SCREENSHOT OF SERVER CERTIFICATE:

[11/04/23]seed@VM:~/.../certS$ sudo su
root@VM:/home/seed/Downloads/Lab 6/TLS_CS/volumes/certS# openssl x509 -in demo_ca.crt -text -noout

```
[11/04/23]seed@VM:~/.../certS$ sudo su
root@VM:/home/seed/Downloads/Lab 6/TLS_CS/volumes/certS# openssl x509 -in demo_ca.crt
-text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4b:b2:ac:25:e0:f9:58:8f:6c:dc:ae:dc:27:09:fa:ea:41:b2:63:30
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CA, ST = Ontario, L = Windsor, O = University of Windsor, OU = Edu
cation, CN = client1-10.9.0.5, emailAddress = lnu8@uwindsor.ca
        Validity
            Not Before: Nov  4 08:19:19 2023 GMT
            Not After : Nov  3 08:19:19 2024 GMT
        Subject: C = CA, ST = Ontario, L = Windsor, O = University of Windsor, OU = Ed
ucation, CN = client1-10.9.0.5, emailAddress = lnu8@uwindsor.ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bb:2c:47:e7:c2:8b:01:11:79:aa:83:fc:80:a5:
                    64:e1:f8:62:b0:ff:ea:11:9c:89:46:f7:86:59:b9:
                    26:b9:fb:5b:86:61:48:73:57:ea:be:a3:b6:2d:ce:
                    7f:e2:a6:ba:3d:d6:11:64:42:98:62:89:83:6b:11:
                    a9:77:ac:4f:51:0e:d9:cb:d1:0b:07:6f:bf:5a:28:
                    26:5b:02:b1:8a:a9:05:d3:98:4b:97:be:67:b9:79:
                    cb:73:e8:14:fe:ff:9c:28:05:67:0b:48:1a:33:70:
                    8e:7e:f9:81:fd:6e:f7:d8:cb:b3:86:83:77:bd:3d:
                    75:fb:1c:3e:be:eb:90:f8:cf:f2:55:55:df:ee:c2:
                    5b:6b:ef:87:60:10:0d:ea:59:32:74:e6:4c:73:07:
                    fe:22:94:be:fa:26:88:87:d0:c9:d7:64:b1:52:09:
                    8b:98:95:c2:9b:a0:d9:fc:df:41:67:df:62:7b:0a:
                    3d:95:88:f1:26:47:18:9c:4b:f7:5d:cf:b4:0d:1c:
                    ef:7d:42:5b:61:29:f3:ad:bc:f0:df:64:e0:a9:97:
                    80:50:1a:57:86:1c:30:79:71:c2:43:bf:a5:5d:7c:
                    5e:93:a4:17:ca:d4:f0:a0:e0:6a:8a:ab:73:40:7b:
                    de:42:ee:0e:4d:66:ef:35:a3:61:52:a0:b1:b5:99:
                    26:73
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

```
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                92:DF:1B:0D:34:90:AF:9A:2A:B0:C1:A5:E1:A0:4E:D6:AA:5C:C0:45
            X509v3 Authority Key Identifier:
                keyid:92:DF:1B:0D:34:90:AF:9A:2A:B0:C1:A5:E1:A0:4E:D6:AA:5C:C0:45

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         19:30:58:f7:e5:c7:7c:fb:b8:14:f9:06:c4:5f:b7:eb:50:88:
         5e:26:71:73:88:9d:7f:29:3c:65:d7:05:70:bc:ef:0b:7c:37:
         22:31:42:f5:53:d9:79:4a:0b:df:cd:10:34:47:86:58:ca:86:
         b4:13:54:66:90:69:37:d0:b4:c5:9d:db:48:32:a1:d7:8d:16:
         9b:31:38:26:c0:d0:73:61:aa:d1:be:90:ae:79:49:da:90:19:
         e5:f5:dc:b5:43:b7:67:8e:af:49:9a:71:b8:94:d6:28:46:a7:
         0b:c9:42:a5:01:cf:e8:ec:6c:23:6c:42:95:64:be:57:b0:5c:
         1d:ca:08:ca:bf:ef:45:f4:27:dd:89:83:22:e3:58:e2:2d:21:
         b1:e8:ae:b7:b3:31:8a:02:06:5c:a8:a9:54:1b:df:24:f9:f0:
         ac:95:e0:51:bd:2a:7e:67:93:c6:eb:c6:70:79:e2:23:eb:41:
         d6:b9:6c:55:7f:a1:30:e9:89:f1:2c:08:ba:65:74:40:20:2e:
         8d:12:28:df:a7:9c:46:ae:af:ca:ea:b2:a5:73:e0:f4:9c:0b:
         70:28:58:ff:3a:a8:cc:48:62:87:97:7c:65:53:3d:c9:e2:da:
         24:fa:b4:99:0b:56:b0:fe:92:58:11:bc:6d:db:d7:7e:c6:ad:
         c8:c3:df:6a
root@VM:/home/seed/Downloads/Lab 6/TLS_CS/volumes/certS#
```