Laboratory Report

Public-Key Infrastructure

The laboratory prompt for this was provided by SEED Security Labs. SEED Security Labs is a project focused on enhancing cybersecurity education through hands-on laboratory exercises. Visit them at https://seedsecuritylabs.org/.

Ramnick Francis P. Ramos
+63 960 277 1720
ramnickfrancisramos@gmail.com

Cybersecurity Portfolio
October 2, 2025

Public-Key Infrastructure

Ramnick Francis P. Ramos
ramnickfrancisramos@gmail.com

Introduction **2**
Environment Setup **3**
Container Setup and Commands 3
DNS Setup 3
Laboratory Tasks and Execution **4**
Becoming a Certificate Authority (CA) 4
Creating the Configuration File openssl.conf 4
Creation of Certificate Authority 5
Task 1 Questions 12
Generating a Certificate Request for Your Web Server 16
POINT OF CONFUSION 21
Generating a Certificate for your server 21
Deploying Certificate in an Apache-Based HTTPS Website 25
Launching a Man-In-The-Middle Attack 30
Setting up the malicious website 30
Becoming the Man in The Middle 30
Launching a Man-In-The-Middle Attack with a Compromised CA 31
Challenges and Troubleshooting **34**
Discussion **34**
References **34**

Introduction

Public key cryptography is utilized nowadays to enable the secure exchange of messages between sender and receiver (Du, 2018). However, they are subject to the vulnerability of man-in-the-middle attacks. This laboratory report aims to explore the different aspects of public key infrastructure which aims to provide a solution on the vulnerabilities of public key cryptography. Specifically, this laboratory report will be expounding the following:

- Public-key encryption, Public-Key Infrastructure (PKI);
- Certificate Authority (CA), X.509 certificate, and root CA;
- Apache, HTTP, and HTTPS; and
- Man-in-the-middle attacks.
-

This in-class draft of the laboratory report will only be discussing the first three tasks of the laboratory prompt from SEED Labs.

Environment Setup

Container Setup and Commands

Docker was also used to make the lab environment for this exercise. This exercise requires the use of a container from task 4 onwards.

For the commands, the following aliases were used: dcbuild for building the container; dcup for running the container; and dcdown for closing the containers. Seen in the figures below are sample runs of the Docker container.

```
[09/29/25]seed@VM:~/.../Labsetup$ dcbuild
Building web-server
Step 1/7 : FROM handsonsecurity/seed-server:apache-php
 ---> 2365d0ed3ad9
Step 2/7 : ARG WWWDIR=/var/www/bank32
 ---> Running in 5d9e0774a796
Removing intermediate container 5d9e0774a796
 ---> edd9897cfd25
Step 3/7 : COPY ./index.html ./index_red.html $WWWDIR/
 ---> ef7a3a6167b8
Step 4/7 : COPY ./bank32_apache_ssl.conf /etc/apache2/sites-available
 ---> 493c6a9fbcba
Step 5/7 : COPY ./certs/bank32.crt ./certs/bank32.key  /certs/
 ---> 98bcef69a360
Step 6/7 : RUN  chmod 400 /certs/bank32.key      && chmod 644 $WWWDIR/index.html      && chmod 644 $WWWD
/index_red.html      && a2ensite bank32_apache_ssl
 ---> Running in c6cbf1acbc6c
Enabling site bank32_apache_ssl.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container c6cbf1acbc6c
 ---> 919e1862f259
```

Figure 1. Building the Docker Container

```
[09/29/25]seed@VM:~/.../Labsetup$ dcup
WARNING: Found orphan containers (victim-10.9.0.80) for this project. If you removed or renamed this servi
ce in your compose file, you can run this command with the --remove-orphans flag to clean it up.
Creating www-10.9.0.80 ... done
Attaching to www-10.9.0.80
```

Figure 2. Running the Docker Container

```
[09/29/25]seed@VM:~/.../Labsetup$ dockps
30265b050d7b  www-10.9.0.80
[09/29/25]seed@VM:~/.../Labsetup$
```

Figure 3. The Docker Container

DNS Setup

The laboratory environment will also be requiring the revision of the etc/hosts. The editing of /etc/hosts was frequently done in some parts of the laboratory.

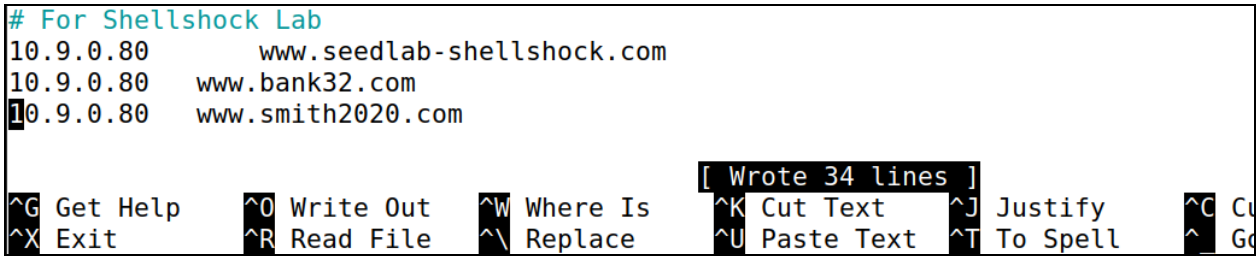

Figure 4. Changing the /etc/hosts

Laboratory Tasks and Execution

Becoming a Certificate Authority (CA)

This task aims to simulate becoming root CA for a system. “The certificate generation tasks will be conducted on the VM, but we will use a container to host the web server.”

Creating the Configuration File openssl.conf

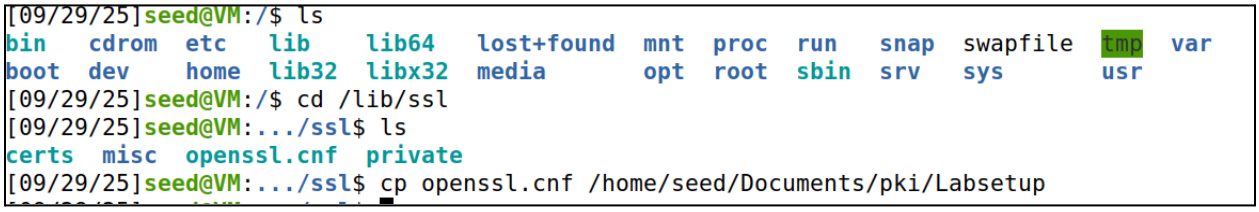

Figure 5. Copying the configuration file to the current working directory

For this task, we will copy the configuration file from usr/lib/ssl/openssl.cnf to our current working directory and instruct the system to use it as the configuration file (See Figure 5).

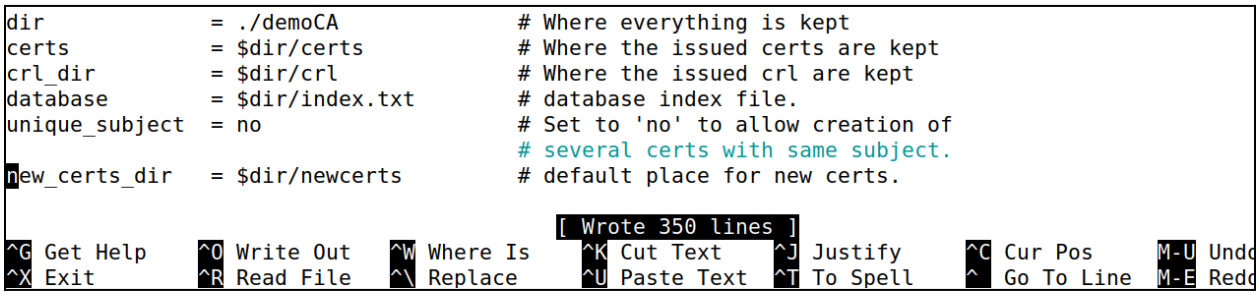

Figure 6. Editing the Configuration File

We will then edit the configuration file to remove the comment on unique_subject.

```
[09/29/25]seed@VM:~/.../work_dir$ mkdir demoCA
[09/29/25]seed@VM:~/.../work_dir$ mkdir certs
[09/29/25]seed@VM:~/.../work_dir$ mkdir crl
[09/29/25]seed@VM:~/.../work_dir$ mkdir newcerts
[09/29/25]seed@VM:~/.../work_dir$ touch serial
[09/29/25]seed@VM:~/.../work_dir$ nano serial
[09/29/25]seed@VM:~/.../work_dir$ cat serial
1000
[09/29/25]seed@VM:~/.../work_dir$
```

Figure 7. Setting up the demoCA directory.

Seen on Figure 7, the directories needed in the configuration file was created. Certs, crl, and newcerts directories were later moved under the demoCA using the File explorer's interface of Linux System.

Creation of Certificate Authority

This subtask aims to use openssl to first generate the self-signed certificate (csr) for the CA.

```
[09/29/25]seed@VM:~/.../work_dir$ 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
```

Figure 8. Generating a self-signed certificate for the CA. The PEM Pass Phrase used is **dees.**

For this certificate, and all certificates that was used throughout the laboratory report, the pass phrase dees was used.

```
[09/29/25]seed@VM:~/.../work_dir$ ls
ca.crt  ca.key  certs  crl  demoCA  index.txt  newcerts  openssl.cnf  serial
[09/29/25]seed@VM:~/.../work_dir$
```

Figure 9. Current working directory after generating the self-assigned certificate.

```
[09/29/25]seed@VM:~/.../work_dir$ cat ca.crt
-----BEGIN CERTIFICATE-----
MIIF/TCCA+WgAwIBAgIUMiI8b7Ie9XQGL5fDyL7Q0FZhWF4wDQYJKoZIhvcNAQEL
BQAwgY0xCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMQ0wCwYDVQQH
DARjaXR5MSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxEDAOBgNV
BAsMB3NlY3Rpb24xDTALBgNVBAMMBG5hbWUxFjAUBgkqhkiG9w0BCQEWB2FkZHJl
c3MwHhcNMjUwOTI5MDYzODU4WhcNMzUwOTI3MDYzODU4WjCBjTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDTALBgNVBAcMBGNpdHkxITAfBgNVBAoM
```


```
[09/29/25]seed@VM:~/.../work_dir$ cat ca.crt
-----BEGIN CERTIFICATE-----
MIIF/TCCA+WgAwIBAgIUMiI8b7Ie9XQGL5fDyL7Q0FZhWF4wDQYJKoZIhvcNAQEL
BQAwgY0xCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMQ0wCwYDVQQH
DARjaXR5MSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxEDAOBgNV
BAsMB3NlY3Rpb24xDTALBgNVBAMMBG5hbWUxFjAUBgkqhkiG9w0BCQEWB2FkZHJl
c3MwHhcNMjUwOTI5MDYzODU4WhcNMzUwOTI3MDYzODU4WjCBjTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDTALBgNVBAcMBGNpdHkxITAfBgNVBAoM
```


Figure 10. Contents of ca.crt and ca.key

Seen in Figure 10 are the decoded continents of the ca.crt and the ca.key.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3
650 \-keyout ca.key -out ca.crt  \-subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" \
-passout pass:cyber
Generating a RSA private key
..............................++++
.....................................................................................
.....................................................................................
.....................................................................................
..............++++
writing new private key to 'ca.key'
-----
[09/29/25]seed@VM:~/.../work_dir$
```

Figure 11. Changing -subj field of the certificate using included -passout pass phrase in the command.

Figure 11 shows that details of they key can be changed using the -passout option.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:ba:a9:c4:87:4a:31:f7:de:db:c9:2c:5c:1c:e3:36:65:30:1a:6e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
```

Figure 12. Decoded contents of ca.crt

Shown below is the complete content of the **ca.crt.**

```
[09/29/25]seed@VM:~/.../work_dir$ openssl x509 -in ca.crt -text
```

```
-noout
Certificate:
      Data:
      Version: 3 (0x2)
      Serial Number:

36:ba:a9:c4:87:4a:31:f7:de:db:c9:2c:5c:1c:e3:36:65:30:1a:6e
      Signature Algorithm: sha256WithRSAEncryption
      Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
      Validity
            Not Before: Sep 29 06:40:25 2025 GMT
            Not After : Sep 27 06:40:25 2035 GMT
      Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
      Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                  RSA Public-Key: (4096 bit)
                  Modulus:
                        00:e1:d8:7f:a7:66:bc:42:ad:82:7d:07:4e:42:e6:
                        43:7b:f7:92:09:f7:8b:ad:4b:98:68:3f:44:b3:4e:
                        59:df:8a:9d:2b:83:7e:ff:29:f8:8a:cf:e4:8c:42:
                        38:88:17:15:f4:93:49:e1:0d:f9:f2:d8:0d:b9:37:
                        c5:ef:4e:9c:6f:19:07:d5:19:f7:f3:53:35:4a:91:
                        01:2b:ee:68:36:0b:bc:49:36:08:58:54:41:58:b1:
                        15:41:4e:ae:6d:0a:df:9a:c9:d0:24:4f:22:c3:6e:
                        ec:37:d2:43:26:96:6e:a1:2e:dd:06:76:6e:bc:b5:
                        6f:d1:7b:0e:31:f4:d3:f4:68:f7:40:0a:be:37:3c:
                        a7:65:7d:3c:24:08:5b:82:78:9a:e3:83:28:ff:0b:
                        91:21:b4:28:80:cb:bd:ba:96:e6:36:c0:64:5f:35:
                        72:5d:45:c7:e3:34:f8:05:6e:08:18:5c:55:74:58:
                        51:4c:11:f4:16:9d:a9:db:6c:0a:e7:2f:04:18:2d:
                        a0:f1:d0:9e:c7:19:78:18:13:e4:55:a5:94:67:27:
                        18:55:55:b2:a1:10:77:e5:9e:0b:2b:31:ac:9d:8e:
                        03:54:e2:c2:ec:32:ba:63:40:8a:2a:08:dd:26:29:
                        30:ac:22:d0:e2:35:c4:60:bd:7f:aa:16:d5:8a:c3:
                        c6:85:78:e5:94:b4:1e:60:44:fa:a1:c6:c2:d0:76:
                        db:51:7b:bf:97:c4:0a:35:f0:8f:8c:66:ad:ad:32:
                        91:5f:09:05:73:0b:43:69:c5:c5:80:6c:76:c7:3b:
                        5c:7a:5b:be:51:e9:c0:b0:e1:6f:f6:66:fd:a6:0d:
                        ee:62:6b:b8:2c:17:24:f7:6e:3f:c8:18:2d:61:2d:
                        f5:d4:c2:74:be:a1:82:1c:25:0e:46:0d:4c:aa:e6:
                        d4:81:f4:aa:b6:30:6e:3d:89:fb:59:0c:ea:96:f7:
                        51:c8:ee:de:1b:8c:ad:fa:72:30:c0:5c:53:3c:3e:
                        34:dd:30:0a:32:df:2f:f9:aa:20:f0:70:d6:ee:1a:
                        c1:3a:fc:96:f2:e4:1c:75:7a:c3:d3:ae:cb:a5:2f:
                        39:63:14:62:89:26:2e:0a:c1:e7:81:24:a7:66:dc:
                        7d:45:89:ee:d6:e7:12:49:86:c7:e1:4e:ee:d3:1b:
                        80:a6:fc:e5:95:ad:f2:91:5b:68:1b:91:ad:6f:59:
                        63:cb:6a:b7:46:2e:f1:8b:fc:9d:48:2d:55:6e:6c:
                        b7:f9:ab:97:15:d2:48:cb:ed:87:9c:49:8c:b9:4b:
                        d1:38:f0:96:60:f7:34:50:73:14:7a:9d:28:99:a9:
                        d1:2a:4f:89:4b:4a:e6:24:fb:de:cf:4e:c5:91:74:
```

```
                    b7:84:1b
                Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:

CF:3B:C4:2E:A5:3F:C6:64:A4:5E:5E:85:7F:9A:EB:8A:2A:FA:23:8E
        X509v3 Authority Key Identifier:

keyid:CF:3B:C4:2E:A5:3F:C6:64:A4:5E:5E:85:7F:9A:EB:8A:2A:FA:23:8E

        X509v3 Basic Constraints: critical
            CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    d7:ec:ed:bc:13:76:7a:9f:4a:6f:45:63:67:fc:b7:0d:dc:00:
    e8:19:a2:0e:12:0f:81:69:84:4e:45:db:db:92:27:95:67:e7:
    ac:48:c1:2b:cf:84:a1:f4:c8:ad:a9:12:ea:57:ee:0d:ae:63:
    90:69:73:a4:c2:d1:a8:40:7e:16:1d:ab:37:66:f8:38:77:8b:
    33:fd:a3:7b:72:71:fb:65:55:b3:f3:4a:81:b5:16:8e:1d:b1:
    1c:bc:2d:49:f4:5e:3d:2a:45:02:d9:ae:f3:46:1b:8d:ad:57:
    1d:eb:5d:e9:73:a6:c6:18:44:2b:9e:9e:0e:71:9a:cd:20:89:
    30:ee:6d:f9:8a:31:31:71:7f:43:52:ec:11:0e:fc:b5:4f:26:
    71:7c:50:5b:35:e3:d7:d6:5c:49:22:05:9a:6e:41:85:12:ca:
    27:91:be:9d:be:92:55:98:80:c6:c4:3e:68:68:74:b7:1e:38:
    51:ca:64:36:ca:bd:29:8f:10:fc:19:60:cb:bd:76:5d:d4:b9:
    0d:14:e7:12:d0:7e:df:ea:c2:1d:1a:0d:79:8e:42:bf:e2:a3:
    2f:88:96:31:c0:d5:41:3a:c3:39:c2:f8:72:c6:6c:1f:76:a5:
    67:53:8a:98:4b:bd:3c:90:16:74:84:8a:6c:66:7f:d1:ca:b4:
    09:0d:d3:bd:b9:66:39:72:03:6e:1b:83:a8:ec:2f:53:18:c1:
    54:07:11:70:25:38:47:0f:9b:e7:a8:9a:4c:14:b0:f0:ba:63:
    28:71:38:b7:0a:48:e0:d8:77:bd:19:e4:1a:f0:71:3b:fc:91:
    cb:b0:9a:fc:35:c5:a0:23:9d:54:16:64:e5:9b:78:a7:23:e6:
    e4:1c:18:70:14:43:57:31:c2:cc:c6:a0:60:8f:c9:e7:94:18:
    55:6e:96:80:c6:22:ba:fc:dd:22:21:04:e1:41:5f:c9:c9:33:
    14:00:bf:33:84:a2:0b:37:76:0d:00:ba:fb:1b:9c:d2:9b:5c:
    76:e6:01:59:25:38:f4:92:ae:e0:11:17:1e:bd:04:f4:d3:a6:
    0c:e4:fd:c3:1a:94:e0:07:a9:9a:de:28:ea:7a:bf:36:35:df:
    bf:d7:5d:51:d0:db:5d:da:65:77:b9:0a:a1:d0:51:9c:5d:59:
    48:75:a9:23:c2:8b:4d:5b:c0:12:0b:94:87:a0:2f:d3:be:14:
    4a:1e:42:ad:6e:f3:01:db:ba:31:2d:70:a6:4a:c6:3b:af:1a:
    e3:26:dd:f8:16:38:a3:98:ab:d0:9d:e5:5b:30:0f:b5:90:35:
    51:60:a3:92:33:4e:f5:6f:ee:99:0d:24:f3:35:08:c5:1b:0f:
    e6:42:c0:7b:ca:90:d9:3f
[09/29/25]seed@VM:~/.../work_dir$
```

```
[09/29/25]seed@VM:~/.../work_dir$ openssl rsa  -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:e1:d8:7f:a7:66:bc:42:ad:82:7d:07:4e:42:e6:
    43:7b:f7:92:09:f7:8b:ad:4b:98:68:3f:44:b3:4e:
    59:df:8a:9d:2b:83:7e:ff:29:f8:8a:cf:e4:8c:42:
    38:88:17:15:f4:93:49:e1:0d:f9:f2:d8:0d:b9:37:
```

Figure 12. Decoded contents of ca.key

Shown below is the content of the **ca.key.**

```
[09/29/25]seed@VM:~/.../work_dir$ openssl rsa  -in ca.key -text
-noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
      00:e1:d8:7f:a7:66:bc:42:ad:82:7d:07:4e:42:e6:
      43:7b:f7:92:09:f7:8b:ad:4b:98:68:3f:44:b3:4e:
      59:df:8a:9d:2b:83:7e:ff:29:f8:8a:cf:e4:8c:42:
      38:88:17:15:f4:93:49:e1:0d:f9:f2:d8:0d:b9:37:
      c5:ef:4e:9c:6f:19:07:d5:19:f7:f3:53:35:4a:91:
      01:2b:ee:68:36:0b:bc:49:36:08:58:54:41:58:b1:
      15:41:4e:ae:6d:0a:df:9a:c9:d0:24:4f:22:c3:6e:
      ec:37:d2:43:26:96:6e:a1:2e:dd:06:76:6e:bc:b5:
      6f:d1:7b:0e:31:f4:d3:f4:68:f7:40:0a:be:37:3c:
      a7:65:7d:3c:24:08:5b:82:78:9a:e3:83:28:ff:0b:
      91:21:b4:28:80:cb:bd:ba:96:e6:36:c0:64:5f:35:
      72:5d:45:c7:e3:34:f8:05:6e:08:18:5c:55:74:58:
      51:4c:11:f4:16:9d:a9:db:6c:0a:e7:2f:04:18:2d:
      a0:f1:d0:9e:c7:19:78:18:13:e4:55:a5:94:67:27:
      18:55:55:b2:a1:10:77:e5:9e:0b:2b:31:ac:9d:8e:
      03:54:e2:c2:ec:32:ba:63:40:8a:2a:08:dd:26:29:
      30:ac:22:d0:e2:35:c4:60:bd:7f:aa:16:d5:8a:c3:
      c6:85:78:e5:94:b4:1e:60:44:fa:a1:c6:c2:d0:76:
      db:51:7b:bf:97:c4:0a:35:f0:8f:8c:66:ad:ad:32:
      91:5f:09:05:73:0b:43:69:c5:c5:80:6c:76:c7:3b:
      5c:7a:5b:be:51:e9:c0:b0:e1:6f:f6:66:fd:a6:0d:
      ee:62:6b:b8:2c:17:24:f7:6e:3f:c8:18:2d:61:2d:
      f5:d4:c2:74:be:a1:82:1c:25:0e:46:0d:4c:aa:e6:
      d4:81:f4:aa:b6:30:6e:3d:89:fb:59:0c:ea:96:f7:
      51:c8:ee:de:1b:8c:ad:fa:72:30:c0:5c:53:3c:3e:
      34:dd:30:0a:32:df:2f:f9:aa:20:f0:70:d6:ee:1a:
      c1:3a:fc:96:f2:e4:1c:75:7a:c3:d3:ae:cb:a5:2f:
      39:63:14:62:89:26:2e:0a:c1:e7:81:24:a7:66:dc:
      7d:45:89:ee:d6:e7:12:49:86:c7:e1:4e:ee:d3:1b:
      80:a6:fc:e5:95:ad:f2:91:5b:68:1b:91:ad:6f:59:
      63:cb:6a:b7:46:2e:f1:8b:fc:9d:48:2d:55:6e:6c:
      b7:f9:ab:97:15:d2:48:cb:ed:87:9c:49:8c:b9:4b:
      d1:38:f0:96:60:f7:34:50:73:14:7a:9d:28:99:a9:
```

```
     d1:2a:4f:89:4b:4a:e6:24:fb:de:cf:4e:c5:91:74:
     b7:84:1b
publicExponent: 65537 (0x10001)
privateExponent:
     45:18:09:25:db:c6:68:d7:d0:7e:13:c8:1b:ab:7a:
     a5:e8:7d:e3:52:ba:86:d0:03:d6:90:d4:a1:ce:ac:
     ac:39:2a:10:6f:f0:60:7c:24:af:c3:1e:76:d2:a3:
     9c:ef:03:26:8a:11:26:2b:32:76:db:26:87:ad:ca:
     7e:86:1c:51:d8:e4:8e:8b:9d:51:f1:f8:f1:d1:1e:
     fc:a3:b9:7a:1f:69:01:34:e8:a4:ad:52:38:a2:24:
     90:90:53:c8:c4:74:d8:54:39:bb:82:02:6e:ab:f6:
     d4:b5:1d:1a:27:17:bd:74:2a:e6:99:41:13:b6:a6:
     78:fe:1e:bf:a5:d9:5a:82:ea:71:cb:57:9a:6a:92:
     03:f8:a6:77:97:9e:f7:71:92:61:5c:75:24:62:13:
     8a:ae:25:5e:11:f6:ff:a8:be:d1:ad:56:87:d2:40:
     24:cc:fe:74:42:76:46:a2:fd:13:06:dc:95:f5:97:
     19:a0:bc:7e:56:c9:ea:79:49:74:a4:eb:a9:c1:fb:
     e5:3f:1f:f4:65:94:5a:39:6b:b7:d0:2a:70:cc:83:
     23:48:4e:97:fc:03:d2:59:e1:ac:db:4b:a6:00:16:
     80:d7:c7:2e:9f:ee:6a:03:0a:c2:05:68:33:0e:92:
     f7:76:c7:55:0d:82:00:de:b8:b9:fe:b6:61:f7:b7:
     39:f7:0d:ac:87:d3:73:91:7f:34:27:ea:88:50:c7:
     0f:41:3f:42:1d:1f:ec:03:a3:9a:26:8c:07:ab:e0:
     47:01:39:99:e1:f9:4e:8d:75:f8:07:aa:60:cc:60:
     1b:3b:19:43:0c:28:7f:a4:fe:c4:40:9f:07:e7:b6:
     54:c7:41:42:33:79:01:b9:89:ee:00:60:6b:21:ce:
     e7:4e:2e:d0:63:0a:75:cd:53:64:51:d3:4c:d0:aa:
     9a:52:d0:e1:61:13:a2:8b:4c:29:5e:ce:b0:24:e7:
     3e:4b:c0:d3:51:f6:42:85:95:6f:e7:f5:39:8e:cd:
     4e:5b:4b:a9:d2:d9:91:bf:a0:90:ce:8a:37:34:33:
     7a:e3:9d:82:3d:1c:76:d2:f8:30:d4:a0:d4:89:15:
     5b:d2:84:e2:eb:6c:3e:ec:98:c3:a1:d8:f4:60:be:
     fc:96:ab:db:c5:12:a6:9c:fc:5a:08:2a:d7:e7:1d:
     50:46:f2:e8:84:ee:ba:30:75:ed:44:ad:35:e0:e3:
     2b:2e:91:2f:fe:a3:91:d9:1d:a3:a3:e5:83:ab:a3:
     86:1a:f6:2f:b9:15:90:c3:63:3f:12:b6:df:0a:82:
     b0:3c:31:14:c3:87:f3:e7:c4:eb:ed:6a:5a:52:56:
     5d:31:0c:5d:8c:d0:48:51:ad:54:1e:59:b9:b8:6a:
     90:71
prime1:
     00:fc:b9:fc:e2:7f:43:c0:59:88:77:52:b5:81:54:
     44:b9:1d:85:7d:3f:d6:e5:2c:35:b5:61:cb:b3:31:
     8e:a9:d9:3f:b9:a8:db:0a:49:30:c8:c4:e1:04:d0:
     04:10:9e:3d:08:50:08:1f:e3:57:3b:2d:10:e8:ce:
     54:92:4c:ae:9a:5d:e2:d2:a1:b7:dd:f1:5d:ac:61:
     1b:d7:d9:86:70:7f:6a:17:89:46:d9:7b:3b:a4:c7:
     9f:ed:b6:8f:a7:9c:be:5e:38:f0:72:84:05:98:26:
     4c:96:f3:f4:f6:d6:63:b6:33:f8:90:f4:15:7a:e9:
     bf:e1:5c:d0:05:14:75:62:e0:64:18:a8:2e:c4:ff:
     31:a8:ee:c8:c9:f1:b4:17:66:45:7e:aa:9e:01:19:
     0f:35:a6:d8:b6:3f:1f:80:48:72:26:e6:8f:a6:f6:
```

```
      31:a8:19:31:43:5e:6d:37:c2:0b:fe:c6:9d:29:8b:
      3c:d9:38:27:f6:ef:be:3b:c8:d1:30:d0:eb:a9:91:
      36:59:2e:74:66:0f:c5:a8:fe:69:d9:12:86:d2:1e:
      f3:53:4a:1d:8f:eb:82:4e:bf:23:b9:70:9c:83:f5:
      cf:81:7f:86:11:9c:60:07:71:98:97:d4:ed:bd:c3:
      73:51:c8:29:c9:1a:2a:8c:de:68:6e:c0:e3:a8:06:
      cb:85
prime2:
      00:e4:c5:60:8a:18:50:51:9f:ac:5b:d6:f6:45:be:
      9d:b9:a3:47:9d:de:4c:eb:5e:df:5c:35:26:a0:09:
      22:0a:f2:58:cf:af:a4:c9:2a:93:8b:74:b5:6d:ec:
      d0:a6:89:d9:b8:82:eb:8a:21:6e:39:e4:f4:27:d4:
      3b:21:54:48:e6:2c:ed:cf:bd:bb:ed:bf:8e:85:aa:
      91:2b:15:67:1a:6c:fd:e5:df:45:90:84:eb:8a:fd:
      30:ea:70:a3:06:15:f6:cb:c2:8d:a4:cb:0a:5e:07:
      4f:aa:fe:b8:1b:18:5e:2c:79:87:f6:34:f8:cc:24:
      b8:05:f3:36:97:5d:1c:89:00:f5:28:02:23:95:aa:
      8e:06:33:5d:2a:a7:86:a2:fd:15:15:c7:b0:0d:49:
      c2:e0:96:97:a3:3e:fe:f5:a1:33:5f:58:51:7a:e4:
      58:1e:80:b5:47:ff:32:3e:14:7a:5f:49:f1:6e:a2:
      dd:2d:29:69:d5:de:4b:2d:eb:c6:59:45:62:62:eb:
      7a:aa:df:d6:eb:70:1b:67:85:11:3a:88:1c:fc:3b:
      97:5b:cb:9e:d0:bc:d1:ff:28:0c:02:5b:fb:42:75:
      aa:90:c1:31:d0:6a:36:09:1b:71:66:ec:26:be:00:
      cc:ad:ce:6d:76:48:39:05:f3:47:64:a1:29:e0:c2:
      13:1f
exponent1:
      25:91:48:24:2b:22:d9:1e:f6:08:36:c5:40:5a:54:
      74:e8:0c:85:d7:cd:8b:f7:8c:6c:50:03:45:b9:e2:
      29:21:60:35:ab:02:14:7f:58:bf:1f:75:0b:90:18:
      6a:97:fb:1e:97:36:fd:f6:7f:6b:0e:81:ea:f9:70:
      dc:e6:85:35:f1:2a:dc:80:a9:a2:56:54:c4:61:13:
      10:7d:07:5d:05:b3:b1:97:f8:6e:2f:c1:67:f7:3c:
      b0:cb:68:83:53:eb:80:7a:1a:54:0b:88:01:5c:00:
      1a:98:5d:1b:ac:36:da:48:d3:74:48:b4:40:b7:2a:
      8c:c7:8d:2c:94:23:f6:f4:c0:2c:62:23:c1:a8:e5:
      aa:e5:03:f7:f0:f4:02:5e:73:8a:26:b6:a2:17:25:
      89:a6:29:a4:bd:b1:63:12:61:d5:a2:84:4c:1f:60:
      b6:4a:38:66:79:4c:e6:f2:f3:71:85:f8:aa:ca:45:
      db:4c:5b:b4:7b:62:dd:e4:36:24:79:89:ee:84:e5:
      7d:50:48:81:3b:6a:f8:7a:09:25:f9:79:0d:17:08:
      b8:a2:d5:ce:25:06:13:ca:99:f6:e0:e4:83:41:30:
      fd:61:05:7e:ec:ad:e1:ad:63:2f:7e:b9:70:71:f3:
      5c:7e:d2:a7:50:3a:6f:02:48:a7:de:08:79:5b:b9:
      39
exponent2:
      52:8f:14:76:e1:ad:62:b7:8f:f9:18:cb:89:81:ef:
      e3:c5:94:1b:d9:d4:c2:80:5b:75:28:4d:47:25:e4:
      9e:34:b5:6e:46:01:df:03:39:79:f3:65:62:45:3b:
      4b:4e:a6:3e:db:28:6b:92:02:f8:6b:b2:dd:08:cf:
      4a:08:e3:c2:05:66:d1:38:b4:b0:69:17:e3:0f:1a:
```

```
      12:85:47:cf:16:94:4e:37:d4:20:02:88:0a:81:b2:
      fc:78:27:ad:13:92:1c:18:9b:0b:64:a6:da:26:23:
      4f:1f:5b:8b:93:b0:b0:b6:2f:25:e0:1a:05:7a:1e:
      db:2e:d9:7d:a8:81:9a:c3:b8:b5:76:88:27:04:04:
      fb:21:e0:36:7b:7c:b0:27:4b:4b:af:e3:cd:f7:d7:
      97:3b:61:7f:ed:45:0f:99:dc:33:45:69:2a:43:6b:
      b5:9e:57:4d:a3:40:1b:7d:42:68:4f:04:0d:1c:43:
      5b:7f:fd:8c:cc:0b:2f:88:4d:ed:7b:87:b5:11:2c:
      14:ac:71:20:48:35:eb:96:ef:0f:c3:7d:4a:5d:ab:
      12:da:99:f6:d4:9d:a8:4a:68:83:15:74:c8:98:34:
      34:c7:33:d5:f5:ee:88:3c:da:20:fd:8a:41:b9:82:
      24:1b:42:0f:94:a2:d7:8d:e3:2e:e2:a6:7d:51:2c:
      9b
coefficient:
      00:ae:11:a8:f9:ec:e2:7c:c4:47:b6:2c:91:77:ca:
      c1:43:6a:4f:6c:b1:d2:d8:b0:f1:f2:fb:0d:e7:37:
      1f:66:de:de:b0:6b:cb:f9:07:fc:b7:e8:90:a5:59:
      8e:4a:84:72:6e:db:ca:97:93:ae:5f:00:c7:d4:97:
      e1:0d:8b:38:3d:42:5d:1a:72:35:69:bf:80:a3:d6:
      19:df:83:f3:88:fa:27:fa:a5:e5:99:72:a6:fd:ac:
      f1:de:da:68:5e:31:07:1a:49:18:18:72:80:56:f3:
      46:1e:cb:7c:fc:44:7e:57:bc:0a:c7:e8:71:5d:88:
      10:a2:07:d7:67:9b:ce:15:ee:8c:be:5a:e7:cf:78:
      5e:cd:4e:af:b3:8b:51:7c:14:52:5c:6b:99:67:be:
      59:45:11:83:d5:0e:d5:9b:06:df:52:31:9f:27:3a:
      31:a1:60:db:7e:c3:b1:f5:5e:fe:c4:d4:38:0c:69:
      e1:53:3a:99:39:e5:72:d8:10:77:32:80:a8:a4:0a:
      6f:65:44:e9:8b:54:7e:f6:33:1e:74:50:9b:f2:75:
      88:9f:ca:0f:df:da:e2:64:8c:64:3f:2e:29:64:dd:
      03:4e:6c:98:76:8d:7c:8e:83:3a:75:7a:ca:46:fc:
      5c:5b:75:18:ca:65:f5:49:7b:40:85:97:52:bc:4d:
      b2:cf
[09/29/25]seed@VM:~/.../work_dir$
```

Task 1 Questions

Using the information printed above, the following are the response to the questions from the laboratory prompt.

1. What part of the certificate indicates this is a CA's certificate?

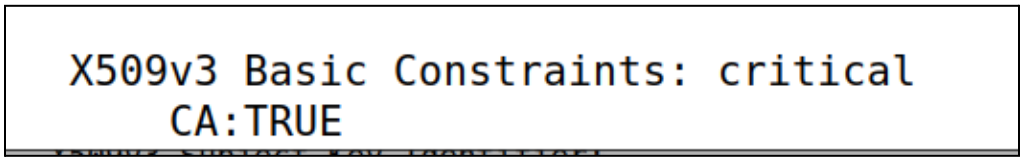

Figure 13. CA:True field

The portion CA:TRUE in the content of ca.crt indicated that it is a CA's certificate (See Figure 13).

2. What part of the certificate indicates this is a self-signed certificate?

```
X509v3 extensions:
    X509v3 Subject Key Identifier:
        CF:3B:C4:2E:A5:3F:C6:64:A4:5E:5E:85:7F:9A:EB:8A:2A:FA:23:8E
    X509v3 Authority Key Identifier:
        keyid:CF:3B:C4:2E:A5:3F:C6:64:A4:5E:5E:85:7F:9A:EB:8A:2A:FA:23:8E

    X509v3 Basic Constraints: critical
        CA:TRUE
```

Figure 14. Subject Key Identifier and Authority Key Identifier being the Same.

Since the Subject Key Identifier and the Authority Key Identifier is the same, it is self-signed certificate(See Figure 14).

3. In the RSA algorithm, we have a public exponent, a private exponent,, a modulus, and two secret numbers p and q, such that n=pq. Please identify the values for these elements in your certificate and key files.

These values were derived from the ca.key
Notably, modulus and publicExponent in the ca.key and ca.crt are the same.

```
modulus:
      00:e1:d8:7f:a7:66:bc:42:ad:82:7d:07:4e:42:e6:
      43:7b:f7:92:09:f7:8b:ad:4b:98:68:3f:44:b3:4e:
      59:df:8a:9d:2b:83:7e:ff:29:f8:8a:cf:e4:8c:42:
      38:88:17:15:f4:93:49:e1:0d:f9:f2:d8:0d:b9:37:
      c5:ef:4e:9c:6f:19:07:d5:19:f7:f3:53:35:4a:91:
      01:2b:ee:68:36:0b:bc:49:36:08:58:54:41:58:b1:
      15:41:4e:ae:6d:0a:df:9a:c9:d0:24:4f:22:c3:6e:
      ec:37:d2:43:26:96:6e:a1:2e:dd:06:76:6e:bc:b5:
      6f:d1:7b:0e:31:f4:d3:f4:68:f7:40:0a:be:37:3c:
      a7:65:7d:3c:24:08:5b:82:78:9a:e3:83:28:ff:0b:
      91:21:b4:28:80:cb:bd:ba:96:e6:36:c0:64:5f:35:
      72:5d:45:c7:e3:34:f8:05:6e:08:18:5c:55:74:58:
      51:4c:11:f4:16:9d:a9:db:6c:0a:e7:2f:04:18:2d:
      a0:f1:d0:9e:c7:19:78:18:13:e4:55:a5:94:67:27:
      18:55:55:b2:a1:10:77:e5:9e:0b:2b:31:ac:9d:8e:
      03:54:e2:c2:ec:32:ba:63:40:8a:2a:08:dd:26:29:
      30:ac:22:d0:e2:35:c4:60:bd:7f:aa:16:d5:8a:c3:
      c6:85:78:e5:94:b4:1e:60:44:fa:a1:c6:c2:d0:76:
      db:51:7b:bf:97:c4:0a:35:f0:8f:8c:66:ad:ad:32:
      91:5f:09:05:73:0b:43:69:c5:c5:80:6c:76:c7:3b:
      5c:7a:5b:be:51:e9:c0:b0:e1:6f:f6:66:fd:a6:0d:
      ee:62:6b:b8:2c:17:24:f7:6e:3f:c8:18:2d:61:2d:
      f5:d4:c2:74:be:a1:82:1c:25:0e:46:0d:4c:aa:e6:
      d4:81:f4:aa:b6:30:6e:3d:89:fb:59:0c:ea:96:f7:
      51:c8:ee:de:1b:8c:ad:fa:72:30:c0:5c:53:3c:3e:
      34:dd:30:0a:32:df:2f:f9:aa:20:f0:70:d6:ee:1a:
      c1:3a:fc:96:f2:e4:1c:75:7a:c3:d3:ae:cb:a5:2f:
      39:63:14:62:89:26:2e:0a:c1:e7:81:24:a7:66:dc:
      7d:45:89:ee:d6:e7:12:49:86:c7:e1:4e:ee:d3:1b:
      80:a6:fc:e5:95:ad:f2:91:5b:68:1b:91:ad:6f:59:
      63:cb:6a:b7:46:2e:f1:8b:fc:9d:48:2d:55:6e:6c:
```

```
     b7:f9:ab:97:15:d2:48:cb:ed:87:9c:49:8c:b9:4b:
     d1:38:f0:96:60:f7:34:50:73:14:7a:9d:28:99:a9:
     d1:2a:4f:89:4b:4a:e6:24:fb:de:cf:4e:c5:91:74:
     b7:84:1b
publicExponent: 65537 (0x10001)
privateExponent:
     45:18:09:25:db:c6:68:d7:d0:7e:13:c8:1b:ab:7a:
     a5:e8:7d:e3:52:ba:86:d0:03:d6:90:d4:a1:ce:ac:
     ac:39:2a:10:6f:f0:60:7c:24:af:c3:1e:76:d2:a3:
     9c:ef:03:26:8a:11:26:2b:32:76:db:26:87:ad:ca:
     7e:86:1c:51:d8:e4:8e:8b:9d:51:f1:f8:f1:d1:1e:
     fc:a3:b9:7a:1f:69:01:34:e8:a4:ad:52:38:a2:24:
     90:90:53:c8:c4:74:d8:54:39:bb:82:02:6e:ab:f6:
     d4:b5:1d:1a:27:17:bd:74:2a:e6:99:41:13:b6:a6:
     78:fe:1e:bf:a5:d9:5a:82:ea:71:cb:57:9a:6a:92:
     03:f8:a6:77:97:9e:f7:71:92:61:5c:75:24:62:13:
     8a:ae:25:5e:11:f6:ff:a8:be:d1:ad:56:87:d2:40:
     24:cc:fe:74:42:76:46:a2:fd:13:06:dc:95:f5:97:
     19:a0:bc:7e:56:c9:ea:79:49:74:a4:eb:a9:c1:fb:
     e5:3f:1f:f4:65:94:5a:39:6b:b7:d0:2a:70:cc:83:
     23:48:4e:97:fc:03:d2:59:e1:ac:db:4b:a6:00:16:
     80:d7:c7:2e:9f:ee:6a:03:0a:c2:05:68:33:0e:92:
     f7:76:c7:55:0d:82:00:de:b8:b9:fe:b6:61:f7:b7:
     39:f7:0d:ac:87:d3:73:91:7f:34:27:ea:88:50:c7:
     0f:41:3f:42:1d:1f:ec:03:a3:9a:26:8c:07:ab:e0:
     47:01:39:99:e1:f9:4e:8d:75:f8:07:aa:60:cc:60:
     1b:3b:19:43:0c:28:7f:a4:fe:c4:40:9f:07:e7:b6:
     54:c7:41:42:33:79:01:b9:89:ee:00:60:6b:21:ce:
     e7:4e:2e:d0:63:0a:75:cd:53:64:51:d3:4c:d0:aa:
     9a:52:d0:e1:61:13:a2:8b:4c:29:5e:ce:b0:24:e7:
     3e:4b:c0:d3:51:f6:42:85:95:6f:e7:f5:39:8e:cd:
     4e:5b:4b:a9:d2:d9:91:bf:a0:90:ce:8a:37:34:33:
     7a:e3:9d:82:3d:1c:76:d2:f8:30:d4:a0:d4:89:15:
     5b:d2:84:e2:eb:6c:3e:ec:98:c3:a1:d8:f4:60:be:
     fc:96:ab:db:c5:12:a6:9c:fc:5a:08:2a:d7:e7:1d:
     50:46:f2:e8:84:ee:ba:30:75:ed:44:ad:35:e0:e3:
     2b:2e:91:2f:fe:a3:91:d9:1d:a3:a3:e5:83:ab:a3:
     86:1a:f6:2f:b9:15:90:c3:63:3f:12:b6:df:0a:82:
     b0:3c:31:14:c3:87:f3:e7:c4:eb:ed:6a:5a:52:56:
     5d:31:0c:5d:8c:d0:48:51:ad:54:1e:59:b9:b8:6a:
     90:71
prime1:
     00:fc:b9:fc:e2:7f:43:c0:59:88:77:52:b5:81:54:
     44:b9:1d:85:7d:3f:d6:e5:2c:35:b5:61:cb:b3:31:
     8e:a9:d9:3f:b9:a8:db:0a:49:30:c8:c4:e1:04:d0:
     04:10:9e:3d:08:50:08:1f:e3:57:3b:2d:10:e8:ce:
     54:92:4c:ae:9a:5d:e2:d2:a1:b7:dd:f1:5d:ac:61:
     1b:d7:d9:86:70:7f:6a:17:89:46:d9:7b:3b:a4:c7:
     9f:ed:b6:8f:a7:9c:be:5e:38:f0:72:84:05:98:26:
     4c:96:f3:f4:f6:d6:63:b6:33:f8:90:f4:15:7a:e9:
     bf:e1:5c:d0:05:14:75:62:e0:64:18:a8:2e:c4:ff:
```

```
      31:a8:ee:c8:c9:f1:b4:17:66:45:7e:aa:9e:01:19:
      0f:35:a6:d8:b6:3f:1f:80:48:72:26:e6:8f:a6:f6:
      31:a8:19:31:43:5e:6d:37:c2:0b:fe:c6:9d:29:8b:
      3c:d9:38:27:f6:ef:be:3b:c8:d1:30:d0:eb:a9:91:
      36:59:2e:74:66:0f:c5:a8:fe:69:d9:12:86:d2:1e:
      f3:53:4a:1d:8f:eb:82:4e:bf:23:b9:70:9c:83:f5:
      cf:81:7f:86:11:9c:60:07:71:98:97:d4:ed:bd:c3:
      73:51:c8:29:c9:1a:2a:8c:de:68:6e:c0:e3:a8:06:
      cb:85
prime2:
      00:e4:c5:60:8a:18:50:51:9f:ac:5b:d6:f6:45:be:
      9d:b9:a3:47:9d:de:4c:eb:5e:df:5c:35:26:a0:09:
      22:0a:f2:58:cf:af:a4:c9:2a:93:8b:74:b5:6d:ec:
      d0:a6:89:d9:b8:82:eb:8a:21:6e:39:e4:f4:27:d4:
      3b:21:54:48:e6:2c:ed:cf:bd:bb:ed:bf:8e:85:aa:
      91:2b:15:67:1a:6c:fd:e5:df:45:90:84:eb:8a:fd:
      30:ea:70:a3:06:15:f6:cb:c2:8d:a4:cb:0a:5e:07:
      4f:aa:fe:b8:1b:18:5e:2c:79:87:f6:34:f8:cc:24:
      b8:05:f3:36:97:5d:1c:89:00:f5:28:02:23:95:aa:
      8e:06:33:5d:2a:a7:86:a2:fd:15:15:c7:b0:0d:49:
      c2:e0:96:97:a3:3e:fe:f5:a1:33:5f:58:51:7a:e4:
      58:1e:80:b5:47:ff:32:3e:14:7a:5f:49:f1:6e:a2:
      dd:2d:29:69:d5:de:4b:2d:eb:c6:59:45:62:62:eb:
      7a:aa:df:d6:eb:70:1b:67:85:11:3a:88:1c:fc:3b:
      97:5b:cb:9e:d0:bc:d1:ff:28:0c:02:5b:fb:42:75:
      aa:90:c1:31:d0:6a:36:09:1b:71:66:ec:26:be:00:
      cc:ad:ce:6d:76:48:39:05:f3:47:64:a1:29:e0:c2:
      13:1f
exponent1:
      25:91:48:24:2b:22:d9:1e:f6:08:36:c5:40:5a:54:
      74:e8:0c:85:d7:cd:8b:f7:8c:6c:50:03:45:b9:e2:
      29:21:60:35:ab:02:14:7f:58:bf:1f:75:0b:90:18:
      6a:97:fb:1e:97:36:fd:f6:7f:6b:0e:81:ea:f9:70:
      dc:e6:85:35:f1:2a:dc:80:a9:a2:56:54:c4:61:13:
      10:7d:07:5d:05:b3:b1:97:f8:6e:2f:c1:67:f7:3c:
      b0:cb:68:83:53:eb:80:7a:1a:54:0b:88:01:5c:00:
      1a:98:5d:1b:ac:36:da:48:d3:74:48:b4:40:b7:2a:
      8c:c7:8d:2c:94:23:f6:f4:c0:2c:62:23:c1:a8:e5:
      aa:e5:03:f7:f0:f4:02:5e:73:8a:26:b6:a2:17:25:
      89:a6:29:a4:bd:b1:63:12:61:d5:a2:84:4c:1f:60:
      b6:4a:38:66:79:4c:e6:f2:f3:71:85:f8:aa:ca:45:
      db:4c:5b:b4:7b:62:dd:e4:36:24:79:89:ee:84:e5:
      7d:50:48:81:3b:6a:f8:7a:09:25:f9:79:0d:17:08:
      b8:a2:d5:ce:25:06:13:ca:99:f6:e0:e4:83:41:30:
      fd:61:05:7e:ec:ad:e1:ad:63:2f:7e:b9:70:71:f3:
      5c:7e:d2:a7:50:3a:6f:02:48:a7:de:08:79:5b:b9:
      39
exponent2:
      52:8f:14:76:e1:ad:62:b7:8f:f9:18:cb:89:81:ef:
      e3:c5:94:1b:d9:d4:c2:80:5b:75:28:4d:47:25:e4:
      9e:34:b5:6e:46:01:df:03:39:79:f3:65:62:45:3b:
```

```
      4b:4e:a6:3e:db:28:6b:92:02:f8:6b:b2:dd:08:cf:
      4a:08:e3:c2:05:66:d1:38:b4:b0:69:17:e3:0f:1a:
      12:85:47:cf:16:94:4e:37:d4:20:02:88:0a:81:b2:
      fc:78:27:ad:13:92:1c:18:9b:0b:64:a6:da:26:23:
      4f:1f:5b:8b:93:b0:b0:b6:2f:25:e0:1a:05:7a:1e:
      db:2e:d9:7d:a8:81:9a:c3:b8:b5:76:88:27:04:04:
      fb:21:e0:36:7b:7c:b0:27:4b:4b:af:e3:cd:f7:d7:
      97:3b:61:7f:ed:45:0f:99:dc:33:45:69:2a:43:6b:
      b5:9e:57:4d:a3:40:1b:7d:42:68:4f:04:0d:1c:43:
      5b:7f:fd:8c:cc:0b:2f:88:4d:ed:7b:87:b5:11:2c:
      14:ac:71:20:48:35:eb:96:ef:0f:c3:7d:4a:5d:ab:
      12:da:99:f6:d4:9d:a8:4a:68:83:15:74:c8:98:34:
      34:c7:33:d5:f5:ee:88:3c:da:20:fd:8a:41:b9:82:
      24:1b:42:0f:94:a2:d7:8d:e3:2e:e2:a6:7d:51:2c:
      9b
coefficient:
      00:ae:11:a8:f9:ec:e2:7c:c4:47:b6:2c:91:77:ca:
      c1:43:6a:4f:6c:b1:d2:d8:b0:f1:f2:fb:0d:e7:37:
      1f:66:de:de:b0:6b:cb:f9:07:fc:b7:e8:90:a5:59:
      8e:4a:84:72:6e:db:ca:97:93:ae:5f:00:c7:d4:97:
      e1:0d:8b:38:3d:42:5d:1a:72:35:69:bf:80:a3:d6:
      19:df:83:f3:88:fa:27:fa:a5:e5:99:72:a6:fd:ac:
      f1:de:da:68:5e:31:07:1a:49:18:18:72:80:56:f3:
      46:1e:cb:7c:fc:44:7e:57:bc:0a:c7:e8:71:5d:88:
      10:a2:07:d7:67:9b:ce:15:ee:8c:be:5a:e7:cf:78:
      5e:cd:4e:af:b3:8b:51:7c:14:52:5c:6b:99:67:be:
      59:45:11:83:d5:0e:d5:9b:06:df:52:31:9f:27:3a:
      31:a1:60:db:7e:c3:b1:f5:5e:fe:c4:d4:38:0c:69:
      e1:53:3a:99:39:e5:72:d8:10:77:32:80:a8:a4:0a:
      6f:65:44:e9:8b:54:7e:f6:33:1e:74:50:9b:f2:75:
      88:9f:ca:0f:df:da:e2:64:8c:64:3f:2e:29:64:dd:
      03:4e:6c:98:76:8d:7c:8e:83:3a:75:7a:ca:46:fc:
      5c:5b:75:18:ca:65:f5:49:7b:40:85:97:52:bc:4d:
      b2:cf
```

Generating a Certificate Request for Your Web Server

This task aims to simulate the generation of certificates from a created webserver. For this task, the custom DNS used was **www.bank32a.com**. This is a derivative of what was used in the laboratory prompts.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl req -newkey rsa:2048 -sha256  \-keyout ser
ver.key   -out server.csr  \-subj "/CN=www.bank32a.com/O=Bank32A Inc./C=US" \-passou
t pass:dees
Generating a RSA private key
.....................................................+++++
...................+++++
writing new private key to 'server.key'
-----
[09/29/25]seed@VM:~/.../work_dir$
```

Figure 15. Creating a Certificate Signing Request (CSR) under the domain name bank32a.com

```
[09/29/25]seed@VM:~/.../work_dir$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.bank32a.com, O = Bank32A Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
```

Figure 16. Decoded Content of server.csr

Shown below is the complete content of server.csr.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl req -in server.csr -text
-noout
Certificate Request:
      Data:
      Version: 1 (0x0)
      Subject: CN = www.bank32a.com, O = Bank32A Inc., C = US
      Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                  RSA Public-Key: (2048 bit)
                  Modulus:
                        00:bf:05:96:31:01:5a:9c:fd:12:41:7e:22:ad:3f:
                        80:7d:fb:2e:d0:d4:3b:c7:6f:b9:8b:12:18:0b:8e:
                        71:bb:63:77:f6:c2:2a:67:2e:56:cf:0f:56:27:f4:
                        84:d3:e6:aa:a6:30:f9:5f:05:4c:e3:0e:5b:98:db:
                        dd:20:8b:71:6c:2b:fe:0b:61:35:db:c7:8e:cd:0a:
                        df:db:c3:3e:05:c3:5d:93:aa:09:52:15:77:58:c6:
                        9b:28:72:8a:a5:14:e2:f1:cd:a8:c2:00:aa:d6:17:
                        2b:5f:fe:ed:69:cc:d4:c9:a4:74:94:03:7b:93:9d:
                        35:5d:62:71:91:4d:1a:f9:86:48:05:1a:86:7c:a9:
                        14:d9:10:12:b8:10:ea:f3:09:94:60:b6:ba:52:68:
                        1b:81:d3:ce:8a:a7:85:ed:1a:66:46:93:e8:c3:6f:
                        f9:be:7c:1d:48:28:5a:d9:a5:d4:54:4f:46:0b:5e:
                        68:e3:a5:e4:6b:98:f3:ca:d1:44:63:42:d9:ac:e6:
                        cc:63:1a:c1:1a:0c:20:35:5a:51:b2:d3:d4:e0:b9:
                        5d:50:33:34:b9:b2:d6:69:66:4b:d1:50:fe:a9:76:
                        7e:4d:bc:94:b9:ae:0b:3a:24:fc:1b:a4:39:95:2b:
                        ec:ab:77:f7:ba:96:59:81:f2:78:b1:9b:21:84:f3:
                        2f:c9
                  Exponent: 65537 (0x10001)
      Attributes:
            a0:00
      Signature Algorithm: sha256WithRSAEncryption
      93:78:bf:da:af:48:ab:11:72:6d:e8:48:ba:f3:6a:fc:9b:32:
      01:64:9e:5e:ea:50:bd:11:b5:90:98:59:9d:bb:32:15:05:a7:
      ff:5c:7c:36:30:1a:c8:ff:cb:0e:38:cd:f4:10:e3:9b:51:64:
```

```
      20:e2:64:16:d2:74:64:fb:78:ad:59:21:14:b2:73:ff:1f:4c:
      d4:c8:7e:cf:cf:e0:30:3e:d0:a0:53:d7:e4:43:3d:c6:63:d1:
      db:84:60:d5:47:c8:b8:f1:4e:18:45:e8:a9:46:69:ca:eb:73:
      e2:1c:9e:de:a4:14:af:b6:7f:ba:5f:a7:32:90:ba:db:2d:c8:
      9d:47:bf:d3:45:11:92:73:3d:8e:c7:03:96:90:1f:3c:b0:2b:
      be:a1:2f:33:83:48:29:05:c4:e1:60:48:da:94:f3:71:46:ba:
      1b:9c:40:8d:0d:71:e0:bc:b2:78:26:ba:49:a8:8b:44:7a:54:
      1d:d6:7f:21:f9:a9:23:82:00:7d:85:f6:c9:04:99:5e:02:1c:
      5b:64:7b:0e:cd:e3:38:d2:4c:47:d0:59:a6:29:59:41:16:e4:
      b6:2f:5e:51:49:22:70:0a:fa:f4:58:0f:df:f8:27:3c:6e:b0:
      3d:82:5f:40:3f:b1:e6:09:7a:5e:69:a1:a1:21:b5:6e:7f:99:
      44:f6:dc:f3
```

```
[09/29/25]seed@VM:~/.../work_dir$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:bf:05:96:31:01:5a:9c:fd:12:41:7e:22:ad:3f:
    80:7d:fb:2e:d0:d4:3b:c7:6f:b9:8b:12:18:0b:8e:
    71:bb:63:77:f6:c2:2a:67:2e:56:cf:0f:56:27:f4:
    84:d3:e6:aa:a6:30:f9:5f:05:4c:e3:0e:5b:98:db:
    dd:20:8b:71:6c:2b:fe:0b:61:35:db:c7:8e:cd:0a:
```

Figure 17. Decoded Content of server.key.

Shown below is the complete content of server.key.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl rsa -in server.key -text
-noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
      00:bf:05:96:31:01:5a:9c:fd:12:41:7e:22:ad:3f:
      80:7d:fb:2e:d0:d4:3b:c7:6f:b9:8b:12:18:0b:8e:
      71:bb:63:77:f6:c2:2a:67:2e:56:cf:0f:56:27:f4:
      84:d3:e6:aa:a6:30:f9:5f:05:4c:e3:0e:5b:98:db:
      dd:20:8b:71:6c:2b:fe:0b:61:35:db:c7:8e:cd:0a:
      df:db:c3:3e:05:c3:5d:93:aa:09:52:15:77:58:c6:
      9b:28:72:8a:a5:14:e2:f1:cd:a8:c2:00:aa:d6:17:
      2b:5f:fe:ed:69:cc:d4:c9:a4:74:94:03:7b:93:9d:
      35:5d:62:71:91:4d:1a:f9:86:48:05:1a:86:7c:a9:
      14:d9:10:12:b8:10:ea:f3:09:94:60:b6:ba:52:68:
      1b:81:d3:ce:8a:a7:85:ed:1a:66:46:93:e8:c3:6f:
      f9:be:7c:1d:48:28:5a:d9:a5:d4:54:4f:46:0b:5e:
      68:e3:a5:e4:6b:98:f3:ca:d1:44:63:42:d9:ac:e6:
      cc:63:1a:c1:1a:0c:20:35:5a:51:b2:d3:d4:e0:b9:
      5d:50:33:34:b9:b2:d6:69:66:4b:d1:50:fe:a9:76:
      7e:4d:bc:94:b9:ae:0b:3a:24:fc:1b:a4:39:95:2b:
      ec:ab:77:f7:ba:96:59:81:f2:78:b1:9b:21:84:f3:
```

```
      2f:c9
publicExponent: 65537 (0x10001)
privateExponent:
      28:2a:ef:93:2c:7a:b6:6a:4c:ed:72:ad:ae:0a:9d:
      65:60:6d:4e:c2:62:33:a4:dd:ba:4d:ba:ba:ab:60:
      65:0c:1c:8c:c9:f5:8a:ae:e6:d8:31:9c:67:58:76:
      99:ec:76:53:ee:16:72:11:b6:42:44:a1:a4:3a:0f:
      7c:a9:75:d7:4e:44:e4:75:b3:92:9c:9a:fd:a8:dc:
      bb:e4:89:65:42:d8:a9:95:66:d2:58:eb:38:c2:c2:
      9b:b5:c2:4b:c6:61:96:81:2d:8c:66:01:86:75:66:
      cc:8f:d9:b2:96:bc:e4:0d:ed:e9:b5:f5:c5:6b:98:
      6e:23:a6:47:ec:93:d0:86:3b:c6:9f:56:2b:f9:de:
      5f:f7:b7:3b:a9:86:dc:66:a8:fd:c7:6b:3d:86:f4:
      67:b0:f3:62:56:05:8e:98:0b:5b:d7:0a:fb:18:66:
      60:d1:03:a2:00:43:8d:c4:9e:dd:92:5e:48:ea:a3:
      91:90:14:84:bf:97:a2:19:40:55:1e:b2:4f:51:d0:
      37:1b:98:72:e7:99:89:e9:94:8a:94:26:1b:38:da:
      86:a4:47:18:e6:7f:cc:11:2d:7f:6f:cb:46:47:b3:
      78:fa:67:d3:07:a1:74:0d:b2:ac:b8:0e:20:a9:d8:
      14:a6:46:f9:67:8a:86:76:18:67:4a:71:03:b9:1f:
      25
prime1:
      00:f0:b3:d0:93:55:2b:76:83:c5:ee:de:d9:6a:1f:
      89:6b:57:8c:d5:54:92:29:8f:39:95:fb:fa:69:d4:
      1b:f1:79:fb:6e:00:cc:e8:64:2f:5e:ce:1a:0e:05:
      dd:c4:cb:a4:a3:b1:8e:67:ba:76:a0:c0:8e:06:b2:
      55:63:19:e5:37:05:8c:88:04:f0:16:51:06:1a:01:
      64:99:dd:1a:62:b1:59:d4:e0:26:d3:7f:36:6d:2a:
      d6:26:d2:3f:a6:4e:be:d2:43:a8:4a:9e:86:45:68:
      97:28:1c:00:d8:d0:46:84:60:78:dc:5b:d0:70:f7:
      7c:32:b5:b1:23:1b:26:f6:97
prime2:
      00:cb:29:7a:4e:c9:0c:4b:e9:c4:af:25:29:43:99:
      9b:71:0c:46:df:87:f7:29:29:ba:f3:72:ba:db:b3:
      63:96:25:53:c0:23:e5:3a:4f:38:94:96:41:b0:bf:
      a4:3b:da:74:22:4c:91:ac:0a:5f:81:66:7e:7b:73:
      9a:51:8e:0a:b3:e9:2a:88:dc:31:1a:4e:dd:68:7f:
      cd:fe:58:f8:c2:8a:0b:7a:d9:65:f0:e4:ee:58:5d:
      d8:94:e3:79:fd:a5:18:f1:2f:b2:d2:c3:8a:83:ef:
      2e:2f:0d:47:39:4c:b9:ff:d4:49:8c:94:81:36:ea:
      0b:4b:83:3a:08:8d:89:38:9f
exponent1:
      5b:2b:50:8a:2d:8d:4b:d3:77:8a:15:80:76:10:c1:
      e5:15:81:33:60:58:08:43:c6:85:07:ae:fe:9c:a7:
      84:dc:36:1e:a1:50:fb:88:ce:e4:72:de:2d:87:8d:
      4b:37:f3:01:49:84:6d:c7:93:9d:29:b1:e1:d9:74:
      3c:18:17:d8:b2:52:5b:46:bb:85:48:65:2e:3e:6e:
      d3:54:8a:e4:ec:d5:e0:aa:92:2a:33:99:f2:d9:71:
      c9:bc:82:fd:44:00:44:f5:f9:6d:62:03:eb:90:45:
      08:9d:2a:b8:f4:92:71:1b:75:4b:c9:be:f6:ba:d6:
```

```
      a1:02:6e:b8:a4:55:2a:bb
exponent2:
      00:c9:08:48:20:c1:cc:cb:29:8d:18:8a:bb:24:4b:
      51:87:31:d0:c7:cc:31:04:a8:68:78:11:e5:59:15:
      4f:cb:f9:2f:c0:87:44:82:c8:75:82:82:94:8a:23:
      78:8e:49:82:75:96:32:e7:7c:74:39:05:84:ce:ff:
      fb:8a:0b:f6:07:45:08:73:d8:ff:35:bb:28:58:09:
      6f:7a:e9:eb:6e:05:4f:8a:c6:a8:9b:10:cd:d0:df:
      3c:3b:48:45:24:7a:44:0e:15:56:ec:3b:d6:4a:eb:
      58:55:f2:db:b1:95:7c:cf:eb:ee:c3:8f:07:b5:a1:
      2e:80:10:60:52:aa:4b:48:9d
coefficient:
      30:56:5e:29:9f:d7:fd:b6:a4:91:b8:a3:cf:d8:be:
      b9:72:19:1e:e8:f1:e6:b4:dc:2a:95:1a:e1:86:57:
      d4:45:15:3e:3f:83:ca:b0:26:83:33:b7:96:5f:1d:
      f2:c8:e9:ae:2d:99:27:4f:17:5a:c8:24:35:5e:2c:
      38:c2:3f:95:8a:63:e4:73:c0:c6:4c:c7:dc:6f:1f:
      17:cc:9e:2c:51:b1:e9:3f:be:e3:e8:fc:c6:ff:0e:
      b7:0c:a7:ba:c1:8c:25:7e:77:b9:b1:33:81:3c:b2:
      54:cc:b5:a9:f2:27:a9:7f:db:d4:20:3b:68:76:08:
      f2:8e:02:88:c8:33:ac:b0
```

```
[09/29/25]seed@VM:~/.../work_dir$ openssl req -newkey rsa:2048 -sha256  \
> -keyout server.key -out server.csr  \
> -subj "/CN=www.bank32a.com/O=Bank32A Inc./C=US" \
> -addext "subjectAltName = DNS:www.bank32A.com,\
> DNS:www.bank32AA.com, \
> DNS:www.bank32AB.com" \
> -passout pass:dees
Generating a RSA private key
..............................+++++
...+++++
writing new private key to 'server.key'
```

Figure 18. Adding an Alternative Name for bank32A.com: bank32AA.com, bank32AB.com,

Additionally, we added alternative bank32A.com. The alternative DNS made were also patterned from the laboratory exercises theme on creating alternative DNS (i.e. adding A and B). The alternative DNS added were bank32AA.com, bank32AB.com,

```
 Requested Extensions:
     X509v3 Subject Alternative Name:
         DNS:www.bank32A.com, DNS:www.bank32AA.com, DNS:www.bank32AB.com
nature Algorithm: sha256WithRSAEncryption
```

Figure 19. Alternative DNS made in the certificate of the server

Seen in Figure 19 is the added field in the decoded content of the server.crt, reflecting the additional alternative DNS.

POINT OF CONFUSION

The new website that I created is bank32A.com. Its aliases are bank32AA.com and bank32AB.com; this is **not** the same as bank32.com with the aliases bank32A.com and bank32B.com that was used as an example in the laboratory prompt.

Generating a Certificate for your server

This task aims to utilize the simulated and create Certificate Authority to generate certificates. At this point of the laboratory exercise, openssl.cnf was renamed to myCA_openssl.cnf to make the distinction between the operating system's original openssl.cnf file and the edited one easier.

```
[09/29/25]seed@VM:~/.../work_dir$ ls *.cnf
myCA_openssl.cnf
[09/29/25]seed@VM:~/.../work_dir$
```

Figure 20. The openssl configuration file used.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl ca -config myCA_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 myCA_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: Sep 29 07:10:23 2025 GMT
            Not After : Sep 27 07:10:23 2035 GMT
        Subject:
            countryName               = US
            organizationName          = Bank32A Inc.
```

Figure 21. Turning the certificate signing request (server.csr) into an X509certificate (server.crt), using the CA's ca.crt and ca.key.

We then created a server certificate using the command shown in Figure 21. This turns the certificate signing request (CSR) of the server into a certificate while using the ca.crt and ca.key

Shown below is the complete content of the terminal:

```
[09/29/25]seed@VM:~/.../work_dir$ openssl ca -config
myCA_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 myCA_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: Sep 29 07:10:23 2025 GMT
            Not After : Sep 27 07:10:23 2035 GMT
      Subject:
            countryName                = US
            organizationName           = Bank32A Inc.
```

```
            commonName                = www.bank32a.com
      X509v3 extensions:
            X509v3 Basic Constraints:
                  CA:FALSE
            Netscape Comment:
                  OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:

19:0D:B1:ED:75:64:8D:AC:22:FE:45:D6:71:70:61:E3:07:D5:84:94
            X509v3 Authority Key Identifier:

keyid:CF:3B:C4:2E:A5:3F:C6:64:A4:5E:5E:85:7F:9A:EB:8A:2A:FA:23:8E

Certificate is to be certified until Sep 27 07:10:23 2035 GMT (3650
days)

Write out database with 1 new entries
Data Base Updated
[09/29/25]seed@VM:~/.../work_dir$
```

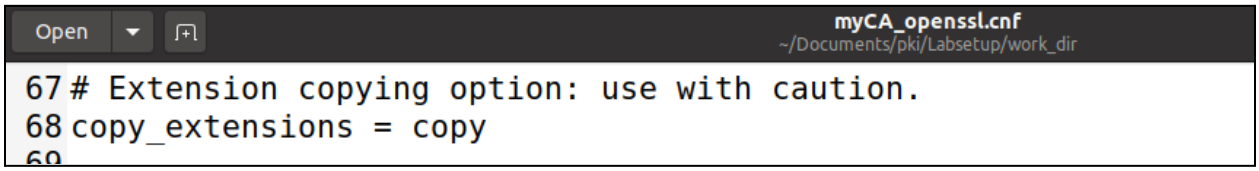

Figure 21. Commenting out the copy_extensions

We then ought to enable the option on copying extensions (See Figure 21).

```
[09/29/25]seed@VM:~/.../work_dir$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Sep 29 07:10:23 2025 GMT
            Not After : Sep 27 07:10:23 2035 GMT
        Subject: C = US, O = Bank32A Inc., CN = www.bank32a.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
```

Figure 22. Decoded content of the certificate for the server.

Shown in Figure 22 is the content of the created certificate for the server.
The entire content of the certificate is as shown below.

```
[09/29/25]seed@VM:~/.../work_dir$ openssl x509 -in server.crt -text
-noout
```

```
Certificate:
     Data:
     Version: 3 (0x2)
     Serial Number: 4096 (0x1000)
     Signature Algorithm: sha256WithRSAEncryption
     Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
     Validity
          Not Before: Sep 29 07:10:23 2025 GMT
          Not After : Sep 27 07:10:23 2035 GMT
     Subject: C = US, O = Bank32A Inc., CN = www.bank32a.com
     Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
               RSA Public-Key: (2048 bit)
               Modulus:
                    00:c1:de:ea:97:3f:5a:cc:cd:76:22:0c:31:0c:71:
                    71:1d:3a:3d:c1:b8:9b:5b:d9:c8:ca:f0:52:22:f6:
                    d2:8e:08:97:24:8f:5d:cc:60:c5:89:f8:5b:8a:d3:
                    e1:0f:19:48:ea:fd:ed:2e:4e:a4:e3:09:c0:7f:bd:
                    4c:14:d4:08:e4:ea:44:8e:84:97:e0:33:ed:ad:81:
                    ce:5b:2f:27:1f:ef:6d:18:4e:0f:ca:bc:a4:61:e9:
                    de:f0:cb:87:d5:27:63:cd:37:24:2c:b2:41:48:ce:
                    ec:0c:ea:17:c1:f1:75:f0:7d:30:43:74:ef:e4:cd:
                    de:cf:b6:9e:5f:d0:0f:1e:51:20:09:3f:f5:23:48:
                    7c:56:8f:04:29:c8:b4:c7:22:b8:1c:55:03:0f:8f:
                    15:75:cc:69:a8:94:b7:b9:ed:ab:82:b7:b8:e5:af:
                    31:de:1e:a2:cb:c9:a3:a9:87:d8:26:1d:10:b1:8a:
                    9f:33:77:d6:4e:9b:53:fa:bd:4d:de:21:24:62:38:
                    ef:1f:3b:2a:67:14:54:da:5f:68:e6:41:51:62:36:
                    6e:64:26:d9:b4:aa:91:20:dc:06:0e:ef:00:59:ab:
                    bc:80:24:d2:e1:4e:d8:34:e1:0a:60:8c:cf:fd:d8:
                    9b:80:c3:bf:e2:5e:f4:ec:83:65:7e:f1:a1:a0:9f:
                    6f:f5
               Exponent: 65537 (0x10001)
     X509v3 extensions:
          X509v3 Basic Constraints:
               CA:FALSE
          Netscape Comment:
               OpenSSL Generated Certificate
          X509v3 Subject Key Identifier:

19:0D:B1:ED:75:64:8D:AC:22:FE:45:D6:71:70:61:E3:07:D5:84:94
          X509v3 Authority Key Identifier:

keyid:CF:3B:C4:2E:A5:3F:C6:64:A4:5E:5E:85:7F:9A:EB:8A:2A:FA:23:8E

     Signature Algorithm: sha256WithRSAEncryption
     2f:44:cd:a6:a8:56:66:e6:c1:db:1d:67:ba:19:12:9e:62:aa:
     de:a6:f7:61:8e:ba:4c:21:96:8b:c6:11:b8:a0:3f:b0:e2:ee:
     4f:16:0d:bb:4a:99:f7:a1:99:85:10:aa:24:97:9a:cd:51:41:
     cd:ee:29:97:22:63:64:42:5a:1c:70:6e:d4:89:04:54:bf:e0:
     6c:64:98:e9:88:6a:48:b6:12:21:85:a7:4c:77:df:07:a5:2c:
```

```
db:7a:73:b1:af:d4:3d:ac:8a:dc:3d:ff:9e:f3:d1:81:8c:0f:
a1:09:d1:00:1e:c0:20:ca:92:de:ce:68:5f:78:b2:ea:21:2a:
ec:5e:ee:d9:d7:0b:58:c1:b9:4d:b7:0a:81:3a:af:7b:c1:32:
42:d9:78:c8:62:4b:11:70:36:a7:d2:e9:bc:bd:9b:78:dd:10:
27:f3:7c:94:b1:b5:e0:00:10:a9:c7:09:94:36:df:4c:73:f5:
ed:95:0f:10:b0:2e:ab:83:c0:76:85:f0:fd:9d:03:4e:bd:94:
d3:92:60:bf:34:18:e9:71:06:39:ee:81:26:93:d0:da:41:5c:
2e:e3:a6:28:f4:3a:1d:77:2c:40:25:dd:93:72:82:ca:08:ac:
5a:69:65:6d:bd:f8:42:b8:88:b2:c7:83:b0:42:67:26:32:56:
47:48:27:44:51:4d:c8:d8:a5:de:1d:75:8d:64:f4:c6:5c:54:
e8:97:5a:a6:da:70:9c:df:f8:77:25:6d:21:80:42:cc:bf:21:
6e:95:e4:1f:bd:23:db:6f:55:b1:67:35:2e:c6:28:82:99:b5:
55:5f:dc:f9:d4:02:9c:d4:2f:40:2d:64:30:56:f1:46:28:f9:
40:59:fc:52:5e:6f:ec:d1:01:5b:b5:62:1c:50:58:0d:fd:a9:
49:2d:a1:15:7d:2d:71:8f:a2:39:bb:44:d9:0f:a6:4c:44:9a:
2e:6d:c1:5d:45:1a:70:82:06:f4:bc:9c:69:f9:4c:34:c3:2d:
cc:eb:9a:0e:f6:ac:ae:c5:e2:44:39:f3:3f:32:f1:39:2f:b0:
ca:02:de:e3:66:68:35:d6:95:d7:c1:c4:fe:4b:12:e8:2d:c5:
cb:7c:4b:c5:58:8a:34:2c:41:df:0a:6e:dc:35:a8:ad:e5:c6:
3f:cc:05:4d:1b:02:52:25:46:43:72:04:15:ac:b8:24:8a:55:
13:28:b9:e2:1c:a8:5d:59:06:aa:a0:7a:fd:07:84:f3:30:aa:
b7:f7:77:54:1b:57:a4:0a:37:b4:3a:b5:da:7b:2e:82:2d:63:
9e:c2:6e:8e:e0:73:89:bf:5a:f0:3b:1d:31:78:3a:5d:55:04:
84:f5:ab:c4:4b:be:39:21
```

Deploying Certificate in an Apache-Based HTTPS Website

In this subtask, the objective is to deploy a certificate authority in an apache-based HTTPS Website. For this, we will be using the exact files made from the previous task when creating the bank32a.com server.

```
[10/02/25]seed@VM:~/.../Labsetup$ cp -r  work_dir/ volumes/
[10/02/25]seed@VM:~/.../Labsetup$ ls volumes/
README.md  work_dir
[10/02/25]seed@VM:~/   /Labsetup$
```

Figure 23. Copying all the Files of the Current Working Directory onto the Container

The first step is to duplicate all of the files made in the Virtual Machine onto the container via the share volumes directory (See Figure 23).

```
[10/02/25]seed@VM:~/.../Labsetup$ docksh e
root@ef27b6152fba:/# ls
bin   certs  etc   lib    lib64   media  opt   root  sbin  sys  usr  volumes
boot  dev    home  lib32  libx32  mnt    proc  run   srv   tmp  var
root@ef27b6152fba:/# cd /etc/apache2
root@ef27b6152fba:/etc/apache2# cd sites-available/
root@ef27b6152fba:/etc/apache2/sites-available# ls
000-default.conf  bank32_apache_ssl.conf  default-ssl.conf
```

Figure 24. Entering the Container

```
root@ef27b6152fba:/# ls /volumes/work_dir/demoCA/certs/
root@ef27b6152fba:/# cp /volumes/work_dir/server.crt /certs/
root@ef27b6152fba:/# cp /volumes/work_dir/server.key /certs/
root@ef27b6152fba:/# ls /certs/
bank32.crt  bank32.key  server.crt  server.key
root@ef27b6152fba:/#
```

Figure 25. Copying the server.crt and the server.key onto the certs directory

We also ought to copy the server's crt and key onto the /cert directory.

```
root@ef27b6152fba:/etc/apache2/sites-available# cat bank32A_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32A
    ServerName www.bank32A.com
    ServerAlias www.bank32AA.com
    ServerAlias www.bank32AB.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32A
    ServerName www.bank32A.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
root@ef27b6152fba:/etc/apache2/sites-available#
```

Figure 26.Editing bank32_apache_ssl.conf to match the used servname bank32A.com

We then edit the bank32_apache_ssl to a custom bank32a_apache_ssl.com specific for the bank32a.com server.

```
root@ef27b6152fba:/var/www# cp -r bank32/ bank32A/
root@ef27b6152fba:/var/www# ls
bank32  bank32A  html
root@ef27b6152fba:/var/www#
```

Figure 27. Creating a /var/www directory for new bank32A.com

```
 GNU nano 4.8                          bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32A
    ServerName www.bank32A.com
    ServerAlias www.bank32AA.com
    ServerAlias www.bank32AB.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/bank32.crt
    SSLCertificateKeyFile /certs/bank32.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    DirectoryIndex index_red.html
</VirtualHost>
```

Figure 28. Editing bank32_apache_ssl.conf to match the used servname bank32A.com

```
root@ef27b6152fba:/etc/apache2/sites-available# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
root@ef27b6152fba:/etc/apache2/sites-available# a2ensite bank32A_apache_ssl
Site bank32A_apache_ssl already enabled
root@ef27b6152fba:/etc/apache2/sites-available# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.bank32A.com:443 (RSA):
 *
root@ef27b6152fba:/etc/apache2/sites-available#
```

Figure 29. Running the scripts to deploy the apache server

After configuring the files, we then deploy the apache serve by using the command shown in Figure 29. Thereafter, we add the new DNS components onto the /etc/hosts.

```
10.9.0.80       www.bank32.com
10.9.0.80 www.smith2020.com
10.9.0.80       www.bank32A.com
10.9.0.80       www.bank32AA.com
10.9.0.80       www.bank32AB.com


                                [ Wrote 39 lines ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text
^X Exit         ^R Read File    ^\ Replace      ^U Paste Text
```

Figure 30. Adding the newDNS in the /etc/hosts file


```
[10/02/25]seed@VM:/$ ping www.bank32A.com
PING www.bank32A.com (10.9.0.80) 56(84) bytes of data.
64 bytes from www.seedlab-shellshock.com (10.9.0.80): icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from www.seedlab-shellshock.com (10.9.0.80): icmp_seq=2 ttl=64 time=0.057 ms
^C
--- www.bank32A.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.057/0.280/0.504/0.223 ms
[10/02/25]seed@VM:/$
```

Figure 31. Successfully Deployed Apache Server

As seen in Figure 31, we can now enter the website bank32A.com. Furthermore, when this website was landed, a security risk message was prompted ontothe user.

Figure 32. Running with just Http

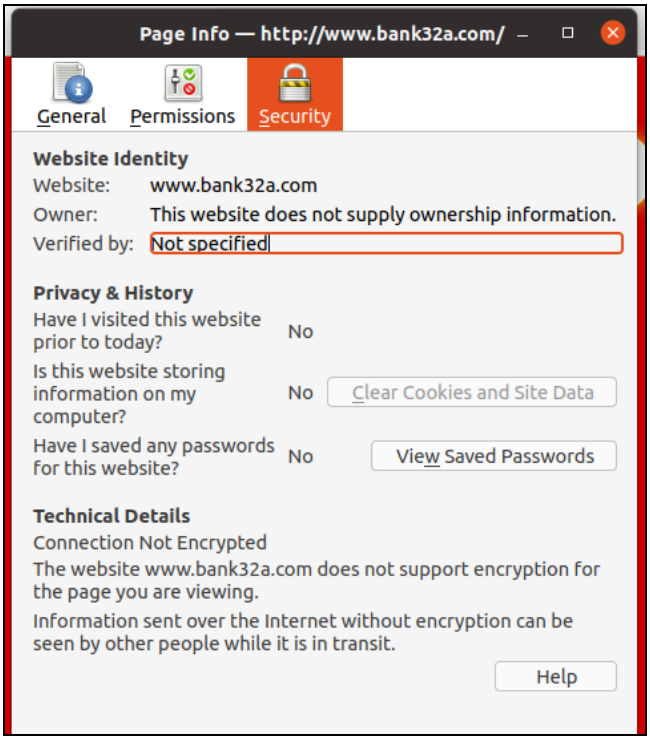

Figure 33.Analyzing the Security Information of [bank32a.com]

Analyzing the Security Details of the Website, it was disclosed that the browser Firefox was not specified on what verification authority (certification authority) was used for this website. That is why it was not trusted, since the CA that we used was just self-made (Mozilla Support, 2025).

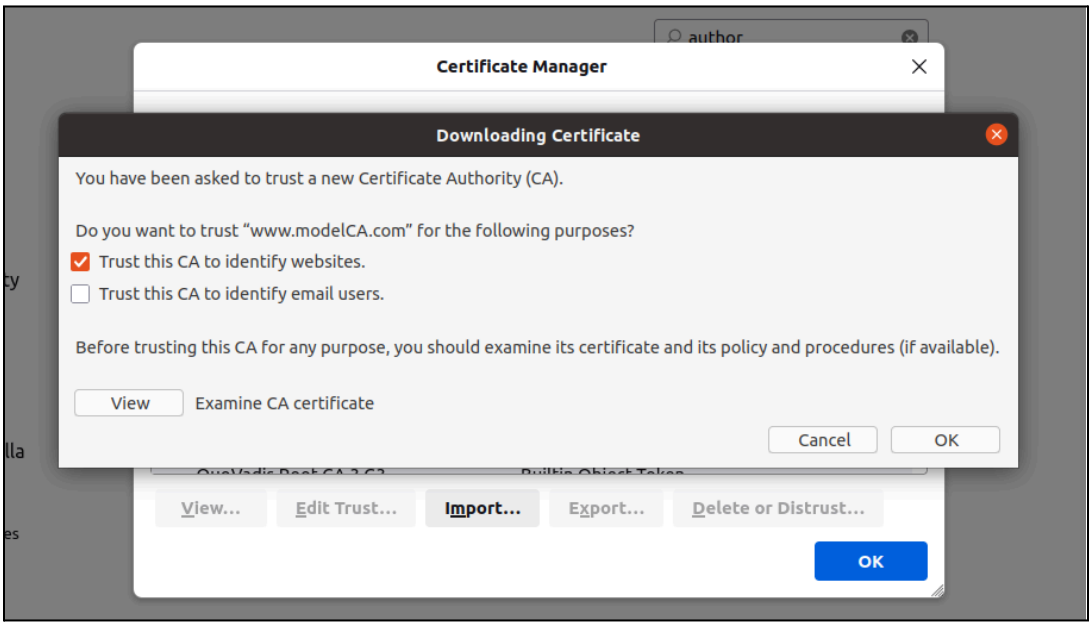

Figure 34. Adding new CA.

After adding the new CA, no security risk prompt was shown.

Launching a Man-In-The-Middle Attack

This task aims to simulate a Man-In-The-Middle Attack via creating a decoy example.com webiste.

Setting up the malicious website.

```
  GNU nano 4.8                        bank32A_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32A
    ServerName www.example.com
    ServerAlias www.bank32AA.com
    ServerAlias www.bank32AB.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32A
    ServerName www.bank32A.com
    DirectoryIndex index_red.html
</VirtualHost>
```

Figure 35. Changing the ServerName into www.example.com

Becoming the Man in The Middle

```
  GNU nano 4.8                                /etc/hosts

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com

10.9.0.80       www.bank32.com
10.9.0.80 www.smith2020.com
10.9.0.80       www.bank32A.com
10.9.0.80       www.bank32AA.com
10.9.0.80       www.bank32AB.com
10.9.0.80       www.example.com


                            [ Wrote 39 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
```

Figure 36. Adding www.example.com in the etc/hosts file

Browsing Target Website

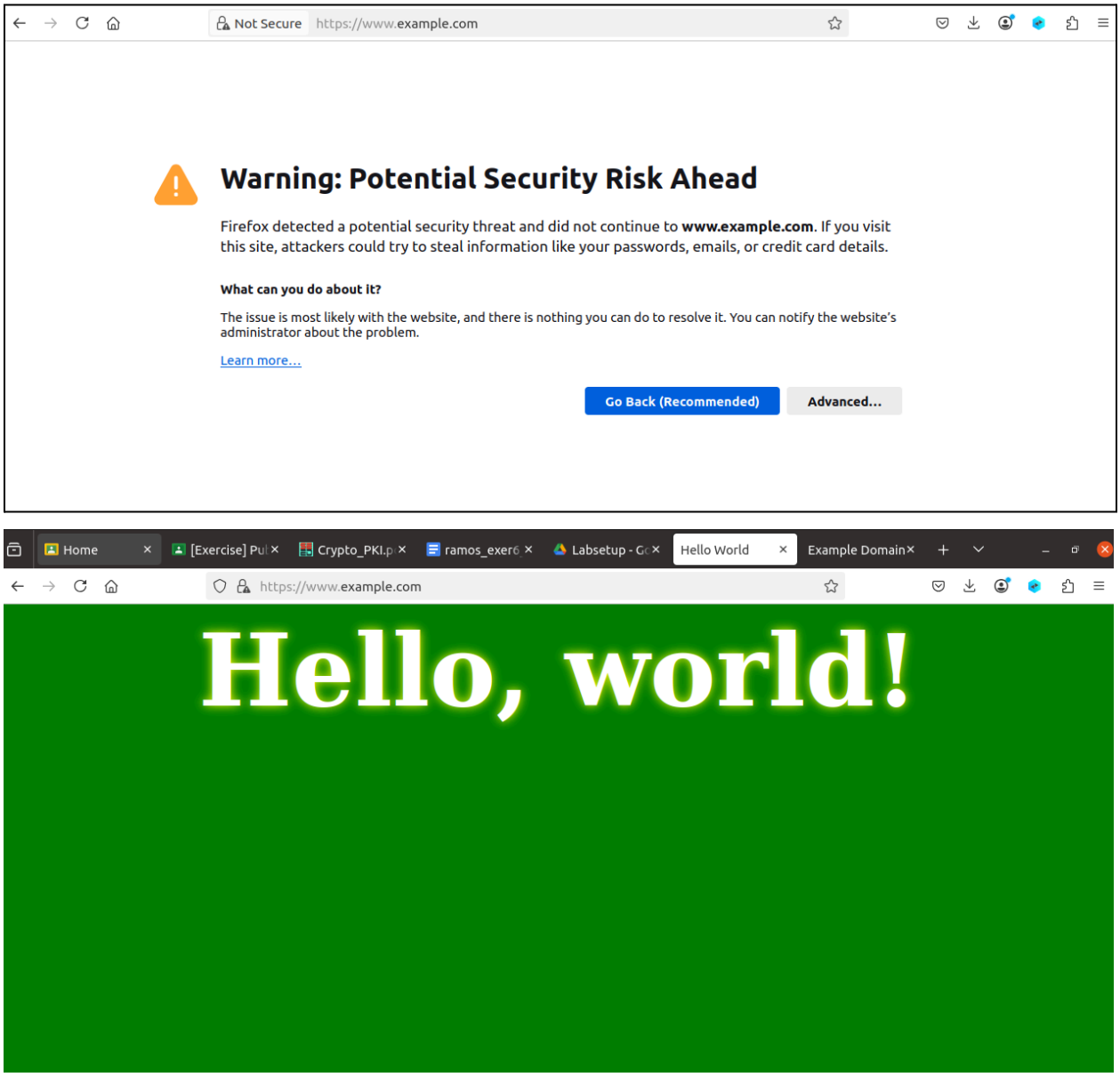

Figure 37. Visiting www.example.com; similar to the browser when visiting www.bank32a.com

This shows that example.com is now posing as a website for bank32a.com server. However, unlike how bank32A.com's security message was resolve, there exists again such message again since the server pass by the browser was only made for the server name bank32a.com

Launching a Man-In-The-Middle Attack with a Compromised CA

For this part of the laboratory report, the main goal is to establish a compromised Certificate Authority that will act as the verification for the man in the middle in bank32a.com – the website we just launched.

For this to be done, we ought to remake the creation of servery keys and server certs for a compromised CA. We then try to replicate the steps from tasks 4 and 5 but with the servername as example.com this time (See Figure 38 to 43).

```
[10/02/25]seed@VM:~/.../work_dir$ openssl req -newkey rsa:2048 -nodes -sha256 \
>   -keyout compromised_key.pem \
>   -out compromised.csr \
>   -subj "/CN=www.example.com/O=Compromised CA Demo/C=US" \
>   -addext "subjectAltName=DNS:www.example.com"
Generating a RSA private key
..................+++++
..................+++++
writing new private key to 'compromised_key.pem'
-----
[10/02/25]seed@VM:~/.../work_dir$ ls
ca.crt  compromised.csr      compromised_www_example_key.pem  myCA_openssl.cnf  server.csr
ca.key  compromised_key.pem  demoCA                           server.crt        server.key
[10/02/25]seed@VM:~/.../work_dir$
```

Figure 38. Creating Compromised key and csr

```
[10/02/25]seed@VM:~/.../work_dir$ ls
ca.crt  compromised.csr      compromised_www_example_key.pem  myCA_openssl.cnf  server.csr
ca.key  compromised_key.pem  demoCA                           server.crt        server.key
[10/02/25]seed@VM:~/.../work_dir$ openssl x509 -req -in compromised.csr \
>   -CA ca.crt -CAkey ca.key -CAcreateserial \
>   -out compromised.crt -days 365 -sha256 \
>   -extfile <(printf "subjectAltName=DNS:www.example.com")
Signature ok
subject=CN = www.example.com, O = Compromised CA Demo, C = US
Getting CA Private Key
Enter pass phrase for ca.key:
[10/02/25]seed@VM:~/.../work_dir$
```

Figure 39.Signing the csr with the Comrpomised CA made

```
root@ef27b6152fba:/# ls
bin   certs  etc   lib    lib64   media  opt   root  sbin  sys  usr  volumes
boot  dev    home  lib32  libx32  mnt    proc  run   srv   tmp  var
root@ef27b6152fba:/# cp volumes/work_dir/compromised.crt /certs/
root@ef27b6152fba:/# cp volumes/work_dir/compromised_key.pem /certs/
root@ef27b6152fba:/# ls certs/
bank32.crt  bank32.key  compromised.crt  compromised_key.pem  server.crt  server.key
root@ef27b6152fba:/#
```

Figure 40. Copying the compromised.crt and the compromised_key.pem to the certs directory

```
  GNU nano 4.8                    example_apache_ssl.conf                    Modif
<VirtualHost *:443>
    DocumentRoot /var/www/html
    ServerName www.example.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/compromised.crt
    SSLCertificateKeyFile /certs/compromised_key.pem
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32A
    ServerName www.bank32A.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost

^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
```

Figure 41. Creating an example_apache_ssl.conf for the example.com

```
root@ef27b6152fba:/etc/apache2/sites-available# nano example_apache_ssl.conf
root@ef27b6152fba:/etc/apache2/sites-available# a2ensite example_apache_ssl
Enabling site example_apache_ssl.
To activate the new configuration, you need to run:
  service apache2 reload
root@ef27b6152fba:/etc/apache2/sites-available# apache2ctl -t
Syntax OK
root@ef27b6152fba:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.bank32A.com:443 (RSA):

root@ef27b6152fba:/etc/apache2/sites-available# ping www.example.com
PING www.example.com (10.9.0.80) 56(84) bytes of data.
64 bytes from ef27b6152fba (10.9.0.80): icmp_seq=1 ttl=64 time=0.168 ms
64 bytes from ef27b6152fba (10.9.0.80): icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from ef27b6152fba (10.9.0.80): icmp_seq=3 ttl=64 time=0.047 ms
^C
--- www.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2057ms
rtt min/avg/max/mdev = 0.047/0.087/0.168/0.057 ms
root@ef27b6152fba:/etc/apache2/sites-available#
```

Figure 42. Starting the new apache server with example.com as the MITM

Figure 43. Successfully Landing example.com without the Security Risk Message.

After conducting the MITM with the compromised CA, it can be seen that the security risk message has been completely obliterated in the landing page of example.com. Meaning, it had completely fooled the CA permitted in the Firefox browser.

Challenges and Troubleshooting

I believe that the main challenge that I faced when creating this laboratory report was devising ways on how to establish the Man-in-the-Middle Attack. This requires a through understanding on how the browser being used, Mozilla Firefox, takes into account the security risk in visiting HTTPS websites. I believe that referencing the documentations such as Help Desk Support was very helpful in understanding the vulnerabilities and the attack surfaces that can be exploited.

To wit, this begs the understanding that MITM Attacks may be browser specific.

Discussion

Public Key Infrastructure, with its incorporation of Certificate Authorities, had truly revolutionized encryption. In a sense, it had utilized asymmetric encryption to make authentication more practical especially for browser verifications. However, there still exists the risks on using such such as how it allows the vulnerability to attacks on Man-In-The-Middle. Nonetheless, PKI could still be used to further strengthen the security of communication between various servers and machines.

References

Du, W. (2016). Public-Key Infrastructure. SEED Project.

Mozilla Support. (2025, August 26). *What do the security warning codes mean? | Firefox Help*. Mozilla Support. Retrieved October 2, 2025, from https://support.mozilla.org/en-US/kb/what-does-your-connection-is-not-secure-mean