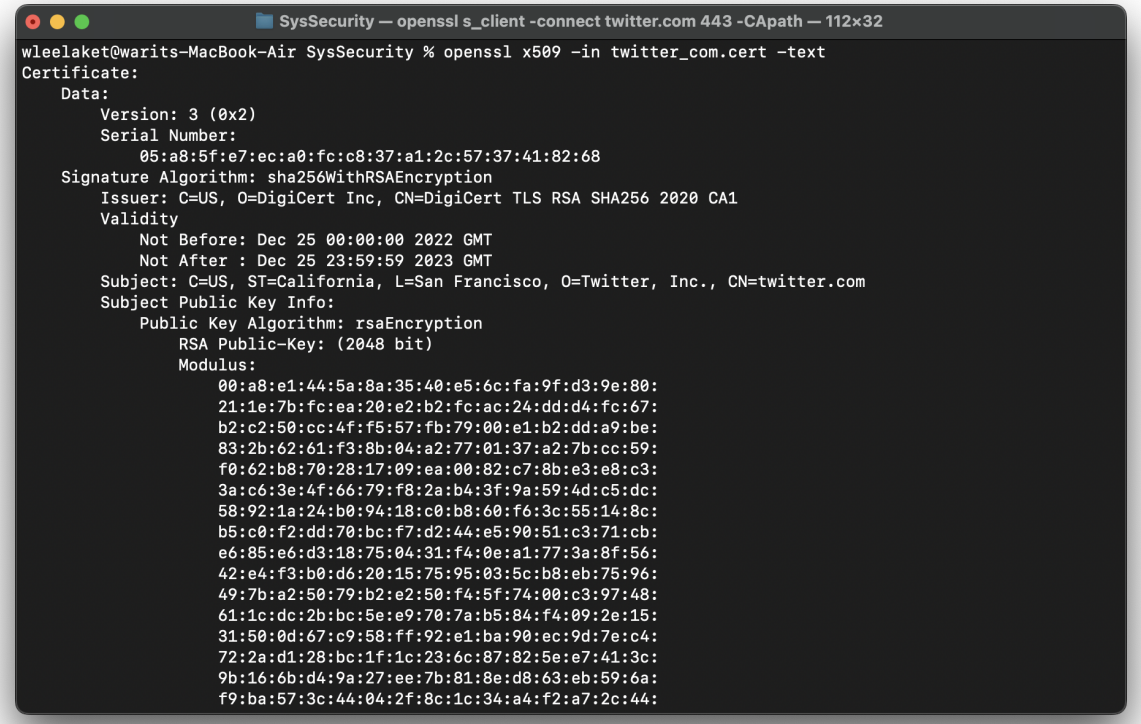
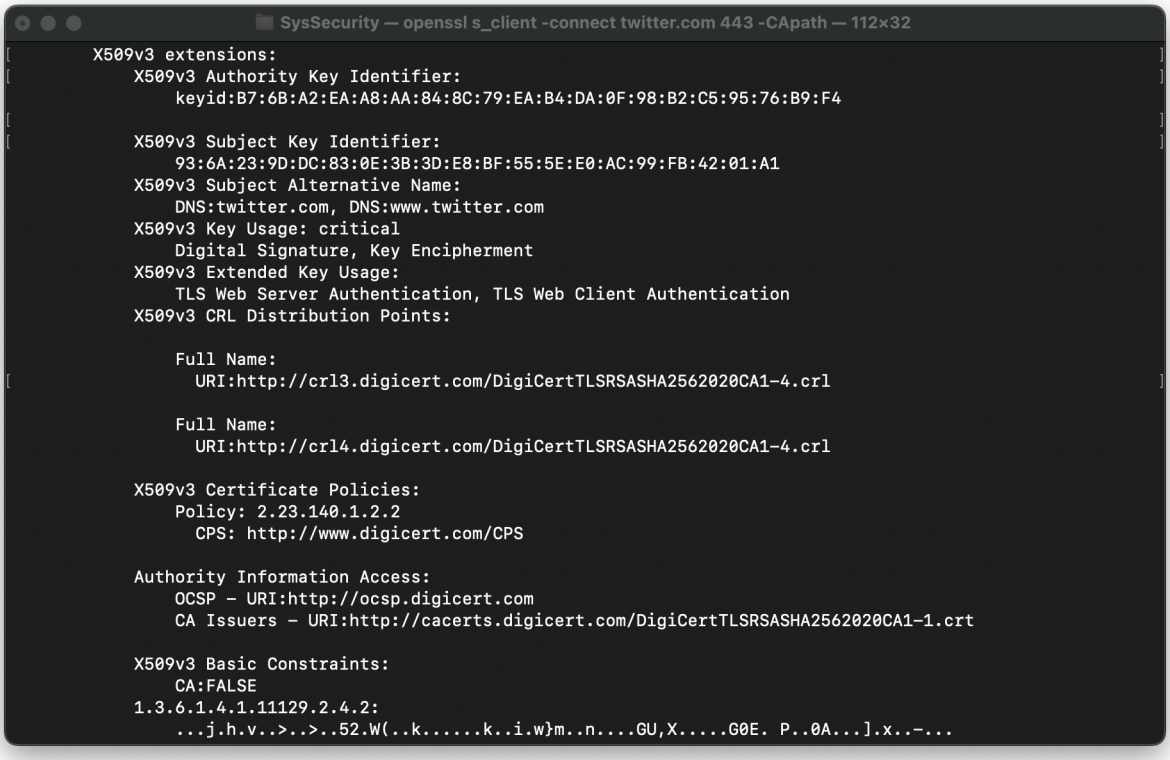
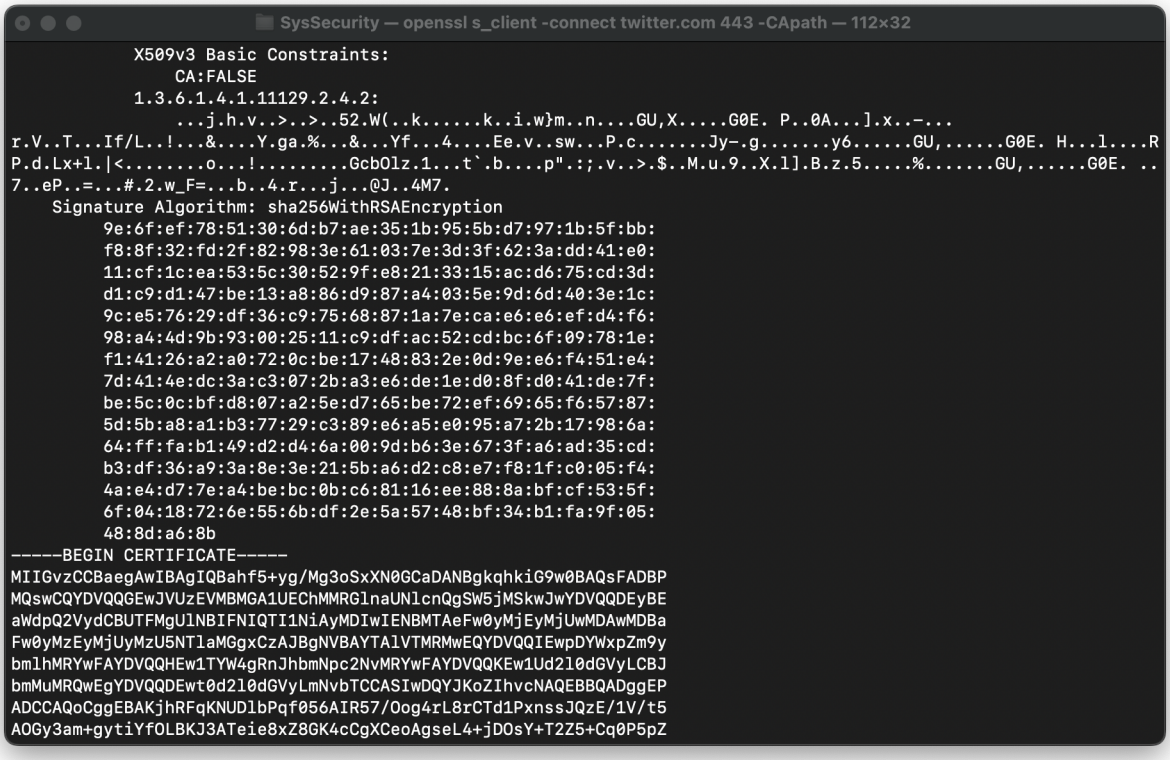
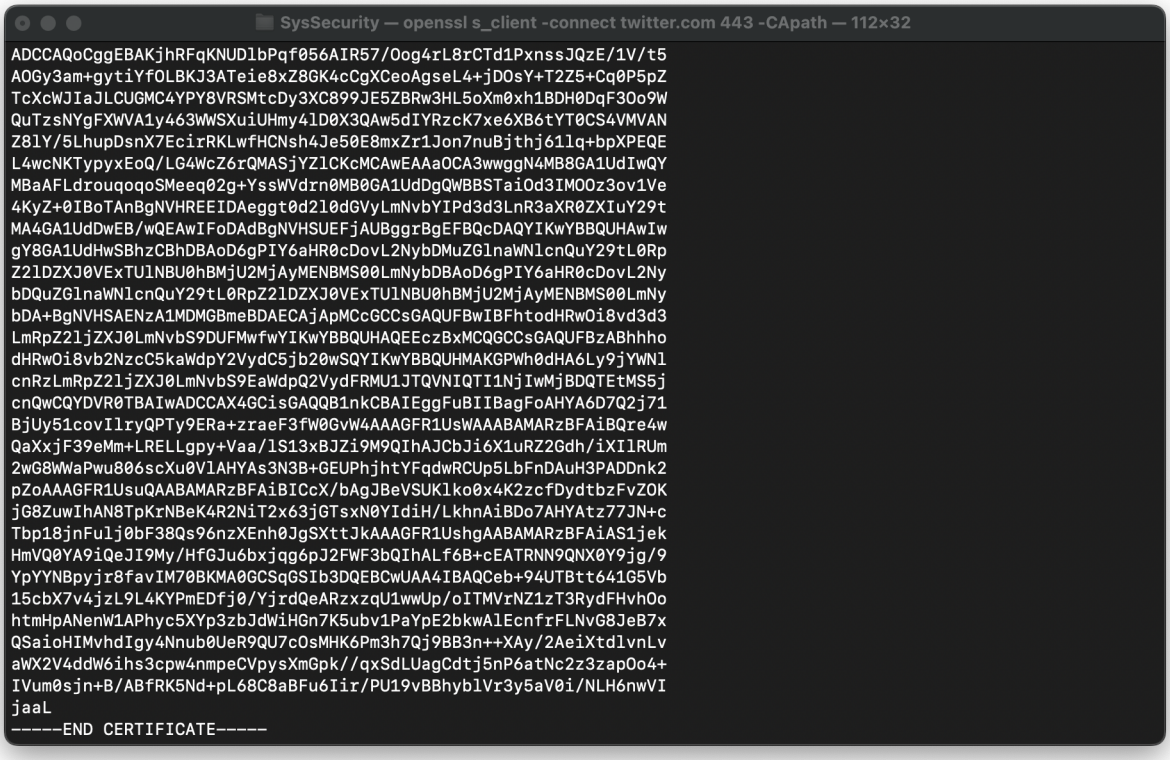
1&2. MacOS user. No difference.

3. Run the **openssl x509 -in twitter_com.cert -text** command






SysSecurity — openssl s_client -connect twitter.com 443 -CApath — 112×32
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...l....R
P.d.Lx+l.|<........o...!.........GcbOlz.1...t`.b....p".:;.v..>.$..M.u.9..X.1].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
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMjEyMjUwMDAwMDBa
Fw0yMzEyMjUyMzU5NTlaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9y
bmlhMRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRYwFAYDVQQKEw1Ud2l0dGVyLCBJ
bmMuMRQwEgYDVQQDEwt0d2l0dGVyLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKjhRFqKNUDlbPqf056AIR57/Oog4rL8rCTd1PxnssJQzE/1V/t5
AOGy3am+gytiYfOLBKJ3ATeie8xZ8GK4cCgXCeoAgseL4+jDOsY+T2Z5+Cq0P5pZ


SysSecurity — openssl s_client -connect twitter.com 443 -CApath — 112×32
ADCCAQoCggEBAKjhRFqKNUDlbPqf056AIR57/Oog4rL8rCTd1PxnssJQzE/1V/t5
AOGy3am+gytiYfOLBKJ3ATeie8xZ8GK4cCgXCeoAgseL4+jDOsY+T2Z5+Cq0P5pZ
TcXcWJIaJLCUGMC4YPY8VRSMtcDy3XC899JE5ZBRw3HL5oXm0xh1BDH0DqF3Oo9W
QuTzsNYgFXWVA1y463WWSXuiUHmy4lD0X3QAw5dIYRzcK7xe6XB6tYT0CS4VMVAN
Z8lY/5LhupDsnX7EcirRKLwfHCNsh4Je50E8mxZr1Jon7nuBjthj61lq+bpXPEQE
L4wcNKTypyxEoQ/LG4WcZ6rQMASjYZlCKcMCAwEAAaOCA3wwggN4MB8GA1UdIwQY
MBaAFLdrouqoqoSMeeq02g+YssWVdrn0MB0GA1UdDgQWBBSTaiOd3IMOOz3ov1Ve
4KyZ+0IBoTAnBgNVHREEIDAeggt0d2l0dGVyLmNvbYIPd3d3LnR3aXR0ZXIuY29t
MA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
gY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDovL2NybDMuZGlnaWNlcnQuY29tL0Rp
Z2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS00LmNybDBAoD6gPIY6aHR0cDovL2Ny
bDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS00LmNy
bDA+BgNVHSAENzA1MDMGBmeBDAECAjApMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3
LmRpZ2ljZXJ0LmNvbS9DUFMwfwYIKwYBBQUHAQEEczBxMCQGCCsGAQUFBzABhhho
dHRwOi8vb2NzcC5kaWdpY2VydC5jb20wSQYIKwYBBQUHMAKGPWh0dHA6Ly9jYWNl
cnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIwMjBDQTEtMS5j
cnQwCQYDVR0TBAIwADCCAX4GCisGAQQB1nkCBAIEggFuBIIBagFoAHYA6D7Q2j71
BjUy51covIlryQPTy9ERa+zraeF3fW0GvW4AAAGFR1UsWAAABAMARzBFAiBQre4w
QaXxjF39eMm+LRELLgpy+Vaa/lS13xBJZi9M9QIhAJCbJi6X1uRZ2Gdh/iXIlRUm
2wG8WWaPwu806scXu0VlAHYAs3N3B+GEUPhjhtYFqdwRCUp5LbFnDAuH3PADDnk2
pZoAAAGFR1UsuQAABAMARzBFAiBICcX/bAgJBeVSUKlko0x4K2zcfDydtbzFvZOK
jG8ZuwIhAN8TpKrNBeK4R2NiT2x63jGTsxN0YIdiH/LkhnAiBDo7AHYAtz77JN+c
Tbp18jnFulj0bF38Qs96nzXEnh0JgSXttJkAAAGFR1UshgAABAMARzBFAiAS1jek
HmVQ0YA9iQeJI9My/HfGJu6bxjqg6pJ2FWF3bQIhALf6B+cEATRNN9QNX0Y9jg/9
YpYYNBpyjr8favIM70BKMA0GCSqGSIb3DQEBCwUAA4IBAQCeb+94UTBtt641G5Vb
15cbX7v4jzL9L4KYPmEDfj0/YjrdQeARzxzqU1wwUp/oITMVrNZ1zT3RydFHvhOo
htmHpANenW1APhyc5XYp3zbJdWiHGn7K5ubv1PaYpE2bkwAlEcnfrFLNvG8JeB7x
QSaioHIMvhdIgy4Nnub0UeR9QU7cOsMHK6Pm3h7Qj9BB3n++XAy/2AeiXtdlvnLv
aWX2V4ddW6ihs3cpw4nmpeCVpysXmGpk//qxSdLUagCdtj5nP6atNc2z3zapOo4+
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.

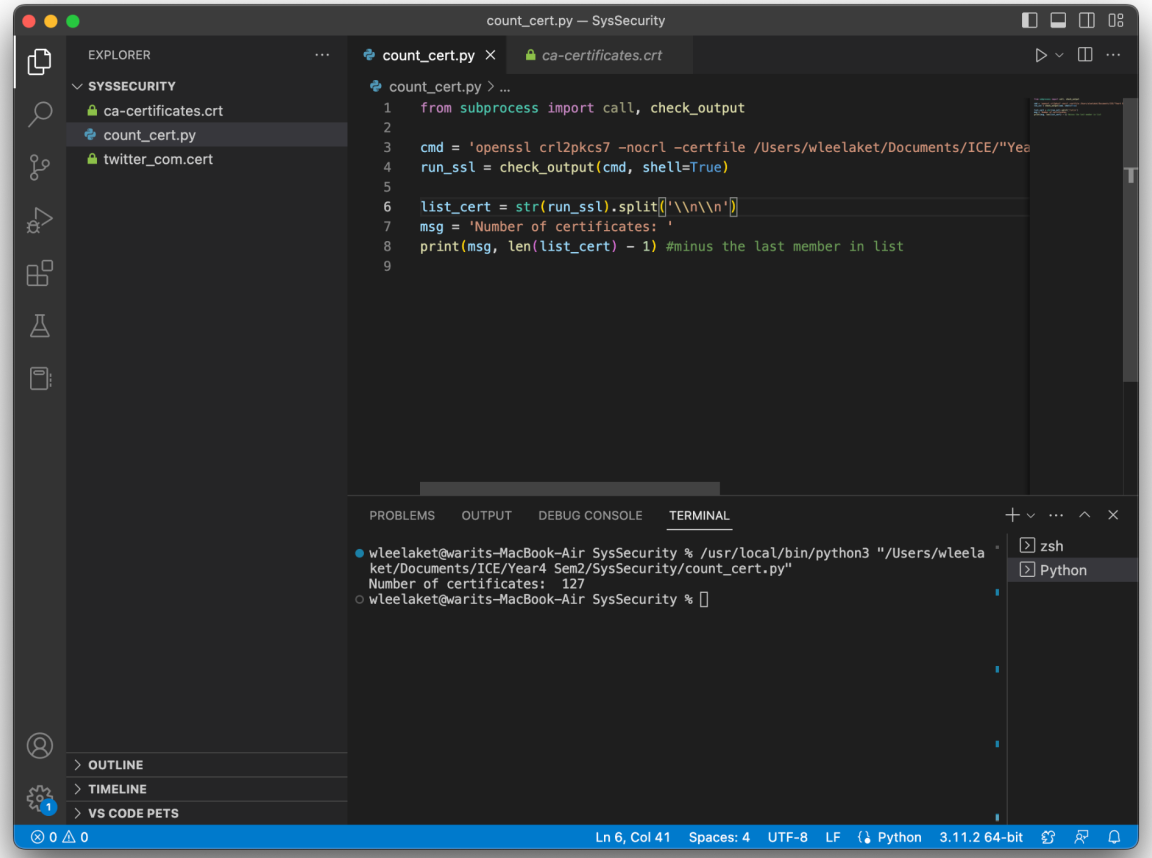
Digital Signature: The signature of this certificate.

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.



: 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
```

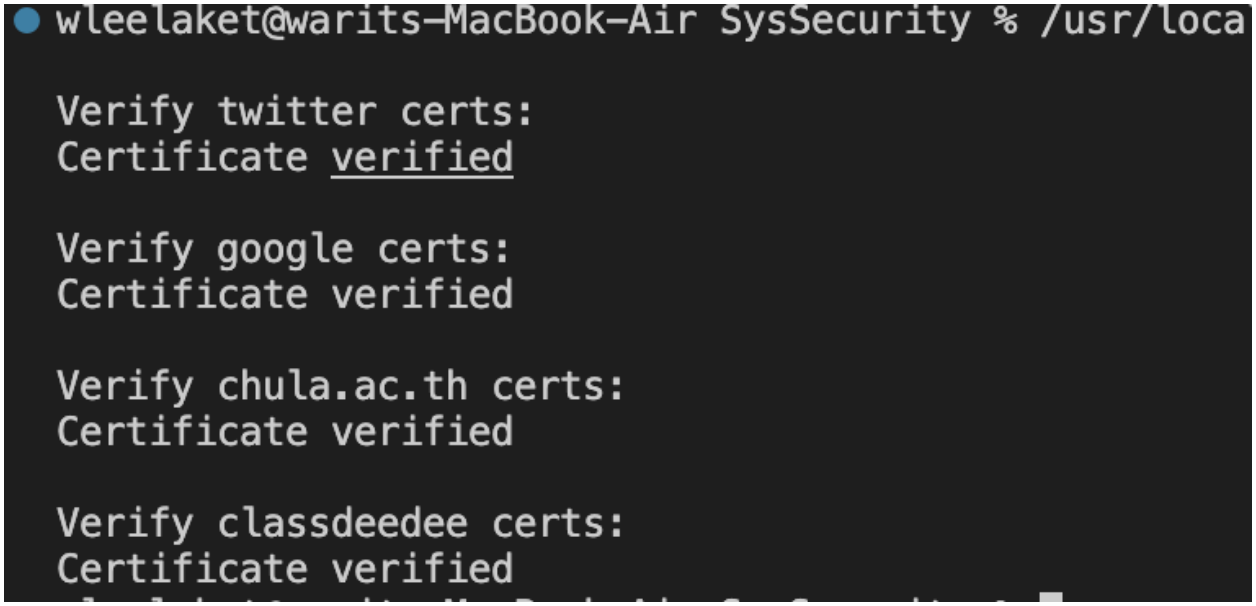
```
subject=/C=US/ST=California/L=San Francisco/O=Twitter, Inc./CN=twitter.com
issuer=/C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
```

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