Download session keys with packet captures

Published: 2022-01-05

You can download a keylog file that includes all captured SSL session keys for SSL packet captures. Then, you can download and open the associated packet capture file with a packet analysis tool like Wireshark that can display the decrypted payload.

Before you begin

- You must have a configured ExtraHop Trace appliance before you can download packets and session keys from a Discover or Command appliance. See our deployment guides 🗗 to get started.
- The Discover appliance must be licensed for SSL Shared Secrets.
- The SSL Session Key Storage 🗗 setting must be enabled on the Discover appliance.
- Users must have either unlimited privileges or limited privileges 🗗 with packets and session keys access to download the keylog file.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. From the top menu, click **Packets**.
3. Optional: Apply filters to refine the packet query.
4. When the query completes, click **Download PCAP**.
5. Click **Download Session Keys**.
   The keylog file is automatically downloaded to your computer and the session key download operation is recorded in the audit log 🗗.

   If there are no session keys available for the downloaded packet capture, the **Download Session Keys** button does not appear.

Configure Wireshark to view the decrypted payload

1. Start the Wireshark application.
2. Open the Wireshark Preferences pane, expand the **Protocols** section, and then click **TLS**.
3. Optional: Click the **Browse...** button next to the TLS debug file field to create a log file.
4. Click the **Browse...** button next to the (Pre)-Master-Secret log filename field, select the `*.pcap.keylog.txt` file you downloaded above, and then click **Open**.
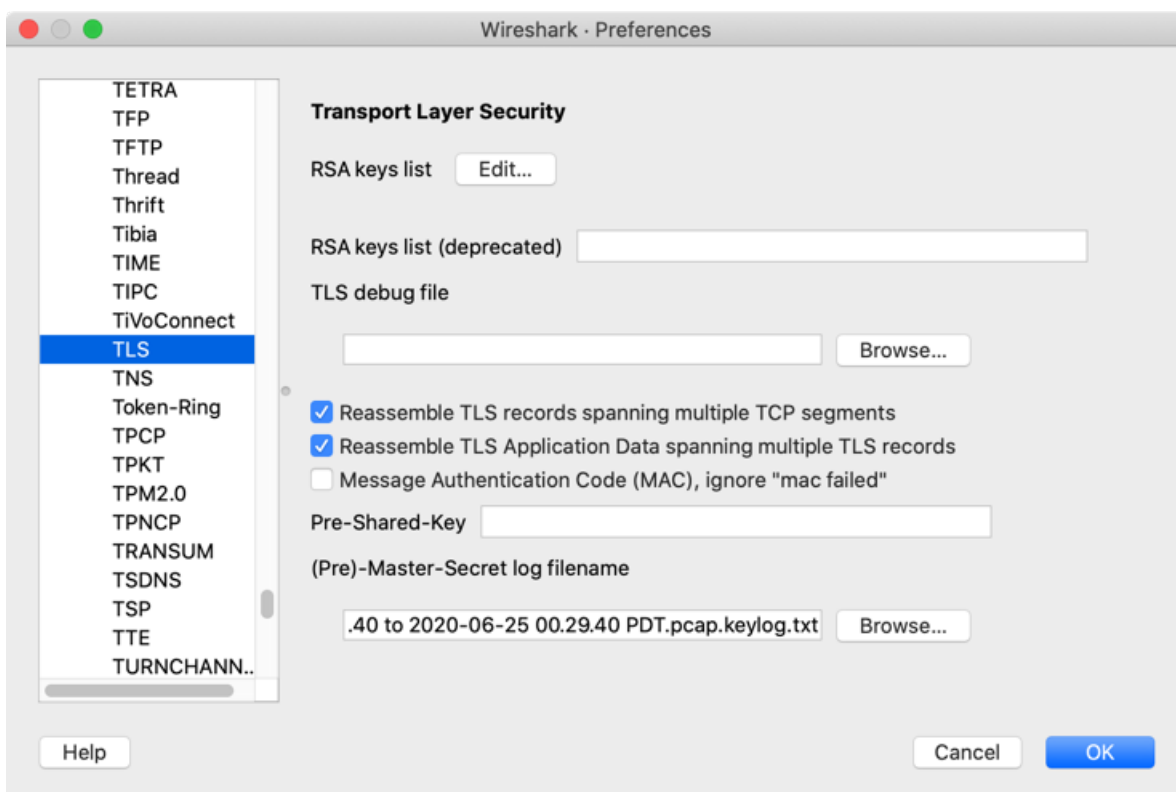
5. Click **OK** to close the Preferences window.
6. Open the downloaded packet capture file in Wireshark.

When an SSL-encrypted frame is selected, the **Decrypted SSL** tab appears at the bottom of the Wireshark window. Click the tab to see the decrypted information in the packet capture as plain text.