Self-Signed SSL Certificate with OPENSSL In Kali Linux

OpenSSL Self-Signed SSL Certificate is open-source command tool that is commonly used to **generate private keys, create CSRs, install your SSL certificate, and identify certificate information**.

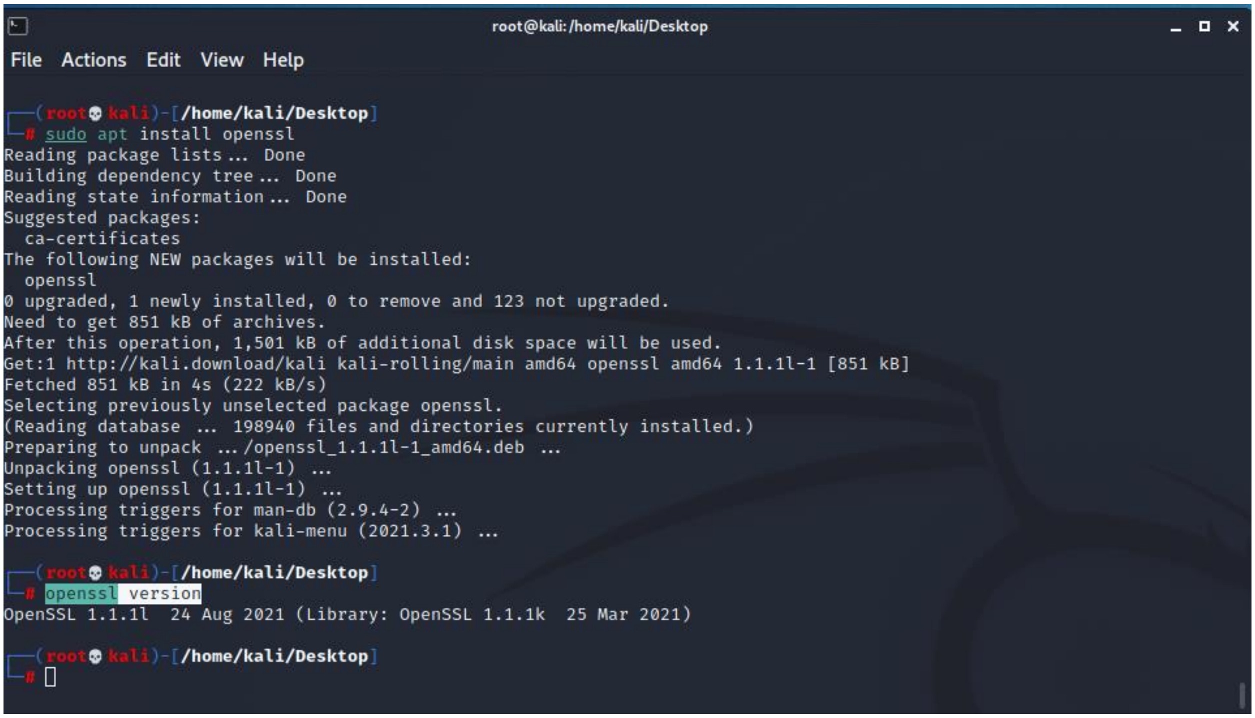
To create a Self-Signed certificate on kali you need to be on the root system in order to generate.

First, check whether the openssl package is installed on your Linux system,

(openssl version)

Or run the following command to install

(sudo apt install openssl)



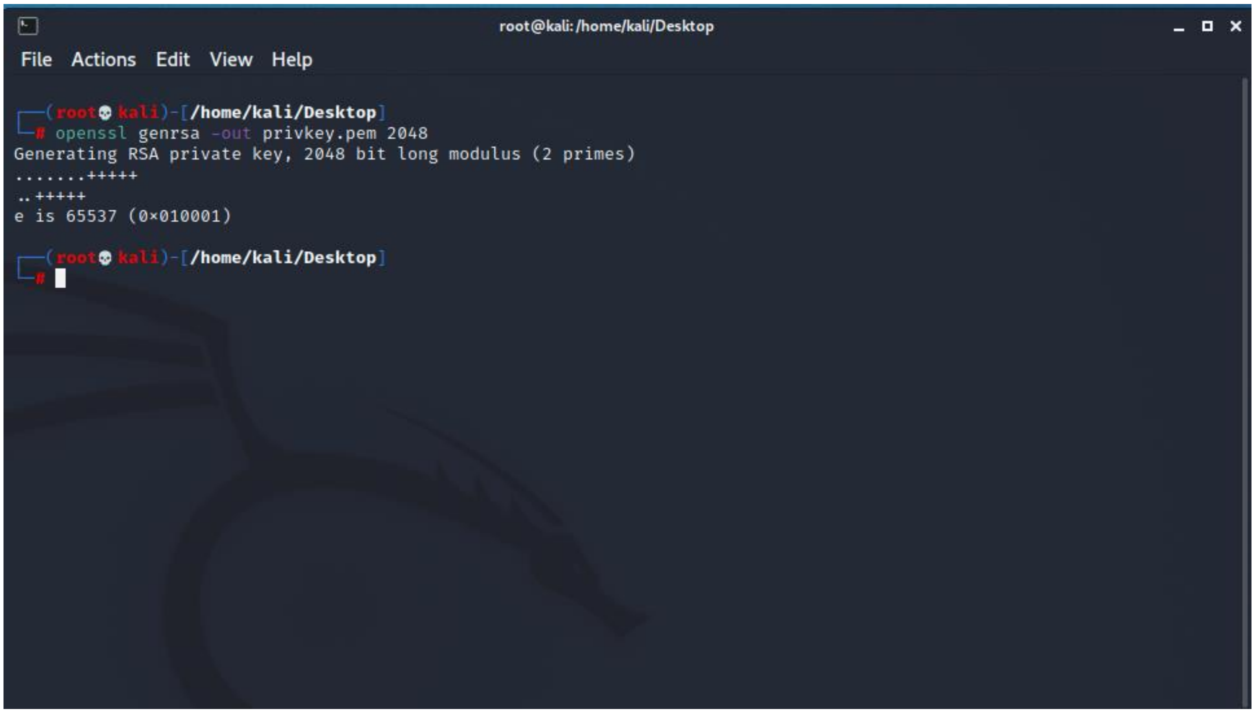
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# sudo apt install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  ca-certificates
The following NEW packages will be installed:
  openssl
0 upgraded, 1 newly installed, 0 to remove and 123 not upgraded.
Need to get 851 kB of archives.
After this operation, 1,501 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 openssl amd64 1.1.1l-1 [851 kB]
Fetched 851 kB in 4s (222 kB/s)
Selecting previously unselected package openssl.
(Reading database ... 198940 files and directories currently installed.)
Preparing to unpack .../openssl_1.1.1l-1_amd64.deb ...
Unpacking openssl (1.1.1l-1) ...
Setting up openssl (1.1.1l-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.3.1) ...

┌──(root💀kali)-[/home/kali/Desktop]
└─# openssl version
OpenSSL 1.1.1l  24 Aug 2021 (Library: OpenSSL 1.1.1k  25 Mar 2021)

┌──(root💀kali)-[/home/kali/Desktop]
└─# ▯
```

Ones have everything installed, follow the steps to generate the certificate

Step 1 – Generate a Private RSA Key

To do so run the command:

“openssl genrsa -out privkey.pem 2048”

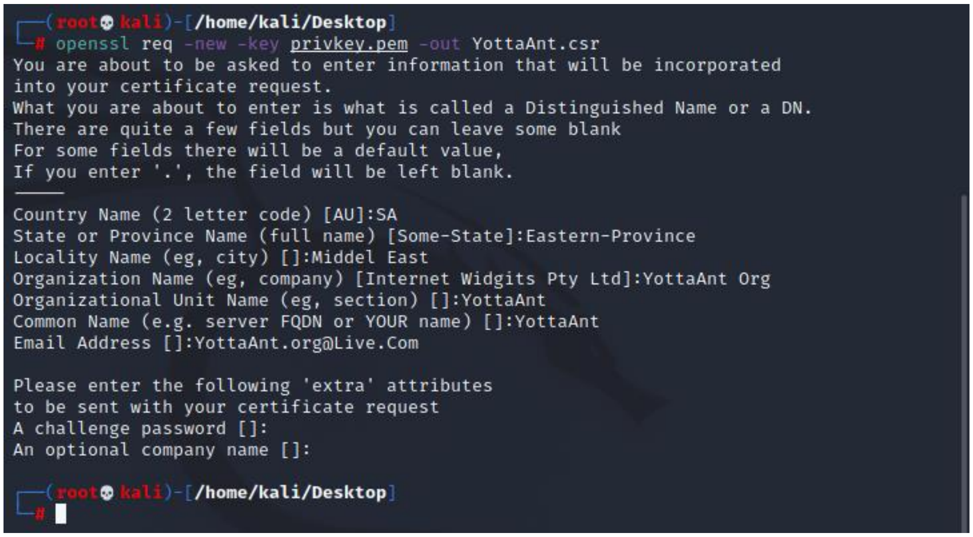


```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# openssl genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.......+++++
..+++++
e is 65537 (0×010001)

┌──(root💀 kali)-[/home/kali/Desktop]
└─# 
```

Step 2 – Generate CSR with Key

generate CSR (Certificate Signing Request) with above created private key.

Command:” openssl req -new -key privkey.pem -out YottaAnt.csr”

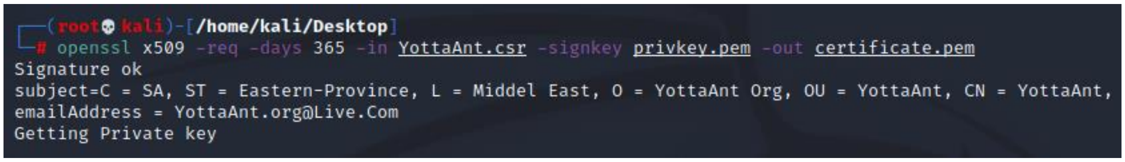


```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# openssl req -new -key privkey.pem -out YottaAnt.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
─────
Country Name (2 letter code) [AU]:SA
State or Province Name (full name) [Some-State]:Eastern-Province
Locality Name (eg, city) []:Middel East
Organization Name (eg, company) [Internet Widgits Pty Ltd]:YottaAnt Org
Organizational Unit Name (eg, section) []:YottaAnt
Common Name (e.g. server FQDN or YOUR name) []:YottaAnt
Email Address []:YottaAnt.org@Live.Com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

┌──(root💀 kali)-[/home/kali/Desktop]
└─# 
```

Step 3 – Sign the CSR with Key

signing the certificate request with the same key that was used to create it.

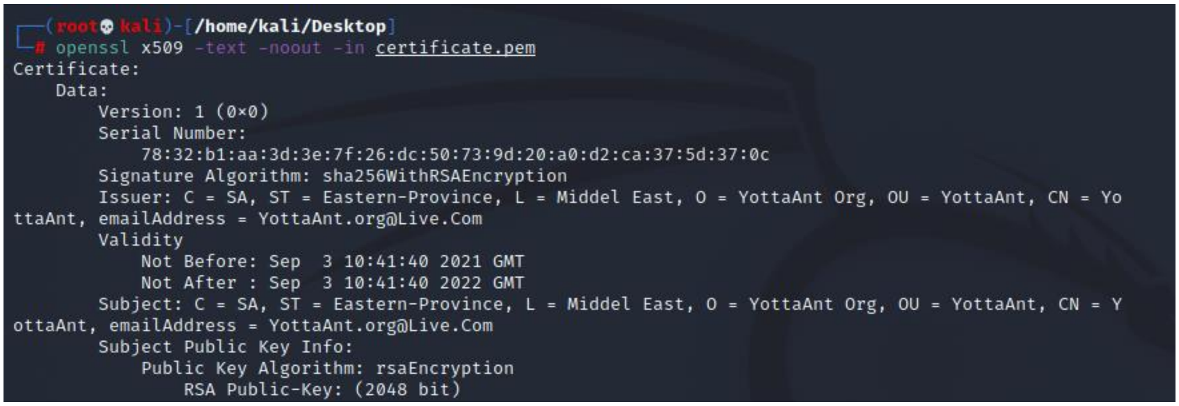
Command “openssl x509 -req -days 365 -in YottaAnt.csr -signkey privkey.pem -out certificate.pem”



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# openssl x509 -req -days 365 -in YottaAnt.csr -signkey privkey.pem -out certificate.pem
Signature ok
subject=C = SA, ST = Eastern-Province, L = Middel East, O = YottaAnt Org, OU = YottaAnt, CN = YottaAnt,
emailAddress = YottaAnt.org@Live.Com
Getting Private key
```

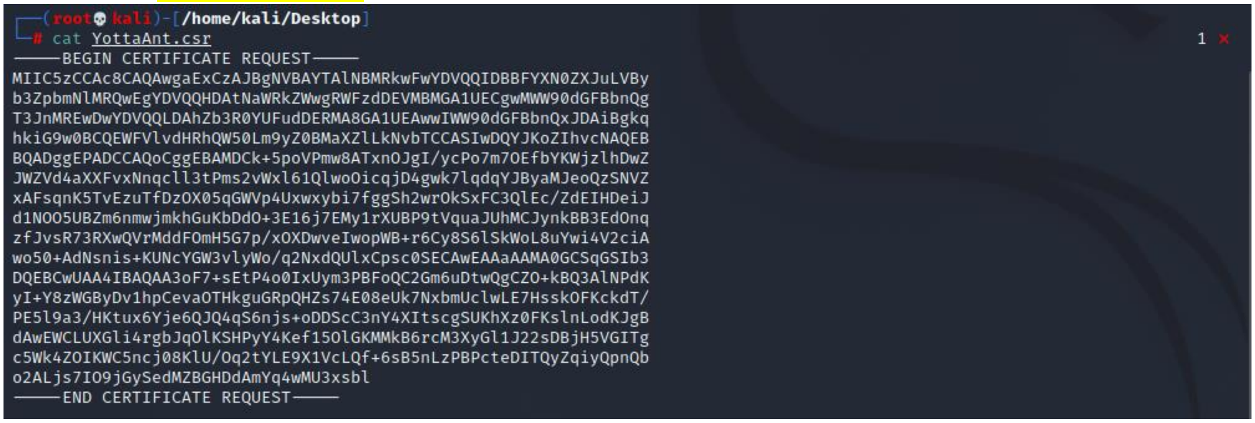
To look and verify the details of the certificate use the command

openssl x509 -text -noout -in certificate.pem



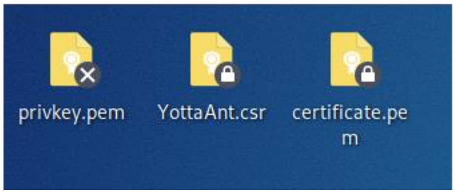
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# openssl x509 -text -noout -in certificate.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            78:32:b1:aa:3d:3e:7f:26:dc:50:73:9d:20:a0:d2:ca:37:5d:37:0c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = SA, ST = Eastern-Province, L = Middel East, O = YottaAnt Org, OU = YottaAnt, CN = Yo
ttaAnt, emailAddress = YottaAnt.org@Live.Com
        Validity
            Not Before: Sep  3 10:41:40 2021 GMT
            Not After : Sep  3 10:41:40 2022 GMT
        Subject: C = SA, ST = Eastern-Province, L = Middel East, O = YottaAnt Org, OU = YottaAnt, CN = Y
ottaAnt, emailAddress = YottaAnt.org@Live.Com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
```

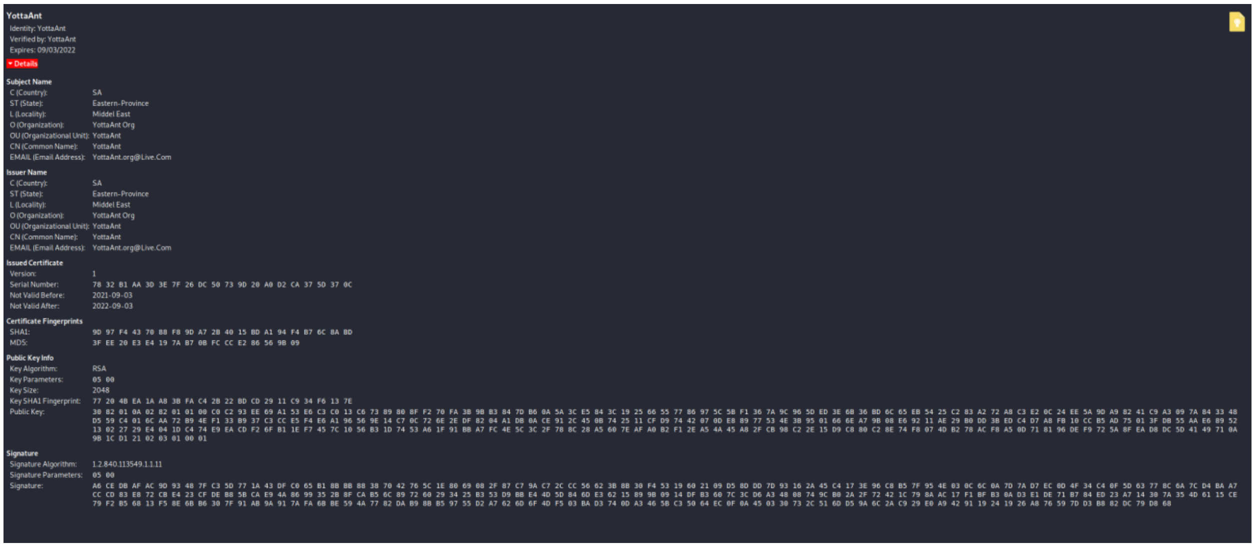
Command “cat YottaAnt.csr”



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# cat YottaAnt.csr                                                                              1 ×
-----BEGIN CERTIFICATE REQUEST-----
MIIC5zCCAc8CAQAwgaExCzAJBgNVBAYTAlNBMRkwFwYDVQQIDBBFYXN0ZXJuLVBy
b3ZpbmNlMRQwEgYDVQQHDAtNaWRkZWwgRWFzdDEVMBMGA1UECgwMWW90dGFBbnQg
T3JnMREwDwYDVQQLDAhZb3R0YUFudDERMA8GA1UEAwwIWW90dGFBbnQxJDAiBgkq
hkiG9w0BCQEWFVlvdHRhQW50Lm9yZ0BMaXZlLkNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMDCk+5poVPmw8ATxnOJgI/ycPo7m7OEfbYKWjzlhDwZ
JWZVd4aXXFvxNnqcll3tPms2vWxl61QlwoOicqjD4gwk7lqdqYJByaMJeoQzSNVZ
xAFsqnK5TvEzuTfDzOX05qGWVp4Uxwxybi7fggSh2wrOkSxFC3QlEc/ZdEIHDeiJ
d1NOO5UBZm6nmwjmkhGuKbDdO+3E16j7EMy1rXUBP9tVquaJUhMCJynkBB3EdOnq
zfJvsR73RXwQVrMddFOmH5G7p/xOXDwveIwopWB+r6Cy8S6lSkWoL8uYwi4V2ciA
wo50+AdNsnis+KUNcYGW3vlyWo/q2NxdQUlxCpsc0SECAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAA3oF7+sEtP4o0IxUym3PBFoQC2Gm6uDtwQgCZO+kBQ3AlNPdK
yI+Y8zWGByDv1hpCevaOTHkguGRpQHZs74E08eUk7NxbmUclwLE7HsskOFKckdT/
PE5l9a3/HKtux6Yje6QJQ4qS6njs+oDDScC3nY4XItscgSUKhXz0FKslnLodKJgB
dAwEWCLUXGli4rgbJqOlKSHPyY4Kef15OlGKMMkB6rcM3XyGl1J22sDBjH5VGITg
c5Wk4ZOIKWC5ncj08KlU/Oq2tYLE9X1VcLQf+6sB5nLzPBPcteDITQyZqiyQpnQb
o2ALjs7IO9jGySedMZBGHDdAmYq4wMU3xsbl
-----END CERTIFICATE REQUEST-----
```

Self-Signed SSL Certificate with OPENSSL





```
YottaAnt
  Identity: YottaAnt
  Verified by: YottaAnt
  Expires: 09/03/2022
▾ Details

Subject Name
  C (Country):                  SA
  ST (State):                   Eastern-Province
  L (Locality):                 Middel East
  O (Organization):             YottaAnt Org
  OU (Organizational Unit):     YottaAnt
  CN (Common Name):             YottaAnt
  EMAIL (Email Address):        YottaAnt.org@Live.Com

Issuer Name
  C (Country):                  SA
  ST (State):                   Eastern-Province
  L (Locality):                 Middel East
  O (Organization):             YottaAnt Org
  OU (Organizational Unit):     YottaAnt
  CN (Common Name):             YottaAnt
  EMAIL (Email Address):        YottaAnt.org@Live.Com

Issued Certificate
  Version:                      1
  Serial Number:                78 32 B1 AA 3D 3E 7F 26 DC 50 73 9D 20 A0 D2 CA 37 5D 37 0C
  Not Valid Before:             2021-09-03
  Not Valid After:              2022-09-03

Certificate Fingerprints
  SHA1:                         9D 97 F4 43 70 88 F8 9D A7 2B 40 15 BD A1 94 F4 B7 6C 8A BD
  MD5:                          3F EE 20 E3 E4 19 7A B7 0B FC CC E2 86 56 9B 09

Public Key Info
  Key Algorithm:                RSA
  Key Parameters:               05 00
  Key Size:                     2048
  Key SHA1 Fingerprint:         77 20 4B EA 1A A8 3B FA C4 2B 22 BD CD 29 11 C9 34 F6 13 7E
  Public Key:                   30 82 01 0A 02 82 01 01 00 C0 C2 93 EE 69 A1 53 E6 C3 C0 13 C6 73 89 80 8F F2 70 FA 3B 9B B3 84 7D B6 0A 5A 3C E5 84 3C 19 25 66 55 77 86 97 5C 5B F1 36 7A 9C 96 5D ED 3E 6B 36 BD 6C 65 EB 54 25 C2 83 A2 72 A8 C3 E2 0C 24 EE 5A 9D A9 82 41 C9 A3 09 7A 84 33 48
                                D5 59 C4 01 6C AA 72 B9 4E F1 33 B9 37 C3 CC E5 F4 E6 A1 96 56 9E 14 C7 0C 72 6E 2E DF 82 04 A1 DB 0A CE 91 2C 45 0B 74 25 11 CF D9 74 42 07 0D E8 89 77 53 4E 3B 95 01 66 6E A7 9B 08 E6 92 11 AE 29 B0 DD 3B ED C4 D7 A8 FB 10 CC B5 AD 75 01 3F D8 55 AA E6 89 52
                                13 02 27 29 E4 04 1D C4 74 E9 EA CD F2 6F B1 1E F7 45 7C 10 56 B3 1D 74 53 A6 1F 91 BB A7 FC 4E 5C 3C 2F 78 8C 28 A5 60 7E AF A0 B2 F1 2E A5 4A 45 A8 2F CB 98 C2 2E 15 D9 C8 80 C2 8E 74 F8 07 4D B2 78 AC F8 A5 0D 71 81 96 DE F9 72 5A 8F EA D8 DC 5D 41 49 71 0A
                                9B 1C D1 21 02 03 01 00 01

Signature
  Signature Algorithm:          1.2.840.113549.1.1.11
  Signature Parameters:         05 00
  Signature:                    A6 CE DB AF AC 9D 93 48 7F C3 5D 77 1A 43 DF C0 65 B1 8B BB 88 38 70 42 76 5C 1E 80 69 08 2F 87 C7 9A C7 2C CC 56 62 3B 8B 30 F4 53 19 60 21 09 D5 8D DD 7D 93 16 2A 45 C4 17 3E 96 C8 B5 7F 95 4E 03 0C 6C 0A 7D 7A D7 EC 0D 4F 34 C4 0F 5D 63 77 8C 6A 7C D4 BA A7
                                CC CD 83 E8 72 CB E4 23 CF DE B8 5B CA E9 4A 86 99 35 2B 8F CA B5 6C 89 72 60 29 34 25 B3 53 D9 BB E4 4D 5D 84 6D E3 62 15 89 9B 09 14 DF B3 60 7C 3C D6 A3 48 08 74 9C B0 2A 2F 72 42 1C 79 8A AC 17 F1 BF B3 0A D3 E1 DE 71 B7 84 ED 23 A7 14 30 7A 35 4D 61 15 CE
                                79 F2 B5 68 13 F5 8E 6B B6 30 7F 91 AB 9A 91 7A FA 6B 8E 59 4A 77 82 DA B9 8B B5 97 55 D2 A7 62 6D 6F 4D F5 03 BA D3 74 0D A3 46 5B C3 50 64 EC 0F 0A 45 03 30 73 2C 51 6D D5 9A 6C 2A C9 29 E0 A9 42 91 19 24 19 26 A8 76 59 7D D3 B8 82 DC 79 D8 68
```