

Guide WireShark

Comment utiliser Wireshark pour capturer, filtrer et inspecter les paquets

Wireshark est un outil d'analyse de réseau anciennement appelé Ethereal, capture les paquets en temps réel et les affiche dans un format lisible par l'homme. Wireshark comprend des filtres, des codes de couleurs et d'autres fonctionnalités qui vous permettent d'examiner en profondeur le trafic réseau et d'inspecter des paquets individuels.

Ce didacticiel vous familiarisera avec les bases de la capture de paquets, de leur filtrage et de leur inspection. Vous pouvez utiliser **Wireshark pour inspecter le trafic réseau** d'un programme suspect, analyser le flux de trafic sur votre réseau ou résoudre des problèmes de réseau.

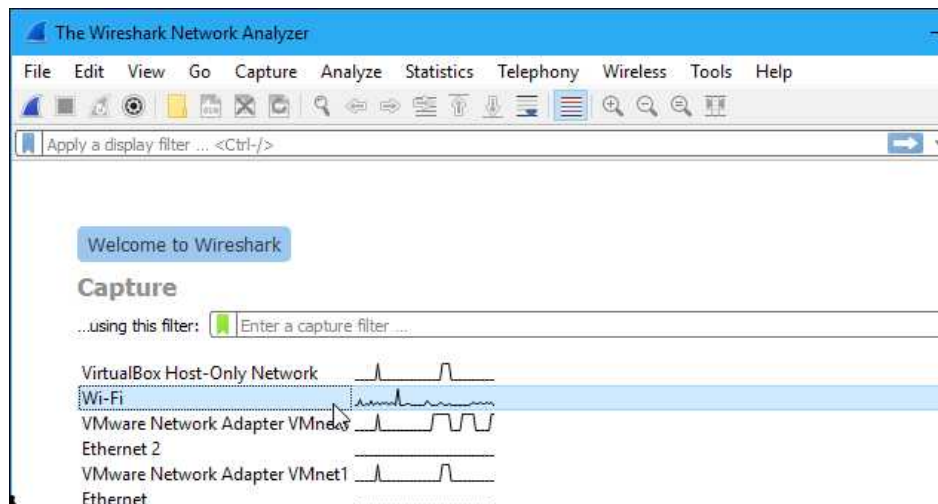
Obtenir Wireshark

Vous pouvez télécharger Wireshark pour Windows ou MacOS depuis son site [Web officiel](#). Si vous utilisez Linux ou un autre système UNIX, vous trouverez probablement Wireshark dans ses référentiels de paquets. Par exemple, si vous utilisez Ubuntu, vous trouverez Wireshark dans le Centre logiciel Ubuntu.

Juste un petit avertissement: de nombreuses organisations n'autorisent pas Wireshark et des outils similaires sur leurs réseaux. N'utilisez pas cet outil au travail sauf si vous en avez l'autorisation.

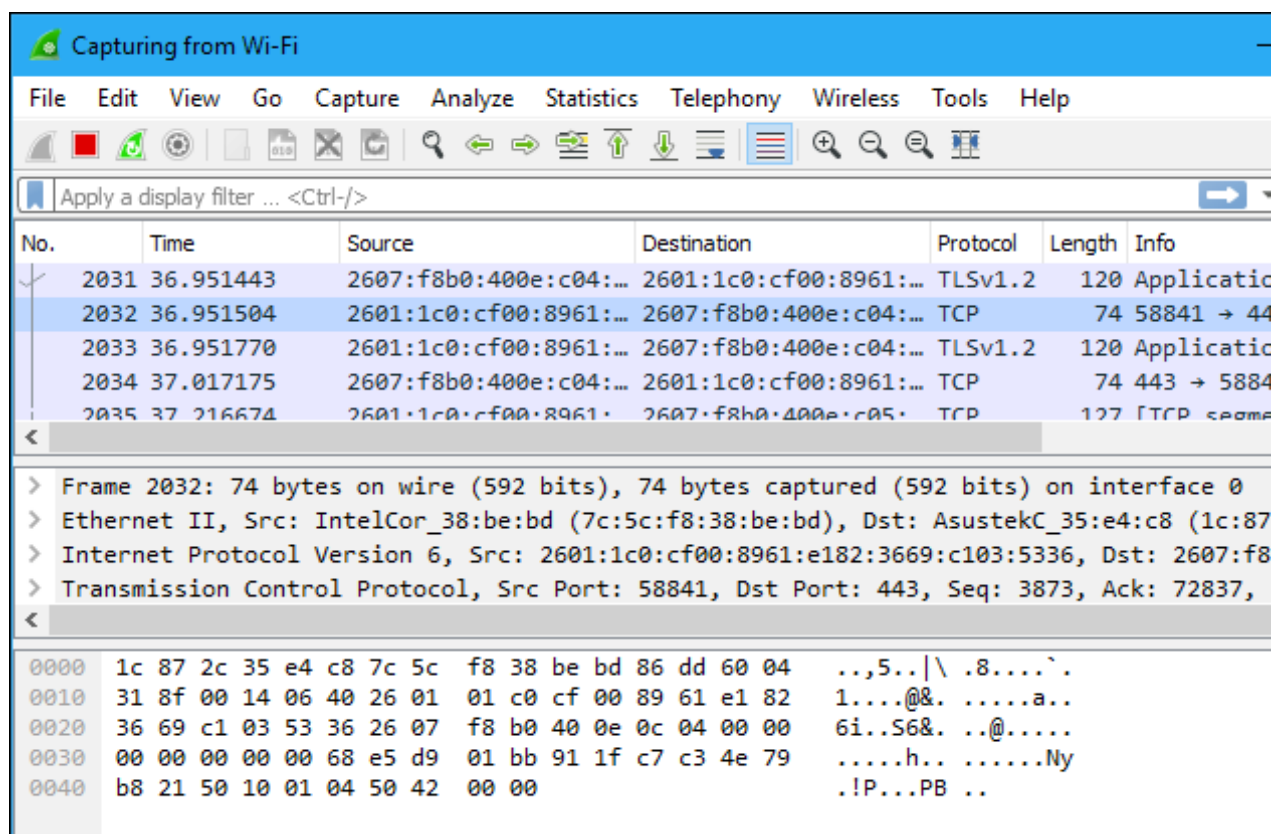
Capture de paquets

Après avoir téléchargé et installé Wireshark, vous pouvez le lancer et double-cliquer sur le nom d'une interface réseau sous Capture pour lancer la capture des paquets sur cette interface. Par exemple, si vous souhaitez capturer du trafic sur votre réseau sans fil, cliquez sur votre interface sans fil. Vous pouvez configurer des fonctionnalités avancées en cliquant sur Capture> Options, mais ce n'est pas nécessaire pour le moment.

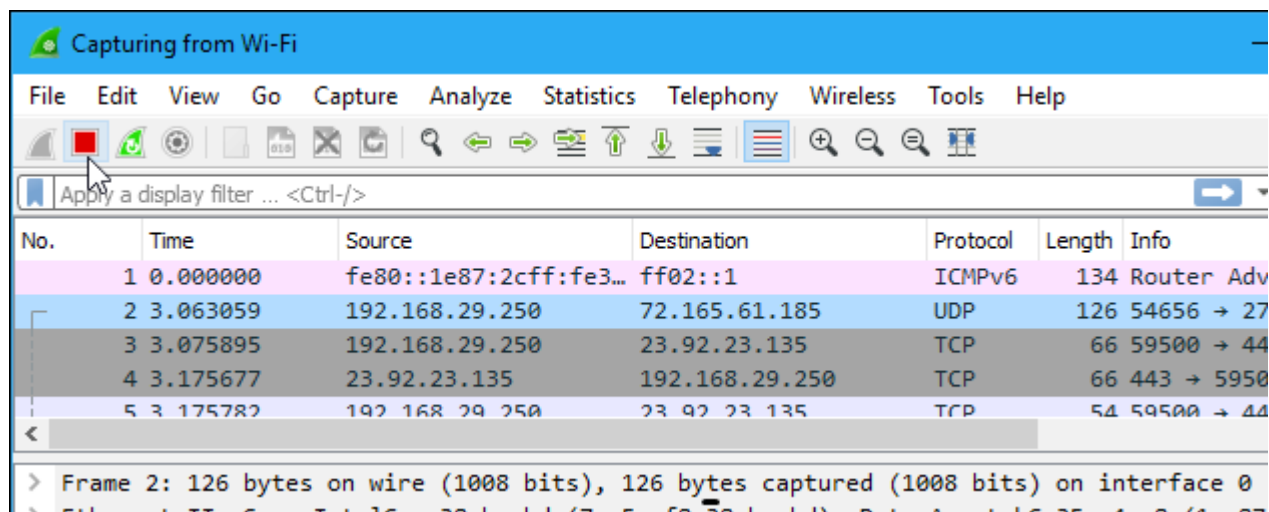


Dès que vous cliquez sur le nom de l'interface, vous verrez que les paquets commencent à apparaître en temps réel. Wireshark capture chaque paquet envoyé vers ou depuis votre système.

Si le mode promiscuous est activé, il est activé par défaut. Vous verrez également tous les autres paquets sur le réseau au lieu des seuls paquets adressés à votre carte réseau. Pour vérifier si le mode promiscuité est activé, cliquez sur Capture > Options et vérifiez que la case à cocher « Activer le mode promiscuous sur toutes les interfaces » est activée au bas de cette fenêtre.



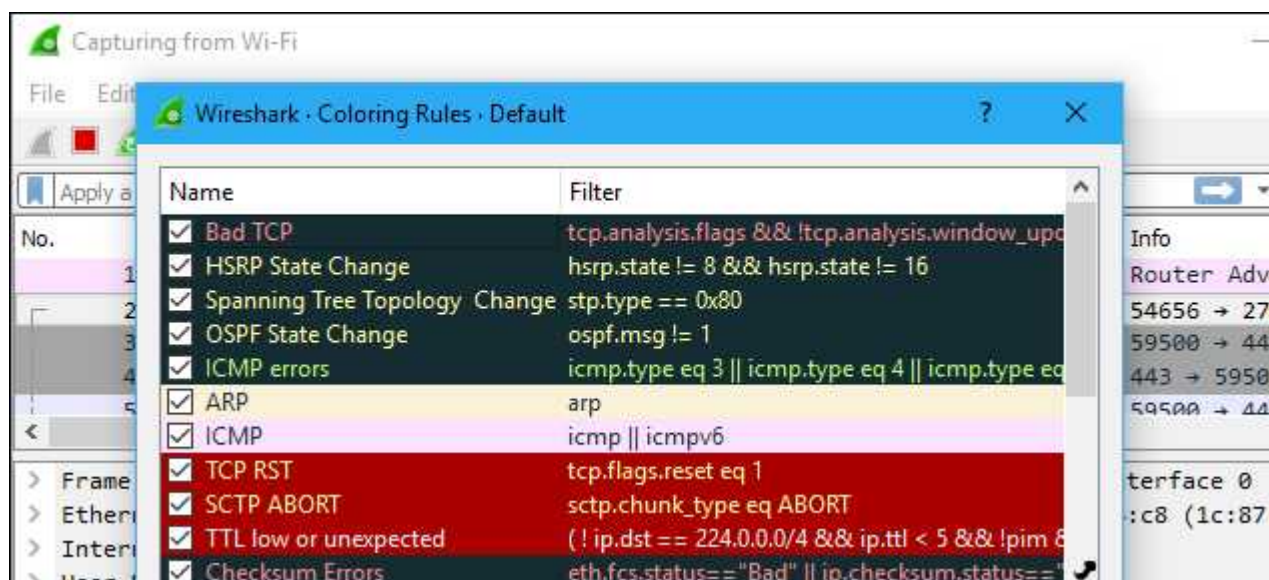
Cliquez sur le bouton rouge « Stop » situé dans le coin supérieur gauche de la fenêtre lorsque vous souhaitez arrêter de capturer le trafic.



Code de couleurs

Vous verrez probablement des paquets mis en évidence dans une variété de couleurs différentes. Wireshark utilise des couleurs pour vous aider à identifier les types de trafic en un coup d'œil. Par défaut, le violet clair est le trafic TCP, le bleu clair est le trafic UDP et le noir identifie les paquets avec des erreurs, par exemple, ils ont pu être livrés dans le désordre.

Pour afficher exactement la signification des codes de couleur, cliquez sur Afficher > Règles de coloration. Vous pouvez également personnaliser et modifier les règles de coloration à partir d'ici, si vous le souhaitez.

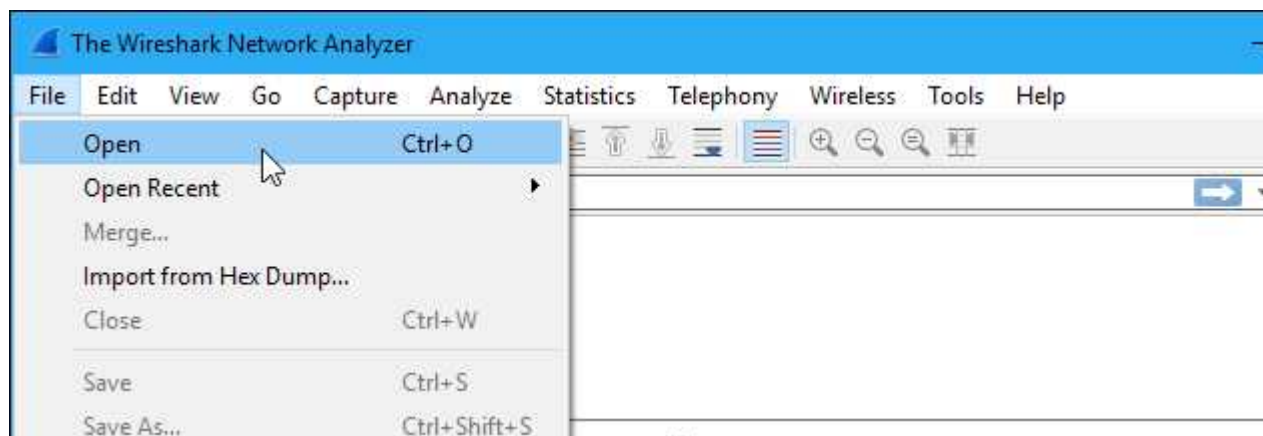


Échantillons de capture

S'il n'y a rien d'intéressant sur votre propre réseau à inspecter, le wiki de Wireshark vous couvre. Le wiki contient une page d'échantillons de fichiers de capture que vous pouvez charger et

inspecter. Cliquez sur Fichier> Ouvrir dans Wireshark et recherchez le fichier téléchargé pour en ouvrir un.

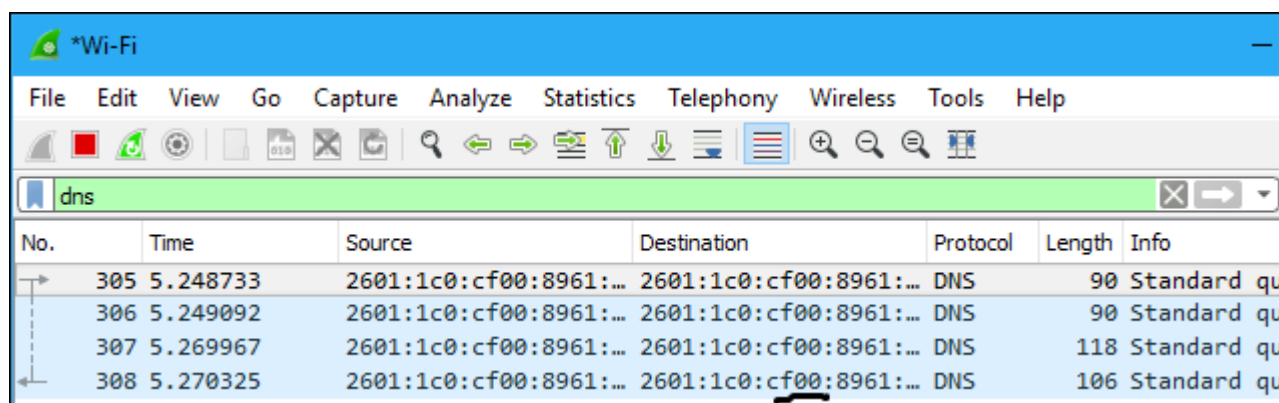
Vous pouvez également enregistrer vos propres captures dans Wireshark et les ouvrir ultérieurement. Cliquez sur Fichier> Enregistrer pour enregistrer vos paquets capturés.



Filtrage des paquets

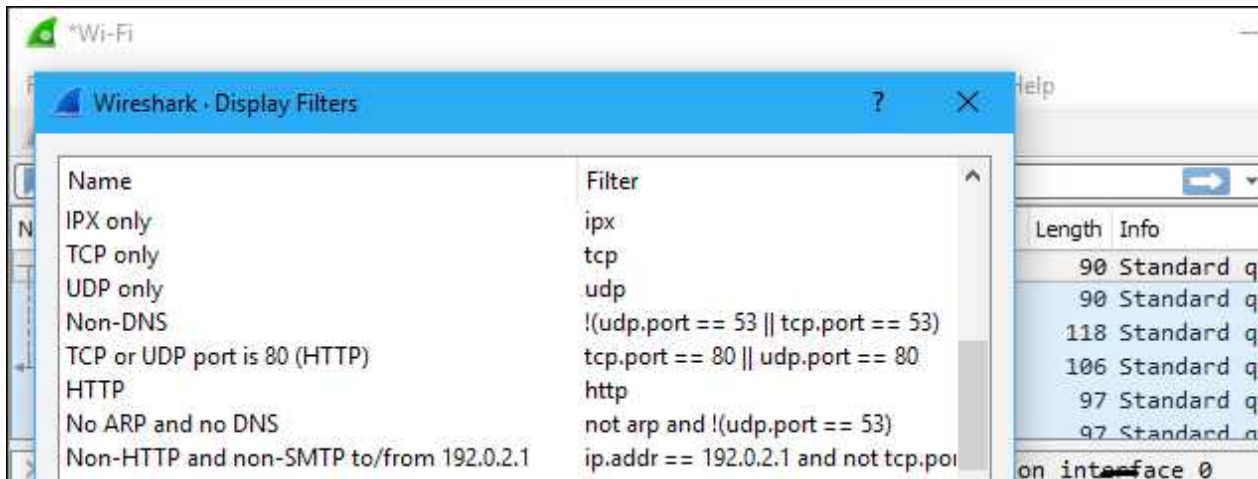
Si vous essayez d'inspecter un élément spécifique, tel que le trafic qu'un programme envoie en téléphonant à la maison, il est utile de fermer toutes les autres applications utilisant le réseau afin de réduire le trafic. Cependant, vous aurez probablement une grande quantité de paquets à parcourir. C'est là que les filtres de Wireshark entrent en jeu.

Le moyen le plus simple d'appliquer un filtre est de le taper dans la zone de filtre en haut de la fenêtre et de cliquer sur Appliquer (ou d'appuyer sur Entrée). Par exemple, tapez « dns » et vous ne verrez que les paquets DNS. Lorsque vous commencez à taper, Wireshark vous aidera à compléter automatiquement votre filtre.

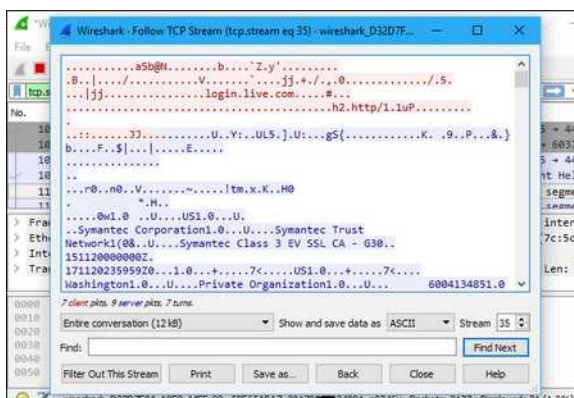


Vous pouvez également cliquer sur Analyser> Afficher les filtres pour choisir un filtre parmi les filtres par défaut inclus dans Wireshark. De là, vous pouvez ajouter vos propres filtres personnalisés et les enregistrer pour y accéder facilement à l'avenir.

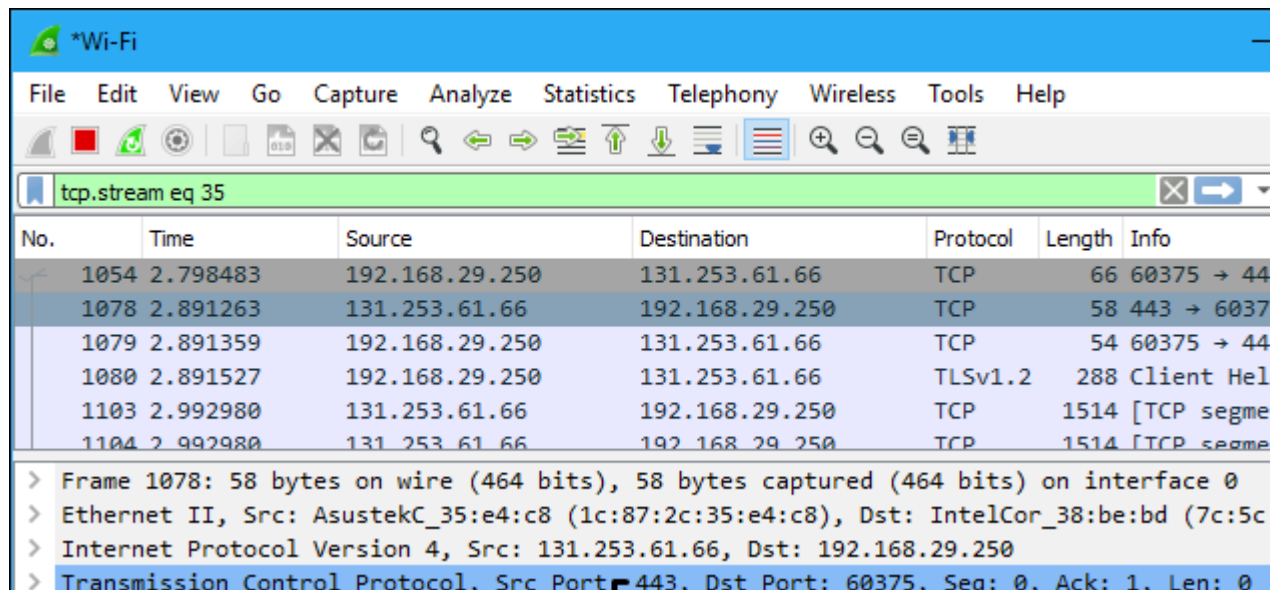
Pour plus d'informations sur le langage de filtrage d'affichage de Wireshark, lisez la page relative aux expressions de filtres d'affichage dans la documentation officielle de Wireshark.



Une autre chose intéressante à faire est de cliquer avec le bouton droit sur un paquet et de sélectionner Suivre> TCP Stream. Vous verrez la conversation TCP complète entre le client et le serveur. Vous pouvez également cliquer sur d'autres protocoles dans le menu Suivre pour voir les conversations complètes pour les autres protocoles, le cas échéant.



Fermez la fenêtre et vous trouverez qu'un filtre a été appliqué automatiquement. Wireshark vous montre les paquets qui composent la conversation.

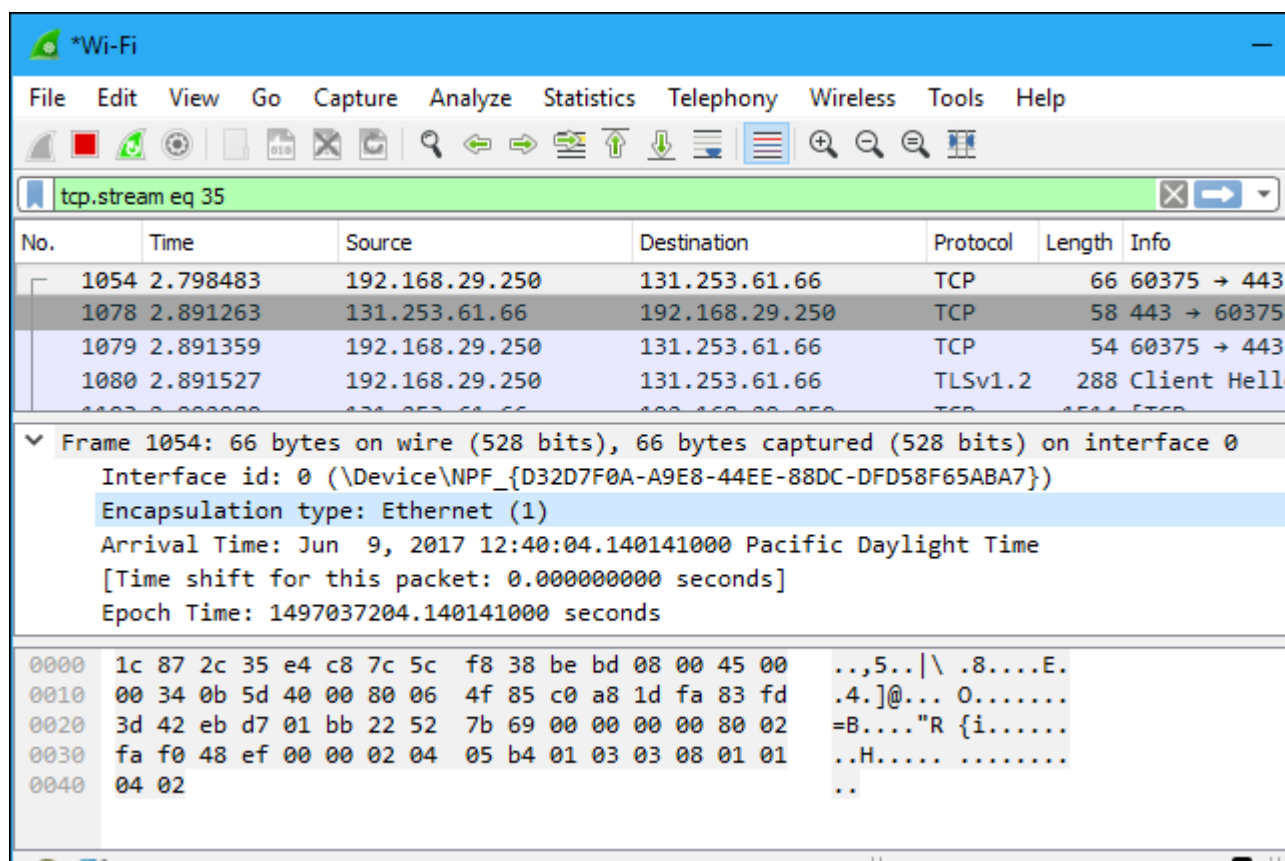


No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 44
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 6037
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 44
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hel
1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segme
1104	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segme

> Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
 > Ethernet II, Src: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor_38:be:bd (7c:5c
 > Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250
 > Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0

Inspection des paquets

Cliquez sur un paquet pour le sélectionner et vous pourrez creuser pour voir ses détails.

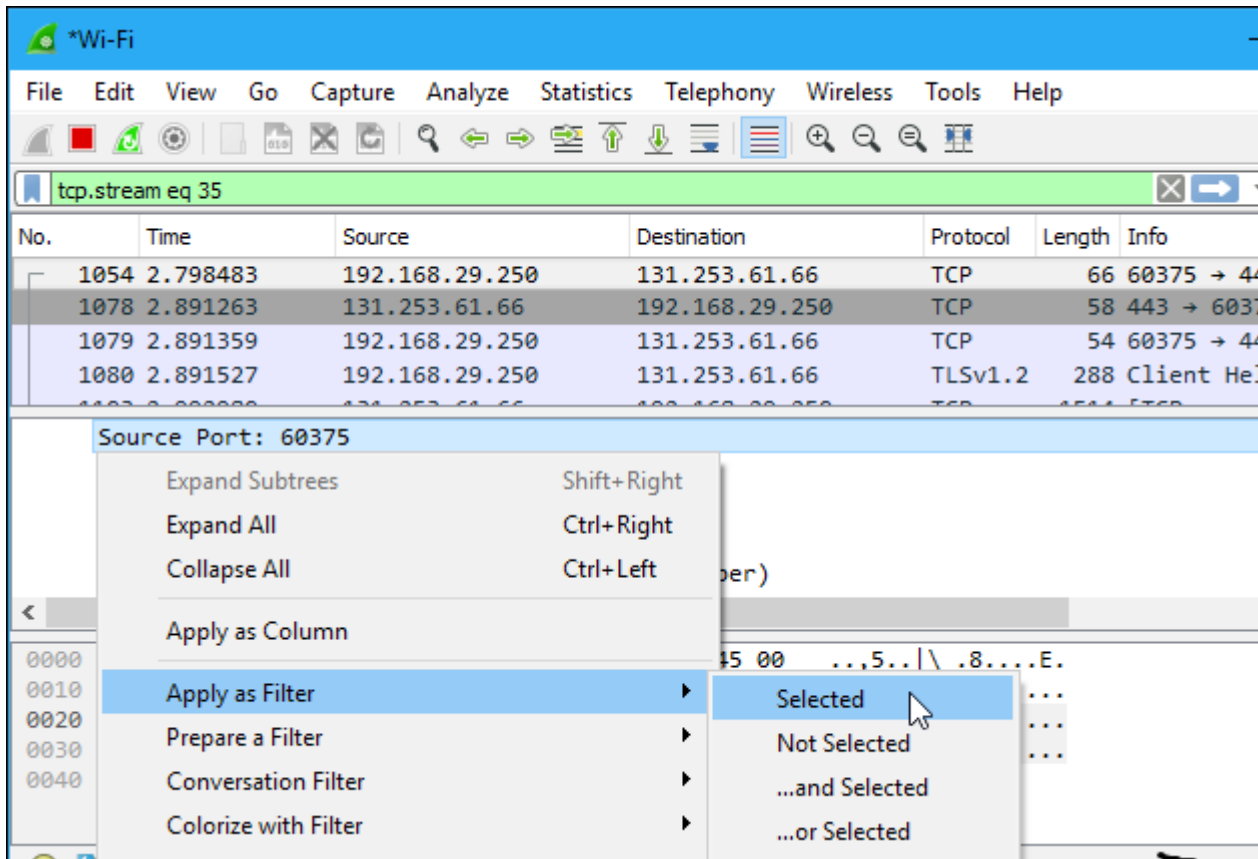


No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hell

Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
 Encapsulation type: Ethernet (1)
 Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1497037204.140141000 seconds

0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00	..,5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd	.4.]@... O.....
0020	3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02	=B...."R {i.....
0030	fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01	..H.....
0040	04 02	..

Vous pouvez également créer des filtres à partir d'ici – faites un clic droit sur l'un des détails et utilisez le sous-menu Appliquer en tant que filtre pour créer un filtre basé sur celui-ci.



Wireshark est un outil extrêmement puissant, et ce tutoriel ne fait que gratter la surface de ce que vous pouvez en faire. Les professionnels l'utilisent pour déboguer les implémentations de protocoles réseau, examiner les problèmes de sécurité et inspecter les composants internes du protocole réseau.