How to decrypt SSL traffic using a session key

On This Page

Problem description

When troubleshooting, you may need to provide Support or Development with SSL encrypted traffic. However, providing the private key could pose a security risk.

Solution

A simple workaround is to export an SSL session key. With such a key, the user can decrypt only one trace and cannot decrypt other traffic from the same SSL server.

Capture SSL traffic

1. Determine the IP addresses and ports of the software services that contain SSL traffic.
2. For Classic AMD, in the *rcon* console, execute the following:

```
rcon
tcpdump 0
"/var/tmp/encrypted_traffic.pcap" "host
X.X.X.X and tcp port YYY"
tcpdump status
tcpdump stop
```

   where X.X.X.X and YY are the IP addresses and ports of the software services containing SSL traffic.
3. For AMD HS use RUM Console -> Tools -> Recorded traffic tool to record the traffic.

Decrypt the trace in Wireshark

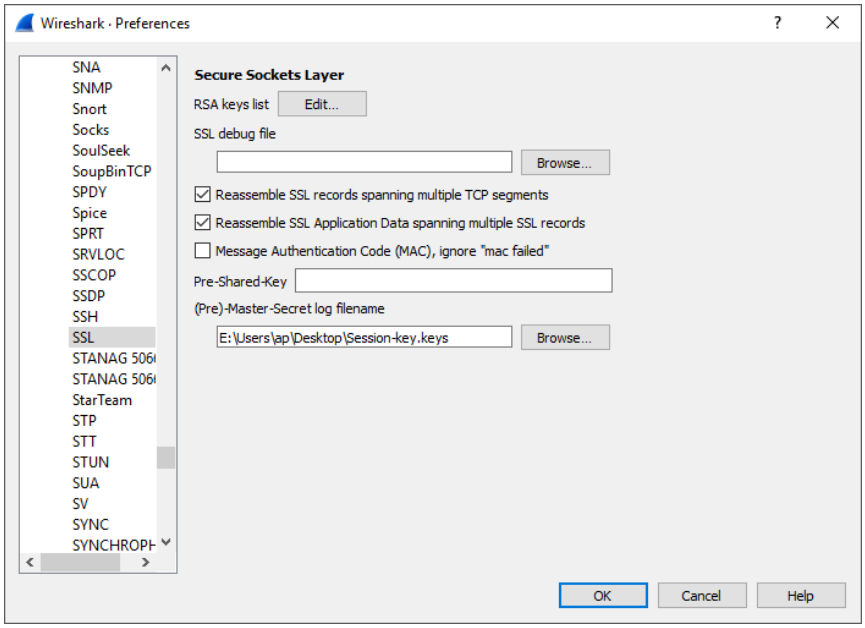
1. Open the captured trace in Wireshark.
2. Apply the private SSL key.
3. Make sure the traffic is decrypted.

Extract the session key

1. In Wireshark, select **File Export SSL Session Keys**, and save the file.

2. Open another Wireshark session, and try to use the session keys to decrypt the same trace. In Wireshark, select **Edit Preferences Protocols SSL (Pre)-Master-Secret log fil**

ename, and select the exported session keys:



You should get the decrypted traffic for this particular SSL session.