**Applied Cryptography (UE20CS314)**

**TLS Lab**

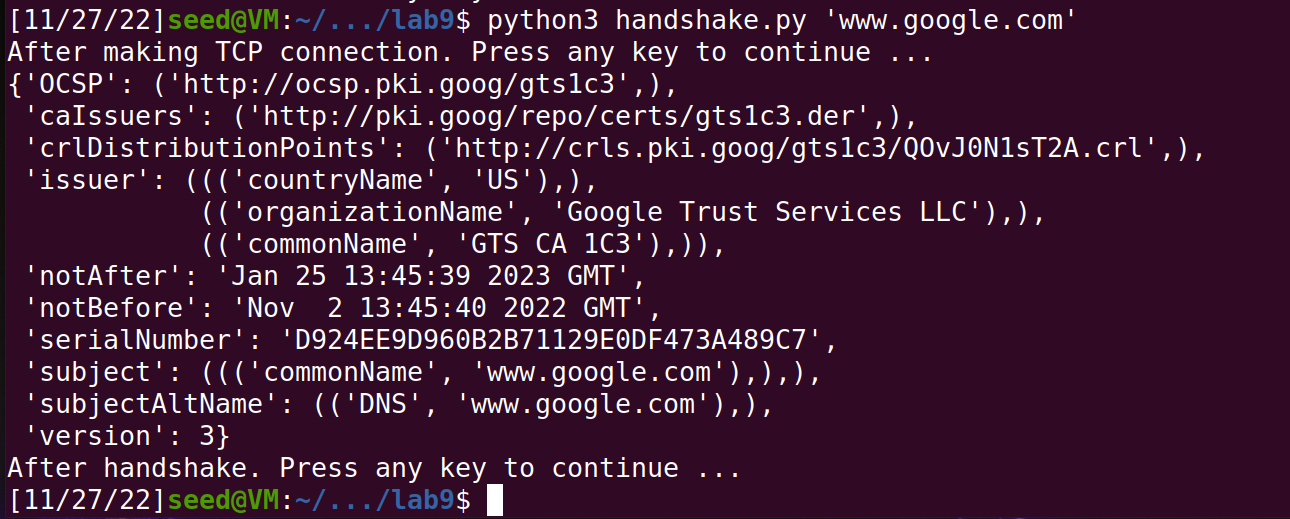
Name: Vishwa Mehul Mehta

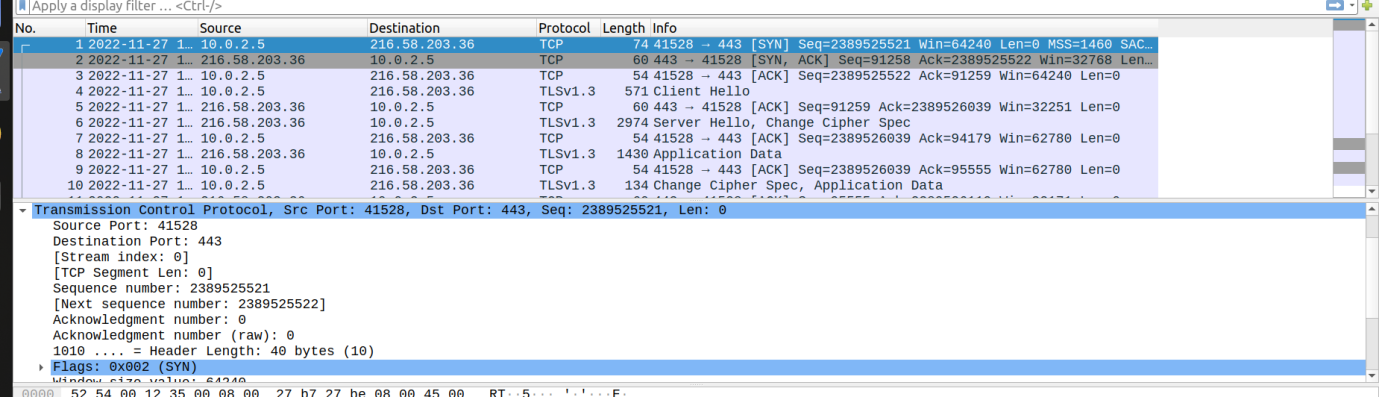
SRN: PES2UG20CS389

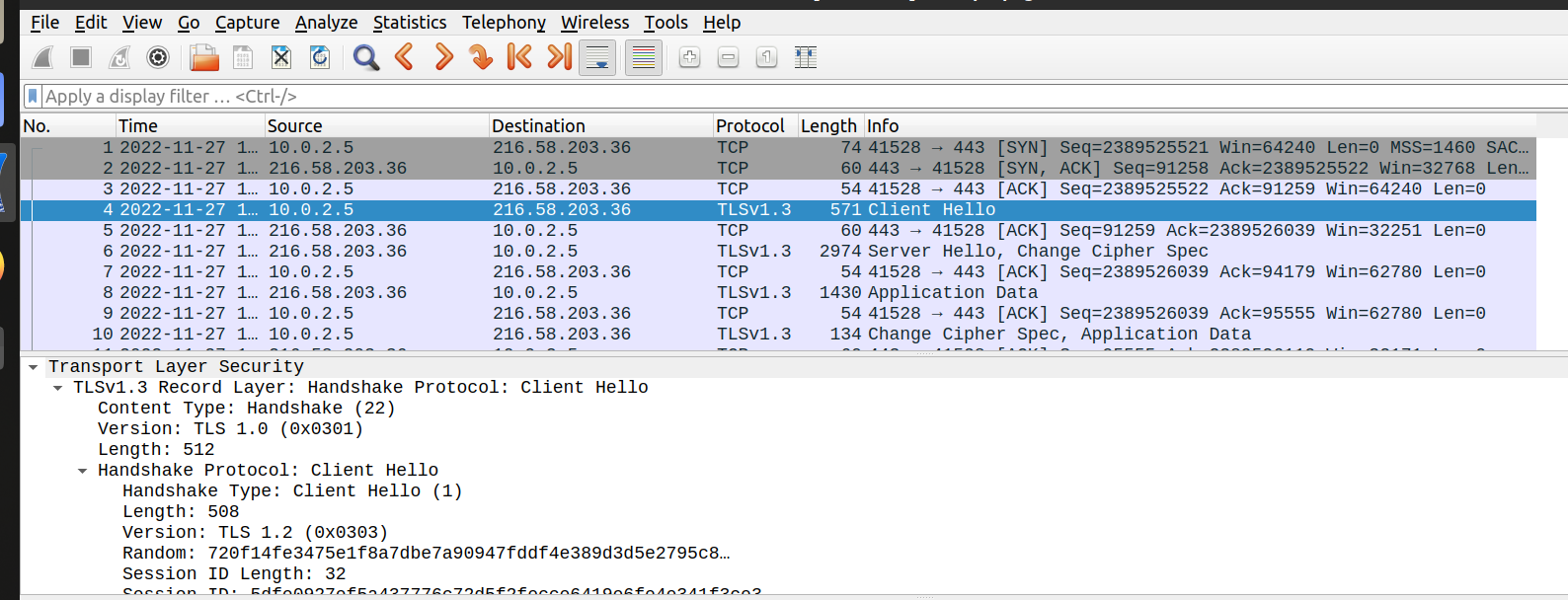
Section: F

Task 1.a:

Screenshot:







Observation:

* Cipher used between client and server is AES.
* /etc/ss/certs is used to obtain the CA certificates to allow SSL-based applications to check for the authenticity of SSL connections.
* The TCP handshake is triggered first with a SYN request to the server and the TLS handshake is triggered only after the TCP handshake is complete and follows the handshake type “Client Hello”

Task 1.b:

Screenshot:

Observation:

Task 2:

Screenshot:

Observation:

Task 3:

Screenshot:

Without key:

Observation:

Task 4:

Screenshot:

Observation: