

Configuring Wireshark for Decrypting Traffic

Module Overview



- Collecting TLS Keys
- Importing Keylogs into Wireshark
- Decrypting HTTPs Traffic

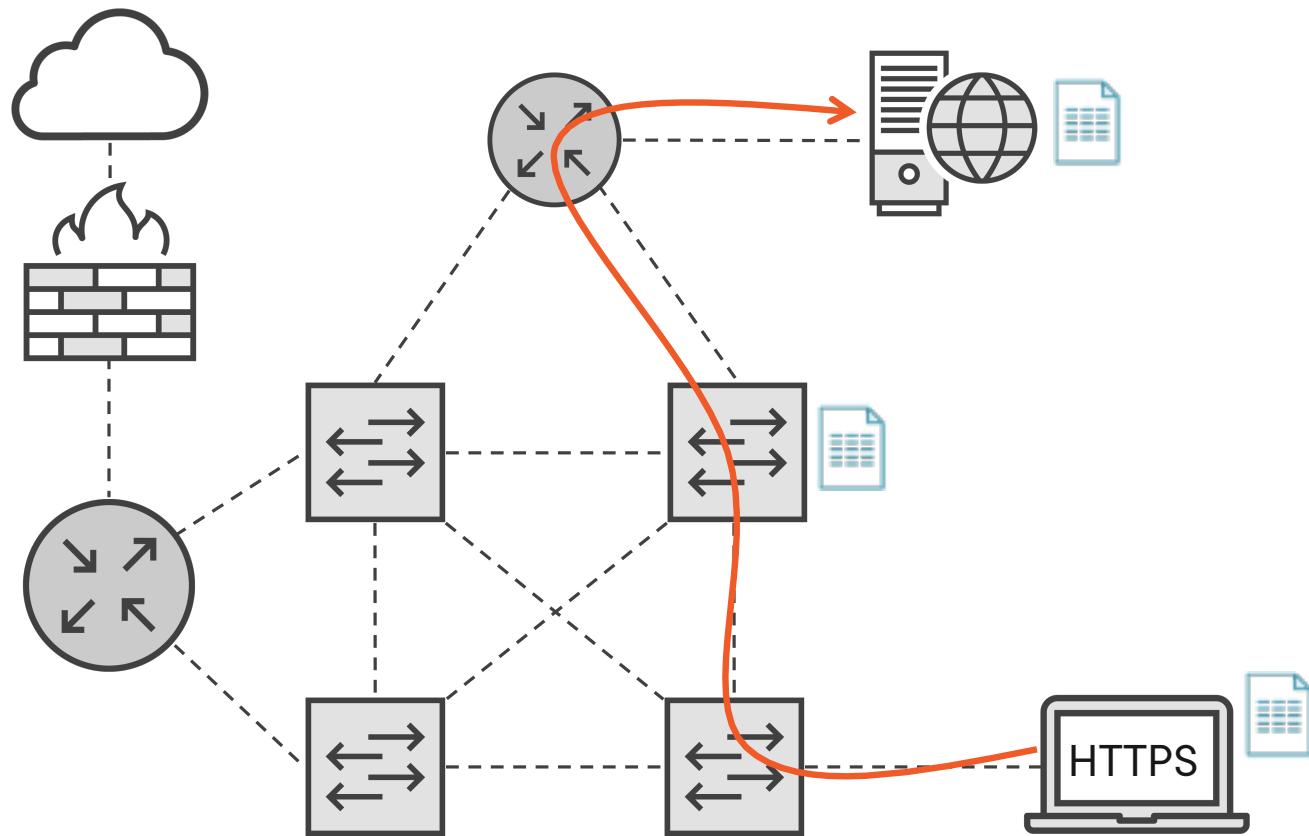


We will go into how to capture the SSL/TLS keys at a very basic level

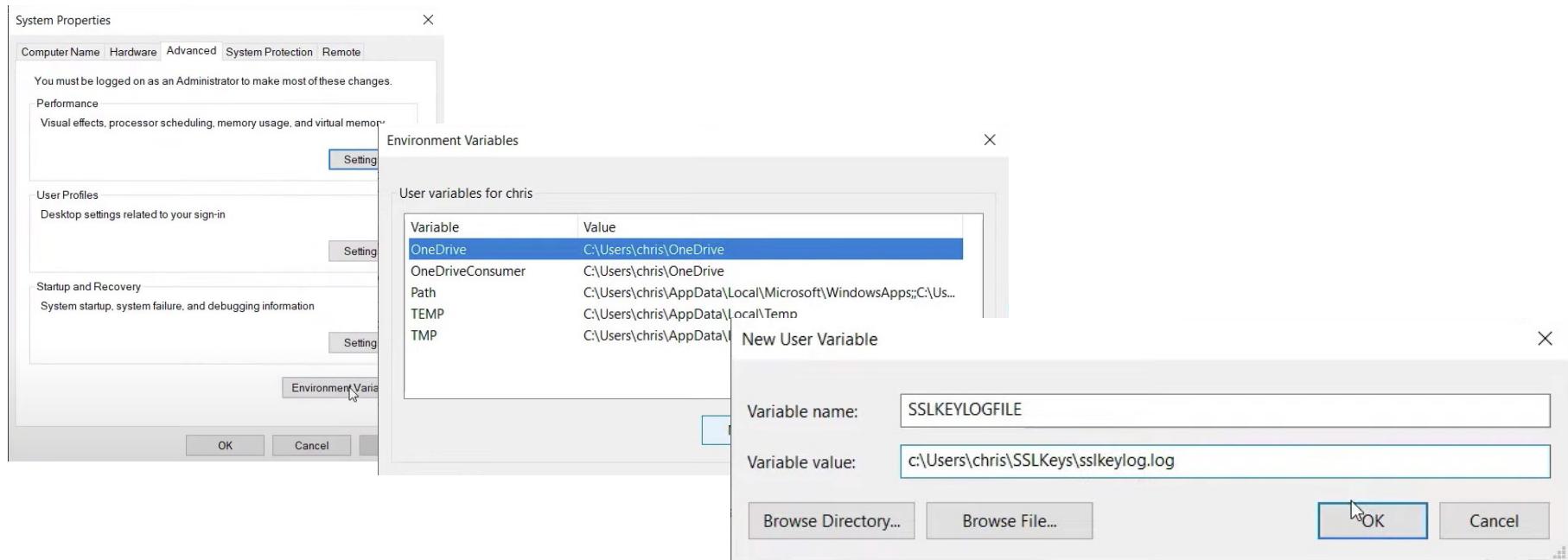
Another Pluralsight course:

Troubleshooting with Wireshark: Analyzing and Decrypting TLS Traffic in Wireshark

Capturing the TLS Keys



Capturing the TLS Keys - Windows



Capturing the TLS Keys – Linux

```
File Actions Edit View Help
└──(chris@kalimac)-[~]
$ export SSLKEYLOGFILE="/home/chris/sslkeylogfile.log"
```

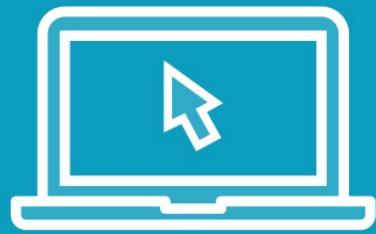
Capture Packets and Keylog

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Server Name	Host	Info
242	2021-07-19.. 10.0.2.15			192.168..		ICMP			Echo (ping) request id=0x131c, seq=0/0, ttl=48
243	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
244	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
245	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
246	2021-07-19.. 10.0.2.15			192.168..		ICMP			Echo (ping) request id=0x9deb, seq=0/0, ttl=48
247	2021-07-19.. 10.0.2.15			192.168..		ICMP			Echo (ping) request id=0x61f5, seq=0/0, ttl=40
248	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
249	2021-07-19.. 192.168..		10.0.2.15			ICMP			Echo (ping) reply id=0x131c, seq=0/0, ttl=42
250	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
251	2021-07-19.. 10.0.2.15			192.168..		ICMP			Echo (ping) request id=0xd0d5, seq=0/0, ttl=39
252	2021-07-19.. 10.0.2.15			192.168..		ICMP			Echo (ping) request id=0x9fd3, seq=0/0, ttl=45
253	2021-07-19.. 10.0.2.15			192.168..		ICMP			Echo (ping) request id=0x7cea, seq=0/0, ttl=56
254	2021-07-19.. 192.168..		10.0.2.15			ICMP			Echo (ping) reply id=0xb590, seq=0/0, ttl=39
255	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
256	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
257	2021-07-19.. 10.0.2.15	43563 (435..	192.168..	https ..	TCP	43563 - https(443)	[SYN]	Seq=0 Win=1024 Len=0	
> Frame 472: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0									
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_01:39:f0 (08:00:27:01:39:f0)									
Internet Protocol Version 4, Src: 192.168.0.21, Dst: 10.0.2.15									
Transmission Control Protocol, Src Port: http (80), Dst Port: 43563 (43563), Seq: 1, Len: 0									
Source Port: http (80) Destination Port: 43563 (43563) [Stream index: 99] [TCP Segment Len: 0] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 2990518198 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 0 Acknowledgment number (raw): 0 0101 = Header Length: 20 bytes (5)									
0000	08 00 27 01 39 f0 52 54 00 12 35 ff 06 4f fe c0 a8 00 15 0a 00								.. 9 RT -5 .. E ..
0010	00 28 9f 05 00 ff 06 af fe c0 a8 00 15 0a 00								(- 0 ..
0020	02 0f 00 50 aa 2b b2 3f af b6 00 00 00 50 04								P + ? .. P ..
0030	00 00 d6 a2 00 00 00 00 00 00 00 00 00 00							

0 packets 0 bytes 0 displayed 5056 (100%) 0 comments 0

```
sskeylog - Notepad
File Edit Format View Help
CLIENT_HANDSHAKE_TRAFFIC_SECRET c5a66dbd4d67e100e2e617488ced7e74c551ea95da1283efaea511c
SERVER_HANDSHAKE_TRAFFIC_SECRET c5a66dbd4d67e100e2e617488ced7e74c551ea95da1283efaea511c
CLIENT_TRAFFIC_SECRET_0 c5a66dbd4d67e100e2e617488ced7e74c551ea95da1283efaea511cede44c6e
SERVER_TRAFFIC_SECRET_0 c5a66dbd4d67e100e2e617488ced7e74c551ea95da1283efaea511cede44c6e
EXPORTER_SECRET c5a66dbd4d67e100e2e617488ced7e74c551ea95da1283efaea511cede44c6e c94315f
CLIENT_HANDSHAKE_TRAFFIC_SECRET 4b84f59d552eb3dcfd79a568742e8e7571357f0fa24c72bfc470bc6c
SERVER_HANDSHAKE_TRAFFIC_SECRET 4b84f59d552eb3dcfd79a568742e8e7571357f0fa24c72bfc470bc6c
CLIENT_TRAFFIC_SECRET_0 4b84f59d552eb3dcfd79a568742e8e7571357f0fa24c72bfc470bc6c73e332b6
SERVER_TRAFFIC_SECRET_0 4b84f59d552eb3dcfd79a568742e8e7571357f0fa24c72bfc470bc6c73e332b6
EXPORTER_SECRET 4b84f59d552eb3dcfd79a568742e8e7571357f0fa24c72bfc470bc6c73e332b6 aaa0ac1
CLIENT_HANDSHAKE_TRAFFIC_SECRET f2b301674708c15e6cbec9b5f86adebfa7556e827bd99bad6f0b99a06375397
SERVER_HANDSHAKE_TRAFFIC_SECRET f2b301674708c15e6cbec9b5f86adebfa7556e827bd99bad6f0b99a06375397
CLIENT_TRAFFIC_SECRET_0 f2b301674708c15e6cbec9b5f86adebfa7556e827bd99bad6f0b99a06375397 SERVER_TRAFFIC_SECRET_0 f2b301674708c15e6cbec9b5f86adebfa7556e827bd99bad6f0b99a06375397 f9b55b7
EXPORTER_SECRET f2b301674708c15e6cbec9b5f86adebfa7556e827bd99bad6f0b99a06375397
```

Demo



Lab 12 - Configuring Wireshark to Decrypt TLS Traffic

Course Overview



Top Five Wireshark Features for Forensic Analysis:

**Statistics, GeoIP, Custom Columns,
Name Resolution, Extracting Files**

Filters and Coloring Rules for Abnormal Traffic

Configuring Wireshark to Decrypt TLS