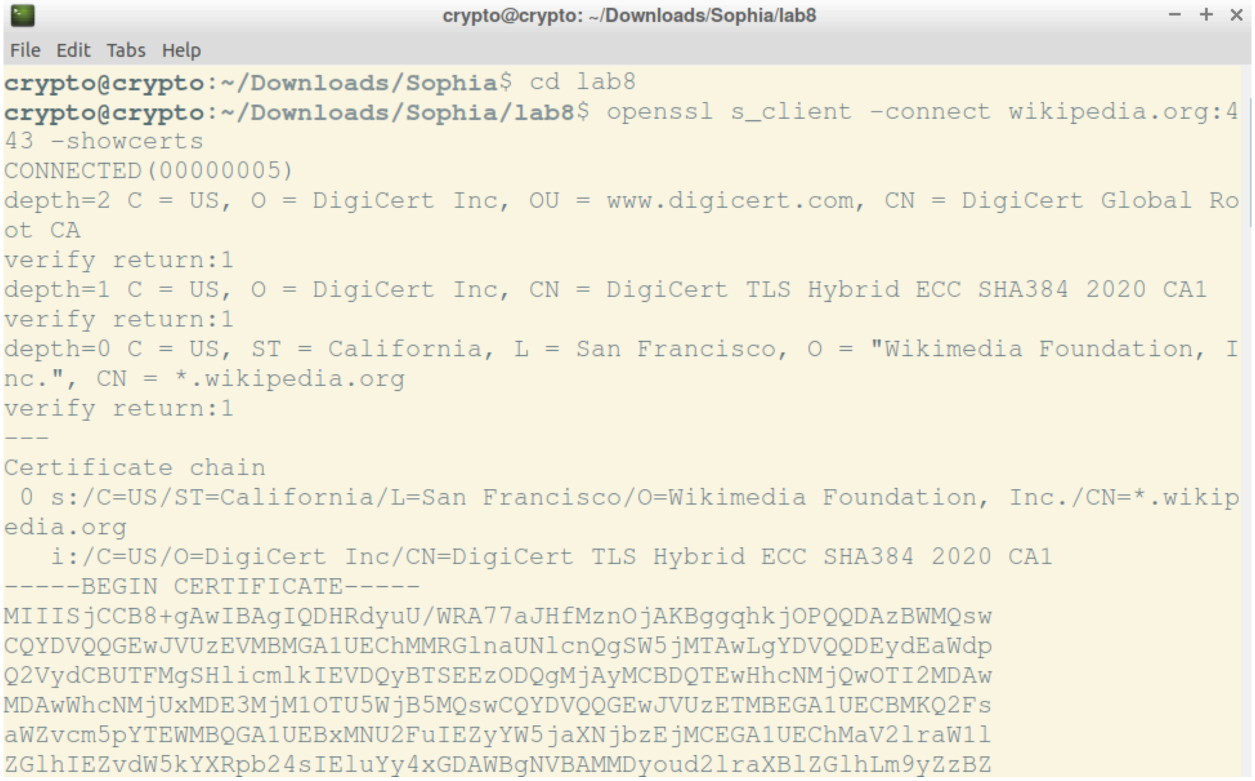
X.509 Certificate

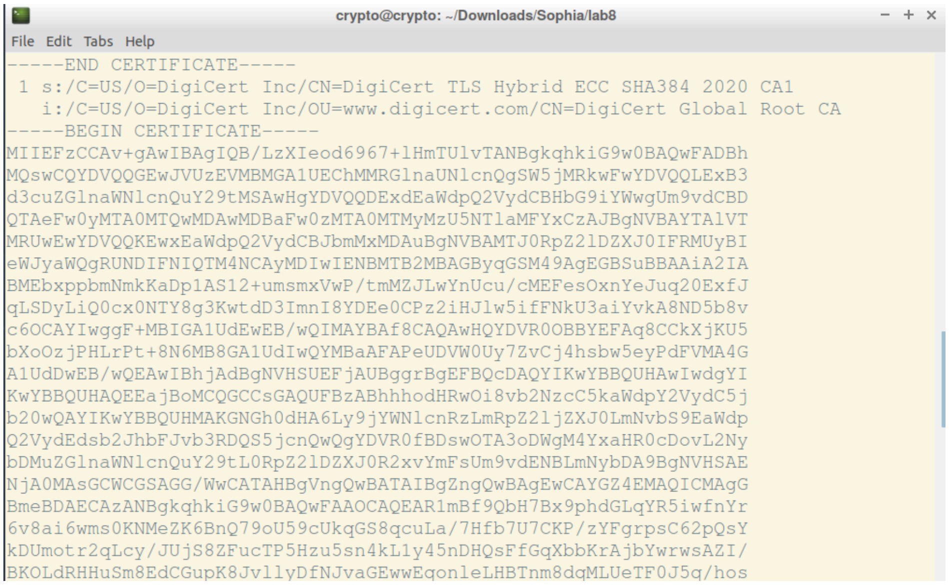
- Verifying it
- Contains public key and signature

Manually verifying an X.509 certificate

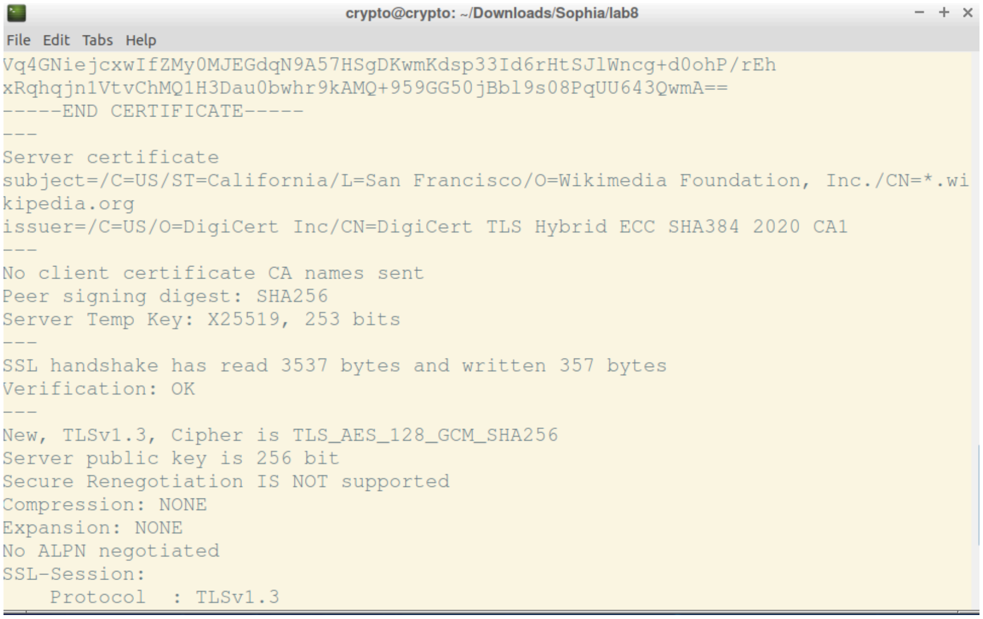
Task 1 - Download a certificate from a real web server.



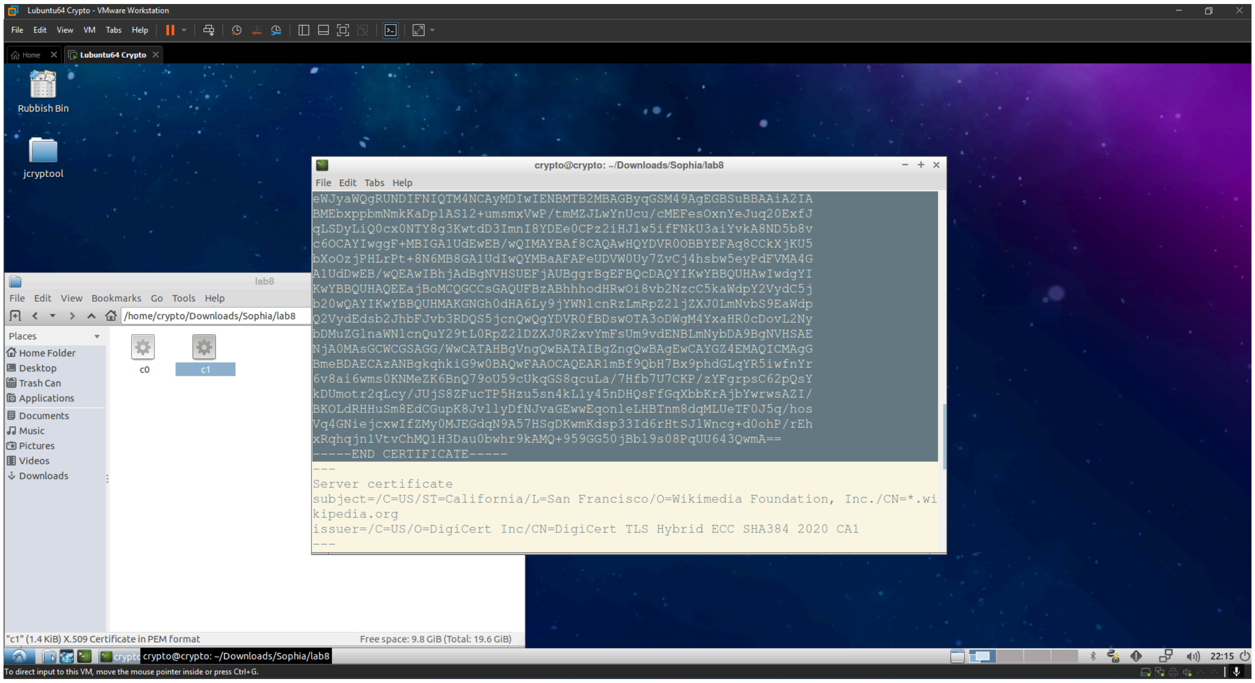
```
crypto@crypto:~/Downloads/Sophia$ cd lab8
crypto@crypto:~/Downloads/Sophia/lab8$ openssl s_client -connect wikipedia.org:4
43 -showcerts
CONNECTED(00000005)
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Ro
ot CA
verify return:1
depth=1 C = US, O = DigiCert Inc, CN = DigiCert TLS Hybrid ECC SHA384 2020 CA1
verify return:1
depth=0 C = US, ST = California, L = San Francisco, O = "Wikimedia Foundation, I
nc.", CN = *.wikipedia.org
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=San Francisco/O=Wikimedia Foundation, Inc./CN=*.wikip
edia.org
   i:/C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
-----BEGIN CERTIFICATE-----
MIISjCCB8+gAwIBAgIQDHRdyuU/WRA77aJHfMznOjAKBggqhkjOPQQDAzBWMQsw
CQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTAwLgYDVQQDEydEaWdp
Q2VydCBUTFMgSHlicmlkIEVDQyBTSEEzODQgMjAyMCBDQTEwHhcNMjQwOTI2MDAw
MDAwWhcNMjUxMDE3MjM1OTU5WjB5MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEjMCEGA1UEChMaV2lraW1l
ZGlhIEZvdW5kYXRpb24sIEluYy4xGDAWBgNVBAMMDyoud2lraXBlZGlhLm9yZzBZ
```



```
-----END CERTIFICATE-----
 1 s:/C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
-----BEGIN CERTIFICATE-----
MIIEFzCCAv+gAwIBAgIQB/LzXIeod6967+1HmTUlvTANBgkqhkiG9w0BAQwFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0yMTA0MTQwMDAwMDBaFw0zMTA0MTMyMzU5NTlaMFYxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxMDAuBgNVBAMTJ0RpZ2lDZXJ0IFRMUyBI
eWJyaWQgRUNDIFNIQTM4NCAyMDIwIENBMTB2MBAGByqGSM49AgEGBSuBBAAiA2IA
BMEbxppbmNmkKaDp1AS12+umsmxVwP/tmMZJLwYnUcu/cMEFesOxnYeJuq20ExfJ
qLSDyLiQ0cx0NTY8g3KwtdD3ImnI8YDEe0CPz2iHJlw5ifFNkU3aiYvkA8ND5b8v
c6OCAYIwggF+MBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFAq8CCkXjKU5
bXoOzjPHLrPt+8N6MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYI
KwYBBQUHAQEEajBoMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5j
b20wQAYIKwYBBQUHMAKGNGh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdp
Q2VydEdsb2JhbFJvb3RDQS5jcnQwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2Ny
bDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNybDA9BgNVHSAE
NjA0MAsGCWCGSAGG/WwCATAHBgVngQwBATAIBgZngQwBAgEwCAYGZ4EMAQICMAgG
BmeBDAECAzANBgkqhkiG9w0BAQwFAAOCAQEAR1mBf9QbH7Bx9phdGLqYR5iwfnYr
6v8ai6wms0KNMeZK6BnQ79oU59cUkqGS8qcuLa/7Hfb7U7CKP/zYFgrpsC62pQsY
kDUmotr2qLcy/JUjS8ZFucTP5Hzu5sn4kL1y45nDHQsFfGqXbbKrAjbYwrwsAZI/
BKOLdRHHuSm8EdCGupK8JvllyDfNJvaGEwwEqonleLHBTnm8dqMLUeTF0J5q/hos
```



```
Vq4GNiejcxwIfZMy0MJEGdqN9A57HSgDKwmKdsp33Id6rHtSJlWncg+d0ohP/rEh
xRqhqjn1VtvChMQ1H3Dau0bwhr9kAMQ+959GG50jBbl9s08PqUU643QwmA==
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=San Francisco/O=Wikimedia Foundation, Inc./CN=*.wi
kipedia.org
issuer=/C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
---
No client certificate CA names sent
Peer signing digest: SHA256
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 3537 bytes and written 357 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.3
```

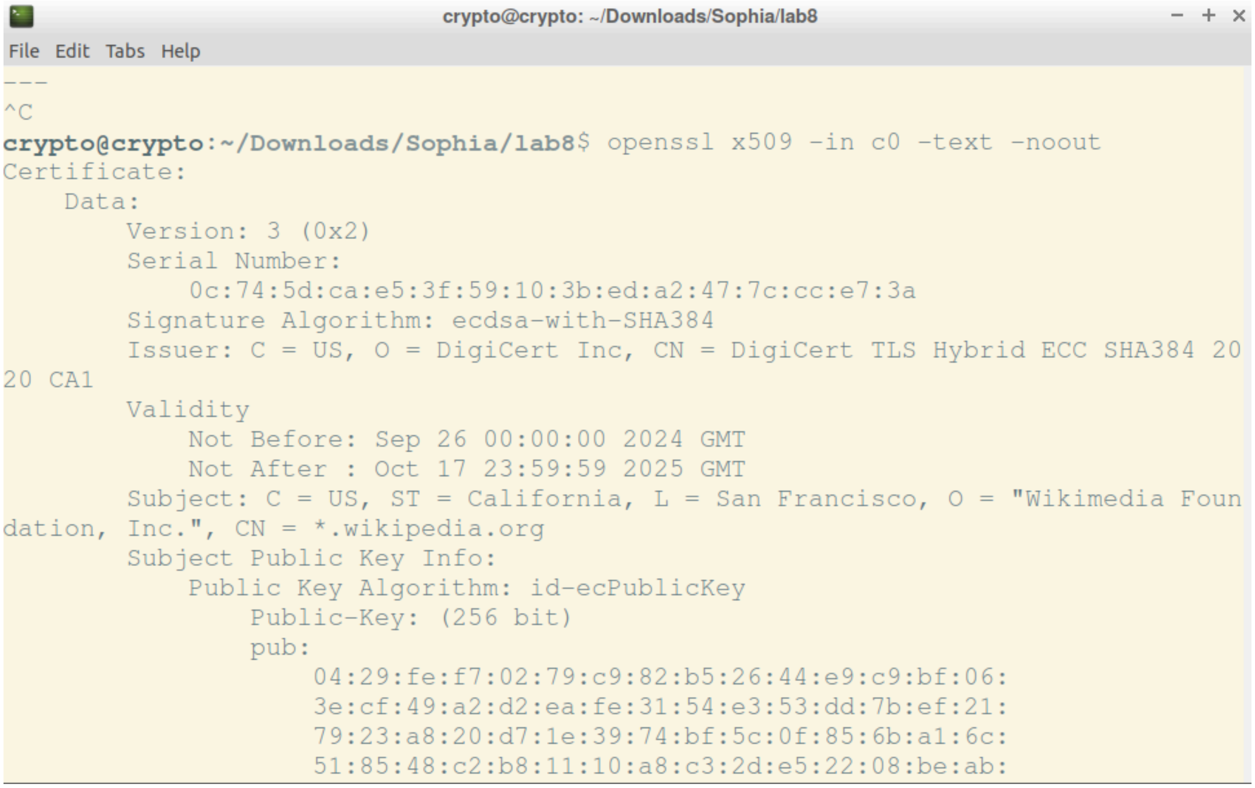

Lubuntu64 Crypto - VMware Workstation
File Edit View VM Tabs Help
Home
Lubuntu64 Crypto
Rubbish Bin
jcryptool
lab8
File Edit View Bookmarks Go Tools Help
/home/crypto/Downloads/Sophia/lab8
Places
Home Folder
Desktop
Trash Can
Applications
Documents
Music
Pictures
Videos
Downloads
c0
c1
"c1" (1.4 KiB) X.509 Certificate in PEM format
Free space: 9.8 GiB (Total: 19.6 GiB)
crypto@crypto: ~/Downloads/Sophia/lab8
22:15
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
crypto@crypto: ~/Downloads/Sophia/lab8
File Edit Tabs Help

```
eWJyaWQgRUNDIFNIQTM4NCAyMDIwIENBMTB2MBAGByqGSM49AgEGBSuBBAAiA2IA
BMEbxppbmNmkKaDp1AS12+umsmxVwP/tmMZJLwYnUcu/cMEFesOxnYeJuq20ExfJ
qLSDyLiQ0cx0NTY8g3KwtdD3ImnI8YDEe0CPz2iHJlw5ifFNkU3aiYvkA8ND5b8v
c6OCAYIwggF+MBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFAq8CCkXjKU5
bXoOzjPHLrPt+8N6MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYI
KwYBBQUHAQEEajBoMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5j
b20wQAYIKwYBBQUHMAKGNGh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdp
Q2VydEdsb2JhbFJvb3RDQS5jcnQwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2Ny
bDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNybDA9BgNVHSAE
NjA0MAsGCWCGSAGG/WwCATAHBgVngQwBATAIBgZngQwBAgEwCAYGZ4EMAQICMAgG
BmeBDAECAzANBgkqhkiG9w0BAQwFAAOCAQEAR1mBf9QbH7Bx9phdGLqYR5iwfnYr
6v8ai6wms0KNMeZK6BnQ79oU59cUkqGS8qcuLa/7Hfb7U7CKP/zYFgrpsC62pQsY
kDUmotr2qLcy/JUjS8ZFucTP5Hzu5sn4kL1y45nDHQsFfGqXbbKrAjbYwrwsAZI/
BKOLdRHHuSm8EdCGupK8JvllyDfNJvaGEwwEqonleLHBTnm8dqMLUeTF0J5q/hos
Vq4GNiejcxwIfZMy0MJEGdqN9A57HSgDKwmKdsp33Id6rHtSJlWncg+d0ohP/rEh
xRqhqjn1VtvChMQ1H3Dau0bwhr9kAMQ+959GG50jBbl9s08PqUU643QwmA==
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=San Francisco/O=Wikimedia Foundation, Inc./CN=*.wi
kipedia.org
issuer=/C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
---
```

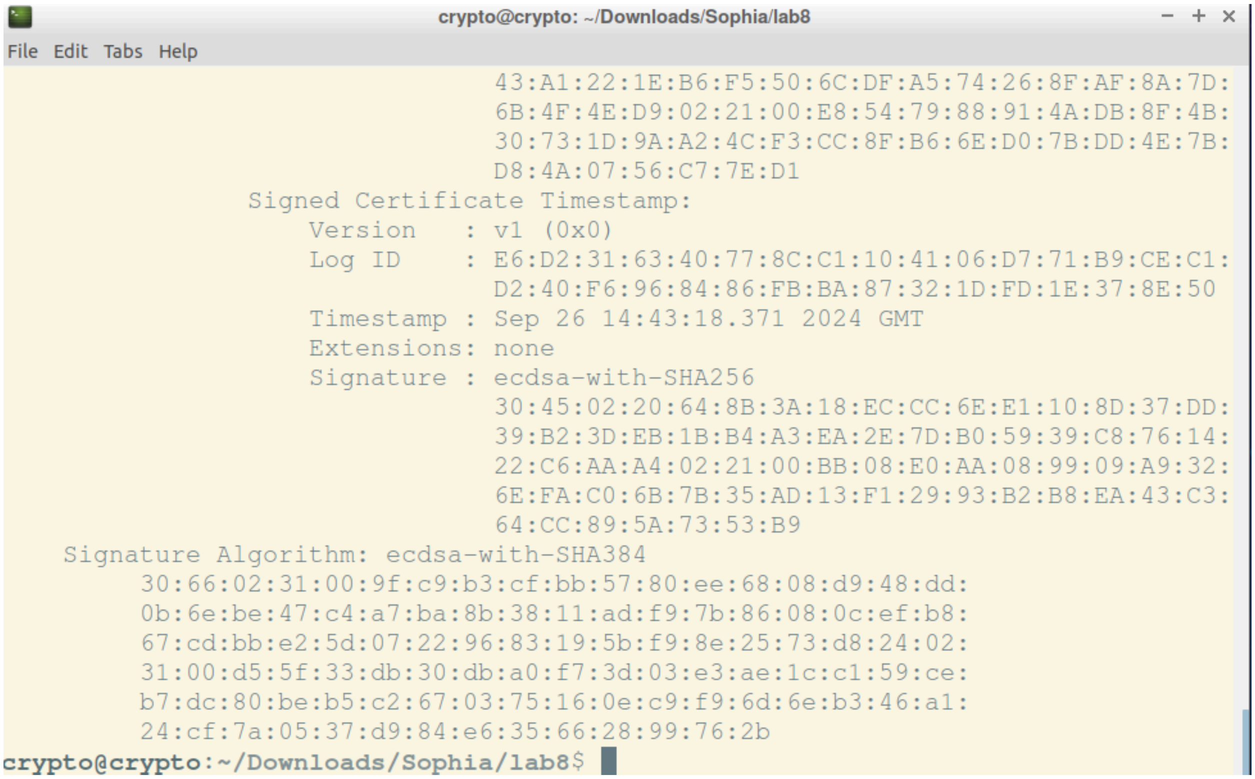
Q1: What are the subject and the issuer of certificate c0? What are the subject and the issuer of certificate c1?

Subject of certificate c0: Wikimedia Foundation, Inc,
Issuer of certificate c0: DigiCert Inc

Subject of certificate c1: DigiCert Inc
Issuer of certificate c2: DigiCert Inc



```
---
^C
crypto@crypto:~/Downloads/Sophia/lab8$ openssl x509 -in c0 -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:74:5d:ca:e5:3f:59:10:3b:ed:a2:47:7c:cc:e7:3a
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = US, O = DigiCert Inc, CN = DigiCert TLS Hybrid ECC SHA384 20
20 CA1
        Validity
            Not Before: Sep 26 00:00:00 2024 GMT
            Not After : Oct 17 23:59:59 2025 GMT
        Subject: C = US, ST = California, L = San Francisco, O = "Wikimedia Foun
dation, Inc.", CN = *.wikipedia.org
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:29:fe:f7:02:79:c9:82:b5:26:44:e9:c9:bf:06:
                    3e:cf:49:a2:d2:ea:fe:31:54:e3:53:dd:7b:ef:21:
                    79:23:a8:20:d7:1e:39:74:bf:5c:0f:85:6b:a1:6c:
                    51:85:48:c2:b8:11:10:a8:c3:2d:e5:22:08:be:ab:
```



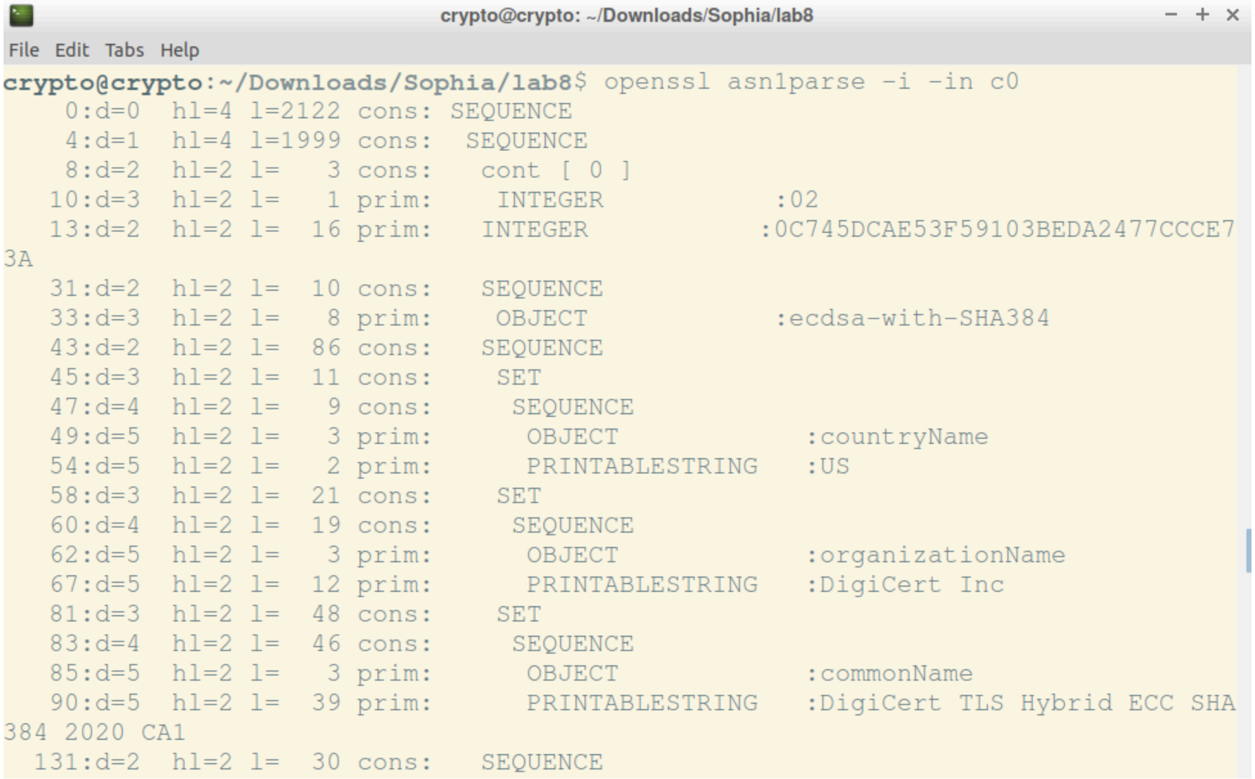
```
                                43:A1:22:1E:B6:F5:50:6C:DF:A5:74:26:8F:AF:8A:7D:
                                6B:4F:4E:D9:02:21:00:E8:54:79:88:91:4A:DB:8F:4B:
                                30:73:1D:9A:A2:4C:F3:CC:8F:B6:6E:D0:7B:DD:4E:7B:
                                D8:4A:07:56:C7:7E:D1
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : E6:D2:31:63:40:77:8C:C1:10:41:06:D7:71:B9:CE:C1:
                                D2:40:F6:96:84:86:FB:BA:87:32:1D:FD:1E:37:8E:50
                    Timestamp : Sep 26 14:43:18.371 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:64:8B:3A:18:EC:CC:6E:E1:10:8D:37:DD:
                                39:B2:3D:EB:1B:B4:A3:EA:2E:7D:B0:59:39:C8:76:14:
                                22:C6:AA:A4:02:21:00:BB:08:E0:AA:08:99:09:A9:32:
                                6E:FA:C0:6B:7B:35:AD:13:F1:29:93:B2:B8:EA:43:C3:
                                64:CC:89:5A:73:53:B9
    Signature Algorithm: ecdsa-with-SHA384
         30:66:02:31:00:9f:c9:b3:cf:bb:57:80:ee:68:08:d9:48:dd:
         0b:6e:be:47:c4:a7:ba:8b:38:11:ad:f9:7b:86:08:0c:ef:b8:
         67:cd:bb:e2:5d:07:22:96:83:19:5b:f9:8e:25:73:d8:24:02:
         31:00:d5:5f:33:db:30:db:a0:f7:3d:03:e3:ae:1c:c1:59:ce:
         b7:dc:80:be:b5:c2:67:03:75:16:0e:c9:f9:6d:6e:b3:46:a1:
         24:cf:7a:05:37:d9:84:e6:35:66:28:99:76:2b
crypto@crypto:~/Downloads/Sophia/lab8$ 
```

Q2:
Which signature algorithm does the certificate c0 use? - uses ecdsa with sha384

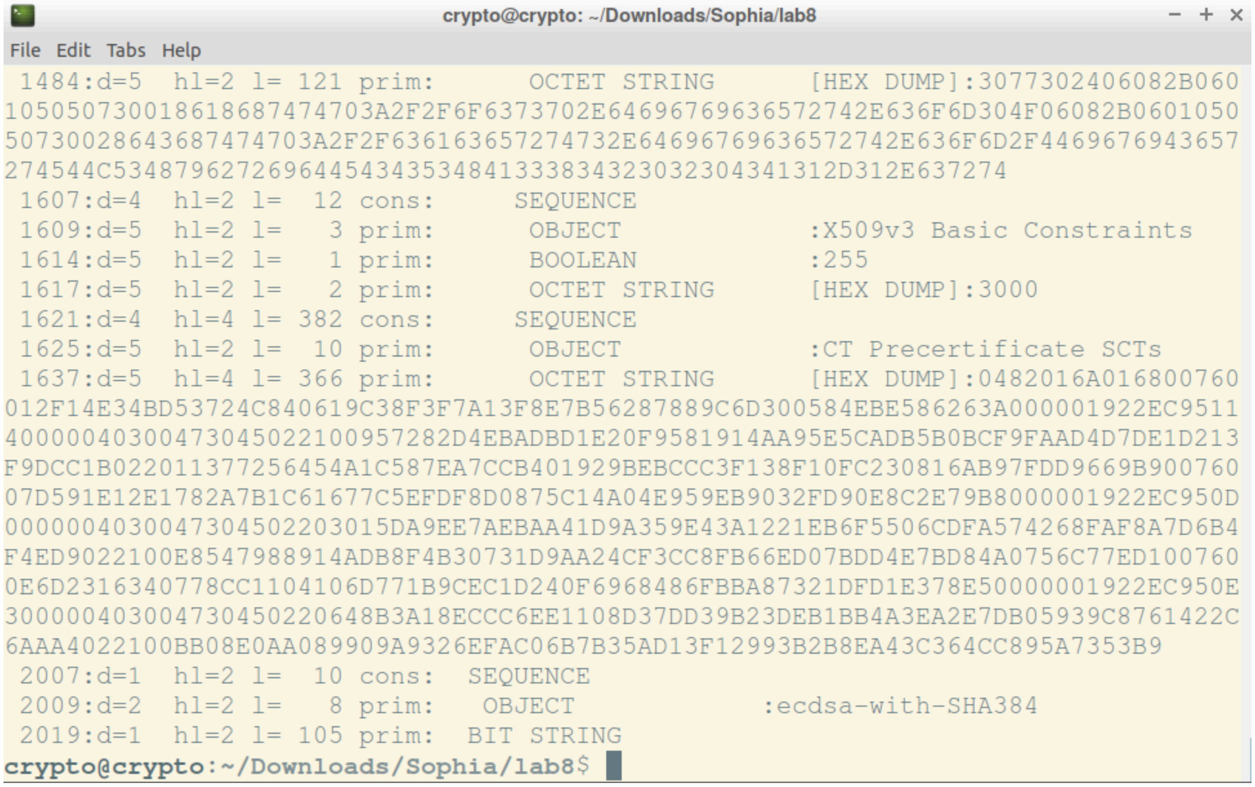
What is the signature value? - 30:66:02:31:00:9f:c9:b3:cf:bb:57:80:ee:68:08:d9:48:dd:0b:6e:be:47:c4:a7:ba:8b:38:11:ad:f9:7b:86:08:0c:ef:b8:67:cd:bb:e2:5d:07:22:96:83:19:5b:f9:8e:25:73:d8:24:02:31:00:d5:5f:33:db:30:db:a0:f7:3d:03:e3:ae:1c:c1:59:ce:b7:dc:80:be:b5:c2:67:03:75:16:0e:c9:f9:6d:6e:b3:46:a1:24:cf:7a:05:37:d9:84:e6:35:66:28:99:76:2b

What is the wikipedia.org's public key, and which public key algorithm does wikipedia.org use? - 04:29:fe:f7:02:79:c9:82:b5:26:44:e9:c9:bf:06:3e:cf:49:a2:d2:ea:fe:31:54:e3:53:dd:7b:ef:21:79:23:a8:20:d7:1e:39:74:bf:5c:0f:85:6b:a1:6c:51:85:48:c2:b8:11:10:a8:c3:2d:e5:22:08:be:ab:40:cf:3c:44:0e, uses Elliptic Curve

- Basic structure in certificate
    - ASN.1 header for sequence tag
    - Part containing information about signature
    - AlgorithmIdentifier - specifies type of signature
    - Actual signature (bit string)



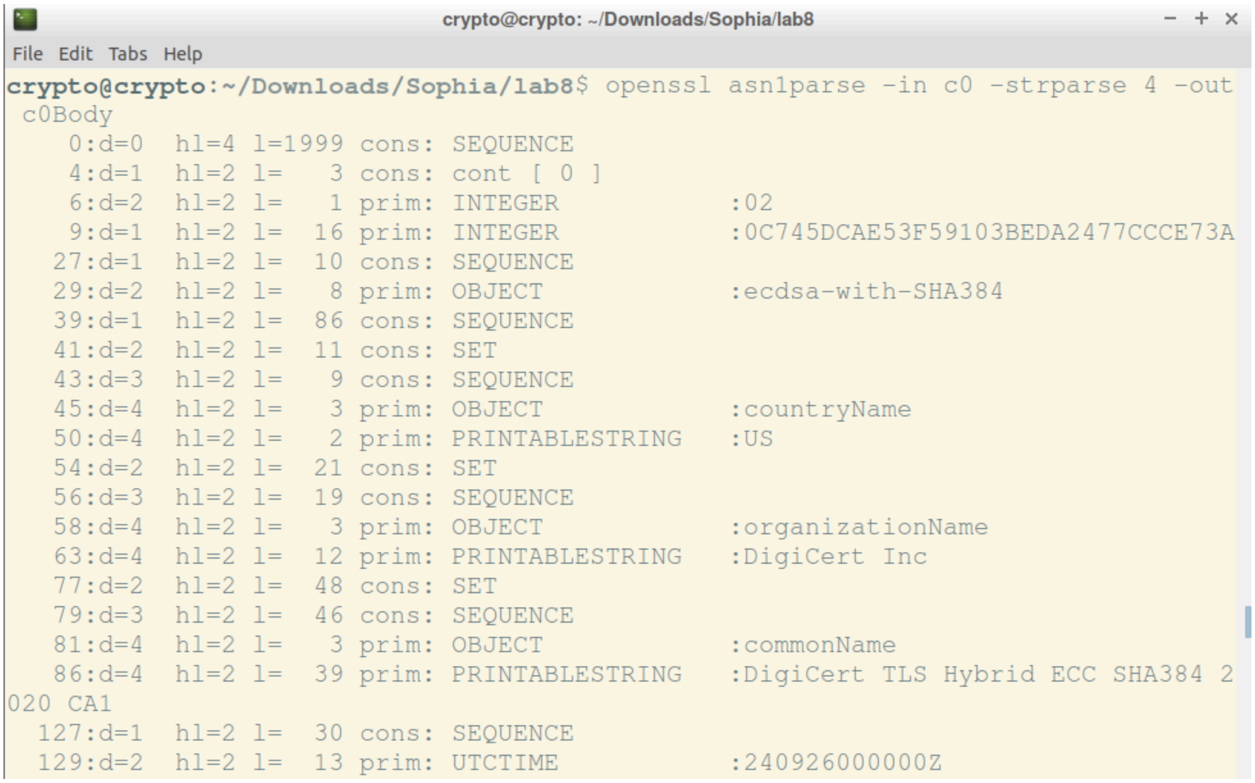
```
crypto@crypto:~/Downloads/Sophia/lab8$ openssl asn1parse -i -in c0
    0:d=0  hl=4 l=2122 cons: SEQUENCE
    4:d=1  hl=4 l=1999 cons:  SEQUENCE
    8:d=2  hl=2 l=   3 cons:   cont [ 0 ]
   10:d=3  hl=2 l=   1 prim:    INTEGER           :02
   13:d=2  hl=2 l=  16 prim:   INTEGER           :0C745DCAE53F59103BEDA2477CCCE7
3A
   31:d=2  hl=2 l=  10 cons:   SEQUENCE
   33:d=3  hl=2 l=   8 prim:    OBJECT            :ecdsa-with-SHA384
   43:d=2  hl=2 l=  86 cons:   SEQUENCE
   45:d=3  hl=2 l=  11 cons:    SET
   47:d=4  hl=2 l=   9 cons:     SEQUENCE
   49:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
   54:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :US
   58:d=3  hl=2 l=  21 cons:    SET
   60:d=4  hl=2 l=  19 cons:     SEQUENCE
   62:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
   67:d=5  hl=2 l=  12 prim:      PRINTABLESTRING   :DigiCert Inc
   81:d=3  hl=2 l=  48 cons:    SET
   83:d=4  hl=2 l=  46 cons:     SEQUENCE
   85:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
   90:d=5  hl=2 l=  39 prim:      PRINTABLESTRING   :DigiCert TLS Hybrid ECC SHA
384 2020 CA1
  131:d=2  hl=2 l=  30 cons:   SEQUENCE
```



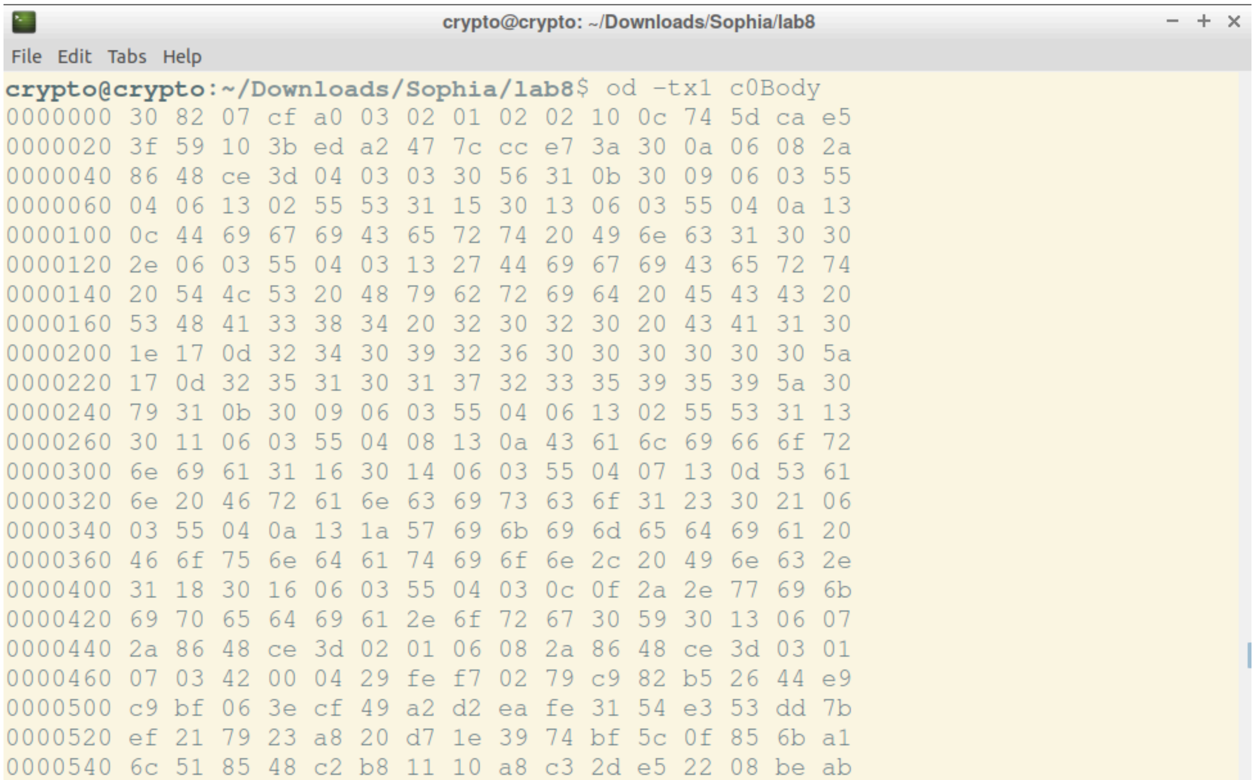
```
 1484:d=5  hl=2 l= 121 prim:       OCTET STRING      [HEX DUMP]:3077302406082B060
10505073001861868747470 3A2F2F6F6373702E6469676963657274 2E636F6D304F06082B0601050
507300286436874747 03A2F2F63616365727473 2E6469676963657274 2E636F6D2F4469676943657
274544C534879627269644543435348413338343230323041312D312E637274
 1607:d=4  hl=2 l=  12 cons:      SEQUENCE
 1609:d=5  hl=2 l=   3 prim:       OBJECT            :X509v3 Basic Constraints
 1614:d=5  hl=2 l=   1 prim:       BOOLEAN           :255
 1617:d=5  hl=2 l=   2 prim:       OCTET STRING      [HEX DUMP]:3000
 1621:d=4  hl=4 l= 382 cons:      SEQUENCE
 1625:d=5  hl=2 l=  10 prim:       OBJECT            :CT Precertificate SCTs
 1637:d=5  hl=4 l= 366 prim:       OCTET STRING      [HEX DUMP]:0482016A016800760
012F14E34BD53724C840619C38F3F7A13F8E7B56287889C6D300584EBE586263A000001922EC9511
400000403004730450221009572 82D4EBADBD1E20F9581914AA95E5CADB5B0BCF9FAAD4D7DE1D213
F9DCC1B022011377256454A1C587EA7CCB401929BEBCCC3F138F10FC230816AB97FDD9669B900760
07D591E12E1782A7B1C61677C5EFDF8D0875C14A04E959EB9032FD90E8C2E79B8000001922EC950D
0000004030047304502203015DA9EE7AEBAA41D9A359E43A1221EB6F5506CDFA574268FAF8A7D6B4
F4ED9022100E8547988914ADB8F4B30731D9AA24CF3CC8FB66ED07BDD4E7BD84A0756C77ED100760
0E6D2316340778CC1104106D771B9CEC1D240F6968486FBBA87321DFD1E378E5000001922EC950E
300000403004730450220648B3A18ECCC6EE1108D37DD39B23DEB1BB4A3EA2E7DB05939C8761422C
6AAA4022100BB08E0AA089909A9326EFAC06B7B35AD13F12993B2B8EA43C364CC895A7353B9
 2007:d=1  hl=2 l=  10 cons:  SEQUENCE
 2009:d=2  hl=2 l=   8 prim:   OBJECT            :ecdsa-with-SHA384
 2019:d=1  hl=2 l= 105 prim:  BIT STRING
crypto@crypto:~/Downloads/Sophia/lab8$ 
```

Task 2 - Prepare the signature data

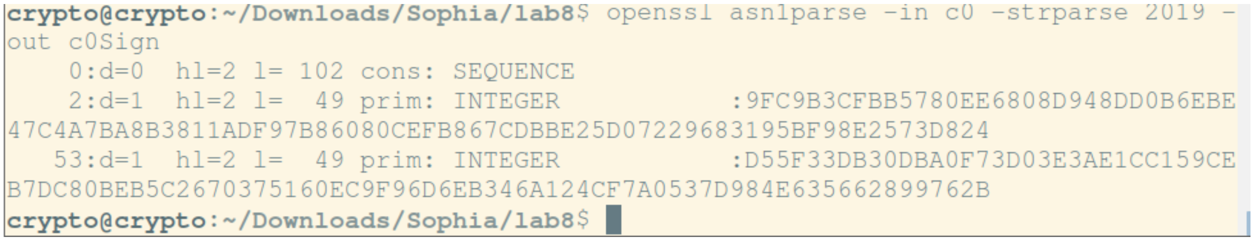
- TBS certificate (to be signed) starts at offset 4
- Signature wrapper starts at offset 1979 (last line)



```
crypto@crypto:~/Downloads/Sophia/lab8$ openssl asn1parse -in c0 -strparse 4 -out
 c0Body
    0:d=0  hl=4 l=1999 cons: SEQUENCE
    4:d=1  hl=2 l=   3 cons: cont [ 0 ]
    6:d=2  hl=2 l=   1 prim: INTEGER           :02
    9:d=1  hl=2 l=  16 prim: INTEGER           :0C745DCAE53F59103BEDA2477CCCE73A
   27:d=1  hl=2 l=  10 cons: SEQUENCE
   29:d=2  hl=2 l=   8 prim: OBJECT            :ecdsa-with-SHA384
   39:d=1  hl=2 l=  86 cons: SEQUENCE
   41:d=2  hl=2 l=  11 cons: SET
   43:d=3  hl=2 l=   9 cons: SEQUENCE
   45:d=4  hl=2 l=   3 prim: OBJECT            :countryName
   50:d=4  hl=2 l=   2 prim: PRINTABLESTRING   :US
   54:d=2  hl=2 l=  21 cons: SET
   56:d=3  hl=2 l=  19 cons: SEQUENCE
   58:d=4  hl=2 l=   3 prim: OBJECT            :organizationName
   63:d=4  hl=2 l=  12 prim: PRINTABLESTRING   :DigiCert Inc
   77:d=2  hl=2 l=  48 cons: SET
   79:d=3  hl=2 l=  46 cons: SEQUENCE
   81:d=4  hl=2 l=   3 prim: OBJECT            :commonName
   86:d=4  hl=2 l=  39 prim: PRINTABLESTRING   :DigiCert TLS Hybrid ECC SHA384 2
020 CA1
  127:d=1  hl=2 l=  30 cons: SEQUENCE
  129:d=2  hl=2 l=  13 prim: UTCTIME           :240926000000Z
```



```
crypto@crypto:~/Downloads/Sophia/lab8$ od -tx1 c0Body
0000000 30 82 07 cf a0 03 02 01 02 02 10 0c 74 5d ca e5
0000020 3f 59 10 3b ed a2 47 7c cc e7 3a 30 0a 06 08 2a
0000040 86 48 ce 3d 04 03 03 30 56 31 0b 30 09 06 03 55
0000060 04 06 13 02 55 53 31 15 30 13 06 03 55 04 0a 13
0000100 0c 44 69 67 69 43 65 72 74 20 49 6e 63 31 30 30
0000120 2e 06 03 55 04 03 13 27 44 69 67 69 43 65 72 74
0000140 20 54 4c 53 20 48 79 62 72 69 64 20 45 43 43 20
0000160 53 48 41 33 38 34 20 32 30 32 30 20 43 41 31 30
0000200 1e 17 0d 32 34 30 39 32 36 30 30 30 30 30 30 5a
0000220 17 0d 32 35 31 30 31 37 32 33 35 39 35 39 5a 30
0000240 79 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13
0000260 30 11 06 03 55 04 08 13 0a 43 61 6c 69 66 6f 72
0000300 6e 69 61 31 16 30 14 06 03 55 04 07 13 0d 53 61
0000320 6e 20 46 72 61 6e 63 69 73 63 6f 31 23 30 21 06
0000340 03 55 04 0a 13 1a 57 69 6b 69 6d 65 64 69 61 20
0000360 46 6f 75 6e 64 61 74 69 6f 6e 2c 20 49 6e 63 2e
0000400 31 18 30 16 06 03 55 04 03 0c 0f 2a 2e 77 69 6b
0000420 69 70 65 64 69 61 2e 6f 72 67 30 59 30 13 06 07
0000440 2a 86 48 ce 3d 02 01 06 08 2a 86 48 ce 3d 03 01
0000460 07 03 42 00 04 29 fe f7 02 79 c9 82 b5 26 44 e9
0000500 c9 bf 06 3e cf 49 a2 d2 ea fe 31 54 e3 53 dd 7b
0000520 ef 21 79 23 a8 20 d7 1e 39 74 bf 5c 0f 85 6b a1
0000540 6c 51 85 48 c2 b8 11 10 a8 c3 2d e5 22 08 be ab
```



```
crypto@crypto:~/Downloads/Sophia/lab8$ openssl asn1parse -in c0 -strparse 2019 -
out c0Sign
    0:d=0  hl=2 l= 102 cons: SEQUENCE
    2:d=1  hl=2 l=  49 prim: INTEGER           :9FC9B3CFBB5780EE6808D948DD0B6EBE
47C4A7BA8B3811ADF97B86080CEFB867CDBBE25D07229683195BF98E2573D824
   53:d=1  hl=2 l=  49 prim: INTEGER           :D55F33DB30DBA0F73D03E3AE1CC159CE
B7DC80BEB5C2670375160EC9F96D6EB346A124CF7A0537D984E635662899762B
crypto@crypto:~/Downloads/Sophia/lab8$ 
```

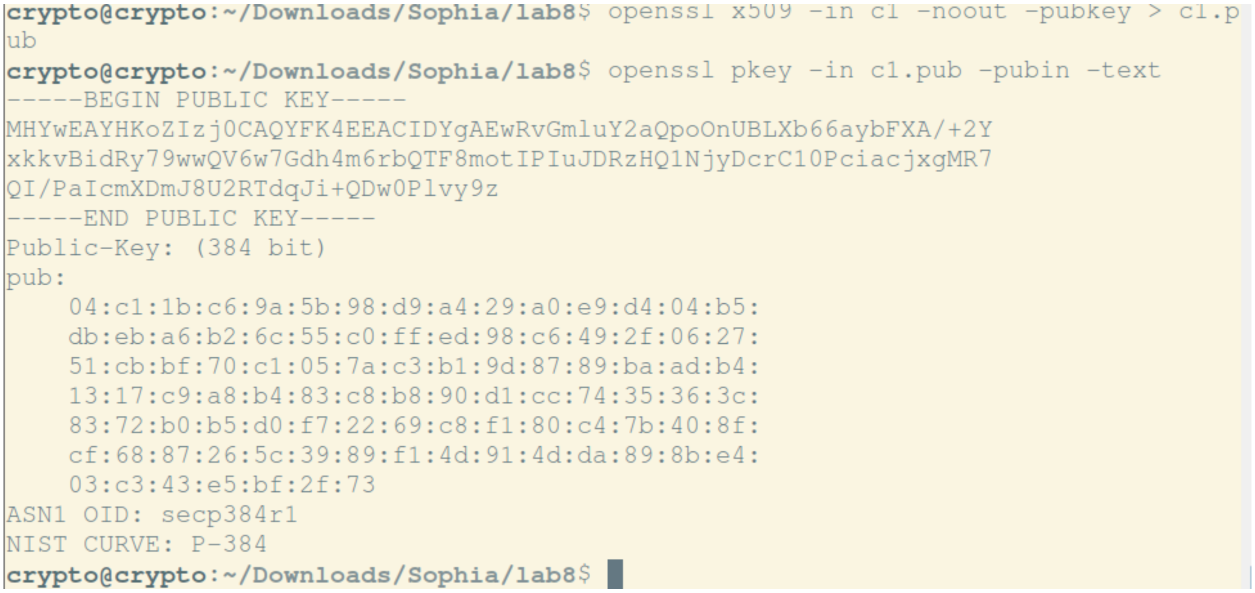
Q3:

Is the signature value identical with the signature value in the last question (Q2)? - no

Who creates this signature, wikipedia or digicert? - Digicert

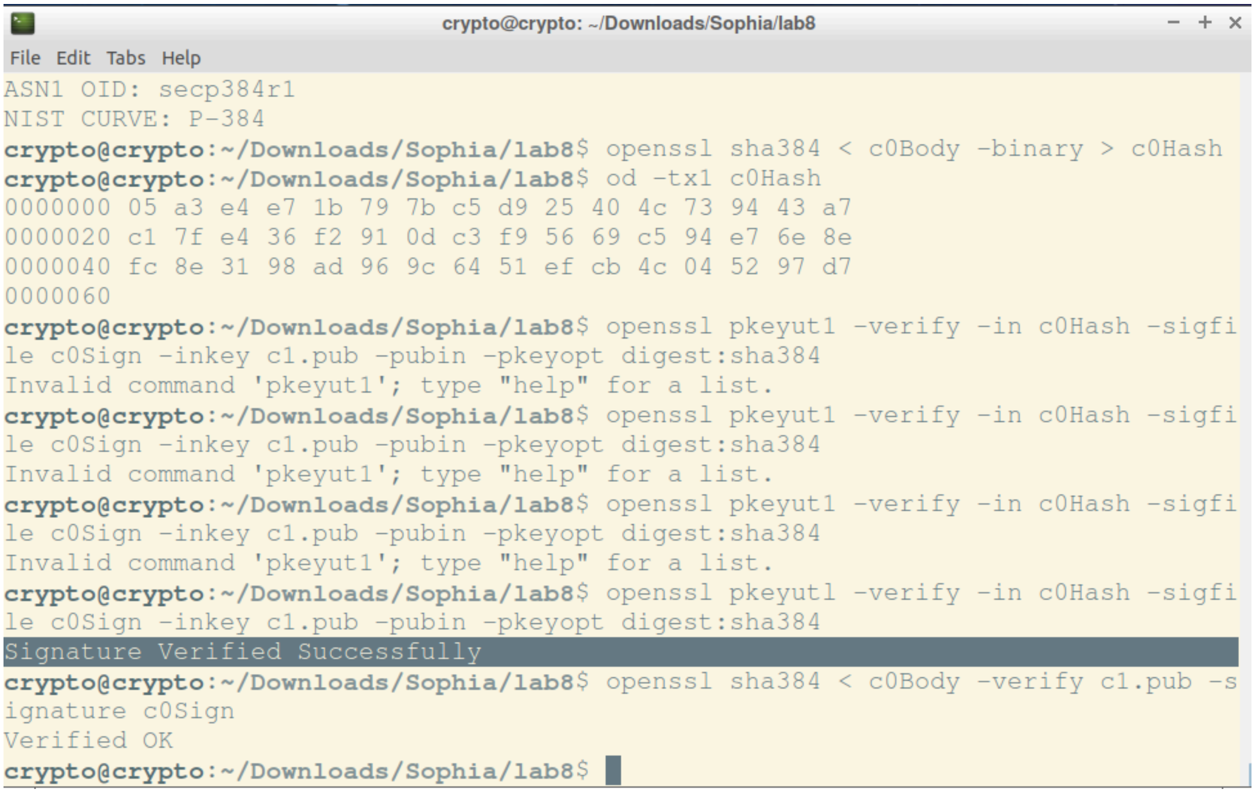
Which key (private or public key) is used for signing? - private key

Task 3 - Get the root public key



```
crypto@crypto:~/Downloads/Sophia/lab8$ openssl x509 -in c1 -noout -pubkey > c1.p
ub
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkey -in c1.pub -pubin -text
-----BEGIN PUBLIC KEY-----
MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEwRvGmluY2aQpoOnUBLXb66aybFXA/+2Y
xkkvBidRy79wwQV6w7Gdh4m6rbQTF8motIPIuJDRzHQ1NjyDcrC10PciacjxgMR7
QI/PaIcmXDmJ8U2RTdqJi+QDw0Plvy9z
-----END PUBLIC KEY-----
Public-Key: (384 bit)
pub:
    04:c1:1b:c6:9a:5b:98:d9:a4:29:a0:e9:d4:04:b5:
    db:eb:a6:b2:6c:55:c0:ff:ed:98:c6:49:2f:06:27:
    51:cb:bf:70:c1:05:7a:c3:b1:9d:87:89:ba:ad:b4:
    13:17:c9:a8:b4:83:c8:b8:90:d1:cc:74:35:36:3c:
    83:72:b0:b5:d0:f7:22:69:c8:f1:80:c4:7b:40:8f:
    cf:68:87:26:5c:39:89:f1:4d:91:4d:da:89:8b:e4:
    03:c3:43:e5:bf:2f:73
ASN1 OID: secp384r1
NIST CURVE: P-384
crypto@crypto:~/Downloads/Sophia/lab8$
```

Task 4 - Verification

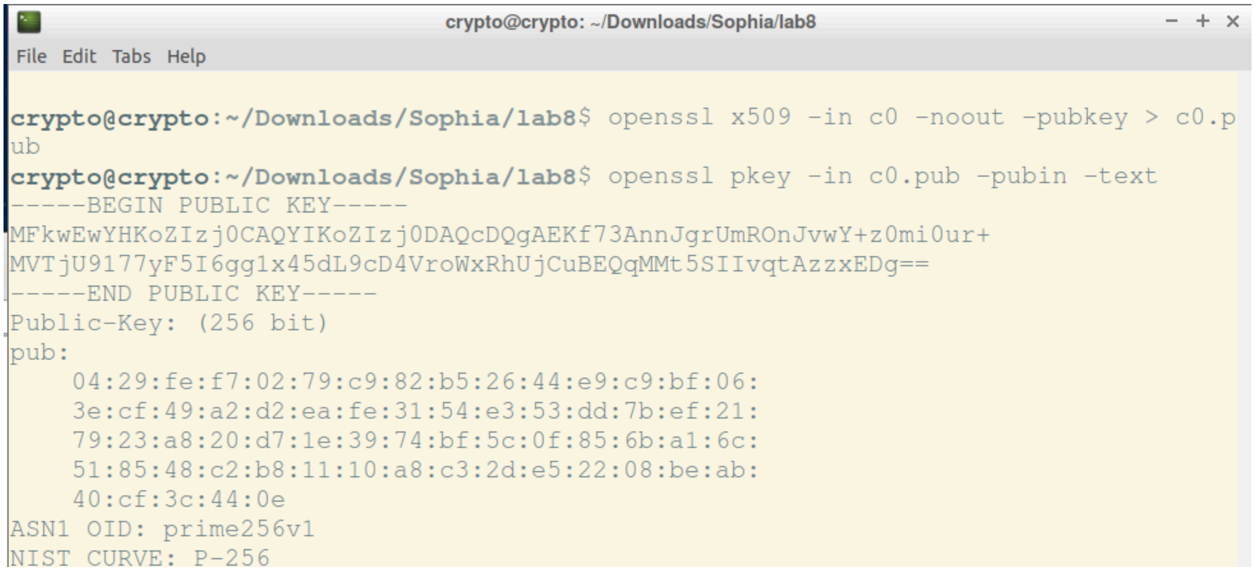


```
ASN1 OID: secp384r1
NIST CURVE: P-384
crypto@crypto:~/Downloads/Sophia/lab8$ openssl sha384 < c0Body -binary > c0Hash
crypto@crypto:~/Downloads/Sophia/lab8$ od -tx1 c0Hash
0000000 05 a3 e4 e7 1b 79 7b c5 d9 25 40 4c 73 94 43 a7
0000020 c1 7f e4 36 f2 91 0d c3 f9 56 69 c5 94 e7 6e 8e
0000040 fc 8e 31 98 ad 96 9c 64 51 ef cb 4c 04 52 97 d7
0000060
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkeyut1 -verify -in c0Hash -sigfi
le c0Sign -inkey c1.pub -pubin -pkeyopt digest:sha384
Invalid command 'pkeyut1'; type "help" for a list.
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkeyut1 -verify -in c0Hash -sigfi
le c0Sign -inkey c1.pub -pubin -pkeyopt digest:sha384
Invalid command 'pkeyut1'; type "help" for a list.
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkeyut1 -verify -in c0Hash -sigfi
le c0Sign -inkey c1.pub -pubin -pkeyopt digest:sha384
Invalid command 'pkeyut1'; type "help" for a list.
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkeyutl -verify -in c0Hash -sigfi
le c0Sign -inkey c1.pub -pubin -pkeyopt digest:sha384
Signature Verified Successfully
crypto@crypto:~/Downloads/Sophia/lab8$ openssl sha384 < c0Body -verify c1.pub -s
ignature c0Sign
Verified OK
crypto@crypto:~/Downloads/Sophia/lab8$ 
```

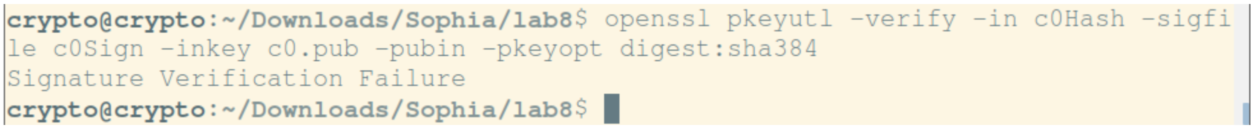
Q4: Explain the parameters in the “openssl pkeyutl” command and the inputs and outputs of the verification process.

- verifies a digital signature using public key: checks if c0Sign correctly signed data in c0Hash using public key from c1.pub
- -pkeyopt digest:sha384: specifies SHA-384 was used during signing

Task 5 - Some error verification



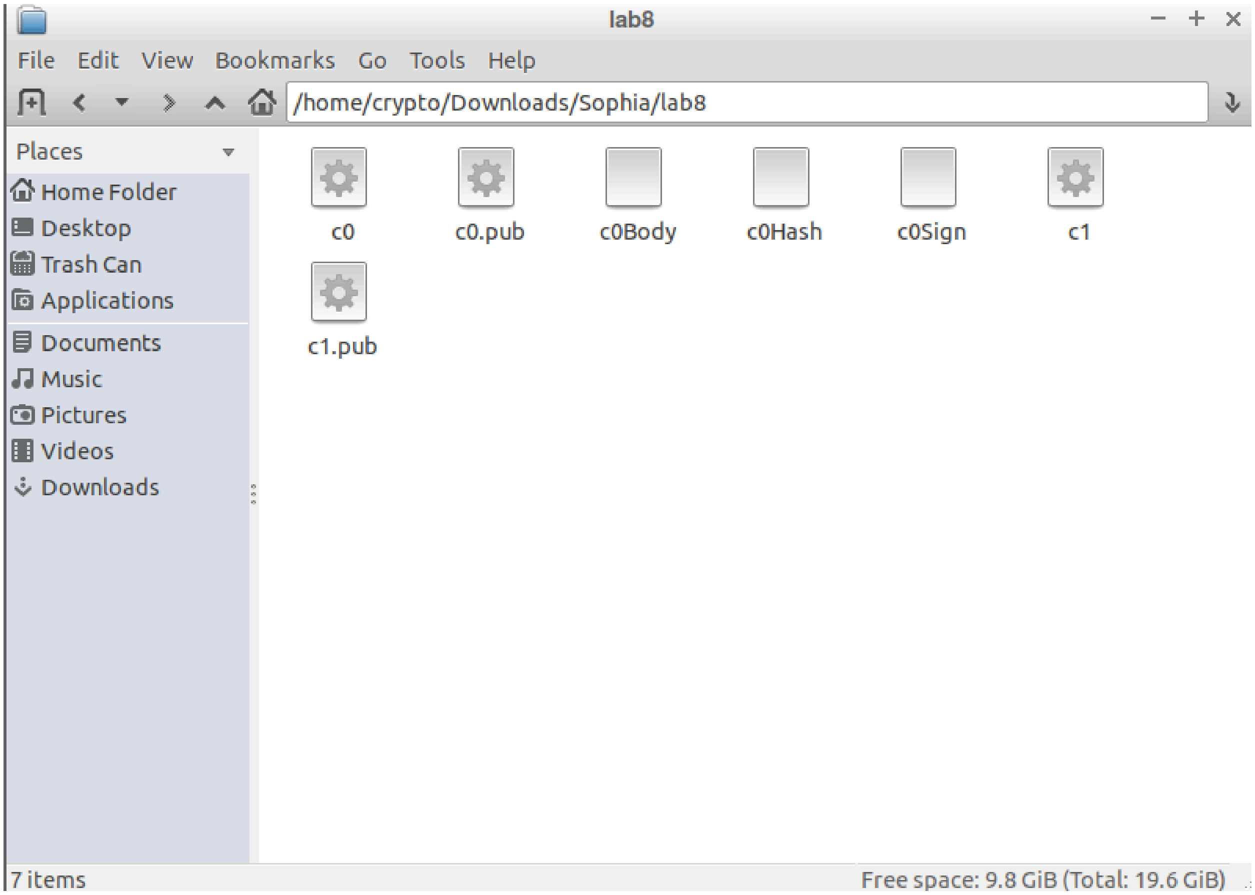
```
crypto@crypto:~/Downloads/Sophia/lab8$ openssl x509 -in c0 -noout -pubkey > c0.p
ub
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkey -in c0.pub -pubin -text
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEKf73AnnJgrUmROnJvwY+z0mi0ur+
MVTjU9177yF5I6gg1x45dL9cD4VroWxRhUjCuBEQqMMt5SIIvqtAzzxEDg==
-----END PUBLIC KEY-----
Public-Key: (256 bit)
pub:
    04:29:fe:f7:02:79:c9:82:b5:26:44:e9:c9:bf:06:
    3e:cf:49:a2:d2:ea:fe:31:54:e3:53:dd:7b:ef:21:
    79:23:a8:20:d7:1e:39:74:bf:5c:0f:85:6b:a1:6c:
    51:85:48:c2:b8:11:10:a8:c3:2d:e5:22:08:be:ab:
    40:cf:3c:44:0e
ASN1 OID: prime256v1
NIST CURVE: P-256
```



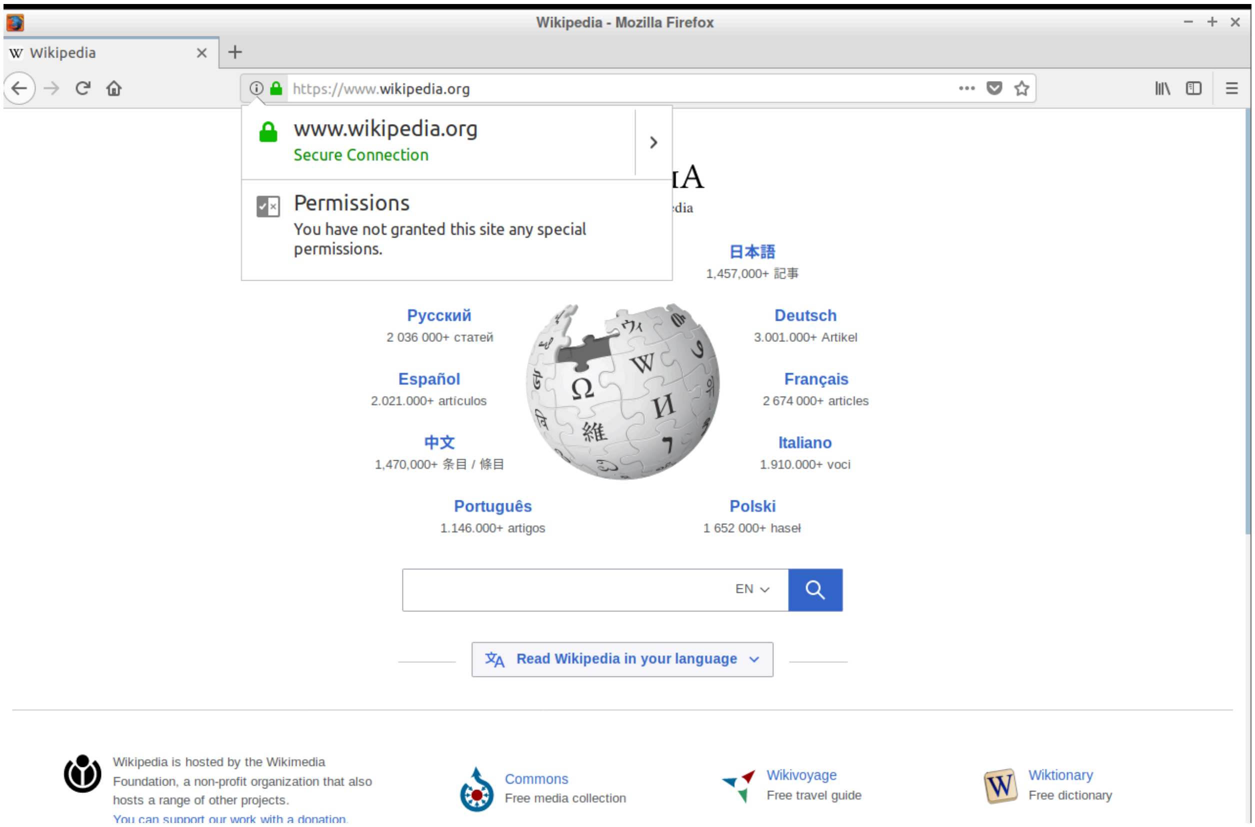
```
crypto@crypto:~/Downloads/Sophia/lab8$ openssl pkeyutl -verify -in c0Hash -sigfi
le c0Sign -inkey c0.pub -pubin -pkeyopt digest:sha384
Signature Verification Failure
crypto@crypto:~/Downloads/Sophia/lab8$ 
```

Q5: Is the public key same with the key in question Q2? - yes
Is verification successful or failed? - failed
Why? - untrusted CA

Task 6 - All the files



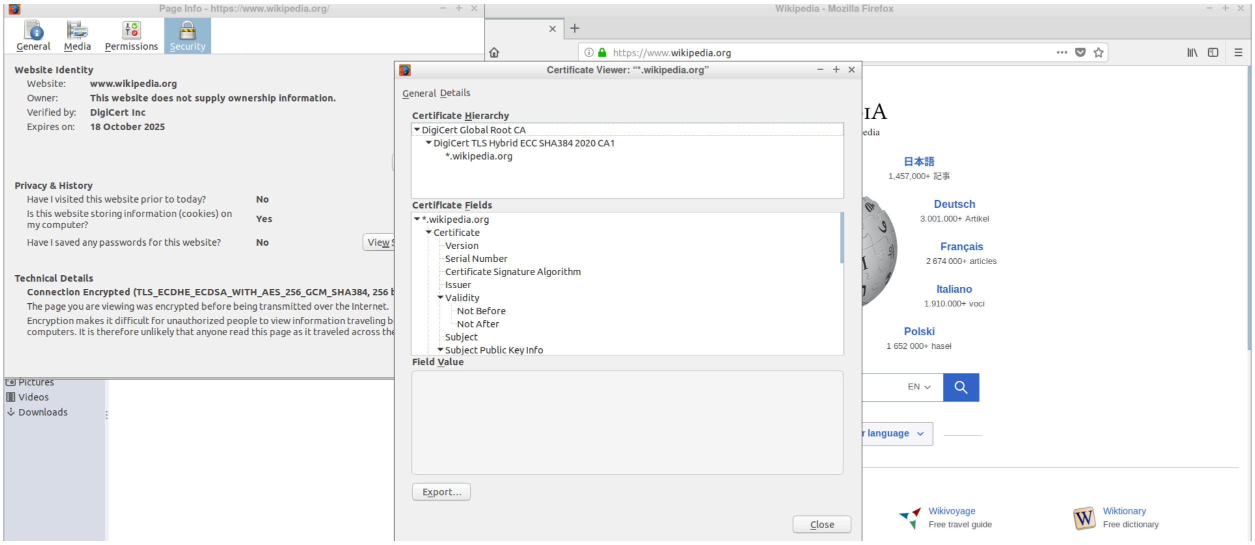
Check certificate using firefox



www.wikipedia.org
Secure Connection

Permissions
You have not granted this site any special permissions.

Wikipedia is hosted by the Wikimedia Foundation, a non-profit organization that also hosts a range of other projects.
You can support our work with a donation.


Page Info - https://www.wikipedia.org/
General
Media
Permissions
Security
Wikipedia - Mozilla Firefox
https://www.wikipedia.org
Pictures
Videos
Downloads

Website Identity
Website: **www.wikipedia.org**
Owner: **This website does not supply ownership information.**
Verified by: **DigiCert Inc**
Expires on: **18 October 2025**

Privacy & History
Have I visited this website prior to today? **No**
Is this website storing information (cookies) on my computer? **Yes**
Have I saved any passwords for this website? **No**

Technical Details
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, 256 b
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling b
computers. It is therefore unlikely that anyone read this page as it traveled across the

Certificate Viewer: "*.wikipedia.org"

General Details

Certificate Hierarchy

```
▾ DigiCert Global Root CA
  ▾ DigiCert TLS Hybrid ECC SHA384 2020 CA1
      *.wikipedia.org
```

Certificate Fields

```
▾ *.wikipedia.org
  ▾ Certificate
      Version
      Serial Number
      Certificate Signature Algorithm
      Issuer
    ▾ Validity
        Not Before
        Not After
      Subject
    ▾ Subject Public Key Info
```

Field Value

Q6: On the details tab, find the value of the following files:
C1.pub - 47 59 81 7f d4 1b 1f b0 71 f6 98 5d 18 ba 98 47 98 b0 7e 76 2b ea ff 1a 8b ac 26 b3
42 8d 31 e6 4a e8 19 d0 ef da 14 e7 d7 14 92 a1 92 f2 a7 2e 2d af fb 1d f6 fb 53 b0 8a 3f fc d8
16 0a e9 b0 2e b6 a5 0b 18 90 35 26 a2 da f6 a8 b7 32 fc 95 23 4b c6 45 b9 c4 cf e4 7c ee e6
c9 f8 90 bd 72 e3 99 c3 1d 0b 05 7c 6a 97 6d b2 ab 02 36 d8 c2 bc 2c 01 92 3f 04 a3 8b 75 11
c7 b9 29 bc 11 d0 86 ba 92 bc 26 f9 65 c8 37 cd 26 f6 86 13 0c 04 aa 89 e5 78 b1 c1 4e 79 bc

```
76 a3 0b 51 e4 c5 d0 9e 6a fe 1a 2c 56 ae 06 36 27 a3 73 1c 08 7d 93 32 d0 c2 44 19 da 8d f4
0e 7b 1d 28 03 2b 09 8a 76 ca 77 dc 87 7a ac 7b 52 26 55 a7 72 0f 9d d2 88 4f fe b1 21 c5 1a
a1 aa 39 f5 56 db c2 84 c4 35 1f 70 da bb 46 f0 86 bf 64 00 c4 3e f7 9f 46 1b 9d 23 05 b9 7d b3
4f 0f a9 45 3a e3 74 30 98
C0.pub -  cb 9c 37 aa 48 13 12 0a fa dd 44 9c 4f 52 b0 f4 df ae 04 f5 79 79 08 a3 24 18 fc 4b 2b
84 c0 2d b9 d5 c7 fe f4 c1 1f 58 cb b8 6d 9c 7a 74 e7 98 29 ab 11 b5 e3 70 a0 a1 cd 4c 88 99
93 8c 91 70 e2 ab 0f 1c be 93 a9 ff 63 d5 e4 07 60 d3 a3 bf 9d 5b 09 f1 d5 8e e3 53 f4 8e 63 fa
3f a7 db b4 66 df 62 66 d6 d1 6e 41 8d f2 2d b5 ea 77 4a 9f 9d 58 e2 2b 59 c0 40 23 ed 2d 28
82 45 3e 79 54 92 26 98 e0 80 48 a8 37 ef f0 d6 79 60 16 de ac e8 0e cd 6e ac 44 17 38 2f 49
da e1 45 3e 2a b9 36 53 cf 3a 50 06 f7 2e e8 c4 57 49 6c 61 21 18 d5 04 ad 78 3c 2c 3a 80 6b
a7 eb af 15 14 e9 d8 89 c1 b9 38 6c e2 91 6c 8a ff 64 b9 77 25 57 30 c0 1b 24 a3 e1 dc e9 df
47 7c b5 b4 24 08 05 30 ec 2d bd 0b bf 45 bf 50 b9 a9 f3 eb 98 01 12 ad c8 88 c6 98 34 5f 8d
0a 3c c6 e9 d5 95 95 6d de
c0Sign - 30 66 02 31 00 9f c9 b3 cf bb 57 80 ee 68 08 d9 48 dd 0b 6e be 47 c4 a7 ba 8b 38 11
ad f9 7b 86 08 0c ef b8 67 cd bb e2 5d 07 22 96 83 19 5b f9 8e 25 73 d8 24 02 31 00 d5 5f 33
db 30 db a0 f7 3d 03 e3 ae 1c c1 59 ce b7 dc 80 be b5 c2 67 03 75 16 0e c9 f9 6d 6e b3 46 a1
24 cf 7a 05 37 d9 84 e6 35 66 28 99 76 2b
```