

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](#)

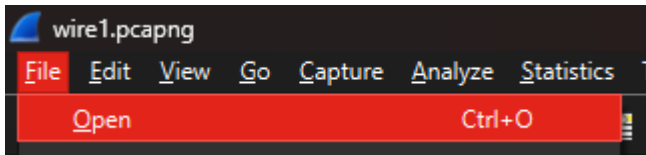
Cette documentation fait suite à : [Wireshark - Installation et utilisation](#)

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

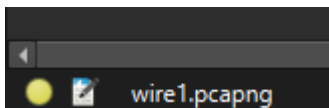
II. Informations de capture

2.1 Voir les détails de la capture

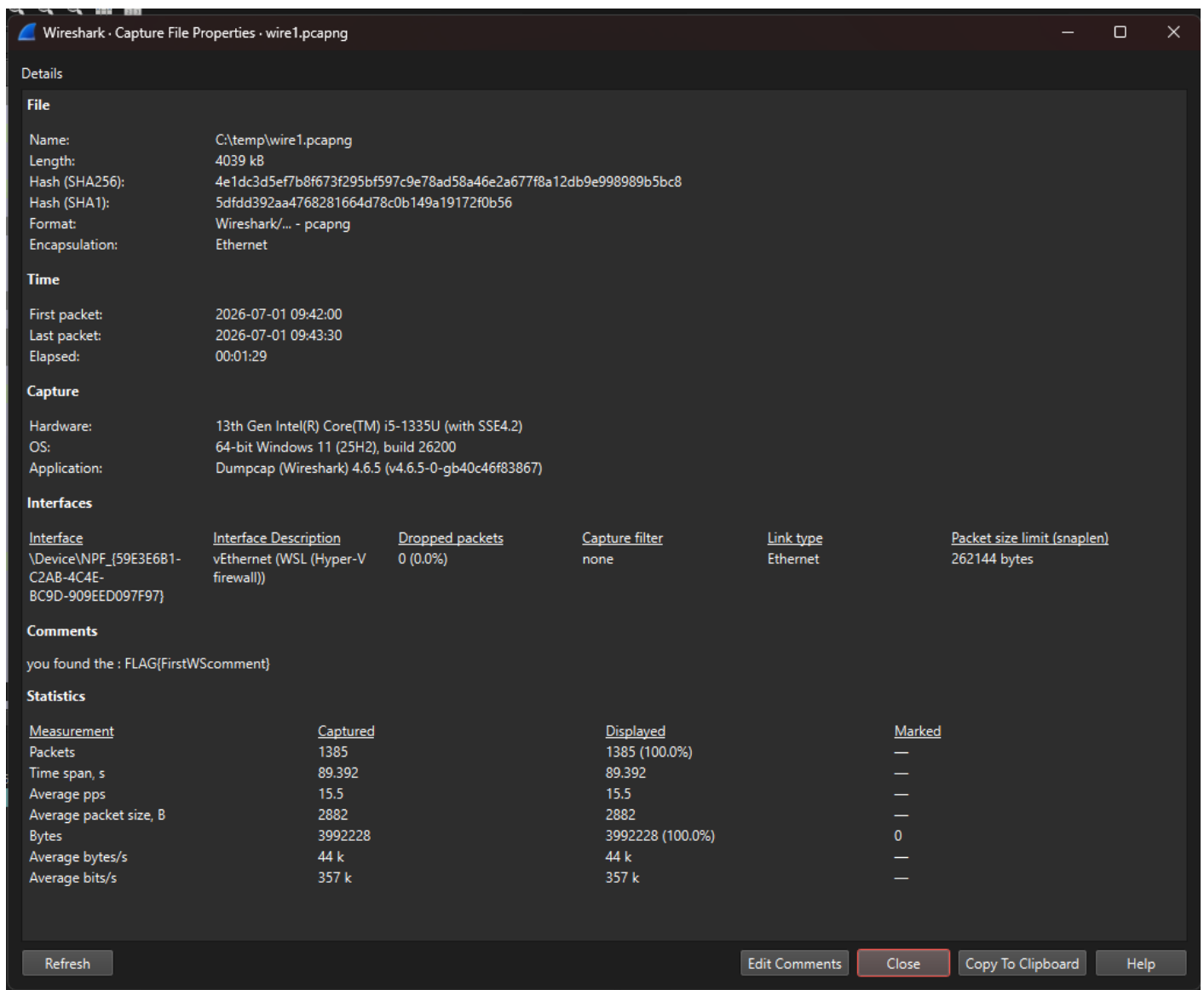
Pour voir les détails d'une capture, ouvrir la capture avec '**Fichier --> Ouvrir**'.



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

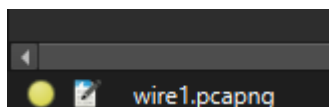


Il est possible d'y trouver les informations de la capture.



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.

Wireshark · Expert Information · wire1.pcapng

Severity	Summary	Group	Protocol	Count
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	47
Warning	TCP Zero Window segment	Sequence	TCP	3
Warning	Connection reset (RST)	Sequence	TCP	3
Warning	D-SACK Sequence	Sequence	TCP	7
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	53
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	6
Note	This frame undergoes the connection closing	Sequence	TCP	3
Note	This frame initiates the connection closing	Sequence	TCP	4
Note	Duplicate ACK	Sequence	TCP	49
Note	This packet's length exceeds MSS (common with TSO or incomplete con...	Protocol	TCP	593
Note	ACK to a TCP keep-alive segment	Sequence	TCP	20
Note	TCP keep-alive segment	Sequence	TCP	26
Chat	Connection finish (FIN)	Sequence	TCP	7
Chat	This legacy_version field MUST be ignored. The supported_versions exte...	Deprecated	TLS	4
Chat	TCP window update	Sequence	TCP	15
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	6
Chat	Connection establish request (SYN)	Sequence	TCP	6

No display filter set.

☐ Limit to Display Filter
 ☒ Group by summary
 Search:

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.

25	23.400259	172.26.48.1	172.26.49.192	TCP	66	54122 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
26	23.400930	172.26.49.192	172.26.48.1	TCP	66	22 → 54122 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=1024
27	23.401156	172.26.48.1	172.26.49.192	TCP	54	54122 → 22 [ACK] Seq=1 Ack=1 Win=65280 Len=0
28	23.456190	172.26.48.1	172.26.49.192	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_for_Windows_9.5)
29	23.456692	172.26.49.192	172.26.48.1	TCP	54	22 → 54122 [ACK] Seq=1 Ack=34 Win=64512 Len=0
30	23.526666	172.26.49.192	172.26.48.1	SSHv2	96	Server: Protocol (SSH-2.0-OpenSSH_10.2p1 Ubuntu-2ubuntu3.2)
31	23.536298	172.26.49.192	172.26.48.1	SSHv2	1094	Server: Key Exchange Init
32	23.536426	172.26.48.1	172.26.49.192	TCP	54	54122 → 22 [ACK] Seq=34 Ack=1083 Win=64256 Len=0
33	23.551528	172.26.48.1	172.26.49.192	SSHv2	1486	Client: Key Exchange Init
34	23.551995	172.26.49.192	172.26.48.1	TCP	54	22 → 54122 [ACK] Seq=1083 Ack=1466 Win=67584 Len=0
35	23.554051	172.26.48.1	172.26.49.192	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
36	23.554501	172.26.49.192	172.26.48.1	TCP	54	22 → 54122 [ACK] Seq=1083 Ack=1514 Win=67584 Len=0
37	23.558909	172.26.49.192	172.26.48.1	SSHv2	546	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=284)
38	23.570835	172.26.48.1	172.26.49.192	TCP	54	54122 → 22 [RST, ACK] Seq=1514 Ack=1575 Win=0 Len=0

ici, par exemple, un flux SSHv2

faire un 'cllic droit --> Follow --> TCP Stream'.

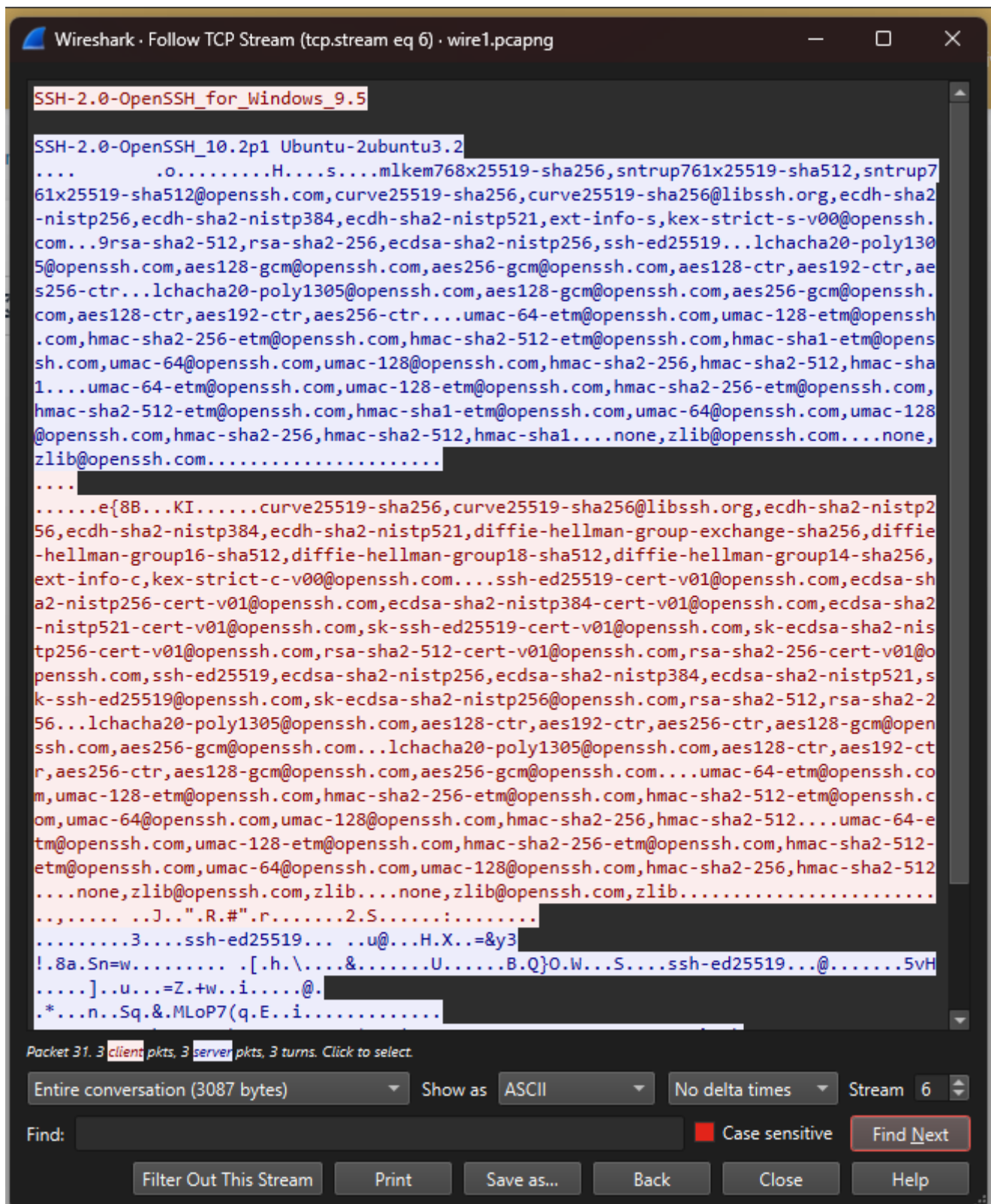
172.26.49.192
TCP
55
[TCP Keep-Alive] 53800 → 9443 [ACK] Seq=
172.26.48.1
TCP
66
[TCP Previous segment not captured] 9443
172.26.49.192
TCP
66
54122 → 22 [SYN] Seq=0 Win=65535 Len=0 MS
172.
Mark/Unmark Selected
Ctrl+M
[SYN, ACK] Seq=0 Ack=1 Win=64
172.
Ignore/Unignore Selected
Ctrl+D
[ACK] Seq=1 Ack=1 Win=65280 L
172.
Set/Unset Time Reference
Ctrl+T
otocol (SSH-2.0-OpenSSH_for_Win
172.
Time Shift...
Ctrl+Shift+T
[ACK] Seq=1 Ack=34 Win=64512 l
otocol (SSH-2.0-OpenSSH_10.2p1
y Exchange Init
[ACK] Seq=34 Ack=1083 Win=6425
y Exchange Init
[ACK] Seq=1083 Ack=1466 Win=6
liptic Curve Diffie-Hellman Key
[ACK] Seq=1083 Ack=1514 Win=6
liptic Curve Diffie-Hellman Key
[RST, ACK] Seq=1514 Ack=1575
Alive] 9443 → 53800 [ACK] Seq=
Alive] 9443 → 59826 [ACK] Seq=
Alive ACK] 53800 → 9443 [ACK]

Follow
TCP Stream
Ctrl+Alt+Shift+T
Copy
\Device\NPF_{59E3E6B1-C2AB-4C
:5d:38:d4:d5)
Protocol Preferences
Decode As...
Show Packet in New Window

Cela va filtrer uniquement les trames liées à cet échange :

tcp.stream eq 6					
No.	Time	Source	Destination	Protocol	Length Info
25	23.400259	172.26.48.1	172.26.49.192	TCP	66 54122 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
26	23.400930	172.26.49.192	172.26.48.1	TCP	66 22 → 54122 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=1024
27	23.401156	172.26.48.1	172.26.49.192	TCP	54 54122 → 22 [ACK] Seq=1 Ack=1 Win=65280 Len=0
28	23.456190	172.26.48.1	172.26.49.192	SSHv2	87 Client: Protocol (SSH-2.0-OpenSSH_for_Windows_9.5)
29	23.456692	172.26.49.192	172.26.48.1	TCP	54 22 → 54122 [ACK] Seq=1 Ack=34 Win=64512 Len=0
30	23.526666	172.26.49.192	172.26.48.1	SSHv2	96 Server: Protocol (SSH-2.0-OpenSSH_10.2p1 Ubuntu-2ubuntu3.2)
31	23.536298	172.26.49.192	172.26.48.1	SSHv2	1094 Server: Key Exchange Init
32	23.536426	172.26.48.1	172.26.49.192	TCP	54 54122 → 22 [ACK] Seq=34 Ack=1083 Win=64256 Len=0
33	23.551528	172.26.49.192	172.26.48.1	SSHv2	1486 Client: Key Exchange Init
34	23.551995	172.26.49.192	172.26.48.1	TCP	54 22 → 54122 [ACK] Seq=1083 Ack=1466 Win=67584 Len=0
35	23.554051	172.26.48.1	172.26.49.192	SSHv2	102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
36	23.554501	172.26.49.192	172.26.48.1	TCP	54 22 → 54122 [ACK] Seq=1083 Ack=1514 Win=67584 Len=0
37	23.558909	172.26.49.192	172.26.48.1	SSHv2	546 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=284)
38	23.570835	172.26.48.1	172.26.49.192	TCP	54 54122 → 22 [RST, ACK] Seq=1514 Ack=1575 Win=0 Len=0

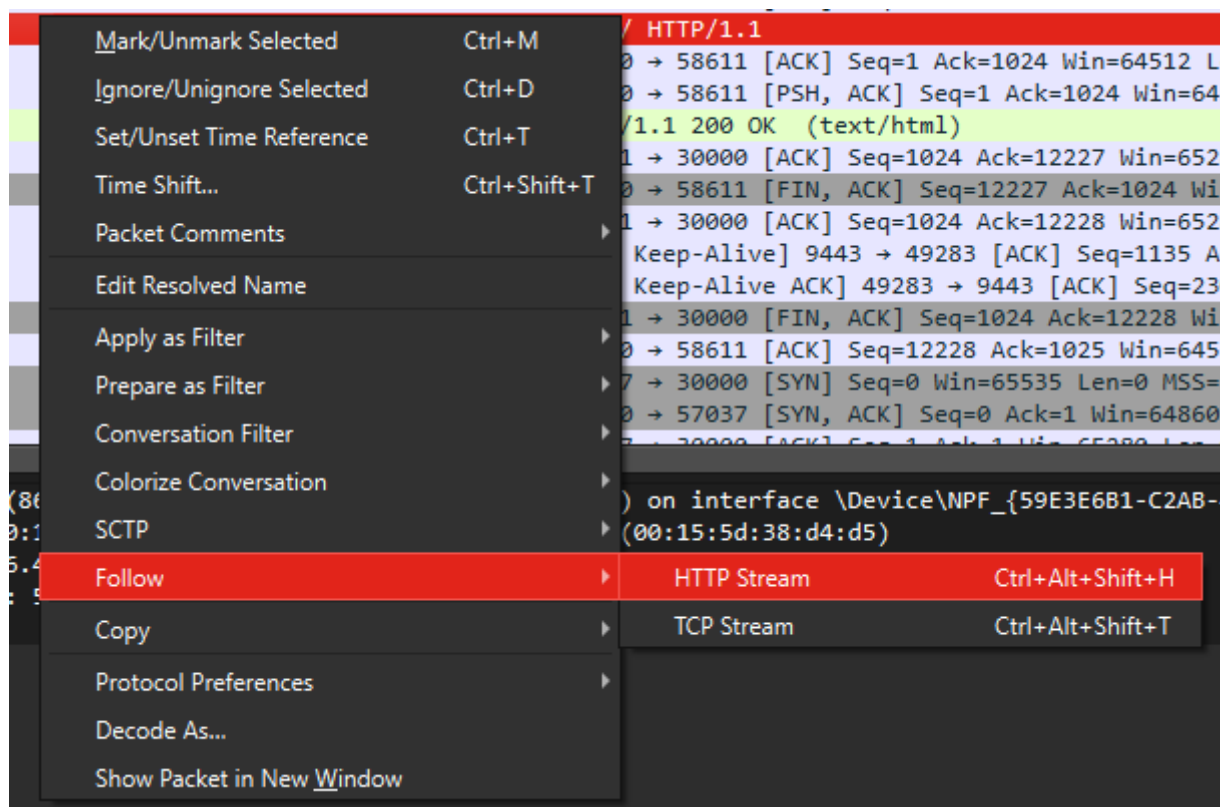
Et également afficher une nouvelle fenêtre dans laquelle sera affiché le détail des échanges.



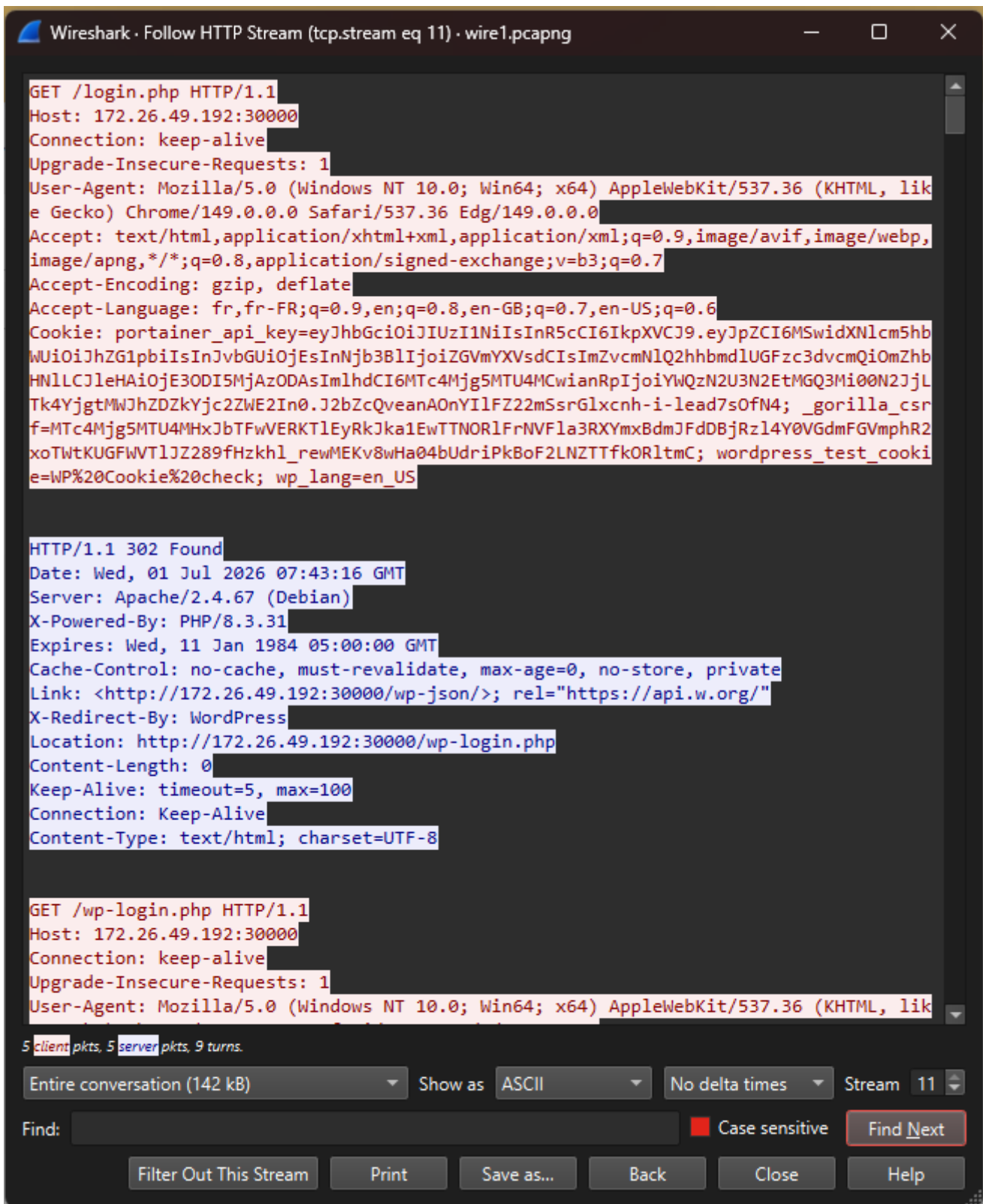
3.2 Suivre un stream HTTP(s)

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

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

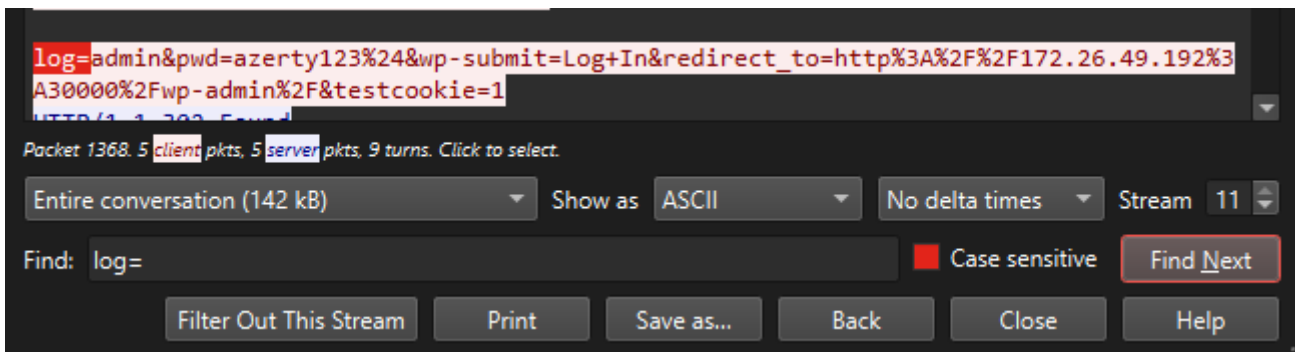


Cela permettra d'afficher la page récapitulative :



3.3 Trouver une information dans le stream

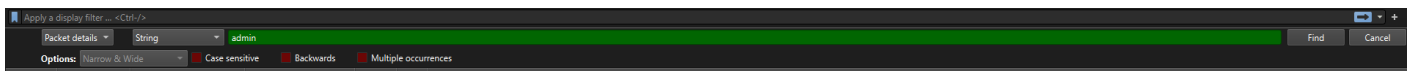
Il est ensuite possible grâce à la barre de recherche en bas de rechercher une information particulière dans le stream.



IV. Actions sur la liste

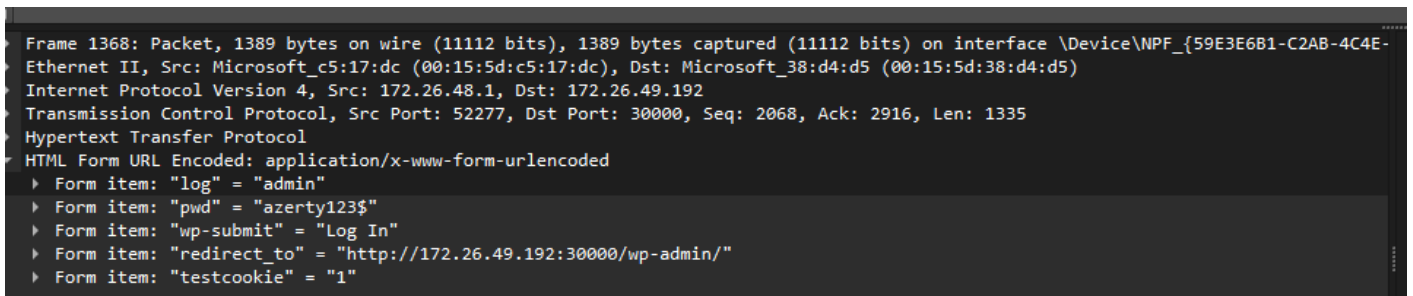
4.1 Rechercher une information

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



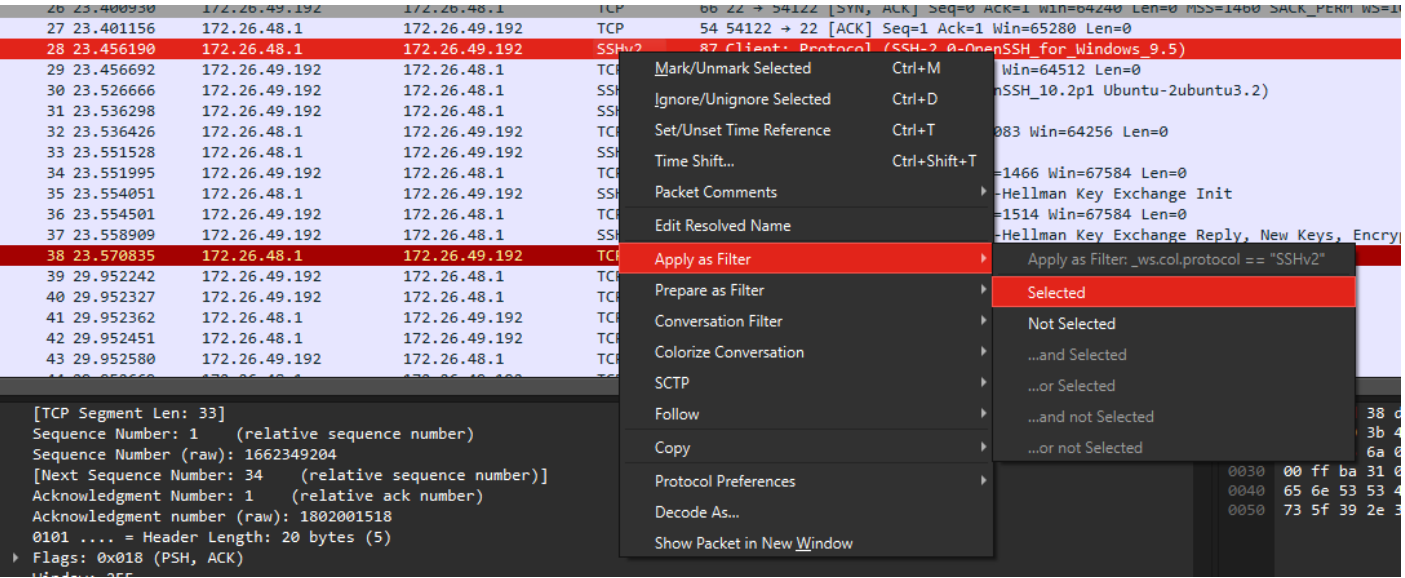
Cette barre permet de rechercher des données dans la liste ou dans le contenu des trames.

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.

