CS 201P Project #8— Public-Key Infrastructure (PKI) Lab

Name: Shikhir Goel

UCI ID: shikhirg@uci.edu

Computing/Cloud Platform Chosen: Google Cloud platform

Task 1: Becoming a Certificate Authority (CA)

Using OpenSSL's default configuration to create certificates.

The following provides us with the configuration setup for creating and issuing certificates:

```
seed@shikhirsvm: ~/security
File  Edit  View  Search  Terminal  Help
seed@shikhirsvm:~/security$ cp /usr/lib/ssl/openssl.cnf
cp: missing destination file operand after '/usr/lib/ssl/openssl.cnf'
Try 'cp --help' for more information.
seed@shikhirsvm:~/security$ cp /usr/lib/ssl/openssl.cnf openssl.cnf
seed@shikhirsvm:~/security$ cd Labsetup
seed@shikhirsvm:~/security/Labsetup$ ls
docker-compose.yml  image_www  mysql_data  volumes
seed@shikhirsvm:~/security/Labsetup$ ls
docker-compose.yml  image_www  mysql_data  volumes
seed@shikhirsvm:~/security/Labsetup$ cd ..
seed@shikhirsvm:~/security$ ls
Labsetup  Labsetup.zip  ca.key  openssl.cnf
seed@shikhirsvm:~/security$ mkdir demoCA
seed@shikhirsvm:~/security$ cd demoCA
seed@shikhirsvm:~/security/demoCA$ mkdir certs crl newcerts
seed@shikhirsvm:~/security/demoCA$ touch index.txt serial
seed@shikhirsvm:~/security/demoCA$ echo 1000 > serial
seed@shikhirsvm:~/security/demoCA$ ls
certs  crl  index.txt  newcerts  serial
seed@shikhirsvm:~/security/demoCA$ cd ..
seed@shikhirsvm:~/security$ ls
```

Uncommenting copy_extensions = copy

```
####################################################################
[ CA_default ]

dir             = ./demoCA              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
unique_subject  = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key

x509_extensions = usr_cert              # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options

 Extension copying option: use with caution.
 copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
```

Adding www.goel2020.com with the IP 10.9.0.80

Generating a self-signed certificate for our CA

It shall serve as the root certificate as follows:

```
seed@shikhirsvm: ~/security/project8/Labsetup
File  Edit  View  Search  Terminal  Help
seed@shikhirsvm:~/security/project8/Labsetup$ openssl req -x509 -newkey rsa:4096
 -sha256 -days 3650 -keyout ca.key -out ca.crt
Generating a RSA private key
..................................++++
.......................................................++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) []:Irvine
Organization Name (eg, company) [Internet Widgits Pty Ltd]:turtlepop
Organizational Unit Name (eg, section) []:tents
Common Name (e.g. server FQDN or YOUR name) []:wendet
Email Address []:fornals@gmail.com
seed@shikhirsvm:~/security/project8/Labsetup$
```

We can see entered information. The output is stored in two files: ca.key and ca.crt.

The file ca.key has the CA's private key and ca.crt has the public-key certificate.

Using the following command, we display the content of ca.crt:

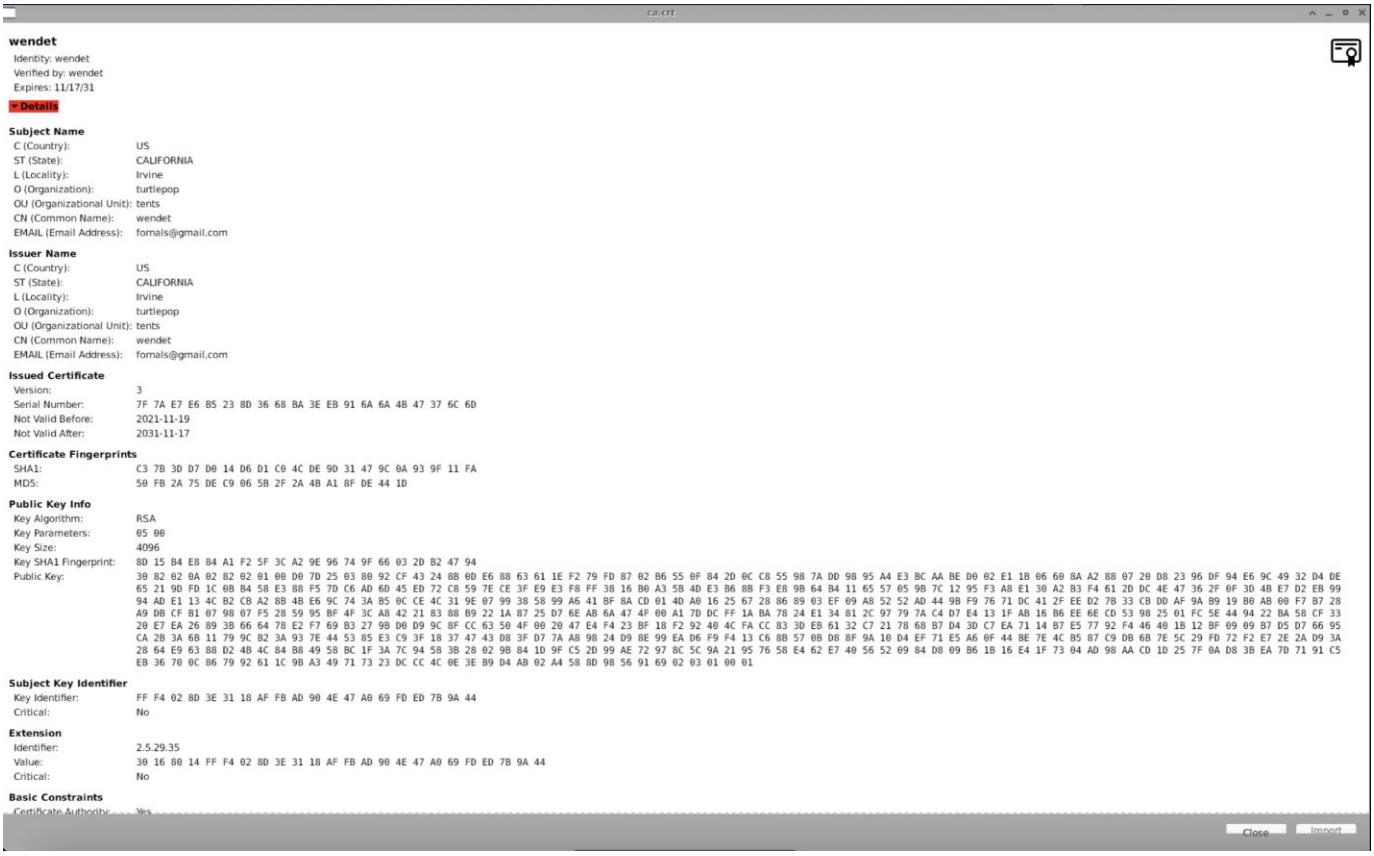
```
seed@shikhirsvm:~/security/project8/Labsetup$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7f:7a:e7:e6:b5:23:8d:36:68:ba:3e:eb:91:6a:6a:4b:47:37:6c:6d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CALIFORNIA, L = Irvine, O = turtlepop, OU = tents, CN = wendet, emailAddress = fornals@gmail.com
        Validity
            Not Before: Nov 19 18:41:48 2021 GMT
            Not After : Nov 17 18:41:48 2031 GMT
        Subject: C = US, ST = CALIFORNIA, L = Irvine, O = turtlepop, OU = tents, CN = wendet, emailAddress = fornals@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:d0:7d:25:03:80:92:cf:43:24:8b:0d:e6:88:63:
                    61:1e:f2:79:fd:87:02:b6:55:0f:84:2d:0c:c8:55:
                    98:7a:dd:98:95:a4:e3:bc:aa:be:d0:02:e1:1b:06:
                    60:8a:a2:88:07:20:d8:23:96:df:94:e6:9c:49:32:
                    d4:de:65:21:9d:fd:1c:0b:b4:58:e3:88:f5:7d:c6:
                    ad:6d:45:ed:72:c8:59:7e:ce:3f:e9:e3:f8:ff:38:
                    16:b0:a3:5b:4d:e3:b6:8b:f3:e8:9b:64:b4:11:65:
                    57:05:9b:7c:12:95:f3:a8:e1:30:a2:b3:f4:61:2d:
                    dc:4e:47:36:2f:0f:3d:4b:e7:d2:eb:99:94:ad:e1:
                    13:4c:b2:cb:a2:8b:4b:e6:9c:74:3a:b5:0c:ce:4c:
                    31:9e:07:99:38:58:99:a6:41:bf:8a:cd:01:4d:a0:
                    16:25:67:28:86:89:03:ef:09:a8:52:52:ad:44:9b:
                    f9:76:71:dc:41:2f:ee:d2:7b:33:cb:dd:af:9a:b9:
                    19:b0:ab:00:f7:b7:28:a9:db:cf:b1:07:98:07:f5:
                    28:59:95:bf:4f:3c:a8:42:21:83:88:b9:22:1a:87:
                    25:d7:6e:ab:6a:47:4f:00:a1:7d:dc:ff:1a:ba:78:
                    24:e1:34:81:2c:97:79:7a:c4:d7:e4:13:1f:ab:16:
                    b6:ee:6e:cd:53:98:25:01:fc:5e:44:94:22:ba:58:
                    cf:33:20:e7:ea:26:89:3b:66:64:78:e2:f7:69:b3:
                    27:9b:d0:d9:9c:8f:cc:63:50:4f:00:20:47:e4:f4:
                    23:bf:18:f2:92:40:4c:fa:cc:83:3d:eb:61:32:c7:
                    21:78:68:b7:d4:3d:c7:ea:71:14:b7:e5:77:92:f4:
                    46:40:1b:12:bf:09:09:b7:d5:d7:66:95:ca:2b:3a:
                    6b:11:79:9c:b2:3a:93:7e:44:53:85:e3:c9:3f:18:
                    37:47:43:d8:3f:d7:7a:a8:98:24:d9:8e:99:ea:d6:
                    f9:f4:13:c6:8b:57:0b:d8:8f:9a:10:d4:ef:71:e5:
                    a6:0f:44:be:7e:4c:b5:87:c9:db:6b:7e:5c:29:fd:
                    72:f2:e7:2e:2a:d9:3a:28:64:e9:63:88:d2:4b:4c:
                    84:b8:49:58:bc:1f:3a:7c:94:58:3b:28:02:9b:84:
                    1d:9f:c5:2d:99:ae:72:97:8c:5c:9a:21:95:76:58:
                    e4:62:e7:40:56:52:09:84:d8:09:b6:1b:16:e4:1f:
                    73:04:ad:98:aa:cd:1d:25:7f:0a:d8:3b:ea:7d:71:
                    91:c5:eb:36:70:0c:86:79:92:61:1c:9b:a3:49:71:
                    73:23:dc:cc:4c:0e:3e:b9:d4:ab:02:a4:58:8d:98:
                    56:91:69
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                FF:F4:02:8D:3E:31:18:AF:FB:AD:90:4E:47:A0:69:FD:ED:7B:9A:44
            X509v3 Authority Key Identifier:
                keyid:FF:F4:02:8D:3E:31:18:AF:FB:AD:90:4E:47:A0:69:FD:ED:7B:9A:44

            X509v3 Basic Constraints: critical
```

Using the following command, we are supplied the content of ca.key:

```
seed@shikhirsvm:~/security/project8/Labsetup$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:d0:7d:25:03:80:92:cf:43:24:8b:0d:e6:88:63:
    61:1e:f2:79:fd:87:02:b6:55:0f:84:2d:0c:c8:55:
    98:7a:dd:98:95:a4:e3:bc:aa:be:d0:02:e1:1b:06:
    60:8a:a2:88:07:20:d8:23:96:df:94:e6:9c:49:32:
    d4:de:65:21:9d:fd:1c:0b:b4:58:e3:88:f5:7d:c6:
    ad:6d:45:ed:72:c8:59:7e:ce:3f:e9:e3:f8:ff:38:
    16:b0:a3:5b:4d:e3:b6:8b:f3:e8:9b:64:b4:11:65:
    57:05:9b:7c:12:95:f3:a8:e1:30:a2:b3:f4:61:2d:
    dc:4e:47:36:2f:0f:3d:4b:e7:d2:eb:99:94:ad:e1:
    13:4c:b2:cb:a2:8b:4b:e6:9c:74:3a:b5:0c:ce:4c:
    31:9e:07:99:38:58:99:a6:41:bf:8a:cd:01:4d:a0:
    16:25:67:28:86:89:03:ef:09:a8:52:52:ad:44:9b:
    f9:76:71:dc:41:2f:ee:d2:7b:33:cb:dd:af:9a:b9:
    19:b0:ab:00:f7:b7:28:a9:db:cf:b1:07:98:07:f5:
    28:59:95:bf:4f:3c:a8:42:21:83:88:b9:22:1a:87:
    25:d7:6e:ab:6a:47:4f:00:a1:7d:dc:ff:1a:ba:78:
    24:e1:34:81:2c:97:79:7a:c4:d7:e4:13:1f:ab:16:
    b6:ee:6e:cd:53:98:25:01:fc:5e:44:94:22:ba:58:
    cf:33:20:e7:ea:26:89:3b:66:64:78:e2:f7:69:b3:
    27:9b:d0:d9:9c:8f:cc:63:50:4f:00:20:47:e4:f4:
    23:bf:18:f2:92:40:4c:fa:cc:83:3d:eb:61:32:c7:
    21:78:68:b7:d4:3d:c7:ea:71:14:b7:e5:77:92:f4:
    46:40:1b:12:bf:09:09:b7:d5:d7:66:95:ca:2b:3a:
    6b:11:79:9c:b2:3a:93:7e:44:53:85:e3:c9:3f:18:
    37:47:43:d8:3f:d7:7a:a8:98:24:d9:8e:99:ea:d6:
    f9:f4:13:c6:8b:57:0b:d8:8f:9a:10:d4:ef:71:e5:
    a6:0f:44:be:7e:4c:b5:87:c9:db:6b:7e:5c:29:fd:
    72:f2:e7:2e:2a:d9:3a:28:64:e9:63:88:d2:4b:4c:
    84:b8:49:58:bc:1f:3a:7c:94:58:3b:28:02:9b:84:
    1d:9f:c5:2d:99:ae:72:97:8c:5c:9a:21:95:76:58:
    e4:62:e7:40:56:52:09:84:d8:09:b6:1b:16:e4:1f:
    73:04:ad:98:aa:cd:1d:25:7f:0a:d8:3b:ea:7d:71:
    91:c5:eb:36:70:0c:86:79:92:61:1c:9b:a3:49:71:
    73:23:dc:cc:4c:0e:3e:b9:d4:ab:02:a4:58:8d:98:
    56:91:69
publicExponent: 65537 (0x10001)
privateExponent:
    00:84:b9:76:6b:c1:59:34:9a:e0:d3:a9:38:be:50:
    cd:ce:3e:bc:cc:5a:3b:ae:c9:7d:c4:3e:4d:a9:e7:
    5b:d7:b3:e4:64:37:81:47:65:47:6d:f2:b7:4d:56:
    04:f5:9c:bc:8e:15:29:a3:96:73:a5:3e:1d:f6:37:
    66:ee:61:61:42:4b:94:a4:1a:de:8f:93:6b:fc:f3:
    13:0a:c2:7e:84:18:e9:68:61:72:ac:ba:15:94:9c:
    27:4d:b1:e0:f9:37:e2:c9:3b:b0:33:e4:ab:01:7c:
    0b:27:25:b1:99:bf:5e:4b:7f:78:4f:cb:d1:e2:5f:
    a8:a5:28:8e:64:ed:05:af:a1:d8:53:66:05:11:a0:
    7c:81:d2:3c:f2:b0:4c:d4:75:7b:44:b8:67:7b:99:
    63:e8:df:9b:7a:14:65:54:42:fc:e6:26:d6:12:8d:
    bc:2b:79:7d:82:10:0d:b2:09:ea:de:e5:85:2a:6d:
    45:25:53:1c:cd:5e:ef:61:8d:4f:0f:14:84:ab:31:
    f5:19:d3:f3:1c:bf:bc:22:4e:2d:ec:dc:11:bb:d7:
    25:25:ca:bf:ec:78:88:00:f9:86:db:ee:47:b8:ad:
    9a:b8:87:da:96:20:e9:39:54:95:64:af:fe:5b:01:
    0b:31:57:14:78:c7:c1:6d:17:8c:fc:c3:f3:e0:1d:
    e8:bb:c1:0d:df:57:b4:99:d6:c1:49:fd:13:f2:82:
    26:b4:b6:9a:64:23:0a:a2:e0:63:43:6d:85:b2:4c:
    08:84:1b:55:81:94:50:9f:37:b9:0c:33:3b:50:f3:
```

```
seed@shikhirsvm: ~/security/project8/Labsetup
File  Edit  View  Search  Terminal  Help
    fa:21:ed:e2:be:e2:23:6a:1c:53:09:d1:ed:e4:b6:
    87:39:3f:f7:af:20:0a:86:bf:b2:1c:f6:87:42:fe:
    a3:31:40:a8:14:92:d8:e9:d4:ac:d0:d0:dd:e4:de:
    b6:69
exponent1:
    00:e1:39:d9:51:aa:26:87:cb:4f:02:7a:be:f2:1c:
    cd:1e:ed:c4:c5:44:cc:0c:38:f7:69:38:dd:c4:35:
    41:64:76:47:9d:28:ee:de:0c:b0:12:fa:4d:5a:63:
    9f:c5:ed:96:23:49:be:fe:37:28:9a:ce:8e:a4:91:
    32:98:61:c0:65:f7:ca:23:cf:46:6b:0d:13:85:78:
    5b:da:44:7c:7a:30:48:70:55:45:e4:98:c7:a6:93:
    9d:30:5a:4f:b2:f7:44:b4:eb:d3:1f:b2:8f:36:c6:
    75:4a:51:04:31:0b:df:e8:6a:c5:d9:1e:ce:7a:b0:
    88:53:a8:4f:e0:ba:f9:0f:6b:86:a7:12:5f:08:2a:
    63:f5:be:cd:69:6d:b8:13:3f:9e:40:ab:23:d2:9d:
    6d:71:cd:11:bb:c4:22:62:4c:b1:5b:f0:7f:8a:21:
    10:e1:16:e5:c6:b6:25:00:06:07:0a:80:bc:2d:7f:
    4e:7d:d7:a0:8e:4d:5e:7d:f0:60:61:9b:a9:95:18:
    18:e4:b0:f5:07:55:89:5c:b3:37:f9:ab:57:b3:2e:
    9c:0c:6d:90:b6:38:0c:ad:1b:55:45:c9:7b:e0:b5:
    1b:52:6b:f5:0b:bd:b7:a6:1d:5c:9f:76:a4:72:32:
    da:99:05:dc:71:e7:85:3c:5b:66:1c:d5:02:ec:80:
    c2:01
exponent2:
    53:99:e7:14:30:d6:46:db:2d:d5:85:24:c2:c5:c7:
    e1:97:b0:b1:34:fe:ff:c8:03:20:9c:6b:67:f3:d8:
    8a:34:bf:f3:e4:69:81:8a:b8:95:5a:0b:18:48:a0:
    72:de:30:5a:ca:47:83:7d:f7:f1:d8:eb:94:ee:7f:
    5f:f9:56:88:ad:72:86:97:c9:02:d9:b9:c5:59:8a:
    bb:7e:2a:72:8b:a3:ed:14:14:35:46:dc:b6:c9:87:
    75:e1:30:fa:e3:eb:51:7c:48:dc:a2:16:1b:5b:c3:
    2f:ab:d2:02:8f:52:54:1d:f5:5b:c6:f1:b2:b7:4d:
    e4:ef:f5:7c:df:1a:ab:13:f9:de:79:a4:08:09:af:
    1b:07:d5:61:d5:1a:a2:b3:ed:d0:d8:c2:aa:e2:4b:
    a7:40:7c:d7:58:b6:b5:77:06:a2:bb:c2:24:38:a6:
    fa:85:c0:76:ba:36:f2:98:1d:9b:08:40:db:e5:b6:
    70:d9:2c:95:1e:0c:6e:cf:81:f6:a4:02:01:2a:3e:
    6f:2a:e8:ec:1a:6a:c8:09:d6:1e:b4:6c:ff:f0:b2:
    0d:cd:c1:0e:9f:d8:0d:16:1e:2b:d2:e2:bc:b4:92:
    53:c9:4e:20:8d:7f:da:ab:63:6c:24:83:e7:75:a3:
    14:30:af:31:93:9f:36:8a:5c:e9:d3:db:c7:8a:71:
    a1
coefficient:
    00:80:bc:4b:4e:df:15:31:7d:9f:1c:8a:2e:70:0e:
    5a:a4:dd:b8:f0:68:d8:72:2d:6a:7b:ba:dd:6b:cd:
    09:ab:c6:df:1c:69:34:2c:2c:00:6b:4a:9e:f0:34:
    fe:27:4e:6c:7e:40:ec:6b:b5:b7:1a:1c:46:5f:bc:
    b8:3a:f5:cf:84:b1:d1:52:93:fc:53:a5:59:fb:af:
    17:87:d4:1d:e0:6e:09:53:99:a9:3a:3a:95:55:3b:
    83:47:fc:b0:c3:06:b4:e8:70:79:bd:99:74:de:47:
    85:af:e6:33:df:c9:c0:67:9b:98:2f:20:97:27:b4:
    cc:74:a0:5f:0a:08:c0:6e:01:c0:d0:9e:c9:64:60:
    4a:28:11:a2:04:8e:da:f1:d9:cb:42:d8:70:6f:4c:
    dc:a9:ac:71:94:aa:b6:7f:4d:4f:71:26:5d:b4:b6:
    ac:24:bc:55:0a:2b:4f:53:c1:25:65:96:a9:a6:8a:
    d7:48:d6:de:cf:a4:90:86:eb:a7:e3:64:a5:f8:92:
    cd:3a:3b:1c:ac:62:04:3e:df:59:b2:19:b8:c8:4c:
    bb:64:b7:29:b8:cb:0f:d8:76:1d:15:9b:53:1a:3a:
    e3:60:4c:6a:5c:66:54:5a:0b:f6:39:11:87:11:31:
    93:74:bd:0c:22:07:bb:21:b4:94:47:49:f9:d5:2e:
    0c:a8
```



ca.crt

wendet
Identity: wendet
Verified by: wendet
Expires: 11/17/31

Details

Subject Name
C (Country): US
ST (State): CALIFORNIA
L (Locality): Irvine
O (Organization): turtlepop
OU (Organizational Unit): tents
CN (Common Name): wendet
EMAIL (Email Address): fornals@gmail.com

Issuer Name
C (Country): US
ST (State): CALIFORNIA
L (Locality): Irvine
O (Organization): turtlepop
OU (Organizational Unit): tents
CN (Common Name): wendet
EMAIL (Email Address): fornals@gmail.com

Issued Certificate
Version: 3
Serial Number: 7F 7A E7 E6 B5 23 8D 36 68 BA 3E EB 91 6A 6A 4B 47 37 6C 6D
Not Valid Before: 2021-11-19
Not Valid After: 2031-11-17

Certificate Fingerprints
SHA1: C3 7B 3D D7 D0 14 D6 D1 C0 4C DE 9D 31 47 9C 0A 93 9F 11 FA
MD5: 50 FB 2A 75 DE C9 06 5B 2F 2A 4B A1 8F DE 44 1D

Public Key Info
Key Algorithm: RSA
Key Parameters: 05 00
Key Size: 4096
Key SHA1 Fingerprint: 8D 15 B4 E8 84 A1 F2 5F 3C A2 9E 96 74 9F 66 03 2D B2 47 94
Public Key:
30 82 02 0A 02 82 02 01 00 D0 7D 25 03 80 92 CF 43 24 8B 0D E6 88 63 61 1E F2 79 FD 87 02 B6 55 0F 84 2D 0C C8 55 98 7A DD 98 95 A4 E3 BC AA BE D0 02 E1 1B 06 60 8A A2 88 07 20 D8 23 96 DF 94 E6 9C 49 32 D4 DE
65 21 9D FD 1C 0B B4 58 E3 88 F5 7D C6 AD 6D 45 ED 72 C8 59 7E CE 3F E9 E3 F8 FF 38 16 B0 A3 5B 4D E3 B6 8B F3 E8 9B 64 B4 11 65 57 05 9B 7C 12 95 F3 A8 E1 30 A2 B3 F4 61 2D DC 4E 47 36 2F 0F 3D 4B E7 D2 EB 99
94 AD E1 13 4C B2 CB A2 8B 4B E6 9C 74 3A B5 0C CE 4C 31 9E 07 99 38 58 99 A6 41 BF 8A CD 01 4D A0 16 25 67 28 86 89 03 EF 09 A8 52 52 AD 44 9B F9 76 71 DC 41 2F EE D2 7B 33 CB DD AF 9A B9 19 B0 AB 00 F7 B7 28
A9 DB CF B1 07 98 07 F5 28 59 95 BF 4F 3C A8 42 21 83 8B B9 22 1A 87 25 D7 6E AB 6A 47 4F 00 A1 7D DC FF 1A BA 78 24 E1 34 81 2C 97 79 7A C4 D7 E4 13 1F AB 16 B6 EE 6E CD 53 98 25 01 FC 5E 44 94 22 BA 58 CF 33
20 E7 EA 26 89 3B 66 64 78 E2 F7 69 B3 27 9B D0 D9 9C 8F CC 63 50 4F 00 20 47 E4 F4 23 BF 18 F2 92 40 4C FA CC 83 3D EB 61 32 C7 21 78 68 B7 D4 3D C7 EA 71 14 B7 E5 77 92 F4 46 40 1B 12 BF 09 09 B7 D5 D7 66 95
CA 2B 3A 6B 11 79 9C B2 3A 93 7E 44 53 85 E3 C9 3F 18 37 47 43 D8 3F D7 7A A8 98 24 D9 BE 99 EA D6 F9 F4 13 C6 8B 57 0B D8 8F 9A 10 D4 EF 71 E5 A6 0F 44 BE 7E 4C B5 87 C9 DB 6B 7E 5C 29 FD 72 F2 E7 2E 2A D9 3A
28 64 E9 63 88 D2 4B 4C 84 B8 49 58 BC 1F 3A 7C 94 58 3B 28 02 9B 84 1D 9F C5 2D 99 AE 72 97 8C 5C 9A 21 95 76 58 E4 62 E7 40 56 52 09 84 D8 09 B6 1B 16 E4 1F 73 04 AD 98 AA CD 1D 25 7F 0A D8 3B EA 7D 71 91 C5
EB 36 70 0C 86 79 92 61 1C 9B A3 49 71 73 23 DC CC 4C 0E 3E B9 D4 AB 02 A4 58 8D 98 56 91 69 02 03 01 00 01

Subject Key Identifier
Key Identifier: FF F4 02 8D 3E 31 18 AF FB AD 90 4E 47 A0 69 FD ED 7B 9A 44
Critical: No

Extension
Identifier: 2.5.29.35
Value: 30 16 80 14 FF F4 02 8D 3E 31 18 AF FB AD 90 4E 47 A0 69 FD ED 7B 9A 44
Critical: No

Basic Constraints
Certificate Authority: Yes

Close Import

We see the subject and issuer are the same, which shows a self-signed certificate.

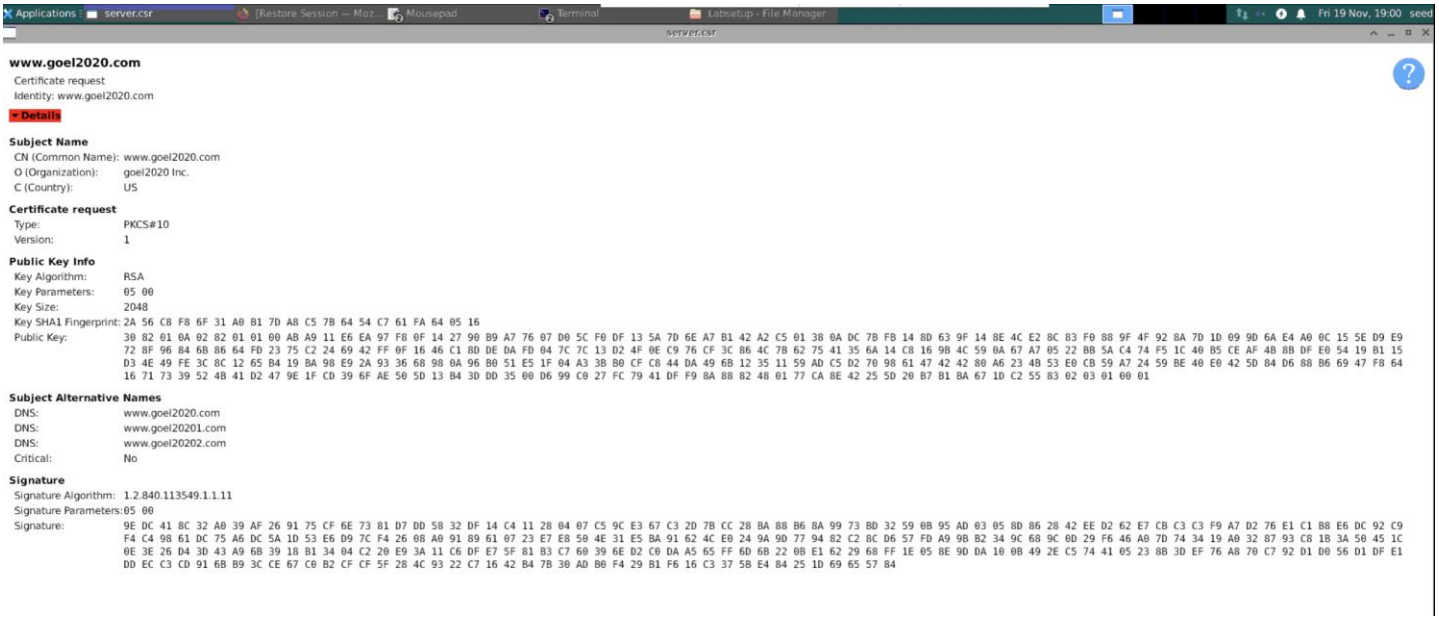
Also, the Certificate Authority (CA) is set to Yes in Basic Constraints, which means that this certificate can be used to sign and issue another certificate, hence this becoming certificate of a Certificate Authority (CA).

Task 2: Generating a Certificate Request for Your Web Server

We are creating an RSA public-private key pair:

```
    0C:A8
seed@shikhirsvm:~/security/project8/Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/CN=www.goel2020.com/O=goel2020 Inc./C=US" -passout pass:1234 -addext "subjectAltNam
e = DNS:www.goel2020.com, DNS:www.goel20201.com, DNS:www.goel20202.com"
Generating a RSA private key
.+++++
..............+++++
writing new private key to 'server.key'
-----
seed@shikhirsvm:~/security/project8/Labsetup$
```

We then create a Certificate Signing Request (CSR) including the company's public key. The CSR has the following details and with company's common name being goel2020.com (company's domain). The CSR file needs the Certificate Authorities signature for the certificate. We change the policy to policy_anything from policy_match to avoid any errors.



www.goel2020.com
Certificate request
Identity: www.goel2020.com

Details

Subject Name
CN (Common Name): www.goel2020.com
O (Organization): goel2020 Inc.
C (Country): US

Certificate request
Type: PKCS#10
Version: 1

Public Key Info
Key Algorithm: RSA
Key Parameters: 05 00
Key Size: 2048
Key SHA1 Fingerprint: 2A 56 C8 F8 6F 31 A0 B1 7D A8 C5 7B 64 54 C7 61 FA 64 05 16
Public Key:
```
30 82 01 0A 02 82 01 01 00 AB A9 11 E6 EA 97 F8 0F 14 27 90 B9 A7 76 07 D0 5C F0 DF 13 5A 7D 6E A7 B1 42 A2 C5 01 38 0A DC 7B FB 14 8D 63 9F 14 8E 4C E2 8C 83 F0 88 9F 4F 92 8A 7D 1D 09 9D 6A E4 A0 0C 15 5E D9 E9
72 8F 96 84 6B 86 64 FD 23 75 C2 24 69 42 FF 0F 16 46 C1 8D DE DA FD 04 7C 7C 13 D2 4F 0E C9 76 CF 3C 86 4C 7B 62 75 41 35 6A 14 C8 16 9B 4C 59 0A 67 A7 05 22 BB 5A C4 74 F5 1C 40 B5 CE AF 4B 8B DF E0 54 19 B1 15
D3 4E 49 FE 3C 8C 12 65 B4 19 BA 98 E9 2A 93 36 68 98 0A 96 B0 51 E5 1F 04 A3 3B B0 CF C8 44 DA 49 6B 12 35 11 59 AD C5 D2 70 98 61 47 42 42 80 A6 23 4B 53 E0 CB 59 A7 24 59 BE 40 E0 42 5D 84 D6 88 B6 69 47 F8 64
16 71 73 39 52 4B 41 D2 47 9E 1F CD 39 6F AE 50 5D 13 B4 3D DD 35 00 D6 99 C0 27 FC 79 41 DF F9 8A 88 82 48 01 77 CA 8E 42 25 5D 20 B7 B1 BA 67 1D C2 55 83 02 03 01 00 01
```

Subject Alternative Names
DNS: www.goel2020.com
DNS: www.goel20201.com
DNS: www.goel20202.com
Critical: No

Signature
Signature Algorithm: 1.2.840.113549.1.1.11
Signature Parameters: 05 00
Signature:
```
9E DC 41 8C 32 A0 39 AF 26 91 75 CF 6E 73 81 D7 DD 58 32 DF 14 C4 11 28 04 07 C5 9C E3 67 C3 2D 7B CC 28 BA 88 B6 8A 99 73 BD 32 59 0B 95 AD 03 05 8D 86 28 42 EE D2 62 E7 CB C3 C3 F9 A7 D2 76 E1 C1 B8 E6 DC 92 C9
F4 C4 98 61 DC 75 A6 DC 5A 1D 53 E6 D9 7C F4 26 08 A0 91 89 61 07 23 E7 E8 50 4E 31 E5 BA 91 62 4C E0 24 9A 9D 77 94 82 C2 8C D6 57 FD A9 9B B2 34 9C 68 9C 0D 29 F6 46 A0 7D 74 34 19 A0 32 87 93 C8 1B 3A 50 45 1C
0E 3E 26 D4 3D 43 A9 6B 39 18 B1 34 04 C2 20 E9 3A 11 C6 DF E7 5F B1 B3 C7 60 39 6E D2 C0 DA A5 65 FF 6D 6B 22 0B E1 62 29 68 FF 1E 05 8E 9D DA 10 0B 49 2E C5 74 41 05 23 BB 3D EF 76 A8 70 C7 92 D1 D0 56 D1 DF E1
DD EC C3 CD 91 6B B9 3C CE 67 C0 B2 CF CF 5F 28 4C 93 22 C7 16 42 B4 7B 30 AD B0 F4 29 B1 F6 16 C3 37 5B E4 B4 25 1D 69 65 57 84
```

We use the following commands to see the CA's server.csr and server.key. We see the details of the CSR.

```
writing new private key to 'server.key'
-----
seed@shikhirsvm:~/security/project8/Labsetup$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.goel2020.com, O = goel2020 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:a9:11:e6:ea:97:f8:0f:14:27:90:b9:a7:76:
                    07:d0:5c:f0:df:13:5a:7d:6e:a7:b1:42:a2:c5:01:
                    38:0a:dc:7b:fb:14:8d:63:9f:14:8e:4c:e2:8c:83:
                    f0:88:9f:4f:92:8a:7d:1d:09:9d:6a:e4:a0:0c:15:
                    5e:d9:e9:72:8f:96:84:6b:86:64:fd:23:75:c2:24:
                    69:42:ff:0f:16:46:c1:8d:de:da:fd:04:7c:7c:13:
                    d2:4f:0e:c9:76:cf:3c:86:4c:7b:62:75:41:35:6a:
                    14:c8:16:9b:4c:59:0a:67:a7:05:22:bb:5a:c4:74:
                    f5:1c:40:b5:ce:af:4b:8b:df:e0:54:19:b1:15:d3:
                    4e:49:fe:3c:8c:12:65:b4:19:ba:98:e9:2a:93:36:
                    68:98:0a:96:b0:51:e5:1f:04:a3:3b:b0:cf:c8:44:
                    da:49:6b:12:35:11:59:ad:c5:d2:70:98:61:47:42:
                    42:80:a6:23:4b:53:e0:cb:59:a7:24:59:be:40:e0:
                    42:5d:84:d6:88:b6:69:47:f8:64:16:71:73:39:52:
                    4b:41:d2:47:9e:1f:cd:39:6f:ae:50:5d:13:b4:3d:
                    dd:35:00:d6:99:c0:27:fc:79:41:df:f9:8a:88:82:
                    48:01:77:ca:8e:42:25:5d:20:b7:b1:ba:67:1d:c2:
                    55:83
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.goel2020.com, DNS:www.goel20201.com, DNS:www.goel20202.com
    Signature Algorithm: sha256WithRSAEncryption
         9e:dc:41:8c:32:a0:39:af:26:91:75:cf:6e:73:81:d7:dd:58:
         32:df:14:c4:11:28:04:07:c5:9c:e3:67:c3:2d:7b:cc:28:ba:
         88:b6:8a:99:73:bd:32:59:0b:95:ad:03:05:8d:86:28:42:ee:
         d2:62:e7:cb:c3:c3:f9:a7:d2:76:e1:c1:b8:e6:dc:92:c9:f4:
         c4:98:61:dc:75:a6:dc:5a:1d:53:e6:d9:7c:f4:26:08:a0:91:
         89:61:07:23:e7:e8:50:4e:31:e5:ba:91:62:4c:e0:24:9a:9d:
         77:94:82:c2:8c:d6:57:fd:a9:9b:b2:34:9c:68:9c:0d:29:f6:
         46:a0:7d:74:34:19:a0:32:87:93:c8:1b:3a:50:45:1c:0e:3e:
         26:d4:3d:43:a9:6b:39:18:b1:34:04:c2:20:e9:3a:11:c6:df:
         e7:5f:81:b3:c7:60:39:6e:d2:c0:da:a5:65:ff:6d:6b:22:0b:
         e1:62:29:68:ff:1e:05:8e:9d:da:10:0b:49:2e:c5:74:41:05:
         23:8b:3d:ef:76:a8:70:c7:92:d1:d0:56:d1:df:e1:dd:ec:c3:
         cd:91:6b:b9:3c:ce:67:c0:b2:cf:cf:5f:28:4c:93:22:c7:16:
         42:b4:7b:30:ad:b0:f4:29:b1:f6:16:c3:37:5b:e4:84:25:1d:
         69:65:57:84
seed@shikhirsvm:~/security/project8/Labsetup$
```

seed@shikhirsvm: ~/security/project8/Labsetup

File Edit View Search Terminal Help

```
seed@shikhirsvm:~/security/project8/Labsetup$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:ab:a9:11:e6:ea:97:f8:0f:14:27:90:b9:a7:76:
    07:d0:5c:f0:df:13:5a:7d:6e:a7:b1:42:a2:c5:01:
    38:0a:dc:7b:fb:14:8d:63:9f:14:8e:4c:e2:8c:83:
    f0:88:9f:4f:92:8a:7d:1d:09:9d:6a:e4:a0:0c:15:
    5e:d9:e9:72:8f:96:84:6b:86:64:fd:23:75:c2:24:
    69:42:ff:0f:16:46:c1:8d:de:da:fd:04:7c:7c:13:
    d2:4f:0e:c9:76:cf:3c:86:4c:7b:62:75:41:35:6a:
    14:c8:16:9b:4c:59:0a:67:a7:05:22:bb:5a:c4:74:
    f5:1c:40:b5:ce:af:4b:8b:df:e0:54:19:b1:15:d3:
    4e:49:fe:3c:8c:12:65:b4:19:ba:98:e9:2a:93:36:
    68:98:0a:96:b0:51:e5:1f:04:a3:3b:b0:cf:c8:44:
    da:49:6b:12:35:11:59:ad:c5:d2:70:98:61:47:42:
    42:80:a6:23:4b:53:e0:cb:59:a7:24:59:be:40:e0:
    42:5d:84:d6:88:b6:69:47:f8:64:16:71:73:39:52:
    4b:41:d2:47:9e:1f:cd:39:6f:ae:50:5d:13:b4:3d:
    dd:35:00:d6:99:c0:27:fc:79:41:df:f9:8a:88:82:
    48:01:77:ca:8e:42:25:5d:20:b7:b1:ba:67:1d:c2:
    55:83
publicExponent: 65537 (0x10001)
privateExponent:
    00:a2:0a:2e:c3:f3:9f:10:a1:eb:3c:8d:f9:32:82:
    d0:4d:77:ee:48:25:54:be:22:be:59:2d:b5:c8:91:
    a5:fd:5a:b4:0e:07:10:90:81:92:3d:e1:85:d9:6e:
    92:97:e5:0a:90:21:fa:88:76:93:0a:5c:56:58:11:
    b4:3f:af:86:5c:d4:90:9b:8f:79:b5:1a:cc:06:3f:
    a8:bd:7d:57:18:88:22:1d:71:c8:f6:1e:4e:04:32:
    11:cc:5f:00:fe:0e:11:ec:14:36:44:72:ba:e3:59:
    07:d4:f8:c2:10:07:dd:32:8b:0e:e6:02:45:64:3d:
    a3:42:d0:32:ce:af:da:78:65:88:a5:60:84:4f:22:
    18:41:0d:c4:c0:34:e4:1e:5e:bb:b3:65:86:fc:bb:
    50:be:0f:23:e8:96:05:8b:5f:3b:d3:07:77:38:c0:
    6d:69:20:c8:68:87:14:41:8f:89:48:af:fd:b1:ea:
    df:53:64:6e:8f:6c:35:b6:72:1a:24:3a:7f:69:92:
    29:dc:dc:d5:09:5f:de:02:cb:26:d9:0c:ce:0f:78:
    c2:e8:db:90:d4:0b:c8:48:87:d6:c4:d5:6d:d6:d4:
    57:32:a7:16:cc:79:49:88:3e:c4:eb:da:2b:cb:b7:
    62:aa:ee:dd:2c:67:c8:96:13:6f:21:95:1c:94:d5:
    b4:41
prime1:
    00:d9:d0:5f:51:03:1f:98:fa:1c:6b:14:a4:78:1e:
    17:c6:db:ff:bc:d3:31:b5:34:dc:38:8b:35:69:4b:
    c6:be:f0:8b:26:9d:2e:ac:43:58:75:e6:42:72:13:
    df:9f:cf:ed:83:35:b0:d4:d2:58:73:7f:26:0b:dd:
    bc:b3:c4:23:60:77:8f:a1:ee:2f:62:ba:4a:03:e9:
    44:7e:28:3b:5e:fb:4b:57:8e:18:14:4f:7b:42:fe:
    67:3c:a2:5f:df:1f:f6:05:0d:ce:38:60:a0:9f:5c:
    ca:da:22:1e:58:d2:46:92:f2:20:03:03:f2:6a:e8:
    30:34:af:70:29:b1:00:8f:af
prime2:
    00:c9:c1:4c:5c:5d:e3:c7:70:c3:6f:e1:b8:ed:02:
    7b:02:10:43:cb:8f:58:3c:1a:d8:f2:f3:d7:dd:72:
    17:a0:38:76:5c:76:a2:27:a0:c7:7d:40:03:30:cb:
    1c:47:84:0f:3f:85:7f:be:cb:84:ff:33:41:92:f8:
    e7:11:f0:43:fd:91:18:aa:4d:de:c3:76:ce:c0:cb:
    6a:11:47:cf:9f:87:a8:43:1d:2c:34:e5:d8:c2:f4:
    5a:83:91:ee:8f:dd:66:79:7a:32:e0:7b:fe:a2:bc:
    b6:87:14:c2:a1:bf:5b:65:33:8d:a4:01:56:07:dd:
    66:df:8c:a6:9c:32:2f:58:6d
```

seed@shikhirsvm: ~/security/project8/Labsetup

File Edit View Search Terminal Help

```
    07:d4:f8:c2:10:07:dd:32:8b:0e:e6:02:45:64:3d:
    a3:42:d0:32:ce:af:da:78:65:88:a5:60:84:4f:22:
    18:41:0d:c4:c0:34:e4:1e:5e:bb:b3:65:86:fc:bb:
    50:be:0f:23:e8:96:05:8b:5f:3b:d3:07:77:38:c0:
    6d:69:20:c8:68:87:14:41:8f:89:48:af:fd:b1:ea:
    df:53:64:6e:8f:6c:35:b6:72:1a:24:3a:7f:69:92:
    29:dc:dc:d5:09:5f:de:02:cb:26:d9:0c:ce:0f:78:
    c2:e8:db:90:d4:0b:c8:48:87:d6:c4:d5:6d:d6:d4:
    57:32:a7:16:cc:79:49:88:3e:c4:eb:da:2b:cb:b7:
    62:aa:ee:dd:2c:67:c8:96:13:6f:21:95:1c:94:d5:
    b4:41
prime1:
    00:d9:d0:5f:51:03:1f:98:fa:1c:6b:14:a4:78:1e:
    17:c6:db:ff:bc:d3:31:b5:34:dc:38:8b:35:69:4b:
    c6:be:f0:8b:26:9d:2e:ac:43:58:75:e6:42:72:13:
    df:9f:cf:ed:83:35:b0:d4:d2:58:73:7f:26:0b:dd:
    bc:b3:c4:23:60:77:8f:a1:ee:2f:62:ba:4a:03:e9:
    44:7e:28:3b:5e:fb:4b:57:8e:18:14:4f:7b:42:fe:
    67:3c:a2:5f:df:1f:f6:05:0d:ce:38:60:a0:9f:5c:
    ca:da:22:1e:58:d2:46:92:f2:20:03:03:f2:6a:e8:
    30:34:af:70:29:b1:00:8f:af
prime2:
    00:c9:c1:4c:5c:5d:e3:c7:70:c3:6f:e1:b8:ed:02:
    7b:02:10:43:cb:8f:58:3c:1a:d8:f2:f3:d7:dd:72:
    17:a0:38:76:5c:76:a2:27:a0:c7:7d:40:03:30:cb:
    1c:47:84:0f:3f:85:7f:be:cb:84:ff:33:41:92:f8:
    e7:11:f0:43:fd:91:18:aa:4d:de:c3:76:ce:c0:cb:
    6a:11:47:cf:9f:87:a8:43:1d:2c:34:e5:d8:c2:f4:
    5a:83:91:ee:8f:dd:66:79:7a:32:e0:7b:fe:a2:bc:
    b6:87:14:c2:a1:bf:5b:65:33:8d:a4:01:56:07:dd:
    66:df:8c:a6:9c:32:2f:58:6d
exponent1:
    2d:c2:fa:93:a1:ad:5c:cd:87:74:f3:e4:4e:1c:3c:
    70:9a:3e:13:a4:e7:77:a3:c0:74:dc:c2:7e:f9:dd:
    aa:b6:0c:f6:32:e5:e0:69:51:c7:8b:76:00:53:ae:
    92:fb:f3:71:b2:b1:11:35:94:41:c7:bf:ed:94:4b:
    96:15:2a:3d:95:41:07:0b:6c:c7:38:4e:5e:9d:fe:
    b6:e6:aa:fa:9c:9f:4a:a8:de:e4:3d:82:af:23:95:
    fb:06:3e:50:39:7d:cd:b8:05:d0:90:74:8e:a6:c7:
    33:a7:21:6b:15:da:9f:fa:e0:c0:e1:6e:68:09:9a:
    3f:27:70:d0:41:90:d5:9f
exponent2:
    00:c8:fa:b2:db:cc:77:ec:a4:4b:3b:f7:ca:a4:e7:
    74:ac:00:91:d8:84:ea:2b:ad:be:f2:7e:b0:4a:1b:
    ae:a7:5f:b7:a0:b2:59:24:4a:c8:8e:df:a6:8e:03:
    b7:1f:12:d1:b1:c0:86:1a:05:59:6e:73:9b:de:11:
    ee:f5:72:b7:f8:2f:83:37:9b:ac:ce:60:5a:e3:b9:
    7e:e6:c9:f7:6c:fe:d1:42:52:1c:48:71:b2:f5:ba:
    3f:34:93:b9:e7:3c:71:29:8f:ee:80:ab:64:64:ae:
    c2:d1:5b:7f:eb:6a:d9:5b:bd:f8:5a:29:2e:8f:55:
    21:76:8e:01:26:d5:e3:4e:1d
coefficient:
    00:bd:e6:95:ed:51:61:af:77:0a:7c:54:71:59:bf:
    cc:24:fe:05:15:ff:30:02:0b:6f:2b:0a:6a:d2:3f:
    e9:ca:57:b4:2a:51:8e:18:f9:c5:d7:50:4d:72:df:
    4a:f1:b8:45:a5:4e:05:fd:d4:dd:67:9a:66:9d:f5:
    d4:5c:ec:12:ca:81:68:e6:4b:ef:68:69:28:e5:4e:
    fe:f2:ad:76:d0:ad:e5:37:71:54:1b:e4:61:7f:d9:
    1f:63:9e:0e:5b:e6:87:3c:a7:33:47:ac:a3:9d:f6:
    5d:67:91:06:83:38:08:a0:50:00:d1:e2:c1:5f:96:
    a9:d3:a3:a2:66:bc:e6:4d:6b
seed@shikhirsvm:~/security/project8/Labsetup$
```

Task 3: Generating a Certificate for your server

We remove the comment from the copy extensions

```
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key

x509_extensions = usr_cert              # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options

#Extension copying option: use with caution.
 copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions        = crl_ext

default_days    = 365                   # how long to certify for
default_crl_days= 30                    # how long before next CRL
default_md      = default               # use public key default MD
preserve        = no                    # keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy          = policy_match

# For the CA policy
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
```

We make policy to policy anything to avoid any errors. Using the previously generated csr file we use openssl to get the certificate (.crt)

```
seed@shikhirsvm:~/security/project8/Labsetup$ openssl ca -config openssl.cnf -policy policy_anything -md sha256 -days 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 19 19:17:03 2021 GMT
            Not After : Nov 17 19:17:03 2031 GMT
        Subject:
            countryName               = US
            organizationName          = goel2020 Inc.
            commonName                = www.goel2020.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                58:25:CE:D0:4B:8B:7A:78:98:37:F8:3A:63:75:DF:8C:7B:79:D2:DF
            X509v3 Authority Key Identifier:
                keyid:FF:F4:02:8D:3E:31:18:AF:FB:AD:90:4E:47:A0:69:FD:ED:7B:9A:44

            X509v3 Subject Alternative Name:
                DNS:www.goel2020.com, DNS:www.goel20201.com, DNS:www.goel20202.com
Certificate is to be certified until Nov 17 19:17:03 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
seed@shikhirsvm:~/security/project8/Labsetup$
```

Here we have displayed the server.crt (certificate) file

```
seed@shikhirsvm: ~/security/project8/Labsetup
File  Edit  View  Search  Terminal  Help
seed@shikhirsvm:~/security/project8/Labsetup$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CALIFORNIA, L = Irvine, O = turtlepop, OU = tents, CN = wendet, emailAddress = fornals@gmail.com
        Validity
            Not Before: Nov 19 19:17:03 2021 GMT
            Not After : Nov 17 19:17:03 2031 GMT
        Subject: C = US, O = goel2020 Inc., CN = www.goel2020.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:a9:11:e6:ea:97:f8:0f:14:27:90:b9:a7:76:
                    07:d0:5c:f0:df:13:5a:7d:6e:a7:b1:42:a2:c5:01:
                    38:0a:dc:7b:fb:14:8d:63:9f:14:8e:4c:e2:8c:83:
                    f0:88:9f:4f:92:8a:7d:1d:09:9d:6a:e4:a0:0c:15:
                    5e:d9:e9:72:8f:96:84:6b:86:64:fd:23:75:c2:24:
                    69:42:ff:0f:16:46:c1:8d:de:da:fd:04:7c:7c:13:
                    d2:4f:0e:c9:76:cf:3c:86:4c:7b:62:75:41:35:6a:
                    14:c8:16:9b:4c:59:0a:67:a7:05:22:bb:5a:c4:74:
                    f5:1c:40:b5:ce:af:4b:8b:df:e0:54:19:b1:15:d3:
                    4e:49:fe:3c:8c:12:65:b4:19:ba:98:e9:2a:93:36:
                    68:98:0a:96:b0:51:e5:1f:04:a3:3b:b0:cf:c8:44:
                    da:49:6b:12:35:11:59:ad:c5:d2:70:98:61:47:42:
                    42:80:a6:23:4b:53:e0:cb:59:a7:24:59:be:40:e0:
                    42:5d:84:d6:88:b6:69:47:f8:64:16:71:73:39:52:
                    4b:41:d2:47:9e:1f:cd:39:6f:ae:50:5d:13:b4:3d:
                    dd:35:00:d6:99:c0:27:fc:79:41:df:f9:8a:88:82:
                    48:01:77:ca:8e:42:25:5d:20:b7:b1:ba:67:1d:c2:
                    55:83
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                58:25:CE:D0:4B:8B:7A:78:98:37:F8:3A:63:75:DF:8C:7B:79:D2:DF
            X509v3 Authority Key Identifier:
                keyid:FF:F4:02:8D:3E:31:18:AF:FB:AD:90:4E:47:A0:69:FD:ED:7B:9A:44

            X509v3 Subject Alternative Name:
                DNS:www.goel2020.com, DNS:www.goel20201.com, DNS:www.goel20202.com
    Signature Algorithm: sha256WithRSAEncryption
         59:76:ef:be:45:a0:f7:11:99:74:1d:fe:94:5a:80:42:f2:c5:
         7e:02:01:17:1b:22:ae:91:54:f8:a3:98:77:dd:4c:f1:55:27:
         63:21:26:97:b4:81:e8:91:c4:26:26:2b:ee:00:13:0f:ca:7c:
         d5:fa:6b:77:a0:7e:43:ea:c2:fd:b3:6e:1b:7e:b2:42:c3:c9:
         73:40:e8:4d:02:51:d7:9d:d4:b8:a6:74:e0:31:d4:24:2f:f7:
         ad:0f:fc:04:37:7a:26:7d:e2:f6:78:c8:30:17:ca:f2:4c:72:
         df:3d:91:2d:50:c1:c0:cd:a1:84:14:b5:2b:c4:69:31:e6:89:
         12:ac:24:b2:c1:78:97:b9:47:94:db:64:f7:ac:05:d4:c0:ab:
         8d:d6:43:22:a0:b5:9b:c7:7d:52:f9:02:97:d4:8c:6e:1a:a9:
         62:24:c5:72:25:50:e1:fc:4f:91:15:66:37:1c:0b:6e:c3:7e:
         ca:20:25:4d:d2:57:ba:33:aa:b7:38:e6:a4:2f:89:d0:f0:59:
         2c:d6:fa:8d:95:8f:d0:16:33:36:ac:5c:49:c1:32:78:70:e0:
         10:b8:a9:58:51:eb:c8:a4:ac:e2:8c:00:4d:1f:92:c2:1c:ce:
         7c:45:0e:3d:78:ac:56:dc:8e:5c:f4:a0:44:f1:64:a4:ed:61:
         b9:a8:d4:9f:ea:21:e0:44:c6:2a:08:be:f2:25:8b:d2:44:82:
```

```
seed@shikhirsvm: ~/security/project8/Labsetup
File  Edit  View  Search  Terminal  Help
                    00:ab:a9:11:e6:ea:97:f8:0f:14:27:90:b9:a7:76:
                    07:d0:5c:f0:df:13:5a:7d:6e:a7:b1:42:a2:c5:01:
                    38:0a:dc:7b:fb:14:8d:63:9f:14:8e:4c:e2:8c:83:
                    f0:88:9f:4f:92:8a:7d:1d:09:9d:6a:e4:a0:0c:15:
                    5e:d9:e9:72:8f:96:84:6b:86:64:fd:23:75:c2:24:
                    69:42:ff:0f:16:46:c1:8d:de:da:fd:04:7c:7c:13:
                    d2:4f:0e:c9:76:cf:3c:86:4c:7b:62:75:41:35:6a:
                    14:c8:16:9b:4c:59:0a:67:a7:05:22:bb:5a:c4:74:
                    f5:1c:40:b5:ce:af:4b:8b:df:e0:54:19:b1:15:d3:
                    4e:49:fe:3c:8c:12:65:b4:19:ba:98:e9:2a:93:36:
                    68:98:0a:96:b0:51:e5:1f:04:a3:3b:b0:cf:c8:44:
                    da:49:6b:12:35:11:59:ad:c5:d2:70:98:61:47:42:
                    42:80:a6:23:4b:53:e0:cb:59:a7:24:59:be:40:e0:
                    42:5d:84:d6:88:b6:69:47:f8:64:16:71:73:39:52:
                    4b:41:d2:47:9e:1f:cd:39:6f:ae:50:5d:13:b4:3d:
                    dd:35:00:d6:99:c0:27:fc:79:41:df:f9:8a:88:82:
                    48:01:77:ca:8e:42:25:5d:20:b7:b1:ba:67:1d:c2:
                    55:83
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                58:25:CE:D0:4B:8B:7A:78:98:37:F8:3A:63:75:DF:8C:7B:79:D2:DF
            X509v3 Authority Key Identifier:
                keyid:FF:F4:02:8D:3E:31:18:AF:FB:AD:90:4E:47:A0:69:FD:ED:7B:9A:44

            X509v3 Subject Alternative Name:
                DNS:www.goel2020.com, DNS:www.goel20201.com, DNS:www.goel20202.com
    Signature Algorithm: sha256WithRSAEncryption
         59:76:ef:be:45:a0:f7:11:99:74:1d:fe:94:5a:80:42:f2:c5:
         7e:02:01:17:1b:22:ae:91:54:f8:a3:98:77:dd:4c:f1:55:27:
         63:21:26:97:b4:81:e8:91:c4:26:26:2b:ee:00:13:0f:ca:7c:
         d5:fa:6b:77:a0:7e:43:ea:c2:fd:b3:6e:1b:7e:b2:42:c3:c9:
         73:40:e8:4d:02:51:d7:9d:d4:b8:a6:74:e0:31:d4:24:2f:f7:
         ad:0f:fc:04:37:7a:26:7d:e2:f6:78:c8:30:17:ca:f2:4c:72:
         df:3d:91:2d:50:c1:c0:cd:a1:84:14:b5:2b:c4:69:31:e6:89:
         12:ac:24:b2:c1:78:97:b9:47:94:db:64:f7:ac:05:d4:c0:ab:
         8d:d6:43:22:a0:b5:9b:c7:7d:52:f9:02:97:d4:8c:6e:1a:a9:
         62:24:c5:72:25:50:e1:fc:4f:91:15:66:37:1c:0b:6e:c3:7e:
         ca:20:25:4d:d2:57:ba:33:aa:b7:38:e6:a4:2f:89:d0:f0:59:
         2c:d6:fa:8d:95:8f:d0:16:33:36:ac:5c:49:c1:32:78:70:e0:
         10:b8:a9:58:51:eb:c8:a4:ac:e2:8c:00:4d:1f:92:c2:1c:ce:
         7c:45:0e:3d:78:ac:56:dc:8e:5c:f4:a0:44:f1:64:a4:ed:61:
         b9:a8:d4:9f:ea:21:e0:44:c6:2a:08:be:f2:25:8b:d2:44:82:
         9c:ae:51:bb:37:33:13:57:b4:d4:e2:b6:ff:af:46:ef:19:9e:
         62:93:85:d6:94:f1:c3:34:d9:1a:97:4d:ca:f3:45:a2:bd:e8:
         7f:64:96:72:40:2b:56:e3:75:92:03:40:74:a2:ed:c4:25:7e:
         6b:22:be:04:5d:e3:b5:d9:7b:38:3c:dc:c0:53:79:a4:88:b2:
         07:40:46:33:da:ea:ca:d2:d1:44:1b:45:66:98:df:39:de:a3:
         24:5e:3e:f5:0b:1a:14:0f:49:cc:e6:9d:d1:73:07:d6:20:b4:
         7b:ae:f4:32:90:36:c9:cc:8e:2d:f4:e0:fe:0f:83:86:97:cf:
         85:cb:69:6d:d8:15:b3:f1:7f:02:47:fe:db:ed:b3:70:8d:cd:
         35:92:1d:da:08:57:e2:d1:17:3b:e0:c6:86:6e:fa:52:a2:58:
         f3:c0:a8:87:1d:12:ac:d4:41:d7:51:e7:78:15:19:7d:2e:e3:
         c0:cd:78:37:24:ea:be:a5:f1:5d:0b:fe:cd:19:9e:f8:52:8d:
         11:7d:f3:43:df:92:ac:56:28:98:c0:9d:a7:ce:e8:2b:db:2f:
         2c:f3:58:02:46:37:21:d6:52:60:74:be:b1:5a:a1:09:98:31:
         8f:b5:3f:04:51:fd:f5:4b
seed@shikhirsvm:~/security/project8/Labsetup$
```

We have successfully created the certificate from the csr file.

Task 4: Deploying Certificate in an Apache-Based HTTPS Website

```
34.123.218.141:5901 (shikhirsvm.c.serene-cathode-329819.internal:1 (seed)) - VNC Viewer
Applications  Firefox  Mousepad  Terminal  volumes - File Manager  Fri 19 Nov, 21:02  seed
root@eb0c430d45c3: /
File  Edit  View  Search  Terminal  Help
ca-certificates.conf   host.conf     machine-id     profile.d   ssl
cron.d                 hostname      magic          protocols   subgid
cron.daily             hosts         magic.mime     rc0.d       subuid
debconf.conf           init.d        mailcap        rc1.d       sysctl.conf
debian_version         iproute2      mailcap.order  rc2.d       sysctl.d
default                issue         mime.types     rc3.d       systemd
deluser.conf           issue.net     mke2fs.conf    rc4.d       terminfo
dpkg                   kernel        mtab           rc5.d       timezone
e2scrub.conf           ld.so.cache   nanorc         rc6.d       ucf.conf
environment            ld.so.conf    networks       rc5.d       ufw
ethertypes             ld.so.conf.d  nsswitch.conf  resolv.conf update-motd.d
fonts                  ldap          opt            rmt         xattr.conf
root@eb0c430d45c3:/etc# etc/apache2/sites-available
bash: etc/apache2/sites-available: No such file or directory
root@eb0c430d45c3:/etc# etc/apache2/
bash: etc/apache2/: No such file or directory
root@eb0c430d45c3:/etc# etc/apache2
bash: etc/apache2: No such file or directory
root@eb0c430d45c3:/etc# cd ..
root@eb0c430d45c3:/# etc/apache2
bash: etc/apache2: Is a directory
root@eb0c430d45c3:/# ls
bin   certs  etc   lib    lib64  media  opt   root  sbin   srv  tmp  var
boot  dev    home  lib32  libx32 mnt    proc  run   shikhir sys usr  volumes
root@eb0c430d45c3:/# cd etc
root@eb0c430d45c3:/etc# ls
adduser.conf           fstab         legal          os-release  rpc
alternatives           gai.conf      libaudit.conf  pam.conf    security
apache2                group         localtime      pam.d       selinux
apt                    group-        logcheck       passwd      services
bash.bashrc            gshadow       login.defs     perl        shadow
bindresvport.blacklist gshadow-      logrotate.d    php         shells
ca-certificates        gss           lsb-release    profile     skel
ca-certificates.conf   host.conf     machine-id     profile.d   ssl
cron.d                 hostname      magic          protocols   subgid
cron.daily             hosts         magic.mime     rc0.d       subuid
debconf.conf           init.d        mailcap        rc1.d       sysctl.conf
debian_version         iproute2      mailcap.order  rc2.d       sysctl.d
default                issue         mime.types     rc3.d       systemd
deluser.conf           issue.net     mke2fs.conf    rc4.d       terminfo
dpkg                   kernel        mtab           rc5.d       timezone
e2scrub.conf           ld.so.cache   nanorc         rc6.d       ucf.conf
environment            ld.so.conf    networks       rc5.d       ufw
ethertypes             ld.so.conf.d  nsswitch.conf  resolv.conf update-motd.d
fonts                  ldap          opt            rmt         xattr.conf
root@eb0c430d45c3:/etc# cd apache2
root@eb0c430d45c3:/etc/apache2# ls
apache2.conf    conf-enabled  magic           mods-enabled  sites-available
conf-available  envvars       mods-available  ports.conf    sites-enabled
root@eb0c430d45c3:/etc/apache2# cd sites-available
root@eb0c430d45c3:/etc/apache2/sites-available# ls
000-default.conf  bank32_apache_ssl.conf  default-ssl.conf
root@eb0c430d45c3:/etc/apache2/sites-available# sudo vim shikhir
bash: sudo: command not found
root@eb0c430d45c3:/etc/apache2/sites-available# vim shikhir.conf
bash: vim: command not found
root@eb0c430d45c3:/etc/apache2/sites-available# nano shikhir.conf
root@eb0c430d45c3:/etc/apache2/sites-available# cd ..
root@eb0c430d45c3:/etc/apache2# cd ..
root@eb0c430d45c3:/etc# cd ..
root@eb0c430d45c3:/# cp volumes/server.crt volumes/server.key certs
root@eb0c430d45c3:/#
```

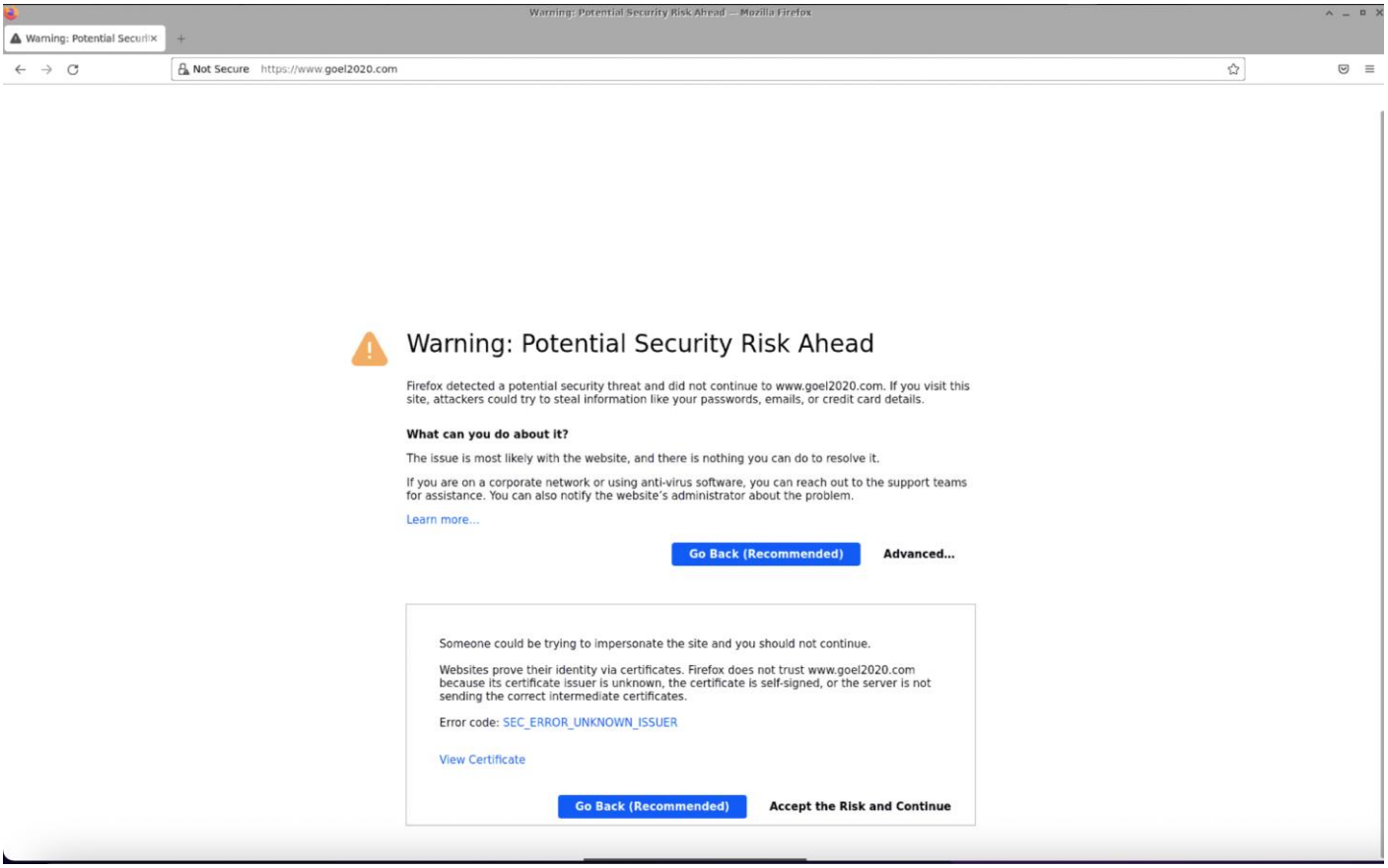
We configure apache server for running our own domain name. After creating a config file named shikhir in /etc/apache2/sites-available we edit it according to our requirements and our key and certificate.

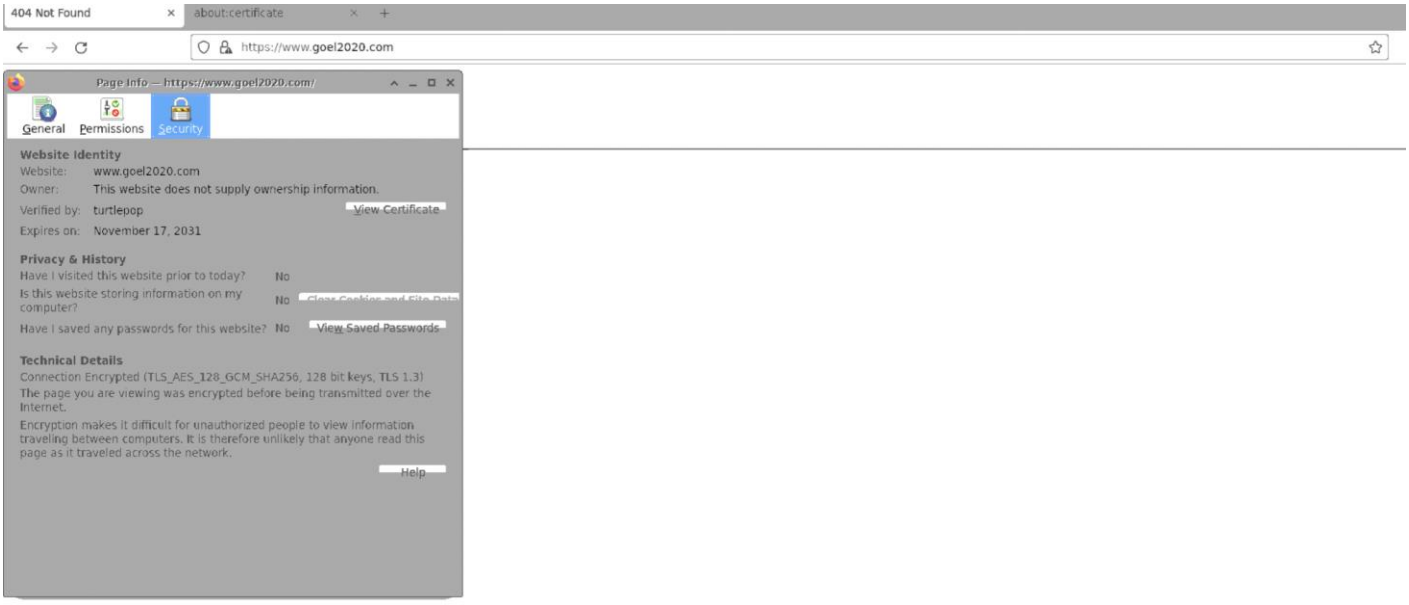
Enabling Apache

```
root@eb0c430d45c3:/# service apache2 start
 * Starting Apache httpd web server apache2
AH00112: Warning: DocumentRoot [/var/www/shikhir] does not exist
AH00112: Warning: DocumentRoot [/var/www/shikhir] does not exist
Enter passphrase for SSL/TLS keys for www.goel2020.com:443 (RSA):
Enter passphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
Action 'start' failed.
The Apache error log may have more information.
 *
root@eb0c430d45c3:/# service apache2 start
 * Starting Apache httpd web server apache2
AH00112: Warning: DocumentRoot [/var/www/shikhir] does not exist
AH00112: Warning: DocumentRoot [/var/www/shikhir] does not exist
Enter passphrase for SSL/TLS keys for www.goel2020.com:443 (RSA):
Enter passphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
 *
root@eb0c430d45c3:/#
```

We see that we are not able to access the webpage. It shows that the website is not secured since the rootCA we have created in our seed is not authorized by firefox.

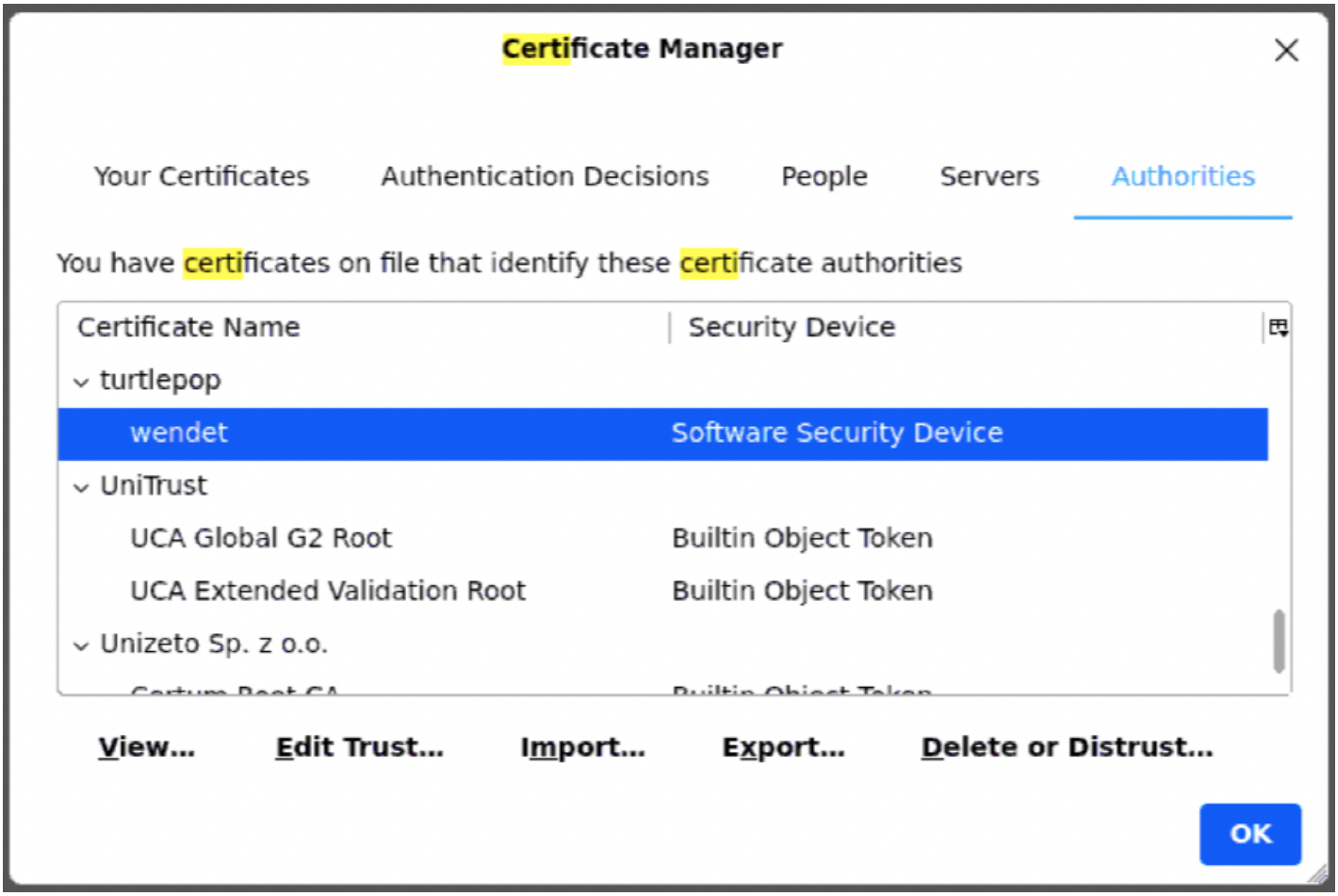
When we open advanced options, we can see the certificate not authorised by firefox.





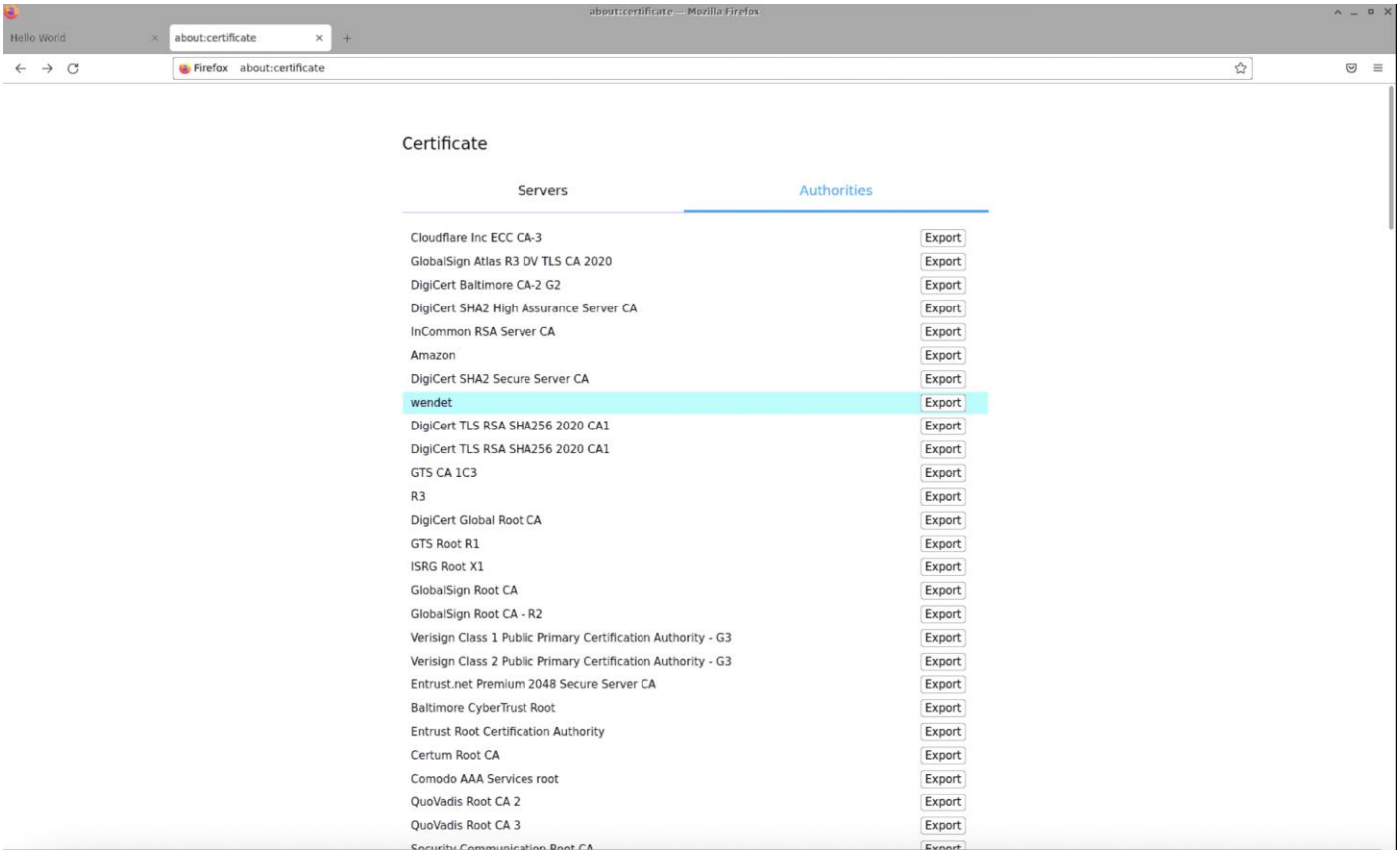
After adding the certificate

After importing our ca.crt file, we can see our certificate listed in the trusted certificates list of firefox.



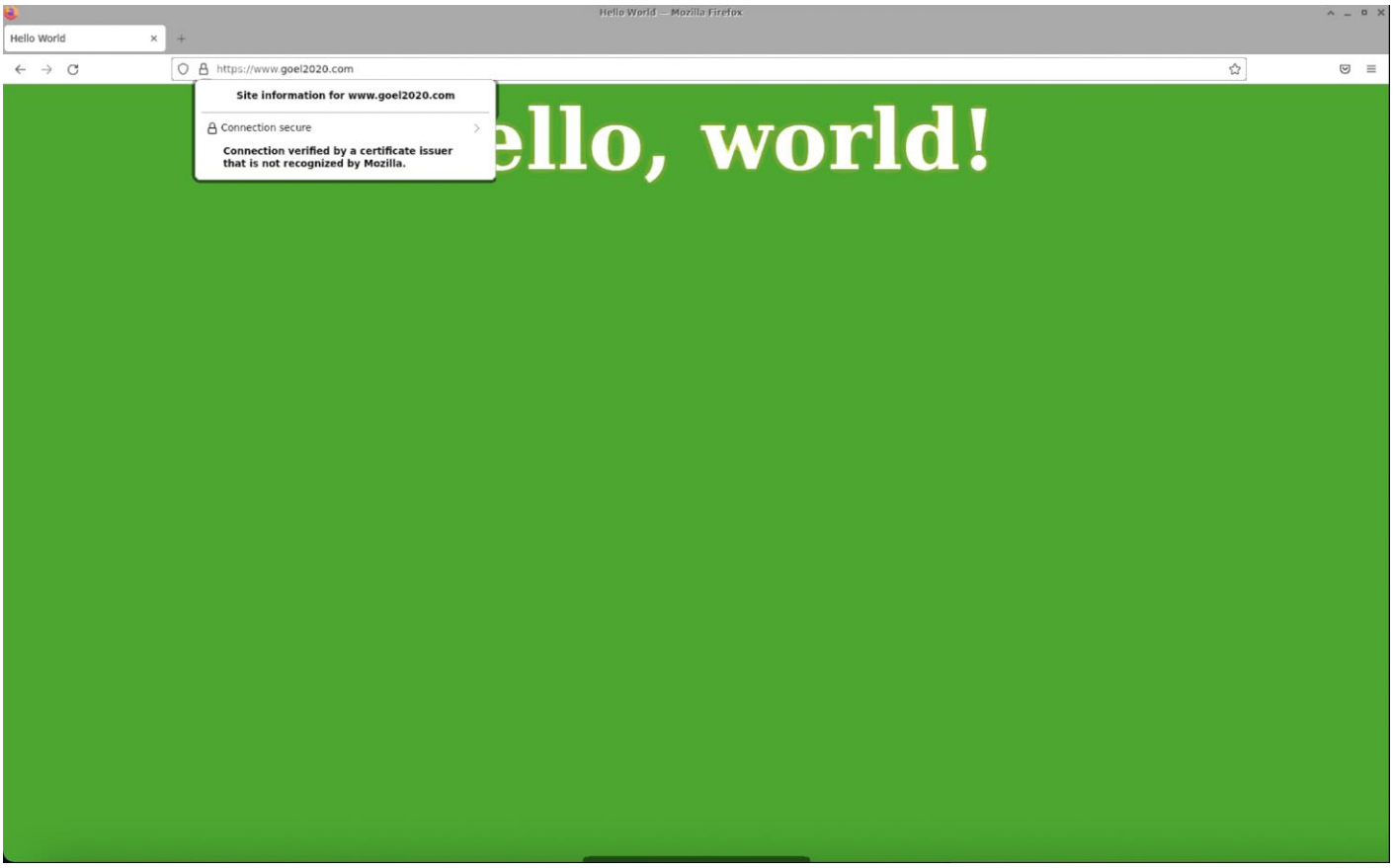
Checking certificate authority:

We can see that we are added as a certificate authority.



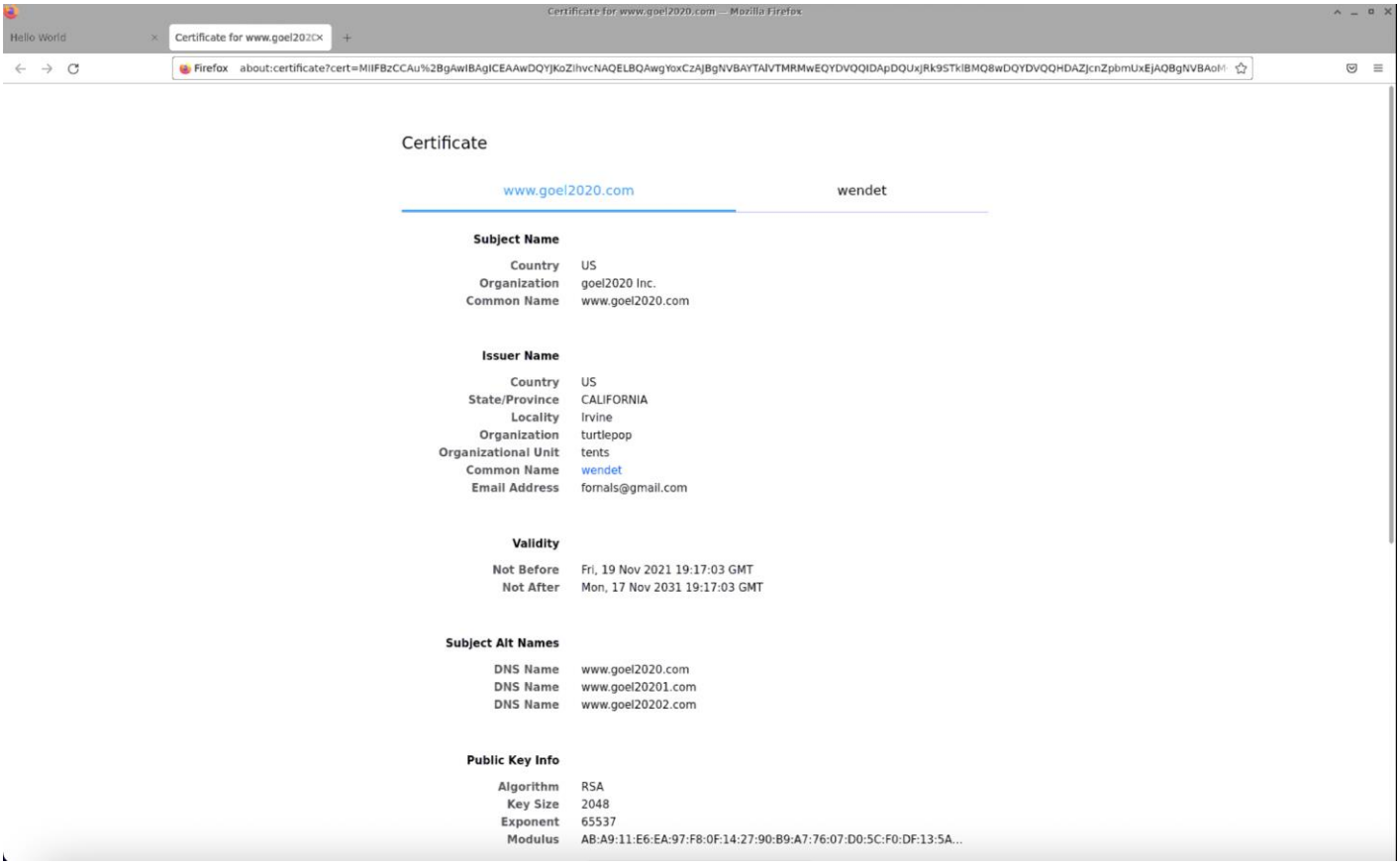
After adding our certificate, we can access the website directly with secure connection, since certificate is already added in trusted certificates.

This the website after adding the certificate



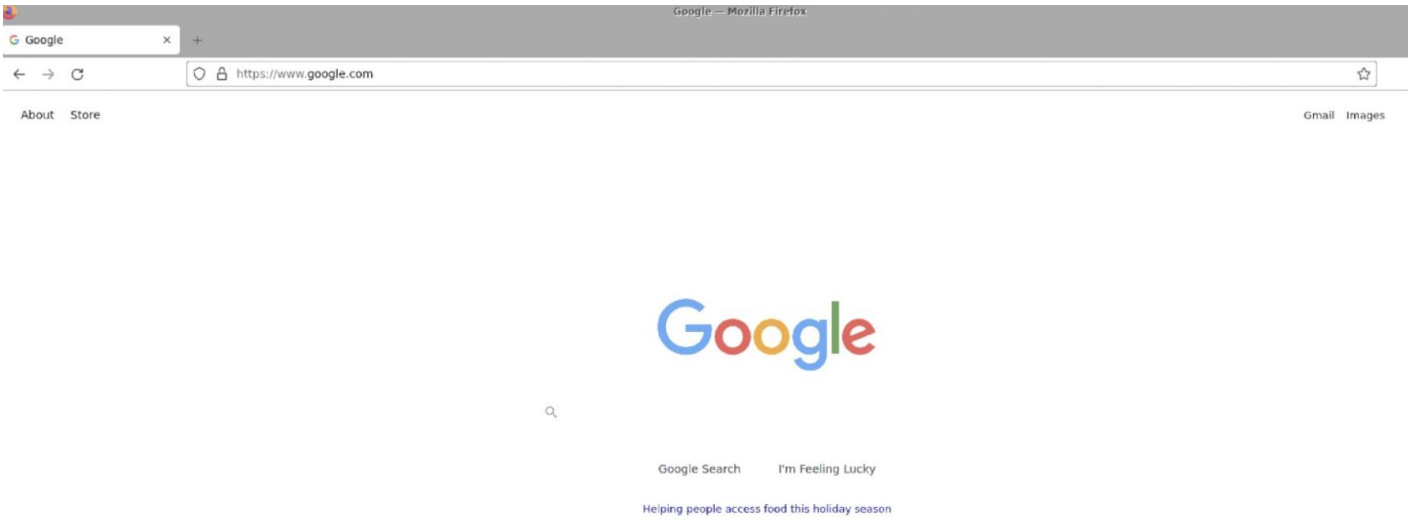
We can now securely access the website as the certificate is successfully added.

This is our certificate.

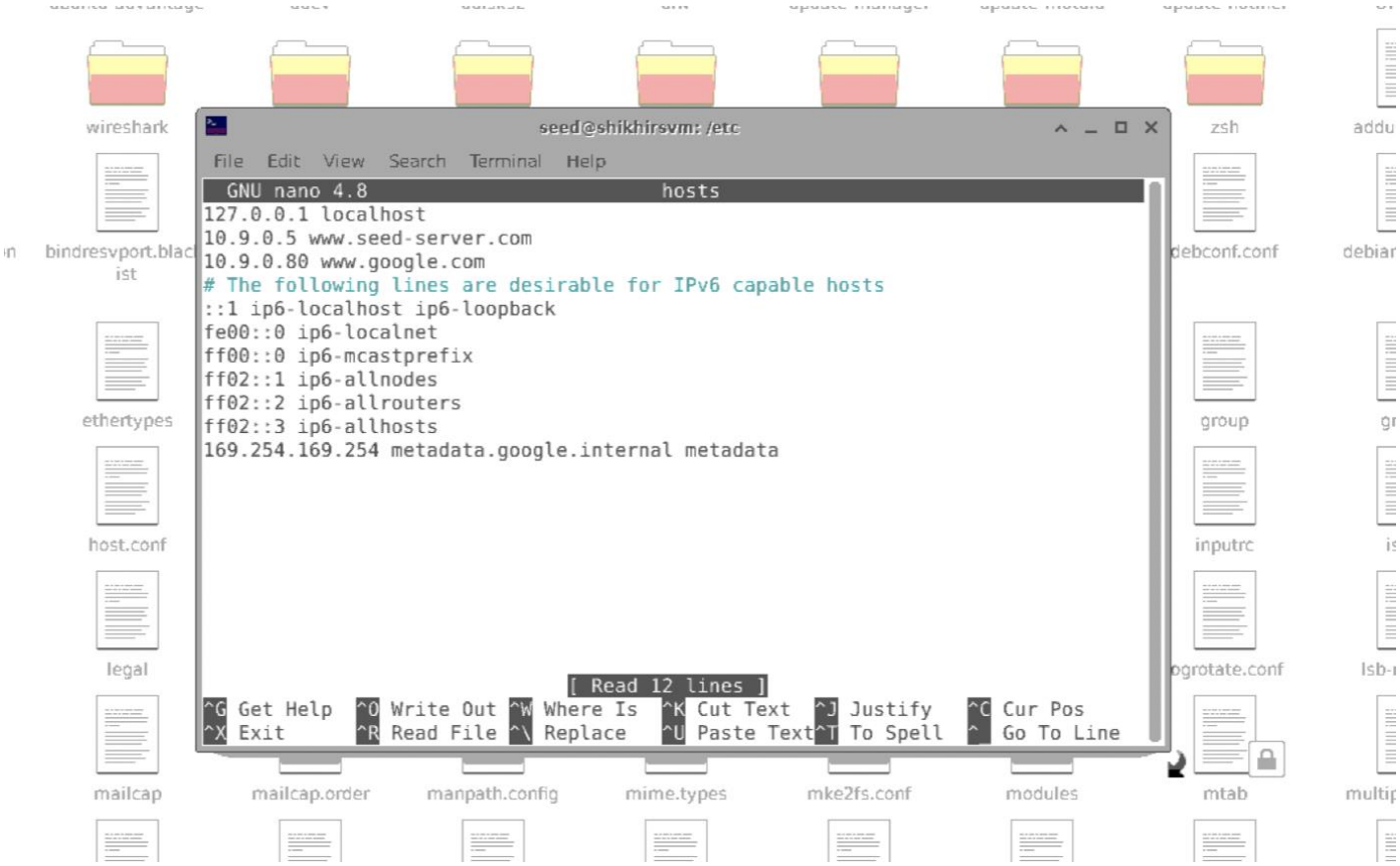


Task 5: Launching a Man-In-The-Middle Attack

We will be launching the man in the middle attack on google.com

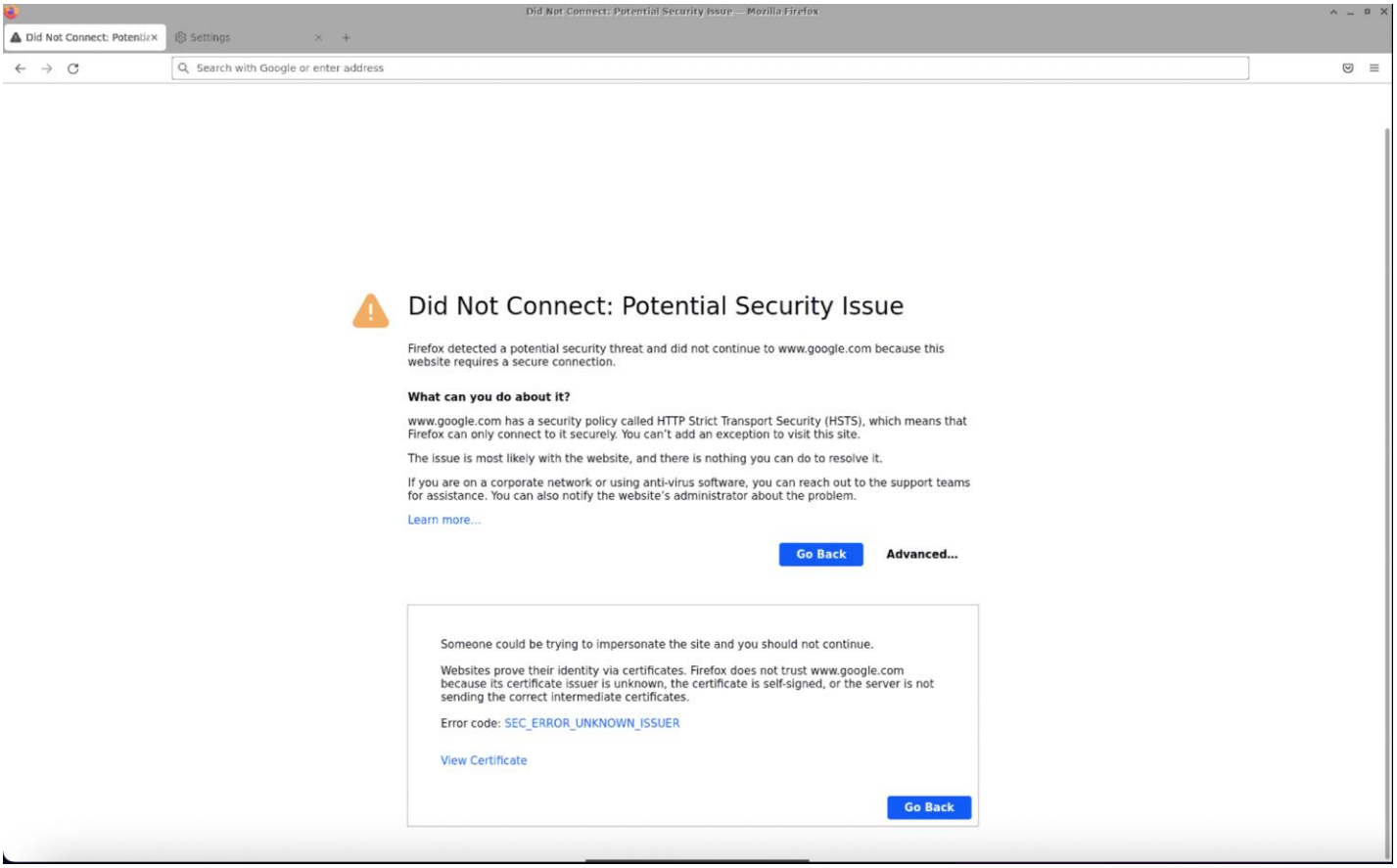


Adding google in out hosts file with an IP



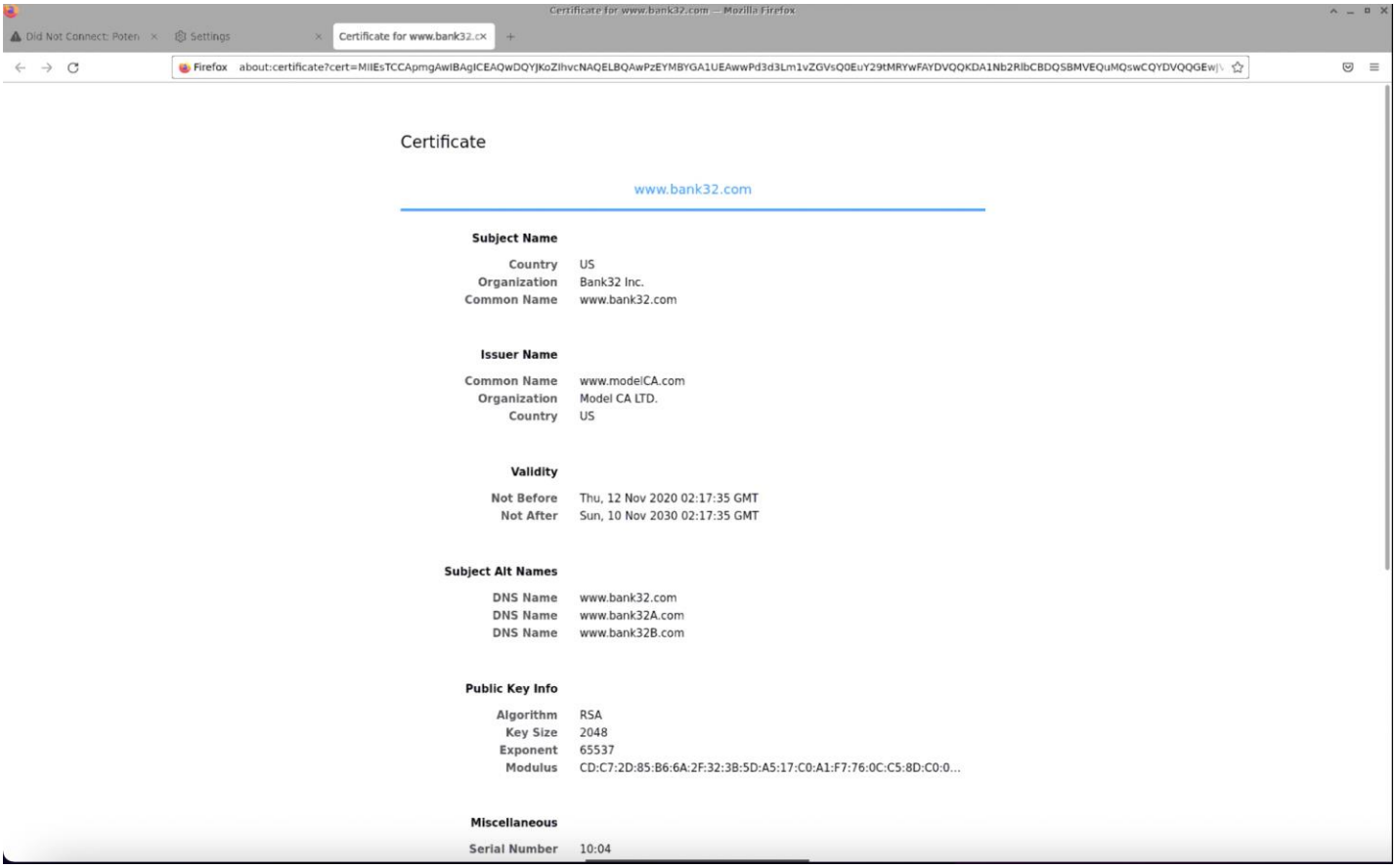
On attaching our certificate for goel2020.com with google (By changing the DNS Cache) we see that we are unable to access google. As the certificate is not trusted by the browser.

Common name of the certificate does not match with the requested url.



The attack fails as the user is warned about the security risk, the user is still unable to access the website and the attacker cannot gain control.

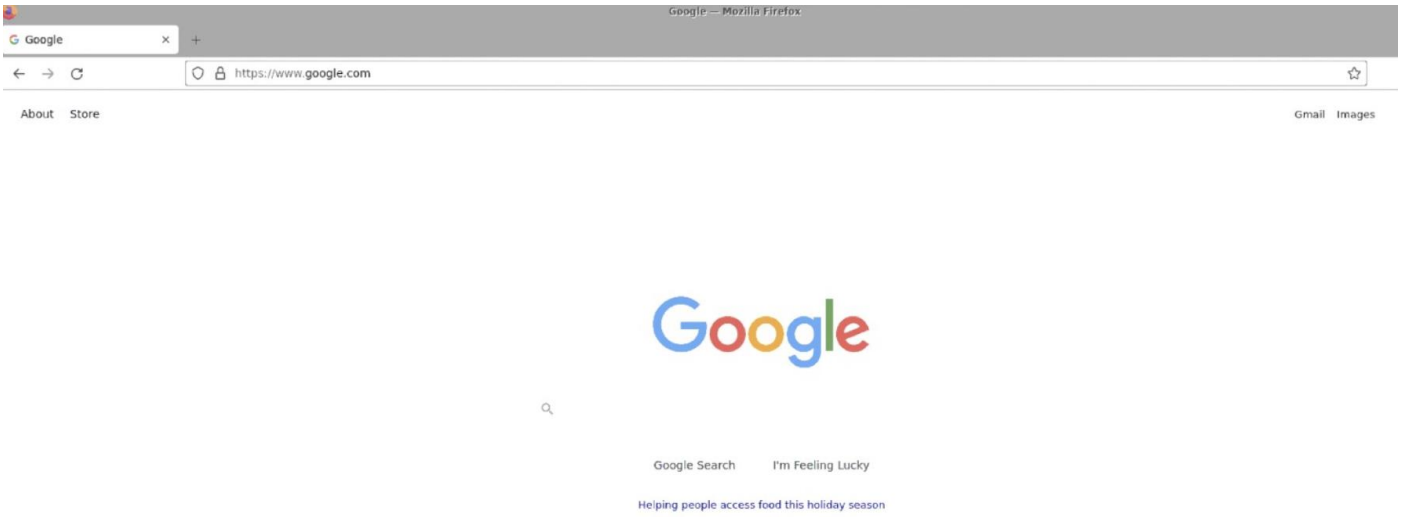
This is out certificate connected with google.



```
root@eb0c430d45c3: /
File  Edit  View  Search  Terminal  Tabs  Help
seed@shikhirsvm:~/security/project8/Labsetup$ cd etc
bash: cd: etc: No such file or directory
seed@shikhirsvm:~/security/project8/Labsetup$ dockps
737b171cf772  mysql-10.9.0.6
eb0c430d45c3  www-10.9.0.80
seed@shikhirsvm:~/security/project8/Labsetup$ docksh eb
root@eb0c430d45c3:/# service apache2 stop
 * Stopping Apache httpd web server apache2
 *
root@eb0c430d45c3:/#
```

Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

This is how google looks without launching the Man in The Middle attack.



Creating server.csr for google.com. Similarly, as Task 2.

```
seed@shikhirsvm: ~/security/Labsetup
File  Edit  View  Search  Terminal  Help
seed@shikhirsvm:~/security/Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyou
t server.key -out server.csr -subj "/CN=www.google.com/O=google Inc./C=US" -pass
out pass:dees
Generating a RSA private key
..............................+++++
.....................................................................................
.......................................................+++++
writing new private key to 'server.key'
-----
seed@shikhirsvm:~/security/Labsetup$
```

Seeing the server.csr using the req command.

```
seed@shikhirsvm:~/security/Labsetup$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.google.com, O = google Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c6:b0:aa:59:c9:95:bf:2a:11:74:2e:c1:84:12:
                    e4:b0:77:cb:fc:30:e9:66:a5:74:bf:89:56:78:a4:
                    0d:03:cb:15:5b:dc:82:07:cb:36:27:d8:5d:04:5d:
                    7f:5b:12:ac:db:97:ea:64:07:b8:08:fd:37:57:cf:
                    75:d3:f9:72:8e:3e:a2:16:bf:80:50:36:31:28:b0:
                    79:74:28:1f:93:cb:08:f6:97:6f:48:a2:00:de:9c:
                    66:13:7b:43:83:2e:f8:ba:ba:f1:71:4d:b2:fd:99:
                    15:a1:da:e7:85:52:48:89:61:29:46:c9:fe:f8:50:
                    7e:e8:6f:90:95:44:df:46:ca:15:3f:37:ed:f2:4c:
                    21:0f:5a:b8:d8:81:fc:e3:d8:48:2a:7e:39:b5:ec:
                    83:b6:9e:cd:c5:79:c8:88:3e:79:ce:53:84:1f:38:
                    c5:42:97:70:df:11:4f:c4:68:17:0d:23:86:a1:ee:
                    ec:f9:7d:bd:b2:f1:e1:1f:40:6d:7e:08:7b:5f:02:
                    2b:6d:a2:2c:0a:fb:60:03:47:fd:20:cf:b3:cd:66:
                    f3:28:ea:d0:73:c5:c3:46:80:2b:9c:9c:2d:66:aa:
                    2c:95:de:f8:19:79:47:13:e4:29:79:02:09:c1:d2:
                    a7:49:cd:19:10:0c:66:eb:a1:f6:c8:9f:70:ff:ea:
                    80:2f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         80:94:6a:46:d7:ab:0d:42:b6:57:79:07:ae:26:7b:89:64:27:
         62:af:15:99:9f:a2:b3:01:bf:34:13:04:2b:40:63:05:37:f6:
         c4:86:5c:7c:24:a5:a2:1a:40:63:5a:b5:60:58:78:80:15:54:
         6d:c7:f9:10:19:43:38:cd:58:06:5f:ed:eb:6e:40:81:2e:58:
         c7:6f:e6:eb:52:cd:1f:38:36:d8:61:fe:94:3d:da:fd:54:cb:
         f8:89:92:1a:c6:c6:76:b8:93:dc:9f:4f:c0:5b:1b:c0:7a:3f:
         0a:22:61:0a:3a:be:00:36:94:1a:fd:46:56:36:1e:ac:d3:18:
         d2:69:c3:13:75:af:56:46:44:d6:d1:41:71:56:d9:b9:a3:0b:
         af:07:a4:fc:0b:f3:93:11:88:f2:40:73:7e:4e:e8:0b:39:c7:
         ba:8b:ef:c1:e8:79:1e:b4:aa:c8:85:42:b6:90:b5:d5:ba:32:
         0a:5c:7b:9a:09:b4:0e:ce:32:7d:ff:18:36:50:d4:b7:bb:26:
         82:13:27:dd:8d:99:d6:ef:5f:a3:0f:e7:7a:89:0a:0d:da:05:
         5b:42:b4:84:49:24:7e:35:dd:e4:02:75:1f:6a:b6:4f:30:c8:
         d7:6a:7b:a7:13:8e:6a:dc:d1:32:13:7b:3c:89:21:38:28:94:
         4f:fb:be:e0
```

Here we see the server.key using rsa

```
seed@shikhirsvm:~/security/Labsetup$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:c6:b0:aa:59:c9:95:bf:2a:11:74:2e:c1:84:12:
    e4:b0:77:cb:fc:30:e9:66:a5:74:bf:89:56:78:a4:
    0d:03:cb:15:5b:dc:82:07:cb:36:27:d8:5d:04:5d:
    7f:5b:12:ac:db:97:ea:64:07:b8:08:fd:37:57:cf:
    75:d3:f9:72:8e:3e:a2:16:bf:80:50:36:31:28:b0:
    79:74:28:1f:93:cb:08:f6:97:6f:48:a2:00:de:9c:
    66:13:7b:43:83:2e:f8:ba:ba:f1:71:4d:b2:fd:99:
    15:a1:da:e7:85:52:48:89:61:29:46:c9:fe:f8:50:
    7e:e8:6f:90:95:44:df:46:ca:15:3f:37:ed:f2:4c:
    21:0f:5a:b8:d8:81:fc:e3:d8:48:2a:7e:39:b5:ec:
    83:b6:9e:cd:c5:79:c8:88:3e:79:ce:53:84:1f:38:
    c5:42:97:70:df:11:4f:c4:68:17:0d:23:86:a1:ee:
    ec:f9:7d:bd:b2:f1:e1:1f:40:6d:7e:08:7b:5f:02:
    2b:6d:a2:2c:0a:fb:60:03:47:fd:20:cf:b3:cd:66:
    f3:28:ea:d0:73:c5:c3:46:80:2b:9c:9c:2d:66:aa:
    2c:95:de:f8:19:79:47:13:e4:29:79:02:09:c1:d2:
    a7:49:cd:19:10:0c:66:eb:a1:f6:c8:9f:70:ff:ea:
    80:2f
publicExponent: 65537 (0x10001)
privateExponent:
    35:23:da:eb:d8:b6:6c:42:5c:18:ae:c8:a3:02:4a:
    97:c7:f2:8e:a8:a6:44:05:cc:8b:cd:b7:8a:dc:95:
    7e:86:3a:58:2f:49:b7:bb:e9:e8:0e:3e:12:84:cf:
    23:14:83:96:d7:b2:a0:be:4f:c2:57:b7:0d:8d:36:
    fe:52:a1:08:da:47:8f:bd:f8:1b:7b:e2:f9:f6:f9:
    04:d0:16:61:f8:d3:94:e0:3b:ab:39:68:f2:20:f2:
    4c:13:93:a2:ea:55:2b:dc:03:e7:41:d8:b5:6a:d4:
    16:4d:ed:ce:02:8b:d3:f2:60:8f:c6:46:a3:33:24:
    3e:16:58:9d:13:a6:83:cf:df:eb:03:98:26:77:d5:
    11:3f:02:6b:b4:59:47:96:2f:2a:cb:57:9f:5e:bd:
    70:e0:d9:71:8d:0f:18:8e:2a:47:c8:92:88:51:f6:
    05:78:7e:c5:49:1d:e7:aa:59:a0:b4:c7:2d:92:b4:
    14:d4:1a:34:1d:17:e9:5b:44:83:e5:e7:68:dd:01:
    7e:2c:50:71:e0:70:8f:09:1b:bc:79:53:7d:77:d1:
    99:26:c8:b5:dc:83:f3:06:63:80:c0:b1:76:3b:79:
    9d:21:05:f2:57:64:f9:35:fe:13:18:1b:6a:ec:eb:
    41:cf:2f:e8:83:8e:0b:f5:df:0b:2b:b8:55:c9:0a:
    c1
prime1:
    00:e2:0b:fa:d0:2d:23:f2:90:65:84:55:94:a4:9b:
    ef:79:d2:09:93:2e:d2:c0:3e:40:f0:c1:ba:4d:65:
    e1:9b:1c:5f:1a:54:99:10:72:a6:eb:cb:fe:84:18:
    44:f0:40:77:70:73:ba:14:81:c2:cd:cc:96:d8:ae:
    ba:6e:42:be:c9:fb:f9:e1:f6:e1:bd:bc:6e:f7:2b:
    b9:b3:2c:73:29:ce:5a:36:ae:79:39:f1:0e:3b:2d:
    b4:db:e8:3a:fe:0e:aa:8e:37:3d:f5:91:1b:5f:f4:
    b5:7b:58:46:e2:e7:c8:e5:6d:95:a9:12:94:b3:51:
    8c:0a:57:fa:46:f3:c3:9a:f5
prime2:
    00:e1:04:af:39:6e:75:f2:4e:86:9e:90:61:c3:5e:
```

Creating server.crt for google.com

```
seed@shikhirsvm: ~/security
File  Edit  View  Search  Terminal  Help
seed@shikhirsvm:~/security$ cp /usr/lib/ssl/openssl.cnf
cp: missing destination file operand after '/usr/lib/ssl/openssl.cnf'
Try 'cp --help' for more information.
seed@shikhirsvm:~/security$ cp /usr/lib/ssl/openssl.cnf openssl.cnf
seed@shikhirsvm:~/security$ cd Labsetup
seed@shikhirsvm:~/security/Labsetup$ ls
docker-compose.yml  image_www  mysql_data  volumes
seed@shikhirsvm:~/security/Labsetup$ ls
docker-compose.yml  image_www  mysql_data  volumes
seed@shikhirsvm:~/security/Labsetup$ cd ..
seed@shikhirsvm:~/security$ ls
Labsetup  Labsetup.zip  ca.key  openssl.cnf
seed@shikhirsvm:~/security$ mkdir demoCA
seed@shikhirsvm:~/security$ cd demoCA
seed@shikhirsvm:~/security/demoCA$ mkdir certs crl newcerts
seed@shikhirsvm:~/security/demoCA$ touch index.txt serial
seed@shikhirsvm:~/security/demoCA$ echo 1000 > serial
seed@shikhirsvm:~/security/demoCA$ ls
certs  crl  index.txt  newcerts  serial
seed@shikhirsvm:~/security/demoCA$ cd ..
seed@shikhirsvm:~/security$ ls
```

Checking the server.crt for google.com

```
seed@shikhirsvm:~/security/project8/Labsetup$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CALIFORNIA, L = Irvine, O = turtlepop, OU = tents, CN = wendet, emailAddress = fornals@gmail.com
        Validity
            Not Before: Nov 19 22:58:03 2021 GMT
            Not After : Nov 17 22:58:03 2031 GMT
        Subject: C = US, O = google Inc., CN = www.google.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c6:b0:aa:59:c9:95:bf:2a:11:74:2e:c1:84:12:
                    e4:b0:77:cb:fc:30:e9:66:a5:74:bf:89:56:78:a4:
                    0d:03:cb:15:5b:dc:82:07:cb:36:27:d8:5d:04:5d:
                    7f:5b:12:ac:db:97:ea:64:07:b8:08:fd:37:57:cf:
                    75:d3:f9:72:8e:3e:a2:16:bf:80:50:36:31:28:b0:
                    79:74:28:1f:93:cb:08:f6:97:6f:48:a2:00:de:9c:
                    66:13:7b:43:83:2e:f8:ba:ba:f1:71:4d:b2:fd:99:
                    15:a1:da:e7:85:52:48:89:61:29:46:c9:fe:f8:50:
                    7e:e8:6f:90:95:44:df:46:ca:15:3f:37:ed:f2:4c:
                    21:0f:5a:b8:d8:81:fc:e3:d8:48:2a:7e:39:b5:ec:
                    83:b6:9e:cd:c5:79:c8:88:3e:79:ce:53:84:1f:38:
                    c5:42:97:70:df:11:4f:c4:68:17:0d:23:86:a1:ee:
                    ec:f9:7d:bd:b2:f1:e1:1f:40:6d:7e:08:7b:5f:02:
                    2b:6d:a2:2c:0a:fb:60:03:47:fd:20:cf:b3:cd:66:
                    f3:28:ea:d0:73:c5:c3:46:80:2b:9c:9c:2d:66:aa:
                    2c:95:de:f8:19:79:47:13:e4:29:79:02:09:c1:d2:
                    a7:49:cd:19:10:0c:66:eb:a1:f6:c8:9f:70:ff:ea:
                    80:2f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                A4:77:95:92:23:67:00:BE:A4:88:A8:FF:2F:8D:74:C0:F5:D1:0E:2C
            X509v3 Authority Key Identifier:
                keyid:FF:F4:02:8D:3E:31:18:AF:FB:AD:90:4E:47:A0:69:FD:ED:7B:9A:44

    Signature Algorithm: sha256WithRSAEncryption
         aa:11:20:16:8e:f0:b0:91:4c:95:7b:27:8e:03:da:b6:fe:12:
         8e:0b:ed:74:e9:a4:38:9a:79:54:50:f5:34:12:dd:7b:10:ce:
         63:40:c7:55:0d:c1:55:a1:43:83:3a:b5:b1:d9:a1:36:ae:c4:
         e2:25:00:11:1c:84:1b:9a:21:e9:eb:64:8c:5e:d0:ce:48:ce:
         1f:44:bc:97:fd:94:e0:aa:1d:da:ea:ec:df:af:b0:ec:d4:42:
         34:50:a7:0b:3d:a6:c9:a6:b7:bd:ab:e5:c1:d2:2f:bd:34:87:
         4e:b7:73:ec:81:65:3c:3a:71:db:bf:21:f6:00:5d:e9:14:b7:
         ca:d7:c8:da:cd:35:65:51:a4:2d:b5:3d:ab:4b:ff:6f:54:aa:
         c9:5d:be:ca:b1:06:f3:7b:cd:2e:29:ed:24:d3:12:da:13:f2:
         80:92:a2:66:b5:b6:00:a2:7e:d0:8c:f9:79:36:06:91:4a:77:
         0d:a9:6e:c5:a1:a5:ed:e9:98:b2:02:9f:cf:0a:d3:6f:e0:e2:
         72:a5:5f:29:5c:48:35:29:ed:7d:de:38:d2:e9:fe:74:b9:cb:
```

Changing the Sites-available files in apache2 and updating the DNS-Cache.

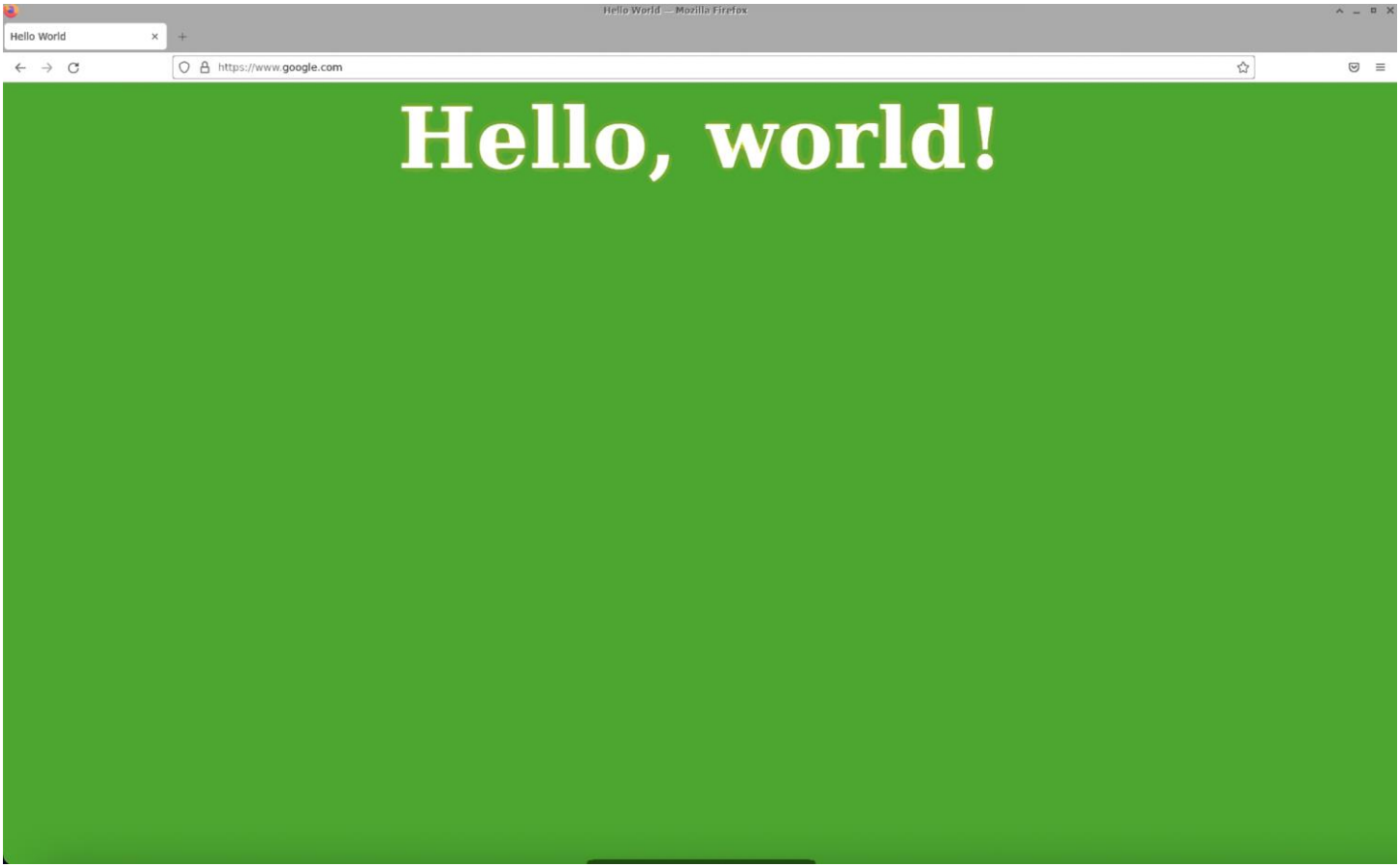
```
image_www   volumes   ca.crt   ca.key   docker-compose.yml   openssl.cnf   server.crt   server.csr   server.key
```

```
root@eb0c430d45c3: /etc/apache2/sites-available
File  Edit  View  Search  Terminal  Help
  GNU nano 4.8                    shikhir.conf
<VirtualHost *:443>
    DocumentRoot /var/www/shikhir123
    ServerName www.google.com
    ServerAlias www.goel2020.com
    ServerAlias www.goel20201.com
    ServerAlias www.goel20202.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/shikhir123
    ServerName www.goel2020.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
                          [ Read 20 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

This is google.com after connecting out duplicate certificate for google. This time the attack would work as our certificate matches the requested url.



We can conclude that our attack is successful as we have modified the user’s access by changing the landing page to our own landing page. The attacker successfully gains control.