Applied Cryptography Lab-06 Manual

20 October 2022 22:23

Name: Vishwas M

SRN: PES2UG20CS390

SEC: F

DATE: 26/10/2022

LAB: 5

Prerequisites

Labsetup files - https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_PKI/

Task 1: Becoming a certificate authority (CA)

Firstly, copy the /usr/lib/ssl/openssl.cnf file to your working directory

Then create the following files and directories in the working directory:

```
pki_lab
  - demoCA
      - certs (dir)
      - crl (dir)
      - newcerts (dir)
      - index.txt (blank text file)
      - Serial (contains a 4 digit number, no line ending)
```

Creating certificate authority

Command

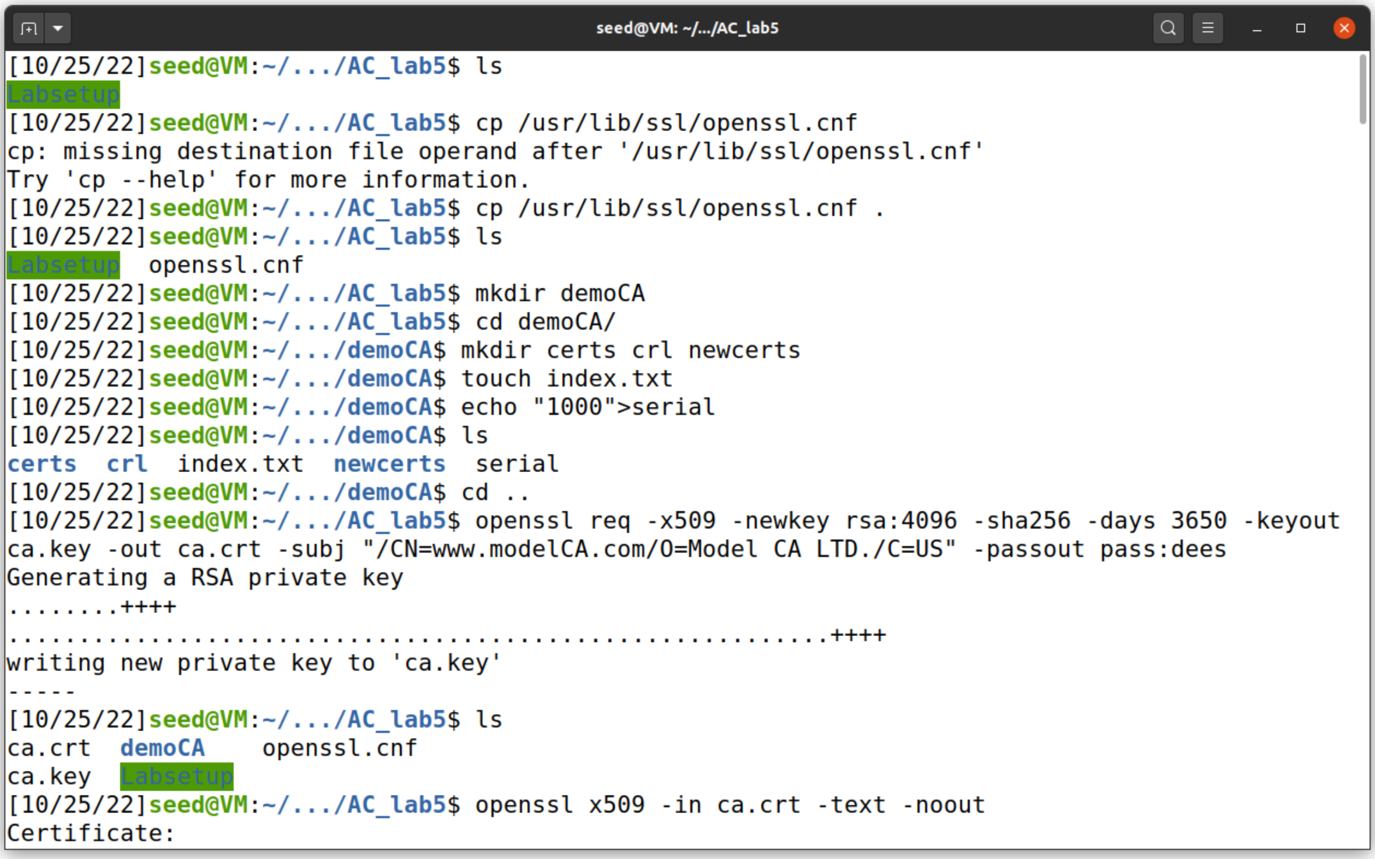
```
$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
 -keyout ca.key -out ca.crt \
 -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" \
 -passout pass:dees
```

Remember the passphrase, you'll have to use it in later tasks!

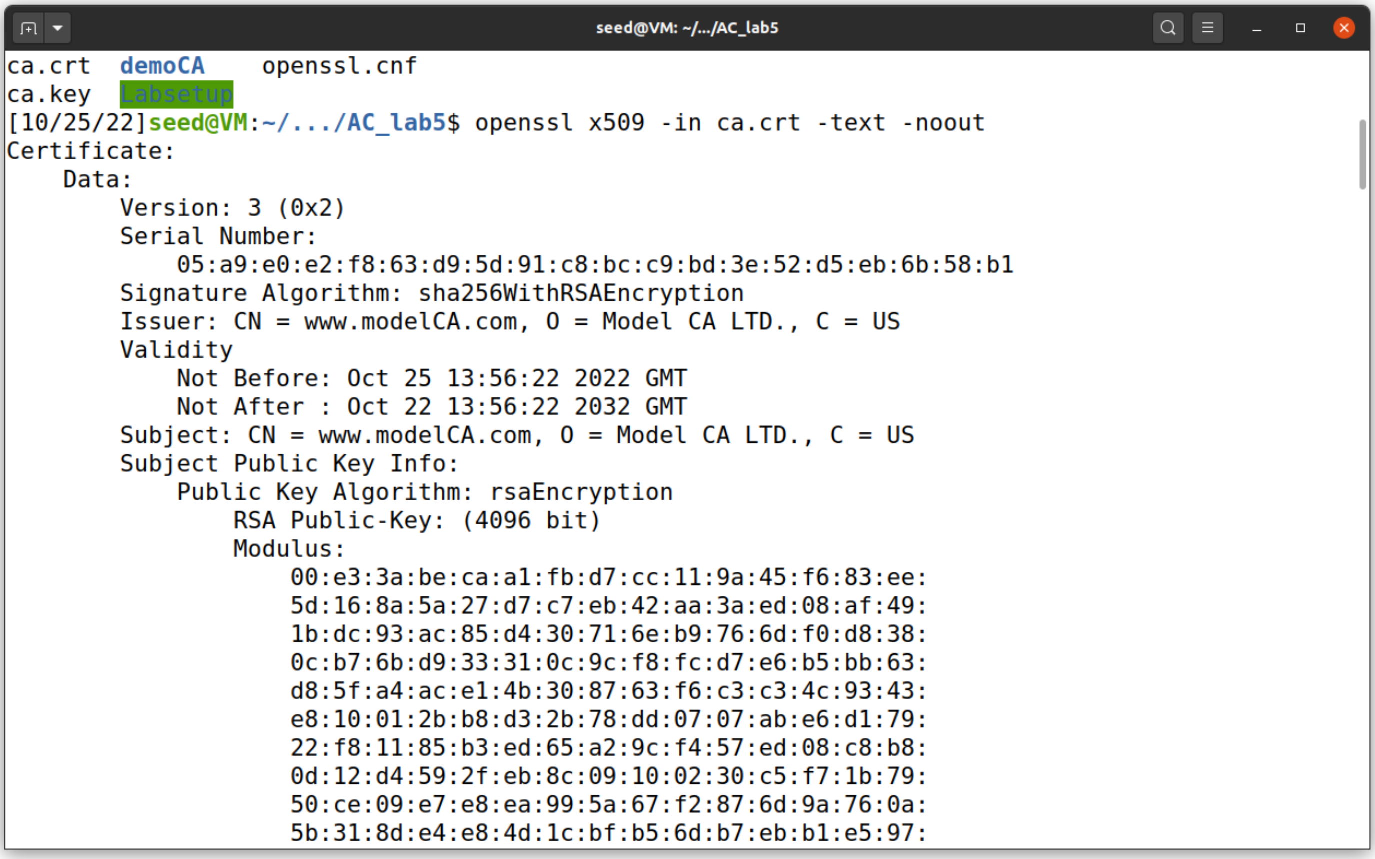
Viewing the contents of files generated

Commands

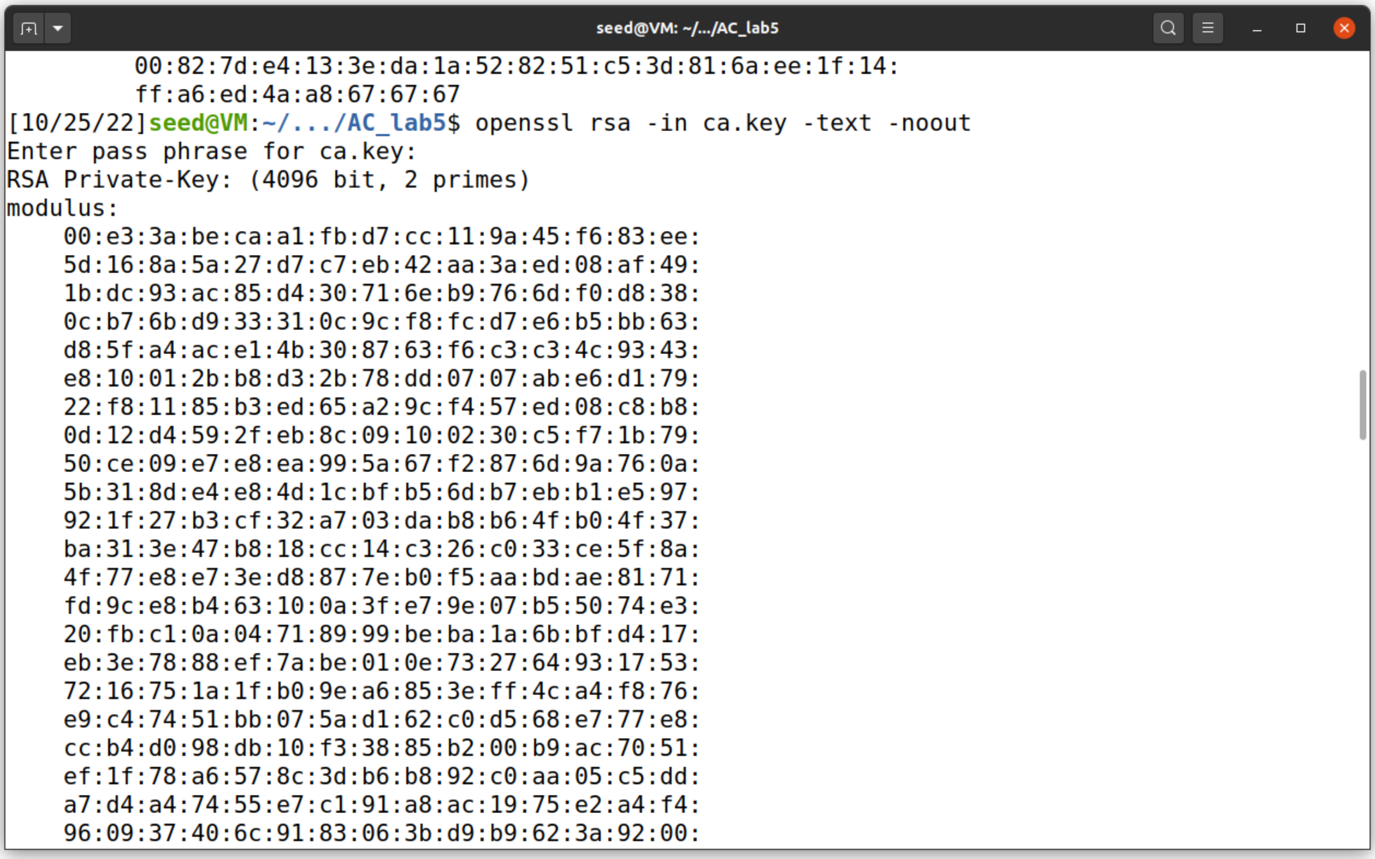
```
$ openssl x509 -in ca.crt -text -noout
$ openssl rsa -in ca.key -text -noout
```



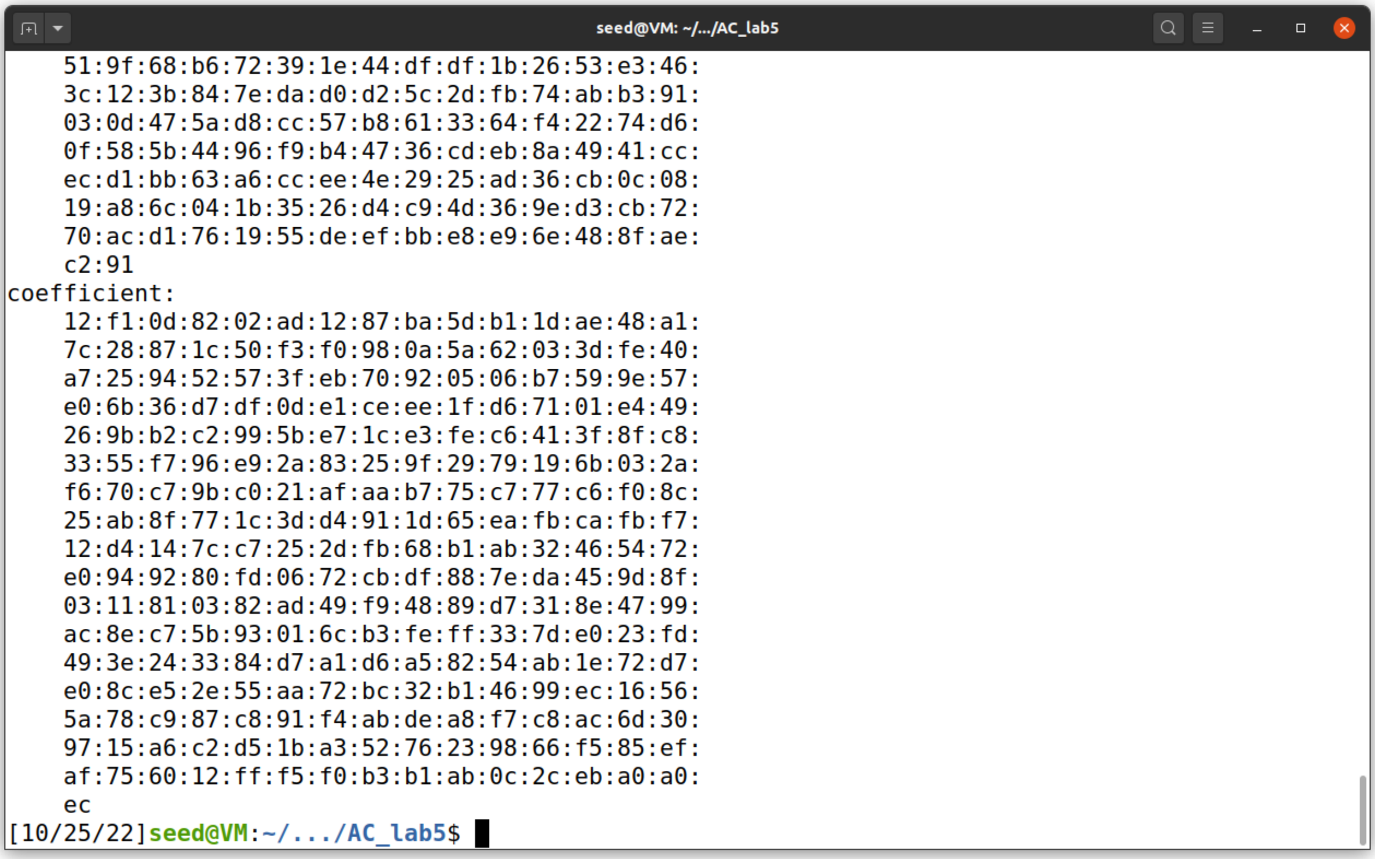
```
[10/25/22]seed@VM:~/.../AC_lab5$ ls
Labsetup
[10/25/22]seed@VM:~/.../AC_lab5$ cp /usr/lib/ssl/openssl.cnf
cp: missing destination file operand after '/usr/lib/ssl/openssl.cnf'
Try 'cp --help' for more information.
[10/25/22]seed@VM:~/.../AC_lab5$ cp /usr/lib/ssl/openssl.cnf .
[10/25/22]seed@VM:~/.../AC_lab5$ ls
Labsetup  openssl.cnf
[10/25/22]seed@VM:~/.../AC_lab5$ mkdir demoCA
[10/25/22]seed@VM:~/.../AC_lab5$ cd demoCA/
[10/25/22]seed@VM:~/.../demoCA$ mkdir certs crl newcerts
[10/25/22]seed@VM:~/.../demoCA$ touch index.txt
[10/25/22]seed@VM:~/.../demoCA$ echo "1000">serial
[10/25/22]seed@VM:~/.../demoCA$ ls
certs  crl  index.txt  newcerts  serial
[10/25/22]seed@VM:~/.../demoCA$ cd ..
[10/25/22]seed@VM:~/.../AC_lab5$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -keyout
ca.key -out ca.crt -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" -passout pass:dees
Generating a RSA private key
........++++
..........................................................++++
writing new private key to 'ca.key'
-----
[10/25/22]seed@VM:~/.../AC_lab5$ ls
ca.crt  demoCA    openssl.cnf
ca.key  Labsetup
[10/25/22]seed@VM:~/.../AC_lab5$ openssl x509 -in ca.crt -text -noout
Certificate:
```



```
ca.crt  demoCA    openssl.cnf
ca.key  Labsetup
[10/25/22]seed@VM:~/.../AC_lab5$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:a9:e0:e2:f8:63:d9:5d:91:c8:bc:c9:bd:3e:52:d5:eb:6b:58:b1
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 25 13:56:22 2022 GMT
            Not After : Oct 22 13:56:22 2032 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:e3:3a:be:ca:a1:fb:d7:cc:11:9a:45:f6:83:ee:
                    5d:16:8a:5a:27:d7:c7:eb:42:aa:3a:ed:08:af:49:
                    1b:dc:93:ac:85:d4:30:71:6e:b9:76:6d:f0:d8:38:
                    0c:b7:6b:d9:33:31:0c:9c:f8:fc:d7:e6:b5:bb:63:
                    d8:5f:a4:ac:e1:4b:30:87:63:f6:c3:c3:4c:93:43:
                    e8:10:01:2b:b8:d3:2b:78:dd:07:07:ab:e6:d1:79:
                    22:f8:11:85:b3:ed:65:a2:9c:f4:57:ed:08:c8:b8:
                    0d:12:d4:59:2f:eb:8c:09:10:02:30:c5:f7:1b:79:
                    50:ce:09:e7:e8:ea:99:5a:67:f2:87:6d:9a:76:0a:
                    5b:31:8d:e4:e8:4d:1c:bf:b5:6d:b7:eb:b1:e5:97:
```



```
        00:82:7d:e4:13:3e:da:1a:52:82:51:c5:3d:81:6a:ee:1f:14:
        ff:a6:ed:4a:a8:67:67:67
[10/25/22]seed@VM:~/.../AC_lab5$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:e3:3a:be:ca:a1:fb:d7:cc:11:9a:45:f6:83:ee:
    5d:16:8a:5a:27:d7:c7:eb:42:aa:3a:ed:08:af:49:
    1b:dc:93:ac:85:d4:30:71:6e:b9:76:6d:f0:d8:38:
    0c:b7:6b:d9:33:31:0c:9c:f8:fc:d7:e6:b5:bb:63:
    d8:5f:a4:ac:e1:4b:30:87:63:f6:c3:c3:4c:93:43:
    e8:10:01:2b:b8:d3:2b:78:dd:07:07:ab:e6:d1:79:
    22:f8:11:85:b3:ed:65:a2:9c:f4:57:ed:08:c8:b8:
    0d:12:d4:59:2f:eb:8c:09:10:02:30:c5:f7:1b:79:
    50:ce:09:e7:e8:ea:99:5a:67:f2:87:6d:9a:76:0a:
    5b:31:8d:e4:e8:4d:1c:bf:b5:6d:b7:eb:b1:e5:97:
    92:1f:27:b3:cf:32:a7:03:da:b8:b6:4f:b0:4f:37:
    ba:31:3e:47:b8:18:cc:14:c3:26:c0:33:ce:5f:8a:
    4f:77:e8:e7:3e:d8:87:7e:b0:f5:aa:bd:ae:81:71:
    fd:9c:e8:b4:63:10:0a:3f:e7:9e:07:b5:50:74:e3:
    20:fb:c1:0a:04:71:89:99:be:ba:1a:6b:bf:d4:17:
    eb:3e:78:88:ef:7a:be:01:0e:73:27:64:93:17:53:
    72:16:75:1a:1f:b0:9e:a6:85:3e:ff:4c:a4:f8:76:
    e9:c4:74:51:bb:07:5a:d1:62:c0:d5:68:e7:77:e8:
    cc:b4:d0:98:db:10:f3:38:85:b2:00:b9:ac:70:51:
    ef:1f:78:a6:57:8c:3d:b6:b8:92:c0:aa:05:c5:dd:
    a7:d4:a4:74:55:e7:c1:91:a8:ac:19:75:e2:a4:f4:
    96:09:37:40:6c:91:83:06:3b:d9:b9:62:3a:92:00:
```



```
    51:9f:68:b6:72:39:1e:44:df:df:1b:26:53:e3:46:
    3c:12:3b:84:7e:da:d0:d2:5c:2d:fb:74:ab:b3:91:
    03:0d:47:5a:d8:cc:57:b8:61:33:64:f4:22:74:d6:
    0f:58:5b:44:96:f9:b4:47:36:cd:eb:8a:49:41:cc:
    ec:d1:bb:63:a6:cc:ee:4e:29:25:ad:36:cb:0c:08:
    19:a8:6c:04:1b:35:26:d4:c9:4d:36:9e:d3:cb:72:
    70:ac:d1:76:19:55:de:ef:bb:e8:e9:6e:48:8f:ae:
    c2:91
coefficient:
    12:f1:0d:82:02:ad:12:87:ba:5d:b1:1d:ae:48:a1:
    7c:28:87:1c:50:f3:f0:98:0a:5a:62:03:3d:fe:40:
    a7:25:94:52:57:3f:eb:70:92:05:06:b7:59:9e:57:
    e0:6b:36:d7:df:0d:e1:ce:ee:1f:d6:71:01:e4:49:
    26:9b:b2:c2:99:5b:e7:1c:e3:fe:c6:41:3f:8f:c8:
    33:55:f7:96:e9:2a:83:25:9f:29:79:19:6b:03:2a:
    f6:70:c7:9b:c0:21:af:aa:b7:75:c7:77:c6:f0:8c:
    25:ab:8f:77:1c:3d:d4:91:1d:65:ea:fb:ca:fb:f7:
    12:d4:14:7c:c7:25:2d:fb:68:b1:ab:32:46:54:72:
    e0:94:92:80:fd:06:72:cb:df:88:7e:da:45:9d:8f:
    03:11:81:03:82:ad:49:f9:48:89:d7:31:8e:47:99:
    ac:8e:c7:5b:93:01:6c:b3:fe:ff:33:7d:e0:23:fd:
    49:3e:24:33:84:d7:a1:d6:a5:82:54:ab:1e:72:d7:
    e0:8c:e5:2e:55:aa:72:bc:32:b1:46:99:ec:16:56:
    5a:78:c9:87:c8:91:f4:ab:de:a8:f7:c8:ac:6d:30:
    97:15:a6:c2:d5:1b:a3:52:76:23:98:66:f5:85:ef:
    af:75:60:12:ff:f5:f0:b3:b1:ab:0c:2c:eb:a0:a0:
    ec
[10/25/22]seed@VM:~/.../AC_lab5$ 
```

Task 2: Generating a Certificate Request for the web server

Step 1 - Generate a public/private key pair

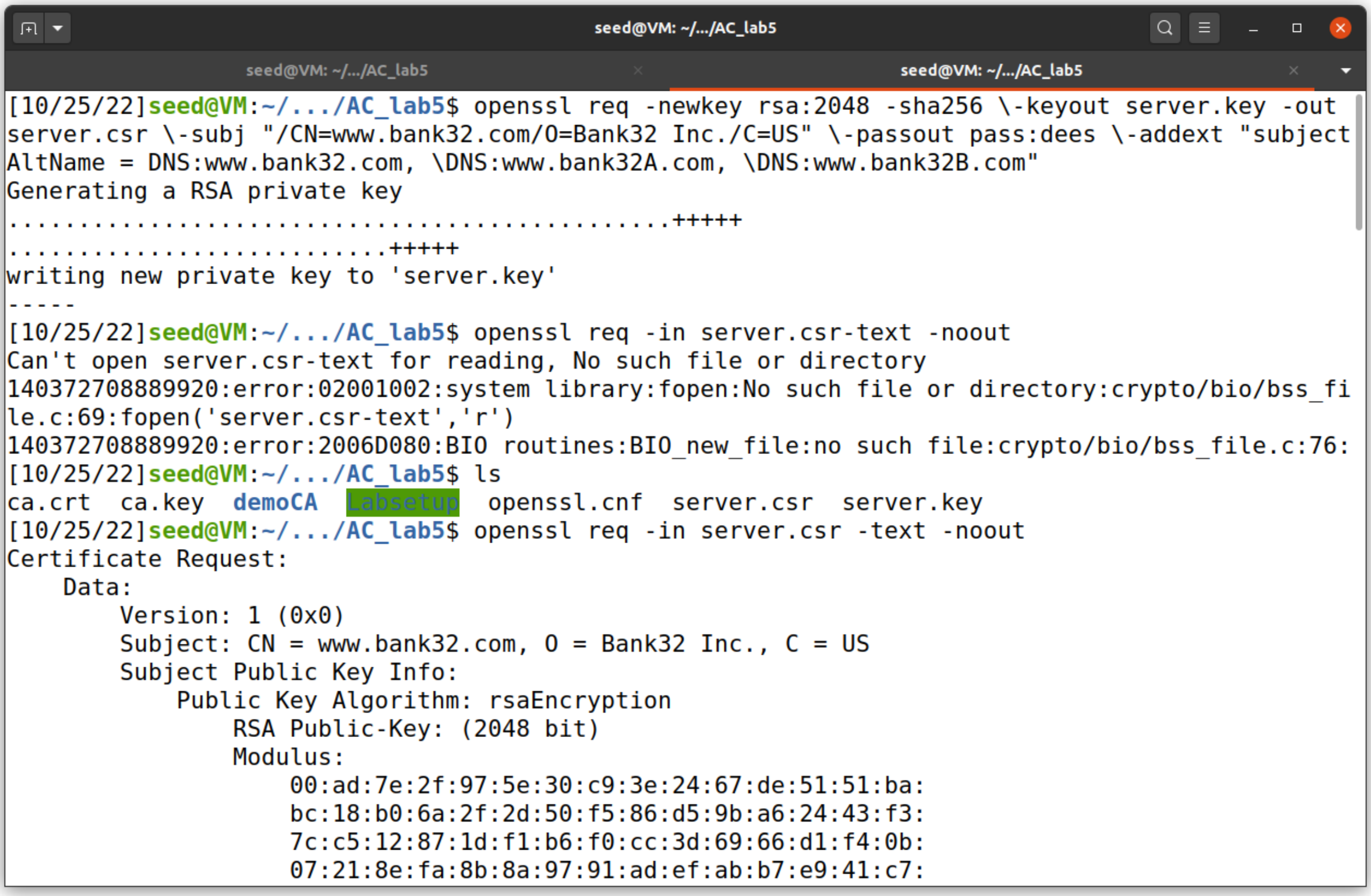
Command

```
$ openssl  req -newkey rsa:2048 -sha256 \
  -keyout server.key -out server.csr \
  -subj "/CN=www.bank32.com/O=Bank32 Inc./C=US" \
  -passout pass:dees \
  -addext "subjectAltName = DNS:www.bank32.com, \
   DNS:www.bank32A.com, \
   DNS:www.bank32B.com"
```

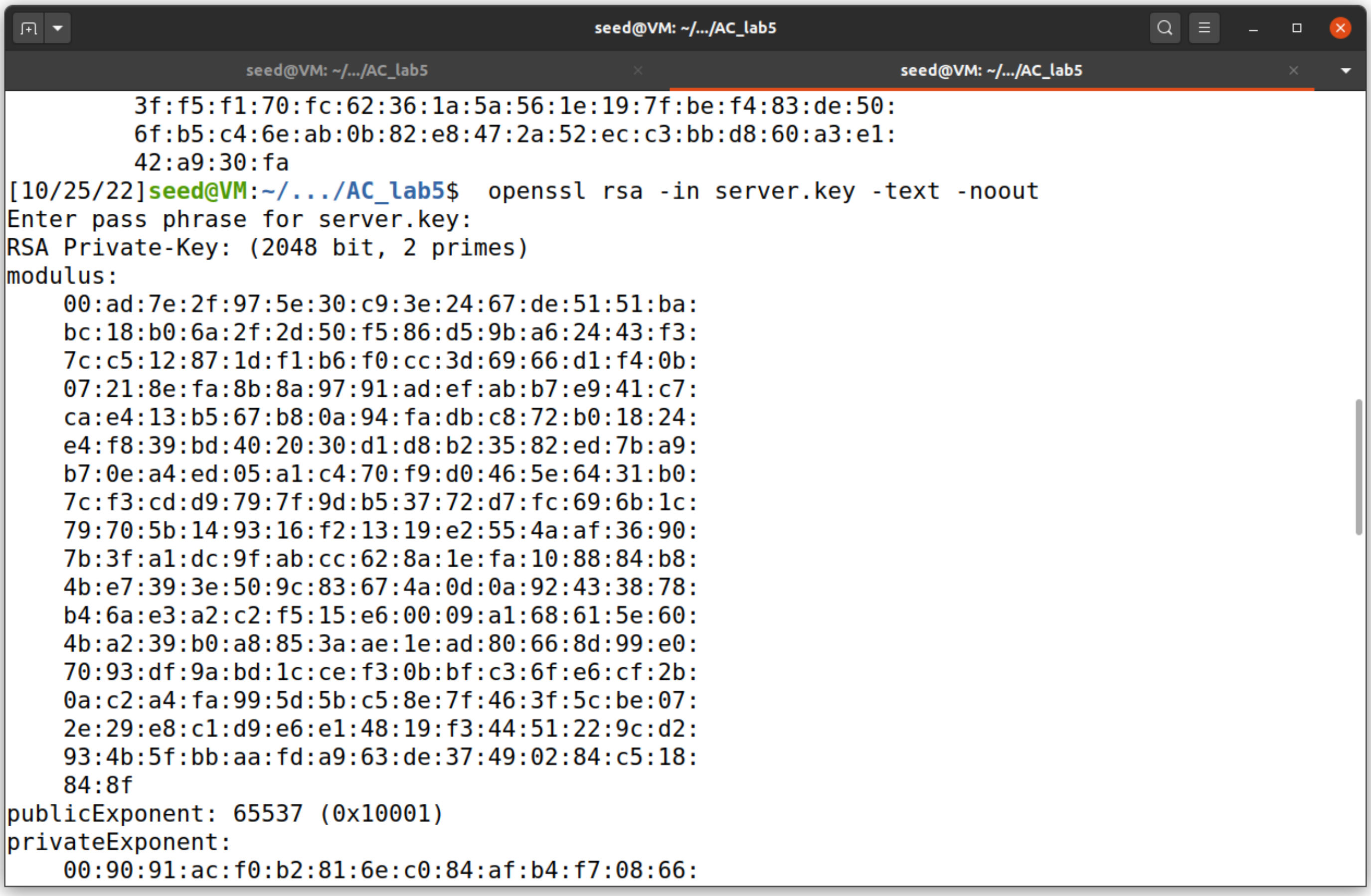
The keys will be stored in server.key
Again, keep track of the passphrase used.
View the created file using the command:

```
$ openssl req -in server.csr-text -noout
$ openssl rsa -in server.key -text -noout
```

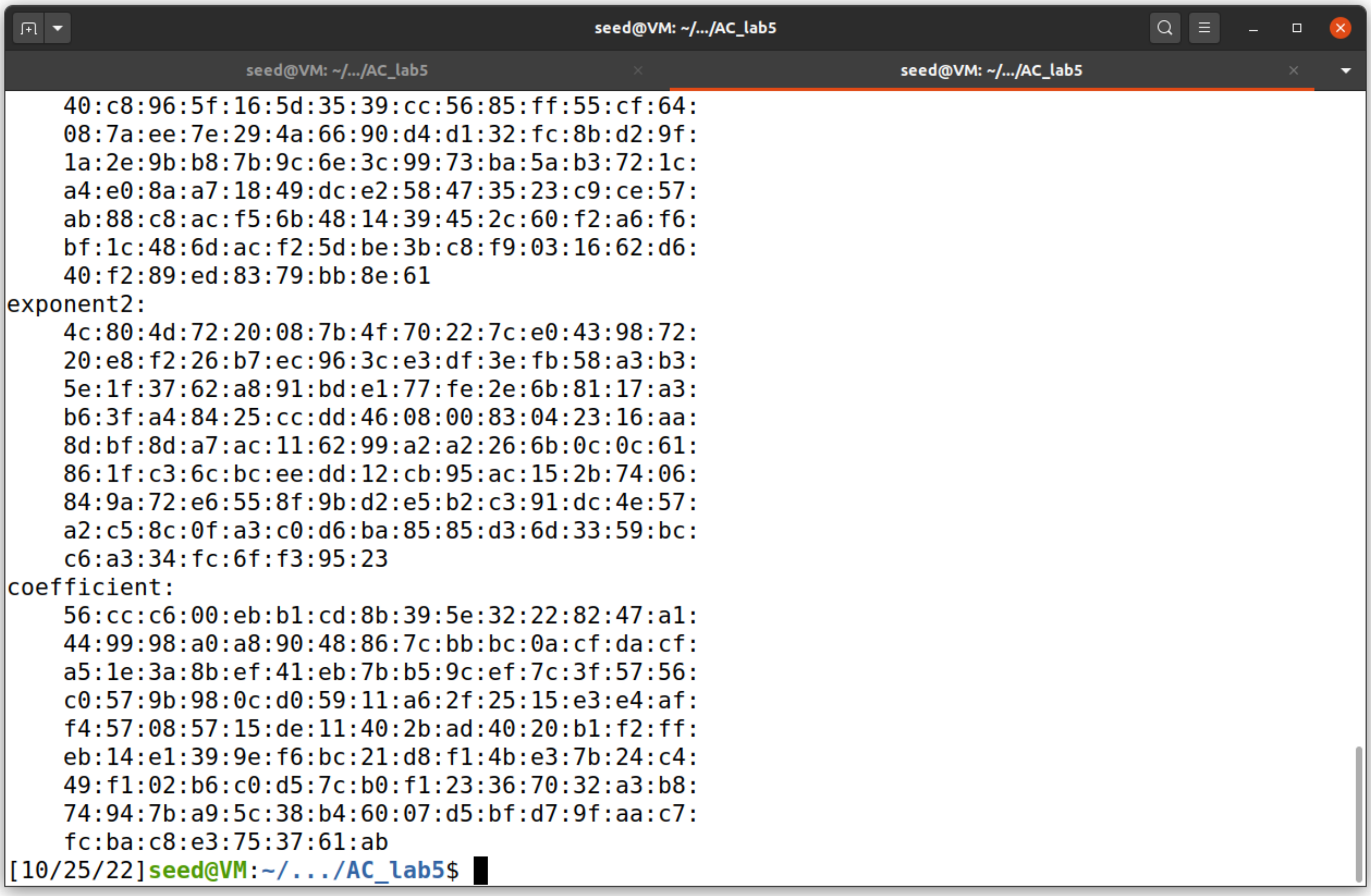
Take a screenshot and note your observations



```
[10/25/22]seed@VM:~/.../AC_lab5$ openssl req -newkey rsa:2048 -sha256 \-keyout server.key -out
server.csr \-subj "/CN=www.bank32.com/O=Bank32 Inc./C=US" \-passout pass:dees \-addext "subject
AltName = DNS:www.bank32.com, \DNS:www.bank32A.com, \DNS:www.bank32B.com"
Generating a RSA private key
...............................................+++++
...........................+++++
writing new private key to 'server.key'
-----
[10/25/22]seed@VM:~/.../AC_lab5$ openssl req -in server.csr-text -noout
Can't open server.csr-text for reading, No such file or directory
140372708889920:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_fi
le.c:69:fopen('server.csr-text','r')
140372708889920:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:76:
[10/25/22]seed@VM:~/.../AC_lab5$ ls
ca.crt  ca.key  demoCA  Labsetup  openssl.cnf  server.csr  server.key
[10/25/22]seed@VM:~/.../AC_lab5$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.bank32.com, O = Bank32 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ad:7e:2f:97:5e:30:c9:3e:24:67:de:51:51:ba:
                    bc:18:b0:6a:2f:2d:50:f5:86:d5:9b:a6:24:43:f3:
                    7c:c5:12:87:1d:f1:b6:f0:cc:3d:69:66:d1:f4:0b:
                    07:21:8e:fa:8b:8a:97:91:ad:ef:ab:b7:e9:41:c7:
```



```
         3f:f5:f1:70:fc:62:36:1a:5a:56:1e:19:7f:be:f4:83:de:50:
         6f:b5:c4:6e:ab:0b:82:e8:47:2a:52:ec:c3:bb:d8:60:a3:e1:
         42:a9:30:fa
[10/25/22]seed@VM:~/.../AC_lab5$  openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:ad:7e:2f:97:5e:30:c9:3e:24:67:de:51:51:ba:
    bc:18:b0:6a:2f:2d:50:f5:86:d5:9b:a6:24:43:f3:
    7c:c5:12:87:1d:f1:b6:f0:cc:3d:69:66:d1:f4:0b:
    07:21:8e:fa:8b:8a:97:91:ad:ef:ab:b7:e9:41:c7:
    ca:e4:13:b5:67:b8:0a:94:fa:db:c8:72:b0:18:24:
    e4:f8:39:bd:40:20:30:d1:d8:b2:35:82:ed:7b:a9:
    b7:0e:a4:ed:05:a1:c4:70:f9:d0:46:5e:64:31:b0:
    7c:f3:cd:d9:79:7f:9d:b5:37:72:d7:fc:69:6b:1c:
    79:70:5b:14:93:16:f2:13:19:e2:55:4a:af:36:90:
    7b:3f:a1:dc:9f:ab:cc:62:8a:1e:fa:10:88:84:b8:
    4b:e7:39:3e:50:9c:83:67:4a:0d:0a:92:43:38:78:
    b4:6a:e3:a2:c2:f5:15:e6:00:09:a1:68:61:5e:60:
    4b:a2:39:b0:a8:85:3a:ae:1e:ad:80:66:8d:99:e0:
    70:93:df:9a:bd:1c:ce:f3:0b:bf:c3:6f:e6:cf:2b:
    0a:c2:a4:fa:99:5d:5b:c5:8e:7f:46:3f:5c:be:07:
    2e:29:e8:c1:d9:e6:e1:48:19:f3:44:51:22:9c:d2:
    93:4b:5f:bb:aa:fd:a9:63:de:37:49:02:84:c5:18:
    84:8f
publicExponent: 65537 (0x10001)
privateExponent:
    00:90:91:ac:f0:b2:81:6e:c0:84:af:b4:f7:08:66:
```



```
    40:c8:96:5f:16:5d:35:39:cc:56:85:ff:55:cf:64:
    08:7a:ee:7e:29:4a:66:90:d4:d1:32:fc:8b:d2:9f:
    1a:2e:9b:b8:7b:9c:6e:3c:99:73:ba:5a:b3:72:1c:
    a4:e0:8a:a7:18:49:dc:e2:58:47:35:23:c9:ce:57:
    ab:88:c8:ac:f5:6b:48:14:39:45:2c:60:f2:a6:f6:
    bf:1c:48:6d:ac:f2:5d:be:3b:c8:f9:03:16:62:d6:
    40:f2:89:ed:83:79:bb:8e:61
exponent2:
    4c:80:4d:72:20:08:7b:4f:70:22:7c:e0:43:98:72:
    20:e8:f2:26:b7:ec:96:3c:e3:df:3e:fb:58:a3:b3:
    5e:1f:37:62:a8:91:bd:e1:77:fe:2e:6b:81:17:a3:
    b6:3f:a4:84:25:cc:dd:46:08:00:83:04:23:16:aa:
    8d:bf:8d:a7:ac:11:62:99:a2:a2:26:6b:0c:0c:61:
    86:1f:c3:6c:bc:ee:dd:12:cb:95:ac:15:2b:74:06:
    84:9a:72:e6:55:8f:9b:d2:e5:b2:c3:91:dc:4e:57:
    a2:c5:8c:0f:a3:c0:d6:ba:85:85:d3:6d:33:59:bc:
    c6:a3:34:fc:6f:f3:95:23
coefficient:
    56:cc:c6:00:eb:b1:cd:8b:39:5e:32:22:82:47:a1:
    44:99:98:a0:a8:90:48:86:7c:bb:bc:0a:cf:da:cf:
    a5:1e:3a:8b:ef:41:eb:7b:b5:9c:ef:7c:3f:57:56:
    c0:57:9b:98:0c:d0:59:11:a6:2f:25:15:e3:e4:af:
    f4:57:08:57:15:de:11:40:2b:ad:40:20:b1:f2:ff:
    eb:14:e1:39:9e:f6:bc:21:d8:f1:4b:e3:7b:24:c4:
    49:f1:02:b6:c0:d5:7c:b0:f1:23:36:70:32:a3:b8:
    74:94:7b:a9:5c:38:b4:60:07:d5:bf:d7:9f:aa:c7:
    fc:ba:c8:e3:75:37:61:ab
[10/25/22]seed@VM:~/.../AC_lab5$ 
```

Task 3: Generating a Certificate for your server

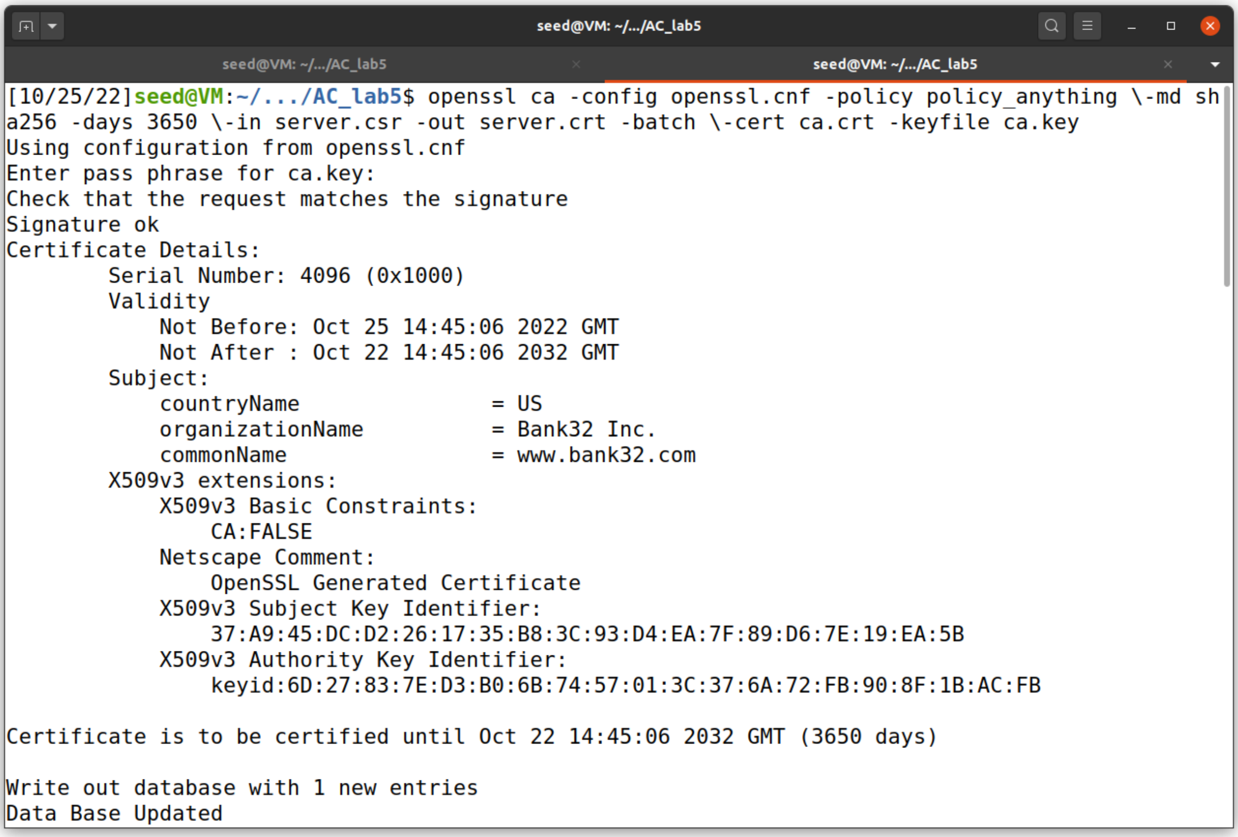
Command

```
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
```

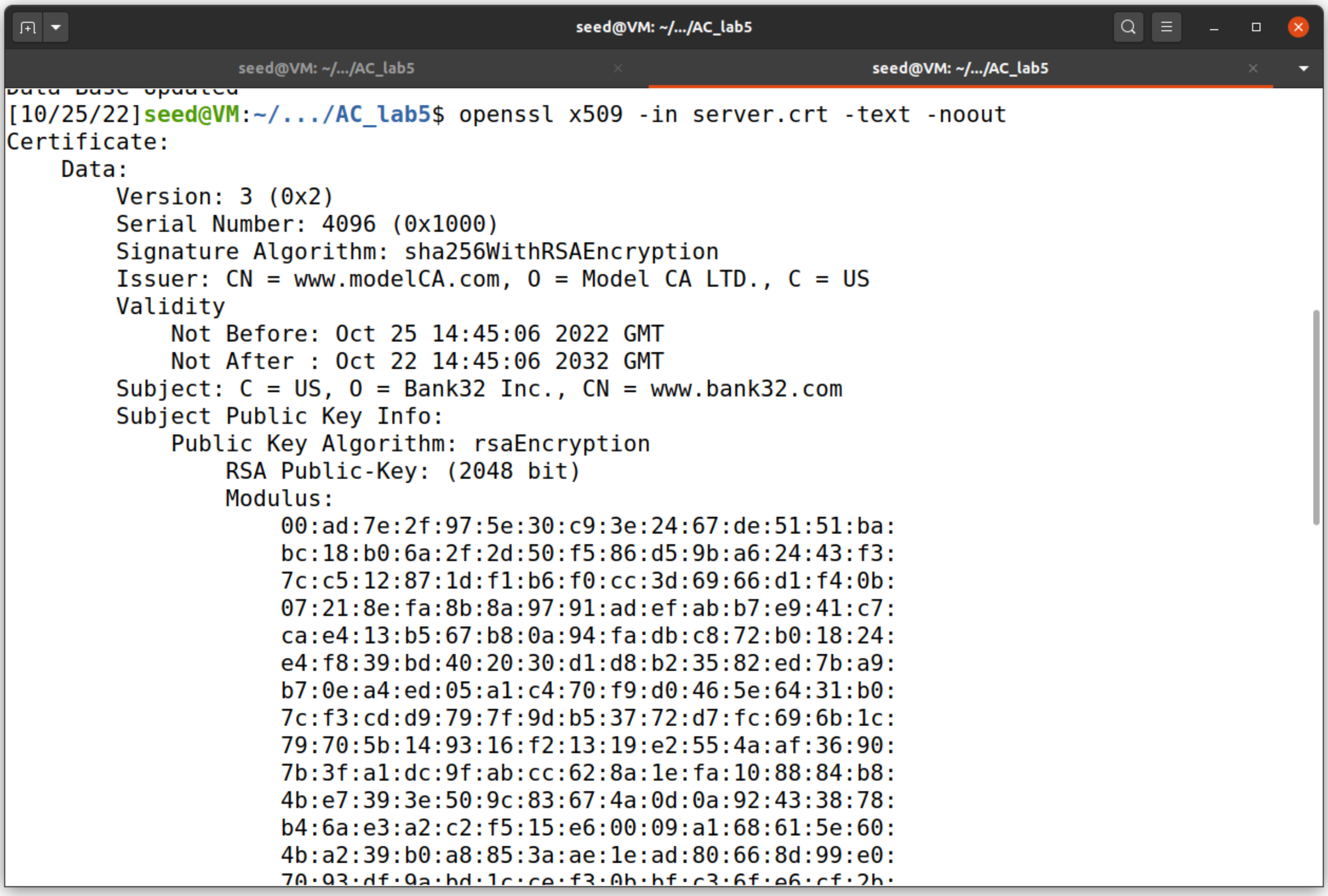
Viewing the contents of files generated

Command

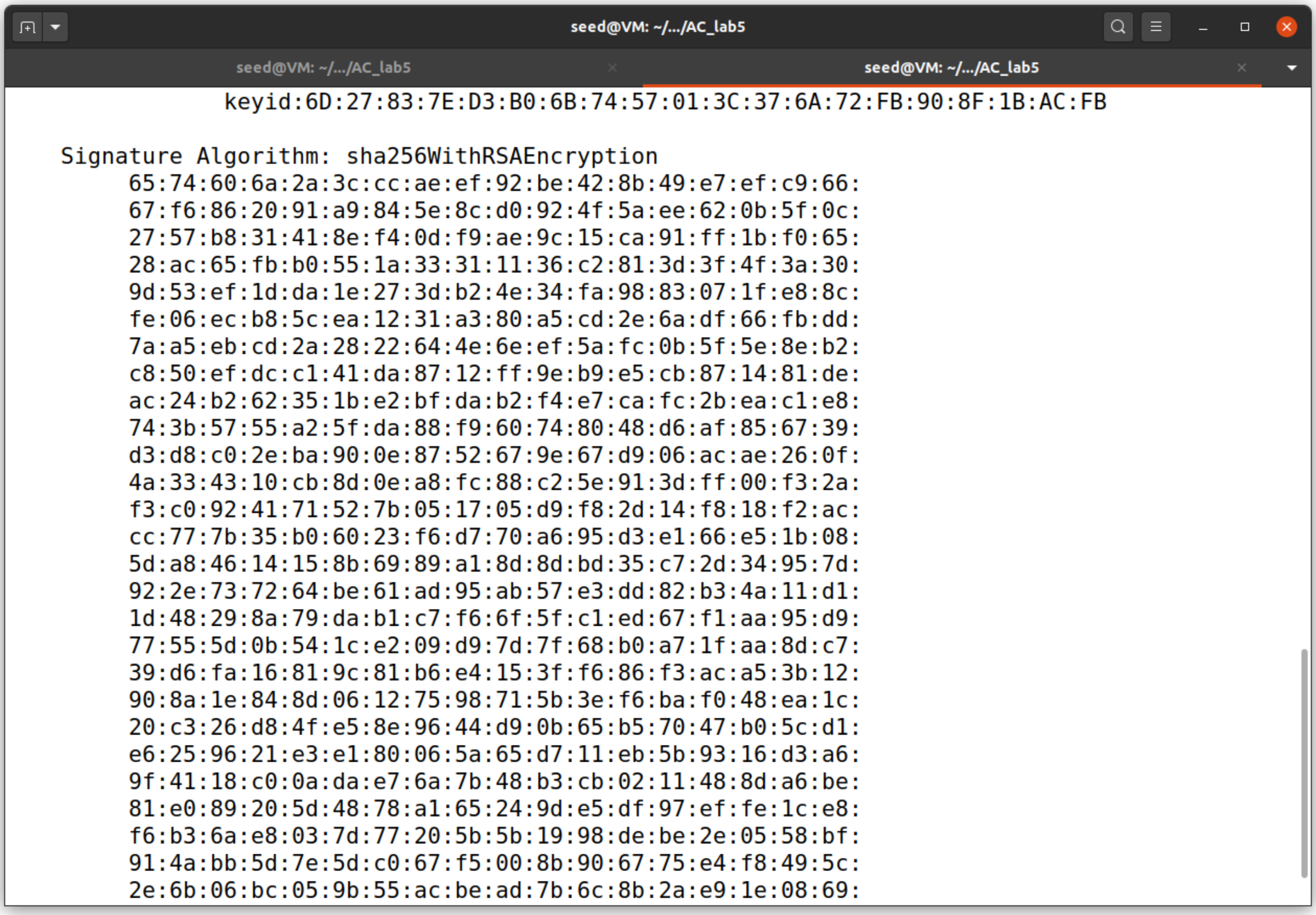
```
$ openssl x509 -in server.crt -text -noout
```



```
[10/25/22]seed@VM:~/.../AC_lab5$ openssl ca -config openssl.cnf -policy policy_anything \-md sh
a256 -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: Oct 25 14:45:06 2022 GMT
            Not After : Oct 22 14:45:06 2032 GMT
        Subject:
            countryName               = US
            organizationName          = Bank32 Inc.
            commonName                = www.bank32.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                37:A9:45:DC:D2:26:17:35:B8:3C:93:D4:EA:7F:89:D6:7E:19:EA:5B
            X509v3 Authority Key Identifier:
                keyid:6D:27:83:7E:D3:B0:6B:74:57:01:3C:37:6A:72:FB:90:8F:1B:AC:FB

Certificate is to be certified until Oct 22 14:45:06 2032 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```



```
Data Base Updated
[10/25/22]seed@VM:~/.../AC_lab5$ 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: Oct 25 14:45:06 2022 GMT
            Not After : Oct 22 14:45:06 2032 GMT
        Subject: C = US, O = Bank32 Inc., CN = www.bank32.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ad:7e:2f:97:5e:30:c9:3e:24:67:de:51:51:ba:
                    bc:18:b0:6a:2f:2d:50:f5:86:d5:9b:a6:24:43:f3:
                    7c:c5:12:87:1d:f1:b6:f0:cc:3d:69:66:d1:f4:0b:
                    07:21:8e:fa:8b:8a:97:91:ad:ef:ab:b7:e9:41:c7:
                    ca:e4:13:b5:67:b8:0a:94:fa:db:c8:72:b0:18:24:
                    e4:f8:39:bd:40:20:30:d1:d8:b2:35:82:ed:7b:a9:
                    b7:0e:a4:ed:05:a1:c4:70:f9:d0:46:5e:64:31:b0:
                    7c:f3:cd:d9:79:7f:9d:b5:37:72:d7:fc:69:6b:1c:
                    79:70:5b:14:93:16:f2:13:19:e2:55:4a:af:36:90:
                    7b:3f:a1:dc:9f:ab:cc:62:8a:1e:fa:10:88:84:b8:
                    4b:e7:39:3e:50:9c:83:67:4a:0d:0a:92:43:38:78:
                    b4:6a:e3:a2:c2:f5:15:e6:00:09:a1:68:61:5e:60:
                    4b:a2:39:b0:a8:85:3a:ae:1e:ad:80:66:8d:99:e0:
                    70:93:df:9a:bd:1c:ce:f3:0b:bf:c3:6f:e6:cf:2b:
```

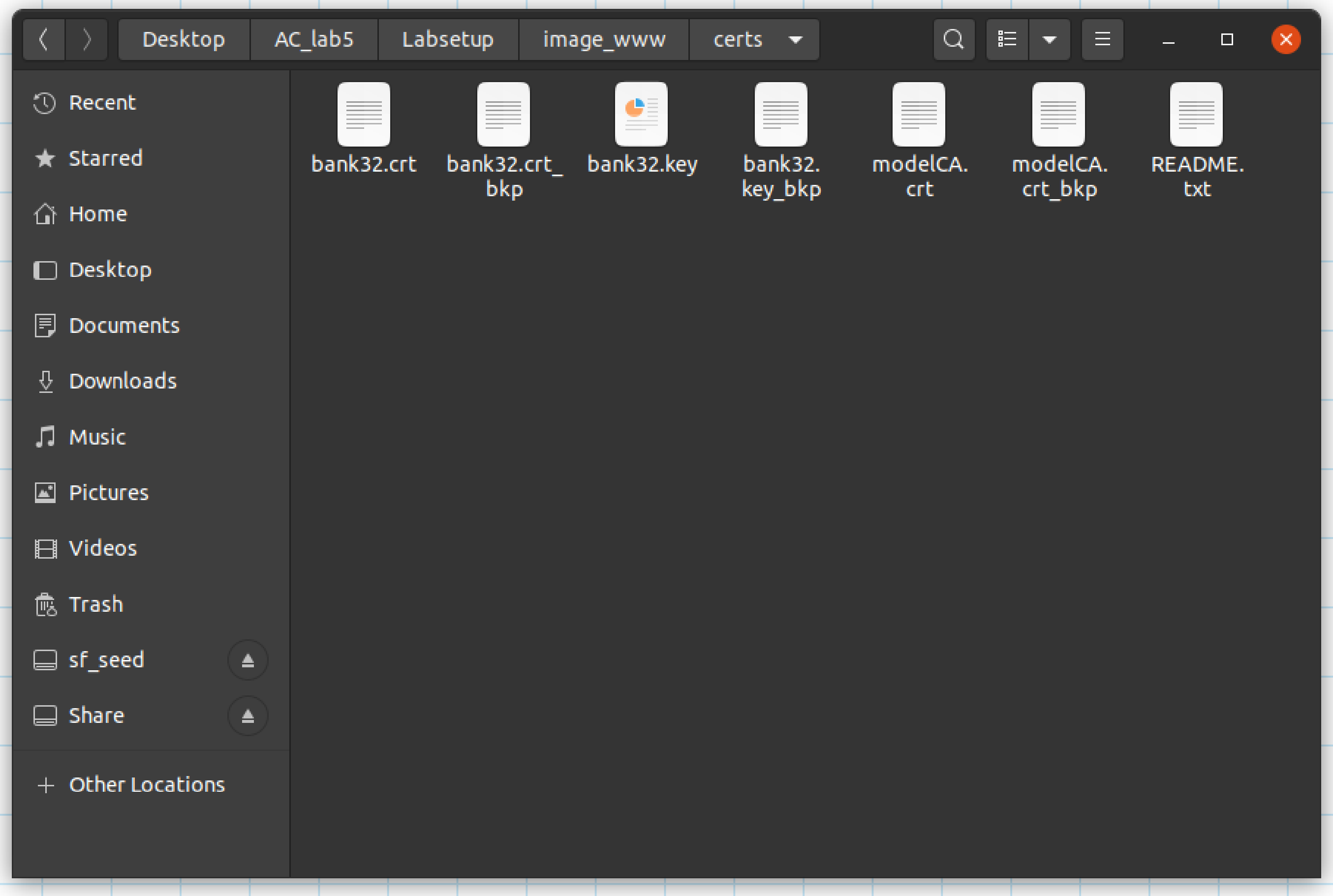


```
                keyid:6D:27:83:7E:D3:B0:6B:74:57:01:3C:37:6A:72:FB:90:8F:1B:AC:FB

    Signature Algorithm: sha256WithRSAEncryption
         65:74:60:6a:2a:3c:cc:ae:ef:92:be:42:8b:49:e7:ef:c9:66:
         67:f6:86:20:91:a9:84:5e:8c:d0:92:4f:5a:ee:62:0b:5f:0c:
         27:57:b8:31:41:8e:f4:0d:f9:ae:9c:15:ca:91:ff:1b:f0:65:
         28:ac:65:fb:b0:55:1a:33:31:11:36:c2:81:3d:3f:4f:3a:30:
         9d:53:ef:1d:da:1e:27:3d:b2:4e:34:fa:98:83:07:1f:e8:8c:
         fe:06:ec:b8:5c:ea:12:31:a3:80:a5:cd:2e:6a:df:66:fb:dd:
         7a:a5:eb:cd:2a:28:22:64:4e:6e:ef:5a:fc:0b:5f:5e:8e:b2:
         c8:50:ef:dc:c1:41:da:87:12:ff:9e:b9:e5:cb:87:14:81:de:
         ac:24:b2:62:35:1b:e2:bf:da:b2:f4:e7:ca:fc:2b:ea:c1:e8:
         74:3b:57:55:a2:5f:da:88:f9:60:74:80:48:d6:af:85:67:39:
         d3:d8:c0:2e:ba:90:0e:87:52:67:9e:67:d9:06:ac:ae:26:0f:
         4a:33:43:10:cb:8d:0e:a8:fc:88:c2:5e:91:3d:ff:00:f3:2a:
         f3:c0:92:41:71:52:7b:05:17:05:d9:f8:2d:14:f8:18:f2:ac:
         cc:77:7b:35:b0:60:23:f6:d7:70:a6:95:d3:e1:66:e5:1b:08:
         5d:a8:46:14:15:8b:69:89:a1:8d:8d:bd:35:c7:2d:34:95:7d:
         92:2e:73:72:64:be:61:ad:95:ab:57:e3:dd:82:b3:4a:11:d1:
         1d:48:29:8a:79:da:b1:c7:f6:6f:5f:c1:ed:67:f1:aa:95:d9:
         77:55:5d:0b:54:1c:e2:09:d9:7d:7f:68:b0:a7:1f:aa:8d:c7:
         39:d6:fa:16:81:9c:81:b6:e4:15:3f:f6:86:f3:ac:a5:3b:12:
         90:8a:1e:84:8d:06:12:75:98:71:5b:3e:f6:ba:f0:48:ea:1c:
         20:c3:26:d8:4f:e5:8e:96:44:d9:0b:65:b5:70:47:b0:5c:d1:
         e6:25:96:21:e3:e1:80:06:5a:65:d7:11:eb:5b:93:16:d3:a6:
         9f:41:18:c0:0a:da:e7:6a:7b:48:b3:cb:02:11:48:8d:a6:be:
         81:e0:89:20:5d:48:78:a1:65:24:9d:e5:df:97:ef:fe:1c:e8:
         f6:b3:6a:e8:03:7d:77:20:5b:5b:19:98:de:be:2e:05:58:bf:
         91:4a:bb:5d:7e:5d:c0:67:f5:00:8b:90:67:75:e4:f8:49:5c:
         2e:6b:06:bc:05:9b:55:ac:be:ad:7b:6c:8b:2a:e9:1e:08:69:
```

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

Step 1 - Setting up the required files

Copy the files server.crt, server.key and ca.crt to Labsetup/image_www/certs and rename them to bank32.crt, bank32.key and modelCA.crt respectively.

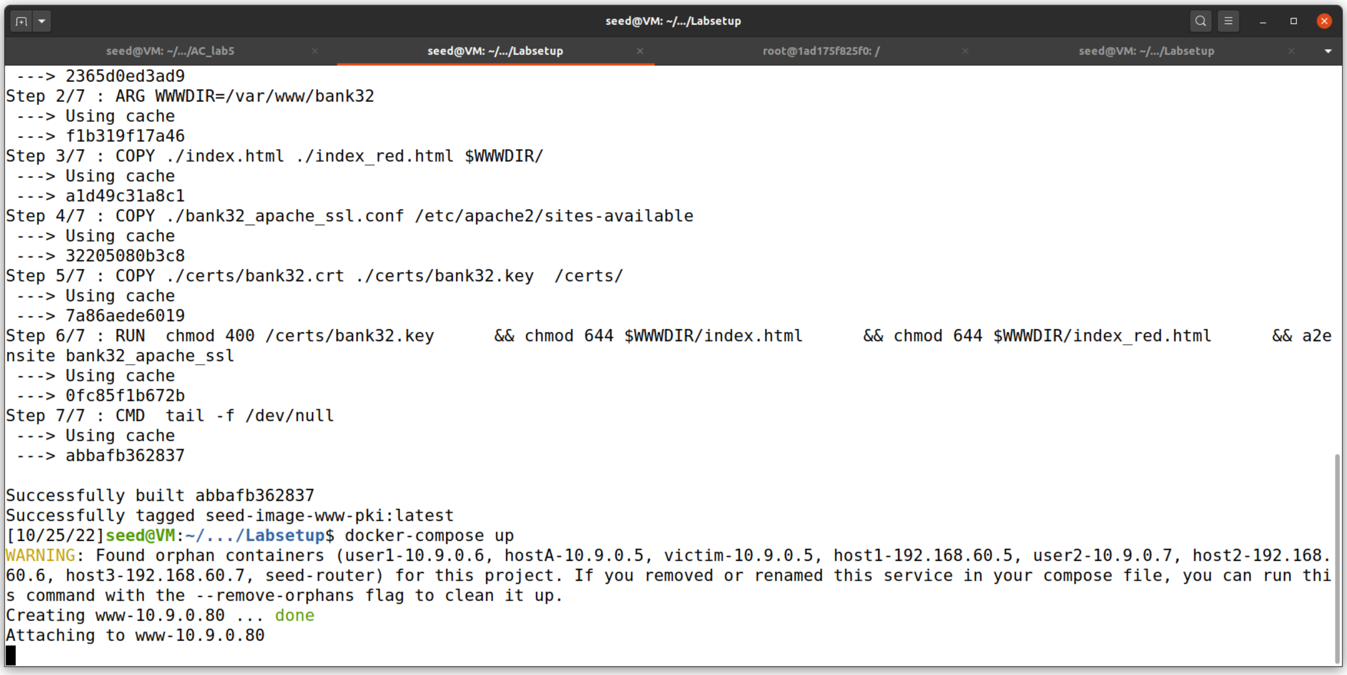


Step 2 - Building docker

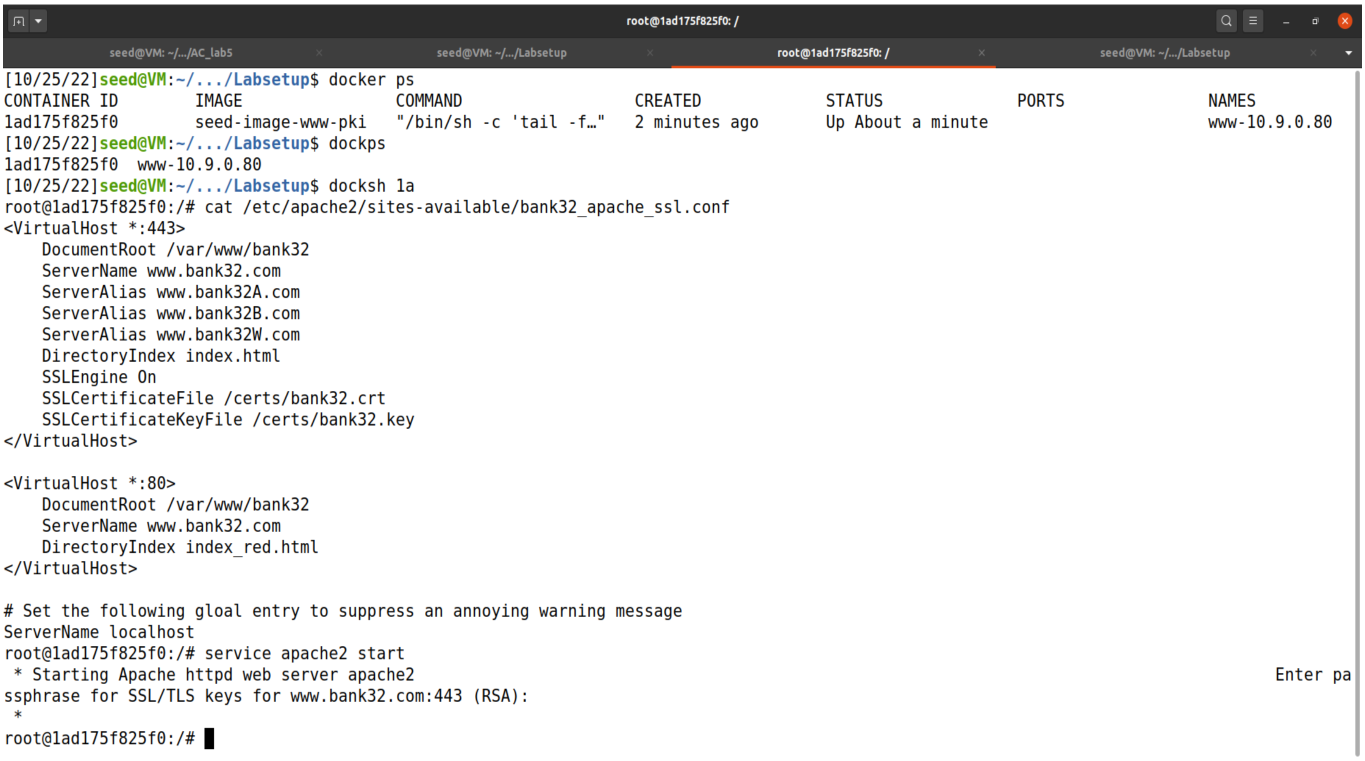
Navigate to Labsetup and run the following commands

Commands

```
$ docker-compose build
$ docker-compose up
# in a different terminal
$ dockps
# Note the id of the container
$ docksh <id of container>
# Inside the docker shell
% service apache2 start
```



```
 ---> 2365d0ed3ad9
Step 2/7 : ARG WWWDIR=/var/www/bank32
 ---> Using cache
 ---> f1b319f17a46
Step 3/7 : COPY ./index.html ./index_red.html $WWWDIR/
 ---> Using cache
 ---> a1d49c31a8c1
Step 4/7 : COPY ./bank32_apache_ssl.conf /etc/apache2/sites-available
 ---> Using cache
 ---> 32205080b3c8
Step 5/7 : COPY ./certs/bank32.crt ./certs/bank32.key  /certs/
 ---> Using cache
 ---> 7a86aede6019
Step 6/7 : RUN  chmod 400 /certs/bank32.key      && chmod 644 $WWWDIR/index.html      && chmod 644 $WWWDIR/index_red.html      && a2e
nsite bank32_apache_ssl
 ---> Using cache
 ---> 0fc85f1b672b
Step 7/7 : CMD  tail -f /dev/null
 ---> Using cache
 ---> abbafb362837

Successfully built abbafb362837
Successfully tagged seed-image-www-pki:latest
[10/25/22]seed@VM:~/.../Labsetup$ docker-compose up
WARNING: Found orphan containers (user1-10.9.0.6, hostA-10.9.0.5, victim-10.9.0.5, host1-192.168.60.5, user2-10.9.0.7, host2-192.168.
60.6, host3-192.168.60.7, seed-router) for this project. If you removed or renamed this service in your compose file, you can run thi
s command with the --remove-orphans flag to clean it up.
Creating www-10.9.0.80 ... done
Attaching to www-10.9.0.80
```

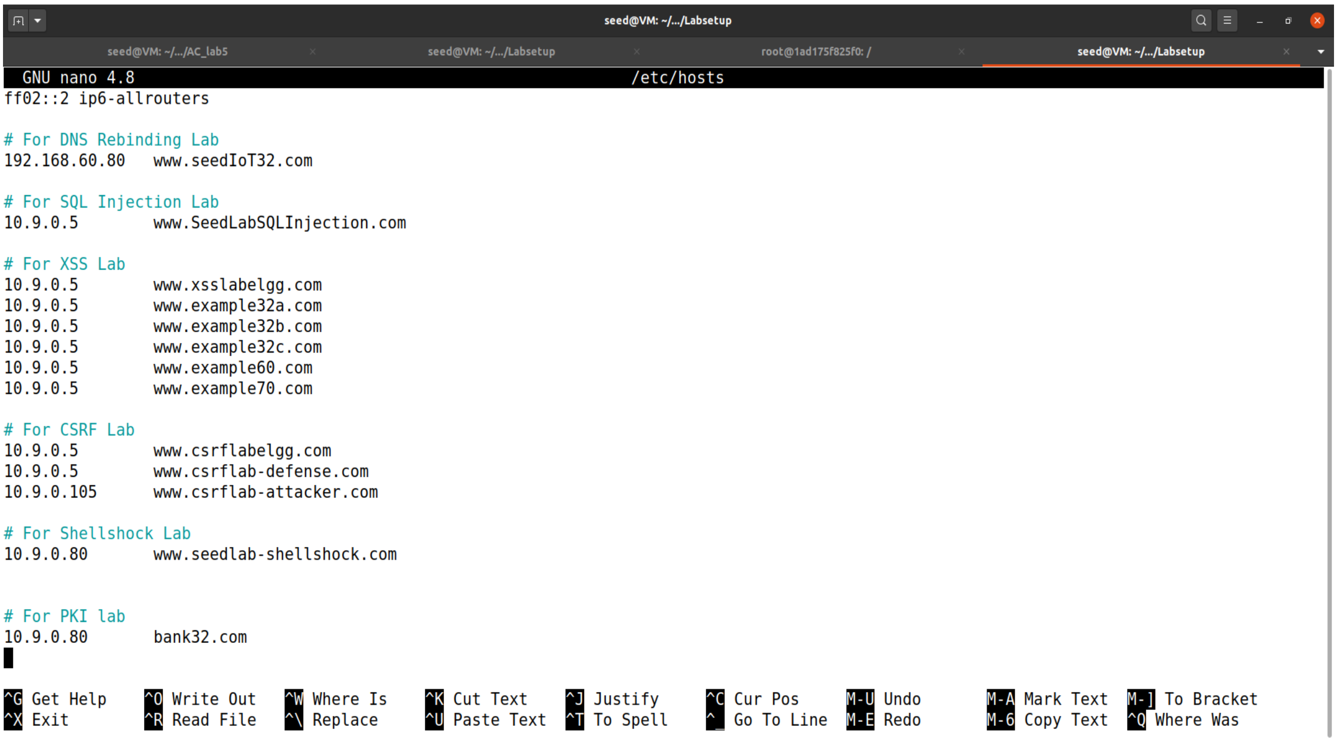


```
[10/25/22]seed@VM:~/.../Labsetup$ docker ps
CONTAINER ID   IMAGE                COMMAND                CREATED         STATUS           PORTS     NAMES
1ad175f825f0   seed-image-www-pki   "/bin/sh -c 'tail -f…"   2 minutes ago   Up About a minute             www-10.9.0.80
[10/25/22]seed@VM:~/.../Labsetup$ dockps
1ad175f825f0  www-10.9.0.80
[10/25/22]seed@VM:~/.../Labsetup$ docksh 1a
root@1ad175f825f0:/# cat /etc/apache2/sites-available/bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    ServerAlias www.bank32A.com
    ServerAlias www.bank32B.com
    ServerAlias www.bank32W.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>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
root@1ad175f825f0:/# service apache2 start
 * Starting Apache httpd web server apache2                                                                                Enter pa
ssphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
 *
root@1ad175f825f0:/# 
```

Step 3 - Setting up DNS

Open /etc/hosts in a text editor as root (in the seed vm)
Add the following entry at the end

10.9.0.80 www.bank32.com

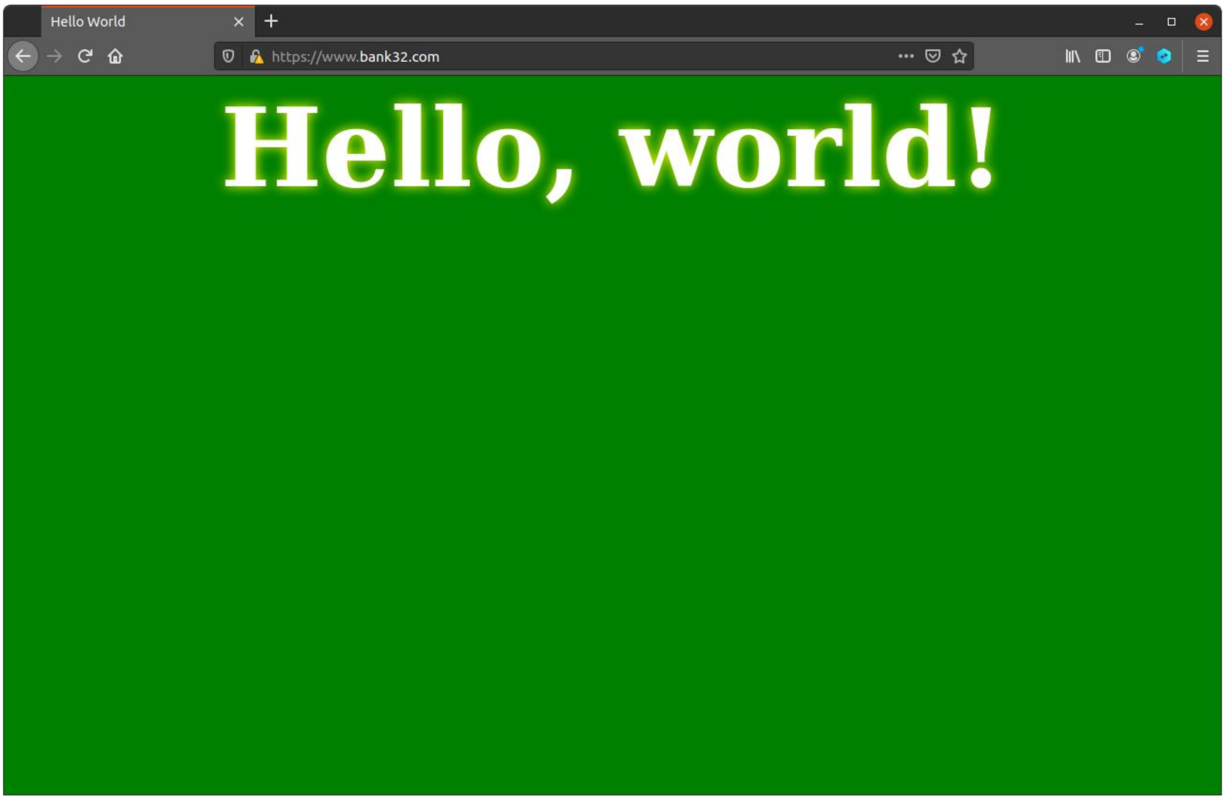


```
  GNU nano 4.8                              /etc/hosts
ff02::2 ip6-allrouters

# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com

# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# 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


# For PKI lab
10.9.0.80       bank32.com


^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text  M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text  ^Q Where Was
```

Step 4

Open firefox and navigate to https://www.bank32.com

Take a screenshot and note your observations

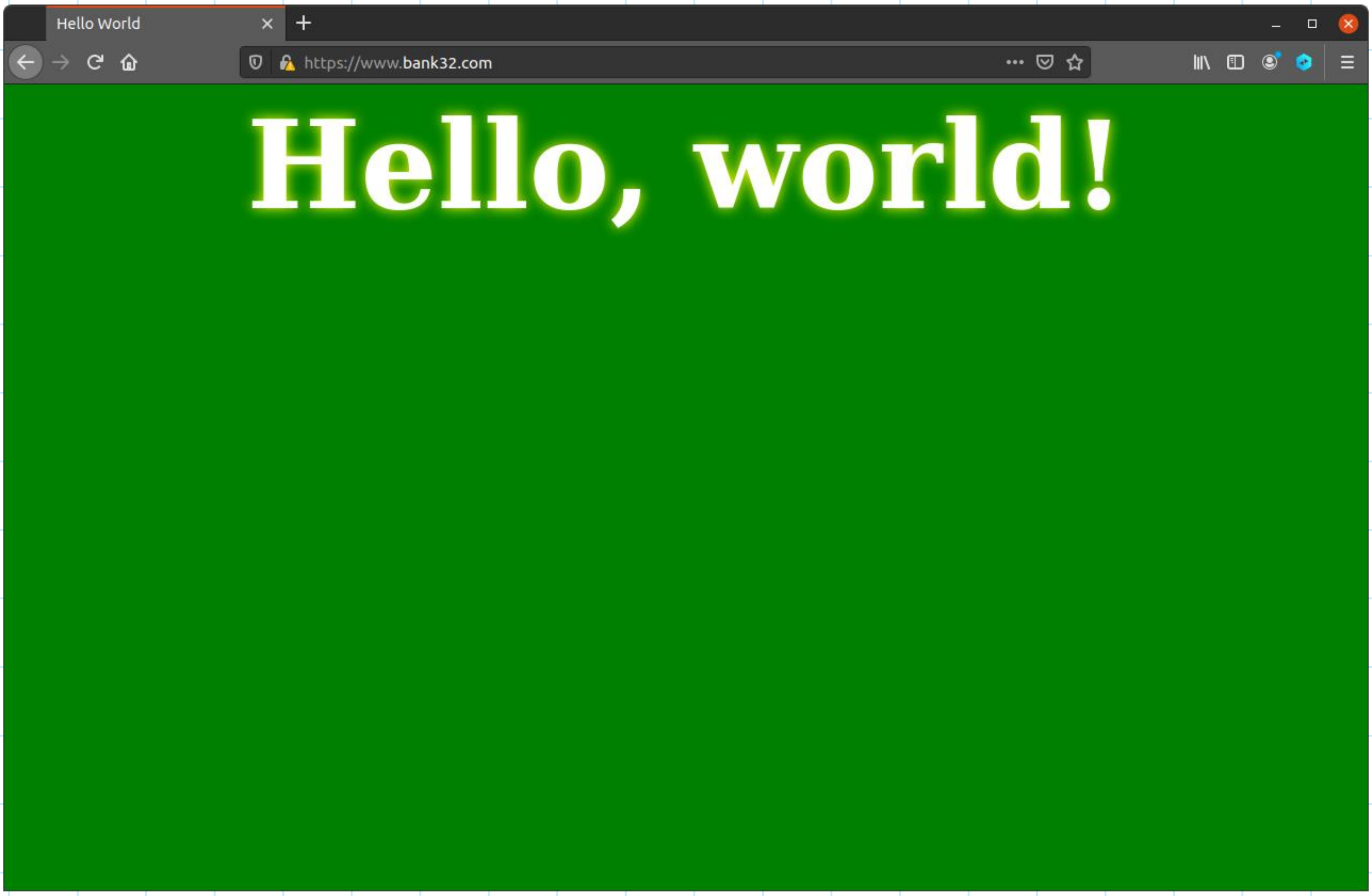


Hello, world!

Step 5

1. Go to about:preferences#privacy
2. At the bottom, under certificates, click on "View Certificates", then "import"
3. Select the ca.crt that you generated and import it
4. Ensure to check the "trust this CA to identify websites"
5. Open https://www.bank32.com again

Take a screenshot and note your observations



Hello, world!

Question

Since bank32.com points to 10.9.0.80, if we use https://10.9.0.80 instead, we will be connecting to the same web server. Please do so, describe and explain your observations

Ans: No, it will not be leading to the Hello World page.

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

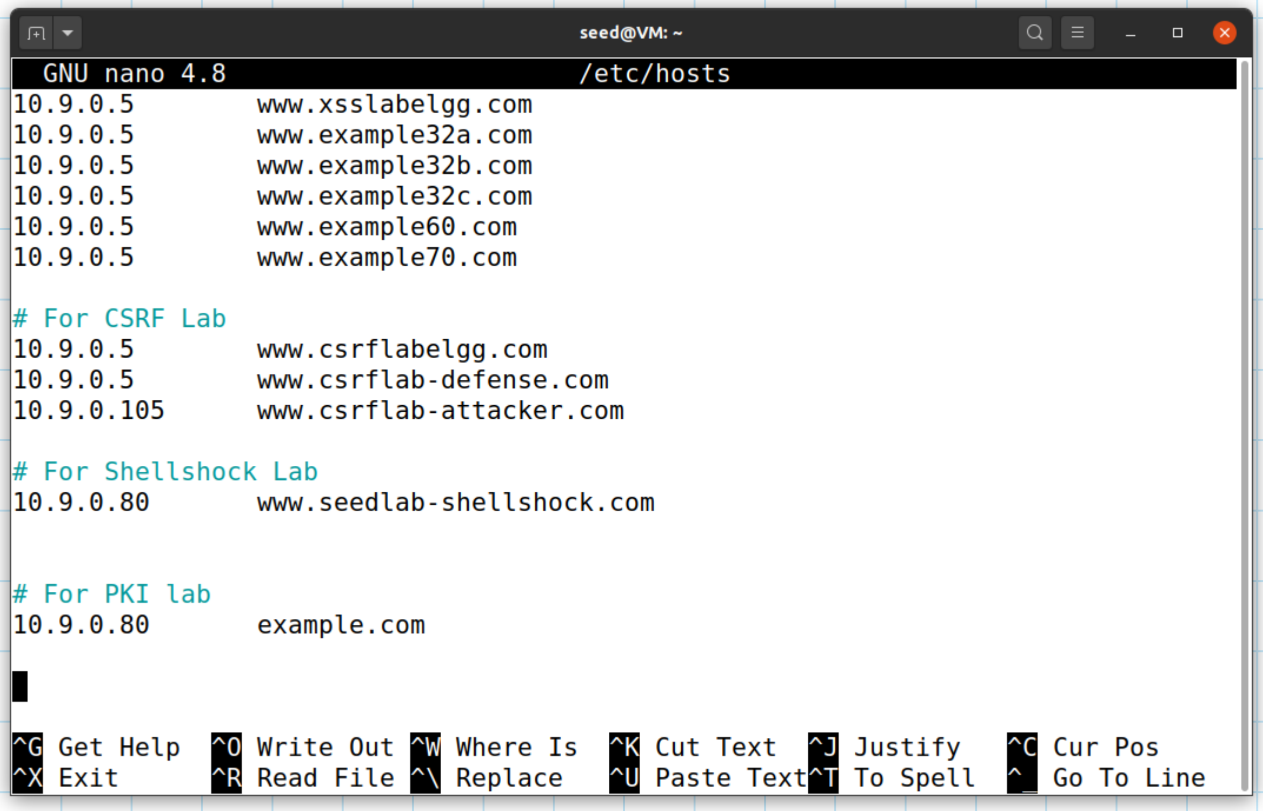
Step 1: Setting up the malicious website.

In Task 4, we have already set up an HTTPS website. We will use the same Apache server to impersonate www.example.com. To achieve that, we will follow the instruction in Task 4 to add a VirtualHost entry to Apache’s SSL configuration file: the ServerName should be www.example.com, but the rest of the configuration can be the same as that used in Task 4.

Step 2: Becoming the man in the middle

Add the following entry to the victim's /etc/hosts file:

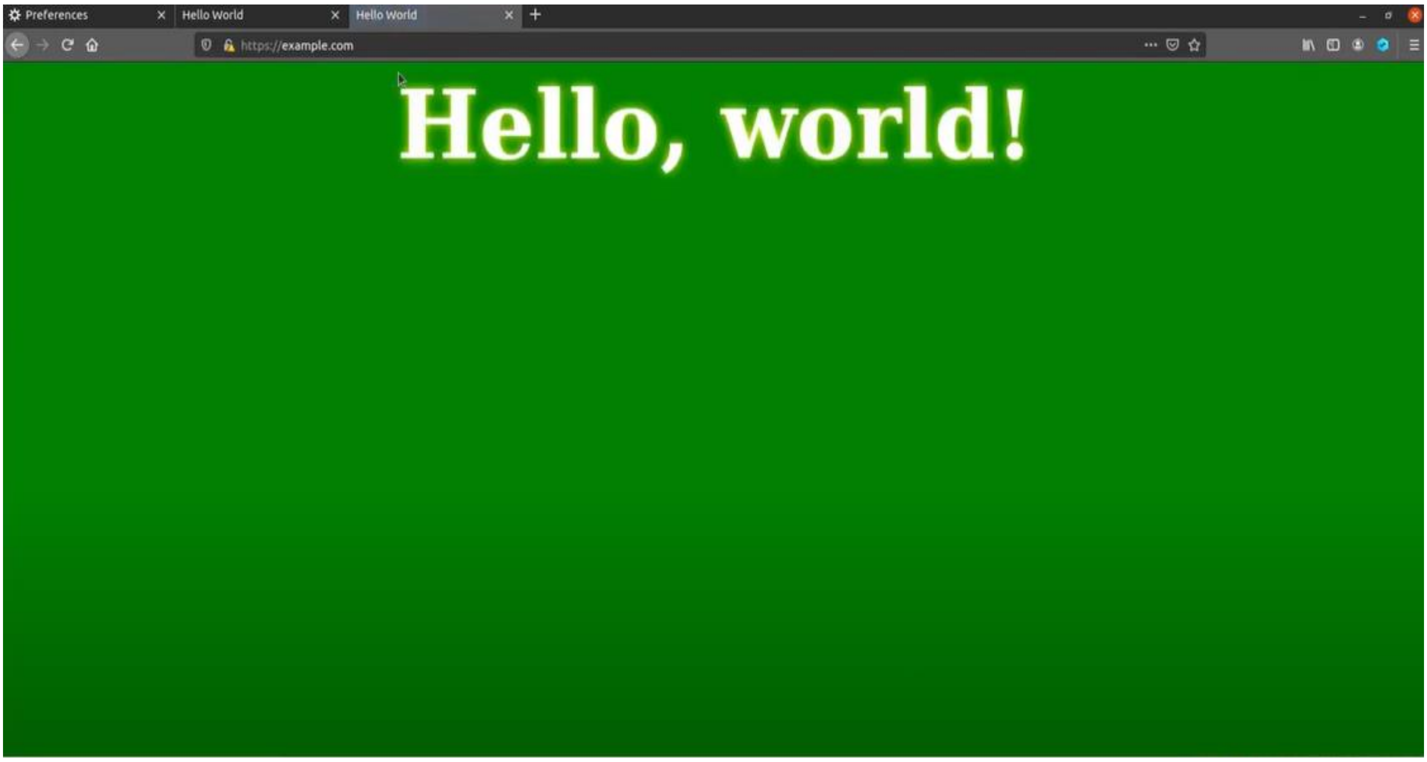
10.9.0.80 www.example.com



```
  GNU nano 4.8                    /etc/hosts
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# 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


# For PKI lab
10.9.0.80       example.com


^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
```

Step 3 - Browse the target website

Open https://www.example.com in firefox and note your observations.



Hello, world!