CSR Decoder and Certificate Decoder

Find and track your certs with CertAlert (https://www.redkestrel.co.uk/products/certalert/)

```
-----BEGIN CERTIFICATE REQUEST-----
MIICwzCCAasCAQAwfjELMAkGA1UEBgwCQkQxDjAMBgNVBAgMBURoYWthMQ8wDQYD
VQQHDAZoamhqaGoxDDAKBgNVBAoMA0JDQzEOMAwGA1UECwwFa2pramsxETAPBgNV
BAMMCFNpZGRpcXVyMQ0wCwYDVQQREwQxMjA3MQ4wDAYDVQQFEwU2MzE4MzCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK8Z0zNJYqR0bNocVw/V2LkSBhI0
sGW6HmmCuzv4N5StbkafAl5IMsgzABKDHJUL07ll7SaPmHyju0koFxlq4iwoTq+U
QDr3rof9gtWK3YAik/ZBomWCT16gpVKT/mER1/M0/9jyT77eYdQcTU9jEvpYJ1Z7
ploUGw5DOeM/+GYYP228iBZh3rWe9k9jaGbmW9jNLCwMAu90bjV3N+eMhDcOSklN
YFSa1S8+4O9XWjTWZwvf2TRwyOYIqTeeWC2atHkX7FOBtUIvouVTxLZoAxsTqjUz
sHg3Y6OjSk4PHPaHFzKI7A4GuJs4zmoSWggtrEVQsoBXLBXPwAJ32K3XazsCAwEA
AaAAMA0GCSqGSIb3DQEBCwUAA4IBAQCdvmPMBhXTXSBf07Wzn8PnH3zN1ve0QO++
Jb4zwMsprS7q6YgEM5sm04dpC+pbQoBOHBqs/m42KY/EYSmflYc5iXqZtcuzC1La
KrpxhSJ3X43TkiT/khedSCdaw2nBdq0oQD0zbV9ARCWFTDAPQTPdj4qmr21NnbdS
QB7PtX2iRh4IqNvTXT06sCBYfZ5qO50OcoaOHTcTFl9fGOYEAXBhnrdmjlINMMEk
7u1hwKJaCIwJRb60RhFcUPcpVJM/iztNzjKdNvgxZx6PrVp3DsT9Cj1/Uj4ZIjDC
QcksVwWu+WdCt9yvBglt15DmFiBPuuzEn80zpEdyEakKLLqW4CWv
```

Select File...

Decode

CSR Summary

CSR Checks

Check	Result
Debian Weak Key	PASSED - Does not use a key on our blacklist - this is good
Key Size	PASSED (2048 bits)
Signature	PASSED - CSR has a valid signature
MD5	PASSED - Not using the MD5 algorithm

CSR Subject

serialNumber	63183

postalCode	1207
Common Name (CN)	Siddiqur
Organizational Unit (OU)	kjkjk
Organization (O)	BCC
Locality (L)	hjhjhj
State (ST)	Dhaka
Country (C)	BD

CSR Properties

Subject	C=BD, ST=Dhaka, L=hjhjhj, O=BCC, OU=kjkjk, CN=Siddiqur, postalCode=1207, serialNumber=63183
Key Size	2048 bits
Key Algorithm	RSA
Sig. Algorithm	sha256WithRSAEncryption
SHA256 Fingerprint	14:5D:F5:83:79:E6:7C:14:C1:B4:9A:F1:04:78:86:FE:95:B3:5C:5D:83:A4:92:01:54:00:A6:51:5B:F3:F8:B0
SHA1 Fingerprint	F7:B5:4F:26:25:6E:75:FD:49:6A:78:DB:1F:30:3D:9F:8D:C6:85:C7
MD5 Fingeprint	02:5C:3B:56:9D:DC:E0:90:7C:D2:BF:4D:42:4A:96:3B
SANs	

CSR Detailed Information

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=BD, ST=Dhaka, L=hjhjhj, O=BCC, OU=kjkjk, CN=Siddiqur/postalCode=1207/seria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:af:19:d3:33:49:62:a4:74:6c:da:1c:57:0f:d5:
                    d8:b9:12:06:12:34:b0:65:ba:1e:69:82:bb:3b:f8:
                    37:94:ad:6e:46:9f:02:5e:48:32:c8:33:00:12:83:
                    1c:95:0b:d3:b9:65:ed:26:8f:98:7c:a3:bb:49:28:
                    17:19:6a:e2:2c:28:4e:af:94:40:3a:f7:ae:87:fd:
                    82:d5:8a:dd:80:22:93:f6:41:a2:65:82:4f:5e:a0:
                    a5:52:93:fe:61:11:d7:f3:34:ff:d8:f2:4f:be:de:
                    61:d4:1c:4d:4f:63:12:fa:58:27:56:7b:a6:5a:14:
                    1b:0e:43:39:e3:3f:f8:66:18:3f:6d:bc:88:16:61:
                    de:b5:9e:f6:4f:63:68:66:e6:5b:d8:cd:2c:2c:0c:
                    02:ef:74:6e:35:77:37:e7:8c:84:37:0e:4a:49:4d:
                    60:54:9a:d5:2f:3e:e0:ef:57:5a:34:d6:67:0b:df:
                    d9:34:70:c8:e6:08:a9:37:9e:58:2d:9a:b4:79:17:
                    ec:53:81:b5:42:2f:a2:e5:53:c4:b6:68:03:1b:13:
                    aa:35:33:b0:78:37:63:a3:a3:4a:4e:0f:1c:f6:87:
                    17:32:88:ec:0e:06:b8:9b:38:ce:6a:12:5a:08:2d:
                    ac:45:50:b2:80:57:2c:15:cf:c0:02:77:d8:ad:d7:
                    6b:3b
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         9d:be:63:cc:06:15:d3:5d:20:5f:d3:b5:b3:9f:c3:e7:1f:7c:
         cd:d6:f7:b4:40:ef:be:25:be:33:c0:cb:29:ad:2e:ea:e9:88:
         04:33:9b:26:d3:87:69:0b:ea:5b:42:80:4e:1c:1a:ac:fe:6e:
         36:29:8f:c4:61:29:9f:95:87:39:89:7a:99:b5:cb:b3:0b:52:
         da:2a:ba:71:85:22:77:5f:8d:d3:92:24:ff:92:17:9d:48:27:
         5a:c3:69:c1:76:ad:28:40:3d:33:6d:5f:40:44:25:85:4c:30:
         0f:41:33:dd:8f:8a:a6:af:6d:4d:9d:b7:52:40:1e:cf:b5:7d:
         a2:46:1e:08:a8:db:d3:5d:3d:3a:b0:20:58:7d:9e:6a:3b:9d:
         0e:72:86:8e:1d:37:13:16:5f:5f:18:e6:04:01:70:61:9e:b7:
         66:8e:52:0d:30:c1:24:ee:ed:61:c0:a2:5a:08:8c:09:45:be:
         b4:46:11:5c:50:f7:29:54:93:3f:8b:3b:4d:ce:32:9d:36:f8:
         31:67:1e:8f:ad:5a:77:0e:c4:fd:0a:3d:7f:52:3e:19:22:30:
         c2:41:c9:2c:57:05:ae:f9:67:42:b7:dc:af:06:09:6d:d7:90:
         e6:16:20:4f:ba:ec:c4:9f:cd:33:a4:47:72:11:a9:0a:2c:ba:
         96:e0:25:af


(Decoded using the following version of OpenSSL: OpenSSL 1.1.1b  26 Feb 2019)
```

CSR ASN.1 Information

```
  0 707: SEQUENCE {
  4 427:   SEQUENCE {
  8   1:     INTEGER 0
 11 126:     SEQUENCE {
 13  11:       SET {
 15   9:         SEQUENCE {
 17   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 22   2:           UTF8String 'BD'
       :           }
       :         }
 26  14:       SET {
 28  12:         SEQUENCE {
 30   3:           OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
 35   5:           UTF8String 'Dhaka'
       :           }
       :         }
 42  15:       SET {
 44  13:         SEQUENCE {
 46   3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 51   6:           UTF8String 'hjhjhj'
       :           }
       :         }
 59  12:       SET {
 61  10:         SEQUENCE {
 63   3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 68   3:           UTF8String 'BCC'
       :           }
       :         }
 73  14:       SET {
 75  12:         SEQUENCE {
 77   3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82   5:           UTF8String 'kjkjk'
       :           }
       :         }
 89  17:       SET {
 91  15:         SEQUENCE {
 93   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 98   8:           UTF8String 'Siddiqur'
       :           }
       :         }
108  13:       SET {
110  11:         SEQUENCE {
112   3:           OBJECT IDENTIFIER postalCode (2 5 4 17)
117   4:           PrintableString '1207'
       :           }
       :         }
123  14:       SET {
125  12:         SEQUENCE {
127   3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
132   5:           PrintableString '63183'
       :           }
       :         }
       :       }
139 290:     SEQUENCE {
143  13:       SEQUENCE {
145   9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
156   0:         NULL
       :         }
158 271:       BIT STRING
```

```
       :         30 82 01 0A 02 82 01 01 00 AF 19 D3 33 49 62 A4
       :         74 6C DA 1C 57 0F D5 D8 B9 12 06 12 34 B0 65 BA
       :         1E 69 82 BB 3B F8 37 94 AD 6E 46 9F 02 5E 48 32
       :         C8 33 00 12 83 1C 95 0B D3 B9 65 ED 26 8F 98 7C
       :         A3 BB 49 28 17 19 6A E2 2C 28 4E AF 94 40 3A F7
       :         AE 87 FD 82 D5 8A DD 80 22 93 F6 41 A2 65 82 4F
       :         5E A0 A5 52 93 FE 61 11 D7 F3 34 FF D8 F2 4F BE
       :         DE 61 D4 1C 4D 4F 63 12 FA 58 27 56 7B A6 5A 14
       :                 [ Another 142 bytes skipped ]
       :       }
433   0:     [0]
       :       Error: Object has zero length.
       :     }
435  13:   SEQUENCE {
437   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
448   0:     NULL
       :     }
450 257:   BIT STRING
       :     9D BE 63 CC 06 15 D3 5D 20 5F D3 B5 B3 9F C3 E7
       :     1F 7C CD D6 F7 B4 40 EF BE 25 BE 33 C0 CB 29 AD
       :     2E EA E9 88 04 33 9B 26 D3 87 69 0B EA 5B 42 80
       :     4E 1C 1A AC FE 6E 36 29 8F C4 61 29 9F 95 87 39
       :     89 7A 99 B5 CB B3 0B 52 DA 2A BA 71 85 22 77 5F
       :     8D D3 92 24 FF 92 17 9D 48 27 5A C3 69 C1 76 AD
       :     28 40 3D 33 6D 5F 40 44 25 85 4C 30 0F 41 33 DD
       :     8F 8A A6 AF 6D 4D 9D B7 52 40 1E CF B5 7D A2 46
       :             [ Another 128 bytes skipped ]
       :   }
```

CSR Hex Encoded

```
308202c3308201ab020100307e310b300906035504060c024244310e300c0603
5504080c054468616b61310f300d06035504070c06686a686a686a310c300a06
0355040a0c03424343310e300c060355040b0c056b6a6b6a6b3111300f060355
04030c0853696464469717572310d300b060355041113043132303731 0e300c06
0355040513053633313833308201223 00d06092a864886f70d01010105000382
010f003082010a0282010100af19d3334962a4746cda1c570fd5d8b912061234
b065ba1e6982bb3bf83794ad6e469f025e4832c8330012831c950bd3b965ed26
8f987ca3bb492817196ae22c284eaf94403af7ae87fd82d58add802293f641a2
65824f5ea0a55293fe6111d7f334ffd8f24fbede61d41c4d4f6312fa5827567b
a65a141b0e4339e33ff866183f6dbc881661deb59ef64f636866e65bd8cd2c2c
0c02ef746e357737e78c84370e4a494d60549ad52f3ee0ef575a34d6670bdfd9
3470c8e608a9379e582d9ab47917ec5381b5422fa2e553c4b668031b13aa3533
b0783763a3a34a4e0f1cf687173288ec0e06b89b38ce6a125a082dac4550b280
572c15cfc00277d8add76b3b0203010001a000300d06092a864886f70d01010b
050003820101009dbe63cc0615d35d205fd3b5b39fc3e71f7ccdd6f7b440efbe
25be33c0cb29ad2eeae98804339b26d387690bea5b42804e1c1aacfe6e36298f
c461299f958739897a99b5cbb30b52da2aba718522775f8dd39224ff92179d48
275ac369c176ad28403d336d5f404425854c300f4133dd8f8aa6af6d4d9db752
401ecfb57da2461e08a8dbd35d3d3ab020587d9e6a3b9d0e72868e1d3713165f
5f18e6040170619eb7668e520d30c124eeed61c0a25a088c0945beb446115c50
f72954933f8b3b4dce329d36f831671e8fad5a770ec4fd0a3d7f523e192230c2
41c92c5705aef96742b7dcaf06096dd790e616204fbaecc49fcd33a4477211a9
0a2cba96e025af
```