

1&2. MacOS user. No difference.

3. Run the **openssl x509 -in twitter\_com.cert -text** command

```
SysSecurity — openssl s_client -connect twitter.com 443 -CApath — 112x32
wleelaket@warits-MacBook-Air SysSecurity % openssl x509 -in twitter_com.cert -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      05:a8:5f:e7:ec:a0:fc:c8:37:a1:2c:57:37:41:82:68
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
    Validity
      Not Before: Dec 25 00:00:00 2022 GMT
      Not After : Dec 25 23:59:59 2023 GMT
    Subject: C=US, ST=California, L=San Francisco, O=Twitter, Inc., CN=twitter.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:a8:e1:44:5a:8a:35:40:e5:6c:fa:9f:d3:9e:80:
        21:1e:7b:fc:ea:20:e2:b2:fc:ac:24:dd:d4:fc:67:
        b2:c2:50:cc:4f:f5:57:fb:79:00:e1:b2:dd:a9:be:
        83:2b:62:61:f3:8b:04:a2:77:01:37:a2:7b:cc:59:
        f0:62:b8:70:28:17:09:ea:00:82:c7:8b:e3:e8:c3:
        3a:c6:3e:4f:66:79:f8:2a:b4:3f:9a:59:4d:c5:dc:
        58:92:1a:24:b0:94:18:c0:b8:60:f6:3c:55:14:8c:
        b5:c0:f2:dd:70:bc:f7:d2:44:e5:90:51:c3:71:cb:
        e6:85:e6:d3:18:75:04:31:f4:0e:a1:77:3a:8f:56:
        42:e4:f3:b0:d6:20:15:75:95:03:5c:b8:eb:75:96:
        49:7b:a2:50:79:b2:e2:50:f4:5f:74:00:c3:97:48:
        61:1c:dc:2b:bc:5e:e9:70:7a:b5:84:f4:09:2e:15:
        31:50:0d:67:c9:58:ff:92:e1:ba:90:ec:9d:7e:c4:
        72:2a:d1:28:bc:1f:1c:23:6c:87:82:5e:e7:41:3c:
        9b:16:6b:d4:9a:27:ee:7b:81:8e:d8:63:eb:59:6a:
        f9:ba:57:3c:44:04:2f:8c:1c:34:a4:f2:a7:2c:44:
```

```
SysSecurity — openssl s_client -connect twitter.com 443 -CApath — 112x32
X509v3 extensions:
  X509v3 Authority Key Identifier:
    keyid:B7:6B:A2:EA:A8:AA:84:8C:79:EA:B4:DA:0F:98:B2:C5:95:76:B9:F4

  X509v3 Subject Key Identifier:
    93:6A:23:9D:DC:83:0E:3B:3D:E8:BF:55:5E:E0:AC:99:FB:42:01:A1
  X509v3 Subject Alternative Name:
    DNS:twitter.com, DNS:www.twitter.com
  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/DigiCertTLRSASHA2562020CA1-4.crl

    Full Name:
      URI:http://crl4.digicert.com/DigiCertTLRSASHA2562020CA1-4.crl

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

  Authority Information Access:
    OCSP - URI:http://ocsp.digicert.com
    CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLRSASHA2562020CA1-1.crt

  X509v3 Basic Constraints:
    CA:FALSE
  1.3.6.1.4.1.11129.2.4.2:
    ...j.h.v.>.>..52.W(..k.....k..i.w}m..n....GU,X....G0E. P..0A...].x..-...
```

```
SysSecurity — openssl s_client -connect twitter.com 443 -CApath — 112x32

X509v3 Basic Constraints:
    CA:FALSE
1.3.6.1.4.1.11129.2.4.2:
    ...j.h.v.>...52.W(..k.....k..i.w}m..n....GU,X....G0E. P..0A...].x..-...
r.V..T...If/L...!...&...Y.ga.%...&...Yf...4....Ee.v..sw...P.c.....Jy-.g.....y6.....GU,.....G0E. H...1....R
P.d.Lx+l.|<.....o...!.....Gcb0Lz.1...t`.b....p".!;:v..>$.M.u.9..X.l].B.z.5....%.....GU,.....G0E. ..
7..eP..=...#.2.w_F=...b..4.r...j...@J..4M7.
    Signature Algorithm: sha256WithRSAEncryption
    9e:6f:ef:78:51:30:6d:b7:ae:35:1b:95:5b:d7:97:1b:5f:bb:
    f8:8f:32:fd:2f:82:98:3e:61:03:7e:3d:3f:62:3a:dd:41:e0:
    11:cf:1c:ea:53:5c:30:52:9f:e8:21:33:15:ac:d6:75:cd:3d:
    d1:c9:d1:47:be:13:a8:86:d9:87:a4:03:5e:9d:6d:40:3e:1c:
    9c:e5:76:29:df:36:c9:75:68:87:1a:7e:ca:e6:e6:ef:d4:f6:
    98:a4:4d:9b:93:00:25:11:c9:df:ac:52:cd:bc:6f:09:78:1e:
    f1:41:26:a2:a0:72:0c:be:17:48:83:2e:0d:9e:e6:f4:51:e4:
    7d:41:4e:dc:3a:c3:07:2b:a3:e6:de:1e:d0:8f:d0:41:de:7f:
    be:5c:0c:bf:d8:07:a2:5e:d7:65:be:72:ef:69:65:f6:57:87:
    5d:5b:a8:a1:b3:77:29:c3:89:e6:a5:e0:95:a7:2b:17:98:6a:
    64:ff:fa:b1:49:d2:d4:6a:00:9d:b6:3e:67:3f:a6:ad:35:cd:
    b3:df:36:a9:3a:8e:3e:21:5b:a6:d2:c8:e7:f8:1f:c0:05:f4:
    4a:e4:d7:7e:a4:be:bc:0b:c6:81:16:ee:88:8a:bf:cf:53:5f:
    6f:04:18:72:6e:55:6b:df:2e:5a:57:48:bf:34:b1:fa:9f:05:
    48:8d:a6:8b
-----BEGIN CERTIFICATE-----
MIIGvzCCBaegAwIBAgIQBahf5+yg/Mg3oSxXN0GCaDANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJlVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMSKwJyYDVQQDEyBE
aWdpQ2V2dCBUTFMglUNBIFNIQTl1NiAyMDIwIENBMTAeFw0yMjUwMDAwMDBa
Fw0yMzEyMjUyMDU5NT1aMGgxChZAJBgNVBAYTA1VTMRMwEQYDVQVQIEwpDYWxpZm9y
bm1hMRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRYwFAYDVQQKEw1Ud2l0dGVyL0CBJ
bmMuMRQwEgYDVQQDEwt0d2l0dGVyLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKjhrFqKNUdlbPqf056AIR57/Oog4rL8rCTd1PxnssJQzE/1V/t5
A0Gy3am+gytiYf0LBKJ3ATeie8xZ8GK4cGgXCeoAgseL4+jD0sY+T2Z5+Cq0P5pZ
```

```
SysSecurity — openssl s_client -connect twitter.com 443 -CApath — 112x32

ADCCAQoCggEBAKjhrFqKNUdlbPqf056AIR57/Oog4rL8rCTd1PxnssJQzE/1V/t5
A0Gy3am+gytiYf0LBKJ3ATeie8xZ8GK4cGgXCeoAgseL4+jD0sY+T2Z5+Cq0P5pZ
TcXcWJiaJLCUGMC4YPY8VRSmtcDy3XC899JE5ZBRw3HL5oXm0xh1BDH0DqF30o9W
QuTzsnYgFXWVA1y463WWSXuIUHmy41D0X3QAw5dIYRzcK7xe6XB6tYT0CS4VMVAN
Z81Y/5LhupDsnX7EcirRKLwrfHCNsh4Je50E8mxZr1J0n7nuBjthj16ll+bpXPEQE
L4wcNKTPypxEOq/LG4WcZ6rQMAsjY21CKcMCAwEAa0CA3wwggN4MB8GA1UdIwQY
MBaAFldrouqoqoSMeeq02g+YsswVdrn0MB0GA1UdDgQWBBSSTa10d3IM00z3ov1Ve
4KyZ+0IBoTAnBgNVHREIEIDAeggt0d2l0dGVyLmNvbYIPd3d3LnR3aXR0ZXIuY29t
MA4GA1UdDwEB/wQEAwIFoDABGgNVHSEUfjAUBggrBgEFBQcDAQYIKwYBBQUHAWIw
gY8GA1UdHwSBhZCBhDBAoD6gPIY6aHR0cDovL2NybDMuZGlnaWNlcnQuY29tL0R0
Z2l0dXJ0VExTU1NB0hBMjU2MjAyMENBMS00LmNybDBAoD6gPIY6aHR0cDovL2Ny
bDQwZGlnaWNlcnQuY29tL0R0Z2l0dXJ0VExTU1NB0hBMjU2MjAyMENBMS00LmNy
bDA+BgNVHSAENzA1MDMGbmeBDAECAjApMCCGCCsGAQUFBwIBFhtodHRwOi8vd3d3
LmR0Z2l0dXJ0LmNvbS9DUFMwfwYIKwYBBQUHAQEeczBxMCQGCCCsGAQUFBzABhhho
dHRwOi8vb2Nzc5kaWdpY2VydC5jb20wSQYIKwYBBQUHMAKGPWh0dHA6Ly9jYWN1
cnRzLmR0Z2l0dXJ0LmNvbS9EaWdpQ2VydFRMU1JTQVNIQTl1NjIwMjU2MjU2MjU2
cnQwCQYDVDR0TBAIwADCCAX4GCisGAQQB1nkCBAIEggFuBIIBagFoAHYA6D7Q2j71
BjYU51covI1ryQPTY9ERa+zraef3fW0GvW4AAAGFR1UsWAAABAMARzBFAiBQre4w
QaXxjF39eMm+LRELlpgy+Vaa/1S13xBJZi9M9QIhAJCbji6X1uRZ2Gdh/iX1IRUm
2wG8WwAPwu806scXu0V1AHYAs3N3B+GEUPhJhtYFqdwRCUp5LbFnDAuH3PADdnk2
pZoAAAGFR1UsuQAABAMARzBFAiBICcX/bAgJBESVUK1ko0x4K2zcFdydtbFvZOK
jG8ZuWIhAN8TpKrnBeK4R2NiT2x63jGTsxN0YIdiH/LkhnaIBDo7AHYA777JN+c
Tbp18jnfUlj0bf38Qs96nzXEnh0JgSXttJkAAAGFR1UshgAABAMARzBFAiAS1jek
HmVQ0YA9iQeJI9My/HfGJu6bxjg6pJ2FWF3bQIhALf6B+cEATRN9QNX0Y9jg/9
YpYNNBpyjr8favIM70BKMA0GCSqGSIb3DQEBBCwAA4IBAQCeb+94UTBtt641G5Vb
15cbX7v4jzL9L4KYPmEdfj0/YjrdQeARzxzqU1wwUp/oITMVRNZ1zT3RydFvH0o
htmHpAnenWlAPhyc5Xyp3zbJdWiHGn7K5ubv1PaYpE2bkwA1EcnfrFLNvG8Jeb7x
QSai0HIMvhdIgy4Nnub0Ue9R9QU7c0sMHK6Pm3h7Qj9BB3n++XAY/2AeixtdlnLv
aWX2V4ddW6hs3cpw4nmpeCVpysXm0pk//qxSdLUagCdtj5nP6atNc2z3zap0o4+
IVum0sjn+B/ABFRK5Nd+pL68C8aBFu6Iir/PU19vBBhyblVr3y5aV0i/NLH6nwVI
jaal
-----END CERTIFICATE-----
```

Version: Version of the certificate.

V3

Serial Number: Unique identifier number issue by CA.

05:a8:5f:e7:ec:a0:fc:c8:37:a1:2c:57:37:41:82:68

Issuer: Information of CA who issued this certificate.

C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1

Validity: Valid period of this certificate.

Not Before: Dec 25 00:00:00 2022 GMT

Not After : Dec 25 23:59:59 2023 GMT

Subject: The owner of this certificate.

C=US, ST=California, L=San Francisco, O=Twitter, Inc., CN=twitter.com

Public Key: Public key of the owner of this certificate.

Algorithm Signature: The algorithm that being use to sign this certificate.

Digital Signature: The signature of this certificate.

4. From the information in exercise 3, is there an intermediate certificate? If yes, what purpose does it serve?

: Yes, There is an intermediate CA issued by root CA.

The purpose of intermediate CA is to make sure that it authorized by the root CA and to establish a trust chain between the root CA and the end-entity certificate.

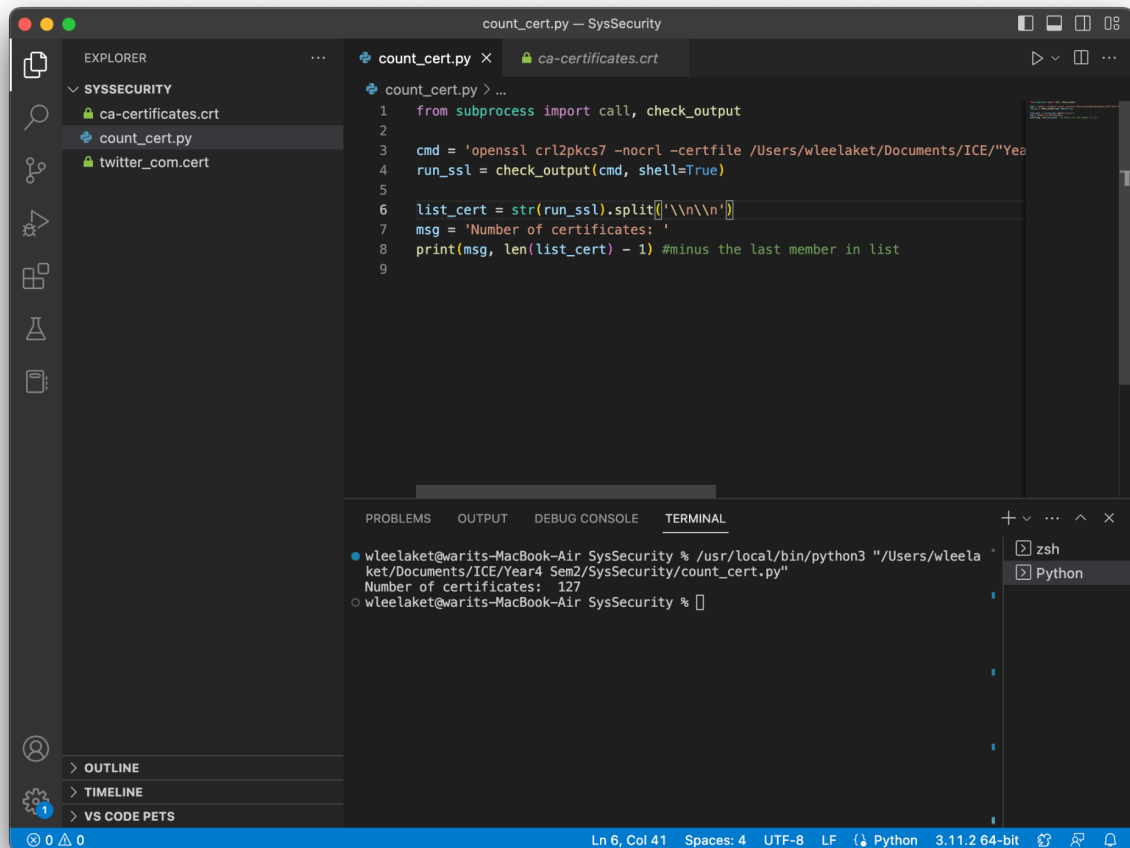
5. Is there an intermediate CA, i.e. is there more than one organization involved in the certification? Say why you think so.

: Yes, the intermediate CA and root CA could come from the different organization. The only important thing is that the the certificated is issued only by the trust root CA.

6. What is the role of ca-certificates.crt?

: The ca-certificates.crt file is a bundle of trusted root CA certificates used by various application and operating systems to authenticate the digital signature whether it is being signed by one of the trust root CA stored in ca-certificates.crt file.

7. Explore the ca-certificates.crt. How many certificates are in there? Give the command/method you have used to count.



```
count_cert.py -- SysSecurity
EXPLORER
  SYSSECURITY
    ca-certificates.crt
    count_cert.py
    twitter_com.crt
count_cert.py
1 from subprocess import call, check_output
2
3 cmd = 'openssl crl2pkcs7 -nocrl -certfile /Users/wleelaket/Documents/ICE/"Yea
4 run_ssl = check_output(cmd, shell=True)
5
6 list_cert = str(run_ssl).split('\n\n')
7 msg = 'Number of certificates: '
8 print(msg, len(list_cert) - 1) #minus the last member in list
9
TERMINAL
wleelaket@warits-MacBook-Air SysSecurity % /usr/local/bin/python3 "/Users/wleela
ket/Documents/ICE/Year4 Sem2/SysSecurity/count_cert.py"
Number of certificates: 127
wleelaket@warits-MacBook-Air SysSecurity %
```

: There are 127 certificates in ca-certificates.crt.

8. Extract a root certificate from ca-certificates.crt. Use the openssl command to explore the details. Do you see any Issuer information? Please compare it to details of twitter's certificate and the details of the intermediate certificate.

```
subject=/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
issuer=/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
```

```
subject=/C=US/ST=California/L=San Francisco/O=Twitter, Inc./CN=twitter.com
issuer=/C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
```

The issuer of root cert and twitter's cert are both DigiCert.

9. Skip

10. From the given python code,1 implement the certificate validation.

```
41  #twitter certs
42  twitter_cert = './twitter.com.cer'
43  int_twt_cert = './intermediate_twt.cer'
44  print('\nVerify twitter certs: ')
45  verify(twitter_cert, int_twt_cert)
46
47  #google certs
48  google_cert = './google.com.cer'
49  int_google_cert = './intermediate_google.cer'
50  print('\nVerify google certs: ')
51  verify(google_cert, int_google_cert)
52
53  # #cu certs
54  chula_cert = './chula.ac.th.cer'
55  int_cu_cert = './intermediate_cu.cer'
56  print('\nVerify chula.ac.th certs: ')
57  verify(chula_cert, int_cu_cert)
58
59  #ClassDeeDee certs
60  cdd_cert = './classdeedee.cer'
61  int_cdd_cert = './intermediate_cdd.cer'
62  print('\nVerify classdeedee certs: ')
63  verify(cdd_cert, int_cdd_cert)
64
```

● wleelaket@warits-MacBook-Air SysSecurity % /usr/loca

Verify twitter certs:  
Certificate verified

Verify google certs:  
Certificate verified

Verify chula.ac.th certs:  
Certificate verified

Verify classdeedee certs:  
Certificate verified