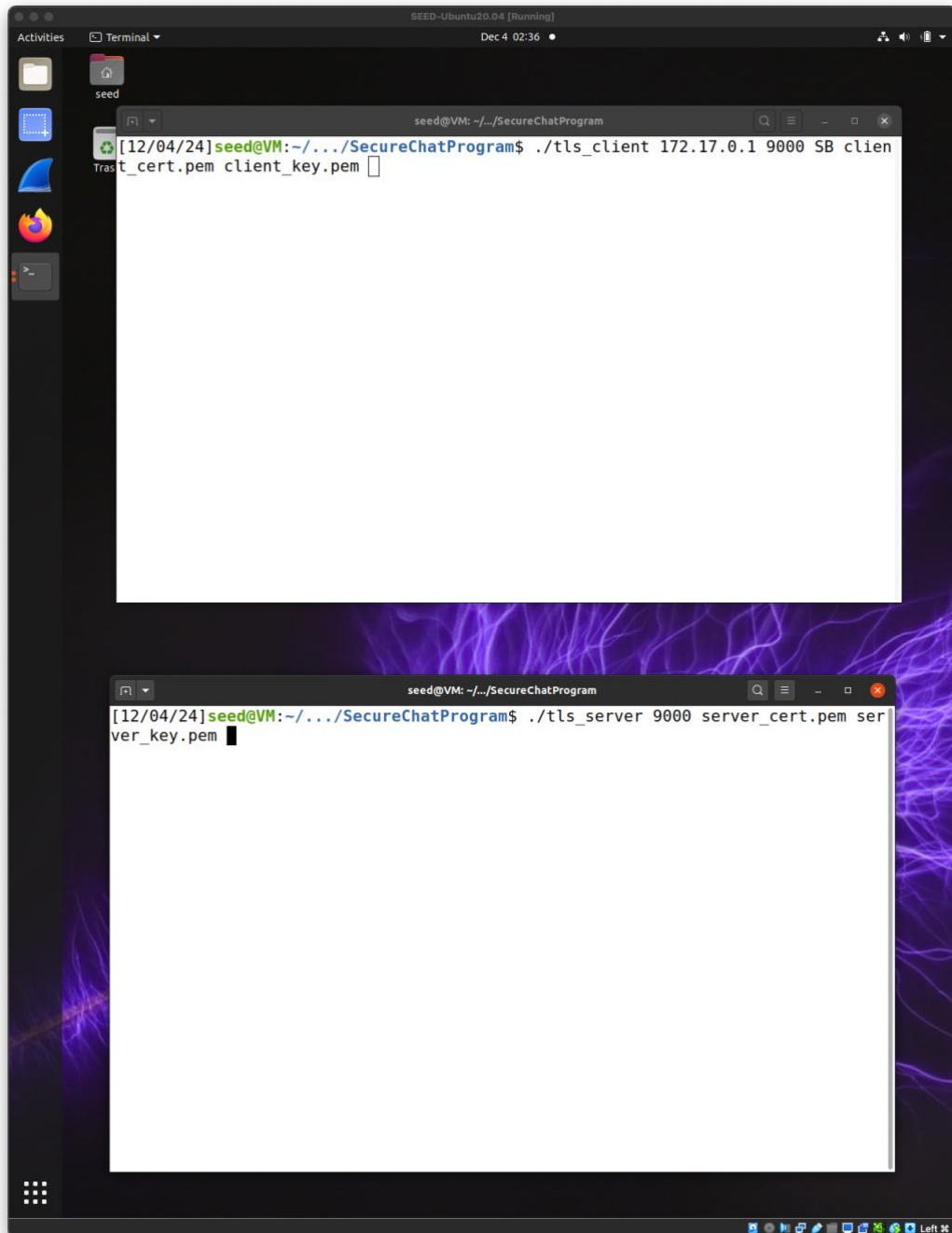


Secure Chat Program
Computer Security
Seongbin Kim 22100113

1. Run commands

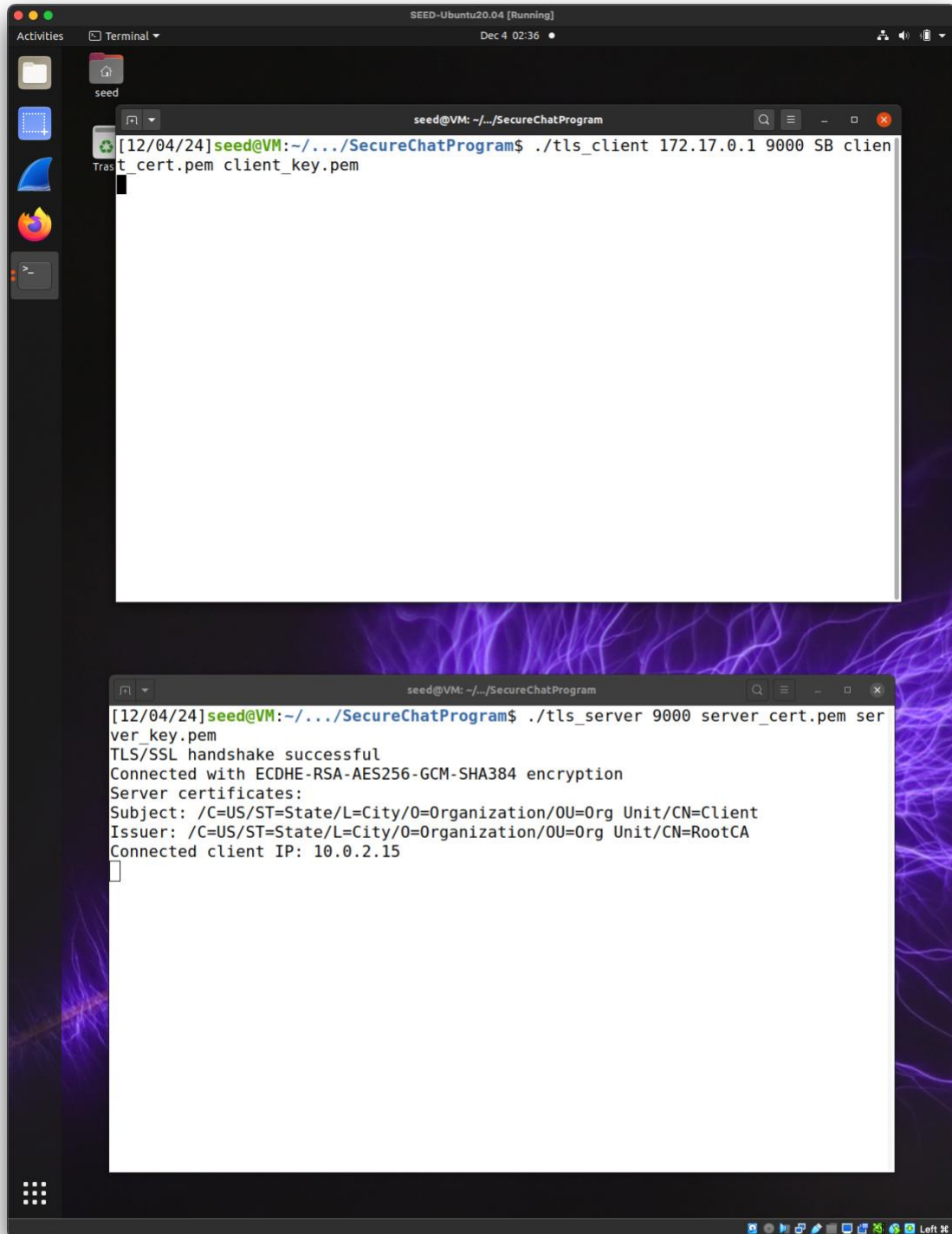


The image shows a terminal window titled "seed@VM: ~/SecureChatProgram" with a date and time of "Dec 4 02:36". The terminal displays two commands entered by the user. The first command is `./tls_client 172.17.0.1 9000 SB client_cert.pem client_key.pem`. The second command is `./tls_server 9000 server_cert.pem server_key.pem`. The terminal window is part of a desktop environment with a purple and blue abstract background. The desktop has a sidebar with icons for Activities, Home, and several applications including a file manager, a terminal, and a web browser. The terminal window is open on top of the desktop.

```
seed@VM: ~/SecureChatProgram  
[12/04/24]seed@VM:~/SecureChatProgram$ ./tls_client 172.17.0.1 9000 SB client_cert.pem client_key.pem  
[12/04/24]seed@VM:~/SecureChatProgram$ ./tls_server 9000 server_cert.pem server_key.pem
```

Shows the commands before running the program.

2. Connect



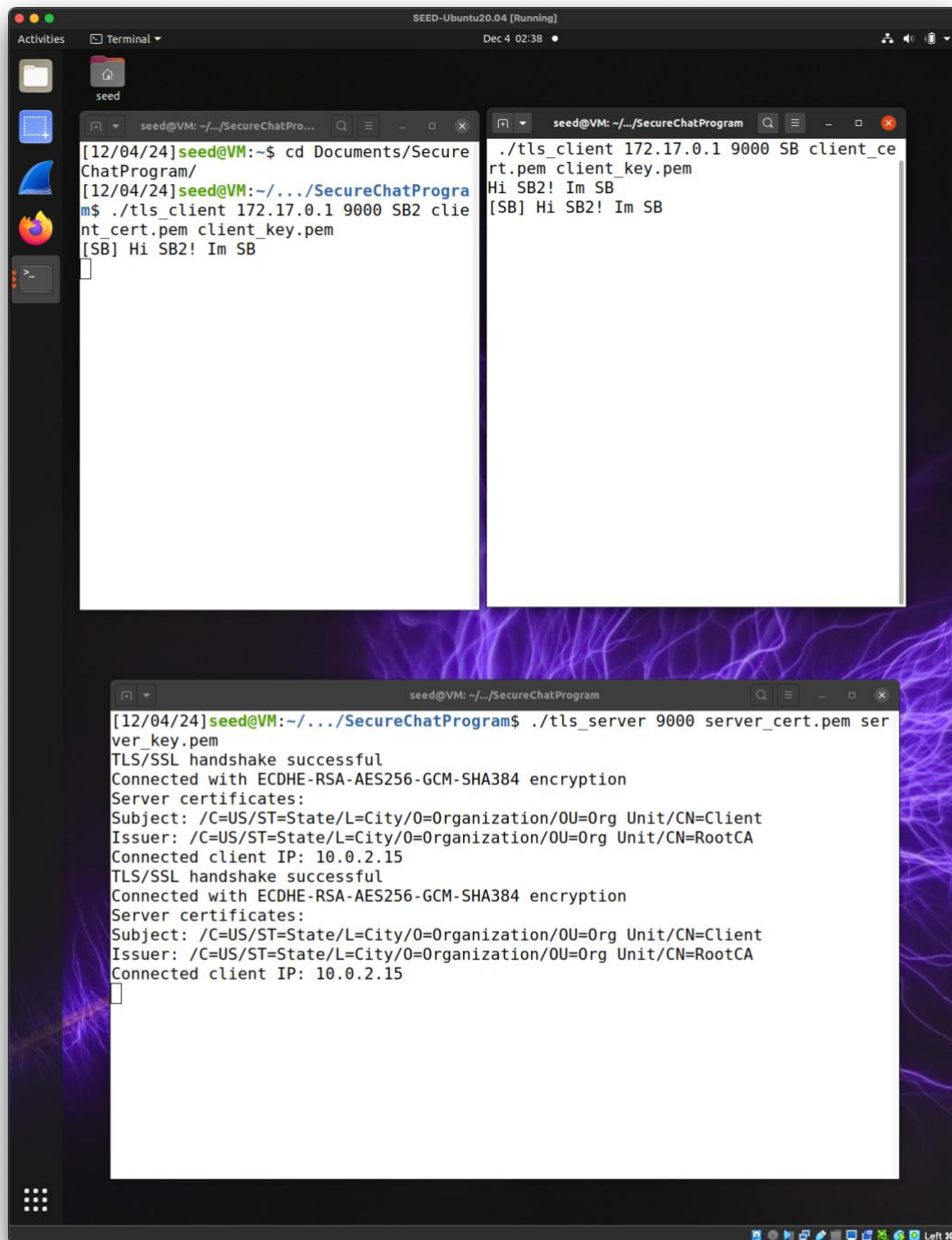
The screenshot shows a terminal window titled "seed@VM: ~/SecureChatProgram" with a date of Dec 4 02:36. The terminal displays the execution of two commands: `./tls_client 172.17.0.1 9000 SB client_cert.pem client_key.pem` and `./tls_server 9000 server_cert.pem server_key.pem`. The output of the server command indicates a successful TLS/SSL handshake with ECDHE-RSA-AES256-GCM-SHA384 encryption, lists the server certificates, and shows the connected client IP as 10.0.2.15.

```
seed@VM: ~/SecureChatProgram
[12/04/24]seed@VM:~/SecureChatProgram$ ./tls_client 172.17.0.1 9000 SB client_cert.pem client_key.pem

seed@VM: ~/SecureChatProgram
[12/04/24]seed@VM:~/SecureChatProgram$ ./tls_server 9000 server_cert.pem server_key.pem
TLS/SSL handshake successful
Connected with ECDHE-RSA-AES256-GCM-SHA384 encryption
Server certificates:
Subject: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=Client
Issuer: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=RootCA
Connected client IP: 10.0.2.15
```

Shows TLS connection is established, and certificates are verified.

3. Send simple text message

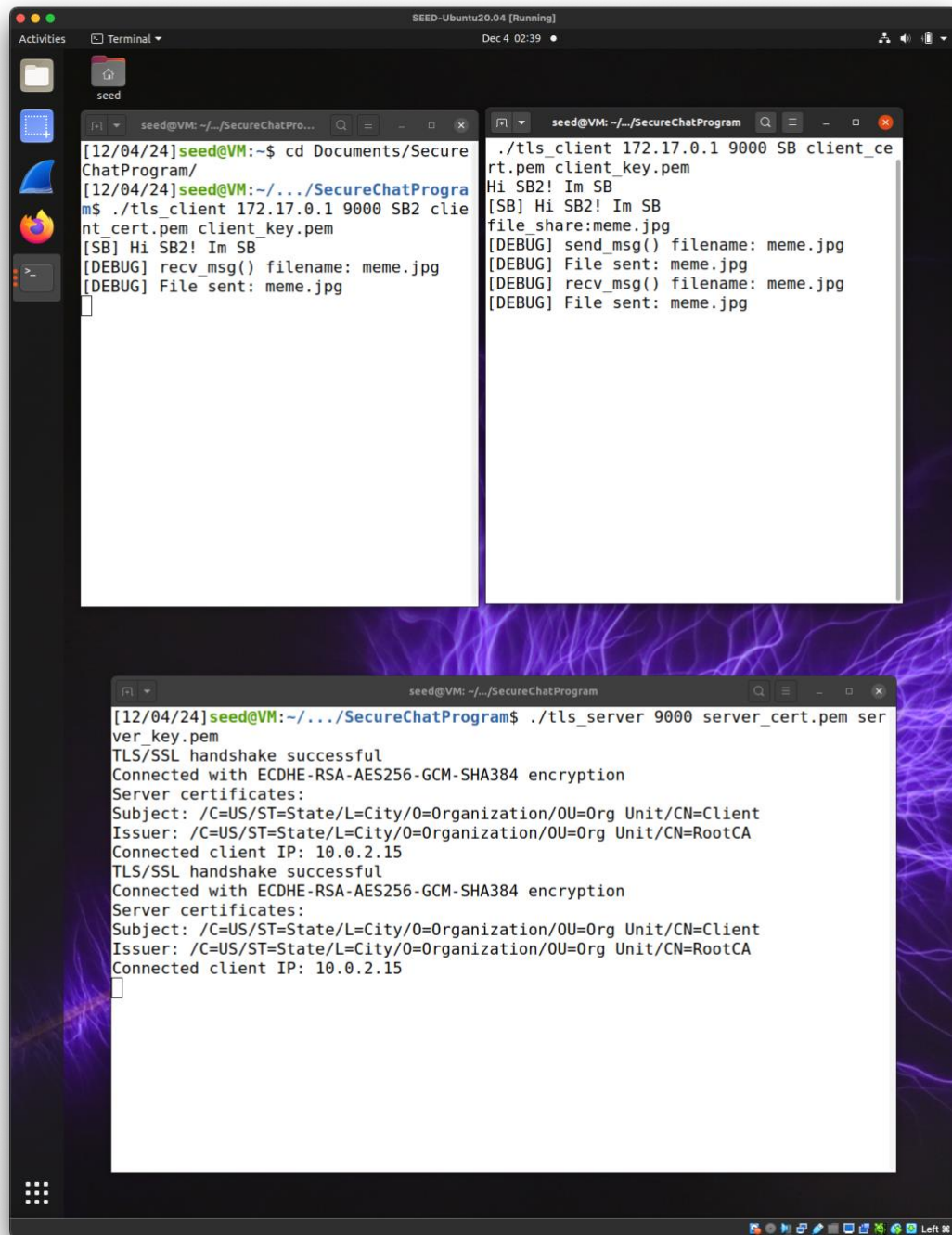


```
[12/04/24]seed@VM: ~/$ cd Documents/SecureChatProgram/
[12/04/24]seed@VM: ~/.../SecureChatProgram$ ./tls_client 172.17.0.1 9000 SB client_cert.pem client_key.pem
[SB] Hi SB2! Im SB

[12/04/24]seed@VM: ~/.../SecureChatProgram$ ./tls_server 9000 server_cert.pem server_key.pem
TLS/SSL handshake successful
Connected with ECDHE-RSA-AES256-GCM-SHA384 encryption
Server certificates:
Subject: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=Client
Issuer: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=RootCA
Connected client IP: 10.0.2.15
TLS/SSL handshake successful
Connected with ECDHE-RSA-AES256-GCM-SHA384 encryption
Server certificates:
Subject: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=Client
Issuer: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=RootCA
Connected client IP: 10.0.2.15
```

Shows when a simple text message of “Hi SB2! Im SB” is sent to the server, the server broadcasts the message to all ‘subscribing’ clients. Assuming both SB and SB2 use the same certification ‘client_cert.pem’ and key ‘client_key.pem’.

4. Send .jpg file message



```
[12/04/24]seed@VM:~$ cd Documents/SecureChatProgram/
[12/04/24]seed@VM:~/SecureChatProgram$ ./tls_client 172.17.0.1 9000 SB client_cert.pem client_key.pem
[SB] Hi SB2! Im SB
file share:meme.jpg
[DEBUG] send_msg() filename: meme.jpg
[DEBUG] File sent: meme.jpg
[DEBUG] recv_msg() filename: meme.jpg
[DEBUG] File sent: meme.jpg

[12/04/24]seed@VM:~/SecureChatProgram$ ./tls_server 9000 server_cert.pem server_key.pem
TLS/SSL handshake successful
Connected with ECDHE-RSA-AES256-GCM-SHA384 encryption
Server certificates:
Subject: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=Client
Issuer: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=RootCA
Connected client IP: 10.0.2.15
TLS/SSL handshake successful
Connected with ECDHE-RSA-AES256-GCM-SHA384 encryption
Server certificates:
Subject: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=Client
Issuer: /C=US/ST=State/L=City/O=Organization/OU=Org Unit/CN=RootCA
Connected client IP: 10.0.2.15
```

Shows when a file is sent. In this case, a .jpg file is sent. Similarly, to Step 3, this example assumes both SB and SB2 use the same certification 'client_cert.pem' and key 'client_key.pem'.