CSE487: Cyber Security, Law, and Ethics
Fall 2022

Project Report
Group No. – 13 (Section 1)

Submitted To:

Dr. Md. Hasanul Ferdaus
Assistant Professor, Department of Computer Science and Engineering
East West University

Submitted by:

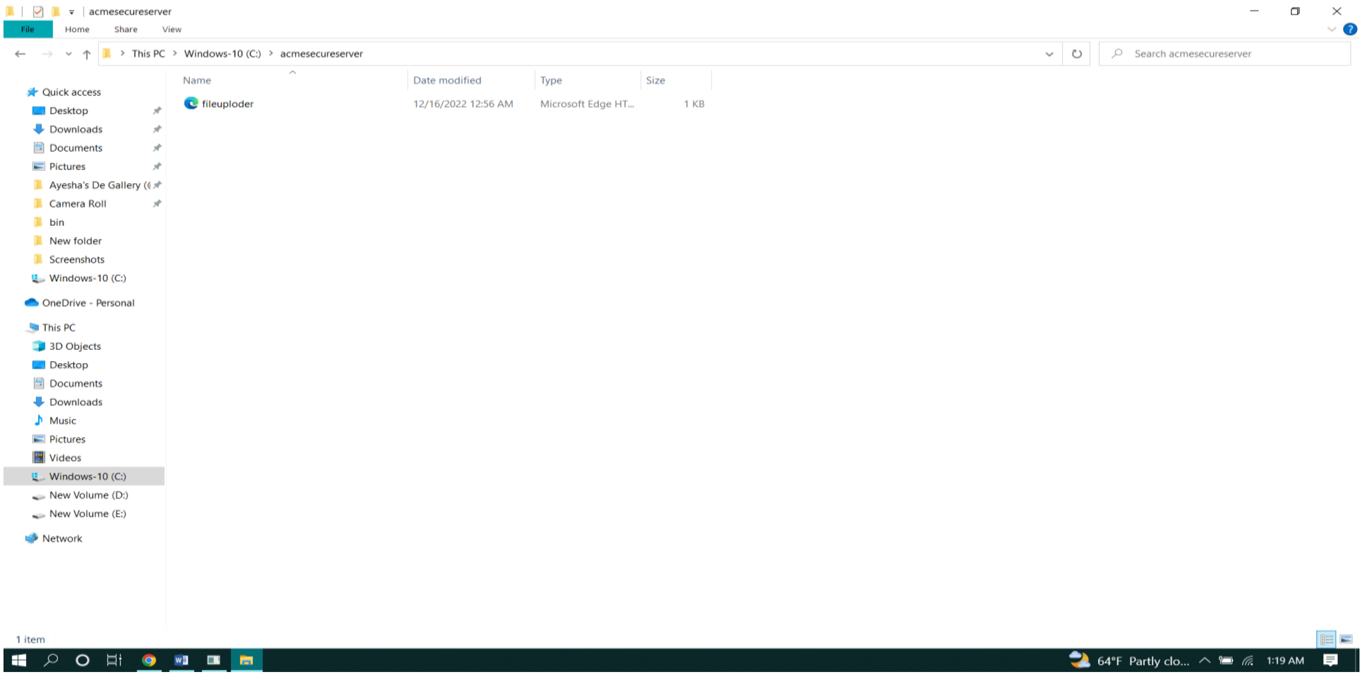
Student ID	Student Name	Contribution Percentage	Signature
2018-3-60-063	Apurba Roy Ajay	50%	Apurba
2018-2-60-035	Monjurul Alam	50%	Monjurul

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

Securing a networked system with PKI:

Here we are using windows-10 as an operating system.

At first, we need to create a folder named acmesecureserver in our C: drive where we will keep our filuploder.html file which is the basic design of a fill uploader page on a server.



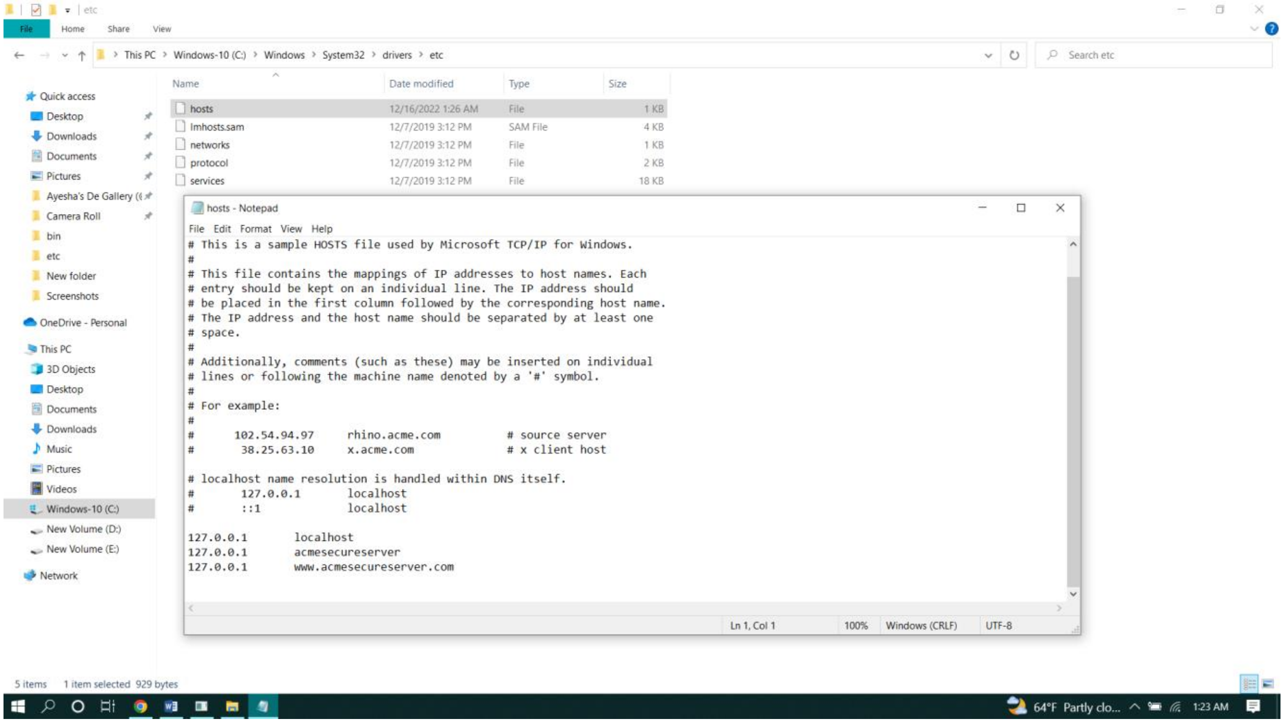
Name	Date modified	Type	Size
fileuploder	12/16/2022 12:56 AM	Microsoft Edge HT...	1 KB

Step 1:

For the DNS Configuration we have go C:\Windows →System32 →drivers →etc →hosts. And add the following lines

```
127.0.0.1       localhost
127.0.0.1       acmesecureserver
127.0.0.1       www.acmesecureserver.com
```

xampp→apache→conf→
httpd.conf:
DocumentRoot "C:/acmesecureserver"
<Directory "C:/acmesecureserver">



Name	Date modified	Type	Size
hosts	12/16/2022 1:26 AM	File	1 KB
lmhosts.sam	12/7/2019 3:12 PM	SAM File	4 KB
networks	12/7/2019 3:12 PM	File	1 KB
protocol	12/7/2019 3:12 PM	File	2 KB
services	12/7/2019 3:12 PM	File	18 KB

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1       localhost
127.0.0.1       acmesecureserver
127.0.0.1       www.acmesecureserver.com
```

Step 2:

Now we have to create openssl environment path configuration:

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

For creating a server certificate→

```
~ req -newkey rsa:2048 -nodes -keyout server.key -out server.csr
Common name: www.acmesecureserver.com
~ x509 -signkey server.key -in server.csr -req -days 365 -out server.crt
```

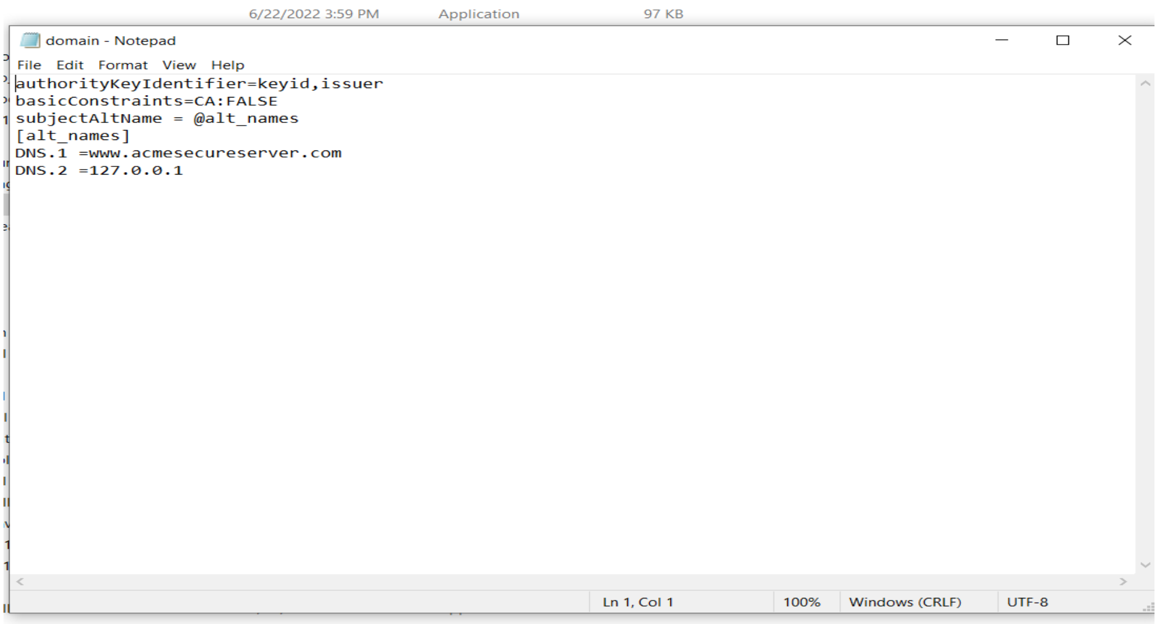
For creating a sub root CA certificate→

```
~  req -newkey rsa:2048 -keyout subrootCA.key -out subrootCA.csr
Common Name: AcmeCA
~  x509 -signkey subrootCA.key -in subrootCA.csr -req -days 365 -out subrootCA.crt
```

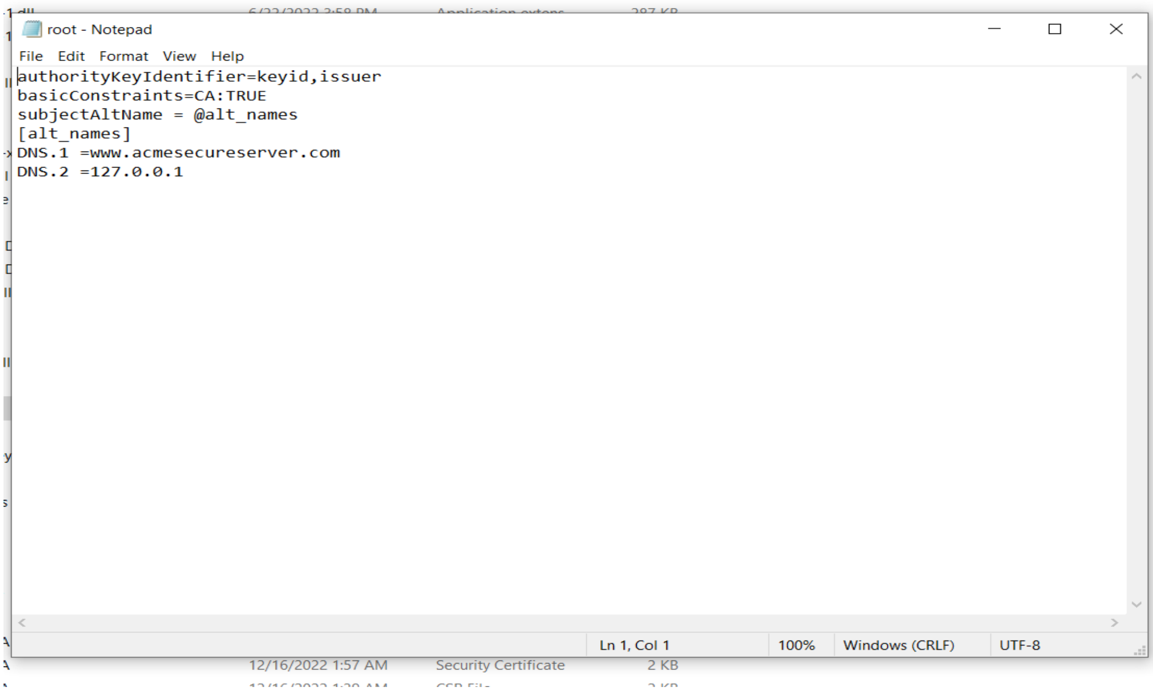
For creating a root CA certificate→

```
~  req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt
Common Name: Acme-RootCA
```

Finally, our three certificates are created. Now we can Sign in to server. But before sign in we need to create two ext. file in apache→bin folder. One is **domain. Ext** and another one is **root. Ext.** And then we have to put some codes into this folder.



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



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

And then for the exporting and signing we have to add some code in cmd. Which are:

Exporting the subrootCA key file in subrootCA pfx file→

```
~ pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx
```

Signing server certificate with subrootCA certificate→

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

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

Exporting the server key file in the server .pfx file→

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

Replacing the RSA encryption from the server and subrootCA key for setting the validity→

```
~ rsa -in server.key -out server.key
~ rsa -in subrootCA.key -out subrootCA.key
```

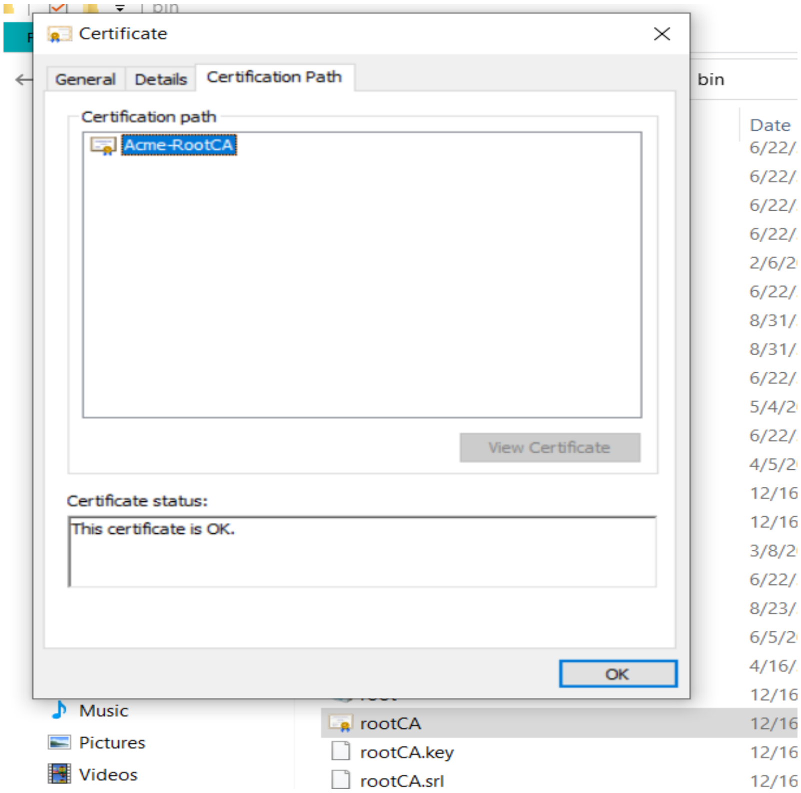
Step -3:

Creating certificate:
Configuring httpd-vhosts:

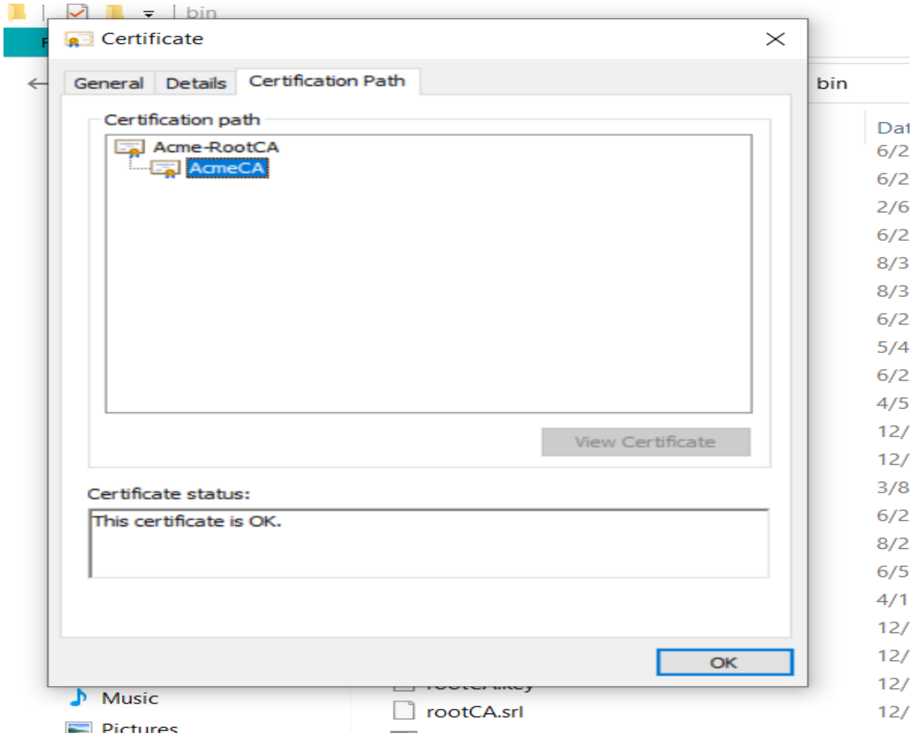
```
<VirtualHost *:443>
   DocumentRoot "C:/acmesecureserver/"
   ServerName acmesecureserver
   ServerAlias www.acmesecureserver.com
   SSLEngine on
   SSLCertificateFile "conf/ssl.crt/server.crt"
   SSLCertificateKeyFile "conf/ssl.key/server.key"
</VirtualHost>
```

Now our certificates are perfectly done. There are our Certificates.

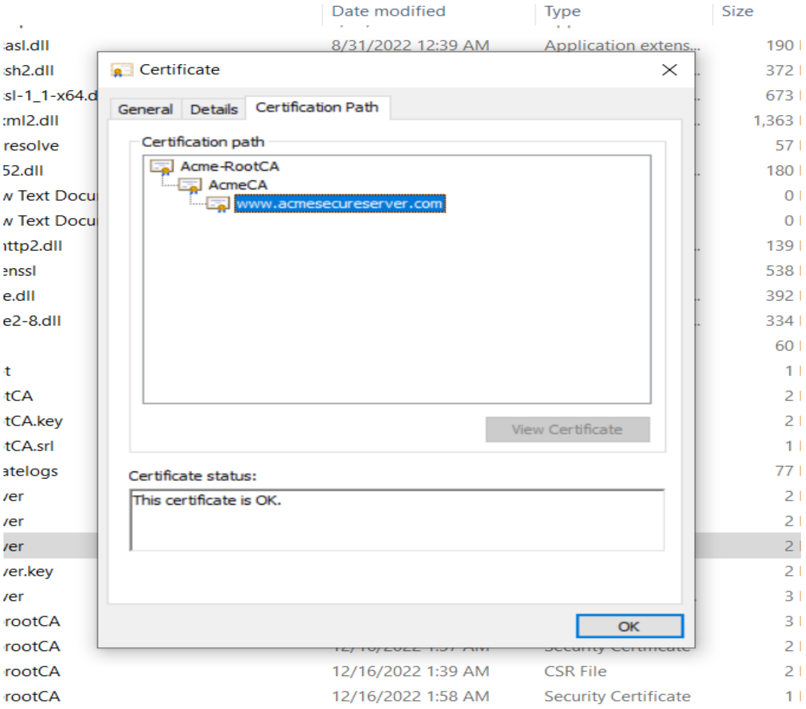
Root Certificates-



Sub root Certificates-



Server Certificates-



Certificate

General | Details | Certification Path

Certification path

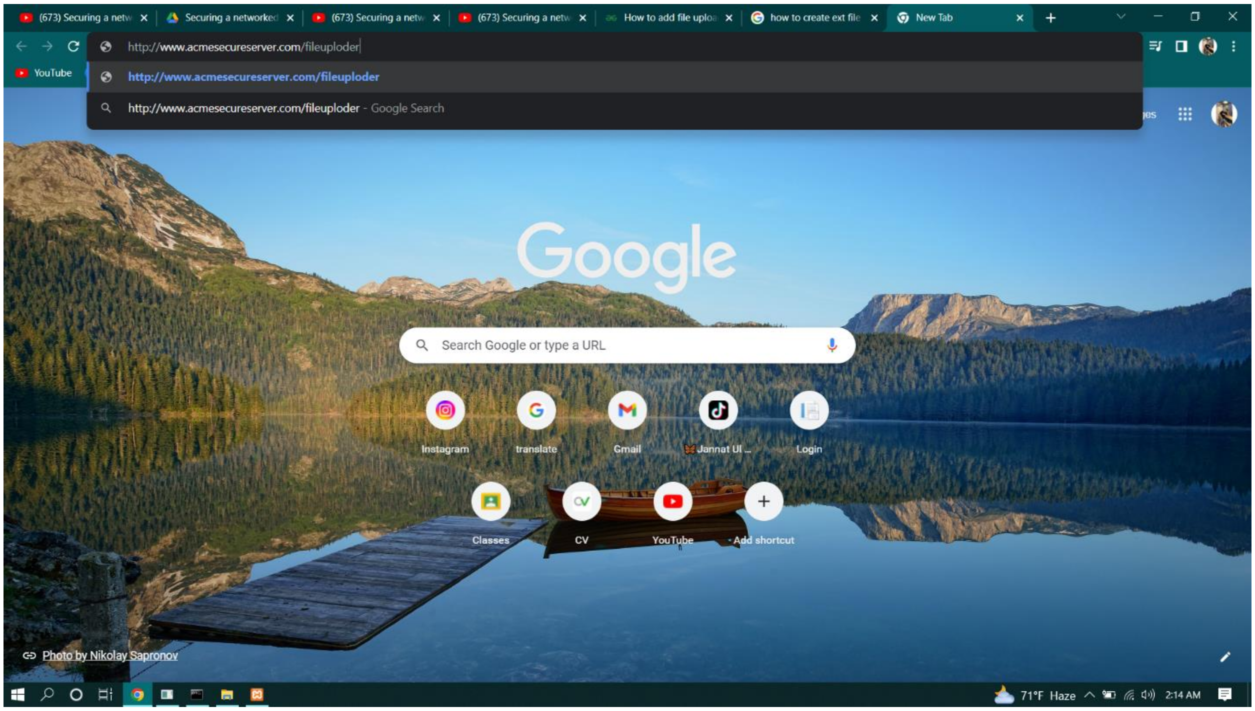
- Acme-RootCA
  - AcmeCA
    - www.acmesecureserver.com

Certificate status:

This certificate is OK.

	Date modified	Type	Size
asl.dll	8/31/2022 12:39 AM	Application extens...	190
sh2.dll			372
sl-1_1-x64.d			673
ml2.dll			1,363
resolve			57
52.dll			180
w Text Docu			0
w Text Docu			0
ttp2.dll			139
enssl			538
e.dll			392
e2-8.dll			334
			60
t			1
tCA			2
tCA.key			2
tCA.srl			1
atelogs			77
ver			2
ver			2
ver			2
ver.key			2
ver			3
rootCA			3
rootCA			2
rootCA	12/16/2022 1:39 AM	CSR File	2
rootCA	12/16/2022 1:58 AM	Security Certificate	1

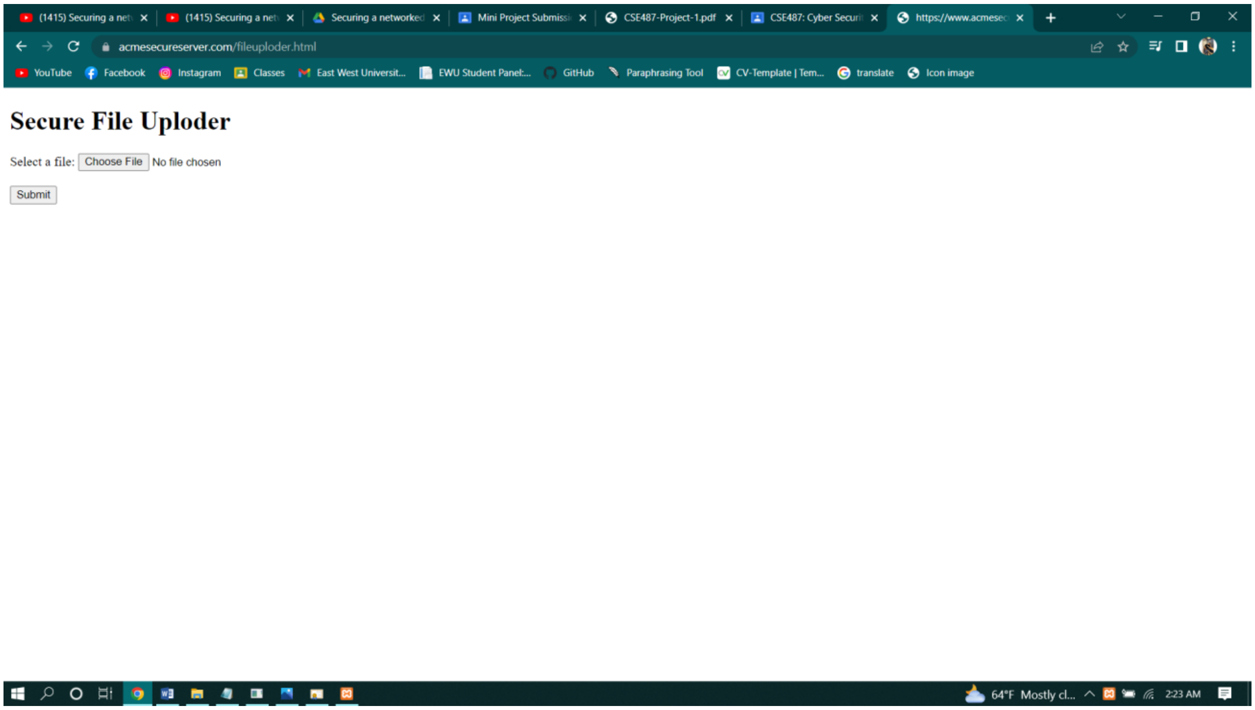
Now all of our Certificates is done. Now we can go to our server.



http://www.acmesecureserver.com/fileuploder

http://www.acmesecureserver.com/fileuploder

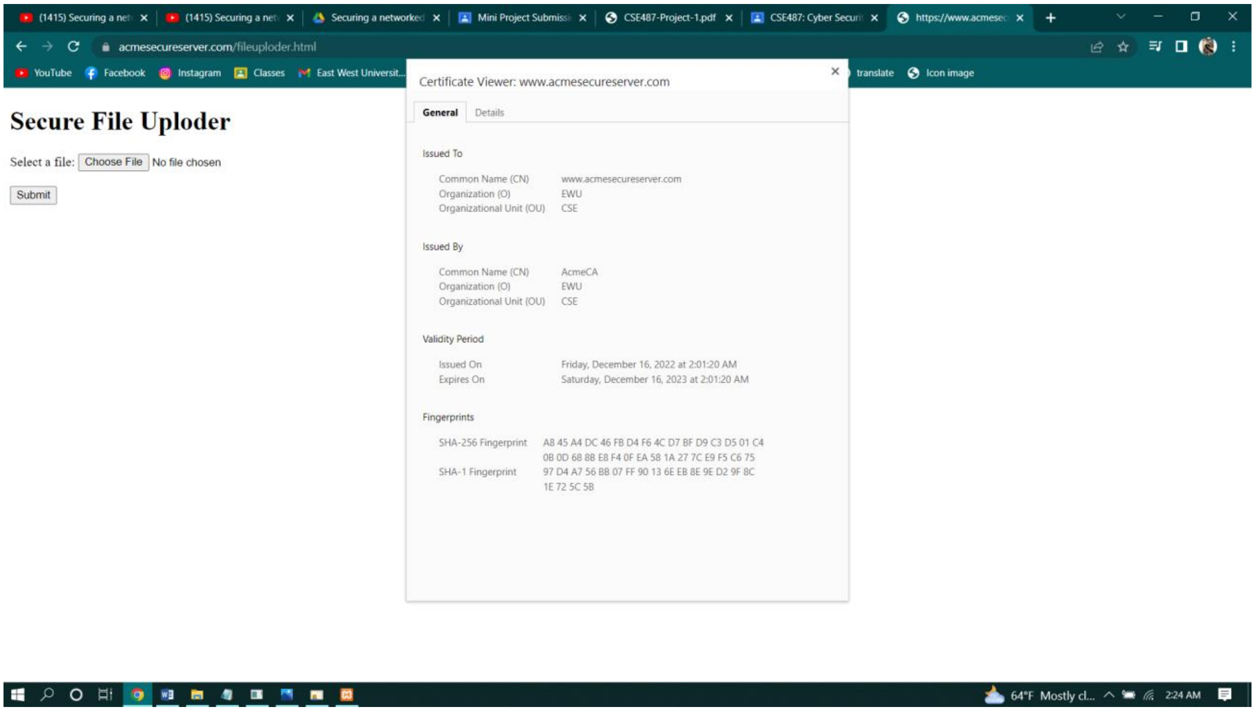
http://www.acmesecureserver.com/fileuploder - Google Search



Secure File Uploder

Select a file: Choose File No file chosen

Submit



Secure File Uploder

Select a file: Choose File No file chosen

Submit

Certificate Viewer: www.acmesecureserver.com

General Details

Issued To

```
Common Name (CN)            www.acmesecureserver.com
Organization (O)            EWU
Organizational Unit (OU)    CSE
```

Issued By

```
Common Name (CN)            AcmeCA
Organization (O)            EWU
Organizational Unit (OU)    CSE
```

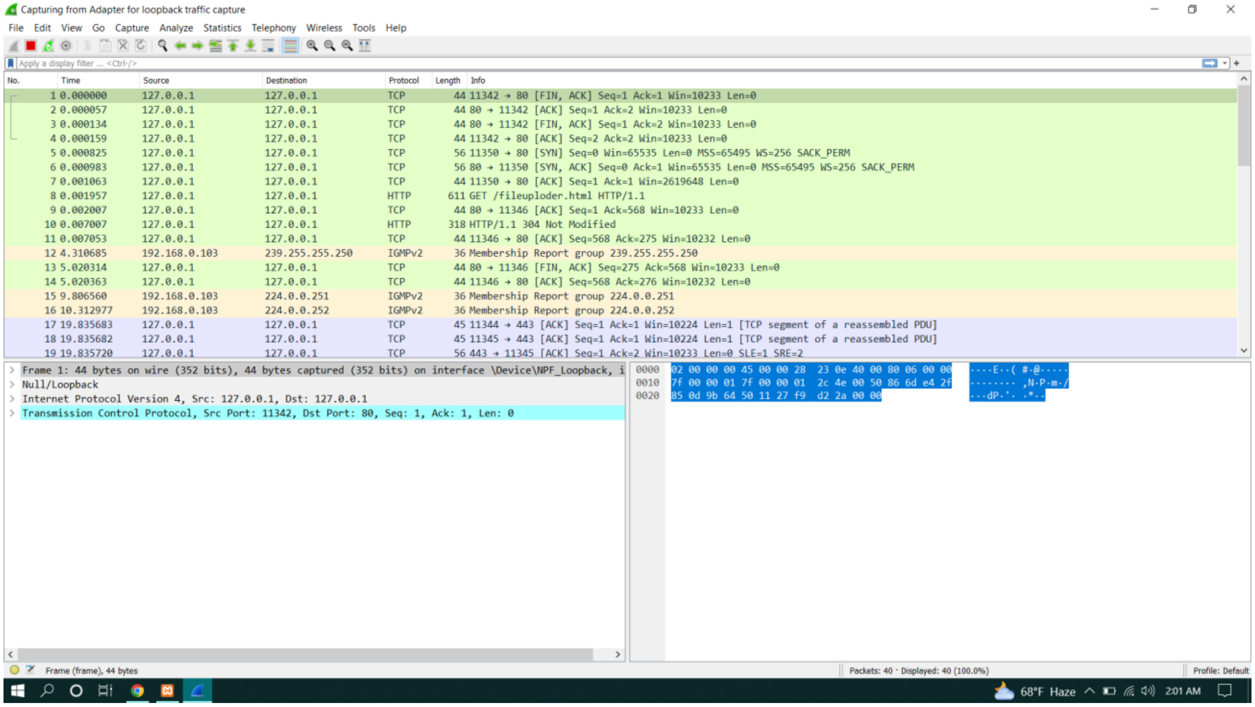
Validity Period

```
Issued On                   Friday, December 16, 2022 at 2:01:20 AM
Expires On                  Saturday, December 16, 2023 at 2:01:20 AM
```

Fingerprints

```
SHA-256 Fingerprint    A8 45 A4 DC 46 FB D4 F6 4C D7 BF D9 C3 D5 01 C4
                       0B 0D 68 8B E8 F4 0F EA 58 1A 27 7C E9 F5 C6 75
SHA-1 Fingerprint      97 D4 A7 56 BB 07 FF 90 13 6E EB 8E 9E D2 9F 8C
                       1E 72 5C 5B
```

Test security in Wireshark: Open wire Wireshark app, filter it by giving the IP address of the web server and start Wireshark.



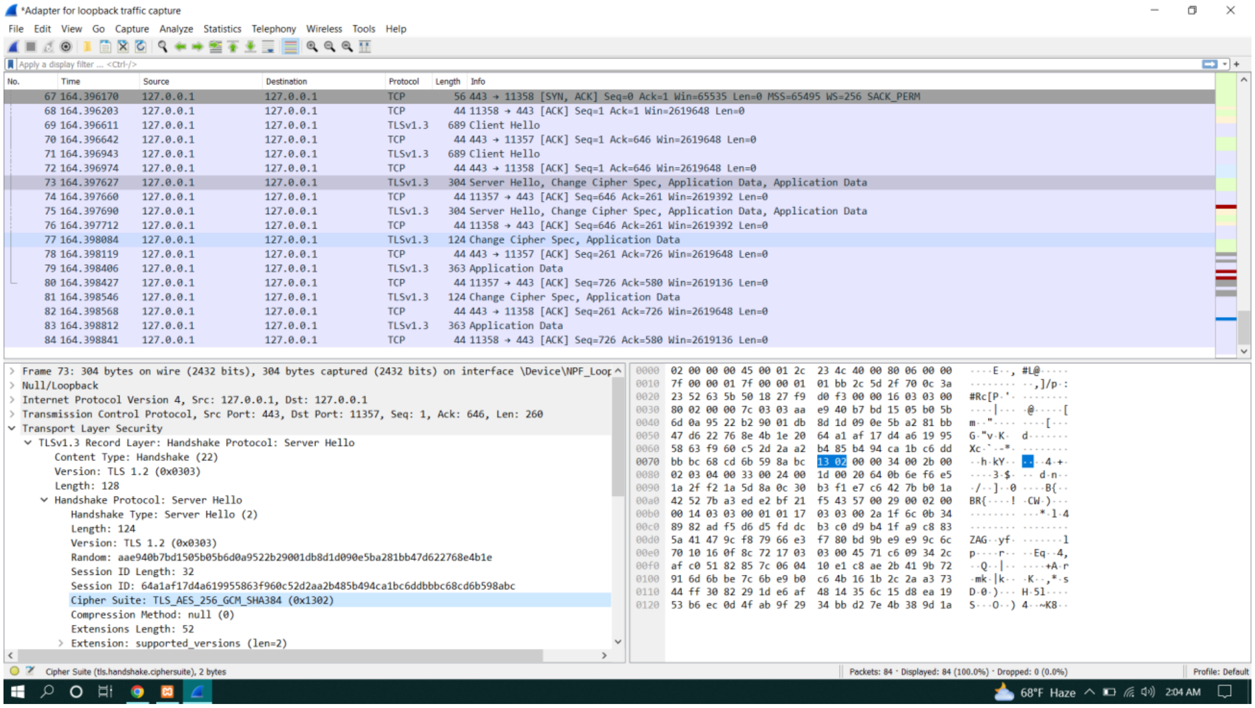
Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source         Destination      Protocol Length Info
    1 0.000000   127.0.0.1      127.0.0.1        TCP        44 11342 → 80 [FIN, ACK] Seq=1 Ack=1 Win=10233 Len=0
    2 0.000057   127.0.0.1      127.0.0.1        TCP        44 80 → 11342 [ACK] Seq=1 Ack=2 Win=10233 Len=0
    3 0.000134   127.0.0.1      127.0.0.1        TCP        44 80 → 11342 [FIN, ACK] Seq=1 Ack=2 Win=10233 Len=0
    4 0.000159   127.0.0.1      127.0.0.1        TCP        44 11342 → 80 [ACK] Seq=2 Ack=2 Win=10233 Len=0
    5 0.000825   127.0.0.1      127.0.0.1        TCP        56 11350 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
    6 0.000983   127.0.0.1      127.0.0.1        TCP        56 80 → 11350 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
    7 0.001063   127.0.0.1      127.0.0.1        TCP        44 11350 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
    8 0.001957   127.0.0.1      127.0.0.1        HTTP      611 GET /fileuploder.html HTTP/1.1
    9 0.002007   127.0.0.1      127.0.0.1        TCP        44 80 → 11346 [ACK] Seq=1 Ack=568 Win=10233 Len=0
   10 0.007007   127.0.0.1      127.0.0.1        HTTP      318 HTTP/1.1 304 Not Modified
   11 0.007053   127.0.0.1      127.0.0.1        TCP        44 11346 → 80 [ACK] Seq=568 Ack=275 Win=10232 Len=0
   12 4.310685   192.168.0.103  239.255.255.250  IGMPv2     36 Membership Report group 239.255.255.250
   13 5.020314   127.0.0.1      127.0.0.1        TCP        44 80 → 11346 [FIN, ACK] Seq=275 Ack=568 Win=10233 Len=0
   14 5.020363   127.0.0.1      127.0.0.1        TCP        44 11346 → 80 [ACK] Seq=568 Ack=276 Win=10232 Len=0
   15 9.806560   192.168.0.103  224.0.0.251      IGMPv2     36 Membership Report group 224.0.0.251
   16 10.312977  192.168.0.103  224.0.0.252      IGMPv2     36 Membership Report group 224.0.0.252
   17 19.835683  127.0.0.1      127.0.0.1        TCP        45 11344 → 443 [ACK] Seq=1 Ack=1 Win=10224 Len=1 [TCP segment of a reassembled PDU]
   18 19.835682  127.0.0.1      127.0.0.1        TCP        45 11345 → 443 [ACK] Seq=1 Ack=1 Win=10224 Len=1 [TCP segment of a reassembled PDU]
   19 19.835720  127.0.0.1      127.0.0.1        TCP        56 443 → 11345 [ACK] Seq=1 Ack=2 Win=10233 Len=0 SLE=1 SRE=2
```

```
> Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_Loopback, i
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 11342, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  02 00 00 00 45 00 00 28  23 0e 40 00 80 06 00 00   ····E··( #·@·····
0010  7f 00 00 01 7f 00 00 01  2c 4e 00 50 86 6d e4 2f   ········ ,N·P·m·/
0020  85 0d 9b 64 50 11 27 f9  d2 2a 00 00               ···dP·'· ·*··
```

```
Frame (frame), 44 bytes          Packets: 40 · Displayed: 40 (100.0%)          Profile: Default
```



*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source      Destination  Protocol Length Info
   67 164.396170  127.0.0.1   127.0.0.1    TCP        56 443 → 11358 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   68 164.396203  127.0.0.1   127.0.0.1    TCP        44 11358 → 443 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
   69 164.396611  127.0.0.1   127.0.0.1    TLSv1.3   689 Client Hello
   70 164.396642  127.0.0.1   127.0.0.1    TCP        44 443 → 11357 [ACK] Seq=1 Ack=646 Win=2619648 Len=0
   71 164.396943  127.0.0.1   127.0.0.1    TLSv1.3   689 Client Hello
   72 164.396974  127.0.0.1   127.0.0.1    TCP        44 443 → 11358 [ACK] Seq=1 Ack=646 Win=2619648 Len=0
   73 164.397627  127.0.0.1   127.0.0.1    TLSv1.3   304 Server Hello, Change Cipher Spec, Application Data, Application Data
   74 164.397660  127.0.0.1   127.0.0.1    TCP        44 11357 → 443 [ACK] Seq=646 Ack=261 Win=2619392 Len=0
   75 164.397690  127.0.0.1   127.0.0.1    TLSv1.3   304 Server Hello, Change Cipher Spec, Application Data, Application Data
   76 164.397712  127.0.0.1   127.0.0.1    TCP        44 11358 → 443 [ACK] Seq=646 Ack=261 Win=2619392 Len=0
   77 164.398084  127.0.0.1   127.0.0.1    TLSv1.3   124 Change Cipher Spec, Application Data
   78 164.398119  127.0.0.1   127.0.0.1    TCP        44 443 → 11357 [ACK] Seq=261 Ack=726 Win=2619648 Len=0
   79 164.398406  127.0.0.1   127.0.0.1    TLSv1.3   363 Application Data
   80 164.398427  127.0.0.1   127.0.0.1    TCP        44 11357 → 443 [ACK] Seq=726 Ack=580 Win=2619136 Len=0
   81 164.398546  127.0.0.1   127.0.0.1    TLSv1.3   124 Change Cipher Spec, Application Data
   82 164.398568  127.0.0.1   127.0.0.1    TCP        44 443 → 11358 [ACK] Seq=261 Ack=726 Win=2619648 Len=0
   83 164.398812  127.0.0.1   127.0.0.1    TLSv1.3   363 Application Data
   84 164.398841  127.0.0.1   127.0.0.1    TCP        44 11358 → 443 [ACK] Seq=726 Ack=580 Win=2619136 Len=0
```

```
> Frame 73: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits) on interface \Device\NPF_Loop
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 443, Dst Port: 11357, Seq: 1, Ack: 646, Len: 260
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 128
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 124
        Version: TLS 1.2 (0x0303)
        Random: aae940b7bd1505b05b6d0a9522b29001db8d1d090e5ba281bb47d622768e4b1e
        Session ID Length: 32
        Session ID: 64a1af17d4a619955863f960c52d2aa2b485b494ca1bc6ddbbbc68cd6b598abc
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 52
      > Extension: supported_versions (len=2)
```

```
0000  02 00 00 00 45 00 01 2c  23 4c 40 00 80 06 00 00   ····E··, #L@·····
0010  7f 00 00 01 7f 00 00 01  01 bb 2c 5d 2f 70 0c 3a   ········ ··,]/p·:
0020  23 52 63 5b 50 18 27 f9  d0 f3 00 00 16 03 03 00   #Rc[P·'· ········
0030  80 02 00 00 7c 03 03 aa  e9 40 b7 bd 15 05 b0 5b   ····|··· ·@·····[
0040  6d 0a 95 22 b2 90 01 db  8d 1d 09 0e 5b a2 81 bb   m··"···· ····[···
0050  47 d6 22 76 8e 4b 1e 20  64 a1 af 17 d4 a6 19 95   G·"v·K·  d·······
0060  58 63 f9 60 c5 2d 2a a2  b4 85 b4 94 ca 1b c6 dd   Xc·`·-*· ········
0070  bb bc 68 cd 6b 59 8a bc  13 02 00 00 34 00 2b 00   ··h·kY·· ····4·+·
0080  02 03 04 00 33 00 24 00  1d 00 20 64 0b 6e f6 e5   ····3·$· ·· d·n··
0090  1a 2f f2 1a 5d 8a 0c 30  b3 f1 e7 c6 42 7b b0 1a   ·/··]··0 ····B{··
00a0  42 52 7b a3 ed e2 bf 21  f5 43 57 00 29 00 02 00   BR{····! ·CW·)···
00b0  00 14 03 03 00 01 01 17  03 03 00 2a 1f 6c 0b 34   ········ ···*·l·4
00c0  89 82 ad f5 d6 d5 fd dc  b3 c0 d9 b4 1f a9 c8 83   ········ ········
00d0  5a 41 47 9c f8 79 66 e3  f7 80 bd 9b e9 e9 9c 6c   ZAG··yf· ·······l
00e0  70 10 16 0f 8c 72 17 03  03 00 45 71 c6 09 34 2c   p····r·· ··Eq··4,
00f0  af c0 51 82 85 7c 06 04  10 e1 c8 ae 2b 41 9b 72   ··Q··|·· ····+A·r
0100  91 6d 6b be 7c 6b e9 b0  c6 4b 16 1b 2c 2a a3 73   ·mk·|k·· ·K··,*·s
0110  44 ff 30 82 29 1d e6 af  48 14 35 6c 15 d8 ea 19   D·0·)··· H·5l····
0120  53 b6 ec 0d 4f ab 9f 29  34 bb d2 7e 4b 38 9d 1a   S···O··) 4··~K8··
```

```
Cipher Suite (tls.handshake.ciphersuite), 2 bytes     Packets: 84 · Displayed: 84 (100.0%) · Dropped: 0 (0.0%)     Profile: Default
```

Step 4:
Revocation of certificate:

Open openssl.exe to revoke the certificate issued to acmesecureserver.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
```