MANDIANT®

APT1

Exposing One of China's Cyber Espionage Units

APPENDIX F: APT1 SSL CERTIFICATES

For the full report visit
http://www.mandiant.com/apt1

APPENDIX F: APT1 SSL CERTIFICATES

The following self-signed X.509 certificates are used by APT1 to encrypt malware communications using SSL. Detection of these SSL certificates may indicate an APT1 malware infection.

VIRTUALLYTHERE

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Some-State, O=www.virtuallythere.com, OU=new, CN=new
        Validity
            Not Before: Oct 23 03:25:49 2007 GMT
            Not After : Oct 22 03:25:49 2008 GMT
        Subject: C=US, ST=Some-State, O=www.virtuallythere.com, OU=new, CN=new
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ee:48:13:76:f1:76:4b:6a:fe:6d:8c:5e:60:44:
                    19:b1:0a:b1:9e:bb:63:80:8f:c8:43:c8:73:ae:77:
                    4e:16:01:4e:8f:88:f8:a2:8c:4d:2e:b2:3d:6b:bd:
                    2e:cc:1b:b0:c3:5d:d6:a6:bc:1e:1a:31:b2:27:84:
                    64:9c:0b:b7:1e:b0:5e:82:96:e8:71:f6:ca:95:cf:
                    e1:40:bd:45:05:94:25:74:a0:90:ce:61:b9:8e:ba:
                    ed:aa:62:d4:10:79:68:eb:fb:31:63:0c:7b:11:2d:
                    8f:cf:57:a8:c4:6c:fd:77:c4:04:f5:46:84:e4:24:
                    c6:fe:dc:3a:06:9c:3e:ed:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                1B:C5:98:18:EB:D2:1F:3A:5B:F9:07:E0:BF:4E:C5:59:9E:FD:51:29
            X509v3 Authority Key Identifier:
                keyid:EA:D7:8A:29:DB:FB:0A:0C:C0:85:B3:BA:8A:C3:D7:80:95:26:11:90
                DirName:/C=US/ST=Some-State/O=www.virtuallythere.com/OU=new/CN=new
                serial:F2:1E:60:49:18:68:08:B6

    Signature Algorithm: sha1WithRSAEncryption
        b8:2c:50:58:a8:29:ce:d1:f3:02:a3:0c:9b:56:9f:45:24:f1:
        48:d3:53:88:d7:2e:61:67:aa:08:e4:7d:d5:50:62:ae:00:d5:
        1a:91:61:01:94:5e:ab:62:e8:53:a5:0d:6a:f4:41:81:ee:2b:
        60:8d:e2:a6:3a:12:2d:aa:08:a5:5a:f4:d2:9e:b2:43:38:57:
        f1:c1:45:54:33:d1:05:8c:e4:37:ad:00:a8:b3:92:3f:2d:21:
        a0:20:ea:0f:48:05:9f:2a:2c:88:da:eb:8b:12:bb:1d:73:85:
        4d:be:7e:36:ac:ad:6b:b4:ae:17:bf:06:d2:df:cd:a9:28:69:
        28:9e
```

IBM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 290 (0x122)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Some-State, O=Internet Widgits Pty Ltd, CN=IBM
```

```
        Validity
            Not Before: May 20 15:39:33 2009 GMT
            Not After : Feb 21 15:39:33 2016 GMT
        Subject: C=US, ST=Some-State, O=Internet Widgits Pty Ltd, CN=IBM
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
                Modulus (2048 bit):
                    00:d3:89:1c:10:09:d8:ec:74:2f:5c:1e:24:c0:89:
                    cd:02:2f:ad:13:fa:37:ea:9a:f9:73:ef:08:dd:3c:
                    6f:43:e3:21:69:f4:72:ff:43:72:c3:cc:1b:79:91:
                    01:c8:75:c9:7a:37:c0:82:a9:25:6e:0a:05:04:64:
                    fd:e2:9e:d9:2c:3d:f1:79:3a:c9:7b:b2:2d:8c:3e:
                    5d:c4:11:98:ac:1a:d4:fd:c0:4d:78:10:98:73:3a:
                    e0:88:a3:ab:a6:5c:6e:47:9a:21:b5:57:c3:a1:7d:
                    5e:f0:b6:6d:84:15:6a:cd:e8:62:31:0e:42:89:8f:
                    f5:1f:48:bc:b3:2d:87:cb:a4:e8:c9:a7:09:15:f6:
                    72:a0:ce:84:1c:29:e8:b0:ff:d5:3d:82:78:25:4b:
                    ef:d8:94:74:69:cc:a4:44:11:d5:97:13:c6:83:d6:
                    e7:8a:f9:a6:e0:71:67:bf:0b:b4:e0:52:2f:4a:e2:
                    3a:25:3a:a4:ec:17:7f:32:0f:3d:67:73:e7:5b:60:
                    2c:56:0c:41:46:e0:87:f8:cc:b9:9c:7f:78:29:e3:
                    7f:00:e0:2f:a5:59:5a:51:20:08:b9:84:3c:30:ea:
                    c1:70:e1:f7:db:97:0e:39:fc:2d:c0:cf:9d:79:cd:
                    eb:2a:e3:9b:ec:c4:d0:c9:15:2f:f9:5c:2a:78:f4:
                    46:bf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                35:BA:68:16:19:9D:96:6D:A5:61:91:BF:DD:E3:7D:49:E5:8B:69:F9
            X509v3 Authority Key Identifier:
                keyid:9F:39:49:81:1D:DD:4D:66:78:CA:58:CD:B9:01:E9:6A:9D:4C:DC:F8

    Signature Algorithm: sha1WithRSAEncryption
        21:55:3e:f5:b6:e7:c0:c3:b3:46:9a:ca:96:cf:59:8e:49:1b:
        73:27:46:31:ad:39:8f:28:ab:ba:0f:4a:d9:62:b9:3f:69:f0:
        a7:79:25:16:f4:57:3a:02:bc:d5:46:1f:97:fd:e9:01:54:cd:
        a5:f7:ff:e0:b8:b3:ff:15:09:ea:67:50:ac:78:67:c8:71:d3:
        ca:a3:80:8f:0d:84:66:4f:e2:52:da:aa:4c:42:67:8b:6d:78:
        fd:dc:65:6f:50:ab:47:c4:a1:72:3c:2a:c2:e4:0e:45:f3:96:
        78:fb:40:25:82:bf:f4:99:c3:29:d8:be:aa:a8:77:67:9b:ea:
        39:6d
```

WEBMAIL

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
             (Negative)4c:0b:1d:19:74:86:a7:66:b4:1a:bf:40:27:21:76:28
        Signature Algorithm: sha1WithRSA
        Issuer: CN=WEBMAIL
        Validity
            Not Before: Mar 7 01:13:05 2011 GMT
            Not After : Mar 7 01:13:04 2016 GMT
        Subject: CN=WEBMAIL
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

```
                Public-Key: (1024 bit)
                Modulus:
                    00:af:6c:48:9f:e0:02:ae:ff:2f:e2:3e:54:11:65:
                    1b:4d:c9:6c:d4:80:28:9e:c0:c0:11:cb:bc:6d:4f:
                    18:c8:9a:7f:7f:e7:cd:6b:1f:d6:3f:5b:29:7b:51:
                    7f:de:c1:ed:bc:80:3b:97:59:ed:6a:ab:fb:99:2d:
                    13:a5:5d:ff:50:57:e5:cd:ab:eb:e6:06:c8:3c:df:
                    c2:b9:9b:08:5b:aa:dc:7d:cd:c3:1f:f0:90:d9:6f:
                    ef:57:2a:8a:26:aa:9e:f1:f8:91:74:9f:37:52:96:
                    72:14:28:b5:e9:03:1c:13:4b:0d:f6:5c:0a:04:ed:
                    96:45:69:0d:86:52:e9:32:41
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        5a:24:20:42:f4:cd:1a:57:b4:f6:7e:4d:32:0f:67:04:4d:8f:
        8a:0d:4c:ff:8b:66:d9:69:94:b2:86:a3:39:e9:23:a8:84:a1:
        14:03:8a:b3:c3:96:a8:52:3d:b9:86:ac:55:83:1b:37:27:4e:
        8a:d1:8a:8a:ae:62:c9:75:f6:21:04:7b:cd:c7:4c:07:79:2f:
        bf:f7:7e:33:20:3f:f5:7d:fa:79:c9:14:dd:99:ae:26:1e:58:
        17:07:78:9b:8b:0a:69:85:fe:03:90:28:e9:f2:4f:44:97:f9:
        dc:e8:83:ea:21:7e:6f:f3:cd:d3:84:20:57:bd:6e:50:26:5e:
        ca:c6
```

ALPHA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
             (Negative)46:37:ea:15:b6:54:96:4c:b6:44:2b:7b:06:1a:a5:30
        Signature Algorithm: sha1WithRSA
        Issuer: CN=ALPHA
        Validity
            Not Before: Dec 13 07:18:23 2011 GMT
            Not After : Dec 13 07:18:21 2016 GMT
        Subject: CN=ALPHA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:de:6f:4a:e4:da:2b:48:fb:2b:47:47:6b:49:8c:
                    d1:11:25:93:b5:6e:98:61:84:10:39:61:62:92:17:
                    28:e0:2f:1f:03:ab:28:8b:9f:51:88:cc:7e:79:4e:
                    64:3d:f2:d4:b5:75:c1:dd:bc:20:a5:1a:31:8f:8a:
                    2f:18:19:e2:05:42:40:6c:8e:71:10:2c:1e:82:85:
                    6f:a8:f7:5f:c9:45:8d:c6:eb:c4:59:80:51:72:fc:
                    9c:e1:63:95:db:2e:f9:56:c8:b9:d6:86:84:5f:45:
                    91:d8:f5:51:0e:b6:76:16:c6:21:67:5a:04:94:e4:
                    e8:24:fb:7e:df:d9:46:ee:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        26:25:26:6c:e4:5f:5c:ec:63:f8:31:a1:5d:62:11:2c:ac:88:
        76:b5:5b:dd:25:16:45:57:7e:c2:92:1e:af:1e:f9:74:8d:30:
```

```
        a9:8a:c0:c7:9a:64:c3:72:9f:a4:2e:66:16:47:88:54:c7:51:
        3d:62:d6:dc:81:3a:c5:1c:53:c8:3c:c5:91:d6:f1:10:be:ab:
        df:5f:27:6c:10:be:bc:65:3b:8b:e7:5d:c4:09:b5:38:a8:df:
        d8:3d:3c:69:1c:8c:97:4b:9b:99:54:97:5f:35:70:6c:e2:04:
        03:73:7d:2e:e8:c8:84:f3:8c:fe:b7:63:64:ad:a7:da:f6:67:
        6f:fa
```

EMAIL

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
             (Negative)2f:09:dd:e0:ff:81:b7:6c:bf:2f:17:92:0c:d8:bd:57
        Signature Algorithm: sha1WithRSA
        Issuer: CN=EMAIL
        Validity
            Not Before: Mar 1 06:55:13 2012 GMT
            Not After : Mar 1 06:55:13 2017 GMT
        Subject: CN=EMAIL
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:92:c0:ca:df:95:b1:5f:42:36:f4:a0:68:db:b2:
                    c3:ad:9e:9b:4a:47:f5:b4:00:19:f7:ce:08:55:45:
                    34:7d:82:d8:d8:b1:f4:13:b3:48:6f:60:ec:76:5b:
                    47:1a:47:13:b7:fb:91:c9:94:89:66:dd:dc:fb:b7:
                    82:0c:dd:eb:63:70:d5:d4:4e:38:c4:84:85:e9:d5:
                    d3:1d:bc:47:34:5c:8d:40:41:f9:09:40:30:4c:8c:
                    a9:f0:84:e1:fe:47:3d:cc:57:0c:ed:6f:15:4a:a4:
                    4b:57:24:e1:ff:f3:fb:ea:05:50:dc:ed:0f:23:a4:
                    35:61:32:af:d3:3e:05:cc:1f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        36:e1:e9:16:5f:13:63:91:11:84:65:26:a8:46:1a:e1:17:a9:
        28:ee:af:af:cb:8c:85:47:f8:e2:f8:66:e0:b8:b2:07:44:f1:
        e8:47:d3:da:fa:de:fa:d6:21:17:58:9f:42:72:56:11:96:95:
        d6:72:5d:a5:3a:b5:cd:b6:61:06:bb:75:9b:b8:cd:fc:f4:10:
        54:f5:d5:75:3b:bb:85:d9:46:f0:0f:77:c6:c9:4b:5d:f9:b6:
        fb:3e:55:e9:55:70:02:48:f6:e0:c1:ad:49:f9:98:3e:39:b9:
        1a:00:18:df:a8:d3:28:7c:bb:75:25:16:dd:b4:0c:ee:ab:18:
        4b:04
```

LAME

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0e:97:88:1c:6c:a1:37:96:42:03:bc:45:42:24:75:6c
        Signature Algorithm: sha1WithRSA
        Issuer: CN=LM-68AB71FBD8F5
        Validity
            Not Before: Sep 20 08:34:24 2011 GMT
            Not After : Sep 20 08:34:23 2016 GMT
        Subject: CN=LM-68AB71FBD8F5
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:d9:18:49:6f:ff:1b:97:40:21:80:7c:14:aa:51:
                    30:73:5a:86:35:ac:b1:40:93:32:9d:b1:fd:bc:b5:
                    65:5e:ef:cf:c7:ad:62:97:0e:f4:04:77:e7:eb:70:
                    f8:b4:37:51:d3:29:3f:9c:80:eb:cc:40:4e:35:82:
                    85:3a:48:d1:07:a2:07:24:f8:28:a9:93:5c:2e:b2:
                    20:f8:cc:5d:75:24:02:7c:4a:76:44:71:b3:51:2d:
                    91:81:1a:71:a3:0a:f3:8d:8d:82:d8:f8:17:0b:32:
                    13:db:65:7e:df:42:06:1e:0e:cd:e0:e4:98:d2:39:
                    6e:a2:d9:5d:11:54:8b:4a:09
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        9b:1e:1e:06:6d:26:8b:0c:2c:1f:8c:6b:7e:e4:29:1d:56:5b:
        45:b8:85:58:76:fe:b4:4d:02:2d:7f:80:1c:90:59:9c:98:a5:
        a4:c1:e4:a2:c2:ca:99:d3:27:03:34:c4:db:ff:ab:36:9f:2a:
        f8:ab:05:3a:e8:dc:da:4d:50:fd:3f:c2:bc:96:51:38:ff:09:
        6f:69:f0:ed:c7:06:5c:43:25:df:e4:81:e1:eb:20:da:f6:4f:
        5d:db:d7:f0:97:00:73:1e:52:22:c0:ac:60:8a:e5:0a:4b:37:
        bd:cb:e9:33:94:80:64:3b:2c:66:54:fa:5b:b2:0f:0a:93:1e:
        7a:3f
```

NS

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            (Negative)72:a2:5c:8a:b4:18:71:4e:bf:c6:6f:3f:98:d6:f7:74
        Signature Algorithm: sha1WithRSA
        Issuer: CN=NS
        Validity
            Not Before: Jan 13 01:25:36 2012 GMT
            Not After : Jan 13 01:25:35 2017 GMT
        Subject: CN=NS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:af:05:10:20:6b:d0:47:8a:6d:03:fd:de:c9:64:
                    22:e1:c0:49:4f:89:97:0d:a8:f9:0f:54:14:4c:a3:
                    94:cc:9d:6f:6b:34:37:90:00:cc:bd:2a:ab:8b:30:
                    a8:0b:88:ef:73:f0:de:2e:22:3f:f4:c7:01:ee:80:
                    d2:c8:8c:84:9a:00:12:cd:89:2b:f0:59:37:30:80:
                    52:3d:df:60:40:e0:25:2f:c7:8e:a3:86:db:c2:28:
                    b8:3d:07:46:a1:4b:18:a0:bc:06:97:97:0e:4f:65:
                    18:95:0c:ac:58:b2:17:1b:ba:66:fd:2d:19:ad:dc:
                    6d:e6:6f:d3:16:b3:b2:cc:fb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        46:50:76:26:19:59:20:a2:93:e2:7e:b5:01:63:ab:d6:e0:ee:
```

```
        82:66:48:94:bc:e6:51:24:79:7d:95:ad:d5:2a:12:8e:cc:31:
        72:99:8a:6b:ab:0f:79:0c:f1:7e:f3:ee:f2:93:eb:78:e2:3f:
        48:2d:04:8a:36:7b:40:24:20:84:79:e6:31:a6:80:7a:85:94:
        ca:ab:ed:1e:9a:94:74:7a:5e:f6:4c:59:c0:1b:a1:80:5a:c0:
        a0:20:d0:3c:b4:82:ce:af:d7:ab:72:fb:70:99:bc:41:a1:ea:
        7e:27:a5:21:38:5a:1c:9e:7a:3e:7b:83:44:75:67:d0:c2:5d:
        86:56
```

SERVER

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            52:55:38:16:fb:0d:1a:8a:4b:45:04:cb:06:bc:c4:af
        Signature Algorithm: sha1WithRSA
        Issuer: CN=SERVER
        Validity
            Not Before: Mar 12 09:56:00 2012 GMT
            Not After : Mar 12 09:55:59 2017 GMT
        Subject: CN=SERVER
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a7:38:c7:c7:43:52:3b:59:c9:7f:cc:bc:9b:fa:
                    40:af:4d:7d:82:97:e6:e3:ec:69:eb:b7:44:d6:75:
                    d5:f4:4b:bb:18:e2:54:8e:67:0e:65:e9:b3:a8:c8:
                    eb:ff:95:ff:42:14:89:7a:31:7e:1b:b0:6d:8f:89:
                    db:ca:a3:1b:ce:8a:62:76:e8:72:b6:62:d0:dd:24:
                    ef:35:af:f0:3a:96:a1:e4:5a:19:76:e9:51:4e:8d:
                    0b:43:2b:fa:af:36:4a:b4:21:88:1b:ff:00:6f:f5:
                    98:63:f5:0d:f3:f5:10:3c:a0:04:78:23:3c:2b:54:
                    41:02:19:b2:35:78:cd:07:5b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        06:c4:35:a3:10:0d:5b:5b:19:7e:58:b3:c1:15:2d:56:07:73:
        e6:d3:cf:58:80:9e:ca:75:da:7c:38:fe:39:ba:71:bc:67:bf:
        63:1b:0d:0c:d3:d9:ab:2a:d0:b0:b7:eb:f9:bc:16:a3:33:6e:
        5e:ee:8f:89:21:d7:ec:4e:a0:bd:56:f3:34:e1:d3:86:ea:64:
        6e:a2:c6:4e:78:66:24:cf:5d:53:a4:71:a0:08:43:08:5b:f6:
        f2:c9:0c:12:90:60:a6:b3:f6:dc:46:62:ba:24:41:80:b5:2f:
        93:3a:0e:7e:ca:1b:a3:34:c9:95:39:f5:c9:20:75:f5:a9:eb:
        6f:69
```

SUR

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            (Negative)20:82:92:3f:43:2c:8f:75:b7:ef:0f:6a:d9:3c:8e:5d
        Signature Algorithm: sha1WithRSA
        Issuer: CN=SUR
        Validity
            Not Before: Dec  8 02:59:14 2011 GMT
            Not After : Dec  8 02:59:13 2016 GMT
        Subject: CN=SUR
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:99:60:d5:ab:5f:52:57:48:98:93:ed:37:59:b3:
                    f1:e6:7d:44:c7:55:25:25:82:3c:9c:a7:9d:ab:d7:
                    7f:a4:56:64:e5:17:31:5a:9c:21:e3:d6:e7:6a:11:
                    65:c9:4b:d2:5c:45:49:de:ae:2d:72:a9:7f:3f:59:
                    f7:cc:ff:56:93:cd:a6:fb:eb:0d:15:0f:76:b8:78:
                    ae:4e:46:ae:e5:98:79:ea:4a:c9:e2:52:52:77:08:
                    8e:1c:0f:f3:29:e1:a8:1c:28:98:a8:eb:76:10:f1:
                    08:06:d9:09:a3:e4:54:35:ba:4d:29:c3:ed:f9:a8:
                    2c:e4:95:b7:f2:a7:89:4d:85
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        31:32:bb:fd:e9:9e:2a:ce:e2:2a:1d:2c:d6:08:9d:0f:95:e2:
        cb:46:11:b6:c2:20:d2:b3:f1:42:57:5b:e8:91:e1:e2:9d:fb:
        42:1f:ac:f5:59:34:de:c4:e9:1c:14:96:c2:16:f4:5a:b8:a0:
        1f:f5:d3:50:02:e5:94:4d:e5:44:0a:ec:ed:e5:7a:16:c2:6e:
        bb:00:b5:da:f7:e4:e9:4c:64:7c:78:66:99:0f:91:12:c0:7b:
        5b:c0:0f:51:e2:6f:d7:47:c7:f4:a7:4e:b9:59:01:06:2f:13:
        f1:34:1e:42:83:c4:24:3f:f2:6b:ce:22:d6:1d:b5:af:84:26:
        08:ed
```

AOL

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            (Negative)7c:a2:74:d0:fb:c3:d1:54:b3:d1:a3:00:62:e3:7e:f6
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=mail.aol.com
        Validity
            Not Before: Apr 19 00:22:21 2010 GMT
            Not After : Dec 31 23:59:59 2039 GMT
        Subject: CN=mail.aol.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b8:68:c6:e9:75:c5:4b:73:27:e3:aa:9d:d9:f2:
                    ba:73:ec:86:5a:1c:89:3c:d0:37:5e:a7:3e:9d:48:
                    84:cd:a4:12:19:15:57:ca:ba:fe:ca:2e:2b:72:70:
                    5f:d7:64:ad:7a:6e:7e:c2:06:dd:99:3c:95:05:19:
                    f2:d7:28:8c:45:8f:91:c8:61:6e:23:2c:b8:2b:07:
                    08:21:b8:9a:4a:4e:12:70:c9:eb:19:3a:e0:f0:3e:
                    72:fb:ad:b3:dd:57:34:e8:18:8b:29:8f:33:bc:32:
                    e3:b0:e8:c0:3a:5c:fa:e5:aa:c2:17:94:1f:81:e7:
                    9b:60:2a:7a:aa:bf:e1:34:e1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                2.5.29.1:
                    0?....<.mW..]......A..0.1.0...U....mail.aol.com...]./.<..L.\....
    Signature Algorithm: md5WithRSAEncryption
        57:90:c4:ca:ca:67:9f:26:f5:27:d8:0b:94:b2:37:fc:cf:24:
```

```
        f1:9a:f8:6d:db:91:60:db:d6:d4:9a:5b:ec:fc:d4:75:5b:d1:
        98:ff:6e:1b:01:c9:e2:f8:45:84:2f:af:e9:da:21:d6:4d:4e:
        64:79:aa:1d:13:d3:97:c1:fc:91:a4:a2:09:71:c9:bb:88:a8:
        07:37:78:5f:b7:27:f3:73:2f:12:f6:f1:56:0e:93:3c:f2:a3:
        9e:5b:94:35:b5:29:09:50:ca:b4:65:69:d5:77:c9:c1:54:49:
        c2:89:10:27:93:78:aa:46:c1:ff:fc:42:ed:fc:80:9c:45:6d:
        7f:69
```

YAHOO

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            (Negative)0a:38:c9:27:08:6f:96:4b:be:75:dc:9f:c0:1a:c6:28
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=mail.yahoo.com
        Validity
            Not Before: Jun 11 00:23:32 2010 GMT
            Not After : Dec  8 02:59:13 2016 GMT
        Subject: CN=mail.yahoo.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:fc:ff:51:f1:18:ff:58:49:43:e6:bb:01:4e:77:
                    64:13:ca:79:1c:4a:24:d4:ec:13:1e:46:68:1d:e3:
                    d0:ac:bc:08:d4:88:d5:62:5c:82:bd:95:2c:66:49:
                    e4:80:2f:c5:79:5a:e2:91:ef:7c:b7:9f:6e:57:6a:
                    ba:f5:13:20:6d:61:9c:db:12:b7:46:32:94:78:4d:
                    58:cf:69:a2:82:43:b4:b9:05:62:75:86:fc:0a:92:
                    21:55:64:fb:03:6a:c8:2e:55:86:e8:68:a5:e9:e3:
                    93:f8:4a:85:91:89:99:d0:3c:5e:c3:16:dc:01:0f:
                    9d:41:5c:7a:d4:0d:6a:8a:49
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                2.5.29.1:
                    0A...}.....LfV.Q.2....0.1.0...U....mail.yahoo.com....6...i.A.#`?.9
.
    Signature Algorithm: md5WithRSAEncryption
        5b:7c:83:e0:41:ff:62:7e:c6:e0:a8:d8:e4:c9:a3:38:e5:31:
        39:20:5e:9a:3f:72:96:9e:ae:78:f5:f5:ba:f5:1e:47:68:34:
        01:fe:f1:71:e2:be:f7:54:24:6b:83:69:f4:b0:f3:32:0c:ab:
        09:98:e2:a4:c1:43:04:ff:55:cc:2e:c1:a9:f8:80:15:40:89:
        28:4f:b9:df:f6:26:ad:c5:65:32:a6:a7:ff:10:1d:ff:6e:24:
        35:01:98:a2:d3:bc:d2:ea:0e:75:83:23:55:e3:15:44:b5:78:
        73:12:c3:44:6a:2c:0f:cd:96:77:d3:51:b9:07:74:ed:2d:cc:
        be:07
```

MOON-NIGHT

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7c:8d:59:39:32:60:9b:8e:45:6b:3f:84:16:92:1f:c2
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=MOON-NIGHT
        Validity
            Not Before: Oct 26 00:31:10 2011 GMT
            Not After : Oct 26 00:31:09 2016 GMT
```

```
        Subject: CN=MOON-NIGHT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b4:41:24:7c:01:23:67:6b:66:ad:47:3d:23:ae:
                    08:9c:e4:4c:2b:9b:ff:25:92:11:ae:9f:55:73:cb:
                    d7:8f:2c:e3:17:d4:e6:81:40:68:4a:cd:a4:ba:33:
                    f8:f3:b7:e9:bc:7d:0c:51:13:35:d9:a8:b9:bd:8c:
                    8d:0d:a6:28:c8:b6:f7:66:1d:e3:69:f2:9e:4c:e4:
                    03:c1:3b:ae:55:a5:c7:3e:de:80:1b:07:5d:0f:a7:
                    a3:f0:50:60:d4:80:29:12:5f:1b:11:8c:8a:3d:e5:
                    b3:ad:c1:76:da:0c:a4:63:a4:8b:22:0d:49:1a:a0:
                    23:99:80:bd:09:3d:60:dc:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        5c:77:f0:fd:6b:e3:28:30:69:91:da:41:e9:5b:6f:25:83:c0:
        92:54:aa:02:c6:95:5a:ab:e7:0f:99:8c:10:e3:14:1f:21:86:
        8b:ce:bc:f9:a9:ee:71:2b:21:4e:f8:37:fe:4d:23:17:ad:ad:
        99:64:2d:4f:a2:70:fc:d9:35:71:4b:e1:2d:69:4c:b0:d6:2c:
        f2:7d:0e:18:21:75:f8:d4:f8:18:48:24:70:47:06:29:55:ac:
        bc:91:5d:cf:0f:81:4c:0d:58:68:2e:91:74:4a:fe:9c:0c:8c:
        a0:ee:e2:e1:49:d1:c1:c3:18:35:0f:48:e7:40:74:e1:ec:ad:
        74:b2
```

NO-NAME

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            83:ed:52:2e:5a:e0:7b:c0
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Anytown, O=ACLU, OU=A@@hole,
CN=NoName/emailAddress=iamnot@home.com
        Validity
            Not Before: Nov 11 15:28:14 2006 GMT
            Not After : Jul 20 15:28:14 2020 GMT
        Subject: C=US, ST=Washington, L=Anytown, O=ACLU, OU=A@@hole,
CN=NoName/emailAddress=iamnot@home.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:9b:cc:f3:67:5c:02:db:83:d0:5d:52:05:3c:8a:
                    66:16:fa:b2:5d:78:43:91:64:80:09:5b:c6:1f:b6:
                    dc:1f:60:fb:e2:d2:15:0b:f5:46:3a:76:c5:4e:91:
                    21:4d:33:46:25:04:28:70:69:25:87:38:01:1d:85:
                    94:9f:49:d0:1c:94:2f:1e:58:e3:49:2a:89:83:c0:
                    0b:76:53:49:34:f7:85:5e:43:35:a4:16:24:76:8d:
                    5b:2a:23:bb:57:34:af:16:74:2b:f8:64:44:15:6d:
                    15:8b:7a:a6:4e:a1:d0:e0:77:b0:2e:d4:d9:00:dd:
                    93:d6:3d:a5:e3:2b:ec:76:49
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                BD:6C:C6:6C:EB:5D:4C:47:25:42:4B:B2:61:8F:DD:1E:7C:3E:87:54
            X509v3 Authority Key Identifier:
```

```
                keyid:BD:6C:C6:6C:EB:5D:4C:47:25:42:4B:B2:61:8F:DD:1E:7C:3E:87:54
                DirName:/C=US/ST=Washington/L=Anytown/O=ACLU/OU=A@@hole/CN=NoName/emai
lAddress=iamnot@home.com
                serial:83:ED:52:2E:5A:E0:7B:C0

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        22:22:b6:2d:77:a5:60:51:d0:23:94:7a:f3:91:35:8f:bc:0b:
        d1:06:48:67:aa:50:d0:c4:6d:9c:0b:8c:bf:28:1f:44:0c:93:
        a1:9c:02:39:df:9b:01:31:f9:c5:1e:e7:2e:5d:a4:7f:0a:1f:
        01:39:56:e2:3b:cf:ae:3e:07:42:4d:d1:87:7c:b5:30:21:80:
        5e:67:cc:13:6f:10:bf:80:1c:5d:d8:e7:86:6e:57:e0:29:59:
        d0:28:b0:3d:dd:1a:18:aa:4e:5d:ff:ab:06:a3:31:3e:81:50:
        75:41:4e:1a:fb:3c:0f:c1:27:9a:24:b6:cf:da:2c:6a:05:4e:
        3d:eb
```