certs\$ openssl verify -verbose -CAfile CAfile.pem alice_2.crt
alice_2.crt: OK
mahanth@mahanth-HP-Laptop-15s-drixxx:~/SecureChat/Assignment/Alice/new_certs\$

mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/new_certs\$ openssl verify -verbose -CAfile CAfile.pem bob_2.crt
bob_2.crt: OK
mahanth@mahanth-HP-Laptop-15s-dr1xxx:~/SecureChat/Assignment/Alice/new_certs\$

TASK 2: Secure Chat

sec_server_client.cpp:

Server starts the app using command:

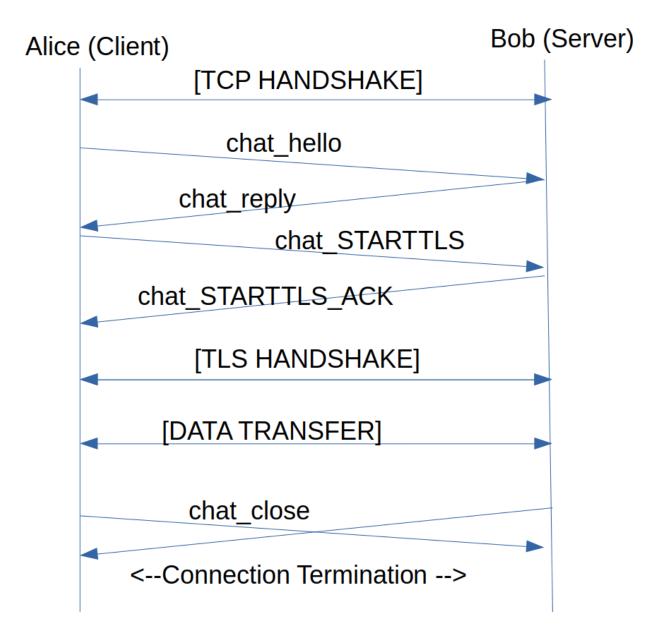
```
sec_server_client.cpp -s
```

Client starts the app using command:

```
sec_server_client.cpp -c bob1
```

This c++ program consists of 2 functions : runServer() and runClient(<server hostname>), which can be triggered by command line arguments -s and -c b server and client respectively.

The Communication Flow chart for this Task 2 has been shown below:



Functions:

1. runServer():

- The socket is initially generated on the server side, attached to its port, and listens to see if any clients are connecting after the client and server certificates have been loaded.
- The chat reply is sent to the client whenever a client connects to the port and the server receives the chat hello.
- The communication will continue in an unsecured way unless the Server receives a chat STARTTLS message from the Client and responds with chat STARTTLS ACK to indicate that it supports Secure Communication.
- As long as neither the Client nor the Server sends the other party a chat close

message, the Client and Server continue exchanging messages. If the Server receives a bye from the terminal, it sends the chat close message to the Client.

With the chat close command, the client and server connection is broken.

2. runClient(<server hostname>):

- We determine the server IP address using gethostbyname(), and after that, we call connect() to establish a connection between the Client and the Server.
- The Client sends a chat hello to the Server upon a successful connection, and the Client then waits for the Server to respond.
- As a reply to chat hello, the Server sends the chat reply message to the Client.
- To begin Secured Communication with the Server, the Client sends chat STARTTLS and waits for a response from the Server.
- If the Server is TLS-capable, it will get a chat STARTTLS ACK, which will trigger the exchange of encrypted data.
- The data will be transmitted with encryption unless it receives the message chat STARTTLS NOT SUPPORTED, which triggers an unencrypted transmission.
- Unless one of the two parties gives the other a chat close message, Client and Server remain exchanging messages.

Alice1 and Bob1 Container Call Flow Terminal:

```
Æ
                                                                                                                                              BOB
oot@alice1:~/programs# ./sc -c bob1
-cchat reply received...
Let's Start TLS Connection ->
                                                                                           Accepted a new connection from 172.31.0.2:49502 chat_hello_received
chat STARTTLS Sent ---->
                                                                                           chat_reply_sent
Security_check
chat_STARTTLS received from Client ---->chat_STARTTLS_ACK
chat_STARTTLS_ACK Sent from Server --->
Security_check
chat_STARTTLS_ACK received from Server ---->
SSL connection established. Server Certificate:
                                                                                             ommunication through secured (TCP+TLS) connection
0x55b5a32fd130
·> Hie,Bob
Msg Received from Server: Hello,Alice!!!!-> chat_close Connection closed by the server.
root@alice1:~/programs#
                                                                                            0x560be1b983f0
                                                                                            Asg Received from Client: Hie,Bob
                                                                                            Send message to client-> Hello,Alice!!!!
Msg Received from Client: chat_close
                                                                                            Closing connection.

Connection closed by the client.
                                                                                             oot@bob1:~/programs#
```

PCAP Evidences:

Taking pcap traces on Alice1 container:

```
CONTAINER HOST
ubuntu@ns00-gold:~$ lxc exec alice1 -- sudo tcpdump -i eth0 -nn not tcp port 22 -w task1_alice.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C33 packets captured
33 packets received by filter
0 packets dropped by_kernel
```

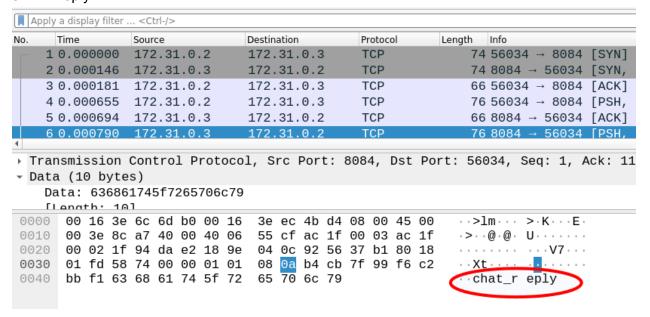
TCP Handshake:

	Time	Source	Destination	Protocol	Length	Info		
1	1 0.000000	172.31.0.2	172.31.0.3	TCP	74	56034 → 8084	[SYN]	Seq=0
2	2 0.000146	172.31.0.3	172.31.0.2	TCP	74	$8084 \rightarrow 56034$	[SYN,	ACK] S
3	3 0.000181	172.31.0.2	172.31.0.3	TCP	66	56034 → 8084	[ACK]	Seq=1

CHAT Hello:

(11.7		,			-																				
No.	1	Time			Sour	ce				Destin	ation			Pr	otoco	ol	l	ength	In	fo						
	1 (0.00	0000	00	172	2.31	L.O.	2		172.	31.	0.3	3	Т	CP			74	4 5	603	4 -	808	84	[SYN]	Seq=	:0 V
	2 (0.00	0014	16	172	2.31	L.O.	3		172.	31.	0.2	2	Т	CP			74	4 8	084	\rightarrow	560	34	[SYN,	ACK]	Se
П	3 (0.00	0018	31	172	2.31	L.O.	2		172.	31.	0.3	3	Т	СР			6	6 5	603	4 -	808	84	[ACK]	Seq=	1 A
	4 (0.00	065	55	172	2.31	L.O.	. 2		172.	31.	0.3	3	Т	СР			7	₃ 5	603	4 –	808	84	[PSH,	ACK]	Se
	5 (0.00	0069	94	172	2.31	L.O.	. 3		172.	31.	0.2	2	Т	CP			6	6 6	084	\rightarrow	560	34	[ACK]	Seq=	:1 A
	6 (0.00	0079	90	172	2.31	L.O.	3		172.	31.	0.2	2	Т	CP			7	6 6	084	\rightarrow	560	34	[PSH,	ACK]	Se
4																										
 	Fram	e 4	: 76	6 by	yte:	s o	n w	ire	(60	98 b.	its),	76	byt	es (cap	ture	d (60	8	bit	s)					
> I	Ethe	rne	t I	Ι, :	Src	: X	ens	our	c_6	::6d	:b0	(0	0:1	6:3	e:6	c:6	d:b0), Ds	t:	Xe	nso	urc_	_ec	:4b:d	4 (00	:16
)	Inte	rne	t Pi	rot	осо.	1 V	ers.	ion	4,	Src	: 1	72.	31.	0.2	, D:	st:	172	.31.0	.3							
٠.	Tran	emi	eei	an (^nn	tro	1 D	rot	റവ	<u> </u>	rc	Dor	+ •	560	2/	De	t Do	rt· 8	คล	1	San	. 1	^	ck· 1	Lon	. 1
00	000	00	16	Зе	ec	4b	d4	00	16	3e	6c	6d	b0	08	00	45	00	>	٠K		>1	m · · ·	٠E٠			
00	910	00	Зе	5b	74	40	00	40	06	87	02	ac	1f	00	02	ac	1f	·>[t@	· @ ·						
00	920	00	03	da	e2	1f	94	92	56	37	a7	18	9e	04	0c	80	18			··V	7 ·					
00	930	01	f6	58	74	00	00	01	01	98	0a	f6	c2	bb	f1	b4	cb	X	t.							
00	940	7f	98	63	68	61	74	5f	68	65	6c	6c	6f					(·c	ha	t_h	el	lo	>			

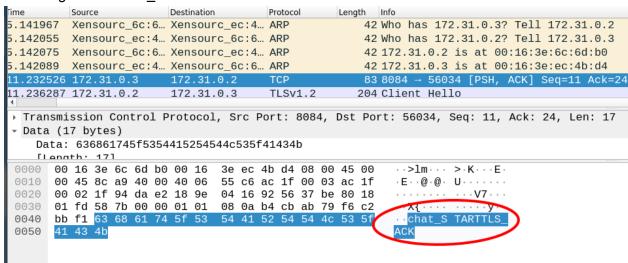
CHAT Reply:



chat_STARTTLS:

```
Source
                            Destination
                                                          Length
                                                                 Info
lime.
                                              Protocol
           172.31.0.2
                            172.31.0.3
                                              TCP
                                                               76 56034 → 8084 [PSH, ACK] S
0.000655
0.000694
           172.31.0.3
                            172.31.0.2
                                              TCP
                                                              66 8084 → 56034 [ACK] Seq=1 A
                                                              76 8084 → 56034 [PSH, ACK] S
0.000790 172.31.0.3
                                              TCP
                            172.31.0.2
0.000852 172.31.0.2
                                              TCP
                                                              66 56034 → 8084 [ACK] Seq=11
                            172.31.0.3
0.000946 172.31.0.2
                            172.31.0.3
                                                               79 56034 → 8084 [PSH, ACK] S
                                              TCP
0.042034 172.31.0.3
                            172.31.0.2
                                              TCP
                                                              66 8084 → 56034 [ACK] Seq=11
Transmission Control Protocol, Src Port: 56034, Dst Port: 8084, Seq: 11, Ack: 1
Data (13 bytes)
    Data: 636861745f5354415254544c53
     [Lanath: 12]
 0000 00 16 3e ec 4b d4 00 16
                                     3e 6c 6d b0 08 00 45 00
                                                                    \cdot \cdot > \cdot \mathsf{K} \cdot \cdot \cdot \cdot > \mathsf{lm} \cdot \cdot \cdot \cdot \mathsf{E} \cdot
                                                                    ·A[v@·@· · · · · · · ·
 0010 00 41 5b 76 40 00 40 06
                                     86 fd ac 1f 00 02 ac 1f
 0020 00 03 da e2 1f 94 92 56
                                     37 b1 18 9e 04 16 80 18
                                                                    . . . . . . . V 7 . . . . . .
                                     08 0a f6 c2 bb f1 b4 cb
 0030 01 f6 58 77 00 00 01 01
                                                                     · Xw
 0040 7f 99 63 68 61 74 5f 53
                                     54 41 52 54 54 4c 53
                                                                      chat
```

Receiving Ack on chat_STARTTLS



TLS Handshake and Data Transfer:

Į.	tis				
No	. Time	Source	Destination	Protocol	Length Info
	15 11.236287	172.31.0.2	172.31.0.3	TLSv1.2	204 Client Hello
	17 11.240285	172.31.0.3	172.31.0.2	TLSv1.2	3112 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
	19 11.245797	172.31.0.2	172.31.0.3	TLSv1.2	3423 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
	21 11.248868	172.31.0.3	172.31.0.2	TLSv1.2	1236 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
	23 20.152034	172.31.0.2	172.31.0.3	TLSv1.2	103 Application Data
	25 28.056029	172.31.0.3	172.31.0.2	TLSv1.2	110 Application Data
	27 34.648240	172.31.0.2	172.31.0.3	TLSv1.2	105 Application Data
	29 34.648570	172.31.0.3	172.31.0.2	TLSv1.2	97 Encrypted Alert
	31 34.648744	172.31.0.2	172.31.0.3	TLSv1.2	97 Encrypted Alert

Taking pcap traces on Bob1 container:

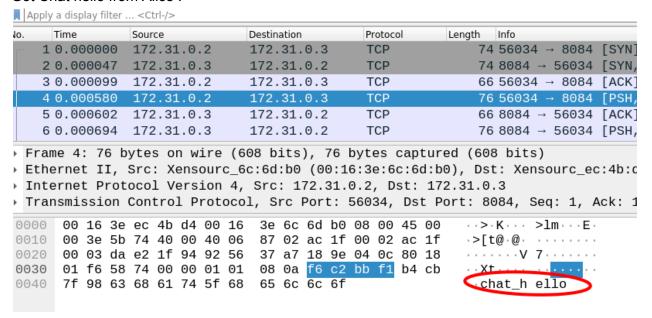
```
CONTAINER HOST

ubuntu@ns00-gold:~$ lxc exec bob1 -- sudo tcpdump -i eth0 -nn not tcp port 22 -w task1_bob.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C33 packets captured
33 packets received by filter
0 packets dropped by_kernel
```

TCP Handshake:

	Time	Source	Destination	Protocol	Length Info
1	0.000000	172.31.0.2	172.31.0.3	TCP	74 56034 → 8084 [SYN] Seq=0 Win=6
2	0.000047	172.31.0.3	172.31.0.2	TCP	74 8084 → 56034 [SYN, ACK] Seq=0
3	0.000099	172.31.0.2	172.31.0.3	TCP	66 56034 → 8084 [ACK] Seq=1 Ack=1

Got Chat hello from Alice:



Sending chat reply to alice:

	_			•																			
	Time			Sour	ce				Destin	ation			Pr	otoco	ol		Length	h	Info				
1	0.00	9000	90	172	2.31	L.O.	2	1	172.	31.	0.3	3	Т	CP				74	560	34 -	→ 80	84	[SY
2	0.00	9004	17	172	2.31	L.O.	3	:	172.	31.	0.2	2	Т	CP				74	808	4 →	560	34	[SY
3	0.00	9009	99	172	2.31	L.O.	2	:	172.	31.	0.3	3	Т	CP				66	560	34 -	→ 80	84	[AC
4	0.00	9058	30	172	2.31	L.O.	2	:	172.	31.	0.3	3	Т	CP				76	560	34 -	→ 80	84	[PS
5	0.00	9066	92	172	2.31	L.O.	3	:	172.	31.	0.2	2	Т	CP				66	808	4 →	560	34	[AC
6	0.00	0069	94	172	2.31	L.O.	3		172.	31.	0.2	2	Т	СР				76	808	4 →	560	34	[PS
the inte	ne 6 erne erne nsmi:	t I t P ssi	I, s	Src oco. Con	: Xo l Vo tro	ens ers 1 P	ouro ion roto	4, ocol	:4b Src ., S	:d4 : 1 rc	(0 72. Por	0:1 31. t:	6:3 0.3 808	e:e , D: 4, I	c:4l st: Dst	172 Por), l .31 t: !	Dst .0. 560	: Xe 2 34,	Sec	q: 1	, Δ	
00		16											08					_			K٠٠	_	
10		3e		a7	40				55		ac	1†	00	03	ac	1†	. >	> (დ. დ.	U.			
20	00	02	1f	94	da	e2	18	9e					37								· V7		
20 30		02 fd											37 7f					Χt			·V7 ···	٠.	

Got a TLS request from Alice:

No.	. 1	Time			Sour	ce				Destin	ation			Pr	otoco	ol		Lengt	h	Info				
	3 (0.00	9009	9	172	2.31	L.O.	. 2		172.	31.	0.3	3	Т	CP				66	5603	34 -	→ 808	34	[ACK
	4 (9.00	9058	30	172	2.31	L.O.	. 2		172.	31.	0.3	3	Т	CP				76	5603	34 -	→ 808	34	[PSF
	5 (0.00	9060	92	172	2.31	L.O.	. 3		172.	31.	0.2	2	Т	CP				66	8084	→	5603	34	[ACK
	6 (9.00	9069	94	172	2.31	L.O.	. 3		172.	31.	0.2	2	Т	CP				76	8084	→	5603	34	[PSF
	7 (0.00	9077	74	172	2.31	L.O.	. 2		172.	31.	0.3	3	Т	CP				66	5603	34 -	→ 808	34	[ACK
	8 (0.00	0086	64	172	2.31	L. 0	. 2		172.	31.	0.3	}	T	СР				79	5603	34 -	→ 808	34	[PSH
>	Fram	e 8	: 79	9 b	yte	s o	n w	ire	(6	32 b.	its),	79	byt	es	сар	ture	d (632	bit	s)			
•	Ethe	rne	t I	Ι,	Src	: X	ens	our	c_6	c:6d	:b0	(0	0:1	6:3	e:6	c:6	d:b0),	Dst	: Xe	nso	ourc_	ec	:4b:
•	Inte	rne	t P	rot	осо	1 V	ers	ion	4,	Src	: 1	72.	31.	0.2	, D	st:	172	.31	.0.	3				
•	Tran	smi	ssi	on (Con	tro.	1 P	rot	осо.	l, S	rc	Por	t:	560	34,	Ds	t Po	rt:	80	84,	Sed	ı: 11	.,	Ack:
0	000	00	16	Зе	ес	4b	d4	00	16	3e	6c	6d	b0	08	00	45	00		. > .	K···	>]	.m · · ·	E٠	
0	010	00	41	5b	76	40	00	40	06	86	fd	ac	1f	00	02	ac	1f		4[v	@·@·				
0	020	00	03	da	e2	1f	94	92	56	37	b1	18	9e	04	16	80	18			$\cdot \cdot \cdot V$	7 -			
0	030	01	f6	58	77	00	00	01	01	98	0a	f6	c2	bb	f1	b4	cb		· Xw					
0	040	7f	99	63	68	61	74	5f	53	54	41	52	54	54	4c	53			ch	at_s	T₽	RTTL	S	\supset

Sending ACK to the TLS:

No).	Ti	ime			Sour	ce				Destin	ation			Pr	otoco	ol		Leng	gth	Info				
	1	LO 5	5.14	1183	5	Xer	ารอน	ırc_	ec:	4	Xens	our	c_6	c:6	A	RP				42	Who	has	1	72.3	31.0.
	1	L1 5	5.14	1197	2	Xer	ารอน	ırc_	6c:	6	Xens	our	с_е	c:4	А	RP				42	Who	has	1	72.3	31.0.
	1	L2 5	5.14	1199	7	Xer	ารอน	ırc_	ec:	4	Xens	our	c_6	c:6	A	RP				42	172	. 31	0.3	3 is	s at
	1	L3 5	5.14	1200	1	Xer	ารอน	ırc_	6c:	6	Xens	our	с_е	c:4	А	RP				42	172	. 31	0.2	2 i	s at
П	1	L4 1	11.2	2324	17	172	2.31	.0.	3		172.	31.	0.2		Т	СР				83	808	4 →	560	934	[PSH
	1	L5 1	11.2	2362	14	172	2.31	.0.	2		172.	31.	0.3	}	Т	LSv	1.2			204	Cli	ent	He.	llo	
Þ	Fr	ame	e 14	4: 8	33 I	byte	es (on v	wire	(6	664 l	bit	s),	83	by	tes	ca	ptu	red	(66	4 b:	its))		
		ha	rnot	+ т		2150		once	21150		3 1 4 h	· d4	(0)	a · 1	6.2	0.0	c · 4	h · d	4.\	Det		nec			
•	ΕT	.ner	rne	r 11	L, :	21 C	: X	51120	Juic		J.4D	. u+	(0)	0.1	0.3	e.e	C.4	u.u	4),	טסנ	. ^	:115	uit	_60	::6d:
										_	Src		•									:1150	Jur	_60	c:6a:
١	In	iter	rnet	t Pr	oto	oco.	1 V	ers:	ion	4,	Src	: 1	72.:	31.0	9.3	, D	st:	17	2.3	1.0.	2				Ack:
+	In	ter	rne:	t Pr ssic	oto on (oco. Con	l Ve	ers: l Pi	ion	4, col	Src l, S	: 1 ⁻	72.: Por	31.0	0.3 808	, D: 4, I	st: Dst	17: Po	2.3: rt:	1.0. 560	2	Sed	; :	11,	Ack:
)	In Tr	ter ans	rnet smis	t Pr ssic	ot on (oco: Cont	l Ve tro:	ers: 1 Pi b0	ion roto	4, col	Src l, S 3e	: 1 [.] rc I ec	72.: Por 4b	31.0 t: 8	0.3 808 08	, D: 4, I	st: Dst 45	17: Po	2.3: rt:	1.0. 560 >1	2 34,	Sec	η: 1 Κ⊷	- 11, ·E·	Ack:
)	In Tr	ter ans	rnet smis 00	t Pr ssic 16 45	on (3e 8c	oco: Con 6c a9	1 Ve tro: 6d 40	ers: 1 Pi b0 00	ion roto 00	4, col 16 06	Src 1, S 3e 55	: 1 ^r rc l ec c6	72.: Por 4b ac	31.0 t: 8 d4	0.3 808 08 00	, D: 4, 1 00 03	st: Dst 45 ac	17: Po 00 1f	2.3: rt:	1.0. 560 >1	2 34, m	Sec > ·	η: 1 Κ··	.E.	Ack:
) (In Tr	ans	oo 00 00	t Pr ssic 16 45 02	on (3e 8c 1f	6c a9	l Ve tro: 6d 40 da	b0 00 e2	ion roto 00 40	4, col 16 06 9e	Src 1, S 3e 55 04	: 1 [.] rc ec c6 16	72.3 Por 4b ac 92	31.0 t: 8 d4 1f	0.3 808 08 00 37	, D: 4, 0 00 03 be	st: Dst 45 ac 80	17: Po 00 1f 18	2.3: rt:	1.0. 560 >1	2 34, m··· @·@·	Sec > · U ·	l: 1 K · ·	ι1, ·Ε·	Ack:
•	In Tr 000	o o o o	oo 00 00 00 01 bb	16 45 02 fd f1	3e 8c 1f 58	6c a9 94 7b	1 Ve tro: 6d 40 da 00	b0 00 e2	ion roto 00 40 18	4, 000] 16 06 9e 01	3e 55 04 08	: 1 ec c6 16 0a	72.3 Por 4b ac 92 b4	31.0 t: 8 d4 1f 56	0.3 808 08 00 37 ab	00 03 06 79	st: Dst 45 ac 80 f6	17: Po 00 1f 18 c2	2.3: rt:	1.0. 560 >l E	2 034, m··· @·@·	Sec U	K · · · · V7	11, ·E·	Ack:
•	In Tr 9001	o cans o o o o o	oo 00 00 00 01 bb	t Pr ssic 16 45 02 fd	3e 8c 1f 58	6c a9 94 7b	1 Ve tro: 6d 40 da 00	b0 00 e2	00 40 18	4, 000] 16 06 9e 01	3e 55 04 08	: 1 ec c6 16 0a	72.3 Por 4b ac 92 b4	31.0 t: 8 d4 1f 56 cb	0.3 808 08 00 37 ab	00 03 06 79	st: Dst 45 ac 80 f6	17: Po 00 1f 18 c2	2.3: rt:	1.0. 560 >1 E	2 034, m··· @·@·	Sec U	K · · · · V7	11, ·E·	Ack:

TLS Handshake and Data Transfer on Bob's side :

N	lo.	Time	Source	Destination	Protocol	Length Info
		5 11.236214			TLSv1.2	204 Client Hello
	17	7 11.240187	172.31.0.3	172.31.0.2	TLSv1.2	3112 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
	19	9 11.245716	172.31.0.2	172.31.0.3	TLSv1.2	3423 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
	21	1 11.248747	172.31.0.3	172.31.0.2	TLSv1.2	1236 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
	23	3 20.151982	172.31.0.2	172.31.0.3	TLSv1.2	103 Application Data
	25	5 28.055916	172.31.0.3	172.31.0.2	TLSv1.2	110 Application Data
	27	7 34.648178	172.31.0.2	172.31.0.3	TLSv1.2	105 Application Data
	29	9 34.648457	172.31.0.3	172.31.0.2	TLSv1.2	97 Encrypted Alert
	31	1 34.648668	172.31.0.2	172.31.0.3	TLSv1.2	97 Encrypted Alert

Cipher Suites that were set in our code that supports the PFS are shown in the client hello as follows:

```
Length Info
              Source
                             Destination
                                            Protocol
  15 11.236214 172.31.0.2
                                                        204 Client Hello
                            172.31.0.3
                                            TLSv1.2
  17 11.240187 172.31.0.3
                             172.31.0.2
                                            TLSv1.2
                                                     3112 Server Hello, Certificate, Serve
  19 11.245716 172.31.0.2
                             172.31.0.3
                                            TLSv1.2
                                                        3423 Certificate, Client Key Exchange
  21 11.248747 172.31.0.3
                             172.31.0.2
                                            TLSv1.2
                                                        1236 New Session Ticket, Change Ciphe
Ethernet II, Src: Xensourc_6c:6d:b0 (00:16:3e:6c:6d:b0), Dst: Xensourc_ec:4b:d4 (00:16:3e:ec
Internet Protocol Version 4, Src: 172.31.0.2, Dst: 172.31.0.3
Transmission Control Protocol, Src Port: 56034, Dst Port: 8084, Seq: 24, Ack: 28, Len: 138

    Transport Layer Security

 - TLSv1.2 Record Layer: Handshake Protocol: Client Hello
     Content Type: Handshake (22)
     Version: TLS 1.0 (0x0301)
     Length: 133
   - Handshake Protocol: Client Hello
       Handshake Type: Client Hello (1)
       Length: 129
       Version: TLS 1.2 (0x0303)
     Random: d38694fa94149a089c97707ef2be834c986d12ead6179934ff1035f38d7c4cd8
       Session ID Length: 0
       Cipher Suites Length
      Cipher Suites (3 suites)
         Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
         Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
         Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
       Compression Methods Length: 1
     Compression Methods (1 method)
       Extensions Length: 82
```

This was set by using the following line of code in client() function:

(SSL_CTX_set_cipher_list(ctx, "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256")

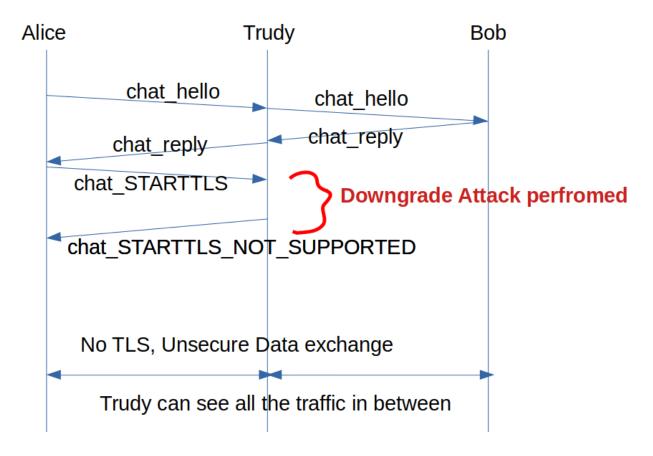
Server selects one of these(preconfigured in server as well) and selects the following Cipher suites among the 3 which the Client offered:

Vo. Time Source Destination Protocol Length Info 15 11.236214 172.31.0.2 172.31.0.3 TLSv1.2 204 Client Hello 17 11.240187 172.31.0.3 172.31.0.2 TLSv1.2 3112 Server Hello, Cer 19 11.245716 172.31.0.2 172.31.0.3 TLSv1.2 3423 Certificate, Client
17 11.240187 172.31.0.3 172.31.0.2 TLSv1.2 3112 Server Hello, Cer
19 11.245716 172.31.0.2 172.31.0.3 TLSv1.2 3423 Certificate, Clie
21 11.248747 172.31.0.3 172.31.0.2 TLSv1.2 1236 New Session Ticke
▶ Ethernet II, Src: Xensourc_ec:4b:d4 (00:16:3e:ec:4b:d4), Dst: Xensourc_6c:6d:
Internet Protocol Version 4, Src: 172.31.0.3, Dst: 172.31.0.2
> Transmission Control Protocol, Src Port: 8084, Dst Port: 56034, Seq: 28, Ack:
→ Transport Layer Security
→ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 65
→ Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 61
Version: TLS 1.2 (0x0303)
Random: d5b76cae5661defe8cc1047439cb9bbd76a44ebb14718977f3066b5a1dbb33d
Session ID Length: 0
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Compression Method: null (0)

TASK 3 : Downgrade Attack

We can see from "sec_server_client.cpp" that anytime the message "chat_STARTTLS_NOT_SUPPORTED" is received, we set the secure variable to "FALSE." For example, it is presumed that Bob does not want to conduct a secure chat conversation if Alice receives a "chat_STARTTLS_NOT_SUPPORTED" message after sending "chat_STARTTLS" to Bob.

Downgrade Attack is done as follows:



- We conducted the attack using the method downGrade() in the "sec_server_client.cpp".
- The socket is initially generated on the client side and is set to listen for connections using the listen address and port=8084 parameters.
- Hence, the false Trudy server receives the connection message sent by the client when it tries to connect to the server.
- All is well until Alice tries to establish a TLS connection and sends the command "chat STARTTLS" to the server. At that point, our function interjects and replies with the message "chat STARTTLS NOT SUPPORTED," eventually disabling all TLS connections between client and server.

We perform the downgrade attack by using command:

```
g++ downgrade.c++ -lssl -lcrypto -o dg
```

We first run the DNS Poisoning script in Container Host:

```
./poison-dns-alice1-bob1.sh
```

By running this script, Trudy has become the MITM, because the DNS resolvers at Alice and Bob side i.e "/etc/hosts" were changed by this script.

As a result, Alice and Bob's DNS have been contaminated, and their IP addresses have been changed. Then, in the container Trudy, we run the file "sec_server_client.cpp" to create a fake client and server socket.

Entire call flow can be seen in the command line below:

In fact, we are operating in an unsafe manner as we run "sec_server_client.cpp" to create a client-server communication between Alice and Bob.

The link between Alice and Bob is split as Alice and Trudy and between Trudy and Bob.

When Alice sends Trudy a "chat hello" message, she simply forwards it to Bob. Likewise, when Bob sends Trudy a "chat reply," she simply transfers the message to Alice.

When Trudy receives the chat STARTTLS from Alice, it blocks the message from Bob and sends chat STARTTLS NOT SUPPORTED to Alice.

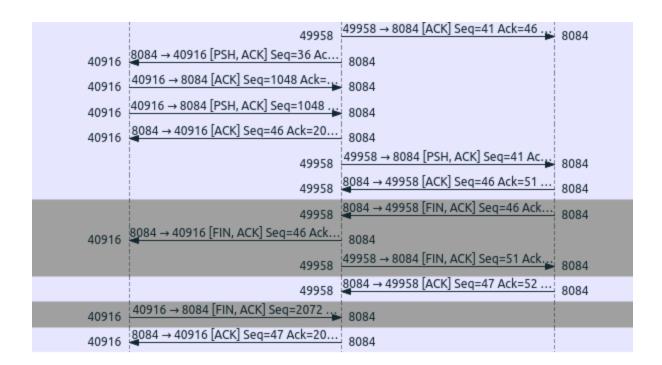
As TLS cannot be started at this time, ALice will continue with insecure mode chat and complete the application data transfer between the two sites. This is Trudy's downgrade attack.

PCAP traces at Trudy:

0.	Time	Source	Destination	Protocol	Length Info
	1 0.000000	172.31.0.2	172.31.0.4	TCP	74 40916 → 808
	2 0.000061	172.31.0.4	172.31.0.2	TCP	74 8084 → 4091
	3 0.000101	172.31.0.2	172.31.0.4	TCP	66 40916 → 808
	4 0.000295	172.31.0.4	172.31.0.3	TCP	74 49958 → 808
	5 0.000346	172.31.0.3	172.31.0.4	TCP	74 8084 → 4995
	6 0.000365	172.31.0.4	172.31.0.3	TCP	66 49958 → 808
	7 0.000916	172.31.0.2	172.31.0.4	TCP	76 40916 → 808
	8 0.000933	172.31.0.4	172.31.0.2	TCP	66 8084 → 4091
	9 0.001048	172.31.0.4	172.31.0.3	TCP	76 49958 → 808
	10 0.001066	172.31.0.3	172.31.0.4	TCP	66 8084 → 4995
	11 0.001247	172.31.0.3	172.31.0.4	TCP	76 8084 → 4995
	12 0.001257	172.31.0.4	172.31.0.3	TCP	66 49958 → 808
	13 0.001316	172.31.0.4	172.31.0.2	TCP	76 8084 → 4091
	14 0.002159	172.31.0.2	172.31.0.4	TCP	66 40916 → 808
	15 0.002161	172.31.0.2	172.31.0.4	TCP	79 40916 → 808
	16 0.002452	172.31.0.4	172.31.0.2	TCP	91 8084 → 4091
	17 0.002497	172.31.0.4	172.31.0.3	TCP	91 49958 → 808
	18 0.002561	172.31.0.3	172.31.0.4	TCP	91 8084 → 4995
	19 0.046059	172.31.0.4	172.31.0.3	TCP	66 49958 → 808
	20 0.046093	172.31.0.2	172.31.0.4	TCP	66 40916 → 808
	21 5.046240	172.31.0.2	172.31.0.4	TCP	1090 40916 → 808
	22 5.046389	172.31.0.4	172.31.0.3	TCP	71 49958 → 808
	23 5.066081	Xensourc cb:b1:38	Xensourc_ec:4b:d4	ARP	42 Who has 172
	24 5.066101	Xensourc cb:b1:38	Xensourc 6c:6d:b0	ARP	42 Who has 172
	25 5.066386	Xensourc ec:4b:d4	Xensourc cb:b1:38	ARP	42 Who has 172
	26 5.066405	Xensourc_cc:45:d4 Xensourc cb:b1:38	Xensourc_cb:d1:d4	ARP	42 172.31.0.4
	27 5.066392	Xensourc_6c:6d:b0	Xensourc_cb:b1:38	ARP	42 Who has 172
	28 5.066418	Xensourc_cb:b1:38	Xensourc_6c:6d:b0	ARP	42 WIIO HAS 172 42 172.31.0.4
	29 5.066422	Xensourc_ec:4b:d4	Xensourc_cb:b1:38	ARP	42 172.31.0.4
		_	_	ARP	
	30 5.066423	Xensourc_6c:6d:b0	Xensourc_cb:b1:38	TCP	42 172.31.0.2 66 8084 → 4091
	31 5.090131	172.31.0.4	172.31.0.2		
	32 5.090151	172.31.0.3	172.31.0.4	TCP	66 8084 → 4995
	33 10.949625	172.31.0.3	172.31.0.4	TCP	76 8084 → 4995
	34 10.949665	172.31.0.4	172.31.0.3	TCP	66 49958 → 808
	35 10.949797	172.31.0.4	172.31.0.2	TCP	76 8084 → 4091
	36 10.949841	172.31.0.2	172.31.0.4	TCP	66 40916 → 808
	37 15.126839	172.31.0.2	172.31.0.4	TCP	1090 40916 → 808
	38 15.126884	172.31.0.4	172.31.0.2	TCP	66 8084 → 4091
	39 15.127035	172.31.0.4	172.31.0.3	TCP	76 49958 → 808
	40 15.127072	172.31.0.3	172.31.0.4	TCP	66 8084 → 4995
	41 15.127209	172.31.0.3	172.31.0.4	TCP	66 8084 → 4995
	42 15.128276	172.31.0.4	172.31.0.2	TCP	66 8084 → 4091
	43 15.128359	172.31.0.4	172.31.0.3	TCP	66 49958 → 808
	44 15.128391	172.31.0.3	172.31.0.4	TCP	66 8084 → 4995
	45 15.129300	172.31.0.2	172.31.0.4	TCP	66 40916 → 808
_	46 15.129322	172.31.0.4	172.31.0.2	TCP	66 8084 → 4091

172.31.0.2 172.31.0.3

172.31.0.4 40916 → 8084 [SYN] Seq=0 Win=642. 8084 40916 8084 → 40916 [SYN, ACK] Seq=0 Ack... 8084 40916 → 8084 [ACK] Seq=1 Ack=1 Wi. 40916 49958 → 8084 [SYN] Seq=0 Win=642. 8084 49958 8084 → 49958 [SYN, ACK] Seq=0 Ack... 8084 49958 → 8084 [ACK] Seq=1 Ack=1 Wi... 8084 49958 40916 → 8084 [PSH, ACK] Seq=1 Ack. 8084 40916 8084 → 40916 [ACK] Seq=1 Ack=11 ... 8084 49958 → 8084 [PSH, ACK] Seq=1 Ack. 8084 49958 8084 → 49958 [ACK] Seq=1 Ack=11 ... 8084 8084 → 49958 [PSH, ACK] Seq=1 Ack... 8084 49958 49958 → 8084 [ACK] Seq=11 Ack=11 ... 8084 49958 8084 → 40916 [PSH, ACK] Seq=1 Ack... 8084 40916 40916 → 8084 [ACK] Seq=11 Ack=11 ... 8084 40916 → 8084 [PSH, ACK] Seq=11 Ac. 8084 40916 8084 → 40916 [PSH, ACK] Seq=11 Ac... 8084 40916 49958 → 8084 [PSH, ACK] Seq=11 Ac. 8084 49958 8084 → 49958 [PSH, ACK] Seq=11 Ac... 8084 49958 → 8084 [ACK] Seq=36 Ack=36 ... 8084 49958 40916 → 8084 [ACK] Seq=24 Ack=36 ... 8084 40916 → 8084 [PSH, ACK] Seq=24 Ac. 8084 40916 49958 → 8084 [PSH, ACK] Seq=36 Ac. 8084 49958 40916 8084 → 40916 [ACK] Seq=36 Ack=10... 8084 49958 8084 → 49958 [ACK] Seq=36 Ack=41 ... 8084 49958 8084 → 49958 [PSH, ACK] Seq=36 Ac... 8084



As you can see, there is no TLS protocol used as a downgrade was performed by Trudy. Important Messages in the call flow according to the call flow diagram:

	Time	2			S	ourc	e					De	stina	atio	n		Protocol	Length I
7	0.0	009	16		1	72.	31.0	0.2				17	2.3	1.0	. 4		TCP	76 4
8	0.0	009	33		1	72.	31.6	0.4				17	2.3	1.0	.2		TCP	66 8
9	0.0	010	48		1	72.	31.6	0.4				17	2.3	1.0	.3		TCP	76 4
ern ern nsm	et I et P	I, rot on	Src oco Con	: X 1 V	ens ers	our ion	c_6 4,	c:6d Src	:b0	(0 .72.	0:1 31.	6:3 0.2	e:6	c:6 st:	d:b0	ed (608 b 0), Dst: 2.31.0.4 ort: 8084	Xensour	c_cb:b1:3
00	16	3e	cb	b1	38	00	16	3e	6c	6d	b0	08	00	45	00	> 8	· · >lm· ·	· E •
	3e										1f							
00	04	9f	d4	1f	94	f6	96	3f	dc	d8	e9	d3	a1	80	18		?	
01	L f6	58	75	00	00	01	01	08	0a	97	5b	77	16	8b	7b	··Xu··	· · · · · [w	• • {
b2	2 1d	63	68	61	74	5f	68	65	6c	6c	6f					··chat_	_h ello	-

Time	Source	Destination	Protocol Lengt
7 0.000916	172.31.0.2	172.31.0.4	TCP
8 0.000933	172.31.0.4	172.31.0.2	TCP
9 0.001048	172.31.0.4	172.31.0.3	TCP

rnet Protocol Version 4, Src: 172.31.0.4, Dst: 172.31.0.3

smission Control Protocol, Src Port: 49958, Dst Port: 8084, Seq: 1, Ack (10 bytes)

ta: 636861745f68656c6c6f

ength: 10]

0.0	16	20	00	4h	d4	00	16	20	ch	h1	20	00	00	45	00	··>·K··· >··8··E·
00	3e	5d	83	40	00	40	06	84	f1	ac	1f	00	04	ac	1f	·>]·@·@· · · · · · · ·
0.0	0.3	с3	26	1f	94	fe	aa	06	1a	69	ce	ff	99	80	18	&
01	. †6	58	76	00	00	01	01	08	0a	82	00	92	c1	d1	21	··Xv····/
h2	a7	63	68	61	74	5f	68	65	6c	60	6f					chat h ello
102		00	00	01	17	01	00	00	00	00	01					01142_11 0110
b2	a7	63	68	61	74	5f	68	65	6c	6c	6f					··chat_h ello

\	lo.	Time	Source	Destination	Protocol	Lengtl
	9	0.001048	172.31.0.4	172.31.0.3	TCP	7
	10	0.001066	172.31.0.3	172.31.0.4	TCP	6
	11	0.001247	172.31.0.3	172.31.0.4	TCP	7

- Ethernet II, Src: Xensourc_ec:4b:d4 (00:16:3e:ec:4b:d4), Dst: Xensourc_cb:b:
- Internet Protocol Version 4, Src: 172.31.0.3, Dst: 172.31.0.4
- > Transmission Control Protocol, Src Port: 8084, Dst Port: 49958, Seq: 1, Ack
- ▼ Data (10 bytes)

Data: 636861745f7265706c79

[Length: 10]

0000	00 16	3e	cb	b1	38	00	16	3e	ec	4b	d4	08	00	45	00	··>··8 <mark>·· ></mark> ·K···E·
0010	00 3e	66	ad	40	00	40	06	7b	с7	ac	1f	00	03	ac	1f	·>f·@·@· {·····
0020	00 04	1f	94	c3	26	e9	ce	ff	99	fe	aa	06	24	80	18	• • • • • • • • • • • • • • • • • • • •
0030	01 fd	58	76	00	00	01	01	08	0a	d1	2f	b2	a7	82	00	··Xv····/···
0040	92 c1	63	68	61	74	5f	72	65	70	6c	79					∴chat_r eply

44		2			20	ourc	e					De	stina	itior	1		P	rotocol	Leng
TT	0.0	012	47		1	72.	31.0	.3				17	2.3	1.0	. 4		Т	CP	
12	0.0	012	57		1	72.	31.0	. 4				17	2.3	1.0	. 3		Т	CP	
13	0.0	013	16		1	72.	31.0	. 4				17	2.3	1.0	. 2		T	CP	
rne smi	t P ssi	rot on	oco Con	1 V	ers	ion	4,	Src	: 1	72.	31.	0.4	, D	st:	172	31.0.	2		
•		-	•	l5f7	265	706	c79												
00	16	3e	6c	6d	b0	00	16	3e	cb	b1	38	08	00	45	00	··>1m		> · · 8	٠E٠
00	3e	75	ec	40	00	40	06	6c	89	ac	1f	00	04	ac	1f	·>u ⋅@	. @ .	1	
00	02	1f	94	9f	d4	d8	e9	d3	a1	f6	96	3f	e6	80	18			?	
01	fd	58	75	00	00	01	01	08	0a	8b	7b	b2	1f	97	5b	· · Xu ·		• • • { •	• • [
77	16	63	68	61	74	5f	72	65	70	6c	79					w∙cha	t_r	eply	-
	erne erne erne esmi (1 ata: enç 00 00 00	ernet I ernet P esmissi (10 b ata: 63 ength: 00 16 00 3e 00 02 01 fd	ernet II, ernet Prot esmission (10 byte ata: 63686 ength: 16 00 16 3e 00 3e 75 00 02 1f 01 fd 58	ernet Protoco smission Con (10 bytes) ata: 63686174 ength: 10] 00 16 3e 6c 00 3e 75 ec 00 02 1f 94 01 fd 58 75	ernet II, Src: X ernet Protocol V esmission Contro (10 bytes) ata: 636861745f7 ength: 10] 00 16 3e 6c 6d 00 3e 75 ec 40 00 02 1f 94 9f 01 fd 58 75 00	ernet II, Src: Xens ernet Protocol Vers esmission Control P (10 bytes) eta: 636861745f7265 ength: 10] 00 16 3e 6c 6d b0 00 3e 75 ec 40 00 00 02 1f 94 9f d4 01 fd 58 75 00 00	rnet II, Src: Xensour rnet Protocol Version smission Control Prot (10 bytes) ata: 636861745f7265706 ength: 10] 00 16 3e 6c 6d b0 00 00 3e 75 ec 40 00 40 00 02 1f 94 9f d4 d8 01 fd 58 75 00 00 01	ernet II, Src: Xensourc_cb ernet Protocol Version 4, esmission Control Protocol (10 bytes) ata: 636861745f7265706c79 ength: 10] 00 16 3e 6c 6d b0 00 16 00 3e 75 ec 40 00 40 06 00 02 1f 94 9f d4 d8 e9	ernet II, Src: Xensourc_cb:b1 ernet Protocol Version 4, Src esmission Control Protocol, S (10 bytes) eta: 636861745f7265706c79 ength: 10] 00 16 3e 6c 6d b0 00 16 3e 00 3e 75 ec 40 00 40 06 6c 00 02 1f 94 9f d4 d8 e9 d3 01 fd 58 75 00 00 01 01 08	ernet II, Src: Xensourc_cb:b1:38 ernet Protocol Version 4, Src: 1 esmission Control Protocol, Src (10 bytes) eta: 636861745f7265706c79 ength: 10] 00 16 3e 6c 6d b0 00 16 3e cb 00 3e 75 ec 40 00 40 06 6c 89 00 02 1f 94 9f d4 d8 e9 d3 a1 01 fd 58 75 00 00 01 01 08 0a	ernet II, Src: Xensourc_cb:b1:38 (0 ernet Protocol Version 4, Src: 172. esmission Control Protocol, Src Por (10 bytes) eta: 636861745f7265706c79 ength: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 00 3e 75 ec 40 00 40 06 6c 89 ac 00 02 1f 94 9f d4 d8 e9 d3 a1 f6 01 fd 58 75 00 00 01 01 08 0a 8b	rnet II, Src: Xensourc_cb:b1:38 (00:1 rnet Protocol Version 4, Src: 172.31. smission Control Protocol, Src Port: (10 bytes) ata: 636861745f7265706c79 length: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 38 00 3e 75 ec 40 00 40 06 6c 89 ac 1f 00 02 1f 94 9f d4 d8 e9 d3 a1 f6 96 01 fd 58 75 00 00 01 01 08 0a 8b 7b	ernet II, Src: Xensourc_cb:b1:38 (00:16:3 ernet Protocol Version 4, Src: 172.31.0.4 esmission Control Protocol, Src Port: 808 a (10 bytes) eta: 636861745f7265706c79 ength: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 38 08 00 3e 75 ec 40 00 40 06 6c 89 ac 1f 00 00 02 1f 94 9f d4 d8 e9 d3 a1 f6 96 3f 01 fd 58 75 00 00 01 01 08 0a 8b 7b b2	ernet II, Src: Xensourc_cb:b1:38 (00:16:3e:cernet Protocol Version 4, Src: 172.31.0.4, Desmission Control Protocol, Src Port: 8084, a (10 bytes) ata: 636861745f7265706c79 Length: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 38 08 00 00 3e 75 ec 40 00 40 06 6c 89 ac 1f 00 04 00 02 1f 94 9f d4 d8 e9 d3 a1 f6 96 3f e6 01 fd 58 75 00 00 01 01 08 0a 8b 7b b2 1f	ernet II, Src: Xensourc_cb:b1:38 (00:16:3e:cb:b2:rnet Protocol Version 4, Src: 172.31.0.4, Dst: 18mission Control Protocol, Src Port: 8084, Dst 1 (10 bytes) 1 (10 bytes) 1 (10 bytes) 2 (10 bytes) 2 (10 bytes) 3 (10 bytes) 4 (10 bytes) 4 (10 bytes) 5 (10 bytes) 6 (10 bytes) 6 (10 bytes) 6 (10 bytes) 7 (10 bytes) 7 (10 bytes) 8 (10 bytes) 8 (10 bytes) 9 (10 bytes)	ernet II, Src: Xensourc_cb:b1:38 (00:16:3e:cb:b1:38) ernet Protocol Version 4, Src: 172.31.0.4, Dst: 172 esmission Control Protocol, Src Port: 8084, Dst Port (10 bytes) eta: 636861745f7265706c79 ength: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 38 08 00 45 00 00 3e 75 ec 40 00 40 06 6c 89 ac 1f 00 04 ac 1f 00 02 1f 94 9f d4 d8 e9 d3 a1 f6 96 3f e6 80 18 01 fd 58 75 00 00 01 01 08 0a 8b 7b b2 1f 97 5b	ernet II, Src: Xensourc_cb:b1:38 (00:16:3e:cb:b1:38), Dst ernet Protocol Version 4, Src: 172.31.0.4, Dst: 172.31.0.3 esmission Control Protocol, Src Port: 8084, Dst Port: 4093 (10 bytes) ata: 636861745f7265706c79 Length: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 38 08 00 45 00 >lm 00 3e 75 ec 40 00 40 06 6c 89 ac 1f 00 04 ac 1f >u 0 00 02 1f 94 9f d4 d8 e9 d3 a1 f6 96 3f e6 80 18 ····	ernet II, Src: Xensourc_cb:b1:38 (00:16:3e:cb:b1:38), Dst: Xernet Protocol Version 4, Src: 172.31.0.4, Dst: 172.31.0.2 (smission Control Protocol, Src Port: 8084, Dst Port: 40916, a (10 bytes) ata: 636861745f7265706c79 Length: 10] 00 16 3e 6c 6d b0 00 16 3e cb b1 38 08 00 45 00	ernet II, Src: Xensourc_cb:b1:38 (00:16:3e:cb:b1:38), Dst: Xensourcernet Protocol Version 4, Src: 172.31.0.4, Dst: 172.31.0.2 (smission Control Protocol, Src Port: 8084, Dst Port: 40916, Seq: 10 (10 bytes) (10

7	Time			S	ourc	e					De	stina	ation	1		Protocol	Lengt
13 (0.00	1316		1	72.	31.0	.4				17	2.3	1.0	. 2		TCP	-
14 (0.00	2159		1	72.	31.0	.2				17	2.3	1.0	. 4		TCP	(
15 (0.00	2161		1	72.	31.0).2				17	2.3	1.0	. 4		TCP	7
erne nsmi u (1 ata:	15 0.002161 172.31.0.2 172.31.0.4 TCP rnet II, Src: Xensourc_6c:6d:b0 (00:16:3e:6c:6d:b0), Dst: Xensourc_cb:b rnet Protocol Version 4, Src: 172.31.0.2, Dst: 172.31.0.4 smission Control Protocol, Src Port: 40916, Dst Port: 8084, Seq: 11, Ac (13 bytes) ta: 636861745f5354415254544c53 ength: 13] 00 16 3e cb b1 38 00 16 3e 6c 6d b0 08 00 45 00																
00	16 3	Be cb	b1	38	00	16	3e	6c	6d	b0	08	00	45	00	>8	· >1m··	٠E٠
00	41 3	39 ca	40	00	40	06	a8	a8	ac	1f	00	02	ac	1f	· A9 · @ · @		
		A - 1 4	4.5	0.4	f6	96	3f	e6	d8	e9	d3	ab	80	18		. 2	
00	04 9	9T 04	ΤI	94	10	50	٠.	-									
	f6 5	8 78	00	00	01	01	08		97	5b	77	17	8b	7b		· · · · [w	· · {
01	f6 5		00	00	01	01		0a			77 54			7b			· · {

Trudy sends TLS not supported message acting as Bob to Client :

-	Time	•			S	ourc	e					De	stina	atior	1		Protocol	Length	Info
14	0.0	921	59		1	72.	31.	9.2				17	2.3	1.0	. 4		TCP	66	409
15	0.0	921	61		1	72.	31.	9.2				17	2.3	1.0	. 4		TCP	79	409
16	0.0	024	52		1	72.	31.	0.4				17	2.3	1.0	. 2		TCP	91	808
erne	t P ssi	rot on	oco Con	l V	ers	ion	4,	Src	: 1	72.	31.	0.4	, D	st:	17	8), Dst: 2.31.0.2 rt: 40916			
ata:	63	686	174	15f5	354	415	5254	5440	535	ōf4€	4f5	545f	535	5550	504	f5254			
Leng	jth:	25	i]																
00	16	3e	6c	6d	b0	00	16	3e	cb	b1	38	08	00	45	00	··>1m·	. >8.	٠E٠	
00	4d	75	ed	40	00	40	06	6c	79	ac	1f	00	04	ac	1f	- Mu - @ - @) · ly · · ·		
00	02	1f	94	9f	d4	d8	e9	d3	ab	f6	96	3f	f3	80	18		?		
01	fd	58	84	00	00	01	01	98	0a	8b	7b	b2	20	97	5b	· · X · · · ·	{.	· [
77	17	63	68	61	74	5f	53	54	41	52	54	54	4c	53	5f	w·chat_	S TARTT	LS_	
4e	4f	54	5f	53	55	50	50	4f	52	54						NOT_SUF	P ORT		

Thus he can decrypt all the messages :

	Time				S	ourc	e					De	stina	ation	1		Protocol	Length Info
19	0.04	605	59		1	72.	31.0	.4				17	2.3	1.0	.3		TCP	66 49
20	0.04	609	93		1	72.	31.0).2				17	2.3	1.0	. 4		TCP	66 40
21	5.04	624	10		1	72.	31.0).2				17	2.3	1.0	. 4		TCP	1090 40
nerne terne ansmi ta (1																		
	34 3							a4										
00	04 9	9f	d4	1f	94	f6	96	3f	f3	d8	e9	d3	c4	80	18		. ?	
01	f6 5	5c	6b	00	00	01	01	08	0a	97	5b	8a	cb	8b	7b	· · \k · · ·	[.	• • {
b2	20 (68	65	6c	6c	6f	00	00	00	00	00	00	00	00	00	· hello		
00	00 (00	00	00	00	00	00	00	00	00	00	00	00	00	00			

	Time	Source	Destination	Protocol	Lengt
32	5.090151	172.31.0.3	172.31.0.4	TCP	E
33	10.949625	172.31.0.3	172.31.0.4	TCP	7
34	10.949665	172.31.0.4	172.31.0.3	TCP	€

Identification: 0x66b0 (26288)
-lags: 0x40, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Γime to Live: 64

```
Protocol: TCP (6)
leader Checksum: 0x7bc4 [validation disabled]
 00 16 3e cb b1 38 00 16
                            3e ec 4b d4 08 00 45 00
                                                                  > · K · · · · E ·
                                                         ..>..8..
 00 3e 66 b0 40 00 40 06
                           7b c4 ac 1f 00 03 ac 1f
                                                        ·>f·@·@· {·····
 00 04 1f 94 c3 26 e9 ce
                           ff bc fe aa 06 42 80 18
                                                         . . . . . & . . . . . . B . .
 01 fd 58 76 00 00 01 01
                            08 0a d1 2f dd 6c 82 00
                                                         ..Xv.... .../.1..
 a6 77 68 69 65 65 2c 41 6c 69 63 65
                                                         ·whiee, A lice
```

TASK 4 : Downgrade Attack [Active MITM Attack]

This attack is different from the downgrade attack of Task 3. In this, TLS is used, despite that, Trudy is able to decrypt all the messages in between Alice and Bob as she was able to compromise the Intermediate CA. So, he can issue fake certificates and thus possesses the keys of both the connection, towards the client and towards the server, thus can decrypt the traffic in between.

We will use an active MITM attack in this work to mess with Alice and Bob's chat communication. First, we're going to poison the DNS and change the IP addresses such that Trudy serves as Alice's server and Bob's client.

./poison-dns-alice1-bob1.sh

We use the "downgrade.c++_task4" instead of mitm():

The Trudy client and server certificates are initially loaded, and a server-side socket is constructed, tied to a port, and listening to see if any clients are connecting.

When the client sends "chat STARTTLS" to the server in an attempt to create a TLS connection, Trudy replies with "chat STARTTLS ACK," and the client SSL connection is formed.

Similar to before, Trudy now assumes the role of the client and requests a TLS connection from the server. When the server responds with the STARTTLS ACK, the SSL connection to the

server is established.

Trudy may now alter texts and data on both sides.

Using the following command, the downgrade is carried out at Trudy container:

```
g++ downgrade_task4.c++ -lssl -lcrypto -o dg
```

Fakebob.crt and fakealice.crt certificates are created by Trudy with key-pairs in .pem files. These thus are verified with the help of openssl. Instead of launching the downgrade in task3, Trudys' certificate gets verified and Client server TLS handshake is carried out. Thus a TLS pipe is established between client and server but in reality there are 2 TLS pipes established: Between Alice and Trudy, and between Trudy and bob.

Call flow in the command line:

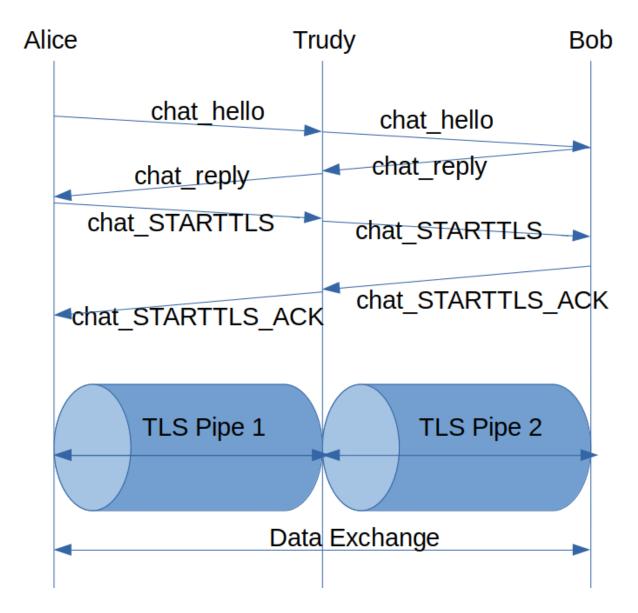
```
P ALICE

TRUDY

TRUCH

TRUDY

TO TRUBHALLE, ASK PATTLS | SWAITING CAN PAINT | SWAITING
```



Now because Trudy is the MITM, he can tamper any messages in between Alice and Bob. This is possible because the CA is compromised and trudy was able to make fake certificates.

Alice sent chat_STARTTLS message thinking its sending to bob and it is then received by Trudy. chat_STARTTLS_ACK is received by Trudy from Bob and it then sends it to Alice in behalf of bob. A handshake takes place with the help of fake certificates.

Trudy gets chat_hello:

	Time	Source	Destination	Protocol	Length	Info
7	0.000709	172.31.0.2	172.31.0.4	TCP	76	41610
8	0.000717	172.31.0.4	172.31.0.2	TCP	66	8084
9	0.000762	172.31.0.4	172.31.0.3	TCP	76	44164
10	0.000772	172.31.0.3	172.31.0.4	TCP	66	8084
11	0.000884	172.31.0.3	172.31.0.4	TCP	76	8084
12	0.000900	172.31.0.4	172.31.0.3	TCP	66	44164
13	0.000922	172.31.0.4	172.31.0.2	TCP	76	8084
14	0.000935	172.31.0.2	172.31.0.4	TCP	66	41610
15	0.001255	172.31.0.2	172.31.0.4	TCP	79	41610

rame 7: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
thernet II, Src: Xensourc_6c:6d:b0 (00:16:3e:6c:6d:b0), Dst: Xensourc_cb:b1:38 (0
nternet Protocol Version 4, Src: 172.31.0.2, Dst: 172.31.0.4
ransmission Control Protocol, Src Port: 41610, Dst Port: 8084, Seq: 1, Ack: 1, Le
ata (10 bytes)

Gets chat reply from bob:

Time	Source	Destination	Proto	col Length Info
6 0.000	618 172.31.0.4	172.31.0.3	TCP	66 441
7 0.000	709 172.31.0.2	172.31.0.4	TCP	76 416
8 0.000	717 172.31.0.4	172.31.0.2	TCP	66 808
9 0.000	762 172.31.0.4	172.31.0.3	TCP	76 441
10 0.000	772 172.31.0.3	172.31.0.4	TCP	66 808
11 0.0008	172.31.0.3	172.31.0.4	TCP	76 808
12 0.0009	900 172.31.0.4	172.31.0.3	TCP	66 441
13 0.0009	922 172.31.0.4	172.31.0.2	TCP	76 808
14 0.0009	935 172.31.0.2	172.31.0.4	TCP	66 416

me 11: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) ernet II, Src: Xensourc_ec:4b:d4 (00:16:3e:ec:4b:d4), Dst: Xensourc_cb:b1:38 ernet Protocol Version 4, Src: 172.31.0.3, Dst: 172.31.0.4 nsmission Control Protocol, Src Port: 8084, Dst Port: 44164, Seq: 1, Ack: 11, a (10 bytes)

```
      00
      16
      3e
      cb
      b1
      3e
      ec
      4b
      d4
      08
      00
      45
      00
      c>
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
      c
```

Time	Source	Destination	Protocol Lengt
15 0.001255	172.31.0.2	172.31.0.4	TCP
16 0.001284	172.31.0.4	172.31.0.3	TCP
17 0.044571	172.31.0.4	172.31.0.2	TCP
18 0.044593	172.31.0.3	172.31.0.4	TCP
ame 15: 79 bytes o	n wire (632 bits), 79	bytes captured (632	bits)
ernet Protocol Ve	nsourc_6c:6d:b0 (00:1 rsion 4, Src: 172.31. Protocol, Src Port:	0.2, Dst: 172.31.0.4	
00 16 3e cb b1 3	8 00 16 3e 6c 6d b0	08 00 45 00>8	·· >lm···E·
00 41 84 69 40 6	0 40 06 5e 09 ac 1f	00 02 ac 1f ·A·i@·@	g). ^
00 04 a2 8a 1f 9	4 d2 21 a5 a8 ac dc	09 0c 80 18 ·····	!
01 f6 58 78 00 0	00 01 01 08 0a 97 75	86 f8 8b 95 ·· Xx · ·	· · · · · u · · · ·
c2 00 63 68 61 7	4 5f 53 54 41 52 54	54 4c 53 ···chat_	_S TARTTLS

Gets ACK from Bob which it then forwards to Alice :

					-								•					.9
25 5	.09682	20		Xens	ourc	_ec	:4b	:d4		Xe	nso	urc	_cb:b1	:38	Α	RP		42 1
26 5	.09682	23		Xens	ourc	_6c	:6d	:b0		Xe	nso	urc	_cb:b1	:38	Α	RP		42 1
27 7	.7237	39		172.	31.0	. 3				17	2.3	1.0	. 4		Т	CP		83 80
28 7	.72390	96		172.	31.0	. 4				17	2.3	1.0	. 2		Т	CP		83 80
me 27	: 83	byte	S 0	n wir	e (6	64	bit	s),	83	by	tes	ca	pture	(664	↓ bi	ts)		
ernet	II,	Src:	Xe	nsour	c_ec	:4b	:d4	(0	0:1	6:3	e:e	c:4	b:d4),	Dst:	Xe	nsour	c_cb	:b1:38
ernet	Prot	ocol	Ve	rsior	14,	Src	: 1	72.	31.	0.3	, D	st:	172.3	31.0.4	l			
ınsmis	sion	Cont	rol	Prot	ocol	, s	rc	Por	t:	808	4,	Dst	Port:	4416	64,	Seq:	11,	Ack: 2
ta (17	byte	s)																
00 1	16 3e	ch h	11 3	88 00	16	36	ec	4h	d4	08	00	45	99	> :	8	> · K · ·	. F.	
	15 1f										03	-			_		_	
	94 1f										6b					·Prq·		
01 1	fd 58	7d 6	90 0	0 01	01	08	0a	d1	49	e0	b3	82				· · · i ·		
a2 a	a3 63	68 6	31 7	74 5f	53	54	41	52	54	54	4c	53	5f	· · cha	t_s	TART	ΓLS_	
41 4	13 4b													ACK				

Time Source Destination Protocol Length In

Thus TLS connection is established.

TLS Call flow at Trudy's Side:

tls			
). Time	Source	Destination	Protocol Length Info
29 7.732414	172.31.0.2	172.31.0.4	TLSV1,2 204 Client Hello
31 7.735898	172.31.0.4	172.31.0.2	TLSV1.2 3112 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
33 7.742108	172.31.0.2	172.31.0.4	TLSv1.2 3423 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
35 7.744141	172.31.0.4	172.31.0.2	TLSv1.2 1236 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
36 7.744373	172.31.0.4	172.31.0.3	TLSv1.2 254 Client Hello
38 7.746916	172.31.0.3	172.31.0.4	TLSv1.2 3112 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
40 7.752383	172.31.0.4	172.31.0.3	TLSv1.2 3423 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
42 7.754279	172.31.0.3	172.31.0.4	TLSv1.2 1236 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
45 15.148178	172.31.0.2	172.31.0.4	TLSv1.2 104 Application Data
46 15.148369	172.31.0.4	172.31.0.3	TLSv1.2 104 Application Data
49 20.396136	172.31.0.3	172.31.0.4	TLSv1.2 110 Application Data
51 20.396366	172.31.0.4	172.31.0.2	TLSv1.2 110 Application Data
53 24.188124	172.31.0.2	172.31.0.4	TLSv1.2 105 Application Data
55 24.188363	172.31.0.4	172.31.0.2	TLSv1.2 97 Encrypted Alert
57 24.188617	172.31.0.2	172.31.0.4	TLSv1.2 97 Encrypted Alert
59 24.188846	172.31.0.4	172.31.0.3	TLSv1.2 97 Encrypted Alert
62 24.190837	172.31.0.3	172.31.0.4	TLSv1.2 97 Encrypted Alert

TLS Call flow at Alice's Side:

Time	Source	Destination	Protocol	Length Info
16 7.732580	172.31.0.2	172.31.0.4	TLSv1.2	204 Client Hello
18 7.736101	172.31.0.4	172.31.0.2	TLSv1.2	3112 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
20 7.742296	172.31.0.2	172.31.0.4	TLSv1.2	3423 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
22 7.744341	172.31.0.4	172.31.0.2	TLSv1.2	1236 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
24 15.148351	172.31.0.2	172.31.0.4	TLSv1.2	104 Application Data
26 20.396585	172.31.0.4	172.31.0.2	TLSv1.2	110 Application Data
28 24.188244	172.31.0.2	172.31.0.4	TLSv1.2	105 Application Data
30 24.188582	172.31.0.4	172.31.0.2	TLSv1.2	97 Encrypted Alert
32 24.188800	172.31.0.2	172.31.0.4	TLSv1.2	97 Encrypted Alert

TLS Call flow at Bob's Side:

Time	Source	Destination	Protocol	Length Info
15 7.743825				254 Client Hello
17 7.746356	172.31.0.3	172.31.0.4		3112 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
19 7.751836	172.31.0.4	172.31.0.3	TLSv1.2	3423 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
21 7.753722	172.31.0.3	172.31.0.4	TLSv1.2	1236 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
23 15.147828	172.31.0.4	172.31.0.3	TLSv1.2	104 Application Data
25 20.395502	172.31.0.3	172.31.0.4	TLSv1.2	110 Application Data
27 24.188299	172.31.0.4	172.31.0.3	TLSv1.2	97 Encrypted Alert
30 24.190267	172.31.0.3	172.31.0.4	TLSv1.2	97 Encrypted Alert

ANTI-PLAGIARISM STATEMENT

We certify that this assignment/report is our own work, based on our personal

study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. We pledge to uphold the principles of honesty and responsibility at CSE@ITH. In addition, We understand my responsibility to report honor violations by other students if we become aware of it.

Names: Tejas Deshmukh (cs22mtech12005), Mahanth Kumar Valluri (cs22mtech11015)

Date: 27/03/2023

Signature: <Tejas, Mahanth

References:

- 1. OpenSSL Cookbook: Chapter 1. OpenSSL Command Line (feistyduck.com)
- 2. /docs/man1.1.1/man3/index.html (openssl.org)
- 3. OpenSSL client and server from scratch, part 1 Arthur O'Dwyer Stuff mostly about C++ (quuxplusone.github.io)
- 4. ssl TLS/SSL wrapper for socket objects Python 3.9.2 documentation
- 5. Secure programming with the OpenSSL API IBM Developer
- 6. Simple TLS Server OpenSSLWiki

- 7. The /etc/hosts file (tldp.org)
- 8. PowerPoint Presentation (owasp.org)
- 9. SEED Project (seedsecuritylabs.org)