Login into the remote system :

```
ssh ubuntu@10.200.13.114
```

Task 1

The Certificate folder contains all of the Certificate Signing Requests (CSRs), all of the certificates (CAs, Alice, Bob).

Task 2

Steps :

1) Run “Makefile_bob_task2” in the Bob container which is present in the “/root” directory :

```
make -f Makefile_bob_task2
```

2) Run “Makefile_alice_task2” in the Alice container which is present in the “/root” directory :

```
make -f Makefile_alice_task2
```

3) Enter one of the following on Bob’s side :
    a) For Encrypted communication : chat_STARTTLS_ACK
    b) For Unencrypted communication : chat_STARTTLS_NOT_SUPPORT

4) Send and receive messages.
5) Send chat_close on any side to stop the communication at any point.

Task 3

Steps :

1) Poison Alice and Bob’s Container on Container Host by running :

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

2) Run “Makefile_bob_task3” in the Bob container which is present in the “/root” directory :

```
make -f Makefile_bob_task3
```

3) Run “Makefile_trudy_task3” in the Trudy container which is present in the “/root” directory :

```
make -f Makefile_trudy_task3
```

4) Run “Makefile_alice_task3” in the Alice container which is present in the “/root” directory :

```
make -f Makefile_alice_task3
```

5) Send and receive messages(Alice and Bob) over the unencrypted channel.
6) Eavesdrop Alice and Bob on the Trudy container.
7) Send chat_close on any side(Alice or Bob) to stop the communication at any point.
8) To unpoison, execute the following on Container host :

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

Task 4

Steps :

1) Poison Alice and Bob’s Container on Container Host by running :

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

2) Run “Makefile_bob_task4” in the Bob container which is present in the “/root” directory :

```
make -f Makefile_bob_task4
```

3) Run “Makefile_trudy_task4” in the Trudy container which is present in the “/root” directory :

```
make -f Makefile_trudy_task4
```

4) Run “Makefile_alice_task4” in the Alice container which is present in the “/root” directory :

```
make -f Makefile_alice_task4
```

5) Enter one of the following on Bob’s side :
    a) For Encrypted communication : chat_STARTTLS_ACK
    b) For Unencrypted communication : chat_STARTTLS_NOT_SUPPORT

6) Send and receive messages(Alice and Bob) over the encrypted/ unencrypted channel as per what you chose in the above step.
7) Carry out the MITM attack on Trudy and can tamper/ eavesdrop on the Trudy container.
8) Send chat_close on any side(Alice or Bob) to stop the communication at any point.
9) To unpoison, execute the following on Container host :

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

If you want to test the tasks without makefiles, detailed description of execution without the makefiles is given below :

Task 2

On the Alice's side :

1. Login into the Alice container using :

```
lxc exec alice1 bash
```

2. Go to the following directory :

```
cd programs
```

3. Compile :

```
g++ sec_server_client.cpp -lssl -lcrypto -o sc
```

4. Run :

```
./sc -c bob1
```

5. Send and receive messages to/from Bob.
6. Send `"chat_close"` to close the connection at any point of time.

On the Bob's side :

1. Login into the Bob container using :

```
lxc exec bob1 bash
```

2. Go to the following directory :

```
cd programs
```

3. Compile :

```
g++ sec_server_client.cpp -lssl -lcrypto -o sc
```

4. Run :

```
./sc -s
```

5. Send `"chat_STARTTLS_ACK"` to establish a TLS connection. Send `"chat_STARTTLS_NOT_SUPPORTED"` to have a data transfer without TLS.
6. Send and receive messages to/from Alice.
7. Send `"chat_close"` to close the connection at any point of time.

Task 3

Poison Alice and Bob's Container on Container Host by running :

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

On Alice's side :

1. Login into the Alice container using :

```
lxc exec alice1 bash
```

2. Go to the following directory :

```
cd programs
```

3. Compile :

```
g++ sec_server_client.cpp -lssl -lcrypto -o sc
```

4. Run :

```
./sc -c bob1
```

5. Send and receive messages to/from Bob.
6. Send `"chat_close"` to close the connection at any point of time.

On Bob's Side :

1. Login into the Bob container using :

```
lxc exec bob1 bash
```

2. Go to the following directory :

```
cd programs
```

3. Compile :

```
g++ sec_server_client.cpp -lssl -lcrypto -o sc
```

4. Run :

```
./sc -s
```

5. Send `"chat_STARTTLS_ACK"` to establish a TLS connection. Send `"chat_STARTTLS_NOT_SUPPORTED"` to have a data transfer without TLS.
6. Send and receive messages to/from Alice.
7. Send `"chat_close"` to close the connection at any point of time.

On Trudy's Side :

1. Login into the Bob container using :

```
lxc exec trud1 bash
```

2. Compile :

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

3. Run :

```
./dg
```

4. Do eavesdropping between Alice and Bob.

To unpoison, run the following on the Container Host :

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

Task 4

Poison Alice and Bob's Container on Container Host by running :

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

On Alice's side :

1. Login into the Alice container using :

```
lxc exec alice1 bash
```

2. Go to the following directory :

```
cd programs
```

3. Compile :

```
g++ sec_server_client.cpp -lssl -lcrypto -o sc
```

4. Run :

```
./sc -c bob1
```

5. Send and receive messages to/from Bob.
6. Send `"chat_close"` to close the connection at any point of time.

On Bob's Side :

1. Login into the Bob container using :

```
lxc exec bob1 bash
```

2. Go to the following directory :

```
cd programs
```

3. Compile :

```
g++ sec_server_client.cpp -lssl -lcrypto -o sc
```

4. Run :

```
./sc -s
```

5. Send `"chat_STARTTLS_ACK"` to establish a TLS connection. Send `"chat_STARTTLS_NOT_SUPPORTED"` to have a data transfer without TLS.
6. Send and receive messages to/from Alice.
7. Send `"chat_close"` to close the connection at any point of time.

On Trudy's Side :

1. Login into the Bob container using :

```
lxc exec trud1 bash
```

2. Compile :

```
g++ /root/fake_certs/fake_certs/downgrade_task4.c++ -lssl -lcrypto -o
dg
```

3. Run :

```
./dg
```

4. MITM attacks to tamper between Alice and Bob.

To unpoison, run the following on the Container Host :

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