## **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 2 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 **Z**.

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**.

## 🍽 🖉 ExtraHop

	Wireshark · Preferences
TETRA TFP TFTP Thread	Transport Layer Security         RSA keys list       Edit
Thrift Tibia TIME TIPC	RSA keys list (deprecated) TLS debug file
TiVoConnect TLS TNS Token-Ring	Browse
TPCP TPKT TPM2.0	<ul> <li>Reassemble TLS records spanning multiple TCP segments</li> <li>Reassemble TLS Application Data spanning multiple TLS records</li> <li>Message Authentication Code (MAC), ignore "mac failed"</li> </ul>
TPNCP TRANSUM TSDNS TSP	Pre-Shared-Key (Pre)-Master-Secret log filename
TTE TURNCHANN	.40 to 2020-06-25 00.29.40 PDT.pcap.keylog.txt Browse
Help	Cancel

- 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.

• •	•						010	extr	raho	p 20	018-	-06	-05	12.0	04.0	4 to 2	201	8-06	-06 1	2.04	.04 F	PST.p	сар								
		đ	۲				X	0	5	C	2	-		۲		= 7	5	♣				Œ	2 (	Ð		Ŧ	Ē				
ssi				-	-						•	-		~	-						_	:	-	•	-		_	Ex	pressio	n	+
	243		80360			. 168					19	2.1		0.4	-		1	Protoc FLSV1	1.2						Ale				√arni	-	1
	252 254	0.32	85950 33030 46940	00 00	192 192	.168 .168 .168	.0.4	1			19) 19)	2.1	68.	0.4	1		1	FLSV: FLSV: FLSV:	1.2					145 232	Ser Cli	ver ent	Key	o, ( Excl	Certi nange		
<ul> <li>▶ Fra</li> <li>▶ Eth</li> <li>▶ Int</li> <li>▶ Tra</li> </ul>	ame hern tern ansm	256: et II et Pr issio	231 b , Sro otoco on Cor cets L	oytes : Vr ol Ve ntrol	s on nware ersic L Pro	wire 2_94: on 4,	8f: Sr	848 96 c: :	(00: 192.	:50 .16	, 23 :56: 8.0.	31 :94 .1,	:8f Dst	:96) t: 1	capt ), [ 192.	ost: 168.	i (1 Vmw 0.4	are_ 1	bits 94:7	d:23			: 56 :	94:7	7d:2		Cinh		, inc		
0000 0010 0020 0030 0040 0050 0060	47 48 32 6f 6e 32	45 5 6f 7 72 3 70 2 74 3	4 20 3 74 2 2e e 63 a 20 3 0d	2f 2 3a 2 6c 6 6f 6 41 7	0 48 0 70 1 62 d 0d 0 61	66 2e 0a 63	73 69 55 68	2d 2e 73 65	77 65 65 42	69 78 72 65	6e 74 2d 6e	32 72 41 63	0d 30 61 67 68 2f	31 68 65 2f	Ho tr ge h/	et / / ost: / rahop ent: / /2.3.	ex a .c a Ap a	ample om Us acheB	e.ex erA Benc												
Frame	e (23	1 byte	:5) [	Decry	pted	SSL (	(100	byte	es)																						
0 7	۲ e	xtraho	p 2018-	06-0	5 12													Packe	ts: 301	17 · Di	splay	ed: 14	00 (4	6.4%	) · Lo	ad tin	ne: 0:0	.192	Profi	e: Def	ault