FORCEPOINT
POWERED BY Raytheon

SHA-1 Deprecation

Migration note for TRITON AP-WEB Cloud and Hybrid Modules

SHA-1 Deprecation – Migration note for Forcepoint TRITON AP-WEB Cloud and Hybrid Module customers

Executive Summary

The IT industry is migrating away from the use of the SHA-1 hash function in securing traffic between browsers and web servers, to the more recent, more secure SHA-2.

This may have an impact on Forcepoint customers who have IT environments containing software that does not support SHA-2, and who rely on Forcepoint to scan “https:” (SSL/TLS protected) traffic. This document describes some approaches that such customers can take to deal with this migration.

Background

Over time, cryptographic algorithms tend to become more vulnerable to attack. There are several factors involved, but there are two main considerations. Firstly, cryptographic research, by both benign and malicious researchers, can uncover design flaws in the algorithms. The probability of this occurring increases with time. Secondly, with the continual improvement in CPU and memory price/performance, attacks against cryptographic algorithms become cheaper to mount over time, since the computational cost in monetary terms is constantly reducing.

As a result of these factors, the industry at large has decided that the SHA-1 hash function is becoming too insecure to use for protecting certificates used in securing SSL/TLS sessions. This process is underway, and there are critical dates in 2016, which may be as early as July. For example, see:

https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html

https://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update/

https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/

As part of Forcepoint’s Cloud Web Protection service, we offer customers the ability to have Forcepoint decrypt SSL/TLS sessions from their users, to enable us to scan the content for security risks. In order to achieve this, a specific root certificate, created by Forcepoint (currently using our previous name, Websense) is installed by the customer’s IT department into the users’ browsers.

When Forcepoint’s web proxies process an SSL/TLS session on behalf of a customer that has enabled SSL/TLS decryption, the proxies will generate a synthetic certificate on behalf of the origin server. This synthetic certificate is signed by the trusted Forcepoint root certificate, and is returned during SSL/TLS negotiations with the client. This allows SSL/TLS sessions to operate normally within the user’s browser, and allows Forcepoint to access the web session data.

Current Situation and Need for Change

The Forcepoint (Websense) root certificate expires in 2032, and SHA-1 is used in its signature. As a result, Forcepoint needs to issue a new root certificate in 2016, using SHA-2, so that modern browsers do not start rejecting our certificate, and thus making it impossible for Forcepoint to handle SSL/TLS sessions.

From 11 July 2016, Forcepoint will change over the production systems from the old SHA-1 root certificate to the new certificate. From that date, customers will need to have the SHA-2 certificate

installed in all web clients that need to access sites that are subject to SSL/TLS decryption, or they will no longer be able to access those sites.

Systems Impacted by New Root Certificate

All modern browsers support SHA-2, and have done for some years.

It's not possible to give an exhaustive list of systems, browsers or software that do not support SHA-2.

According to Forcepoint's statistics gathered from our anonymised web traffic logs, the most widespread affected software that is still in use is Internet Explorer 6 on Microsoft Windows XP pre-SP3.

If a Forcepoint customer has enabled SSL/TLS decryption, then once the new SHA-2 signed root certificate is put into use, SHA-1 only browsers will produce errors when trying to access SSL/TLS protected sites, and will be unable to access these sites.

The new root certificate has been available for use since 19 April 2016. Forcepoint has made a specific Web Proxy available with the new certificate chain installed, to allow testing by customers against their installed browsers and applications.

How to Obtain and Test with the New Root Certificate

The new certificate is available at https://pki.forcepoint.net/certs/forcepoint-ca-20160302.crt . Customers should download this certificate and install it on their web client systems. Until Forcepoint switches the cloud service to using the new certificate, it will be necessary for web clients to have both the old and new root certificates installed.

To test the new certificate, once it is installed, browsers need to be directed to a specific Forcepoint web proxy that is configured to use only the new certificate. This allows for verification that browsing will continue to work as expected once Forcepoint's switch from SHA-1 to SHA-2 happens.

Details of how to test using the specially configured proxy are in Appendix A.

Note that the capacity of the test environment will not be suitable for use as part of a customer's production service, and the environment is provided for non-performance-critical testing only. We expect that all modern browsers will operate successfully in this test environment.

Mitigations for Lack of SHA-2 Support in Installed Base

Forcepoint have identified a number of steps that customers can take to mitigate lack of SHA-2 support in their installed base of software. As every customer has a different environment, we recommend that you evaluate the each approach separately, and decide which of them are applicable. The following list is in Forcepoint's recommended order of preference, from our perspective as a company whose customers rely on us to enforce their IT security.

1. Upgrade Windows XP devices to later Microsoft Windows versions which include SHA-2 support, and use any supported browser.
    - This has the advantage that the systems will be further protected by security enhancements from later versions of the operating system

2. Install Firefox or Chrome on Windows XP, since these browsers both support SHA-2.
    - This approach may be potentially easier to implement, but still retains exposure to

Windows XP, which is no longer maintained with security patches by Microsoft.

3. Create a separate Web enforcement policy that will be used for all browsers or systems that lack SHA-2 support. This would allow SSL/TLS exceptions to be created just for the affected devices, and would thus allow access to those sites, but will also stop Forcepoint from decrypting the traffic, and thus from scanning content for threats.
    - This restricts the level of security enforcement that Forcepoint can provide for such sites, but minimises the number or systems or users that this affects.

4. Add SSL/TLS exceptions in your policies for sites that need to be accessed by devices that lack SHA-2 support. This will allow access to those sites, but will stop Forcepoint from decrypting the traffic, and thus from scanning content for threats.
    - This restricts the level of security enforcement that Forcepoint can provide for such sites, and potentially affects more users.

Appendix A : Testing with the New Root Certificate

Testing with the new certificate requires the following steps:

1. Download and install the new certificate on the test system(s).
2. Configure the test system(s) to use the specially configured Forcepoint proxy.
3. Verify that the service is being accessed via the correct proxy.
4. Verify that access to sites, for which your policy specifies SSL decryption, is working.

A.1 : Download and Install the new Certificate

Download the new certificate from this URL: https://pki.forcepoint.net/certs/forcepoint-ca-20160302.crt

Install it within your test system's OS or Browser environment as appropriate. Detailed instructions on how to do this are beyond the scope of this document.

A.2 : Configure the Test Systems

There are various methods that can be used to configure a test system to access the specially configured proxy. They are listed here in relative order of preference. In general, the technique is to avoid using the usual DNS hostname for the relevant service (webdefence.global.blackspider.com or hybrid-web.global.blackspider.com), but instead use the specific IP address of a proxy.

webdefence.global.blackspider.com ➔ 208.87.234.172 (Hosted, Cloud-only, service)

hybrid-web.global.blackspider.com ➔ 208.87.234.173 (Hybrid, On-premise + Cloud, service)

Option 1: hosts File

Make a specific entry in the test system's "hosts" file (/etc/hosts, or \windows\system32\drivers\etc\hosts) to locally translate these DNS names to the relevant IP addresses. E.g:

```
# static entry for certificate testing

208.87.234.172 webdefence.global.blackspider.com

208.87.234.173 hybrid-web.global.blackspider.com
```

You may need to perform a system-specific action to flush the DNS resolver cache after doing this, to ensure that the setting takes effect. For example, in Microsoft Windows, use the command "ipconfig /flushdns".

Option 2: Manual browser configuration

Within the chosen web browser, configure settings to use a manual proxy IP address, on TCP port 8081 or 80 depending on your network infrastructure requirements. Use of a proxy in both Microsoft IE and Google Chrome browsers is configured using common Windows settings. Firefox has its own private settings accessible via Options->Advanced->Network->Settings.

Option 3: Custom PAC File Modification

Take an appropriate PAC file that is currently in use within your organisation, and edit the file to change all occurrences in PROXY statements of the two DNS names previously mentioned, with the corresponding IP addresses.

```
{       return 'PROXY webdefence.global.blackspider.com:8081';    }
```
becomes

```
{       return 'PROXY 208.87.234.172:8081';    }
```

Deploy the edited file as a custom local PAC file within the chosen browser, either by referring to a "file:" URL, or by hosting the PAC file on a webserver within your network, and accessing it from there. The latter technique may be necessary when using Microsoft IE 11.

Option 4: Use Pre-Configured PAC files

For Hosted customers, Forcepoint has made available a number of generic PAC files, as follows:

Basic/NTLM Authorization, Port 8081	https://pki.forcepoint.net/sha2-test-pac-files/forcepoint-ca-20160302-basic.pac
Basic/NTLM Authorization, Port 80	https://pki.forcepoint.net/sha2-test-pac-files/forcepoint-ca-20160302-basic-80.pac
Secure Form Authorization, Port 8081/8089	https://pki.forcepoint.net/sha2-test-pac-files/forcepoint-ca-20160302-form.pac

To use them, configure settings within your chosen browser(s) to use the most appropriate of these files for your network configuration. In many cases, these PAC files will be sufficient to test that a browser is successfully able to access SSL/TLS-protected sites. However, these PAC files do not contain any specific details about any customer's network, such as Non-Proxied-Domains.

A.3 : Verify Configuration

Within a browser, visit the following URL:

http://query.webdefence.global.blackspider.com/?with=all

If the system is configured correctly, you will see a page confirming that you are using the Triton AP-Web Filtering Proxy Server, and the Hostname listed will be "prx21h.srv.mailcontrol.com"

If the correct page is not displayed, revisit the previous steps and ensure they have been correctly carried out.

A.4 : Verify SSL/TLS Decryption

Browse to a site that you know is specified to be subject to SSL/TLS decryption, according to your organisation's configured policy.

If the previous steps have been successful, you will successfully connect to the site, and on clicking on the URL's padlock icon, you should see details of a Forcepoint web certificate.

If you are unable to access the site as expected, re-check all previous steps, correct problems discovered, and retry to access the site.

Appendix B : New Forcepoint Root Certificate

This is available to download from https://pki.forcepoint.net/certs/forcepoint-ca-20160302.crt

```
Certificate:
```

```
Data:
    Version: 3 (0x2)
    Serial Number: 11421213470513723009 (0x9e804d23a5e07681)
Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=Texas, L=Austin, O=Forcepoint LLC, CN=Forcepoint Cloud CA
    Validity
        Not Before: Mar  2 14:11:55 2016 GMT
        Not After : Mar  1 14:11:55 2021 GMT
    Subject: C=US, ST=Texas, L=Austin, O=Forcepoint LLC, CN=Forcepoint Cloud CA
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
                00:ec:11:54:e5:61:52:0e:d6:bc:a3:a2:51:10:ba:
                16:0b:73:7a:76:7d:71:f2:ef:10:5d:6c:54:75:1e:
                10:15:23:a2:fd:9a:29:9c:84:ce:51:62:5b:3b:72:
                22:cb:45:ca:4d:9a:94:21:63:4c:70:49:c2:f4:4b:
                f6:86:ba:77:e5:04:2b:95:f7:2f:99:63:ec:25:14:
                cb:89:12:49:d4:f5:15:fc:49:a8:b1:f7:ca:ab:06:
                69:9f:1a:7d:7f:b6:3a:d1:55:46:68:b7:9b:18:f2:
                73:f4:bd:60:8d:5e:59:90:1e:4b:3e:63:36:5e:91:
                d7:16:13:de:9f:95:5e:47:01:3f:60:53:1d:3c:f3:
                db:42:d7:28:67:51:69:5b:3a:88:63:79:3d:0b:72:
                e2:d3:0b:0b:4a:95:70:9d:d7:c7:31:0f:15:49:1a:
                d1:da:c7:fa:b1:85:59:44:23:cd:82:f5:21:b7:a6:
                71:da:bc:d3:fb:83:49:50:4e:38:5e:62:9c:03:04:
                0e:3f:db:b1:f8:d1:2c:d7:b4:00:6b:b7:52:5e:1f:
                9c:3b:bd:77:43:ee:d1:2e:dc:17:7f:55:e6:3c:23:
                b1:16:00:29:ba:55:db:05:2e:0a:74:90:a4:ec:63:
                c3:48:57:44:b2:7b:ab:51:c1:f9:b8:9b:c0:62:a1:
                54:fc:e0:ce:30:74:92:cd:34:79:83:8e:f2:ef:0e:
                ec:4c:29:15:cc:e1:01:47:75:a4:bb:a2:13:5f:4c:
                10:8c:59:83:91:58:2f:ea:32:c3:a7:f5:51:ea:25:
                3c:b0:99:1a:58:fb:91:5c:c6:45:cb:5b:b9:51:91:
                d1:24:6d:f1:02:47:5a:65:99:06:0e:0b:fb:a6:2a:
                c7:1f:f6:76:b0:c6:3e:24:7c:3b:2f:fb:a0:fc:ce:
                92:bd:1c:c6:71:88:67:1c:75:cc:83:a6:32:4a:a0:
                dd:69:b4:f5:66:92:86:e0:7f:79:f7:4a:41:76:06:
                a2:da:93:6b:10:d0:56:04:b6:95:0e:8c:a5:10:5b:
                ef:19:8d:c3:50:01:68:26:c6:bf:f7:a6:f8:5f:28:
                9d:d0:17:75:bb:8c:58:bb:63:44:5f:5d:9a:96:0f:
                65:e8:cf:49:7c:af:89:f8:3d:8b:77:b7:8b:5b:ef:
                9d:18:9e:4c:36:81:40:19:f6:7b:21:94:70:2d:30:
                80:ac:23:ff:be:35:9b:cb:79:6d:df:9b:b8:f4:7a:
                97:21:cf:53:5d:5e:dd:98:8b:64:0d:6d:cb:86:88:
                2b:93:c6:9d:b1:8b:32:97:5a:45:18:78:09:ef:db:
                03:d2:46:e2:37:94:94:00:e1:7f:3a:12:58:07:ac:
                c3:cb:29
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            66:65:5C:5B:A0:8E:33:EE:55:E1:26:78:B5:29:89:DD:22:37:D4:1C
        X509v3 Authority Key Identifier:
            keyid:66:65:5C:5B:A0:8E:33:EE:55:E1:26:78:B5:29:89:DD:22:37:D4:1C

        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:5
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
     a3:5f:d5:d2:2d:0b:9b:aa:cd:7c:89:f1:0d:47:25:00:d7:42:
     e1:d2:ec:81:8c:ab:49:e4:eb:f6:fd:f3:d3:43:68:50:03:d5:
     46:f7:e2:ff:ce:9b:0d:ef:74:a8:8f:d8:36:05:6b:2a:39:0e:
     b8:53:1e:06:c4:a1:79:df:e3:77:d9:ef:42:ce:8f:86:fc:92:
     34:57:6c:f6:6e:8a:04:d0:ae:1c:06:06:3a:20:ed:ae:f0:1d:
     c2:82:58:09:22:2e:d9:62:b0:87:b5:c6:02:67:e4:3e:d4:f3:
     1a:be:6f:25:86:d1:f6:f6:ab:97:52:55:08:37:4a:b4:f8:93:
     7c:60:dc:99:bc:36:1d:4c:b0:51:1e:fc:b5:33:4e:e3:7c:de:
     89:2f:5f:91:cd:f0:f9:07:12:de:27:1e:16:d3:47:1e:0f:ae:
     ea:b2:88:9b:94:ce:9c:5a:79:2e:44:f3:44:27:a6:2e:78:69:
     c6:cf:30:83:63:a4:d4:10:bd:66:2f:f2:de:53:9d:60:90:a8:
     35:19:e7:eb:4a:cd:7c:8f:e4:86:c7:43:07:37:19:d8:83:3b:
     71:47:6d:ce:2c:01:20:09:f1:6c:2a:65:05:98:a2:b7:85:2d:
     e9:7b:6b:cc:35:71:23:fc:8e:2b:0c:e6:4e:93:03:f8:24:30:
     01:05:83:c9:57:61:a6:28:c6:bd:7e:90:34:de:24:50:98:46:
     cf:12:29:e4:58:0f:48:13:c5:7c:87:a3:15:eb:b0:48:a0:5f:
     fc:0c:08:ea:e4:b8:78:a3:10:e1:fe:20:cd:d5:9d:5e:97:b7:
     d5:92:d1:27:8a:78:5c:cd:8e:30:ef:01:69:a7:20:a0:1a:0b:
```

```
        13:00:9b:c5:41:06:ff:a2:04:37:56:65:60:52:fb:28:34:6d:
        48:c8:ee:92:cf:d6:5b:5b:53:e6:92:f2:76:e6:bf:13:99:e7:
        e6:bc:03:7a:be:11:98:23:cd:e7:7d:98:42:2c:b5:79:51:45:
        ad:99:03:43:fe:83:64:fc:bc:a9:0d:e6:a6:85:78:84:16:f8:
        fd:de:5c:fc:56:74:f1:c3:b3:cb:b9:44:3d:92:ca:be:f6:b1:
        0c:71:e9:47:35:13:c9:25:e7:a8:14:bd:35:35:38:b3:76:f1:
        f7:e1:29:c6:e7:d4:8a:a5:02:68:4c:cf:3c:b9:f2:0a:73:d5:
        a4:f3:15:07:6a:a4:7a:27:b8:72:f1:63:56:aa:64:70:9f:aa:
        45:e8:dd:b2:05:ab:f5:14:62:4c:c9:c7:05:20:0f:8e:98:76:
        55:c3:c7:e7:77:d4:bc:85:ef:75:29:4f:5d:43:42:8e:21:8d:
        8a:9f:70:f4:1d:9a:98:56
```

Appendix C : Current Websense Root Certificate

This is available to download from https://admin.websense.net/crl/wbsnca.crt

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 18049233882905340820 (0xfa7bc2966a846b94)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: OU=Websense Internet Authority, CN=Websense Inc., L=San Diego, C=US
        Validity
            Not Before: Jun 26 09:38:57 2012 GMT
            Not After : Jun 21 09:38:57 2032 GMT
        Subject: OU=Websense Internet Authority, CN=Websense Inc., L=San Diego, C=US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ca:39:8d:68:5e:ca:3e:28:85:21:f8:79:2f:76:
                    e4:cc:4d:24:c4:a6:84:c1:bc:9b:50:16:f8:38:a6:
                    ec:45:db:57:08:c7:2d:ab:bd:bb:c7:81:a5:bc:e2:
                    92:da:86:2c:3b:d6:82:81:89:fc:4d:42:fb:90:11:
                    76:e3:f4:fd:8f:7c:fe:94:60:84:c9:a7:a0:f3:8a:
                    15:2c:bc:a3:85:2b:6a:23:e5:d8:77:5f:6d:a6:be:
                    50:25:b5:7d:82:8f:00:3f:2e:a6:03:d6:09:48:6a:
                    c9:62:91:5c:08:23:ff:35:a8:73:f8:25:db:d7:2e:
                    43:9b:44:8d:50:d6:9e:9f:3c:e0:a4:fa:08:20:be:
                    1d:01:6e:8d:15:a8:71:7b:bb:e2:68:f5:ed:30:ea:
                    1e:cd:b0:23:b5:ef:d4:fd:09:91:55:4e:49:f4:f6:
                    33:9a:4a:1c:e0:b0:c1:33:6f:a4:de:5a:b1:64:b5:
                    32:91:4d:53:64:a4:68:c7:89:1f:ed:f7:ea:6f:86:
                    3d:50:7d:11:26:a6:dc:3f:b4:33:d1:e2:02:37:0f:
                    5e:96:11:07:a2:a3:9a:0f:a2:85:a1:eb:5f:44:8a:
                    7f:c0:0b:24:25:4b:52:f9:63:70:3f:b1:7f:8b:b7:
                    41:b7:82:0e:11:8b:9d:c1:a8:31:96:50:7d:d1:b9:
                    9d:7a:96:1c:5f:80:96:25:a3:e6:1f:3c:39:9c:27:
                    1f:00:bd:86:37:32:38:a2:1d:0d:07:4f:a4:4a:5e:
                    45:24:87:1e:00:e3:75:ce:e0:e4:7a:86:7e:b9:ef:
                    13:1c:6d:58:2c:cb:a1:2d:7f:52:46:c8:3f:8f:79:
                    27:62:1d:b7:df:8b:8f:6b:ab:70:ad:55:04:a9:1c:
                    8c:68:5c:aa:03:07:dd:02:fa:7f:4c:0e:af:7d:d4:
                    03:d7:d2:c2:41:f3:a6:0e:9c:bc:2e:65:b0:e7:f5:
                    42:0d:ea:da:96:13:f0:69:31:ad:cf:1d:d1:ae:2d:
                    05:32:17:02:32:be:a6:57:ae:a2:1d:45:b5:07:72:
                    9b:5f:d3:57:e7:67:a9:ef:77:d3:bb:4c:35:3e:c3:
                    a8:e3:c7:9a:a4:77:3a:65:35:55:28:e9:82:f5:1c:
                    b9:53:21:14:ac:eb:12:aa:b8:b6:58:86:0c:00:fe:
                    f5:2f:3d:a3:98:a5:3b:19:08:79:e1:82:09:a2:33:
                    dd:0e:c0:cf:bf:b1:1c:94:aa:8d:2a:77:0d:eb:42:
                    f3:29:1c:53:80:4d:b2:a9:65:4d:43:4e:e6:b8:01:
                    40:68:db:b7:6f:af:40:3c:52:94:5d:65:19:38:ef:
                    d5:53:11:36:61:76:ef:11:d5:db:37:14:d9:56:21:
                    14:26:5f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                90:77:6D:F5:18:E9:4C:FA:20:AB:05:CF:AC:01:79:66:12:A9:A1:08
            X509v3 Authority Key Identifier:
                keyid:90:77:6D:F5:18:E9:4C:FA:20:AB:05:CF:AC:01:79:66:12:A9:A1:08

            X509v3 Basic Constraints: critical
                CA:TRUE
```

```
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 CRL Distribution Points:

            Full Name:
              URI:http://www.mailcontrol.com/crl/rootca.crl

Signature Algorithm: sha1WithRSAEncryption
     87:71:68:3e:85:73:b0:ed:f3:d9:86:14:9e:e9:ea:e7:16:26:
     c5:93:4d:0a:bd:b2:40:22:a5:dd:e3:31:25:33:29:05:62:b5:
     37:1f:0b:01:35:29:7a:60:82:2e:3c:1c:57:21:97:0c:60:01:
     49:8e:8b:d9:97:c8:27:1e:f0:b9:1d:25:0b:62:48:bd:94:b7:
     9f:b9:74:9a:68:4c:a3:67:c5:04:6b:81:79:73:c8:34:f1:ce:
     4d:ef:e2:3a:0a:37:11:57:94:bc:27:1a:47:6c:7c:f7:41:46:
     03:8f:e6:a0:6e:74:0c:f7:b0:5c:6a:54:24:30:d8:ca:f8:79:
     ae:15:ba:31:fe:0e:3c:81:c7:d4:fa:f1:b3:b7:c8:31:82:0d:
     78:3c:e4:51:fb:a3:e3:58:40:77:a3:ea:09:51:8c:d8:e3:6d:
     f0:0f:27:42:3d:38:ab:58:86:cd:32:bf:25:2f:8e:a2:10:fb:
     44:68:30:70:3d:c9:5a:7c:15:07:b7:a3:86:bb:6f:42:07:23:
     c6:ca:ec:42:93:1d:01:59:38:e4:18:e9:84:de:02:7a:41:96:
     3c:3c:1e:bc:7b:d8:38:59:3c:00:ea:df:71:ce:1d:06:1b:93:
     41:85:cd:ca:7d:9a:a3:71:aa:cd:df:e9:77:be:37:d3:06:89:
     f0:21:2c:d1:2c:3b:99:f1:62:6b:8e:02:07:62:d7:80:2e:29:
     ca:d1:72:44:7c:c0:51:21:48:2e:d2:f8:4a:90:f4:7c:b7:2d:
     02:8e:60:ca:3e:70:4e:75:2e:68:ba:54:3d:d9:23:d2:28:75:
     cd:12:6b:e5:e2:66:7b:12:fd:dd:2c:12:32:12:50:09:66:34:
     e4:5c:56:60:b4:79:ae:94:46:17:e3:dc:14:a4:c4:ce:a4:0c:
     18:5e:d5:0e:c4:84:d3:67:ca:87:74:e6:f0:8f:2f:01:18:aa:
     93:a8:ea:5a:3d:9d:a3:f9:36:83:0a:4a:25:cd:d2:47:50:ed:
     14:f0:6b:3a:5d:13:22:f2:82:5f:db:25:88:58:79:5b:84:41:
     c9:72:31:8d:ec:0c:62:88:62:78:70:40:67:85:33:5f:a9:71:
     78:41:ab:cd:7a:65:34:89:5c:1a:1b:7b:fb:f7:8b:a8:ed:15:
     1e:ca:97:96:af:59:20:f5:0d:fb:c5:d2:eb:0a:37:33:c2:8e:
     38:58:1b:0d:77:4b:40:7d:56:91:a9:ab:7c:0e:f1:e0:00:31:
     a9:7c:c6:11:0d:bb:35:98:c0:f1:c2:06:36:ec:37:e0:74:76:
     8a:2a:c5:6f:1a:7d:5d:46:41:dc:b2:a6:f8:ad:b3:2c:3e:89:
     1f:fd:42:c6:68:df:a5:ee
```