Come Usare Wireshark per decriptare le connessioni TLS

La crittografia SSL rende l'utilizzo di Wireshark più impegnativo perché impedisce di visualizzare il contenuto dei dati trasportati da ciascun pacchetto a meno che non si ha a disposizione l'apposita **chiave di decifratura***.
In questa guida vedremo come è possibile configurare correttamente Wireshark al fine di consentirgli di decifrare il contenuto dei pacchetti TLS e visualizzarne il loro contenuto.

Step 1. Salvare la chiave segreta per la decifratura

Come anticipato, per poter decifrare correttamente le connessioni TLS, abbiamo bisogno di una chiave di decifratura. Tale chiave viene generata dal client nel momento in cui si stabilisce la connessione con il server ed è chiamata "**pre-master-secret key**".

È possibile visualizzare/salvare la pre-master-secret key in Windows/Linux/MacOS aggiungendo tra le variabili d'ambiente del nostro sistema operativo la SSLKEYLOGFILE seguita dal path in cui vogliamo salvare il file contenente la chiave segreta:
Ad esempio, su Linux e MacOS basterà aprire un terminale e scrivere:

```
export SSLKEYLOGFILE="/home/<account_name>/sslkeyfile.key"
```

Similarmente, è possibile esportare la variabile d'ambiente in windows usando il comando **set** tramite il prompt dei comandi o powershell:

```
set SSLKEYLOGFILE=%USERPROFILE%\Desktop\keylogfile.txt
```

Infine, avviare il browser e navigare su un sito a scelta.

Step 2. Configurare Wireshark per decifrare le connessioni

1. Aprire Wireshark
2. Recarsi in: preferenze → protocolli → TLS
3. Cliccare sul tasto **Browse** sotto il menù **(Pre)-Master-Secret log filename**
4. Specificare il path scelto allo step 1 per la chiave pre-master-secret
5. Salvare ed avviare la cattura

Suggerimenti.

È possible usare i seguenti script per automatizzare la procedura dello step 1.

- **Chiave di decifratura:** Una chiave segreta pre-master viene generata dal client e utilizzata dal server per derivare una chiave master che crittografa il traffico della sessione. È lo standard attuale in crittografia. Solitamente viene implementato tramite Diffie-Hellman.

Windows (start-chrome.cmd)

```
@echo off
set SSLKEYLOGFILE=%USERPROFILE%\Desktop\key.log
start chrome
```

MacOS (start-chrome.sh)

```
export SSLKEYLOGFILE=~/Desktop/key.log
open -n /Applications/Google\ Chrome.app
```

Linux (start-chrome.sh)

```
export SSLKEYLOGFILE=$HOME/Scrivania/key.log
google-chrome &
```

- **Chiave di decifratura:** Una chiave segreta pre-master viene generata dal client e utilizzata dal server per derivare una chiave master che crittografa il traffico della sessione. È lo standard attuale in crittografia. Solitamente viene implementato tramite Diffie-Hellman.