CSR Decoder and Certificate Decoder

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCBpQIBADBrMQswCQYDVQQGDAJCRDEOMAwGA1UECAwFRGhha2ExDjAMBgNV
BAcMBURoYWthMQwwCgYDVQQKDANCQ0MxCzAJBgNVBAsMAkNBMREwDwYDVQQDDAhT
aWRkaXF1cjEOMAwGA1UEBRMFNjMxNjgwMTANBgkqhkiG9w0BAQEFAAMgADAdAgAC
GRyjD8kR1ISaAAUCtSEiAgAAAAAAAAqAACgADANBgkqhkiG9w0BAQsFAAOCAQEA
frpHw9yVPsfNkWZEBd9GGSWxZl082F9oOjUSXXiKsUmUwerjZ2FIp2QN9fFXFOjj
5a32FYRUE4TjBe7fm9k2FYwWKsrKA9enKzvtUhX2Bb2FTEiG6iz4HWlRU0P85msk
vlHYWtYWd0q3lXMQ0Q572Bw5iM0yuh882Byv3p3vHWeYnDaElm51HtsBZlwUZxRw
mMI3gF8zk2FdwNlt4mWU2jidRvlYx0DQAk1tARxFBDHEEdxcZu7x2BN2XpXGDQ3L
brB31zhQjR0TSwvBTlv1Bmvla05bMxH30M92BgjZrHzVX0gyv2BEiMgpZ3w2PiAg
Lvg2BG5k66SFj0otlc42BoBkDXQFV6yc5r9Q3D3D
-----END CERTIFICATE REQUEST-----
```

Select File...

Decode

CSR Summary

CSR Checks

Check	Result
Debian Weak Key	Unable to check
Key Size	WARNING (0 bits)
Signature	FAILED - CSR has an invalid signature
MD5	PASSED - Not using the MD5 algorithm

CSR Subject

serialNumber	63168
Common Name (CN)	Siddiqur
Organizational Unit (OU)	CA
Organization (O)	BCC
Locality (L)	Dhaka
State (ST)	Dhaka
Country (C)	BD

CSR Properties

Subject	C=BD, ST=Dhaka, L=Dhaka, O=BCC, OU=CA, CN=Siddiqur, serialNumber=63168
Key Size	0 bits
Key Algorithm	RSA
Sig. Algorithm	sha256WithRSAEncryption
SHA256 Fingerprint	1A:69:04:76:BB:67:95:25:80:36:2A:00:69:0F:29:46:86:49:EF:79:42:2D:07:30:F7:D4:0F:93:8E:F6:10:71
SHA1 Fingerprint	44:AE:44:C3:90:8A:DF:12:32:21:54:48:BD:08:F4:B6:AE:D5:AE:60
MD5 Fingeprint	B4:94:C1:AB:A2:B1:D5:FF:82:E2:22:39:29:B5:A9:9E
SANs	

CSR Detailed Information

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=BD, ST=Dhaka, L=Dhaka, O=BCC, OU=CA, CN=Siddiqur/serialNumber=63168
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (0 bit)
                Modulus: 0
                Exponent:
                    1c:a3:0f:c9:11:d4:84:9a:00:05:02:b5:21:22:02:
                    00:00:00:00:00:00:00:2a:00:00
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         7e:ba:47:c3:dc:95:3e:c7:cd:91:66:44:05:df:46:19:25:b1:
         66:5d:3c:d8:5f:68:3a:35:12:5d:78:8a:b1:49:94:c1:ea:e3:
         67:61:48:a7:64:0d:f5:f1:57:14:e8:e3:e5:ad:f6:15:84:54:
         13:84:e3:05:ee:df:9b:d9:36:15:8c:16:2a:ca:ca:03:d7:a7:
         2b:3b:ed:52:15:f6:05:bd:85:4c:48:86:ea:2c:f8:1d:69:51:
         53:43:fc:e6:6b:24:be:51:d8:5a:d6:16:77:4a:b7:95:73:10:
         d1:0e:7b:d8:1c:39:88:cd:32:ba:1f:3c:d8:1c:af:de:9d:ef:
         1d:67:98:9c:36:84:96:6e:75:1e:db:01:66:5c:14:67:14:70:
         98:c2:37:80:5f:33:93:61:5d:c0:d9:6d:e2:65:94:da:38:9d:
         46:f9:58:c7:40:d0:02:4d:6d:01:1c:45:04:31:c4:11:dc:5c:
         66:ee:f1:d8:13:76:5e:95:c6:0d:0d:cb:6e:b0:77:d7:38:50:
         8d:1d:13:4b:0b:c1:4e:5b:f5:06:6b:e5:6b:4e:5b:33:11:f7:
         d0:cf:76:06:08:d9:ac:7c:d5:5f:48:32:bf:60:44:88:c8:29:
         67:7c:36:3e:20:20:2e:f8:36:04:6e:64:eb:a4:85:8f:4a:2d:
         95:ce:36:06


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

CSR ASN.1 Information

```
  0 444: SEQUENCE {
  4 165:   SEQUENCE {
  7   1:     INTEGER 0
 10 107:     SEQUENCE {
 12  11:       SET {
 14   9:         SEQUENCE {
 16   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 21   2:           UTF8String 'BD'
       :           }
       :         }
 25  14:       SET {
 27  12:         SEQUENCE {
 29   3:           OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
 34   5:           UTF8String 'Dhaka'
       :           }
       :         }
 41  14:       SET {
 43  12:         SEQUENCE {
 45   3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 50   5:           UTF8String 'Dhaka'
       :           }
       :         }
 57  12:       SET {
 59  10:         SEQUENCE {
 61   3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 66   3:           UTF8String 'BCC'
       :           }
       :         }
 71  11:       SET {
 73   9:         SEQUENCE {
 75   3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 80   2:           UTF8String 'CA'
       :           }
       :         }
 84  17:       SET {
 86  15:         SEQUENCE {
 88   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 93   8:           UTF8String 'Siddiqur'
       :           }
       :         }
103  14:       SET {
105  12:         SEQUENCE {
107   3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
112   5:           PrintableString '63168'
       :           }
       :         }
       :       }
119  49:     SEQUENCE {
121  13:       SEQUENCE {
123   9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
134   0:         NULL
       :         }
136  32:       BIT STRING
       :         30 1D 02 00 02 19 1C A3 0F C9 11 D4 84 9A 00 05
       :         02 B5 21 22 02 00 00 00 00 00 00 00 2A 00 00
       :       }
170   0:     [0]
       :       Error: Object has zero length.
```

```
       :     }
172  13:   SEQUENCE {
174   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
185   0:     NULL
       :     }
187 257:   BIT STRING
       :     7E BA 47 C3 DC 95 3E C7 CD 91 66 44 05 DF 46 19
       :     25 B1 66 5D 3C D8 5F 68 3A 35 12 5D 78 8A B1 49
       :     94 C1 EA E3 67 61 48 A7 64 0D F5 F1 57 14 E8 E3
       :     E5 AD F6 15 84 54 13 84 E3 05 EE DF 9B D9 36 15
       :     8C 16 2A CA CA 03 D7 A7 2B 3B ED 52 15 F6 05 BD
       :     85 4C 48 86 EA 2C F8 1D 69 51 53 43 FC E6 6B 24
       :     BE 51 D8 5A D6 16 77 4A B7 95 73 10 D1 0E 7B D8
       :     1C 39 88 CD 32 BA 1F 3C D8 1C AF DE 9D EF 1D 67
       :             [ Another 128 bytes skipped ]
       :   }
```

CSR Hex Encoded

```
308201bc3081a5020100306b310b300906035504060c024244310e300c060355
04080c054468616b61310e300c06035504070c054468616b61310c300a060355
040a0c03424343310b3009060355040b0c0243413111300f06035504030c0853
6964646971757231 0e300c06035504051305363331363830313 00d06092a8648
86f70d0101010500032000301d020002191ca30fc911d4849a000502b5212202
000000000000002a0000a000300d06092a864886f70d01010b05000382010100
7eba47c3dc953ec7cd91664405df461925b1665d3cd85f683a35125d788ab149
94c1eae3676148a7640df5f15714e8e3e5adf61584541384e305eedf9bd93615
8c162acaca03d7a72b3bed5215f605bd854c4886ea2cf81d69515343fce66b24
be51d85ad616774ab7957310d10e7bd81c3988cd32ba1f3cd81cafde9def1d67
989c3684966e751edb01665c1467147098c237805f3393615dc0d96de26594da
389d46f958c740d0024d6d011c450431c411dc5c66eef1d813765e95c60d0dcb
6eb077d738508d1d134b0bc14e5bf5066be56b4e5b3311f7d0cf760608d9ac7c
d55f4832bf604488c829677c363e20202ef836046e64eba4858f4a2d95ce3606
80640d740557ac9ce6bf50dc3dc3
```