Utilisation de Wireshark sur un point d'accès sans fil Cisco Business pour l'analyse de paquets : Télécharger le fichier

Objectif

Cet article explique comment utiliser un point d'accès sans fil professionnel (WAP) Cisco et Wireshark pour effectuer, enregistrer et télécharger une capture de paquets.

Introduction

Les modifications de configuration, la surveillance et le dépannage sont souvent des problèmes auxquels un administrateur réseau doit faire face. Avoir un outil simple à utiliser est inestimable! L'objectif de cet article est d'être plus à l'aise avec les bases des captures de paquets ainsi que la façon de télécharger un fichier sur Wireshark. Si vous n'êtes pas familier avec ce processus, répondez à quelques questions que vous avez peut-être déjà posées.

Tout d'abord, Wireshark est un analyseur de paquets gratuit pour quiconque cherche à dépanner son réseau. Wireshark fournit de nombreuses options pour la capture ainsi que le tri du trafic par plusieurs paramètres différents. Rendez-vous sur Wireshark pour plus de détails sur cette option open source.

Qu’est-ce qu’une capture de paquets ?

Une capture de paquets, également appelée fichier PCAP, est un outil qui peut être utile pour le dépannage. Il peut enregistrer chaque paquet envoyé entre les périphériques de votre réseau, en temps réel. La capture de paquets vous permet d'entrer dans les détails du trafic réseau, qui peut inclure tout, depuis la découverte de périphériques, les conversations de protocole et l'échec de l'authentification. Vous pouvez voir le chemin d'un flux de trafic spécifique et chaque interaction entre des périphériques sur des réseaux sélectionnés. Ces paquets peuvent être enregistrés pour une analyse plus approfondie si nécessaire. C'est comme une radiographie du fonctionnement interne du réseau via le transfert de paquets.

Quels types de paquets peuvent être capturés ?

Le périphérique WAP peut capturer les types de paquets suivants :

·paquets 802.11 reçus et transmis sur les interfaces radio. Les paquets capturés sur les interfaces radio incluent l’en-tête 802.11.

·paquets 802.3 reçus et transmis sur l’interface Ethernet.

·paquets 802.3 reçus et transmis sur les interfaces logiques internes, telles que les points d'accès virtuels (VAP) et les interfaces WDS (Wireless Distribution System).

Comment effectuer une capture de paquets ?

Deux méthodes de capture de paquets sont disponibles :

1. *Remote Capture Method* - Les paquets capturés sont redirigés en temps réel vers un ordinateur externe exécutant Wireshark. Vous pouvez choisir *Stream to a Remote Host* pour sélectionner la méthode de capture distante. Si vous préférez la méthode de capture à distance, extrayez Utilisation de Wireshark sur un WAP pour l'analyse de paquets : Flânez directement vers Wireshark.
2. *Local Capture Method* - Les paquets capturés sont stockés dans un fichier sur le périphérique WAP. Le périphérique WAP peut transférer le fichier vers un serveur TFTP (Trivial File Transfer Protocol). Le fichier est formaté au format PCAP et peut être examiné à l'aide de Wireshark. Vous pouvez choisir *Enregistrer le fichier sur ce périphérique* pour sélectionner la méthode de capture locale.

Cet article vise à télécharger un fichier sur Wireshark contenant la dernière interface graphique utilisateur (GUI). Si vous préférez afficher un article qui utilise l'ancienne interface utilisateur graphique pour la méthode de capture locale, consultez Configurer la capture de paquets pour optimiser les performances sur un point d'accès sans fil.

Que dois-je faire avec une capture de paquets une fois que j'ai le fichier PCAP ?

La fonctionnalité de capture de paquets sans fil permet de capturer et de stocker les paquets reçus et transmis par le périphérique WAP. Les paquets capturés peuvent ensuite être analysés par un analyseur de protocole réseau pour le dépannage ou l'optimisation des performances. De nombreuses applications tierces d'analyse de paquets sont disponibles en ligne. Dans cet article, nous nous concentrons sur Wireshark.

Wireshark n'est pas la propriété ou la prise en charge de Cisco. Pour obtenir de l'aide, contactez Wireshark.

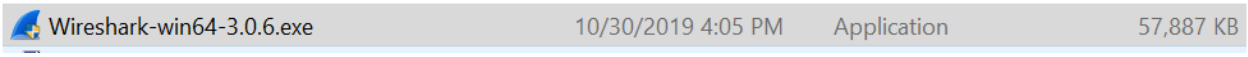
Périphériques | Version du logiciel

- WAP125 |1.0.2.0
- WAP150 |1.1.1.0
- WAP121 |1.0.6.8
- WAP361 |1.1.1.0
- WAP581 |1.0.2.0
- WAP571 |1.1.0.4
- WAP571E |1.1.0.4

Télécharger Wireshark

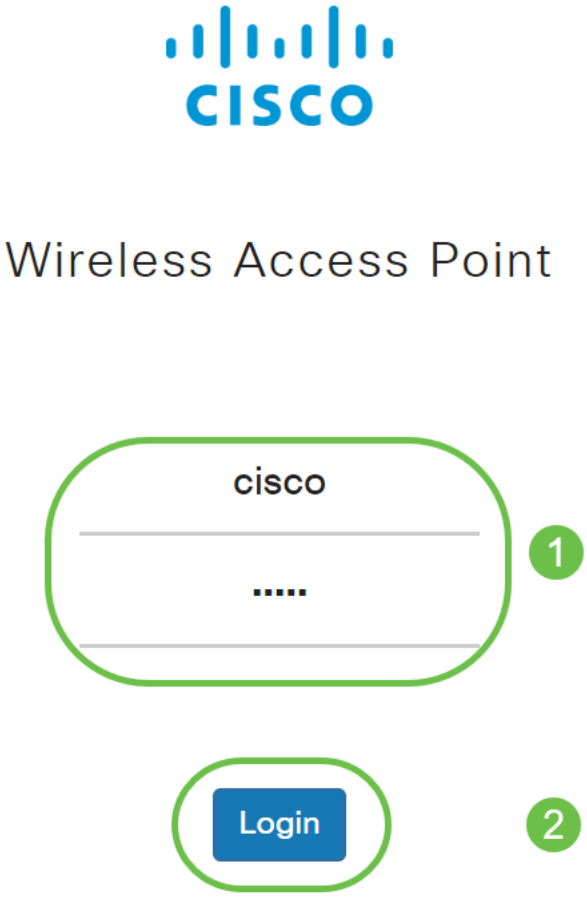
Étape 1. Accédez au site Wireshark. Cliquez sur **Download**. Sélectionnez la version appropriée à télécharger. Vous verrez la progression du téléchargement en bas à gauche de l'écran.

Étape 2. Accédez à *Téléchargements* sur votre ordinateur et sélectionnez le fichier Wireshark pour installer son application.



Se connecter au WAP

Dans votre navigateur Web, saisissez l'adresse IP du WAP. Entrez dans vos informations d'identification. Si vous accédez à ce périphérique pour la première fois ou si vous avez effectué une réinitialisation en usine, le nom d'utilisateur et le mot de passe par défaut sont *cisco*. Si vous avez besoin d'instructions pour vous connecter, vous pouvez suivre les étapes de l'article Accéder à l'utilitaire Web du point d'accès sans fil (WAP).



Enregistrer une capture de paquets sur un PC et télécharger sur Wireshark

Étape 1. Accédez à **Dépannage > Capture de paquets**.

Assurez-vous que **Save File on this Device** est sélectionné pour la *méthode Packet Capture*.

Configurez ces paramètres :

·*Interface* - Entrez un type d'interface de capture pour la capture de paquets :

·*Ethernet* - trafic 802.3 sur le port Ethernet.

·*Radio 1 (5 GHz) / Radio 2 (2,4 GHz)* - Trafic 802.11 sur l'interface radio.

·*Duration* - Saisissez la durée en secondes de la capture. Elle est située entre 10 et 3600. Il est défini par défaut à 60.

·*Taille maximale du fichier* - Entrez la taille maximale autorisée pour le fichier de capture en kilo-octets (Ko). Elle est située entre 64 et 4096. Il est défini par défaut à 1024.

Il existe deux modes de capture de paquets.

·*All Wireless Traffic* - Capture tous les paquets sans fil.

·*Trafic vers/depuis ce point d'accès* - Capture les paquets envoyés par le point d'accès ou reçus par le point d'accès.

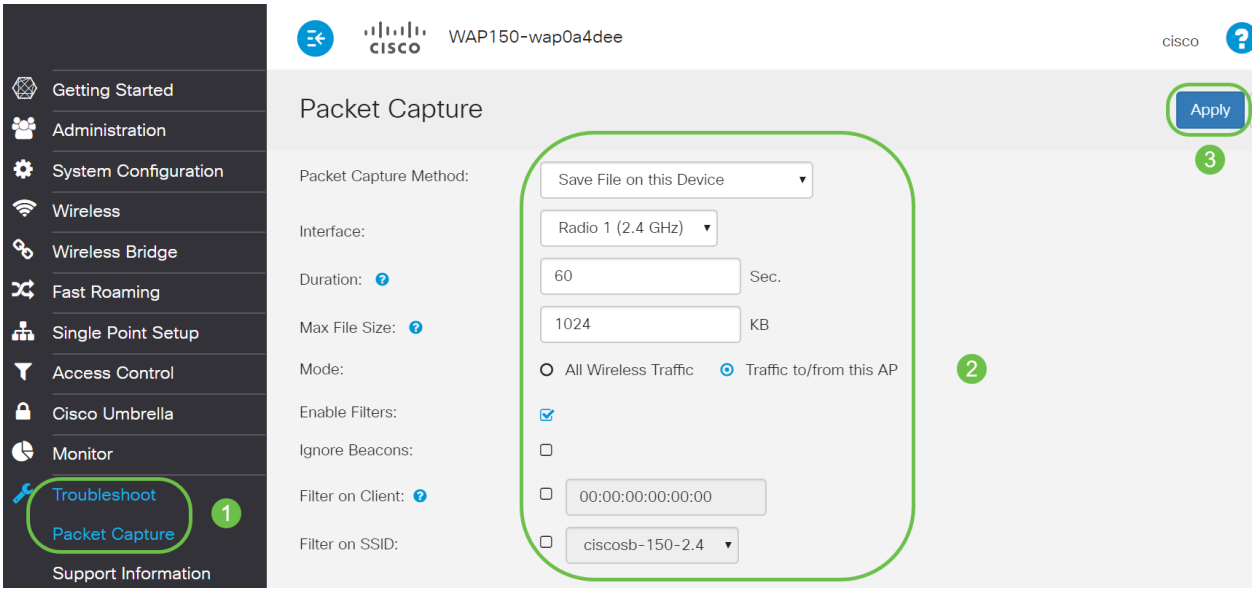
Cliquez sur **Activer les filtres**. Trois cases à cocher sont disponibles : *Ignorer les balises, Filtrer sur le client* et *Filtrer sur SSID*.

·*Ignorer les balises* : activez ou désactivez la capture des balises 802.11 détectées ou transmises par la radio. Les trames de balise sont des trames de diffusion qui transportent des informations relatives à un réseau. L'objectif d'une balise est d'annoncer le réseau sans fil existant. Si vous ne recherchez pas ce type de trafic, vous pouvez sélectionner Ignorer les balises.

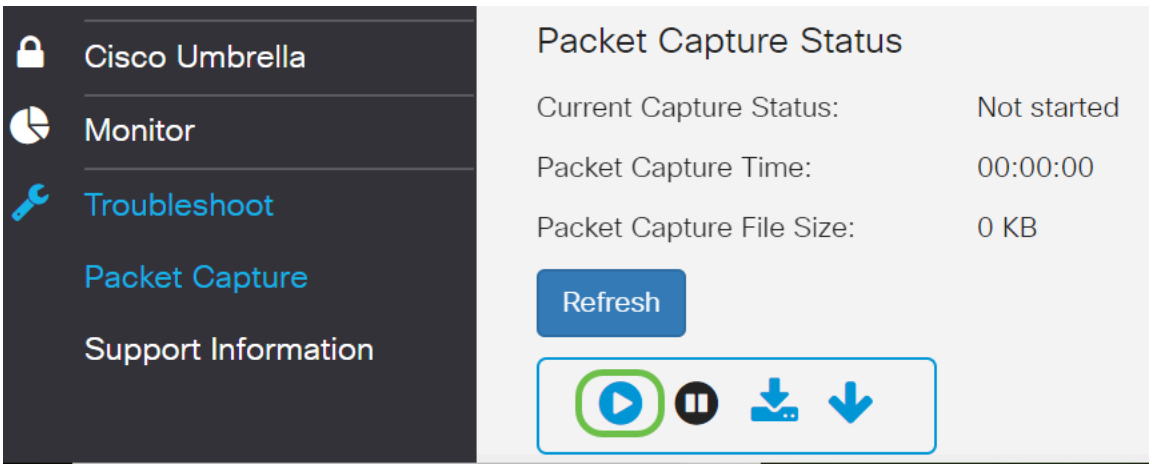
·*Filter on Client* - Spécifie l'adresse MAC pour le filtre client WLAN. Notez que le filtre Client est actif uniquement lorsqu'une capture est effectuée sur une interface 802.11.

·*Filter on SSID* - Sélectionnez un nom SSID pour la capture de paquets.

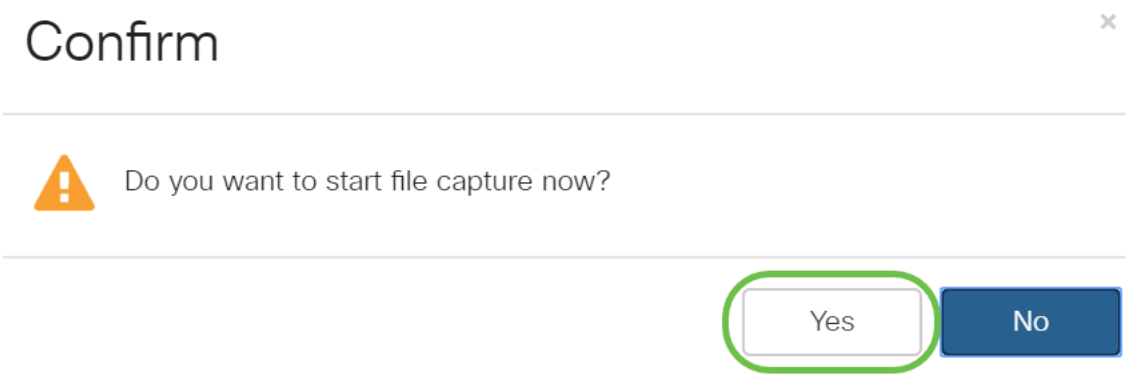
Cliquez sur **Apply** pour enregistrer la configuration de démarrage.



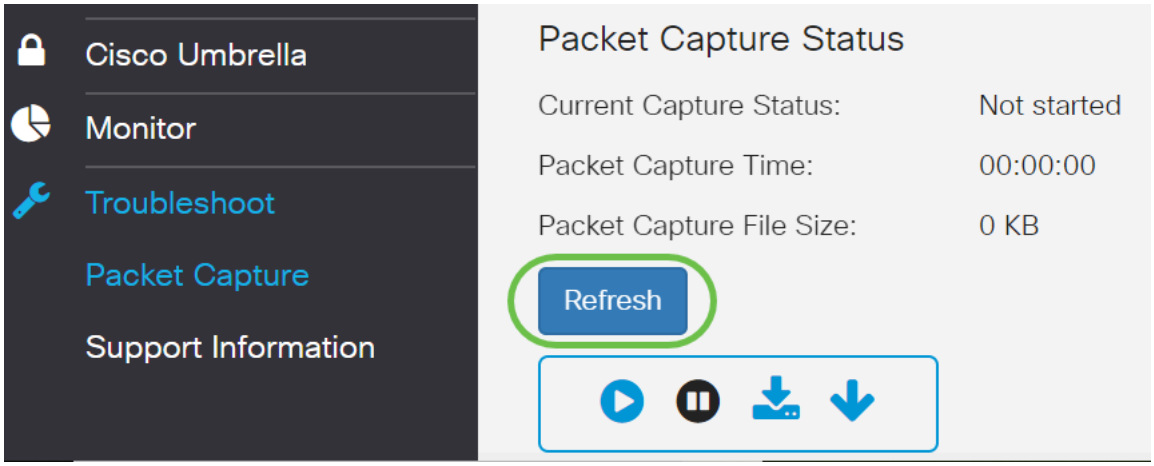
Étape 2. Cliquez sur l'icône **Start Capture**.



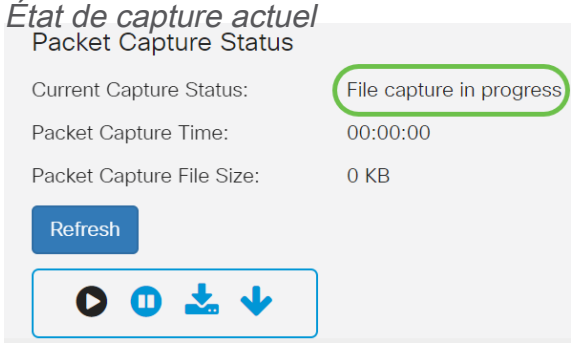
Étape 3. Une fenêtre contextuelle *Confirmer* s'ouvre pour obtenir la confirmation de téléchargement du fichier, cliquez sur **Oui** pour démarrer le téléchargement du fichier.



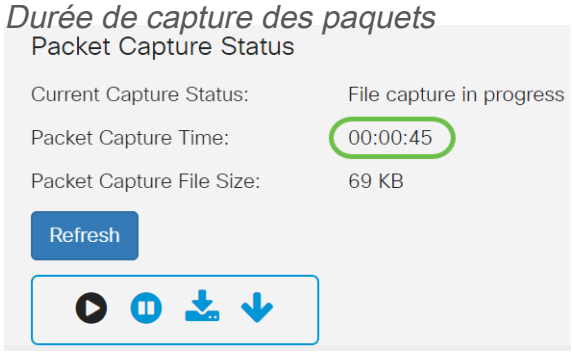
Étape 4. Cliquez sur **Refresh** pour obtenir l'*état de capture de paquets* qui contient les données suivantes :



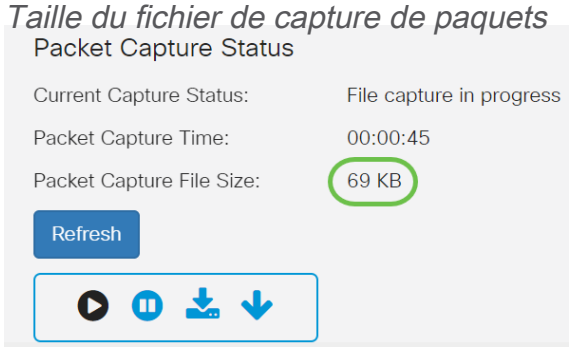
1. *État de capture actuel*



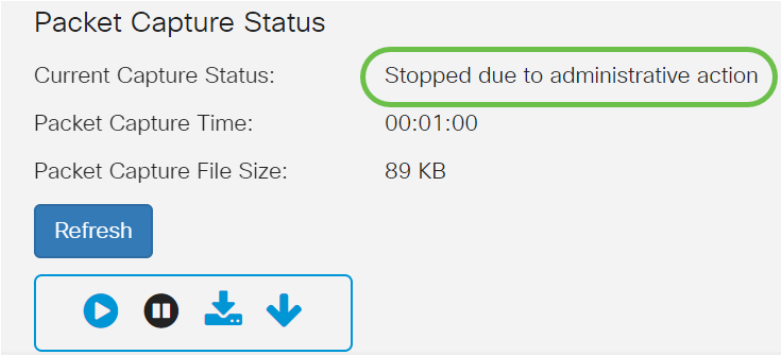
2. *Durée de capture des paquets*



3. *Taille du fichier de capture de paquets*

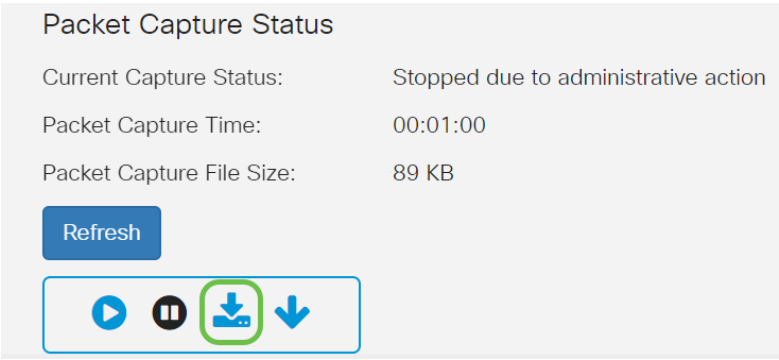


4. En mode *Packet File Capture*, le périphérique WAP stocke les paquets capturés dans le système de fichiers de mémoire vive (RAM). Lors de l'activation, la capture de paquets se poursuit jusqu'à ce qu'un de ces événements se produise :
·Le temps de capture atteint la durée configurée.
·le fichier de capture atteint sa taille maximale.
·L'administrateur arrête la capture.

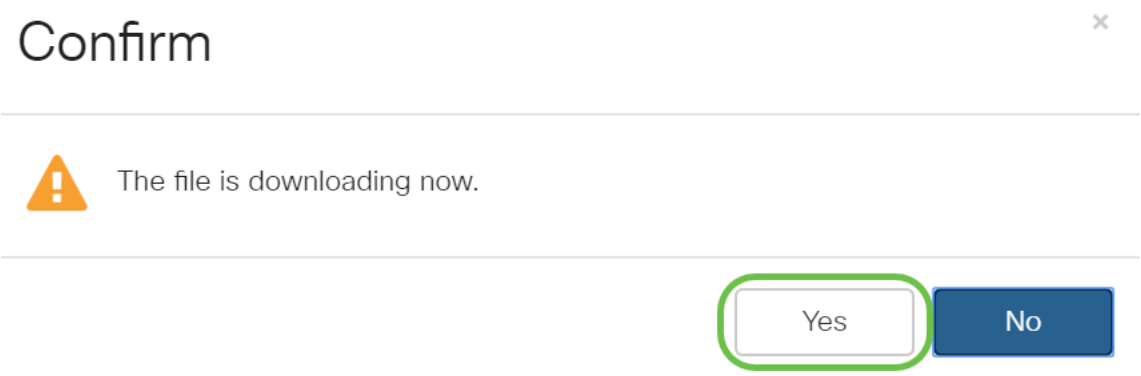


Le fichier de capture de paquets sera stocké dans l'AP jusqu'au redémarrage de l'AP.

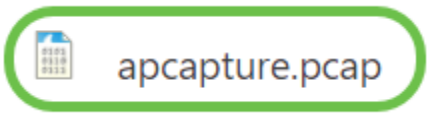
Étape 5. Cliquez sur l'icône **Télécharger sur ce périphérique** pour télécharger le fichier récemment capturé.



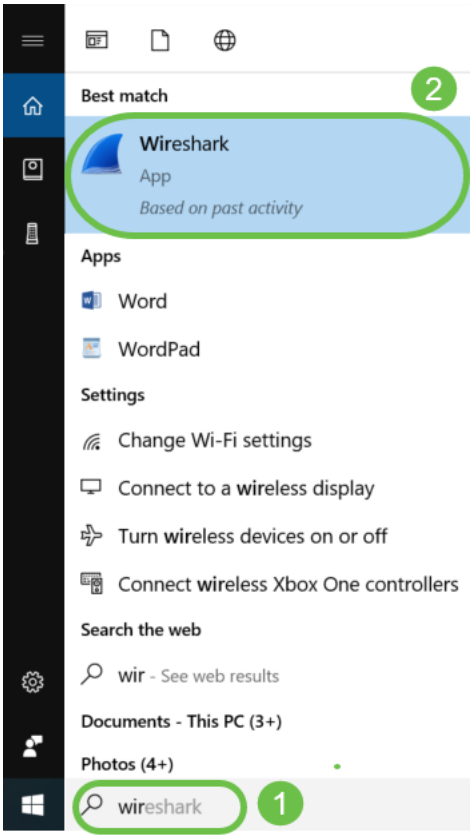
Étape 6. Une fenêtre contextuelle *Confirmer* s'ouvre pour confirmer le téléchargement du fichier, cliquez sur **Oui**.



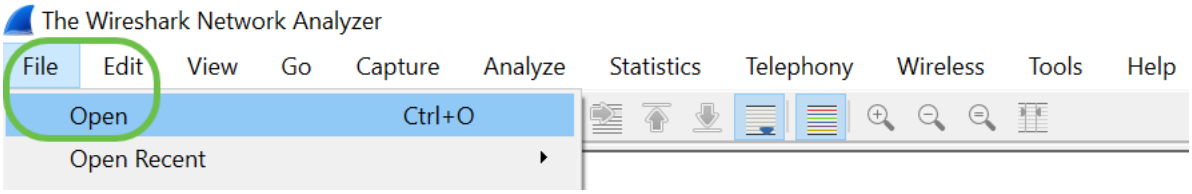
Étape 7. Le fichier de capture de paquets sera téléchargé sur votre ordinateur. Dans cet exemple, *apcapture.pcap* est le nom du fichier.



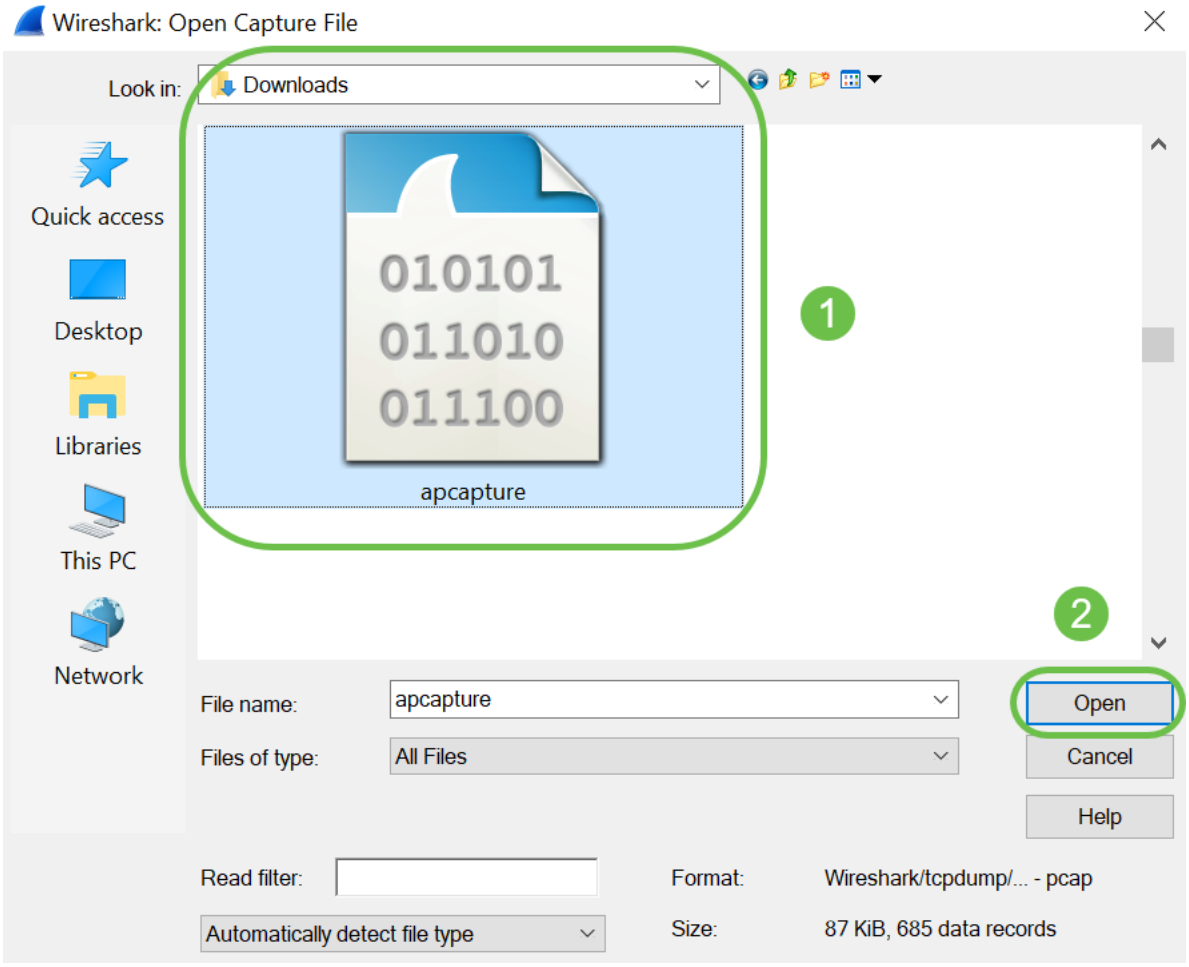
Étape 8. Étant donné que Wireshark a déjà été téléchargé, vous pouvez y accéder en tapant *Wireshark* dans la barre de recherche de Microsoft Windows et en sélectionnant l'application lorsqu'il s'agit d'une option.



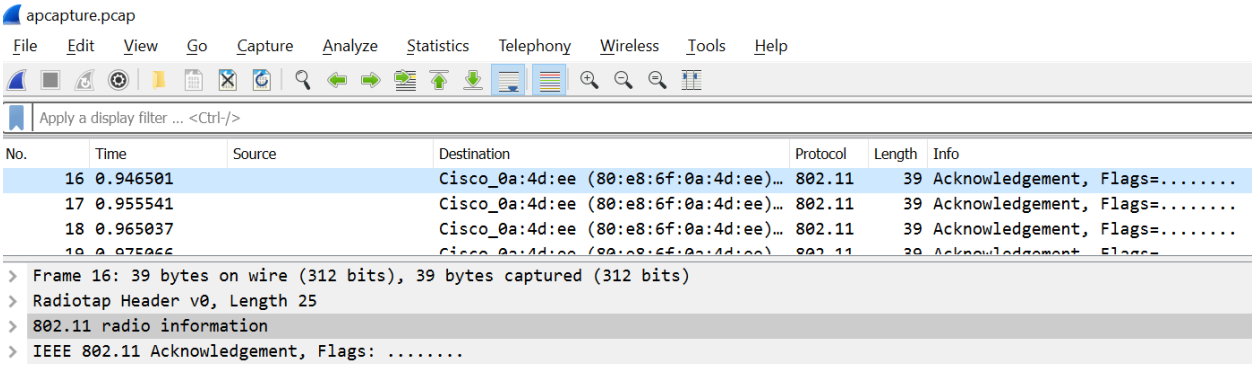
Étape 9. Accédez à **Fichier > Ouvrir**.



Étape 10. Dans la nouvelle fenêtre contextuelle, recherchez le fichier, dans ce cas, *apcapture.pcap*. Cliquez sur **Open**.



Étape 11. Le fichier s'ouvrira sur l'application *Wireshark* et vous pourrez voir les détails des paquets.



Conclusion

Votre paquet est capturé et téléchargé sur Wireshark. Vous pouvez maintenant l'analyser. Vous ne savez pas où aller ? Il y a beaucoup de vidéos et d'articles disponibles en ligne à explorer. Ce que vous recherchez dépend des besoins de votre situation. Vous avez ceci !