Wireshark - Déchiffrer trafic https

Difficulté : Confirmé

Notions : TLS, chiffrement, capture de paquet.

I. Introduction

Cette procédure vise à expliquer comment déchiffrer du traffic https capturé avec wireshark.

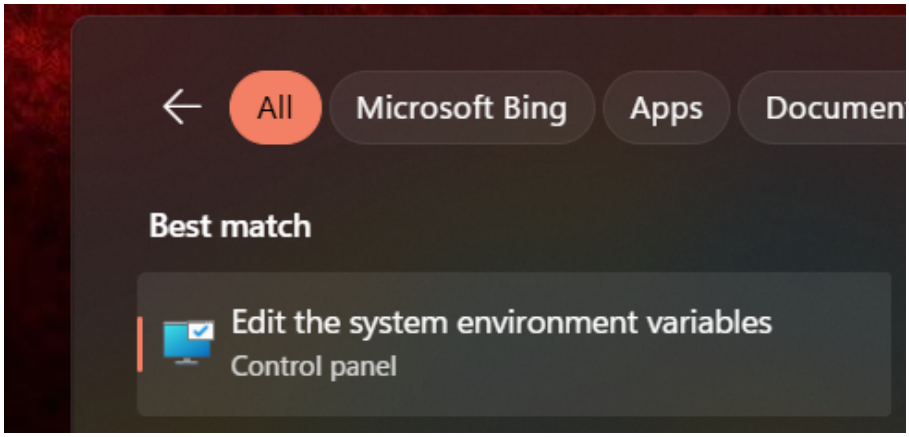
II. Préparation

Afin de déchiffrer le trafic HTTPS, il faudra au préalable disposer des clés qui ont été négociées lors du handshake.

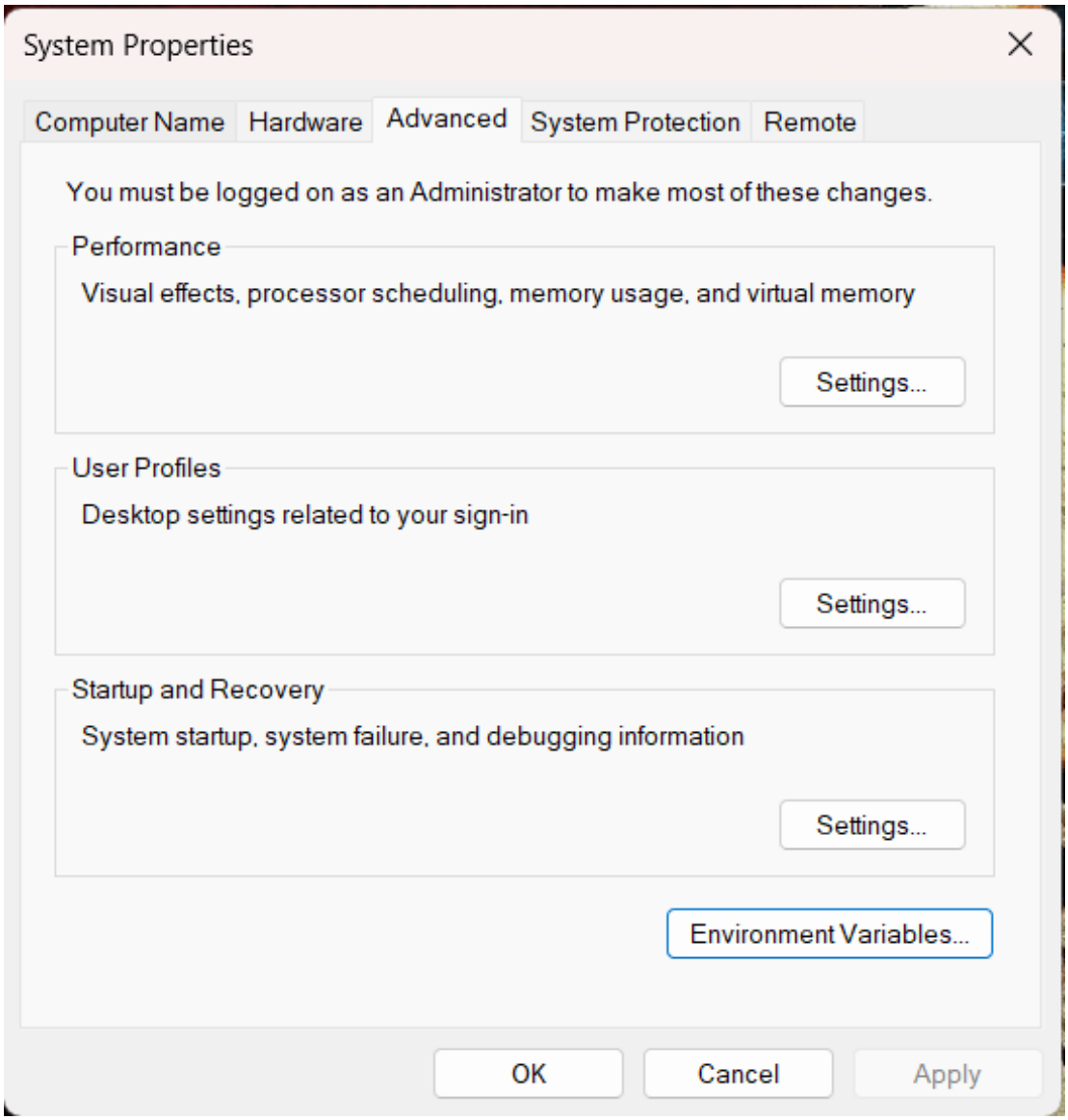
Les navigateurs basés sur Chrome / Chromium et firefox peuvent utiliser une variable d’environnement afin de logguer les clés qui ont été générée lors des Handshakes.

Sur windows (GUI)

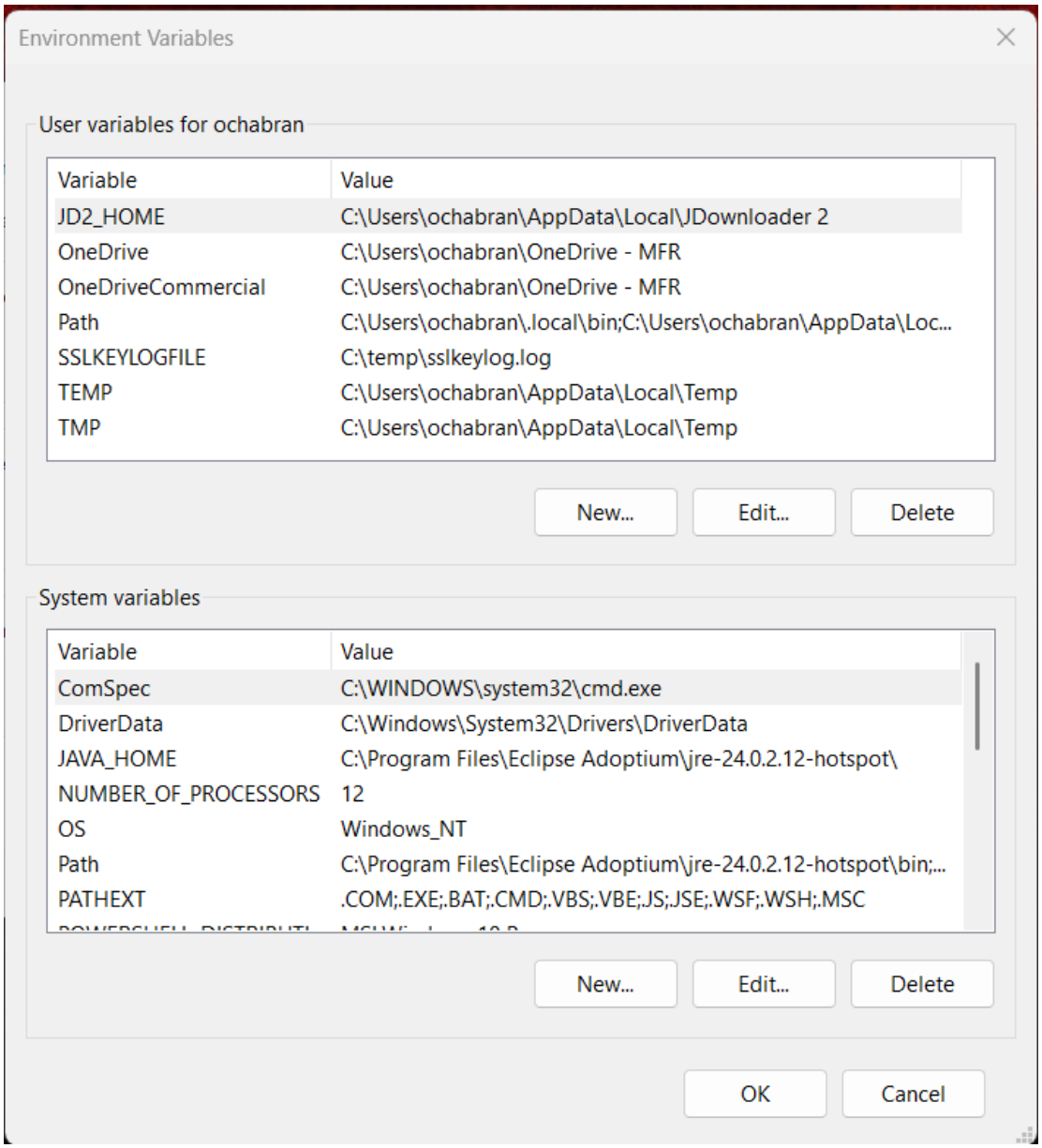
Ouvrir le menu démarrer et rechercher '***ENV***'.



Cliquer sur '***Environment variables...***'

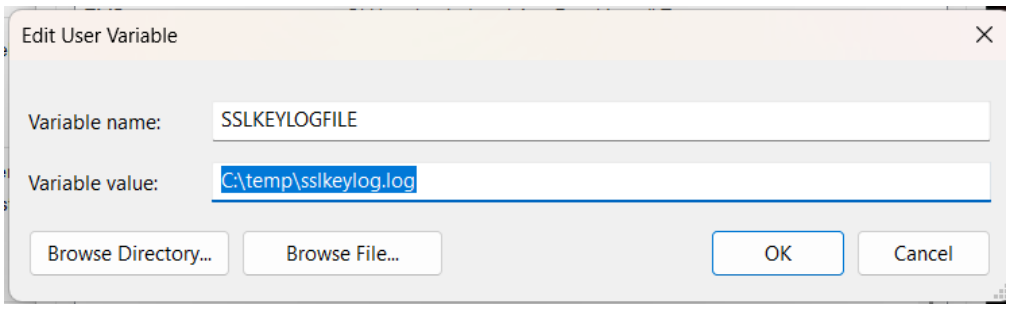


Ajouter une nouvelle variable d’environnement **utilisateur** en cliquant sur '***New***'.



Créer la variable suivante et valider en cliquant sur '***OK***'.

> **Attention** : Le fichier spécifié doit exister.



La variable sera prise en compte à la prochaine ouverture de session.

Sur linux (CLI)

> **Attention** : Le fichier spécifié doit exister.

Pour ajouter la variable temporairement :

```
export SSLKEYLOGFILE=/chemin/vers/le/fichier
```

Pour l'ajouter de façon permanente, il faut la déclarer dans le fichier ***~/.bashrc*** de l'utilisateur.

```
echo 'export SSLKEYLOGFILE=/chemin/vers/le/fichier' >> ~/.bashrc
```

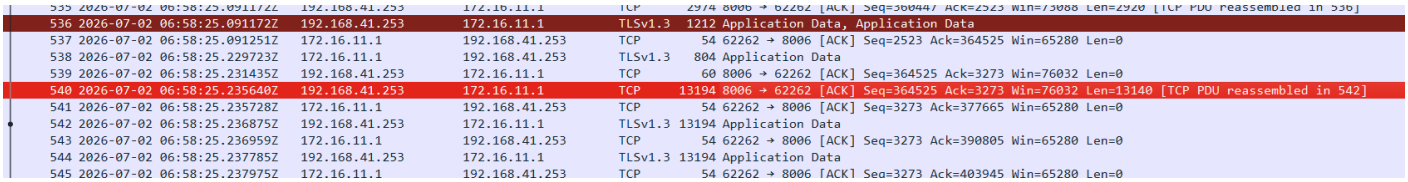
Elle prendra effet à la prochaine ouverture de session.

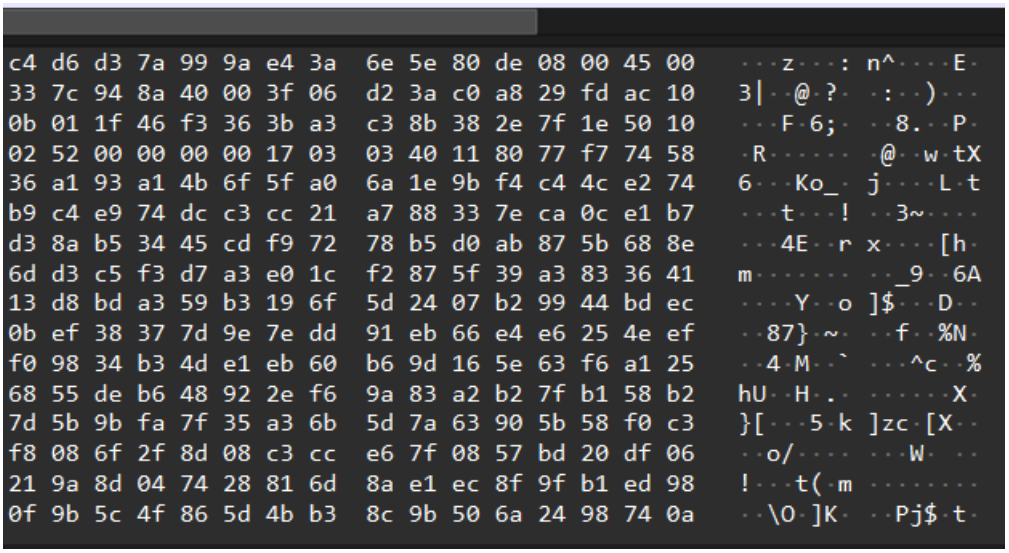
Après réouverture de session, il suffira de lancer la capture wireshark et de lancer le navigateur.

A la fin de la capture, l'enregistrer.

III. Déchiffrement des trames

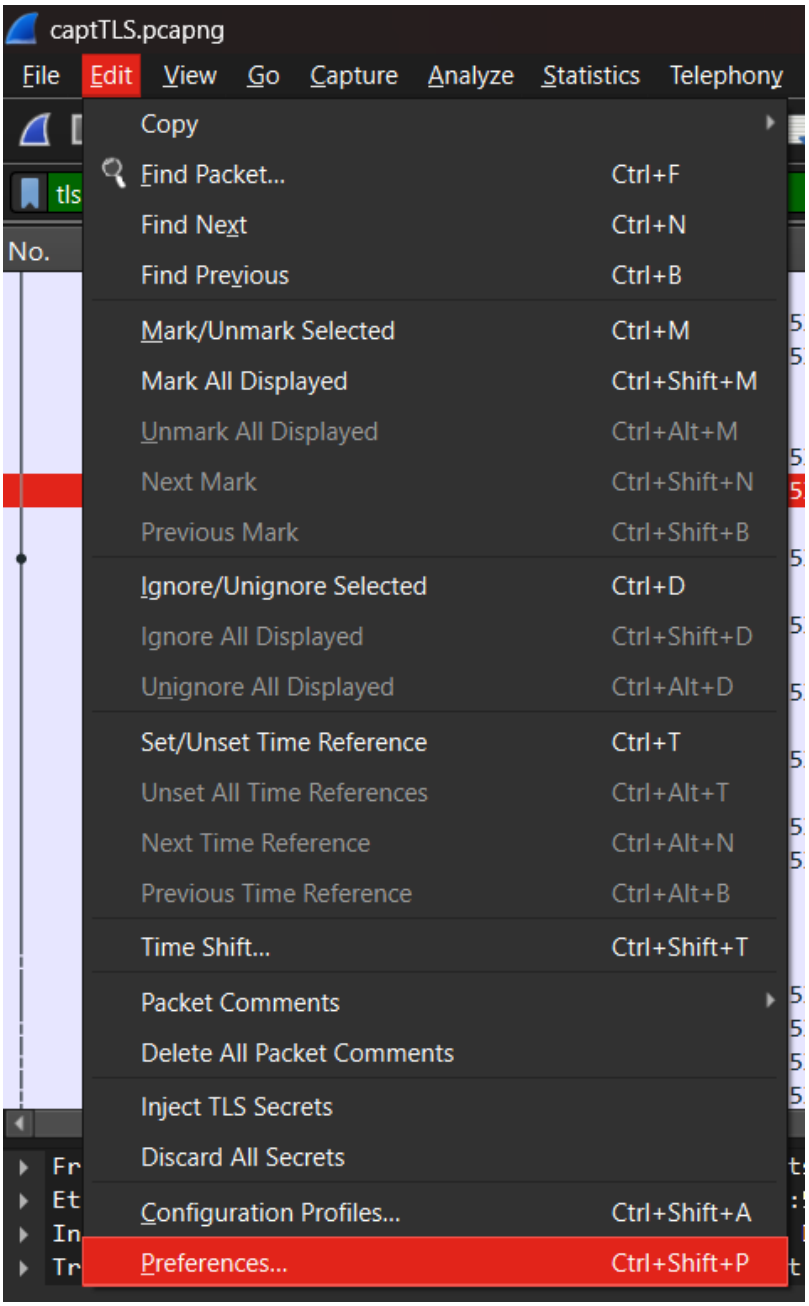
Ouvrir le fichier de capture. Celui-ci est pour lors chiffré.



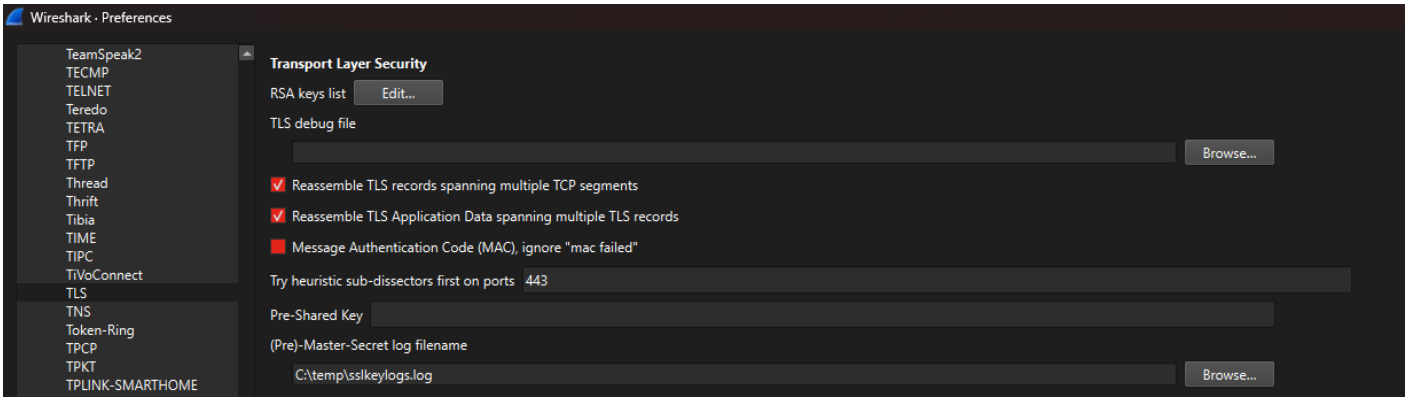


Pour le déchiffrer, il faut appliquer le fichier de clés récupérées lors des handshakes.

Pour cela, faire : '***Edit --> Preferences...***'.

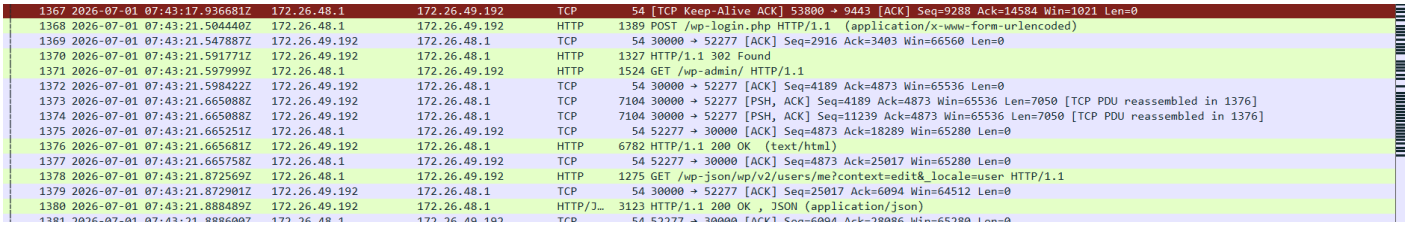


Dans la nouvelle fenêtre, se déplacer dans '***protocoles --> TLS***' puis entrer le chemin vers le fichier de capture dans le champ '***(Pre)-Master-Secret log filename***'.



Valider en cliquant sur '***Apply***'.

Cela aura pour effet de déchiffrer et d'ajouter tout le trafic qui était auparavant encapsulé dans la couche de présentation.



> **Astuce** : Cette méthode peut également servir sur d'autres protocoles comme ssh par exemple mais peut nécessiter des variantes.

Revision #2
Created 2026-07-29 14:04:54 UTC by Olivier
Updated 2026-07-29 14:14:40 UTC by Olivier