Download session keys with packet captures

Published: 2024-04-02

You can download PCAP Next Generation (pcapng) file that includes all captured SSL session keys and encrypted packets. You can then open the packet capture file in a tool such as Wireshark, which can apply the session keys and display the decrypted packets.

Before you begin

- You must have a configured packetstore or packet capture disk before you can download packets and session keys from a sensor or a console. See our deployment guides to get started.
- The console must be licensed for SSL Shared Secrets.
- The SSL Session Key Storage setting must be enabled on the sensor.
- Reveal(x) Enterprise users must have either system access and administration privileges or limited privileges with packets and session keys access. Reveal(x) 360 users must have packets and session keys access.

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 + Session Keys**.
5. Click **Download PCAP + Session Keys**.
   The pcapng 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 PCAP + Session Keys** button does not appear.

View the decrypted payload in Wireshark

1. Start the Wireshark application.
2. Open the downloaded packet capture (pcapng) 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.