## **Download session keys with packet captures**

Published: 2024-05-15

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.
- RevealX Enterprise users must have either system access and administration privileges or limited privileges with packets and session keys access. RevealX 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.

p.stream eq 19 Time Source 331 125.5824110. 10.10.9.229 333 125.5825180. 10.10.254.58 334 125.5825370. 10.10.9.229	Q         Image: mail of the standard stand	8 🖘 🔹
Time         Source           331         125.5824110.         10.10.9.229           333         125.5825180.         10.10.254.58           334         125.5825370         10.10.9.229	10.10.254.58 TCP 10.10.9.229 TCP	N  Length  Info 74 59934 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1162276 TSec
331         125.5824110         10.10.9.229           333         125.5825180         10.10.254.58           334         125.5825370         10.10.9.229	10.10.254.58 TCP 10.10.9.229 TCP	74 59934 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1162276 TSec
335       125.5825930.       10.10.9,229         336       125.58444130.       10.10.254.58         337       125.5844440.       10.10.9,229         338       125.5866420.       10.10.9,229         339       125.5866420.       10.10.9,229         340       125.5866420.       10.10.254.58         340       125.5869320.       10.10.254.58         341       125.5877900.       10.10.9,229	10.10.254.58         TCP           10.10.254.58         TLSv1.           10.10.254.58         TLSv1.           10.10.254.58         TCP           10.10.254.58         TCP           10.10.254.58         TLSv1.           10.10.254.58         TLSv1.           10.10.254.58         HTTP           10.10.254.58         HTTP	66         59934 → 443         (ACK)         Seq=1         Ack=1         Win=29312         Len=0         TSval=1162276         TSecr=227215419           2         583         Client Hello
342 125.5878320 10.10.9.229	10.10.254.58 TL5v1.	2 151 Alert (Level: Warning, Description: Close Notify)
rame 340: 247 bytes on wire (1976 bit: thernet II, Src: Whware_94:40:10 (00: nternet Protocol Version 4, Src: 10.10 ransmission Control Protocol, Src Port ransport Layer Security - TLSv1.2 Record Layer: Application Data (2: Version: TLS 1.2 (0x0303) Length: 176 For the State of Content Protocol Parts Content 176 Version: TLS 1.2 (0x0303)	50:56:94:40:10), Dst: VHware_94 0.9.229, Dst: 10.10.254.58 t: 59934, Dst Port: 443, Seq: 7 ata Protocol: Hypertext Transfe 3)	4:4f:bc (00::         00:10         0a 48 6f 73 74 3a 20 70         66 73 2d 77 69 6e 32 30         -Host: p fs-win20           0020         31 32 72 32 2e 6c 61 62         2e 69 2e 65 78 74 72 61         12r2.lab .i.extra           0030         68 6f 70 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67         hop.om         User-Ag           0040         65 6e 74 3a 20 41 70 61         63 68 65 42 65 6e 63 68         ent: Apa cheBench           0050         21 32 2e 30 dd 0a 41 63         63 65 70 74 3a 20 2a 2f         /2.3·Ac cept: */           er Protocol         0060         2a 0d 0a 0d 0a         *····
Encrypted Application Data: 37bc84 [Application Data Protocol: Hyper Hypertext Transfer Protocol		Frame (247 bytes) Decrypted TLS (101 bytes)
<ul> <li>Record layer version (tis.record.version), 2 bytes</li> </ul>		Packets: 1788 - Displayed: 29 (1.6%) Profile: Defi