**Running handshake.py**

A computer screen shot of a computer code

Description automatically generated

**Q1.** What is the cipher used between the client and the server?

The cypher used is TLS-AES-128-GCM-SHA256, TLSv1.3, 128.

**Q2.** What is the server's public certificate used for after the client verifies the server's identity and its public key?

After the client verifies the server's identity and its public key using the server's public certificate, the certificate is primarily used for encryption and authentication purposes during the TLS handshake. Once the server's identity is verified, its public key is used by the client to establish a secure communication channel. This includes encrypting data sent from the client to the server and decrypting data received from the server. Additionally, the server's public certificate helps ensure the integrity and authenticity of the communication by allowing the client to verify that it is indeed communicating with the intended server and not an impostor.

**Explain the purpose of cadir = ’/etc/ssl/certs’:**

In the handshake.py code, cadir is set to '/etc/ssl/certs', storing the directory where trusted CA certificates are kept. These certificates are used for verifying the authenticity of the server's certificate during the TLS handshake process.

**Using ifconfig:**

A screenshot of a computer screen

Description automatically generated

**Running handshake.py:**

A screenshot of a computer

Description automatically generated

**We can clearly see the handshake process, with the ‘Client Hello’ , ‘Server hello’, etc.. in the info column:**

A screenshot of a computer

Description automatically generated

**Proxy container is seeing the communication:**

A screenshot of a computer

Description automatically generated