EAST WEST UNIVERSITY

Securing a Networked System with PKI

Computer and Cybersecurity – **CSE487**
Section - **1**

Submitted to:
Rashedul Amin Tuhin
Senior lecturer, Department of Computer Science & Engineering
East West University

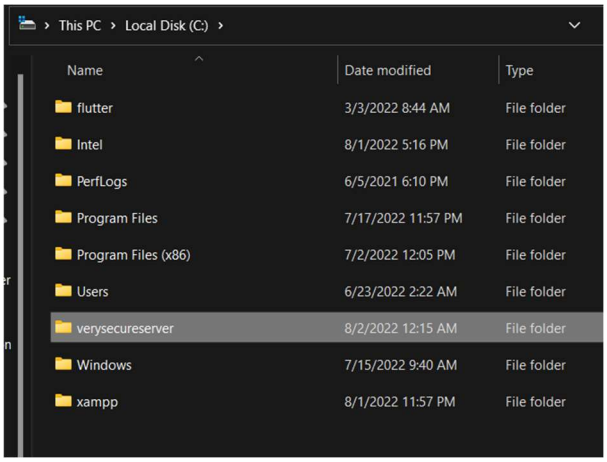
Submitted by:
ASM Saeedus Salehin – **2018-3-60-103**
Nusrat Jahan Piya – **2018-2-60-034**
Tanveer Ahmed – **2018-2-60-120**

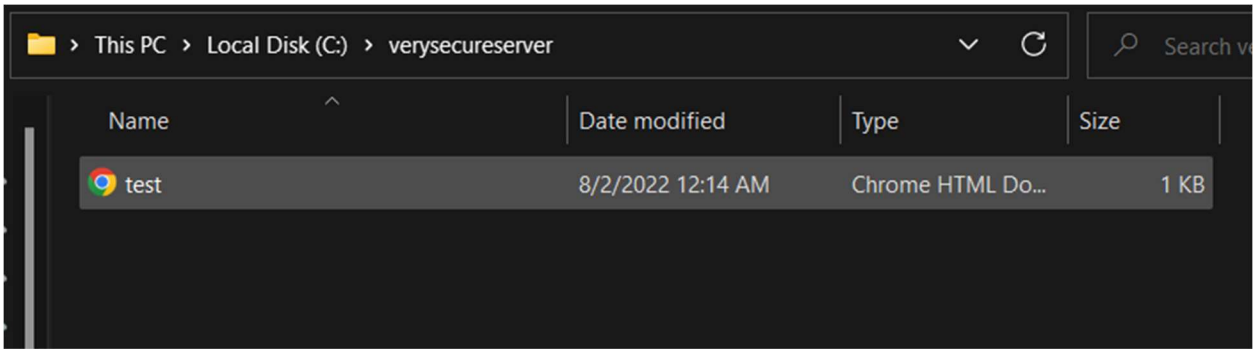
Date of submission: 24 August 2022

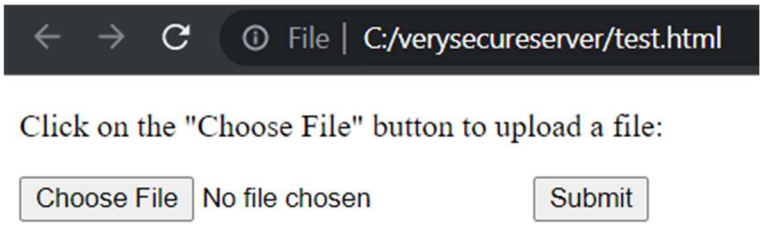
Securing a networked system with Public Key Infrastructure, Implementing Transport Layer Security on HTTP for https:// connection

A simple file uploading page will be created in the server to implement transport layer security. Step by step process is described with images below.

Step 1:
Create a folder in C directory named ***verysecureserver*** and put the HTML code there (a simple file uploading page using HTML).







Step 2:

Install **Xampp** and navigate to **xampp/apache/conf.** Open **httpd.conf** file in an editor. In line 252 and 253 change the **DocumentRoot** and **Directory** to "C:\verysecureserver".

```
246
247  #
248  # DocumentRoot: The directory out of which you will serve your
249  # documents. By default, all requests are taken from this directory, but
250  # symbolic links and aliases may be used to point to other locations.
251  #
252  DocumentRoot "C:\verysecureserver"
253  <Directory "C:\verysecureserver">
254      #
255      # Possible values for the Options directive are "None", "All",
256      # or any combination of:
257      #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
258      #
259      # Note that "MultiViews" must be named *explicitly* --- "Options All"
260      # doesn't give it to you.
261      #
```

Configuring DNS: Navigate to **C:/Windows/System32/drivers/etc** and open **hosts** file on an notepad++ (must run it as administrator). Add the following lines and save it.

127.0.0.1 localhost

127.0.0.1 verysecureserver

127.0.0.1 www.verysecureserver.com

```
19  # localhost name resolution is handled within DNS itself.
20  #   127.0.0.1       localhost
21  #   ::1             localhost
22
23  127.0.0.1       localhost
24  127.0.0.1       verysecureserver
25  127.0.0.1       www.verysecureserver.com
```

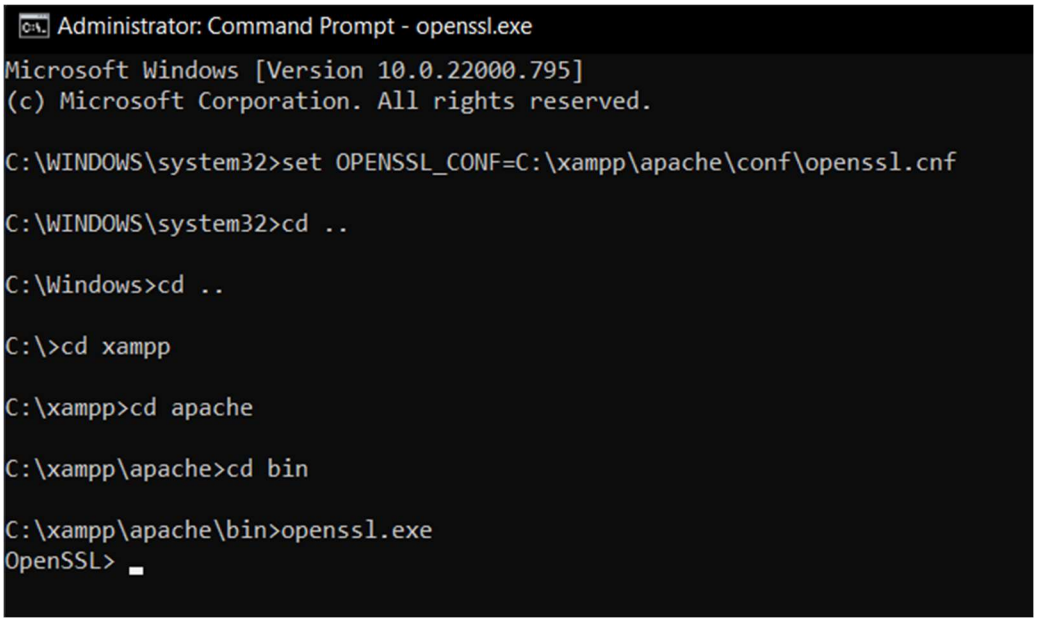
Step 3 (Configuring OpenSSL):

In this step, open command prompt as an administrator. Run the following command for openssl configuration.

set OPENSSL_CONF=C:\xampp\apache\conf\openssl.cnf

After that, change directory **to C:/xampp/apache/bin**. In this directory write –

openssl.exe



OpenSSL is now ready to be used.

Step 4 (Creating server, sub root and root certificates):

Run the following command to create a server certificate.

req -newkey rsa:2048 -nodes -keyout server.key -out server.csr

```
OpenSSL> req -newkey rsa:2048 -nodes -keyout server.key -out server.csr
Generating a RSA private key
..............+++++
....+++++
writing new private key to 'server.key'
-----
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]:BD
State or Province Name (full name) [Some-State]:Bangladesh
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nothing
Organizational Unit Name (eg, section) []:Nothing unit
Common Name (e.g. server FQDN or YOUR name) []:www.verysecureserver.com
Email Address []:saeedussalehin@outlook.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:ghost
An optional company name []:Nothing
OpenSSL>
```

Fill out the attributes. In the common name section give the server's name, which is ***www.verysecureserver.com***. Fill out the extra attributes. Then give a password and run the following command to sign key:

x509 -signkey server.key -in server.csr -req -days 365 -out server.crt

```
OpenSSL> x509 -signkey server.key -in server.csr -req -days 365 -out server.crt
Signature ok
subject=C = BD, ST = Dhaka, L = Dhaka, O = Nothing, OU = Nothing unit, CN = www.verysecureserver.com, emailAddress = sae
edussalehin@outlook.com
Getting Private key
OpenSSL>
```

After that, configure the subCA with the following command:

req -newkey rsa:2048 -keyout Acme-subrootCA.key -out Acme-subrootCA.csr

```
C:\xampp\apache\bin>openssl.exe
OpenSSL> req -newkey rsa:2048 -keyout Acme-subrootCA.key -out Acme-subrootCA.csr
Generating a RSA private key
........+++++
.............................+++++
writing new private key to 'Acme-subrootCA.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]:BD
State or Province Name (full name) [Some-State]:Bangladesh
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nothing
Organizational Unit Name (eg, section) []:Nothing unit
Common Name (e.g. server FQDN or YOUR name) []:Acme-subrootCA
Email Address []:saeedussalehin@outlook.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:ghost
An optional company name []:Nothing
OpenSSL>
```

*** Please note that, you might face some error. In this case, close the command prompt, re-run it as administrator, configure openssl and then running the command will solve the issue.

Now, fill out the information similar to the first command. In the common name attribute write **Acme-subrootCA**. Fill the attributes and then to sign run this command below-

x509 -signkey Acme-subrootCA.key -in Acme-subrootCA.csr -req -days 365 -out Acme-subrootCA.crt

```
OpenSSL> x509 -signkey Acme-subrootCA.key -in Acme-subrootCA.csr -req -days 365 -out Acme-subrootCA.crt
Signature ok
subject=C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = Acme-subrootCA, emailAddress = saeeduss
alehin@outlook.com
Getting Private key
Enter pass phrase for Acme-subrootCA.key:
OpenSSL>
```

For the rootCA:

req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout Acme-rootCA.key -out Acme-rootCA.crt

```
OpenSSL> req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout Acme-rootCA.key -out Acme-rootCA.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'Acme-rootCA.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]:BD
State or Province Name (full name) [Some-State]:Bangladesh
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nothing
Organizational Unit Name (eg, section) []:Nothing unit
Common Name (e.g. server FQDN or YOUR name) []:Acme-rootCA
Email Address []:saeedussalehin@outlook.com
OpenSSL>
```

Similarly, fill the attributes after giving PEM phrase. Write **Acme-rootCA** in the common name attribute.

Step 5 (creating .ext files):

- Navigate to the xampp folder and then apache/bin. In the folder create 2 .ext files named ***root.ext*** and ***domain.ext.***
- Open the ***domain.ext*** file in an editor, write the following code containing server and DNS address and save.

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.verysecureserver.com
DNS.2 =127.0.0.1
```

- Similarly, open the ***root.ext*** file in an editor and write the following lines and save.

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:TRUE
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.verysecureserver.com
DNS.2 =127.0.0.1
```

Step 6 (Signing subCA with rootCA):

x509 -req -CA Acme-rootCA.crt -CAkey Acme-rootCA.key -in Acme-subrootCA.csr -out Acme-subrootCA.crt -days 365 -CAcreateserial -extfile root.ext

```
OpenSSL> x509 -req -CA Acme-rootCA.crt -CAkey Acme-rootCA.key -in Acme-subrootCA.csr -out Acme-subrootCA.crt -days 365 -
CAcreateserial -extfile root.ext
Signature ok
subject=C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = Acme-subrootCA, emailAddress = saeeduss
alehin@outlook.com
Getting CA Private Key
12468:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\objects\obj_dat.c:699:
Enter pass phrase for Acme-rootCA.key:
OpenSSL>
```

Check the subCA certificate –

x509 -text -noout -in Acme-subrootCA.crt

```
OpenSSL> x509 -text -noout -in Acme-subrootCA.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            13:ba:18:c2:ac:5c:36:8d:00:7c:94:ec:eb:12:05:5c:0d:cc:78:99
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = Acme-rootCA, emailAddress = saeedussalehin@outl
ook.com
        Validity
            Not Before: Aug  4 03:52:55 2022 GMT
            Not After : Aug  4 03:52:55 2023 GMT
        Subject: C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = Acme-subrootCA, emailAddress = saeedussalehin@
outlook.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:f2:24:b8:61:18:97:1b:6f:6c:94:8b:d1:bd:f9:
                    b1:1d:89:c9:7a:1d:1f:4f:bd:c8:13:bb:5b:a7:a8:
                    4d:2b:67:33:22:70:3a:69:c9:42:16:2c:7f:b1:fb:
                    c3:bd:6e:ef:9f:0c:dc:f0:fb:fc:64:0f:0c:d2:b7:
                    bc:7a:9a:9a:38:70:21:6d:f8:5e:64:f5:36:3c:1d:
                    87:0f:93:55:7b:3f:ee:22:a1:12:d3:66:6b:d3:72:
                    c2:7b:e8:dd:ea:5b:50:9c:8d:6c:20:10:f7:6d:c4:
                    a1:39:15:c7:be:e2:d0:fb:44:01:ac:f8:86:2f:19:
                    55:34:5f:49:82:36:3e:ab:c6:57:0c:5e:c1:6d:99:
                    8d:7d:68:e4:05:79:c0:81:ce:58:c1:de:94:02:e5:
                    49:5a:72:21:12:fa:0f:f7:5a:69:af:32:fa:bb:35:
                    1f:f8:dd:b3:c2:a7:a1:39:1b:eb:0a:86:12:a9:bf:
                    22:23:25:cc:18:dc:46:29:e4:df:c1:04:f3:63:b1:
                    4f:85:89:ad:04:65:d5:84:25:ae:10:eb:71:16:69:
                    e0:82:e6:ac:ec:b8:a0:57:d0:63:af:db:c2:b3:52:
                    9a:a9:8f:3d:3a:4c:98:8d:ae:e6:11:72:c6:06:b3:
                    e3:1d:81:7f:86:ab:9b:ed:9d:5e:cf:a5:d5:50:db:
                    3e:77
                Exponent: 65537 (0x10001)
```

```
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:8B:B4:21:9E:B1:CE:1D:0B:5C:30:31:81:37:1A:A7:DD:CE:94:D1:EF

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Alternative Name:
                DNS:www.verysecureserver.com, DNS:127.0.0.1
    Signature Algorithm: sha256WithRSAEncryption
         65:6b:52:5a:d2:e1:b7:10:3b:c0:22:24:78:26:6c:59:bf:e3:
         cb:56:35:7e:8d:5d:d5:df:9d:52:84:4a:28:d3:09:d9:09:d4:
         95:12:e9:0d:de:a4:60:b1:01:fa:7a:83:20:65:53:f5:40:cb:
         e4:de:0b:4d:c2:6f:90:7b:12:1a:81:0f:1c:ed:fe:af:e4:95:
         15:9a:cb:04:d3:f6:27:0e:c8:c6:20:f6:03:51:90:b2:06:86:
         21:7f:42:40:f0:5c:c5:1d:87:e2:ed:50:b6:10:7e:cf:3a:e0:
         af:75:c1:1e:7b:d3:06:57:65:b6:21:3d:d4:cd:62:db:9d:df:
         5d:30:91:e4:ab:d9:38:6e:a5:f9:fc:ee:2f:07:1f:14:ec:34:
         48:82:36:b2:ce:ad:e6:81:bc:35:d3:07:38:a6:be:70:e8:df:
         7e:e6:f8:58:50:18:db:3a:3d:b8:8a:84:d6:a5:7c:8d:64:0f:
         54:4b:ff:28:ec:75:23:76:40:0e:d8:57:83:b4:6f:7a:2a:8f:
         24:7e:24:fb:d5:9e:d9:1f:3b:72:eb:61:b8:0a:ef:43:63:65:
         c8:52:90:97:0d:0b:f9:c0:26:e4:7e:9b:75:e2:7f:d3:d4:f9:
         87:3c:1b:fd:6d:e1:bd:12:2d:c3:ee:e1:ff:b5:dc:cb:e1:f8:
         69:fb:bd:09
OpenSSL>
```

Now, create a ***.der*** file for Acme-subrootCA.

x509 -in Acme-subrootCA.crt -outform der -out Acme-subrootCA.der

```
OpenSSL> x509 -in Acme-subrootCA.crt -outform der -out Acme-subrootCA.der
OpenSSL>
```

Export subCA key file in subCA pfx file –

pkcs12 -inkey Acme-subrootCA.key -in Acme-subrootCA.crt -export -out Acme-subrootCA.pfx

```
penSSL> pkcs12 -inkey Acme-subrootCA.key -in Acme-subrootCA.crt -export -out Acme-subrootCA.pfx
2468:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\objects\obj_dat.c:699:
nter pass phrase for Acme-subrootCA.key:
nter Export Password:
erifying - Enter Export Password:
penSSL>
```

Step 8 (Signing sever certificate with subCA certificate):

x509 -req -CA Acme-subrootCA.crt -CAkey Acme-subrootCA.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile domain.ext

```
OpenSSL> x509 -req -CA Acme-subrootCA.crt -CAkey Acme-subrootCA.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile do
main.ext
Signature ok
subject=C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = www.verysecureserver.com, emailAddress = saeedussalehin
@outlook.com
Getting CA Private Key
12468:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\objects\obj_dat.c:699:
Enter pass phrase for Acme-subrootCA.key:
OpenSSL>
```

Checking server certificate –

x509 -text -noout -in server.crt

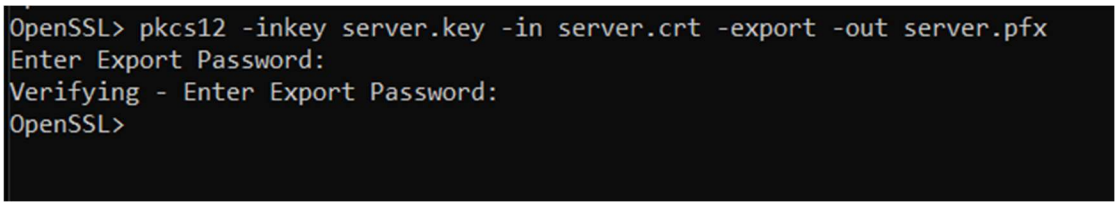
```
OpenSSL> x509 -text -noout -in server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            13:49:7c:e9:5a:ed:bf:54:5d:5a:28:eb:01:bd:b0:b6:25:34:0d:7b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = Acme-subrootCA, emailAddress = saeedussalehin@o
utlook.com
        Validity
            Not Before: Aug  4 03:56:15 2022 GMT
            Not After : Aug  4 03:56:15 2023 GMT
        Subject: C = BD, ST = Bangladesh, L = Dhaka, O = Nothing, OU = Nothing unit, CN = www.verysecureserver.com, emailAddress = saeed
ussalehin@outlook.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c4:f8:bf:4c:70:b0:9c:41:7f:20:cc:e6:32:d9:
                    e5:98:f9:4a:ae:18:d0:97:b8:14:32:fa:76:90:e9:
                    1e:71:56:06:d4:40:a9:1d:d6:b3:db:d1:0f:ca:de:
                    04:5f:53:9a:19:43:b2:25:92:61:0e:3e:ef:f9:88:
                    f2:84:72:93:c4:d0:28:24:79:83:10:16:89:19:22:
                    27:b3:25:cb:6c:a2:54:38:16:b2:d6:7c:d7:3e:2a:
                    39:d8:1e:53:30:69:ed:bd:44:e3:5d:7b:2b:a4:9c:
                    00:e5:50:89:08:47:b3:68:21:67:9c:45:72:fd:80:
                    9e:83:f1:15:a5:92:ac:d5:77:c7:60:1a:d3:6b:1d:
                    56:08:31:fb:1b:ab:df:5b:09:d3:3b:c9:7c:ad:df:
                    bc:f4:a5:7a:93:0f:69:6b:b8:55:92:94:76:38:42:
                    99:3f:03:d5:59:84:79:f9:0f:39:10:bc:48:33:74:
                    fe:63:c0:18:05:f4:d7:a1:12:a4:e5:ec:7b:b1:30:
                    72:aa:02:ed:65:07:d6:4d:0e:9d:31:b8:ac:2b:67:
                    06:9f:ea:c5:1c:20:14:cf:e7:1e:aa:ce:ba:98:00:
                    5c:3f:fd:83:71:32:35:3c:e9:39:c8:70:d1:e0:35:
                    21:6d:22:9f:7f:3e:ce:c6:92:46:59:e4:59:b8:13:
                    7c:9d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                DirName:/C=BD/ST=Bangladesh/L=Dhaka/O=Nothing/OU=Nothing unit/CN=Acme-rootCA/emailAddress=saeedussalehin@outlook.com
                serial:13:BA:18:C2:AC:5C:36:8D:00:7C:94:EC:EB:12:05:5C:0D:CC:78:99

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Alternative Name:
                DNS:www.verysecureserver.com, DNS:127.0.0.1
    Signature Algorithm: sha256WithRSAEncryption
         a3:41:52:15:ab:9d:c0:2e:23:8d:d7:13:ef:63:03:e9:a4:9d:
         50:5b:bc:8f:0d:ed:b4:3a:c1:ff:ed:bf:31:8a:7b:d2:c0:02:
         b6:03:f9:a8:88:53:72:94:b1:eb:3d:4f:a4:fa:18:bf:d3:d1:
         9b:4b:7b:b1:fd:68:17:8e:ae:ca:bd:ba:c5:28:b9:8e:d0:c4:
         52:80:b4:ad:a1:34:b3:a5:b6:9d:95:9c:21:63:27:82:bd:48:
         a2:32:38:91:98:e5:7d:7c:cd:1e:aa:93:0a:79:ac:89:bb:53:
         ba:4e:49:6e:91:5e:41:ee:a4:dc:4c:a2:1f:c0:b5:b1:b8:8a:
         c0:c1:34:ce:8f:89:9a:12:fc:05:8e:16:51:6a:06:07:ea:ea:
         fb:68:12:c7:ed:37:42:00:78:18:38:dd:ae:40:e9:7d:6d:69:
         01:10:4d:81:66:f3:a7:3f:8a:d9:c5:37:96:4b:ff:c5:7f:4e:
         f5:2d:6d:4e:25:71:fd:fa:e8:f4:f0:e8:99:9c:32:2c:eb:05:
         78:bc:b1:f1:2e:37:43:0f:4c:8f:37:06:b2:29:4c:29:c1:c4:
         b1:89:b7:c6:5d:05:de:46:ce:4c:f6:c3:b6:4a:bf:a5:77:85:
         6e:d8:13:49:23:c1:45:9d:93:89:0b:c9:eb:83:c4:bd:47:52:
         c7:06:b2:d1
penSSL>
```

Now, create a ***.der*** file for server

x509 -in server.crt -outform der -out server.der

Exporting the server key to server .pfx file –

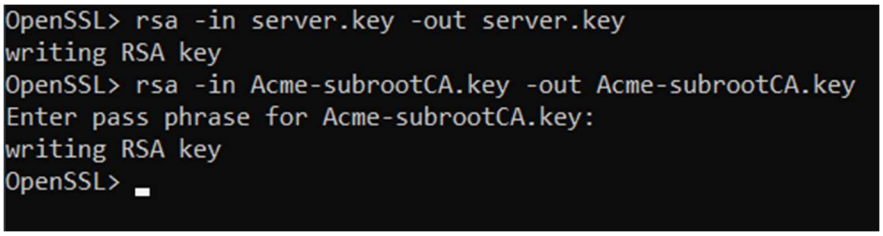
pkcs12 -inkey server.key -in server.crt -export -out server.pfx



Replacing RSA encryption from the server and subCA key –

rsa -in server.key -out server.key

rsa -in Acme-subrootCA.key -out Acme-subrootCA.key

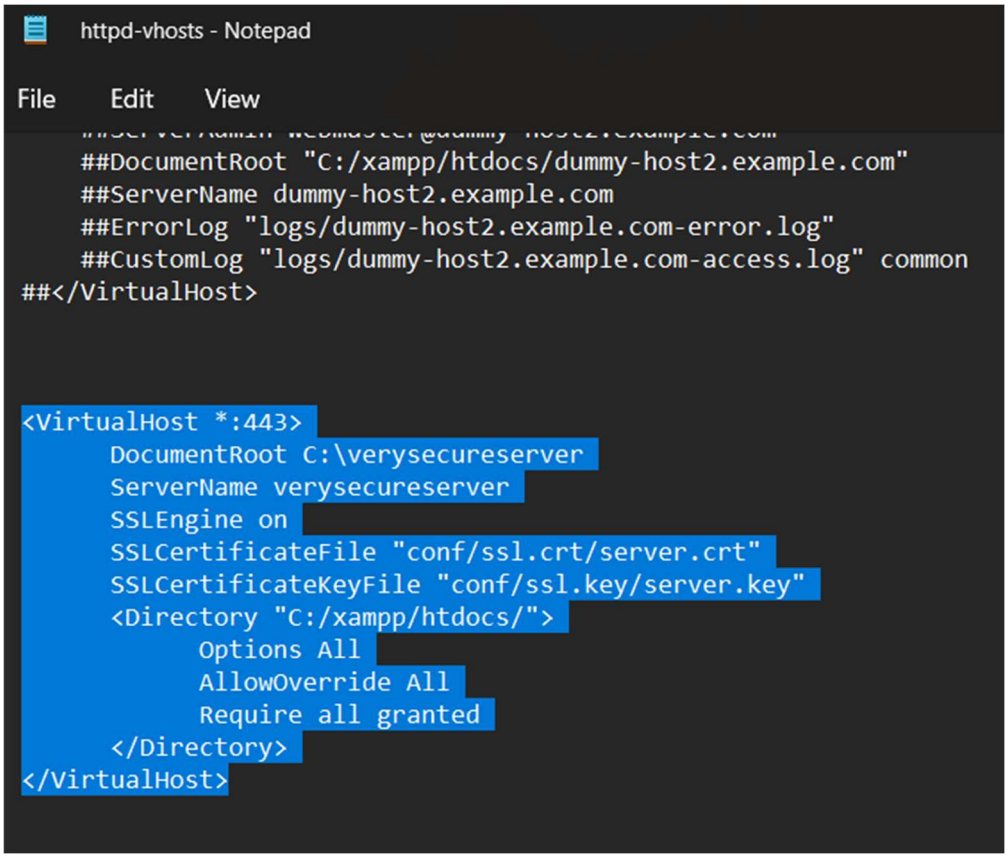


Step 9 (Configuring httpd-vhosts):

Navigate to **xampp/apache/conf/extra** and open ***httpd-vhosts.conf*** file in an editor and add the following lines and save the file.

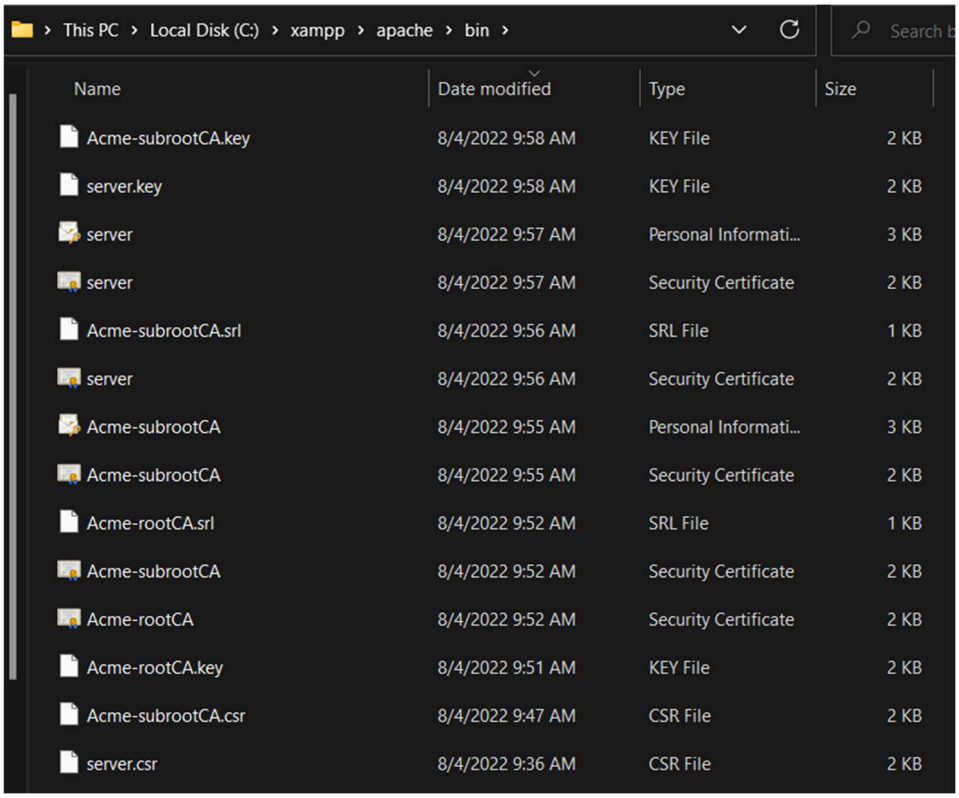
```
<VirtualHost *:443>
        DocumentRoot C:\verysecureserver
        ServerName verysecureserver
        SSLEngine on
        SSLCertificateFile "conf/ssl.crt/server.crt"
        SSLCertificateKeyFile "conf/ssl.key/server.key"
        <Directory "C:/xampp/htdocs/">
```

```
        Options All
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

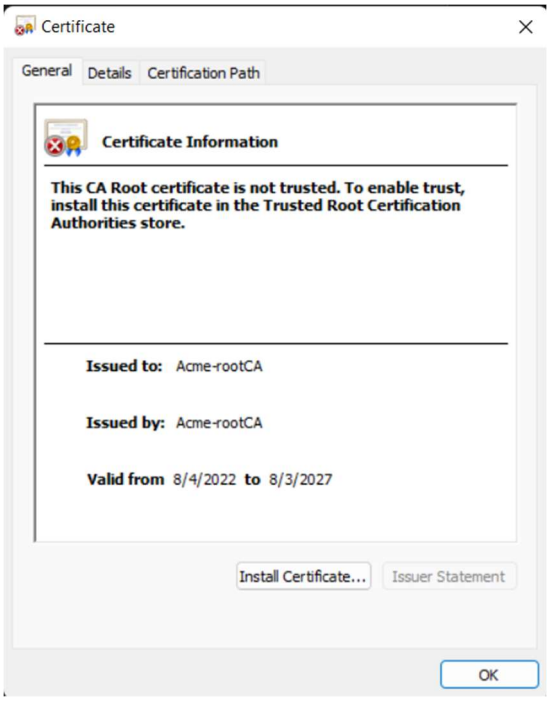


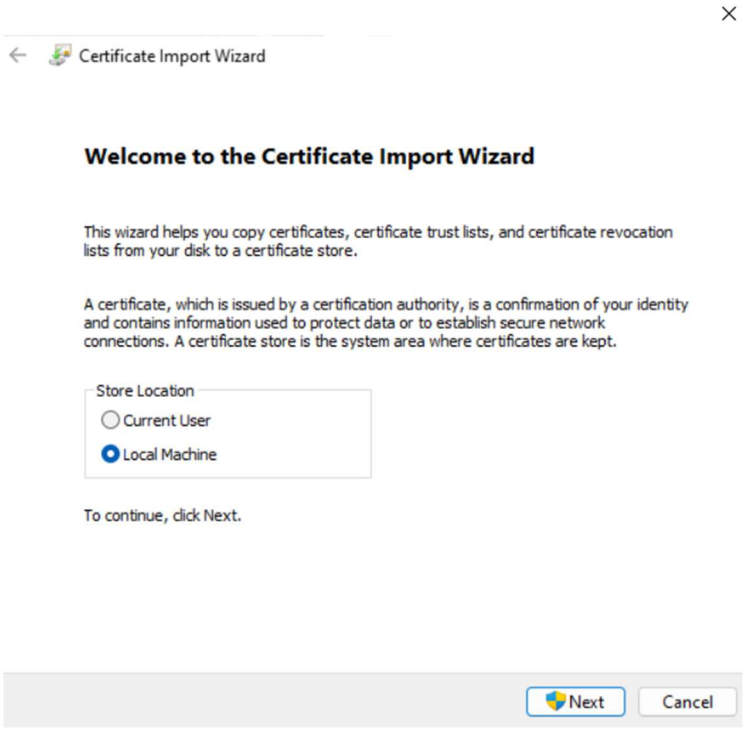
Step 10 (Installing the certificates):

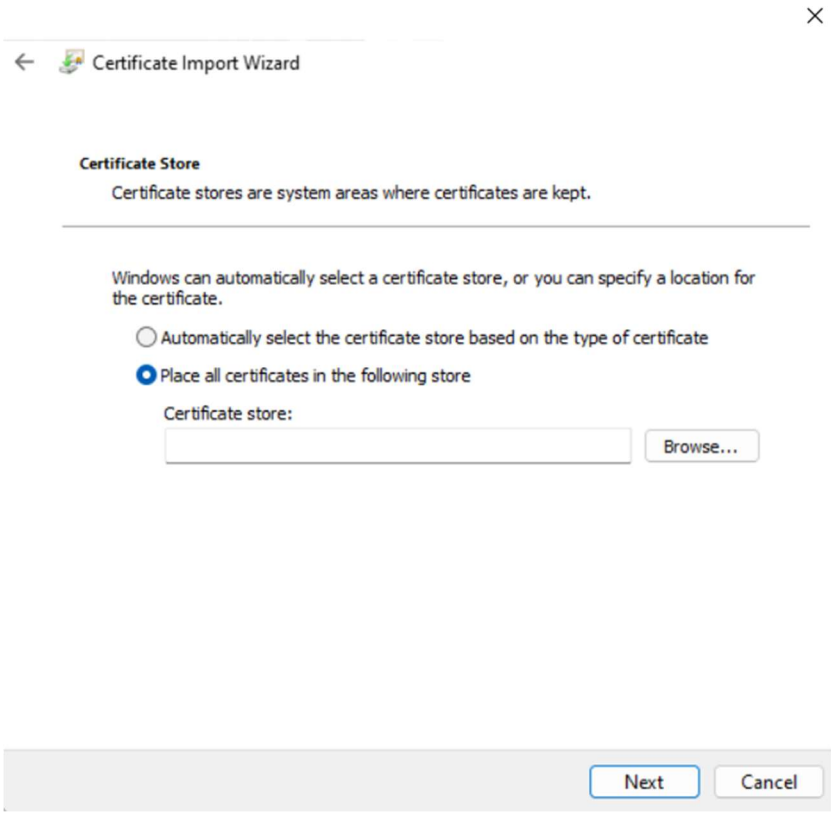
Navigate to **C:/xampp/apache/bin** folder and their will be the files we've just created.

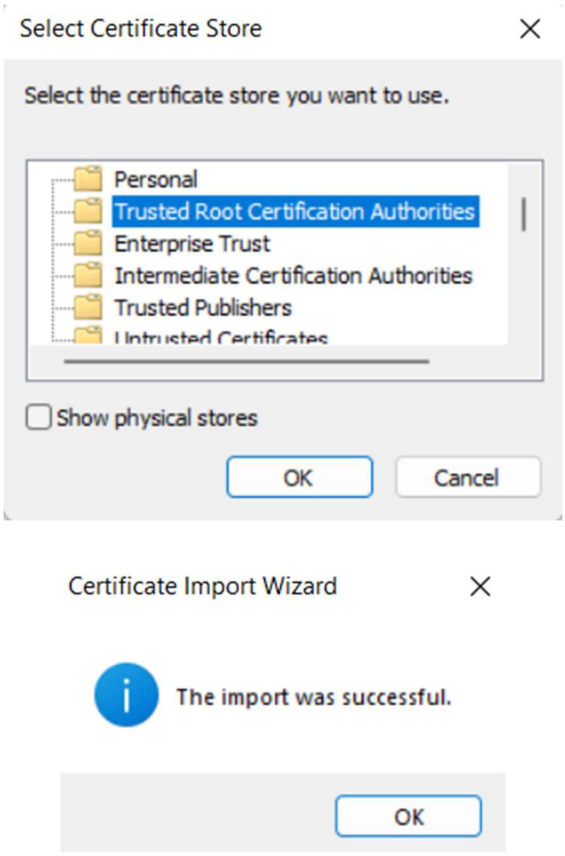


Double click on **Acme-rootCA.crt** to install the certificate in the local machine. Then in the next screen select “place all certificate in the following store”, then browse and select “trusted root authentication authorities”. Press OK and in the next screen press finish. If the import is successful, a popup window will open with the success message.

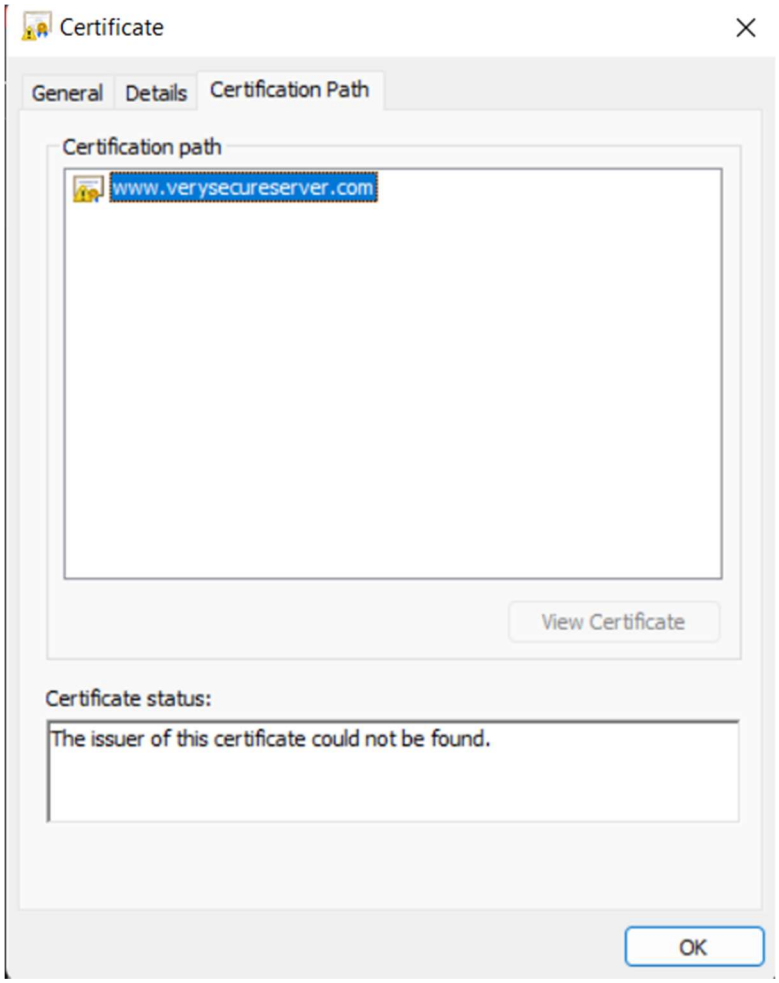



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Next
Cancel



Install **Acme-subrootCA** and **server.crt** following the same procedure.
Now, double click on **server.crt** to see the certification path.

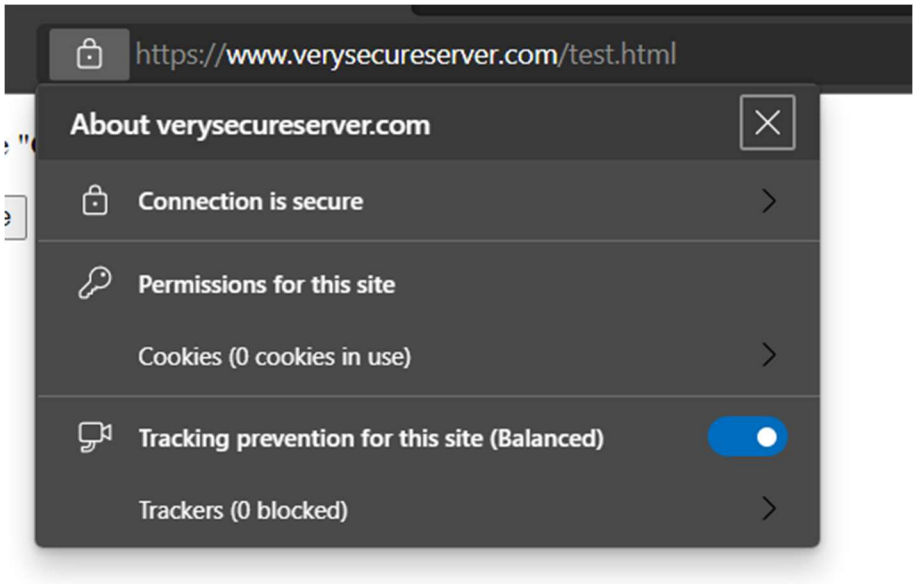


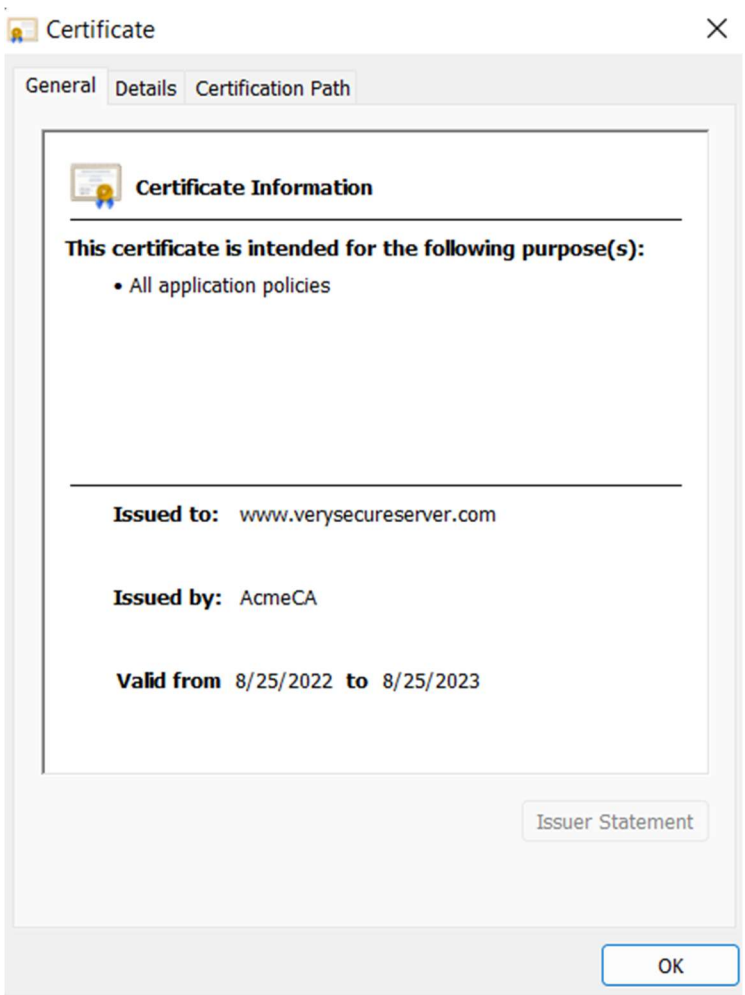
It's seen that issuer of the certificate is not found, it's because subrootCA.pfx file isn't imported. Install the subrootCA.pfx file found in xampp/apache/bin folder.

Lastly copy **server.crt, server.csr, server.key** from **C:/xampp/apache/bin** and paste it in **C:/xampp/apache/conf/ssl.crt, C:/xampp/apache/conf/ssl.csr, C:/xampp/apache/conf/ssl.key** directory respectively, replacing existing **server.crt** from that directory.

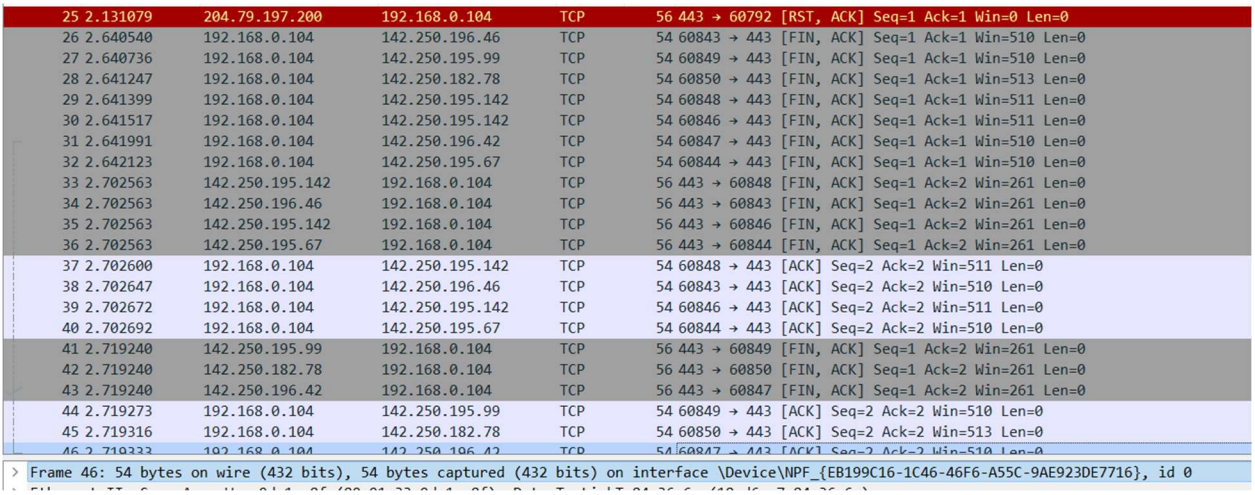
Checking the padlock icon:

Go to **Xampp control panel**, run the apache server and open ***www.verysecureserver.com*** on a browser. A padlock icon will be seen, indicating that the certificate we've just created is valid and the site is secured.


https://www.verysecureserver.com/test.html
About verysecureserver.com
Connection is secure
Permissions for this site
Cookies (0 cookies in use)
Tracking prevention for this site (Balanced)
Trackers (0 blocked)


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: www.verysecureserver.com
Issued by: AcmeCA
Valid from 8/25/2022 to 8/25/2023
Issuer Statement
OK

Checking with WireShark:



25	2.131079	204.79.197.200	192.168.0.104	TCP	56 443 → 60792 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	2.640540	192.168.0.104	142.250.196.46	TCP	54 60843 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
27	2.640736	192.168.0.104	142.250.195.99	TCP	54 60849 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
28	2.641247	192.168.0.104	142.250.182.78	TCP	54 60850 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
29	2.641399	192.168.0.104	142.250.195.142	TCP	54 60848 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
30	2.641517	192.168.0.104	142.250.195.142	TCP	54 60846 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
31	2.641991	192.168.0.104	142.250.196.42	TCP	54 60847 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
32	2.642123	192.168.0.104	142.250.195.67	TCP	54 60844 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
33	2.702563	142.250.195.142	192.168.0.104	TCP	56 443 → 60848 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
34	2.702563	142.250.196.46	192.168.0.104	TCP	56 443 → 60843 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
35	2.702563	142.250.195.142	192.168.0.104	TCP	56 443 → 60846 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
36	2.702563	142.250.195.67	192.168.0.104	TCP	56 443 → 60844 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
37	2.702600	192.168.0.104	142.250.195.142	TCP	54 60848 → 443 [ACK] Seq=2 Ack=2 Win=511 Len=0
38	2.702647	192.168.0.104	142.250.196.46	TCP	54 60843 → 443 [ACK] Seq=2 Ack=2 Win=510 Len=0
39	2.702672	192.168.0.104	142.250.195.142	TCP	54 60846 → 443 [ACK] Seq=2 Ack=2 Win=511 Len=0
40	2.702692	192.168.0.104	142.250.195.67	TCP	54 60844 → 443 [ACK] Seq=2 Ack=2 Win=510 Len=0
41	2.719240	142.250.195.99	192.168.0.104	TCP	56 443 → 60849 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
42	2.719240	142.250.182.78	192.168.0.104	TCP	56 443 → 60850 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
43	2.719240	142.250.196.42	192.168.0.104	TCP	56 443 → 60847 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
44	2.719273	192.168.0.104	142.250.195.99	TCP	54 60849 → 443 [ACK] Seq=2 Ack=2 Win=510 Len=0
45	2.719316	192.168.0.104	142.250.182.78	TCP	54 60850 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0
46	2.719333	192.168.0.104	142.250.196.42	TCP	54 60847 → 443 [ACK] Seq=2 Ack=2 Win=510 Len=0

> Frame 46: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{EB199C16-1C46-46F6-A55C-9AE923DE7716}, id 0

Revoking certificate:

Open openssl.exe to revoke the certificate issued to verysecureserver.com from the AcmeCA –
ca -config subrootCA.conf -revoke server.crt

To generate revocation crl file –
ca -config subrootCA.conf -gencrl -out rev.crl

To see the revocation file in the form of text –
crl -in rev.crl -noout -text