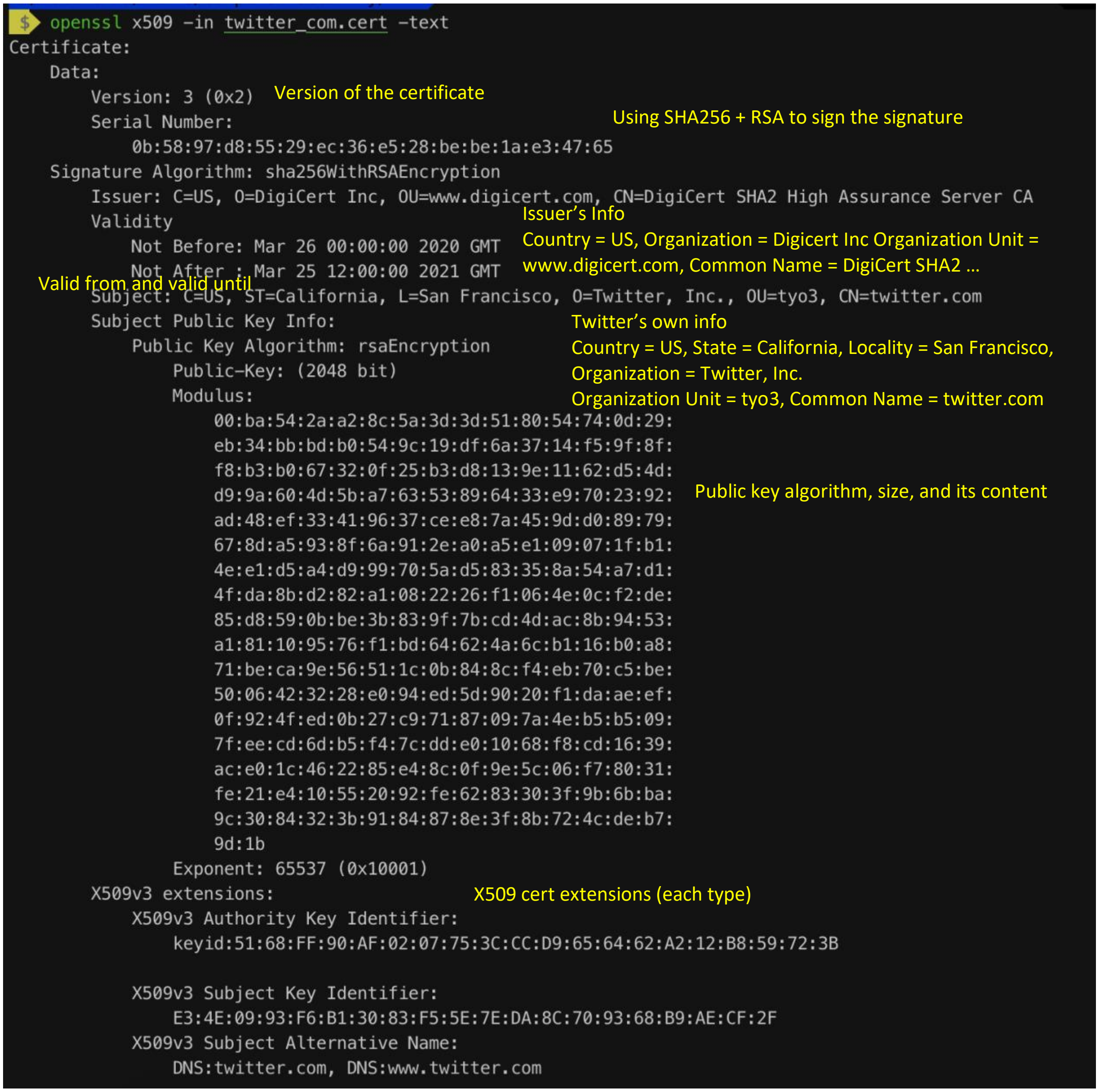
Phatcharapon Jumruspun 6031040921

Activity PKI

1. (I’m a Mac user)
2. (I’m a Mac user)
3.



```
$ openssl x509 -in twitter_com.cert -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0b:58:97:d8:55:29:ec:36:e5:28:be:be:1a:e3:47:65
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
        Validity
            Not Before: Mar 26 00:00:00 2020 GMT
            Not After : Mar 25 12:00:00 2021 GMT
        Subject: C=US, ST=California, L=San Francisco, O=Twitter, Inc., OU=tyo3, CN=twitter.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:54:2a:a2:8c:5a:3d:3d:51:80:54:74:0d:29:
                    eb:34:bb:bd:b0:54:9c:19:df:6a:37:14:f5:9f:8f:
                    f8:b3:b0:67:32:0f:25:b3:d8:13:9e:11:62:d5:4d:
                    d9:9a:60:4d:5b:a7:63:53:89:64:33:e9:70:23:92:
                    ad:48:ef:33:41:96:37:ce:e8:7a:45:9d:d0:89:79:
                    67:8d:a5:93:8f:6a:91:2e:a0:a5:e1:09:07:1f:b1:
                    4e:e1:d5:a4:d9:99:70:5a:d5:83:35:8a:54:a7:d1:
                    4f:da:8b:d2:82:a1:08:22:26:f1:06:4e:0c:f2:de:
                    85:d8:59:0b:be:3b:83:9f:7b:cd:4d:ac:8b:94:53:
                    a1:81:10:95:76:f1:bd:64:62:4a:6c:b1:16:b0:a8:
                    71:be:ca:9e:56:51:1c:0b:84:8c:f4:eb:70:c5:be:
                    50:06:42:32:28:e0:94:ed:5d:90:20:f1:da:ae:ef:
                    0f:92:4f:ed:0b:27:c9:71:87:09:7a:4e:b5:b5:09:
                    7f:ee:cd:6d:b5:f4:7c:dd:e0:10:68:f8:cd:16:39:
                    ac:e0:1c:46:22:85:e4:8c:0f:9e:5c:06:f7:80:31:
                    fe:21:e4:10:55:20:92:fe:62:83:30:3f:9b:6b:ba:
                    9c:30:84:32:3b:91:84:87:8e:3f:8b:72:4c:de:b7:
                    9d:1b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:51:68:FF:90:AF:02:07:75:3C:CC:D9:65:64:62:A2:12:B8:59:72:3B

            X509v3 Subject Key Identifier:
                E3:4E:09:93:F6:B1:30:83:F5:5E:7E:DA:8C:70:93:68:B9:AE:CF:2F
            X509v3 Subject Alternative Name:
                DNS:twitter.com, DNS:www.twitter.com
```

Version of the certificate

Using SHA256 + RSA to sign the signature

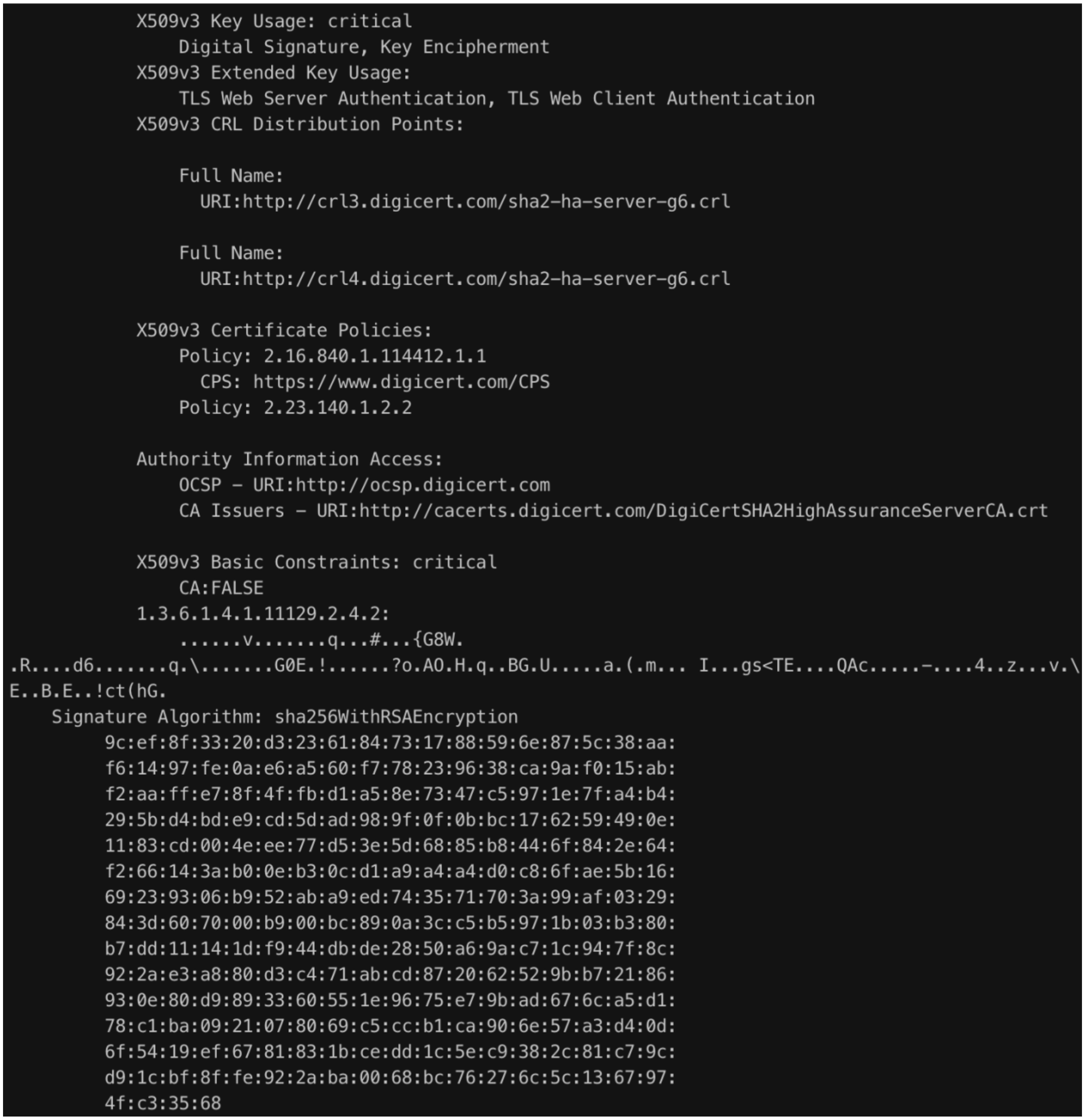
Issuer’s Info
Country = US, Organization = Digicert Inc Organization Unit = www.digicert.com, Common Name = DigiCert SHA2 ...

Valid from and valid until

Twitter’s own info
Country = US, State = California, Locality = San Francisco, Organization = Twitter, Inc.
Organization Unit = tyo3, Common Name = twitter.com

Public key algorithm, size, and its content

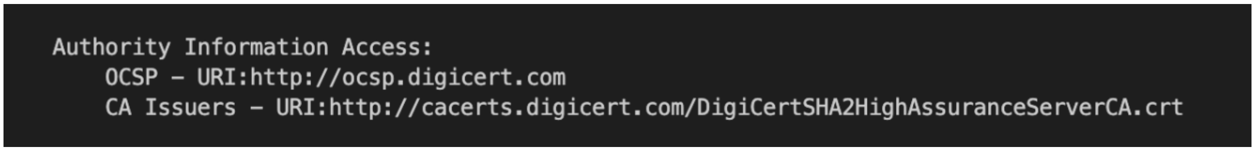
X509 cert extensions (each type)



```
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl3.digicert.com/sha2-ha-server-g6.crl

                Full Name:
                  URI:http://crl4.digicert.com/sha2-ha-server-g6.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114412.1.1
                  CPS: https://www.digicert.com/CPS
                Policy: 2.23.140.1.2.2

            Authority Information Access:
                OCSP - URI:http://ocsp.digicert.com
                CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt

            X509v3 Basic Constraints: critical
                CA:FALSE
            1.3.6.1.4.1.11129.2.4.2:
                ......v.......q...#...{G8W.
.R....d6.......q.\.......G0E.!......?o.AO.H.q..BG.U.....a.(.m... I...gs<TE....QAc.....-....4..z...v.\
E..B.E..!ct(hG.
    Signature Algorithm: sha256WithRSAEncryption
         9c:ef:8f:33:20:d3:23:61:84:73:17:88:59:6e:87:5c:38:aa:
         f6:14:97:fe:0a:e6:a5:60:f7:78:23:96:38:ca:9a:f0:15:ab:
         f2:aa:ff:e7:8f:4f:fb:d1:a5:8e:73:47:c5:97:1e:7f:a4:b4:
         29:5b:d4:bd:e9:cd:5d:ad:98:9f:0f:0b:bc:17:62:59:49:0e:
         11:83:cd:00:4e:ee:77:d5:3e:5d:68:85:b8:44:6f:84:2e:64:
         f2:66:14:3a:b0:0e:b3:0c:d1:a9:a4:a4:d0:c8:6f:ae:5b:16:
         69:23:93:06:b9:52:ab:a9:ed:74:35:71:70:3a:99:af:03:29:
         84:3d:60:70:00:b9:00:bc:89:0a:3c:c5:b5:97:1b:03:b3:80:
         b7:dd:11:14:1d:f9:44:db:de:28:50:a6:9a:c7:1c:94:7f:8c:
         92:2a:e3:a8:80:d3:c4:71:ab:cd:87:20:62:52:9b:b7:21:86:
         93:0e:80:d9:89:33:60:55:1e:96:75:e7:9b:ad:67:6c:a5:d1:
         78:c1:ba:09:21:07:80:69:c5:cc:b1:ca:90:6e:57:a3:d4:0d:
         6f:54:19:ef:67:81:83:1b:ce:dd:1c:5e:c9:38:2c:81:c7:9c:
         d9:1c:bf:8f:fe:92:2a:ba:00:68:bc:76:27:6c:5c:13:67:97:
         4f:c3:35:68
```

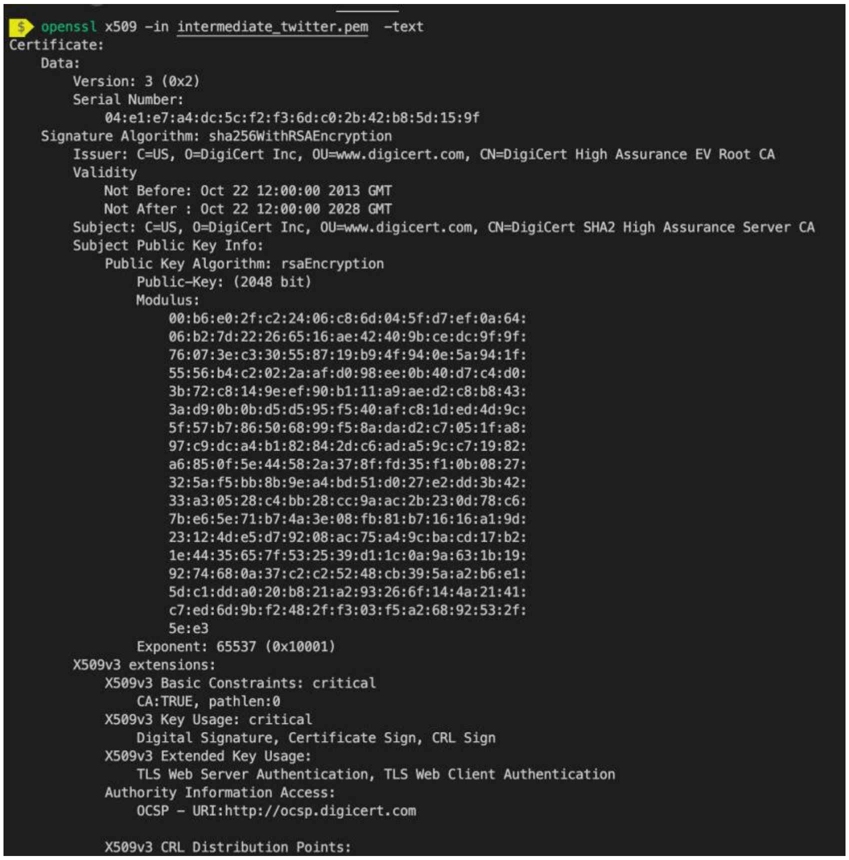
4.

The picture below shows information about the intermediate certificate. The purpose of it is to make people “trust” the subject’s certificate more (in this case, twitter’s).



```
    Authority Information Access:
        OCSP - URI:http://ocsp.digicert.com
        CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt
```

This part indicates issuer’s URI, which is the download link of the intermediate cert



```
$ openssl x509 -in intermediate_twitter.pem  -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:e1:e7:a4:dc:5c:f2:f3:6d:c0:2b:42:b8:5d:15:9f
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA
        Validity
            Not Before: Oct 22 12:00:00 2013 GMT
            Not After : Oct 22 12:00:00 2028 GMT
        Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:e0:2f:c2:24:06:c8:6d:04:5f:d7:ef:0a:64:
                    06:b2:7d:22:26:65:16:ae:42:40:9b:ce:dc:9f:9f:
                    76:07:3e:c3:30:55:87:19:b9:4f:94:0e:5a:94:1f:
                    55:56:b4:c2:02:2a:af:d0:98:ee:0b:40:d7:c4:d0:
                    3b:72:c8:14:9e:ef:90:b1:11:a9:ae:d2:c8:b8:43:
                    3a:d9:0b:0b:d5:d5:95:f5:40:af:c8:1d:ed:4d:9c:
                    5f:57:b7:86:50:68:99:f5:8a:da:d2:c7:05:1f:a8:
                    97:c9:dc:a4:b1:82:84:2d:c6:ad:a5:9c:c7:19:82:
                    a6:85:0f:5e:44:58:2a:37:8f:fd:35:f1:0b:08:27:
                    32:5a:f5:bb:8b:9e:a4:bd:51:d0:27:e2:dd:3b:42:
                    33:a3:05:28:c4:bb:28:cc:9a:ac:2b:23:0d:78:c6:
                    7b:e6:5e:71:b7:4a:3e:08:fb:81:b7:16:16:a1:9d:
                    23:12:4d:e5:d7:92:08:ac:75:a4:9c:ba:cd:17:b2:
                    1e:44:35:65:7f:53:25:39:d1:1c:0a:9a:63:1b:19:
                    92:74:68:0a:37:c2:c2:52:48:cb:39:5a:a2:b6:e1:
                    5d:c1:dd:a0:20:b8:21:a2:93:26:6f:14:4a:21:41:
                    c7:ed:6d:9b:f2:48:2f:f3:03:f5:a2:68:92:53:2f:
                    5e:e3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            Authority Information Access:
                OCSP - URI:http://ocsp.digicert.com

            X509v3 CRL Distribution Points:
```

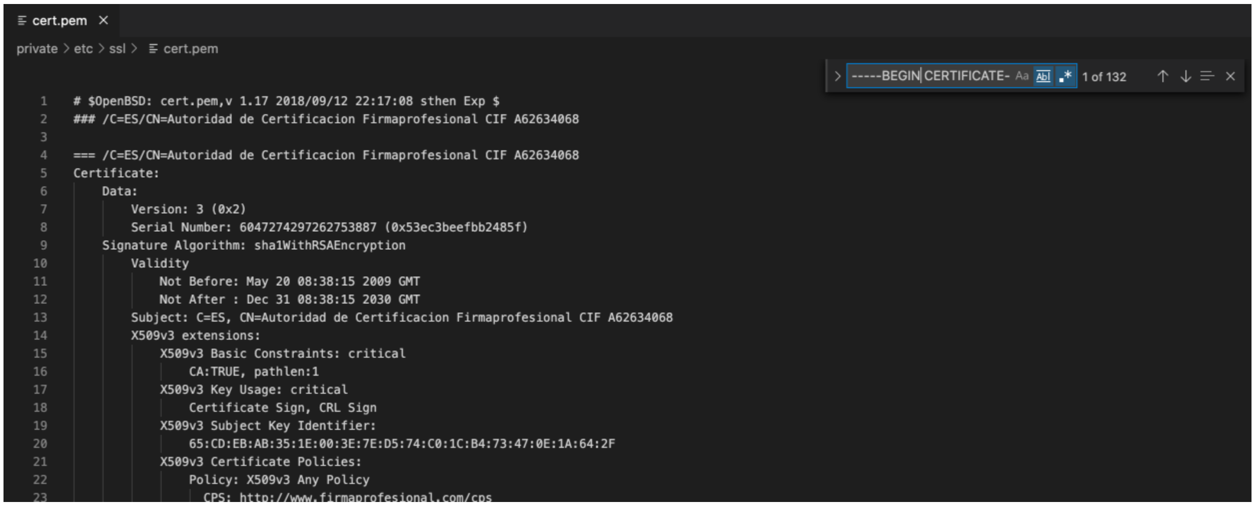
Intermediate certificate downloaded and translated

5. The intermediate CA is the same organization as the root CA (digicert.com) as labeled in the pic above.

6. It’s a file containing root and intermediate CAs (chain of trusts). Used to ensure the user to trust that particular site.

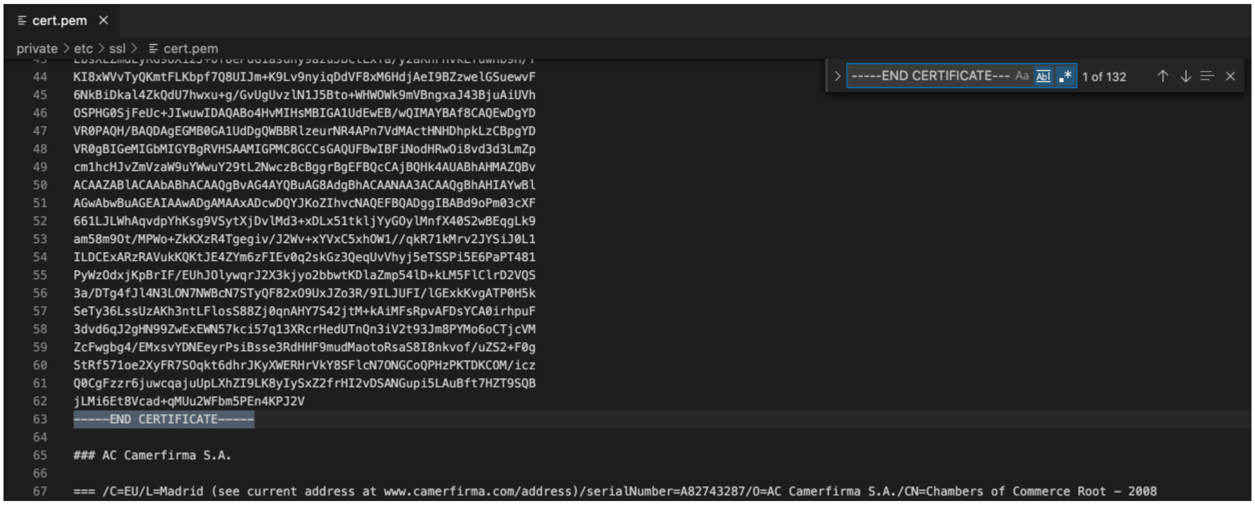
7. 132 Certificates

Counted by VSCode Search function on “-----BEGIN CERTIFICATE-----”
(“-----END CERTIFICATE-----“ also yields the same result)



```
# $OpenBSD: cert.pem,v 1.17 2018/09/12 22:17:08 sthen Exp $
### /C=ES/CN=Autoridad de Certificacion Firmaprofesional CIF A62634068

=== /C=ES/CN=Autoridad de Certificacion Firmaprofesional CIF A62634068
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 6047274297262753887 (0x53ec3beefbb2485f)
    Signature Algorithm: sha1WithRSAEncryption
        Validity
            Not Before: May 20 08:38:15 2009 GMT
            Not After : Dec 31 08:38:15 2030 GMT
        Subject: C=ES, CN=Autoridad de Certificacion Firmaprofesional CIF A62634068
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://www.firmaprofesional.com/cps
```

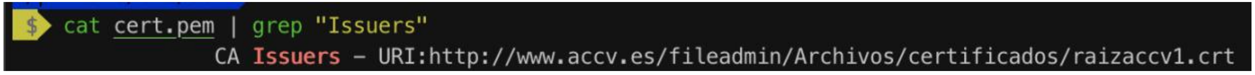
Search function with -----BEGIN CERTIFICATE-----



```
KI8xWVvTyQKmtFLKbpf7Q8UIJm+K9Lv9nyiqDdVF8xM6HdjAeI9BZzwelGSuewvF
6NkBiDkal4ZkQdU7hwxu+g/GvUgUvzlN1J5Bto+WHWOWk9mVBngxaJ43BjuAiUVh
OSPHG0SjFeUc+JIwuwIDAQABo4HvMIHsMBIGA1UdEwEB/wQIMAYBAf8CAQEwDgYD
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRlzeurNR4APn7VdMActHNHDhpkLzCBpgYD
VR0gBIGeMIGbMIGYBgRVHSAAMIGPMC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LmZp
cm1hcHJvZmVzaW9uYWwuY29tL2NwczBcBggrBgEFBQcCAjBQHk4AUABhAHMAZQBv
ACAAZABlACAAbABhACAAQgBvAG4AYQBuAG8AdgBhACAANAA3ACAAQgBhAHIAYwBl
AGwAbwBuAGEAIAAwADgAMAAxADcwDQYJKoZIhvcNAQEFBQADggIBABd9oPm03cXF
661LJLWhAqvdpYhKsg9VSytXjDvlMd3+xDLx51tkljYyGOylMnfX40S2wBEqgLk9
am58m9Ot/MPWo+ZkKXzR4Tgegiv/J2Wv+xYVxC5xhOW1//qkR71kMrv2JYSiJ0L1
ILDCExARzRAVukKQKtJE4ZYm6zFIEv0q2skGz3QeqUvVhyj5eTSSPi5E6PaPT481
PyWzOdxjKpBrIF/EUhJOlywqrJ2X3kjyo2bbwtKDlaZmp54lD+kLM5FlClrD2VQS
3a/DTg4fJl4N3LON7NWBcN7STyQF82xO9UxJZo3R/9ILJUFI/lGExkKvgATP0H5k
SeTy36LssUzAKh3ntLFlosS88Zj0qnAHY7S42jtM+kAiMFsRpvAFDsYCA0irhpuF
3dvd6qJ2gHN99ZwExEWN57kci57q13XRcrHedUTnQn3iV2t93Jm8PYMo6oCTjcVM
ZcFwgbg4/EMxsvYDNEeyrPsiBsse3RdHHF9mudMaotoRsaS8I8nkvof/uZS2+F0g
StRf571oe2XyFR7SOqkt6dhrJKyXWERHrVkY8SFlcN7ONGCoQPHzPKTDKCOM/icz
Q0CgFzzr6juwcqajuUpLXhZI9LK8yIySxZ2frHI2vDSANGupi5LAuBft7HZT9SQB
jLMi6Et8Vcad+qMUu2WFbm5PEn4KPJ2V
-----END CERTIFICATE-----

### AC Camerfirma S.A.

=== /C=EU/L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287/O=AC Camerfirma S.A./CN=Chambers of Commerce Root - 2008
```

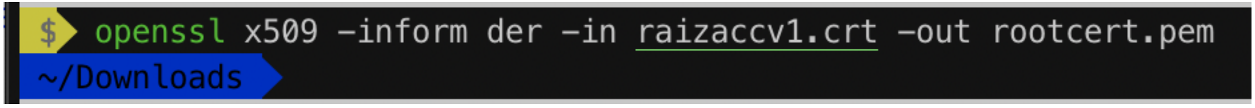
Search function with -----END CERTIFICATE-----

8. I found exactly one line with “Issuers”, suspecting this is the root certificate

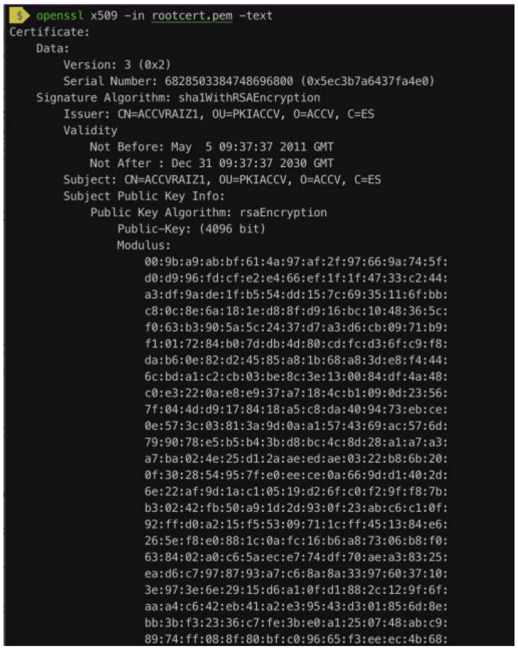


```
$ cat cert.pem | grep "Issuers"
                CA Issuers - URI:http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt
```

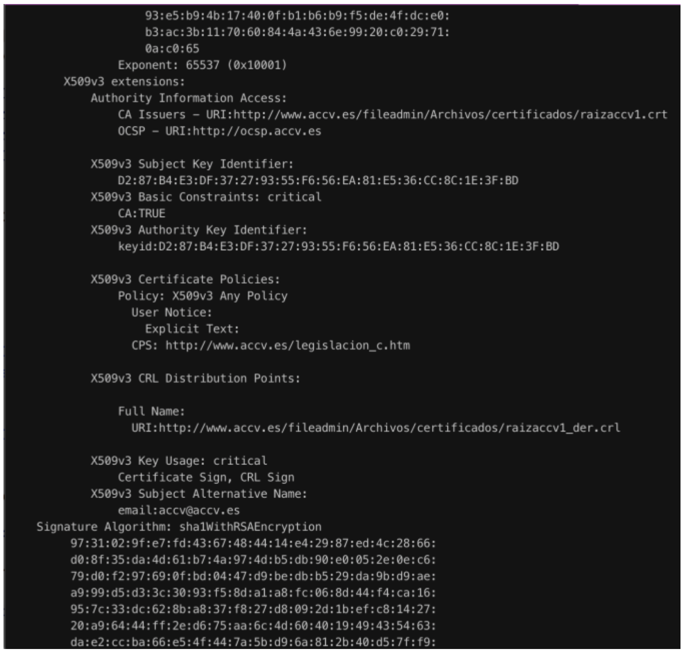
Then I convert the crt to pem



```
$ openssl x509 -inform der -in raizaccv1.crt -out rootcert.pem
~/Downloads
```



```
$ openssl x509 -in rootcert.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 6828503384748696800 (0x5ec3b7a6437fa4e0)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES
        Validity
            Not Before: May  5 09:37:37 2011 GMT
            Not After : Dec 31 09:37:37 2030 GMT
        Subject: CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:9b:a9:ab:bf:61:4a:97:af:2f:97:66:9a:74:5f:
                    d0:d9:96:fd:cf:e2:e4:66:ef:1f:1f:47:33:c2:44:
                    a3:df:9a:de:1f:b5:54:dd:15:7c:69:35:11:6f:bb:
                    c8:0c:8e:6a:18:1e:d8:8f:d9:16:bc:10:48:36:5c:
                    f0:63:b3:90:5a:5c:24:37:d7:a3:d6:cb:09:71:b9:
                    f1:01:72:84:b0:7d:db:4d:80:cd:fc:d3:6f:c9:f8:
                    da:b6:0e:82:d2:45:85:a8:1b:68:a8:3d:e8:f4:44:
                    6c:bd:a1:c2:cb:03:be:8c:3e:13:00:84:df:4a:48:
                    c0:e3:22:0a:e8:e9:37:a7:18:4c:b1:09:0d:23:56:
                    7f:04:4d:d9:17:84:18:a5:c8:da:40:94:73:eb:ce:
                    0e:57:3c:03:81:3a:9d:0a:a1:57:43:69:ac:57:6d:
                    79:90:78:e5:b5:b4:3b:d8:bc:4c:8d:28:a1:a7:a3:
                    a7:ba:02:4e:25:d1:2a:ae:ed:ae:03:22:b8:6b:20:
                    0f:30:28:54:95:7f:e0:ee:ce:0a:66:9d:d1:40:2d:
                    6e:22:af:9d:1a:c1:05:19:d2:6f:c0:f2:9f:f8:7b:
                    b3:02:42:fb:50:a9:1d:2d:93:0f:23:ab:c6:c1:0f:
                    92:ff:d0:a2:15:f5:53:09:71:1c:ff:45:13:84:e6:
                    26:5e:f8:e0:88:1c:0a:fc:16:b6:a8:73:06:b8:f0:
                    63:84:02:a0:c6:5a:ec:e7:74:df:70:ae:a3:83:25:
                    ea:d6:c7:97:87:93:a7:c6:8a:8a:33:97:60:37:10:
                    3e:97:3e:6e:29:15:d6:a1:0f:d1:88:2c:12:9f:6f:
                    aa:a4:c6:42:eb:41:a2:e3:95:43:d3:01:85:6d:8e:
                    bb:3b:f3:23:36:c7:fe:3b:e0:a1:25:07:48:ab:c9:
                    89:74:ff:08:8f:80:bf:c0:96:65:f3:ee:ec:4b:68:
```



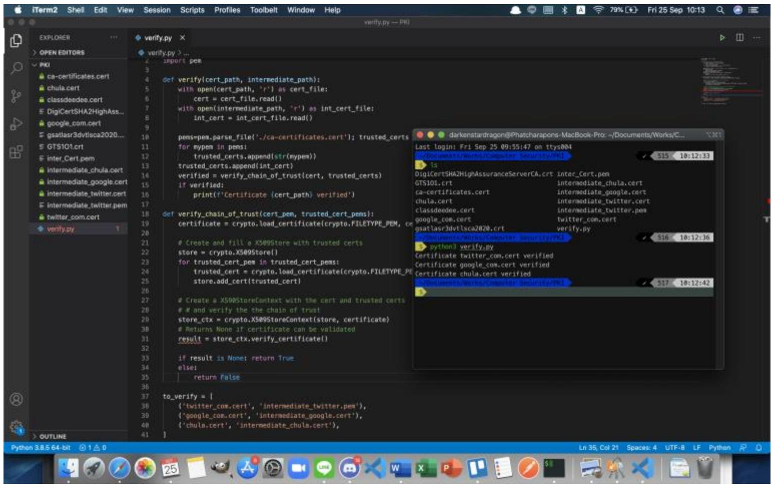
```
                    93:e5:b9:4b:17:40:0f:b1:b6:b9:f5:de:4f:dc:e0:
                    b3:ac:3b:11:70:60:84:4a:43:6e:99:20:c0:29:71:
                    0a:c0:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt
                OCSP - URI:http://ocsp.accv.es

            X509v3 Subject Key Identifier:
                D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:
                keyid:D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD

            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  User Notice:
                    Explicit Text:
                  CPS: http://www.accv.es/legislacion_c.htm

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Alternative Name:
                email:accv@accv.es
    Signature Algorithm: sha1WithRSAEncryption
         97:31:02:9f:e7:fd:43:67:48:44:14:e4:29:87:ed:4c:28:66:
         d0:8f:35:da:4d:61:b7:4a:97:4d:b5:db:90:e0:05:2e:0e:c6:
         79:d0:f2:97:69:0f:bd:04:47:d9:be:db:b5:29:da:9b:d9:ae:
         a9:99:d5:d3:3c:30:93:f5:8d:a1:a8:fc:06:8d:44:f4:ca:16:
         95:7c:33:dc:62:8b:a8:37:f8:27:d8:09:2d:1b:ef:c8:14:27:
         20:a9:64:44:ff:2e:d6:75:aa:6c:4d:60:40:19:49:43:54:63:
         da:e2:cc:ba:66:e5:4f:44:7a:5b:d9:6a:81:2b:40:d5:7f:f9:
```

Comparing to twitter’s certificate,

- This one has much longer valid duration (up until 2030) and
- Is issued by another company. In fact this certificate signed by itself as the issuer and the subject is the same organization.
- Has 4096 bit public key

9. (Already has .pem readable file)

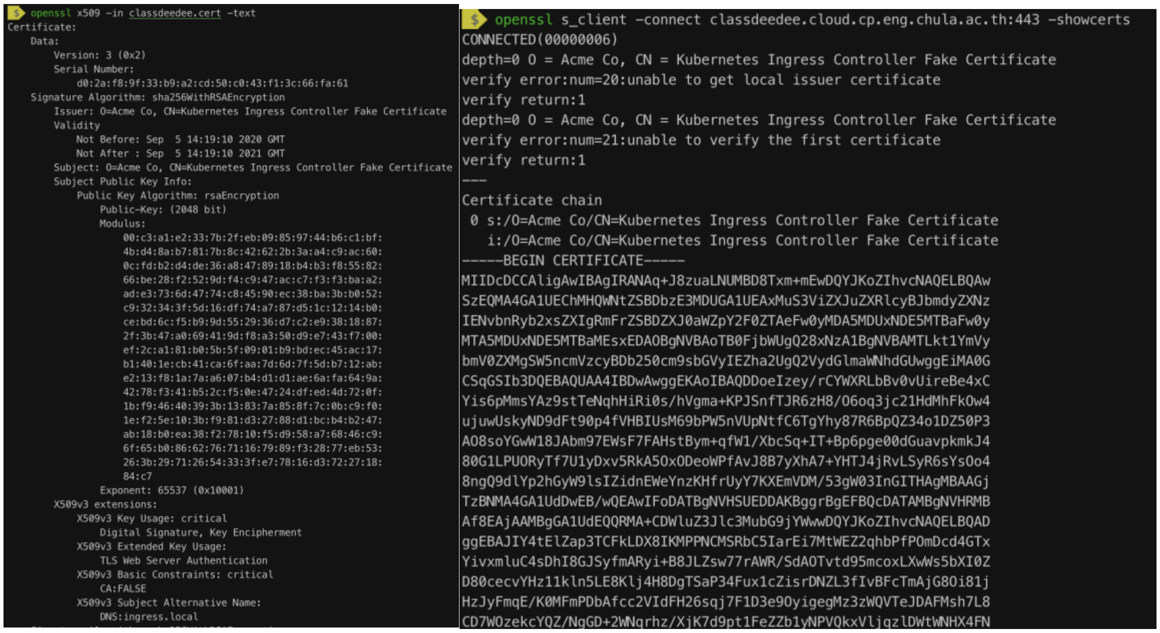
10. twitter.com, google.com, and chula.ac.th all can be verified with this program. Though classdeedee has no intermidate certificate and yields verify error result when trying to connect to it with option -showcerts



```python
import pem

def verify(cert_path, intermediate_path):
    with open(cert_path, 'r') as cert_file:
        cert = cert_file.read()
    with open(intermediate_path, 'r') as int_cert_file:
        int_cert = int_cert_file.read()

    pems=pem.parse_file('./ca-certificates.cert'); trusted_certs
    for mypem in pems:
        trusted_certs.append(str(mypem))
    trusted_certs.append(int_cert)
    verified = verify_chain_of_trust(cert, trusted_certs)
    if verified:
        print(f'Certificate {cert_path} verified')

def verify_chain_of_trust(cert_pem, trusted_cert_pems):
    certificate = crypto.load_certificate(crypto.FILETYPE_PEM, ce

    # Create and fill a X509Store with trusted certs
    store = crypto.X509Store()
    for trusted_cert_pem in trusted_cert_pems:
        trusted_cert = crypto.load_certificate(crypto.FILETYPE_PE
        store.add_cert(trusted_cert)

    # Create a X509StoreContext with the cert and trusted certs
    # # and verify the the chain of trust
    store_ctx = crypto.X509StoreContext(store, certificate)
    # Returns None if certificate can be validated
    result = store_ctx.verify_certificate()

    if result is None: return True
    else:
        return False

to_verify = [
    ('twitter_com.cert', 'intermediate_twitter.pem'),
    ('google_com.cert', 'intermediate_google.cert'),
    ('chula.cert', 'intermediate_chula.cert'),
]
```

```
darkenstardragon@Phatcharapons-MacBook-Pro: ~/Documents/Works/C...
Last login: Fri Sep 25 09:55:47 on ttys004
~/Documents/Works/Computer Security/PKI                    ✓  515  10:12:33
$ ls
DigiCertSHA2HighAssuranceServerCA.crt inter_Cert.pem
GTS1O1.crt                            intermediate_chula.cert
ca-certificates.cert                  intermediate_google.cert
chula.cert                            intermediate_twitter.cert
classdeedee.cert                      intermediate_twitter.pem
google_com.cert                       twitter_com.cert
gsatlasr3dvtlsca2020.crt              verify.py
~/Documents/Works/Computer Security/PKI                    ✓  516  10:12:36
$ python3 verify.py
Certificate twitter_com.cert verified
Certificate google_com.cert verified
Certificate chula.cert verified
~/Documents/Works/Computer Security/PKI                    ✓  517  10:12:42
$
```

Twitter, google, and chula verified



```
$ openssl x509 -in classdeedee.cert -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d0:2a:f8:9f:33:b9:a2:cd:50:c0:43:f1:3c:66:fa:61
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=Acme Co, CN=Kubernetes Ingress Controller Fake Certificate
        Validity
            Not Before: Sep  5 14:19:10 2020 GMT
            Not After : Sep  5 14:19:10 2021 GMT
        Subject: O=Acme Co, CN=Kubernetes Ingress Controller Fake Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c3:a1:e2:33:7b:2f:eb:09:85:97:44:b6:c1:bf:
                    4b:d4:8a:b7:81:7b:8c:42:62:2b:3a:a4:c9:ac:60:
                    0c:fd:b2:d4:de:36:a8:47:89:18:b4:b3:f8:55:82:
                    66:be:28:f2:52:9d:f4:c9:47:ac:c7:f3:f3:ba:a2:
                    ad:e3:73:6d:47:74:c8:45:90:ec:38:ba:3b:b0:52:
                    c9:32:34:3f:5d:16:df:74:a7:87:d5:1c:12:14:b0:
                    ce:bd:6c:f5:b9:9d:55:29:36:d7:c2:e9:38:18:87:
                    2f:3b:47:a0:69:41:9d:f8:a3:50:d9:e7:43:f7:00:
                    ef:2c:a1:81:b0:5b:5f:09:01:b9:bd:ec:45:ac:17:
                    b1:40:1e:cb:41:ca:6f:aa:7d:6d:7f:5d:b7:12:ab:
                    e2:13:f8:1a:7a:a6:07:b4:d1:d1:ae:6a:fa:64:9a:
                    42:78:f3:41:b5:2c:f5:0e:47:24:df:ed:4d:72:0f:
                    1b:f9:46:40:39:3b:13:83:7a:85:8f:7c:0b:c9:f0:
                    1e:f2:5e:10:3b:f9:81:d3:27:88:d1:bc:b4:b2:47:
                    ab:18:b0:ea:38:f2:78:10:f5:d9:58:a7:68:46:c9:
                    6f:65:b0:86:62:76:71:16:79:89:f3:28:77:eb:53:
                    26:3b:29:71:26:54:33:3f:e7:78:16:d3:72:27:18:
                    84:c7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Alternative Name:
                DNS:ingress.local
```

```
$ openssl s_client -connect classdeedee.cloud.cp.eng.chula.ac.th:443 -showcerts
CONNECTED(00000006)
depth=0 O = Acme Co, CN = Kubernetes Ingress Controller Fake Certificate
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 O = Acme Co, CN = Kubernetes Ingress Controller Fake Certificate
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/O=Acme Co/CN=Kubernetes Ingress Controller Fake Certificate
   i:/O=Acme Co/CN=Kubernetes Ingress Controller Fake Certificate
-----BEGIN CERTIFICATE-----
MIIDcDCCAligAwIBAgIRANAq+J8zuaLNUMBD8Txm+mEwDQYJKoZIhvcNAQELBQAw
SzEQMA4GA1UEChMHQWNtZSBDbzE3MDUGA1UEAxMuS3ViZXJuZXRlcyBJbmdyZXNz
IENvbnRyb2xsZXIgRmFrZSBDZXJ0aWZpY2F0ZTAeFw0yMDA5MDUxNDE5MTBaFw0y
MTA5MDUxNDE5MTBaMEsxEDAOBgNVBAoTB0FjbWUgQ28xNzA1BgNVBAMTLkt1YmVy
bmV0ZXMgSW5ncmVzcyBDb250cm9sbGVyIEZha2UgQ2VydGlmaWNhdGUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDDoeIzey/rCYWXRLbBv0vUireBe4xC
Yis6pMmsYAz9stTeNqhHiRi0s/hVgma+KPJSnfTJR6zH8/O6oq3jc21HdMhFkOw4
ujuwUskyND9dFt90p4fVHBIUsM69bPW5nVUpNtfC6TgYhy87R6BpQZ34o1DZ50P3
AO8soYGwW18JAbm97EWsF7FAHstBym+qfW1/XbcSq+IT+Bp6pge00dGuavpkmkJ4
80G1LPUORyTf7U1yDxv5RkA5OxODeoWPfAvJ8B7yXhA7+YHTJ4jRvLSyR6sYsOo4
8ngQ9dlYp2hGyW9lsIZidnEWeYnzKHfrUyY7KXEmVDM/53gW03InGITHAgMBAAGj
TzBNMA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMB
Af8EAjAAMBgGA1UdEQQRMA+CDWluZ3Jlc3MubG9jYWwwDQYJKoZIhvcNAQELBQAD
ggEBAJIY4tElZap3TCFkLDX8IKMPPNCMSRbC5IarEi7MtWEZ2qhbPfPOmDcd4GTx
YivxmluC4sDhI8GJSyfmARyi+B8JLZsw77rAWR/SdAOTvtd95mcoxLXwWs5bXI0Z
D80cecvYHz11kln5LE8Klj4H8DgTSaP34Fux1cZisrDNZL3fIvBFcTmAjG8Oi81j
HzJyFmqE/K0MFmPDbAfcc2VIdFH26sqj7F1D3e9OyigegMz3zWQVTeJDAFMsh7L8
CD7WOzekcYQZ/NgGD+2WNqrhz/XjK7d9pt1FeZZb1yNPVQkxVljqzlDWtWNHX4FN
```

No intermidiate certificate URI (left) and verifiying failed (right)

11.

Class 1 Certificate

Assurance Level: Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.
Applicability: This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance.

Class 3 Certificate

Assurance Level: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.
Applicability: This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

Conclusion: Class 1 is more of a basic certificate with easier process of getting approved, while class 3 is more complicated but also provide more ensurance of the trustworthiness of the website.

Source: https://www.e-mudhra.com/Class-of-certificates.html

12. The attacker could impersonate to be one of the so-called trusted Root CA, granting a reliable certificate to their own malicious websites and still showing the safety of certificate in the browser as if nothing happened. If the hacker created a fake, malicious banking websites, this could lead to a huge lose for the banks themselves as well as the users.

CRL (Certificate revocation list) isn't reliable enough in this case as there is no certificate being revoked. All the attacker need to do is to create a fake certificate for their own websites. As the problem said, no one knows about this breach so there is no way the real CA will put the fake certificate in the CRLs as well.

Source about CRL: https://searchsecurity.techtarget.com/definition/Certificate-Revocation-List

OSCP (Online Certificate Status Protocol) while is an optimized version of CRL by letting the user connect directly to Cas to ask for the revocation status of the certificate, still can't check if the target Root CA has been hacked, as the fake certificate is still there and still not being revoked.

Source about OCSP:
https://docs.microfocus.com/NNMi/10.30/Content/Administer/NNMi_Deployment/Advanced_Configurations/Cert_Validation_CRL_and_OCSP.htm