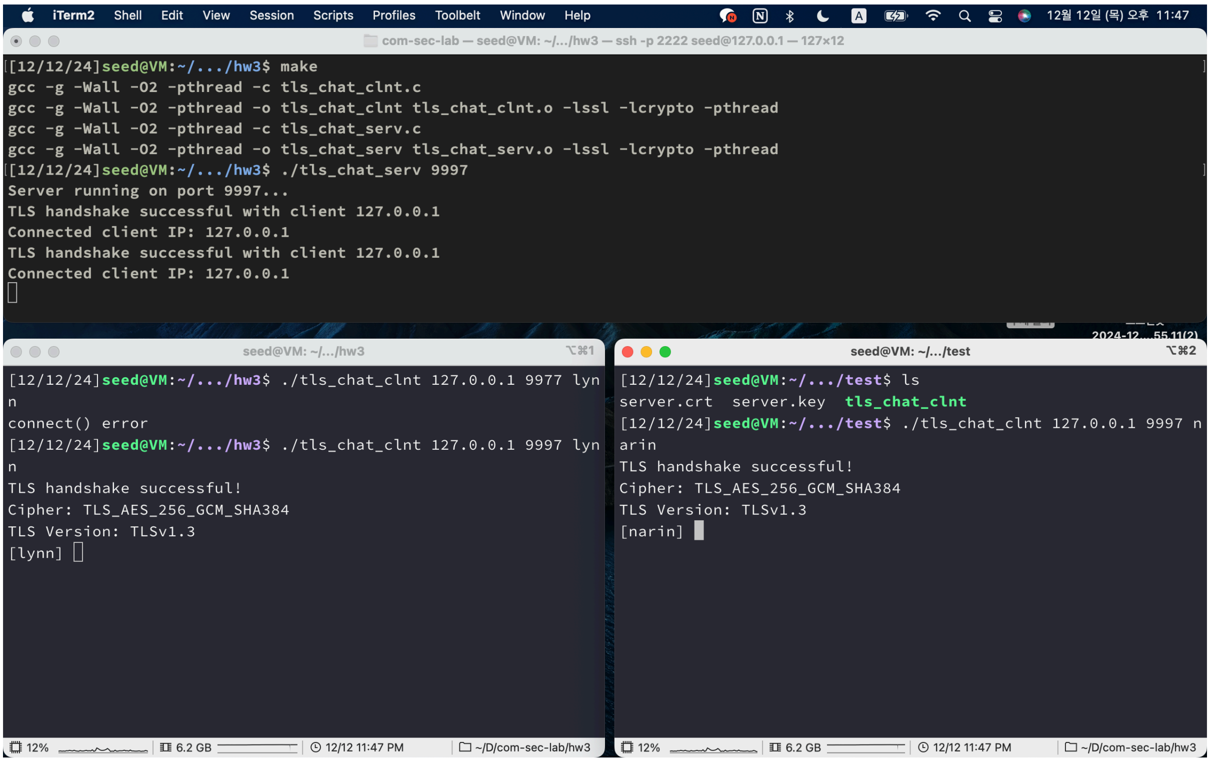
1. Connection made

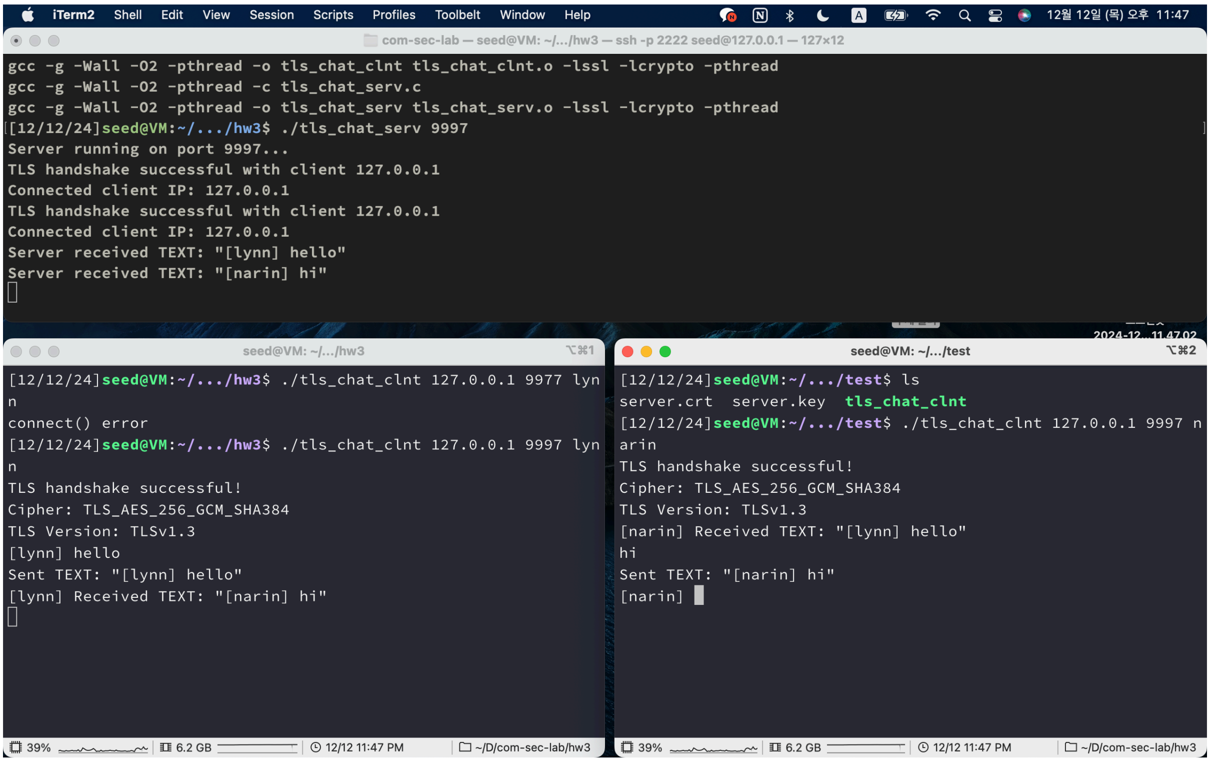


```
[12/12/24]seed@VM:~/.../hw3$ make
gcc -g -Wall -O2 -pthread -c tls_chat_clnt.c
gcc -g -Wall -O2 -pthread -o tls_chat_clnt tls_chat_clnt.o -lssl -lcrypto -pthread
gcc -g -Wall -O2 -pthread -c tls_chat_serv.c
gcc -g -Wall -O2 -pthread -o tls_chat_serv tls_chat_serv.o -lssl -lcrypto -pthread
[12/12/24]seed@VM:~/.../hw3$ ./tls_chat_serv 9997
Server running on port 9997...
TLS handshake successful with client 127.0.0.1
Connected client IP: 127.0.0.1
TLS handshake successful with client 127.0.0.1
Connected client IP: 127.0.0.1
```

```
[12/12/24]seed@VM:~/.../hw3$ ./tls_chat_clnt 127.0.0.1 9977 lyn
n
connect() error
[12/12/24]seed@VM:~/.../hw3$ ./tls_chat_clnt 127.0.0.1 9997 lyn
n
TLS handshake successful!
Cipher: TLS_AES_256_GCM_SHA384
TLS Version: TLSv1.3
[lynn]
```

```
[12/12/24]seed@VM:~/.../test$ ls
server.crt  server.key  tls_chat_clnt
[12/12/24]seed@VM:~/.../test$ ./tls_chat_clnt 127.0.0.1 9997 n
arin
TLS handshake successful!
Cipher: TLS_AES_256_GCM_SHA384
TLS Version: TLSv1.3
[narin]
```

2. Simple text messages transferred

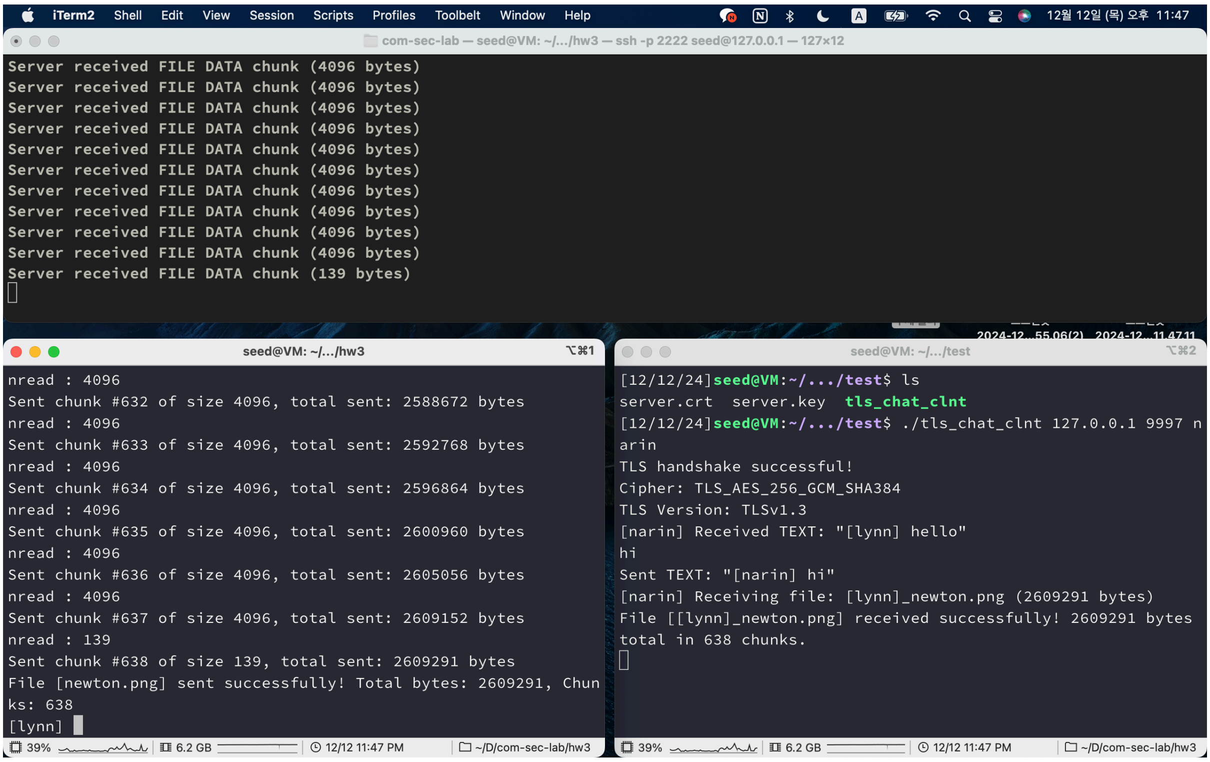


```
gcc -g -Wall -O2 -pthread -o tls_chat_clnt tls_chat_clnt.o -lssl -lcrypto -pthread
gcc -g -Wall -O2 -pthread -c tls_chat_serv.c
gcc -g -Wall -O2 -pthread -o tls_chat_serv tls_chat_serv.o -lssl -lcrypto -pthread
[12/12/24]seed@VM:~/.../hw3$ ./tls_chat_serv 9997
Server running on port 9997...
TLS handshake successful with client 127.0.0.1
Connected client IP: 127.0.0.1
TLS handshake successful with client 127.0.0.1
Connected client IP: 127.0.0.1
Server received TEXT: "[lynn] hello"
Server received TEXT: "[narin] hi"
```

```
[12/12/24]seed@VM:~/.../hw3$ ./tls_chat_clnt 127.0.0.1 9977 lyn
n
connect() error
[12/12/24]seed@VM:~/.../hw3$ ./tls_chat_clnt 127.0.0.1 9997 lyn
n
TLS handshake successful!
Cipher: TLS_AES_256_GCM_SHA384
TLS Version: TLSv1.3
[lynn] hello
Sent TEXT: "[lynn] hello"
[lynn] Received TEXT: "[narin] hi"
```

```
[12/12/24]seed@VM:~/.../test$ ls
server.crt  server.key  tls_chat_clnt
[12/12/24]seed@VM:~/.../test$ ./tls_chat_clnt 127.0.0.1 9997 n
arin
TLS handshake successful!
Cipher: TLS_AES_256_GCM_SHA384
TLS Version: TLSv1.3
[narin] Received TEXT: "[lynn] hello"
hi
Sent TEXT: "[narin] hi"
[narin]
```

3. Left side client sends “newton.png”

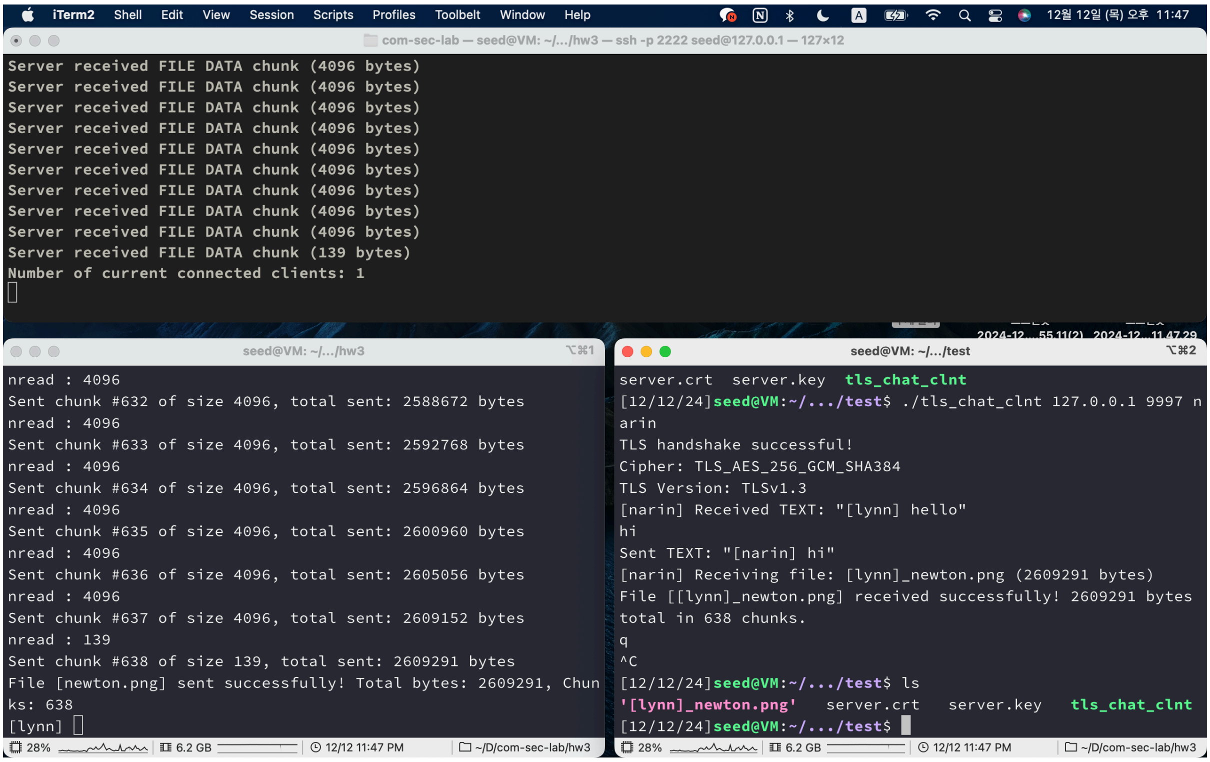

iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
12월 12일 (목) 오후 11:47
com-sec-lab — seed@VM: ~/.../hw3 — ssh -p 2222 seed@127.0.0.1 — 127×12
seed@VM: ~/.../hw3 ⌥⌘1
seed@VM: ~/.../test ⌥⌘2
39% 6.2 GB 12/12 11:47 PM ~/D/com-sec-lab/hw3

```
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (139 bytes)
```

```
nread : 4096
Sent chunk #632 of size 4096, total sent: 2588672 bytes
nread : 4096
Sent chunk #633 of size 4096, total sent: 2592768 bytes
nread : 4096
Sent chunk #634 of size 4096, total sent: 2596864 bytes
nread : 4096
Sent chunk #635 of size 4096, total sent: 2600960 bytes
nread : 4096
Sent chunk #636 of size 4096, total sent: 2605056 bytes
nread : 4096
Sent chunk #637 of size 4096, total sent: 2609152 bytes
nread : 139
Sent chunk #638 of size 139, total sent: 2609291 bytes
File [newton.png] sent successfully! Total bytes: 2609291, Chun
ks: 638
[lynn]
```

```
[12/12/24]seed@VM:~/.../test$ ls
server.crt  server.key  tls_chat_clnt
[12/12/24]seed@VM:~/.../test$ ./tls_chat_clnt 127.0.0.1 9997 n
arin
TLS handshake successful!
Cipher: TLS_AES_256_GCM_SHA384
TLS Version: TLSv1.3
[narin] Received TEXT: "[lynn] hello"
hi
Sent TEXT: "[narin] hi"
[narin] Receiving file: [lynn]_newton.png (2609291 bytes)
File [[lynn]_newton.png] received successfully! 2609291 bytes
total in 638 chunks.
```

4. Right side client received “newton.png”


iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
12월 12일 (목) 오후 11:47
com-sec-lab — seed@VM: ~/.../hw3 — ssh -p 2222 seed@127.0.0.1 — 127×12
seed@VM: ~/.../hw3 ⌥⌘1
seed@VM: ~/.../test ⌥⌘2
28% 6.2 GB 12/12 11:47 PM ~/D/com-sec-lab/hw3

```
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (4096 bytes)
Server received FILE DATA chunk (139 bytes)
Number of current connected clients: 1
```

```
nread : 4096
Sent chunk #632 of size 4096, total sent: 2588672 bytes
nread : 4096
Sent chunk #633 of size 4096, total sent: 2592768 bytes
nread : 4096
Sent chunk #634 of size 4096, total sent: 2596864 bytes
nread : 4096
Sent chunk #635 of size 4096, total sent: 2600960 bytes
nread : 4096
Sent chunk #636 of size 4096, total sent: 2605056 bytes
nread : 4096
Sent chunk #637 of size 4096, total sent: 2609152 bytes
nread : 139
Sent chunk #638 of size 139, total sent: 2609291 bytes
File [newton.png] sent successfully! Total bytes: 2609291, Chun
ks: 638
[lynn]
```

```
server.crt  server.key  tls_chat_clnt
[12/12/24]seed@VM:~/.../test$ ./tls_chat_clnt 127.0.0.1 9997 n
arin
TLS handshake successful!
Cipher: TLS_AES_256_GCM_SHA384
TLS Version: TLSv1.3
[narin] Received TEXT: "[lynn] hello"
hi
Sent TEXT: "[narin] hi"
[narin] Receiving file: [lynn]_newton.png (2609291 bytes)
File [[lynn]_newton.png] received successfully! 2609291 bytes
total in 638 chunks.
q
^C
[12/12/24]seed@VM:~/.../test$ ls
'[lynn]_newton.png'   server.crt   server.key   tls_chat_clnt
[12/12/24]seed@VM:~/.../test$
```