Wireshark - Notions avancées

Difficulté : Confirmé

Notions : Réseaux, protocoles, analyse de trame.

I.Introduction

Ce document a pour but de vous apprendre à utiliser les fonctions avancées de wireshark

> Wireshark peut être téléchargé ici : Download Wireshark

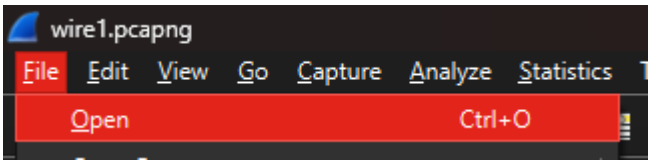
> Cette documentation fait suite à : Wireshark - Installation et utilisation

> Prérequis : Un poste sous Windows 7 minimum, Une carte réseau RJ45 ou une carte wifi.

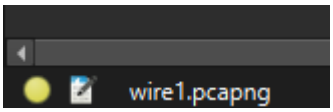
II. Informations de capture

2.1 Voir les détails de la capture

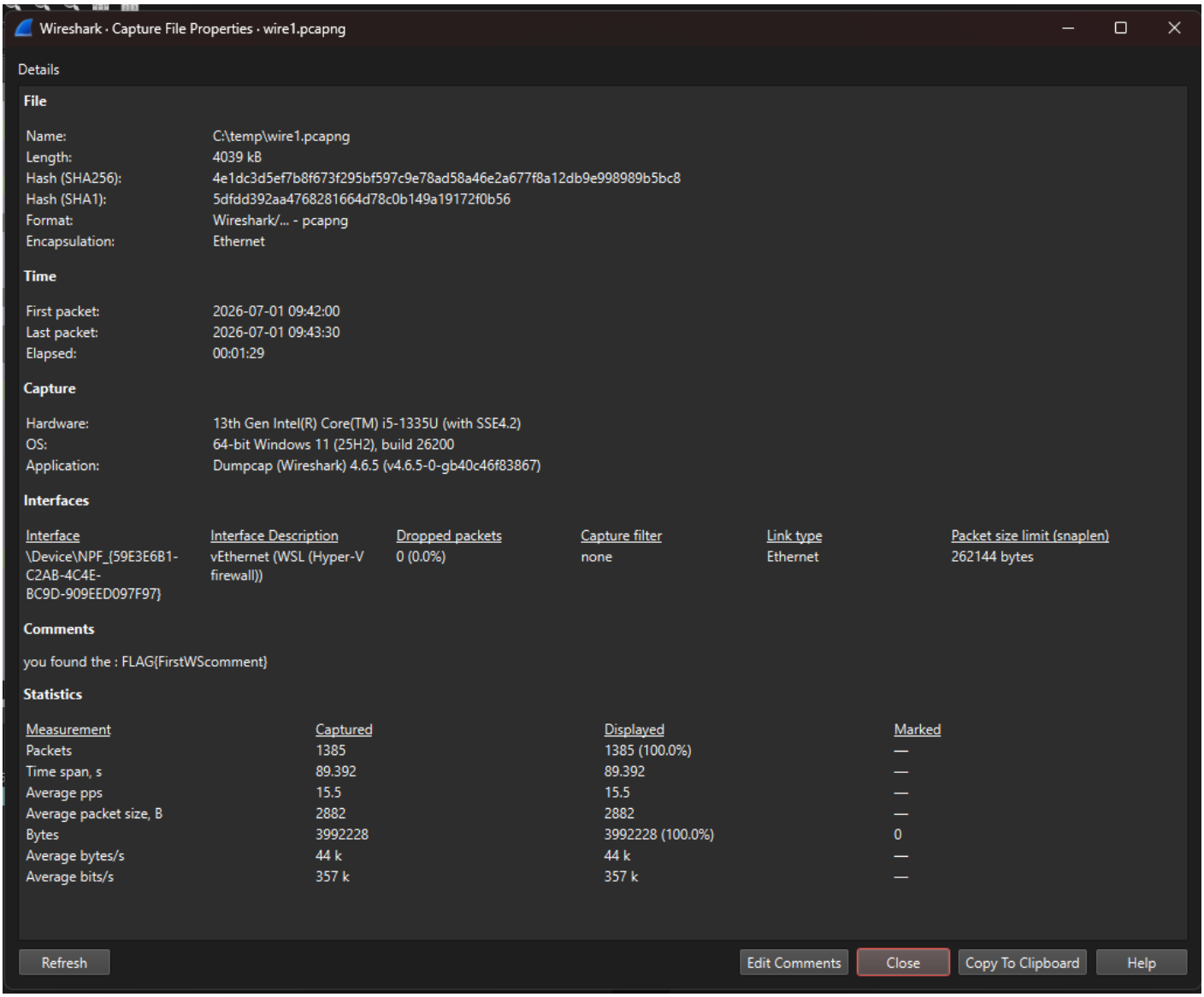
Pour voir les détails d'une capture, ouvrir la capture avec '***Fichier --> Ouvrir***'.



En bas à gauche, cliquer sur l'icône du fichier de capture.

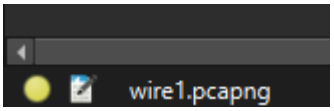


Il est possible d'y trouver les informations de la capture.

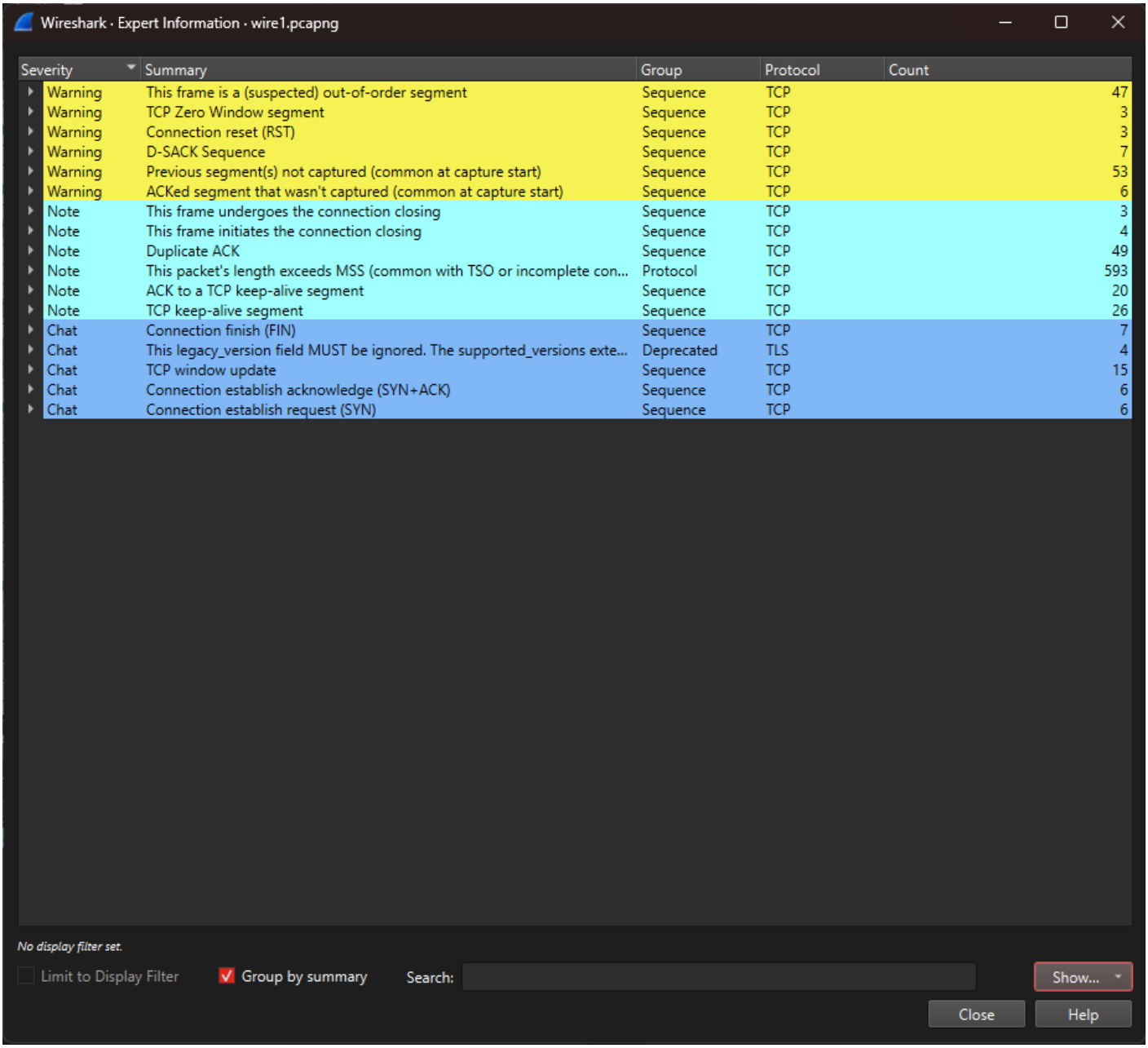


2.2 Voir les résultats de capture

En bas à gauche, cliquer sur l'icône du rond vert.



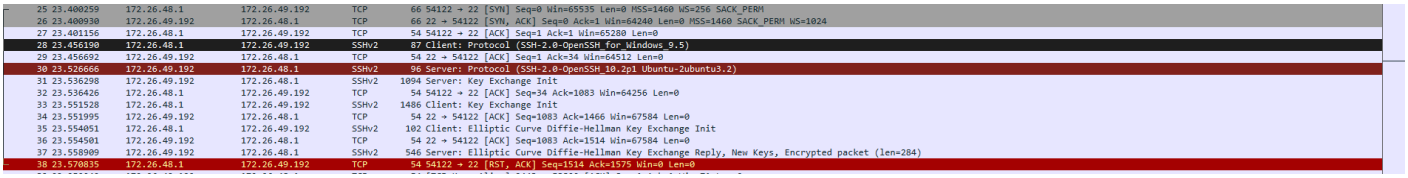
Il est possible de voir les résultats et statistiques de la capture.



III. Suivre un stream

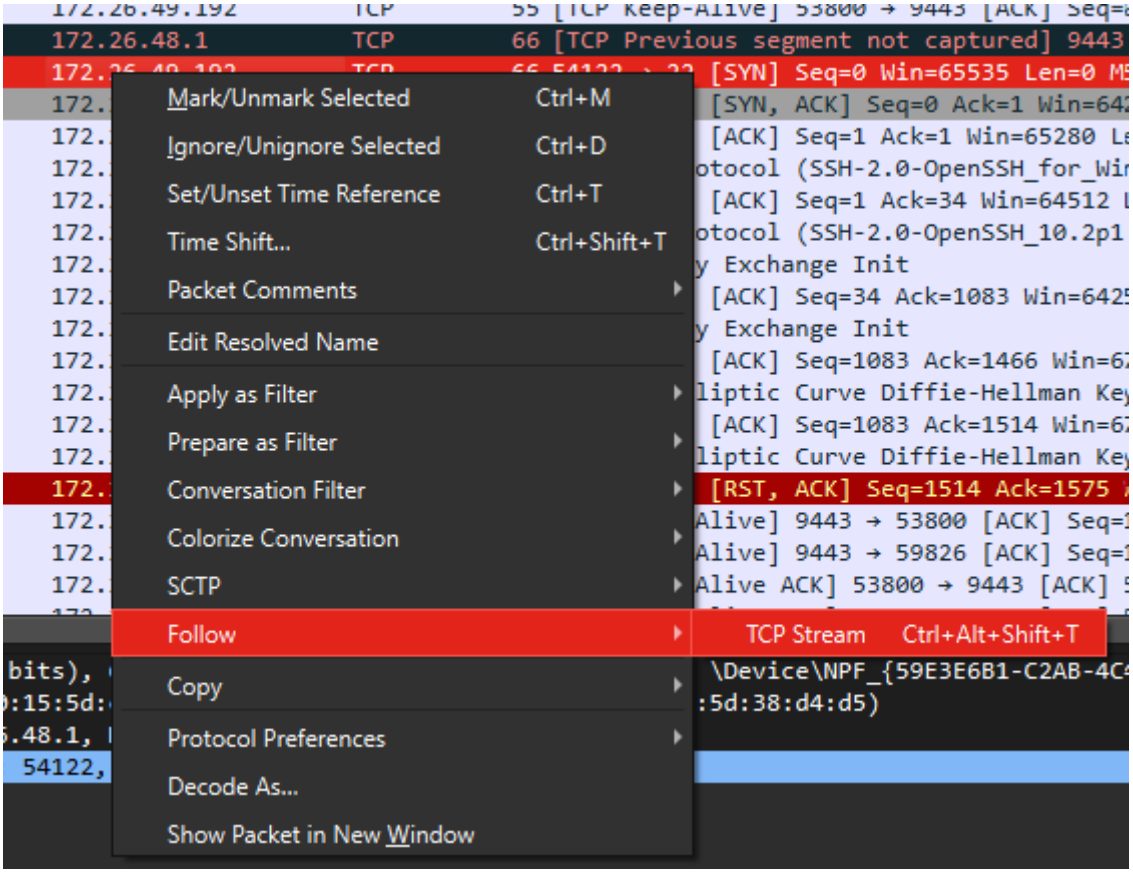
3.1 Suivre un stream TCP

Pour filtrer la vue sur un échange en particulier, clic droit sur l'un des paquets du stream.

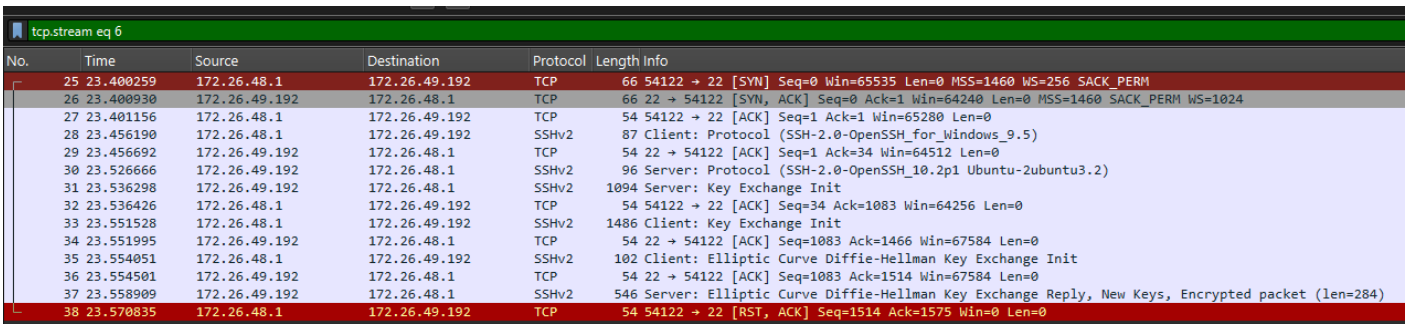


ici, par exemple, un flux SSHv2

faire un '**clic droit --> Follow --> TCP Stream**'.



Cela va filtrer uniquement les trames liées à cet échange :

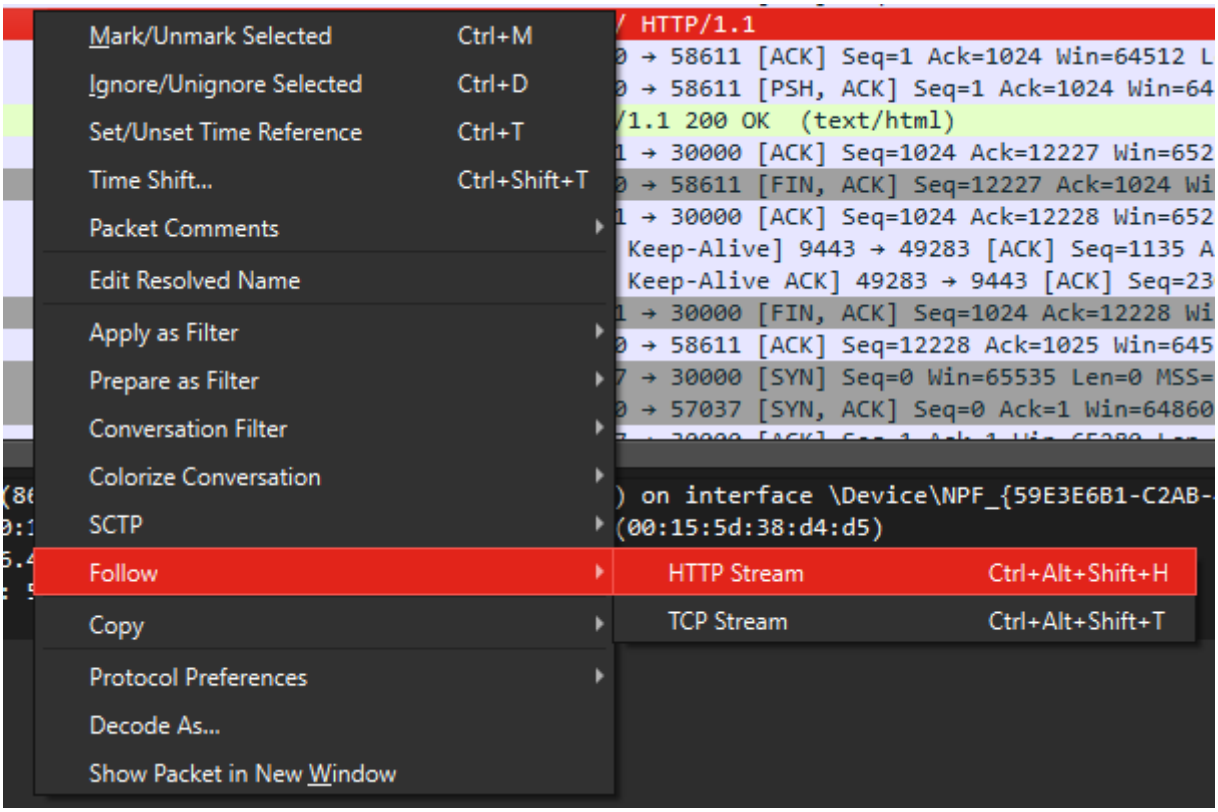


Et également afficher une nouvelle fenêtre dans laquelle sera affiché le détail des échanges.

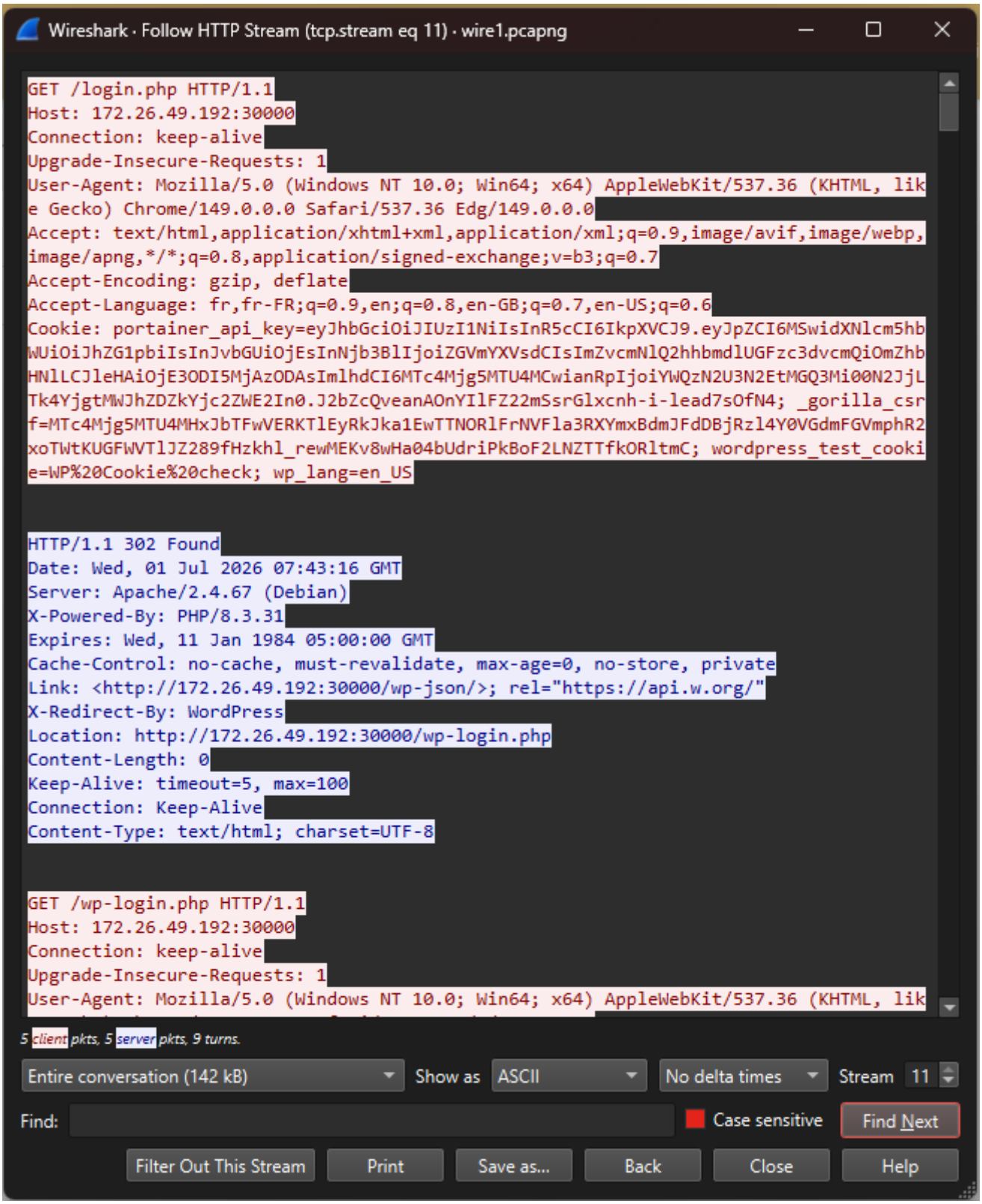
3.2 Suivre un stream HTTP(s)

De la même manière il est possible de suivre un stream HTTP ou HTTPS :

faire un '**clic droit --> Follow --> HTTP Stream**'.

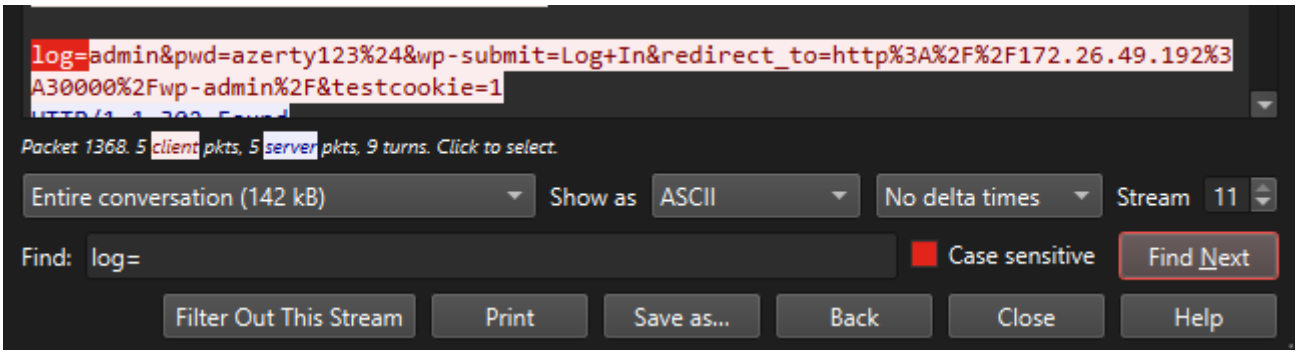


Cela permettra d'afficher la page récapitulative :



3.3 Trouver une information dans le stream

Il est ensuite possible grâce à la barre de recherche en bas de rechercher une information particulière dans le stream.



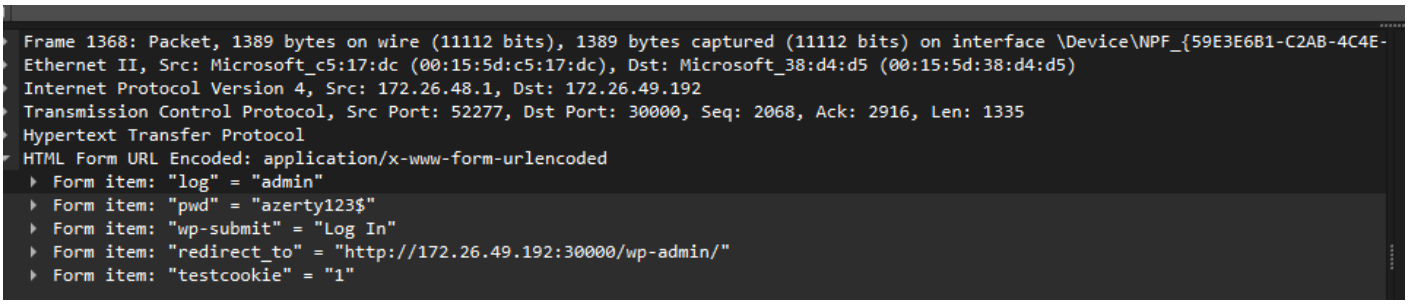
IV. Actions sur la liste

4.1 Rechercher une information

Faire '***ctrl+F***' pour activer la barre de recherche :

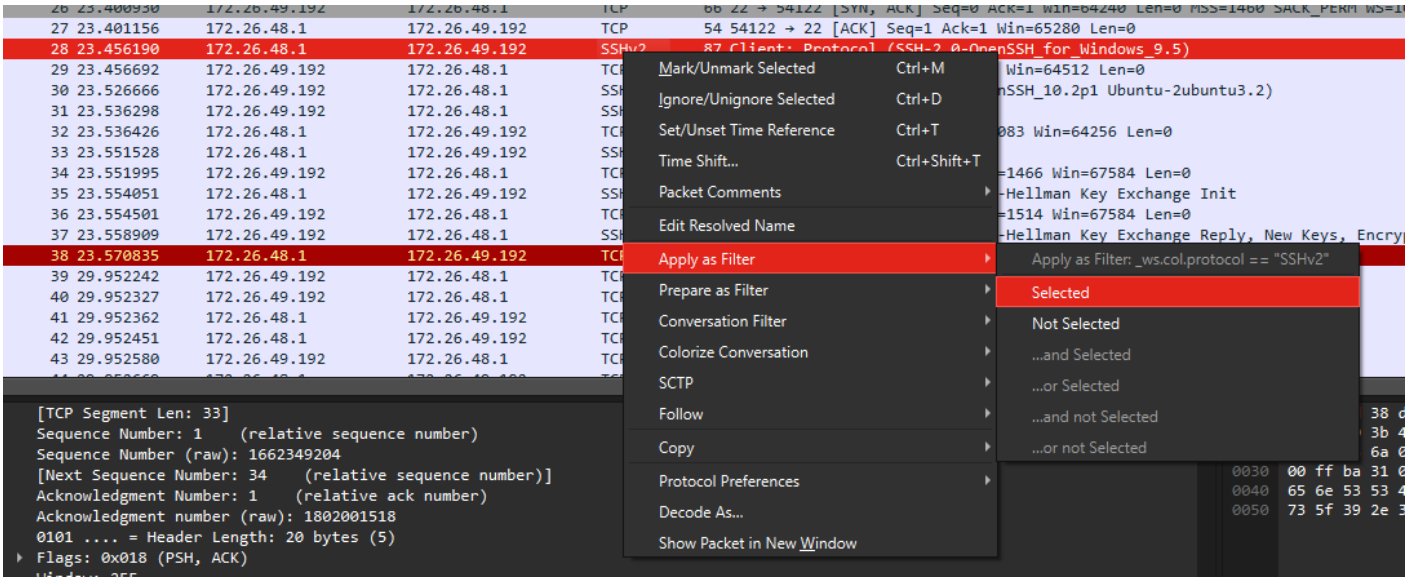
Cette barre permet de rechercher des données dans la liste ou dans le contenu des trames.

Par exemple avec les critères '***Packet Details***' et '***String***' puis la valeur '***admin***' :



4.2 Appliquer un filtre dynamique

Pour appliquer un filtre dynamique, il est possible de faire un clic droit sur l'une des informations disponible (ip, port, protocole, etc...) et de faire un '***clic droit --> Apply as Filter --> Selected***' pour appliquer ce filtre.

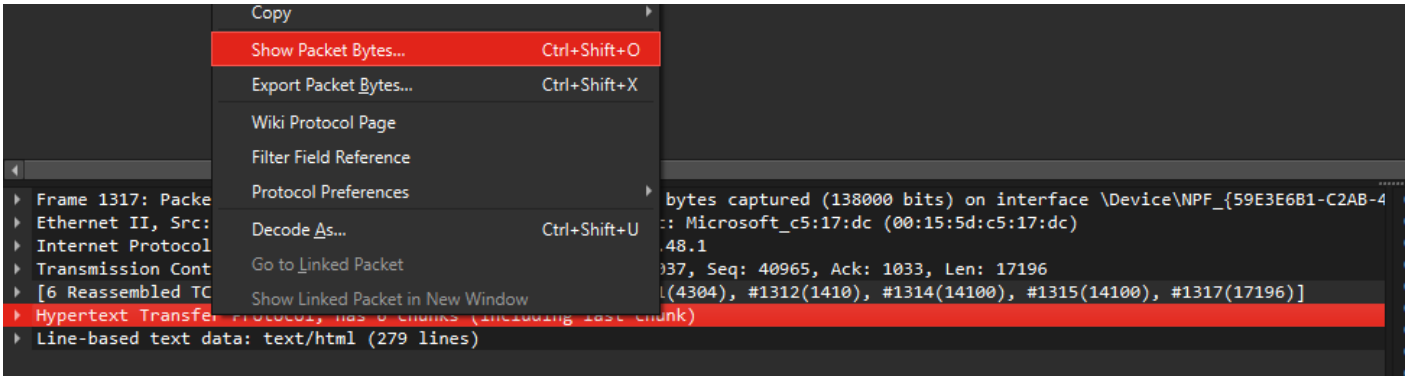


4.3 Afficher / Exporter des données

Cliquer sur une trame, puis sur un morceau de trame, il est possible d'afficher ou d'exporter la donnée contenue.

Faire un '***clic droit --> Show Packet Bytes***' pour afficher le contenu.

Si il s'agit d'un contenu spécifique (page web, image, email, fichier), faire un '***clic droit --> Export Packet Bytes***' Pour le sauvegarder au bon format.



Revision #3
Created 2026-07-29 14:04:53 UTC by Olivier
Updated 2026-07-29 14:14:22 UTC by Olivier