Source Code:

Server.py

```
import socket, ssl
HOST, PORT = '127.0.0.1', 443
def handle(conn):
    print(conn.recv())
    conn.write(b'HTTP/1.1 200 OK\n\n%s' % conn.getpeername()[0].encode())

def main():
    sock = socket.socket()
    sock.bind((HOST, PORT))
    sock.listen(5)
    context = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
    context.load_cert_chain('cert.pem','cert.key' )
    context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1
    context.set_ciphers('EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH')
    while True:
        conn = None
        ssock, addr = sock.accept()
        try:
            conn = context.wrap_socket(ssock, server_side=True)
            handle(conn)
        except ssl.SSLError as e:
            print(e)
        finally:
            if conn:
                conn.close()
if __name__ == '__main__':
    main()
```

Client.py

```
import socket, ssl

HOST, PORT, server_sni_hostname = '127.0.0.1', 443, 'Weijian Xiong'
server_cert = 'cert.pem'


def handle(conn):
        conn.write(b'GET / HTTP/1.1\n')
        print(conn.recv().decode())
```

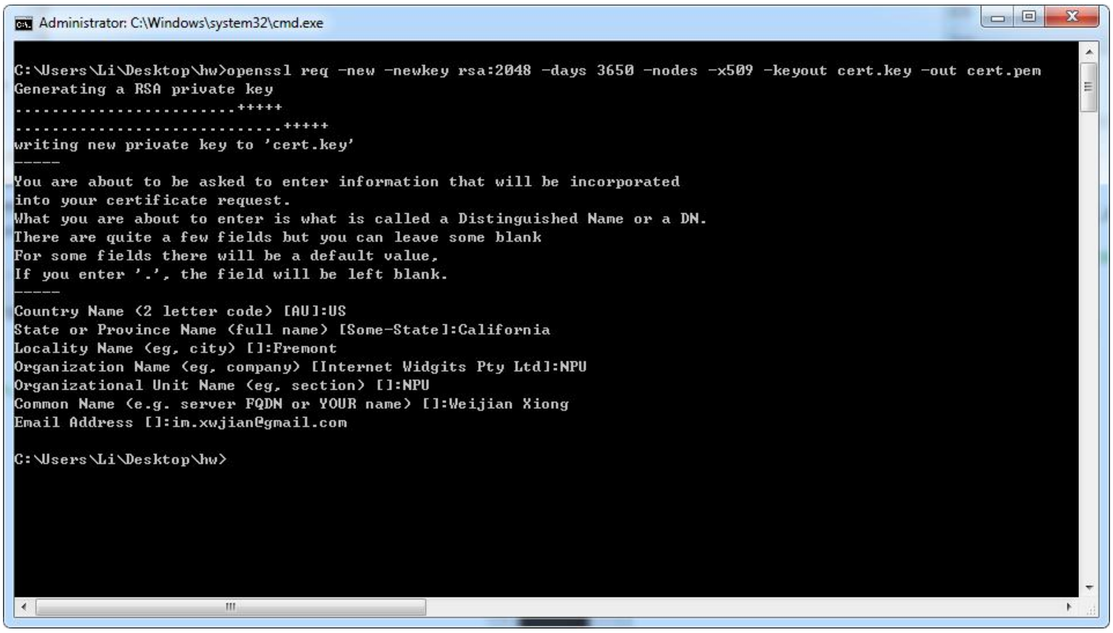
```
    print('client successfully connected!')

def main():

    context = ssl.create_default_context(ssl.Purpose.SERVER_AUTH, cafile=server_cert)
    context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    conn = context.wrap_socket(sock,server_side=False, server_hostname =
server_sni_hostname)
    try:
        conn.connect((HOST, PORT))
        handle(conn)
    finally:
        conn.close()

if __name__ == '__main__':
    main()
```

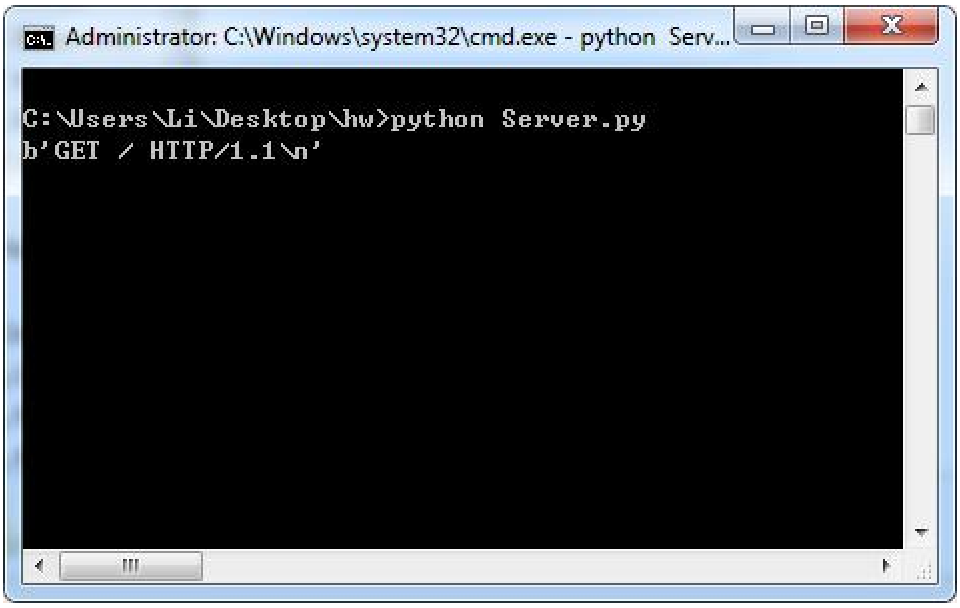
Generate certificate and key:



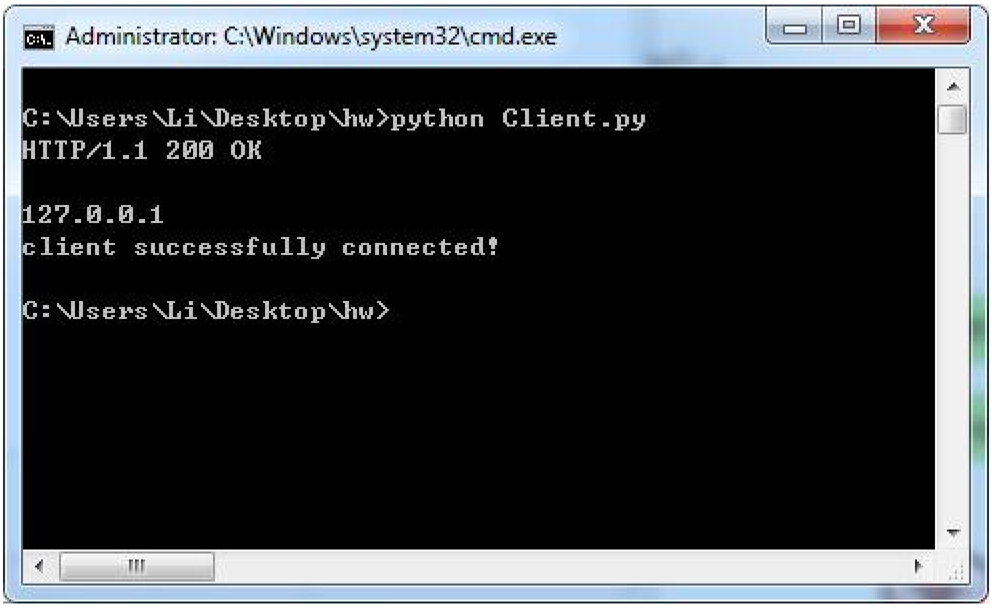
```
C:\Users\Li\Desktop\hw>openssl req -new -newkey rsa:2048 -days 3650 -nodes -x509 -keyout cert.key -out cert.pem
Generating a RSA private key
........................+++++
.............................+++++
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Fremont
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NPU
Organizational Unit Name (eg, section) []:NPU
Common Name (e.g. server FQDN or YOUR name) []:Weijian Xiong
Email Address []:im.xwjian@gmail.com

C:\Users\Li\Desktop\hw>
```

Run server and client:



```
C:\Users\Li\Desktop\hw>python Server.py
b'GET / HTTP/1.1\n'
```



```
C:\Users\Li\Desktop\hw>python Client.py
HTTP/1.1 200 OK

127.0.0.1
client successfully connected!

C:\Users\Li\Desktop\hw>
```