How to decrypt TLS FIX with Wireshark

Overview

To view FIX traffic the Wireshark tool can be used.

The traffic can be encrypted with Transport Layer Security (TLS) that provides security in the communication between two hosts.

It provides integrity, authentication, and confidentiality. It is used most commonly in web browsers but can be used with any protocol that uses TCP as the transport layer.

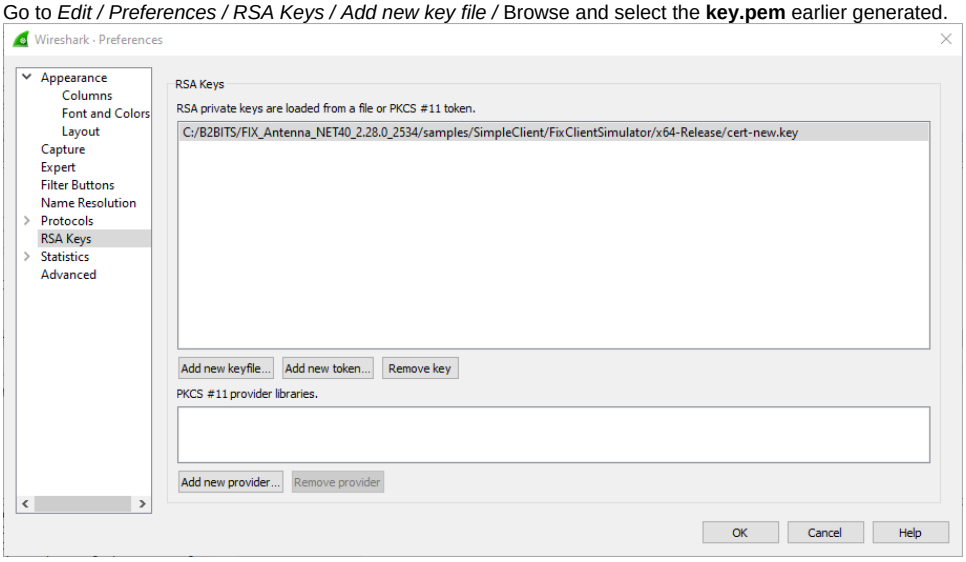
Wireshark supports TLS Decryption

Wireshark TLS Decryption

1. Create a self-signed SSL certificate via open SSL using the following How to configure built-in SSL support for FIX session in FIXEdge
2. Configure SSL Acceptors in FIXEdge
3. Configure Wireshark
4. Capture traffic
5. Decrypt traffic

Wireshark configuration

- Add the RSA private key file to the configuration.
  Go to *Edit* / *Preferences* / *RSA Keys* / *Add new key file* / Browse and select the **key.pem** earlier generated.

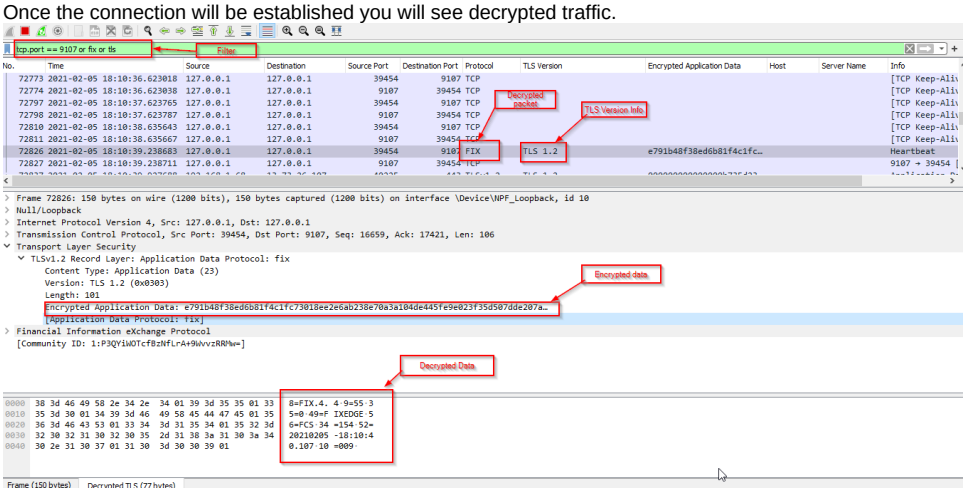


Start capturing packages on Wireshark

> Note
>
> If the session is established before starting the listening the traffic would not be decrypted.
>
> If the connection is acting as an initiator it must have the server's private key to decrypt packets.

- Start acceptor.

- Once the connection will be established you will see decrypted traffic.



Troubleshooting

Usage of (Pre)-Master-Secret (SSLKEYLOGFILE) to decrypt TLS FIX packets

As per Wireshark's official docs, the usage of (Pre)-Master-Secret (SSLKEYLOGFILE) is to decrypt HTTP + (over) TLS/SSL = HTTPS e.g. TLS traffic from Chrome, Firefox, and curl.

Alternatively, to debug FIX traffic it must be performed by TLS Decryption using an RSA private key.

Decoding SBE (Simple Binary Encoding) messages

CME works with data in CME MDP 3.0 and Streamlined formats.

There are guides:

- How to capture the data: https://www.cmegroup.com/confluence/display/EPICSANDBOX/Packet+Capture+Dataset
- How to decode it with Wireshark plugins https://github.com/Open-Markets-Initiative/wireshark-lua

Related pages

- How to configure built-in SSL support
- FIX Engine parameters SSL parameters
- Ciphers configuration in FIX Antenna C++ based applications
- Wireshark TLS Decryption