HTTPS-Analyse

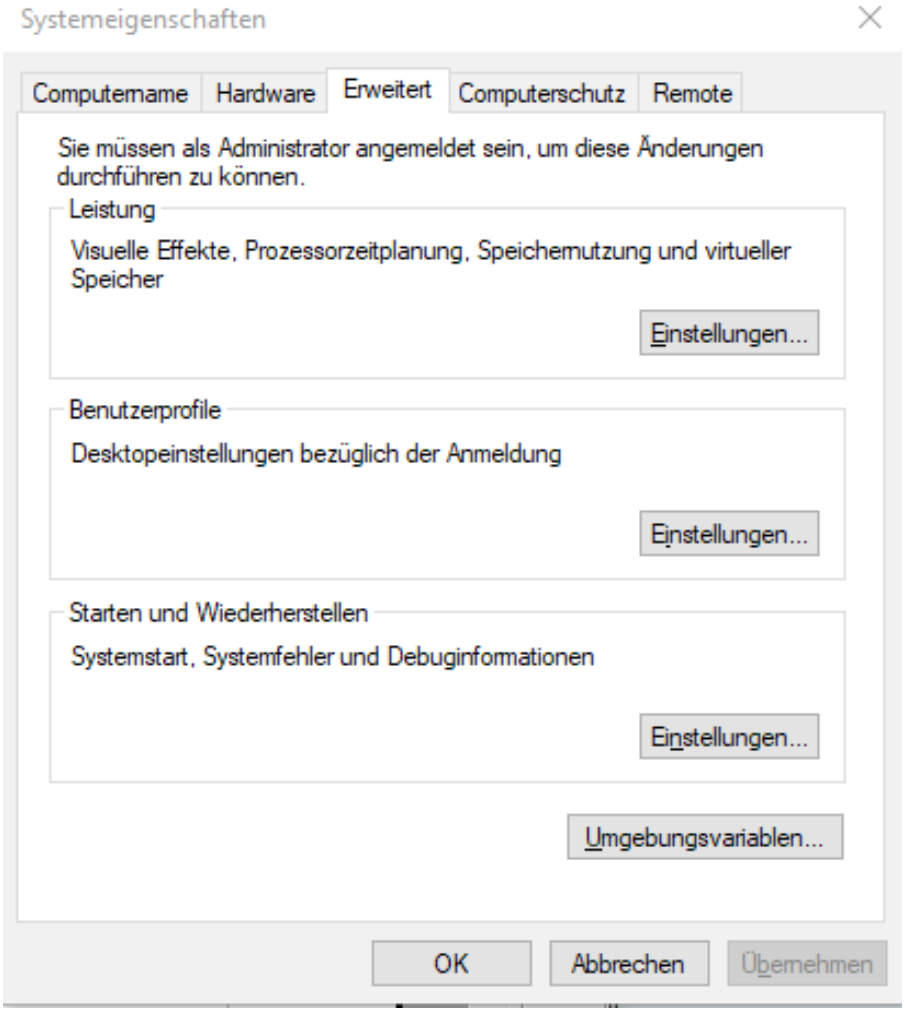
Wireshark unterstützt die Entschlüsselung von SSL/TLS Sessions, wenn man das Master-Secret berechnen kann.Bei Cipher Suites, welche das RSA-Kryptosystem verwenden, kann der private RSA-Schlüssel zum Entschlüsseln des pre-master secret verwendet werden. Wenn jedoch die Diffie-Hellman cipher-suites verwendet werden, wird der private RSA-Key nur zum Signieren der Diffie-Hellman Parameter verwendet.

Wenn man nun Wireshark verwendet gibt es mehrere Methoden SSL/TLS zu entschlüsseln. Die erste Möglichkeit ist das Entschlüsseln des Pre-Master-Secret mit dem privaten RSA-Key, jedoch funktioniert dies nur nur bei RSA-Kryptosystemen. Die andere Möglichkeit ist eine SSL Keylogfile festzulegen, welche das Master-Secret speichert.

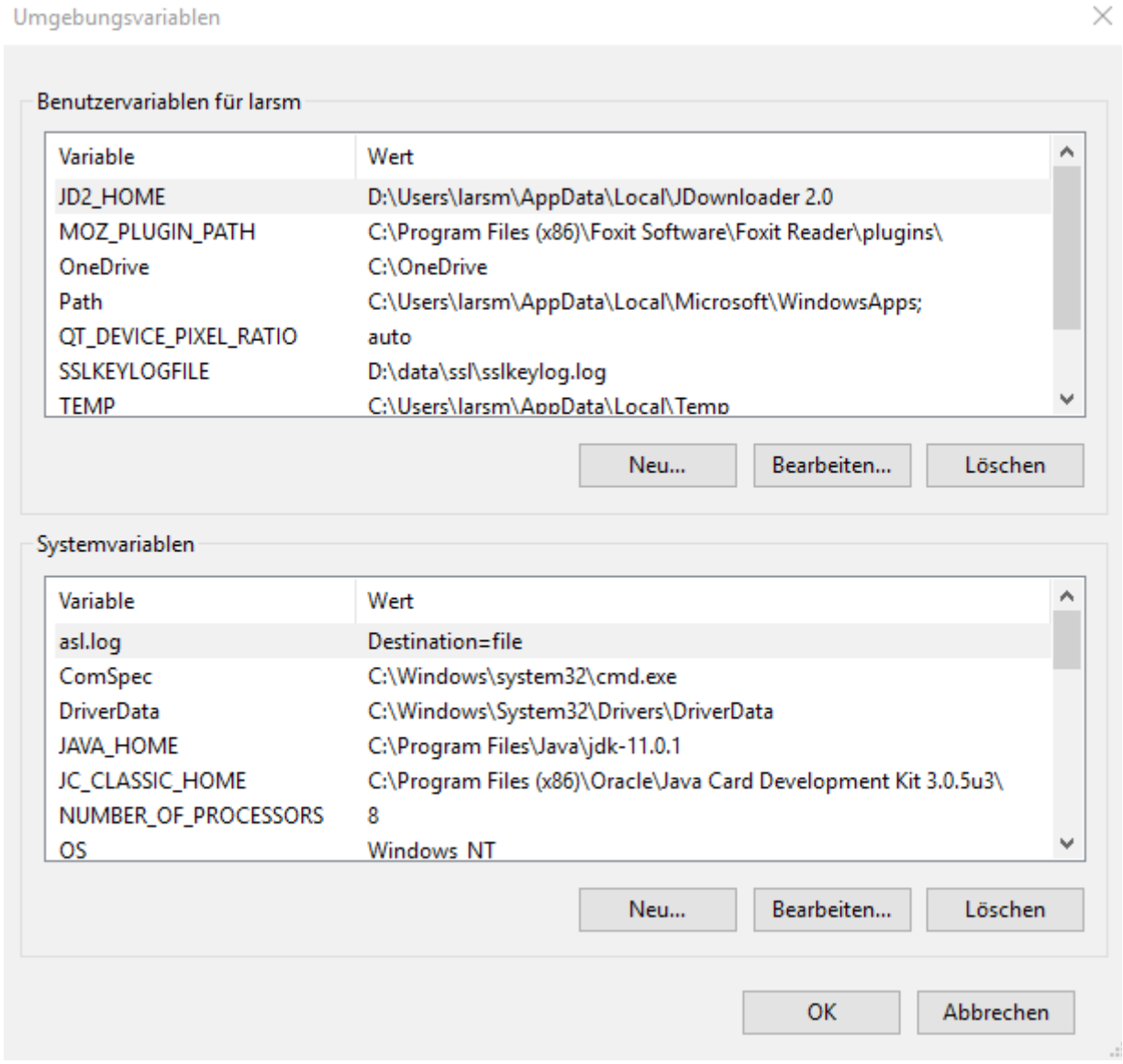
In den folgenden Schritten zeige ich wie man nun ein SSL Keylog File generiert und anschließend per Wireshark mitgeschnitten Traffic entschlüsselt.

Unter Windows

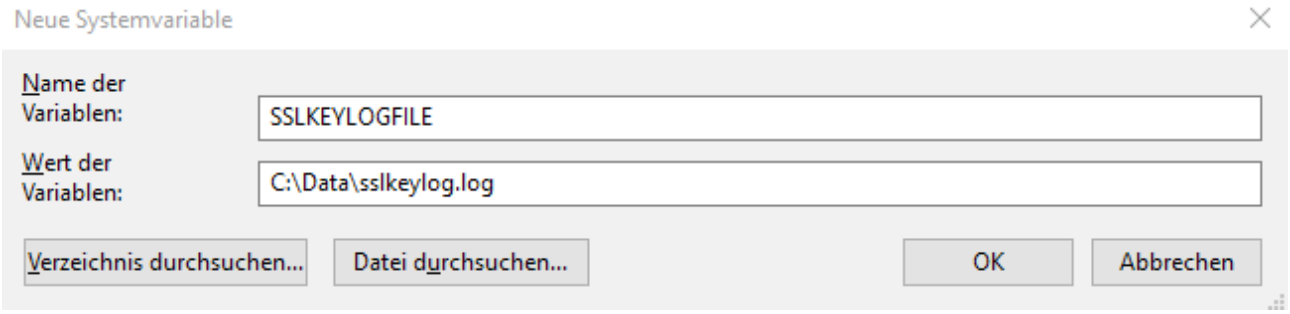
1. Unter *Systemeigenschaften*, klickt man auf *Erweitert* dann auf *Umgebungsvariable*.



2. Anlegen einer neuen Systemvariable indem man auf *Neu* klickt.



3. Unter Name der Variable gibt man „SSLKEYLOGFILE“ ein und verweist unter Wert der Variable auf einen selbstgewählten Ort wo man die Protokolldatei speichern möchte.



Unter Linux

Man verwendet den export Befehl um eine zu exportierende Umgebungsvariable zu definieren. Der Befehl für SSLKEYLOGFILE ist:

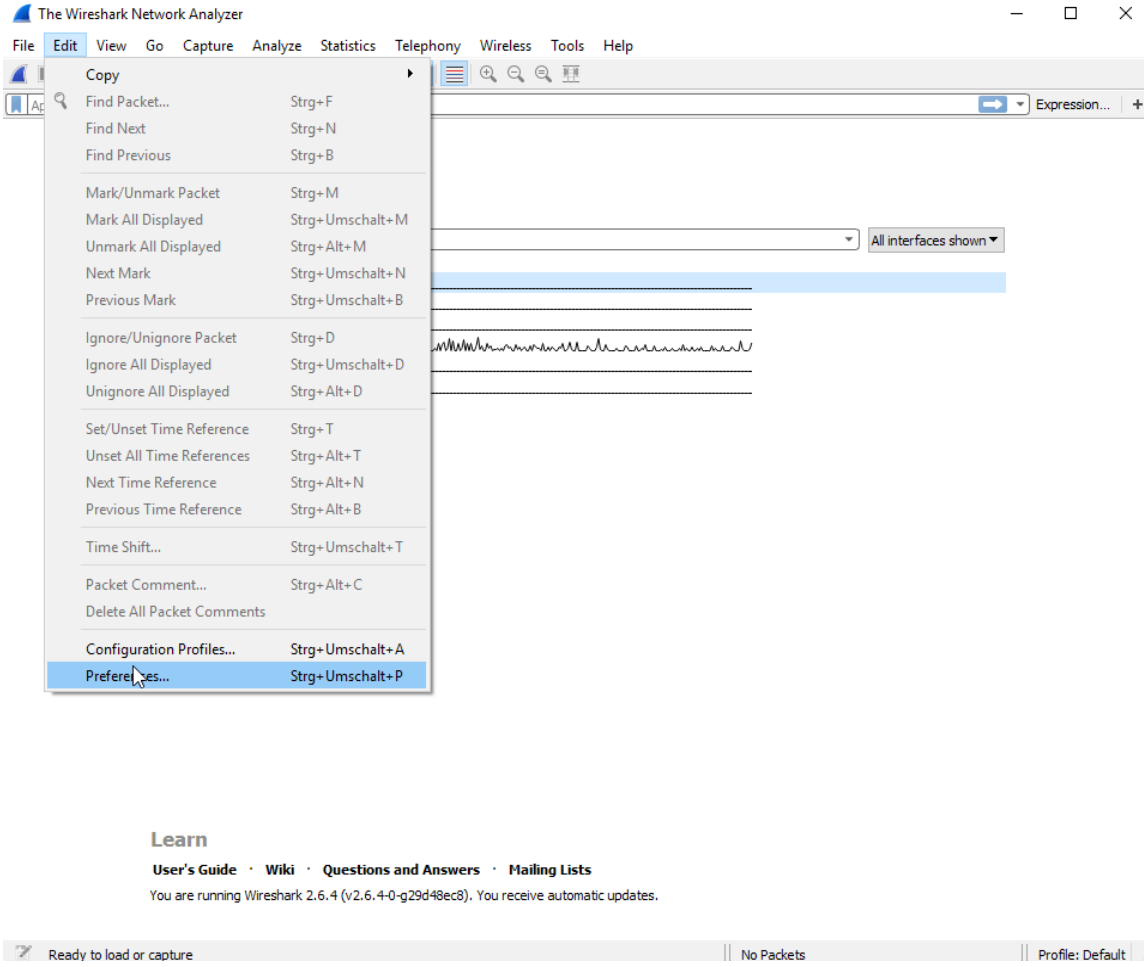
export SSLKEYLOGFILE="VALUE"

VALUE ersetzt man durch einen selbstgewählten Ort wo man die Datei speichern möchte. Ein Beispiel wäre *~/Desktop/sessionkey.log*

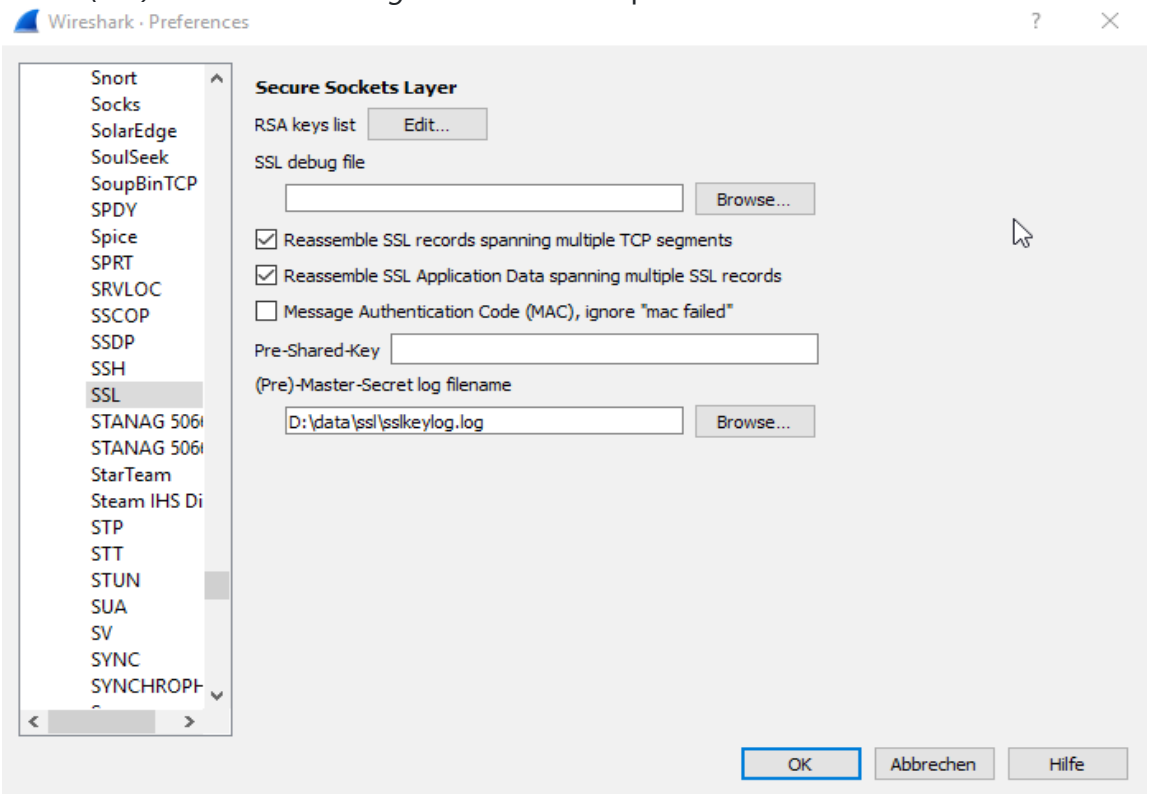
Einrichtung von Wireshark

Wenn man Firefox 63, Chromium 68 oder Chrome 66 verwendet, wird der symmetrische Sitzungsschlüssel auf jeden Fall mitgeschnitten. Jedoch muss man auch noch Wireshark einrichten damit der mitgeschnitte Datenverkehr entschlüsselt werden kann.

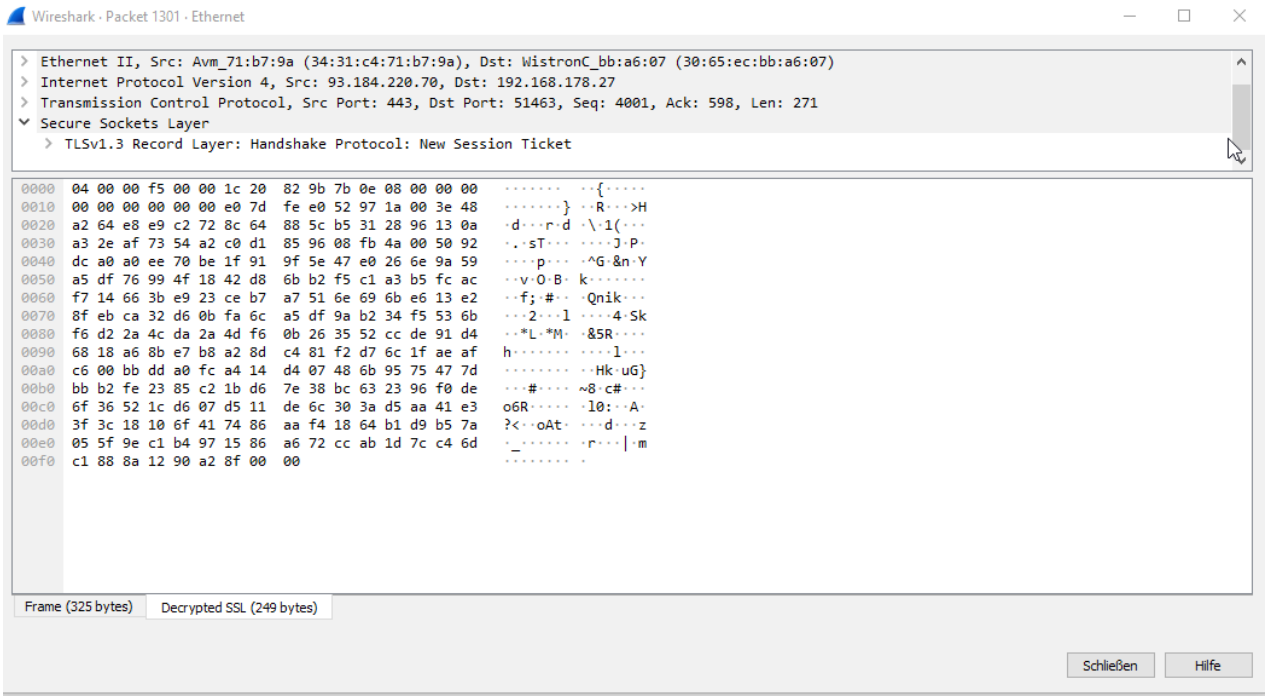
1. In Wireshark klickt man auf Bearbeiten und dann auf Einstellungen.



2. Wenn man das Tab Protokolle erweitert und dann auf SSL geht, setzt man im Feld von *(Pre)-Master-Secret log Filename* den Speicherort von SSLKEYLOGFILE ein.



3. Wenn man nun per Wireshark den Internetverkehr mitschneidet, und diesen anschließend analysiert, gibt es nun einen neuen Tab „Decrypted SSL Tab“



Eine Erklärung der Einträge in der SSL Keylogfile kann man unter folgendem Link nachlesen:
https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Key_Log_Format