

Wireshark - Déchiffrer trafic https



Difficulté : Confirmé

Notions : TLS, chiffrement, capture de paquet.

I. Introduction

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

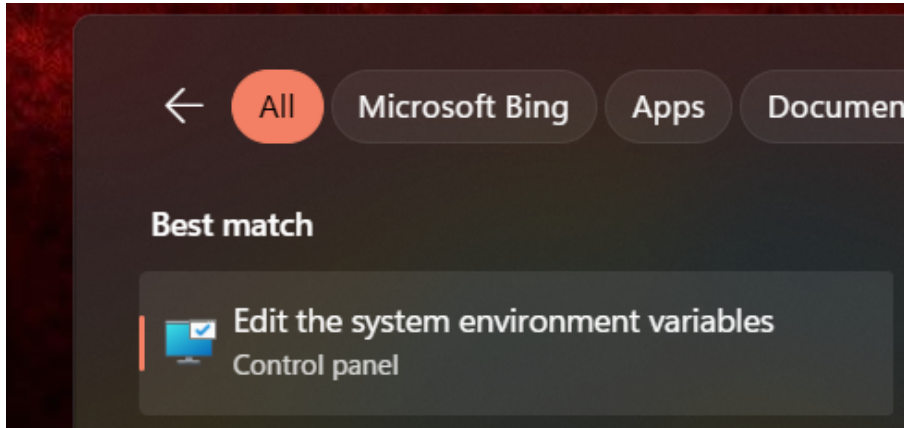
II. Préparation

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

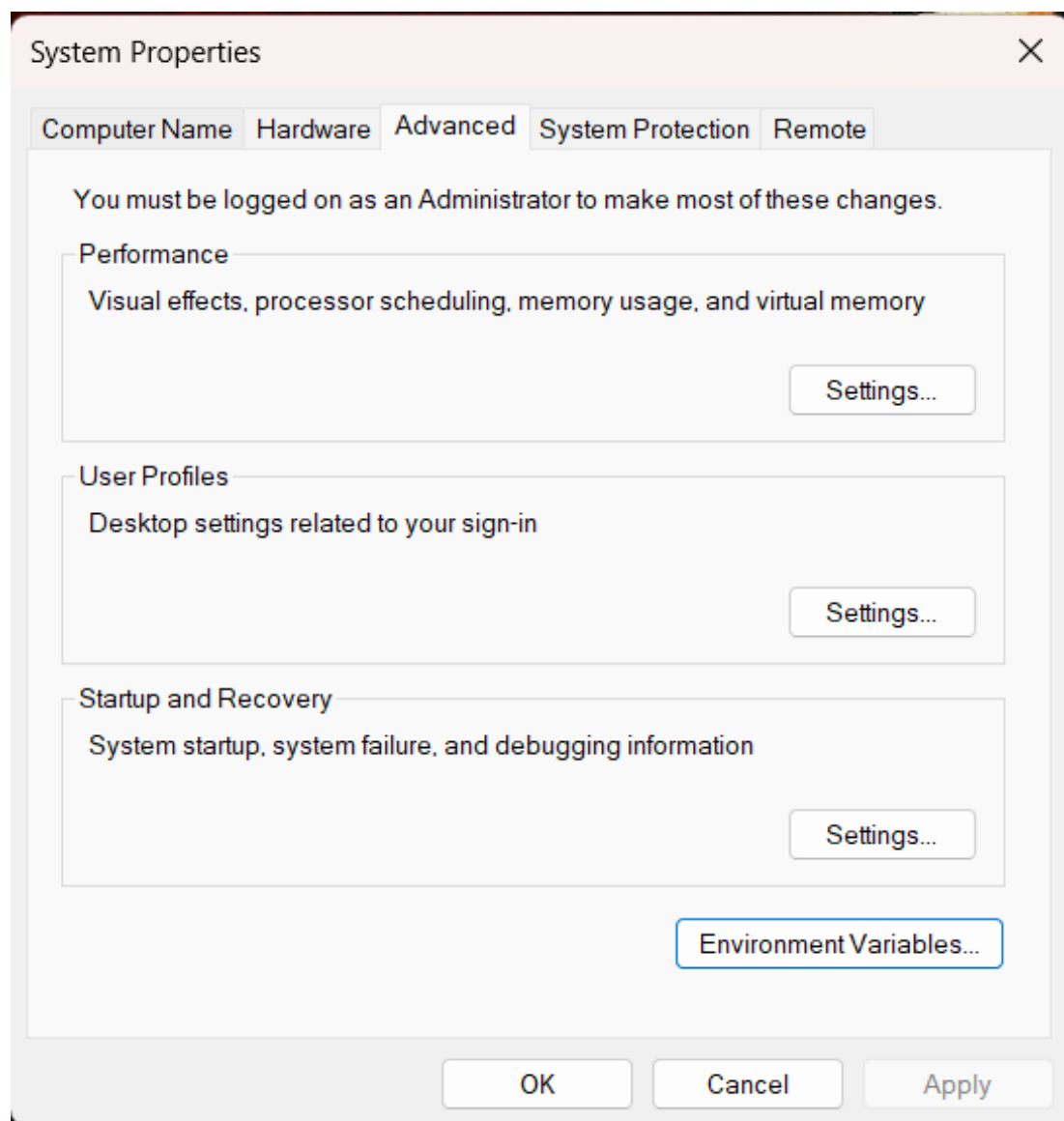
Les navigateurs basés sur Chrome / Chromium et firefox peuvent utiliser une variable d'environnement afin de logger les clés qui ont été générée lors des Handshakes.

Sur windows (GUI)

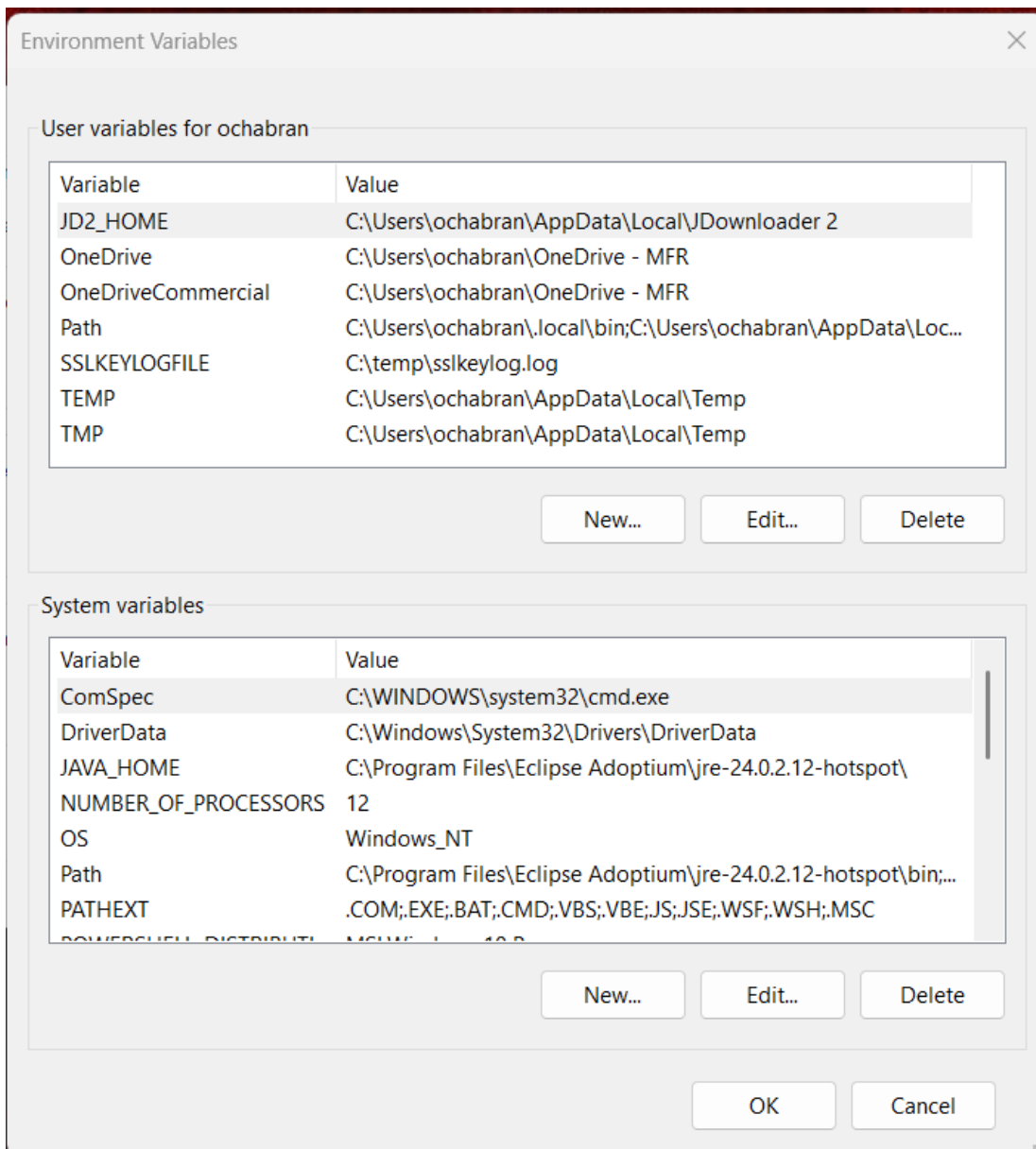
Ouvrir le menu démarrer et rechercher '**ENV**'.



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

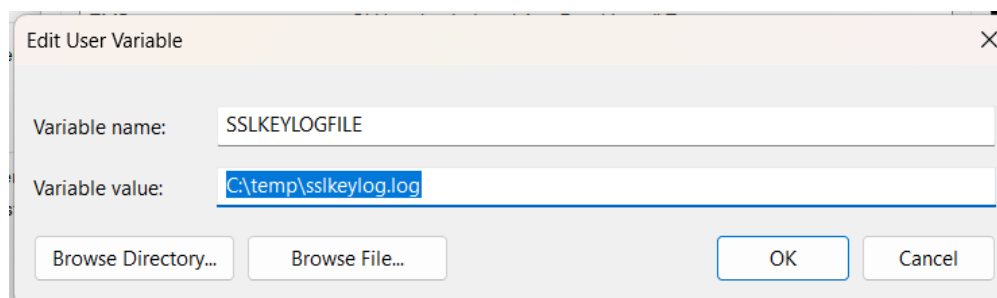


Ajouter une nouvelle variable d'environnement **utilisateur** en cliquant sur '**New**'.



Cr  er la variable suivante et valider en cliquant sur '**OK**'.

Attention : Le fichier sp  cifi   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.

536	2026-07-02 06:58:25.0911722	192.168.41.253	172.16.11.1	TCP	2974 8006 → 62262 [ACK] Seq=364525 Ack=403945 Win=3088 Len=2920 [TCP PDU reassembled in 536]
537	2026-07-02 06:58:25.0912517	172.16.11.1	192.168.41.253	TLSv1.3	1212 Application Data, Application Data
538	2026-07-02 06:58:25.2297232	172.16.11.1	192.168.41.253	TCP	54 62262 → 8006 [ACK] Seq=2523 Ack=364525 Win=65280 Len=0
539	2026-07-02 06:58:25.2314352	192.168.41.253	172.16.11.1	TLSv1.3	804 Application Data
540	2026-07-02 06:58:25.2356402	192.168.41.253	172.16.11.1	TCP	60 8006 → 62262 [ACK] Seq=364525 Ack=3273 Win=76032 Len=0
541	2026-07-02 06:58:25.2357282	172.16.11.1	192.168.41.253	TCP	13194 8006 → 62262 [ACK] Seq=364525 Ack=3273 Win=76032 Len=13140 [TCP PDU reassembled in 542]
542	2026-07-02 06:58:25.2368752	192.168.41.253	172.16.11.1	TCP	54 62262 → 8006 [ACK] Seq=3273 Ack=377665 Win=65280 Len=0
543	2026-07-02 06:58:25.2369592	172.16.11.1	192.168.41.253	TLSv1.3	13194 Application Data
544	2026-07-02 06:58:25.2377852	192.168.41.253	172.16.11.1	TCP	54 62262 → 8006 [ACK] Seq=3273 Ack=403945 Win=65280 Len=0
545	2026-07-02 06:58:25.2379752	172.16.11.1	192.168.41.253	TCP	54 62262 → 8006 [ACK] Seq=3273 Ack=403945 Win=65280 Len=0

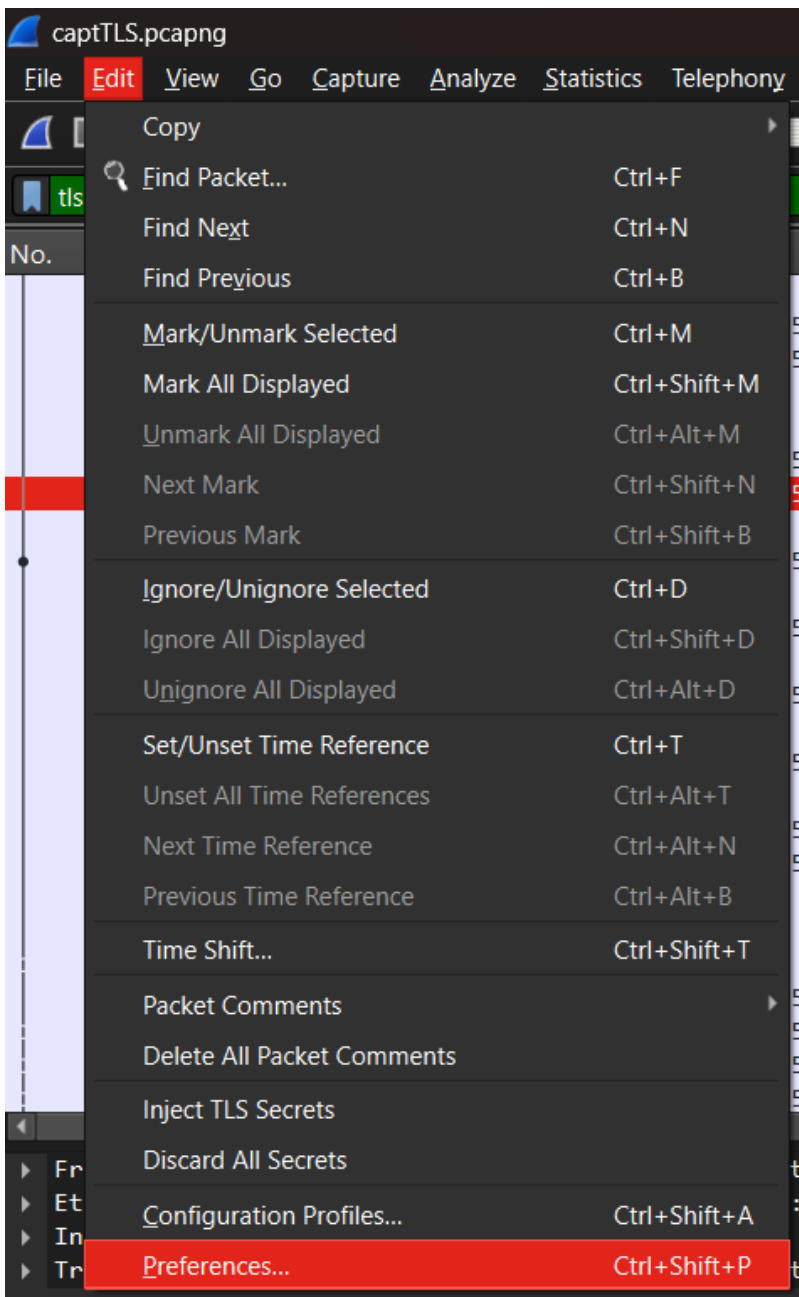
```

c4 d6 d3 7a 99 9a e4 3a 6e 5e 80 de 08 00 45 00  ...z...: n^...E
33 7c 94 8a 40 00 3f 06 d2 3a c0 a8 29 fd ac 10  3|...@?...:...)...
0b 01 1f 46 f3 36 3b a3 c3 8b 38 2e 7f 1e 50 10  ...F6;...8...P
02 52 00 00 00 00 17 03 03 40 11 80 77 f7 74 58  ...R.....@...w.tX
36 a1 93 a1 4b 6f 5f a0 6a 1e 9b f4 c4 4c e2 74  6...Ko_...j...L.t
b9 c4 e9 74 dc c3 cc 21 a7 88 33 7e ca 0c e1 b7  ...t...!...3~...
d3 8a b5 34 45 cd f9 72 f8 b5 d0 ab 87 5b 68 8e  ...4E...r x...[h
6d d3 c5 f3 d7 a3 e0 1c f2 87 5f 39 a3 83 36 41  m....._9...6A
13 d8 bd a3 59 b3 19 6f 5d 24 07 b2 99 44 bd ec  ...Y...o ]$...D...
0b ef 38 37 7d 9e 7e dd 91 eb 66 e4 e6 25 4e ef  ...87}...~...f...%N
f0 98 34 b3 4d e1 eb 60 b6 9d 16 5e 63 f6 a1 25  ...4.M...^c...%
68 55 de b6 48 92 2e f6 9a 83 a2 b2 7f b1 58 b2  hU...H...X
7d 5b 9b fa 7f 35 a3 6b 5d 7a 63 90 5b 58 f0 c3  }[...5.k ]zc[X
f8 08 6f 2f 8d 08 c3 cc e6 7f 08 57 bd 20 df 06  ...o/...W...
21 9a 8d 04 74 28 81 6d 8a e1 ec 8f 9f b1 ed 98  !...t(m.....
0f 9b 5c 4f 86 5d 4b b3 8c 9b 50 6a 24 98 74 0a  ...\0...K...Pj$.t

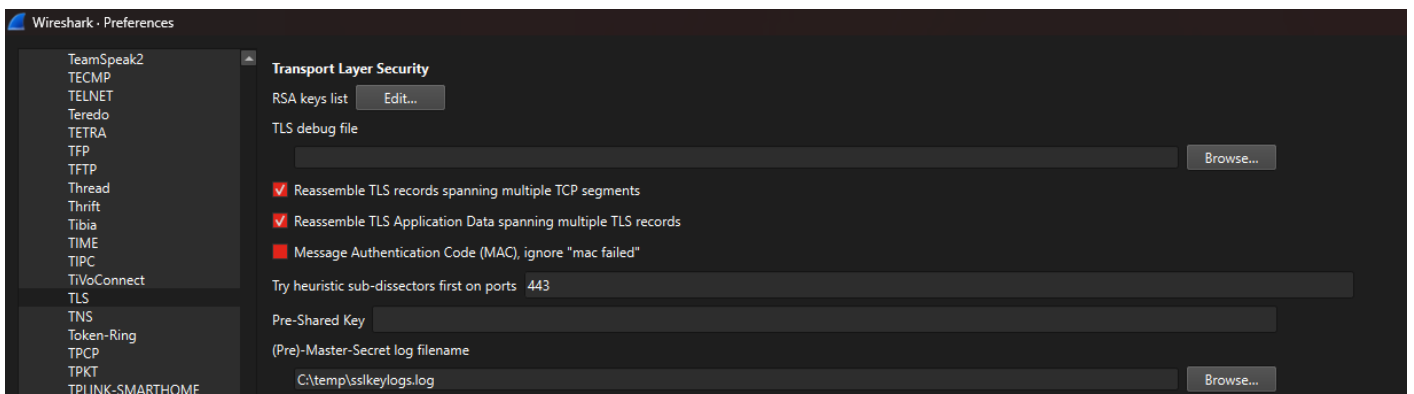
```

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.

1367	2026-07-01	07:43:17.936681Z	172.26.48.1	172.26.49.192	TCP	54 [TCP Keep-Alive ACK] Seq=53800 → 9443 [ACK] Seq=9288 Ack=14584 Win=1021 Len=0
1368	2026-07-01	07:43:21.504440Z	172.26.48.1	172.26.49.192	HTTP	1389 POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
1369	2026-07-01	07:43:21.547887Z	172.26.49.192	172.26.48.1	TCP	54 30000 → 52277 [ACK] Seq=2916 Ack=3403 Win=66560 Len=0
1370	2026-07-01	07:43:21.591771Z	172.26.49.192	172.26.48.1	HTTP	1327 HTTP/1.1 302 Found
1371	2026-07-01	07:43:21.597999Z	172.26.48.1	172.26.49.192	HTTP	1524 GET /wp-admin/ HTTP/1.1
1372	2026-07-01	07:43:21.598422Z	172.26.49.192	172.26.48.1	TCP	54 30000 → 52277 [ACK] Seq=4189 Ack=4873 Win=65536 Len=0
1373	2026-07-01	07:43:21.665088Z	172.26.49.192	172.26.48.1	TCP	7104 30000 → 52277 [PSH, ACK] Seq=4189 Ack=4873 Win=65536 Len=7050 [TCP PDU reassembled in 1376]
1374	2026-07-01	07:43:21.665088Z	172.26.49.192	172.26.48.1	TCP	7104 30000 → 52277 [PSH, ACK] Seq=11239 Ack=4873 Win=65536 Len=7050 [TCP PDU reassembled in 1376]
1375	2026-07-01	07:43:21.665251Z	172.26.48.1	172.26.49.192	TCP	54 52277 → 30000 [ACK] Seq=4873 Ack=18289 Win=65280 Len=0
1376	2026-07-01	07:43:21.665681Z	172.26.49.192	172.26.48.1	HTTP	6782 HTTP/1.1 200 OK (text/html)
1377	2026-07-01	07:43:21.665758Z	172.26.48.1	172.26.49.192	TCP	54 52277 → 30000 [ACK] Seq=4873 Ack=25017 Win=65280 Len=0
1378	2026-07-01	07:43:21.872569Z	172.26.48.1	172.26.49.192	HTTP	1275 GET /wp-json/wp/v2/users/me?context=edit&_locale=user HTTP/1.1
1379	2026-07-01	07:43:21.872901Z	172.26.49.192	172.26.48.1	TCP	54 30000 → 52277 [ACK] Seq=25017 Ack=6094 Win=64512 Len=0
1380	2026-07-01	07:43:21.888489Z	172.26.49.192	172.26.48.1	HTTP/1.1	3123 HTTP/1.1 200 OK , JSON (application/json)
1381	2026-07-01	07:43:21.888600Z	172.26.48.1	172.26.49.192	TCP	54 52277 → 30000 [ACK] Seq=6094 Ack=30000 Win=65280 Len=0

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