# Verwenden von Wireshark auf einem Cisco Business WAP für die Paketanalyse: Datei hochladen

## Ziel

In diesem Artikel wird erläutert, wie Sie mit einem Cisco Business Wireless Access Point (WAP) und Wireshark eine Paketerfassung durchführen, speichern und hochladen.

## Einführung

Konfigurationsänderungen, Überwachung und Fehlerbehebung sind häufig ein Thema, mit dem sich Netzwerkadministratoren auseinander setzen müssen. Ein einfaches Tool zu verwenden ist unschätzbar! Ziel dieses Artikels ist es, sich mit den Grundlagen der Paketerfassung vertraut zu machen und eine Datei nach Wireshark hochzuladen. Wenn Sie mit diesem Prozess nicht vertraut sind, lassen Sie uns einige Fragen beantworten, die Sie möglicherweise bereits gestellt haben.

Zunächst einmal ist Wireshark ein kostenloser Paket-Analyzer für alle, die eine Fehlerbehebung im Netzwerk durchführen möchten. Wireshark bietet viele Optionen für die Erfassung und Sortierung des Datenverkehrs durch mehrere verschiedene Parameter. Weitere Informationen zu dieser Open-Source-Option finden Sie unter Wireshark.

### Was ist eine Paketerfassung?

Eine Paketerfassung, auch als PCAP-Datei bezeichnet, ist ein Tool, das bei der Fehlerbehebung hilfreich sein kann. Sie kann jedes Paket, das zwischen Geräten in Ihrem Netzwerk gesendet wird, in Echtzeit aufzeichnen. Durch das Erfassen von Paketen können Sie die Details des Netzwerkverkehrs eingehend untersuchen. Dies kann alles von der Geräteerkennung, der Protokollierung und der fehlgeschlagenen Authentifizierung umfassen. Sie können den Pfad eines bestimmten Datenverkehrsflusses und jede Interaktion zwischen Geräten in ausgewählten Netzwerken sehen. Diese Pakete können bei Bedarf zur weiteren Analyse gespeichert werden. Es ist wie eine Röntgenaufnahme der internen Abläufe des Netzwerks durch die Übertragung von Paketen.

### Welche Arten von Paketen können erfasst werden?

Das WAP-Gerät kann die folgenden Pakettypen erfassen:

·802.11-Pakete, die über die Funkschnittstellen empfangen und übertragen werden. Zu den auf den Funkschnittstellen erfassten Paketen gehört der 802.11-Header.

·802.3-Pakete, die über die Ethernet-Schnittstelle empfangen und übertragen werden.

·802.3-Pakete, die über die internen logischen Schnittstellen empfangen und übertragen werden, z. B. Virtual Access Points (VAPs) und Wireless Distribution System (WDS)-Schnittstellen.

## Wie kann eine Paketerfassung durchgeführt werden?

Es stehen zwei Methoden zur Paketerfassung zur Verfügung:

1. *Remote Capture Method* - Erfasste Pakete werden in Echtzeit an einen externen Computer umgeleitet, auf dem Wireshark ausgeführt wird. Sie können *Stream zu einem Remote-Host* auswählen, um die Remote-Erfassungsmethode auszuwählen. Wenn Sie die Remote-Erfassungsmethode bevorzugen, überprüfen Sie **mithilfe von Wireshark auf einem WAP für die Paketanalyse: Direkter Stream zu Wireshark**.
2. *Local Capture Method* - Erfasste Pakete werden in einer Datei auf dem WAP-Gerät gespeichert. Das WAP-Gerät kann die Datei auf einen TFTP-Server (Trivial File Transfer Protocol) übertragen. Die Datei ist im PCAP-Format formatiert und kann mit Wireshark überprüft werden. Sie können *Datei auf diesem Gerät speichern* auswählen, um die lokale Erfassungsmethode auszuwählen.

Der Schwerpunkt dieses Artikels besteht darin, eine Datei mit der neuesten grafischen Benutzeroberfläche (GUI) in Wireshark hochzuladen. Wenn Sie einen Artikel anzeigen möchten, der die ältere GUI für die lokale Erfassungsmethode verwendet, sehen Sie sich Configure Packet Capture to Optimize Performance on a Wireless Access Point an.

## Was mache ich mit einer Paketerfassung, sobald ich die PCAP-Datei habe?

Die Funktion zur Wireless-Paketerfassung ermöglicht das Erfassen und Speichern der vom WAP-Gerät empfangenen und übertragenen Pakete. Die erfassten Pakete können dann von einem Netzwerkprotokollanalysator zur Fehlerbehebung oder Leistungsoptimierung analysiert werden. Online sind zahlreiche Paketanalyseanwendungen von Drittanbietern verfügbar. In diesem Artikel konzentrieren wir uns auf Wireshark.

Wireshark ist nicht Eigentum von Cisco oder wird von Cisco nicht unterstützt. Wenden Sie sich für Unterstützung an Wireshark.

## Geräte | Softwareversion

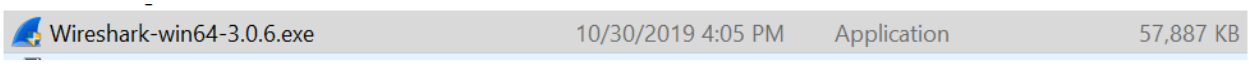
- WAP125 | 1,0/2,0
- WAP150 | 1,1/1,0
- WAP121 | 1,0/6,8
- WAP361 | 1,1/1,0
- WAP581 | 1,0/2,0

- WAP571 | 1,1/0,4
- WAP571E | 1,1/0,4

## Wireshark herunterladen

Schritt 1: Öffnen Sie die Wireshark-Website. Klicken Sie auf **Download (Herunterladen).** Wählen Sie die entsprechende Version zum Herunterladen aus. Sie sehen den Fortschritt des Downloads unten links im Bildschirm.

Schritt 2: Gehen Sie zu *Downloads* auf Ihrem Computer, und wählen Sie die Wireshark-Datei aus, um die Anwendung zu installieren.




## Melden Sie sich beim WAP an.

Geben Sie in Ihrem Webbrowser die IP-Adresse des WAP ein. Geben Sie Ihre Anmeldeinformationen ein. Wenn Sie zum ersten Mal auf dieses Gerät zugreifen oder das Gerät auf die Werkseinstellungen zurückgesetzt haben, lautet der Standardbenutzername und das Standardkennwort *cisco*. Wenn Sie Anweisungen zur Anmeldung benötigen, können Sie die Schritte im Artikel Access the Web-based Utility (Zugriff auf das webbasierte Dienstprogramm) des Wireless Access Point (WAP) befolgen.

# Speichern einer Paketerfassung auf einem PC und Hochladen auf Wireshark

Schritt 1: Navigieren Sie zu **Problembehandlung > Paketerfassung**.

Stellen Sie sicher, dass **Save File (Datei auf diesem Gerät speichern)** für die *Paketerfassungsmethode* ausgewählt ist.

Konfigurieren Sie diese Parameter:

·*Interface* - Geben Sie einen Schnittstellentyp für die Erfassung von Paketen ein:

·*Ethernet* - 802.3-Datenverkehr am Ethernet-Port

·*Radio 1 (5 GHz)/Radio 2 (2,4 GHz)* - 802.11-Datenverkehr an der Funkschnittstelle.

·*Duration (Dauer*): Geben Sie die Zeitdauer für die Erfassung in Sekunden ein. Der Bereich liegt zwischen 10 und 3600. Der Standardwert ist 60.

·*maximale Dateigröße*: Geben Sie die maximal zulässige Größe für die Erfassungsdatei in Kilobyte (KB) ein. Der Bereich liegt zwischen 64 und 4096. Der Standardwert ist 1024.

Es gibt zwei Modi für die Paketerfassung.

·*Gesamter Wireless-Datenverkehr* - Erfasst alle Wireless-Pakete.

·*Datenverkehr von/zu diesem AP* - Erfasst die Pakete, die vom WAP gesendet oder vom WAP empfangen wurden.

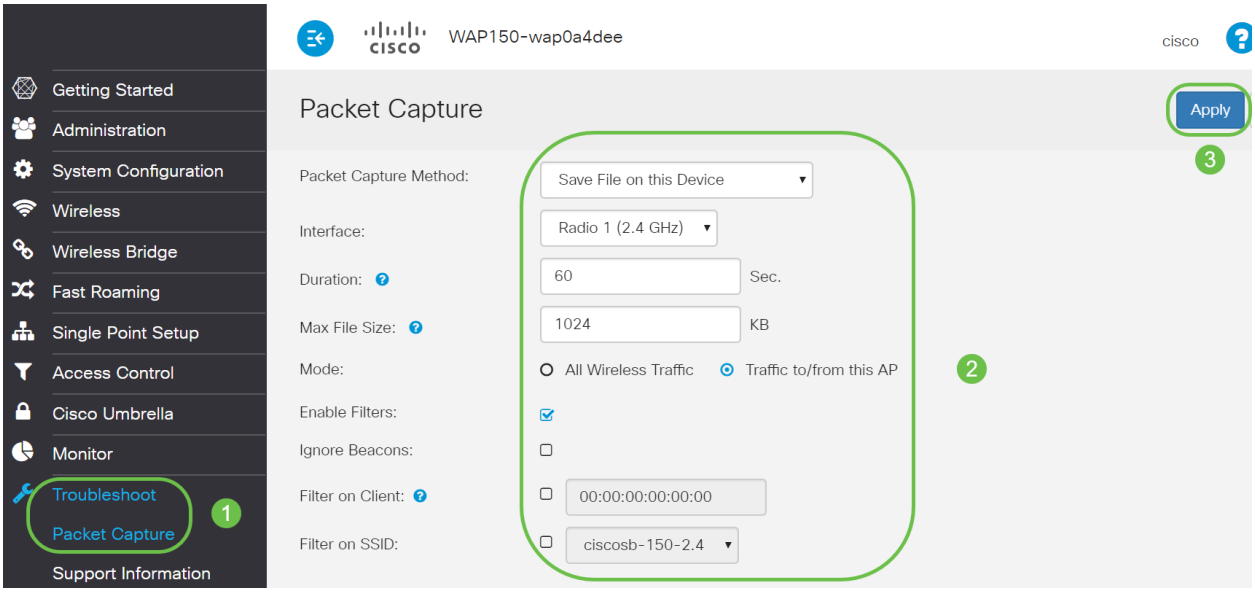
Klicken Sie auf **Filter aktivieren**. Es sind drei Kontrollkästchen verfügbar: *Beacons ignorieren, auf Client filtern* und *SSID filtern*.

·*Ignore Beacons*: Aktivieren oder Deaktivieren der Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder übertragen werden. Beacon-Frames sind Broadcast-Frames, die Informationen über ein Netzwerk übertragen. Der Zweck eines Beacons besteht darin, das vorhandene Wireless-Netzwerk anzukündigen. Wenn Sie diesen Datenverkehr nicht suchen, können Sie Beacons ignorieren auswählen.

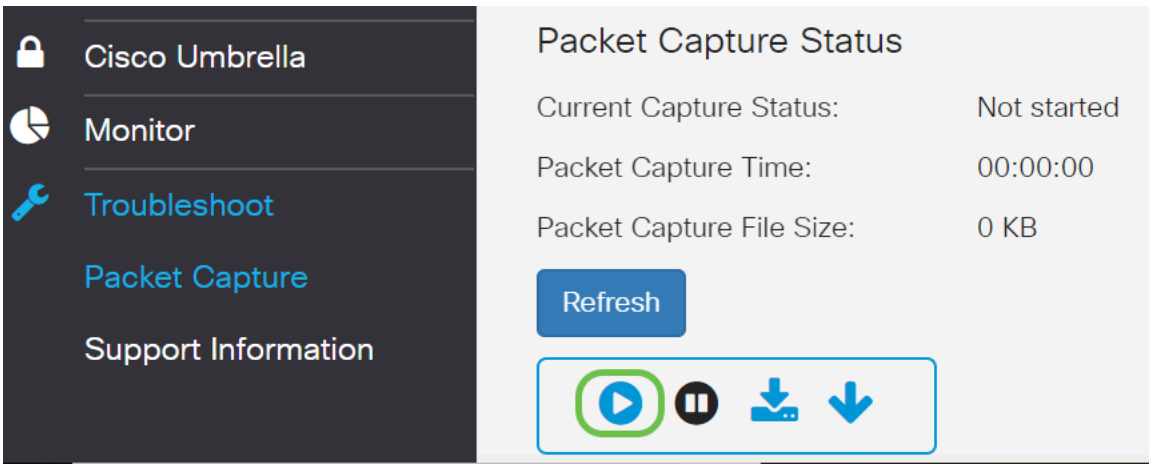
·*Filter on Client*: Gibt die MAC-Adresse für den WLAN-Clientfilter an. Beachten Sie, dass der Client-Filter nur aktiv ist, wenn eine Erfassung auf einer 802.11-Schnittstelle durchgeführt wird.

·*Filter on SSID*: Wählen Sie einen SSID-Namen für die Paketerfassung aus.

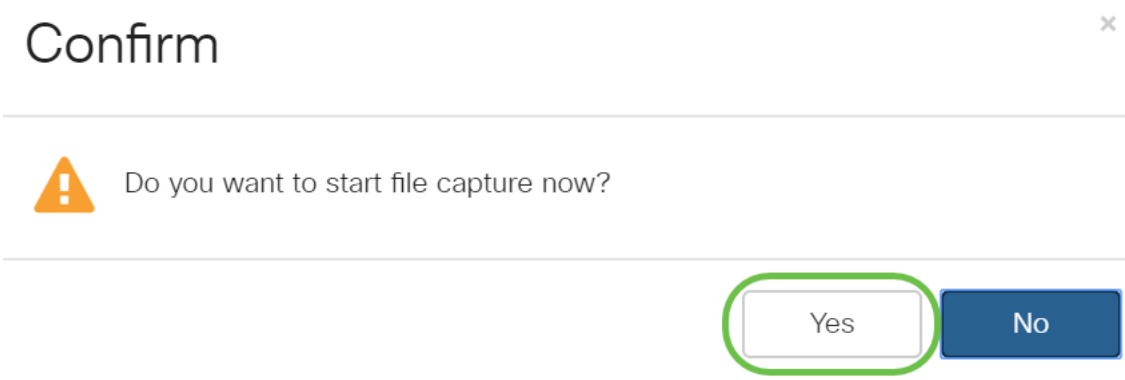
Klicken Sie auf **Übernehmen**, um die Startkonfiguration zu speichern.



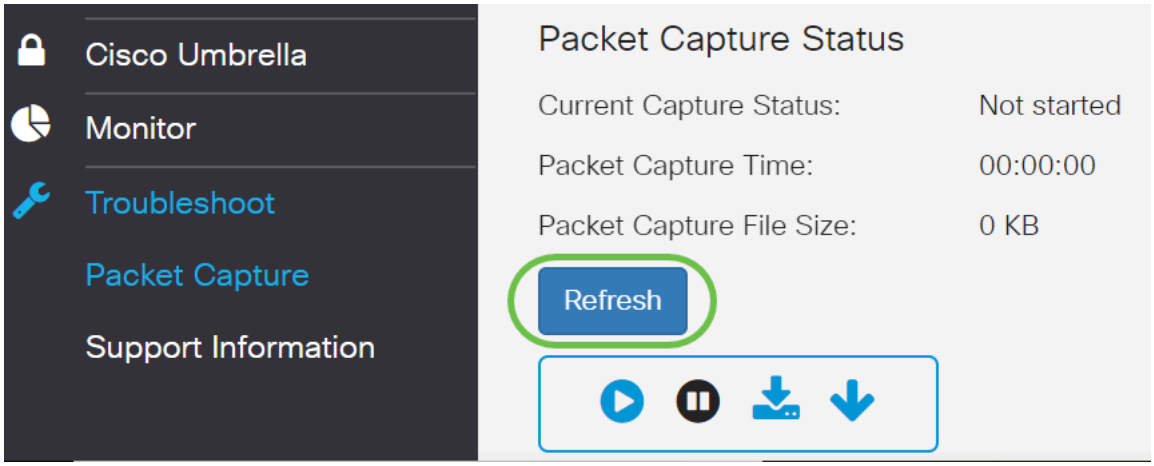

Schritt 2: Klicken Sie auf das Symbol **Erfassung starten**.



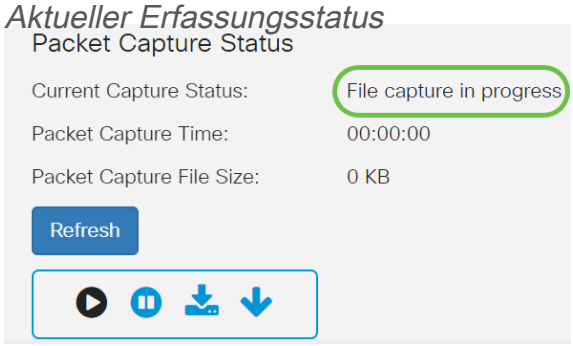

Schritt 3: Ein Popup-Fenster *Bestätigen* wird geöffnet, um die Bestätigung zum Herunterladen der Datei zu erhalten. Klicken Sie auf **Ja**, um den Download der Datei zu starten.



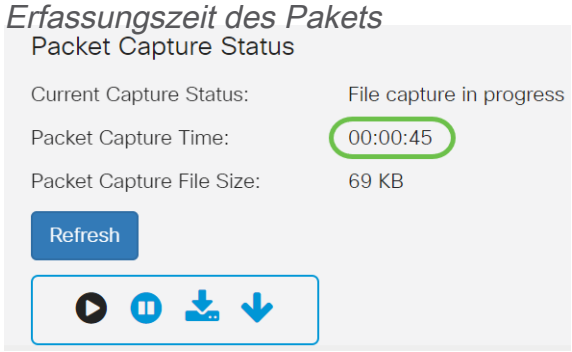

Schritt 4: Klicken Sie auf **Aktualisieren**, um den *Paketerfassungsstatus* abzurufen, der die folgenden Daten enthält:



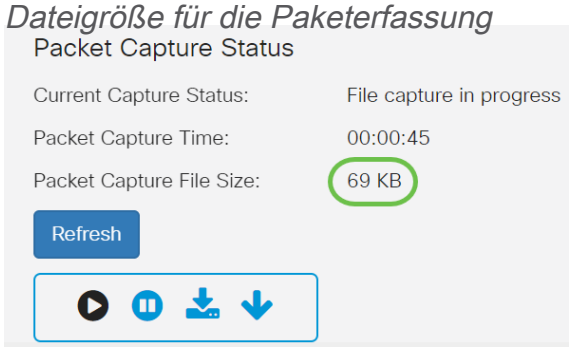

1. *Aktueller Erfassungsstatus*



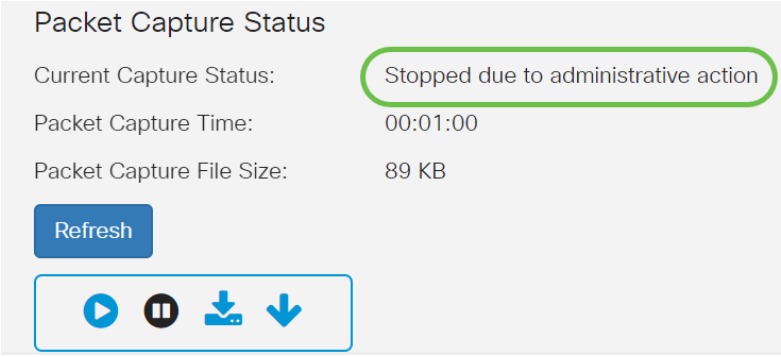

2. *Erfassungszeit des Pakets*




3. *Dateigröße für die Paketerfassung*

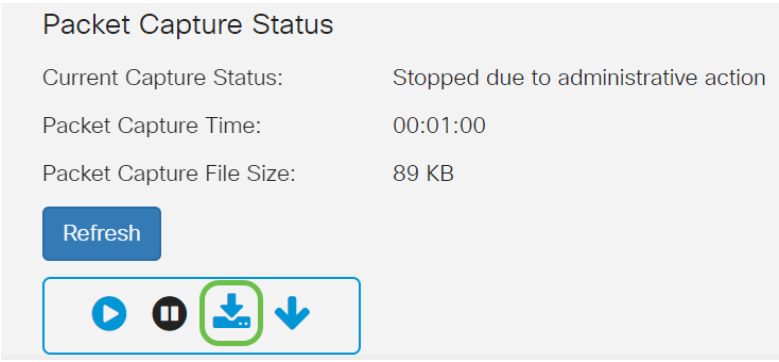



4. Im *Packet File Capture*-Modus speichert das WAP-Gerät die erfassten Pakete im RAM-Dateisystem (Random Access Memory). Bei der Aktivierung wird die Paketerfassung fortgesetzt, bis eines dieser Ereignisse eintritt:
   ·Die Erfassungszeit erreicht die konfigurierte Dauer.
   ·Die Erfassungsdatei erreicht ihre maximale Größe.
   ·Der Administrator beendet die Erfassung.

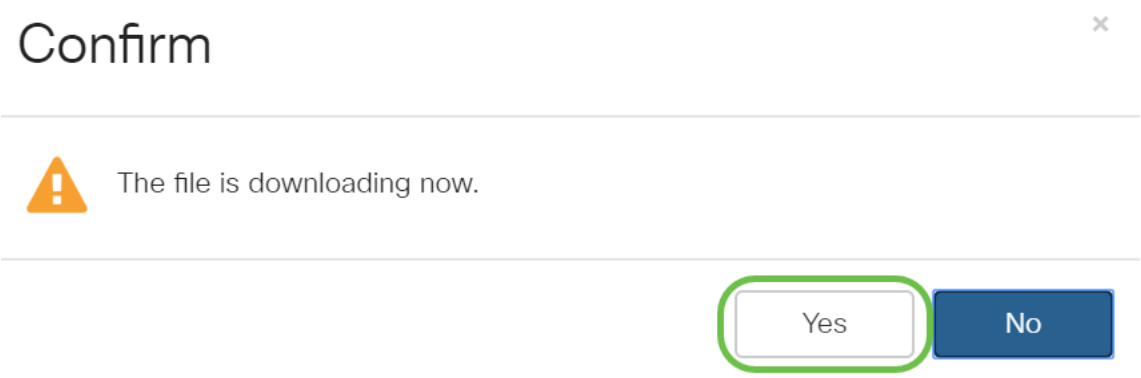



Die Paketerfassungsdatei wird im Access Point gespeichert, bis Sie den Access Point neu starten.

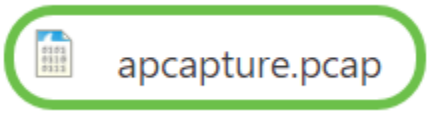
Schritt 5: Klicken Sie auf das Symbol **Download to this Device** (Zu diesem Gerät herunterladen), um die kürzlich erfasste Datei herunterzuladen.



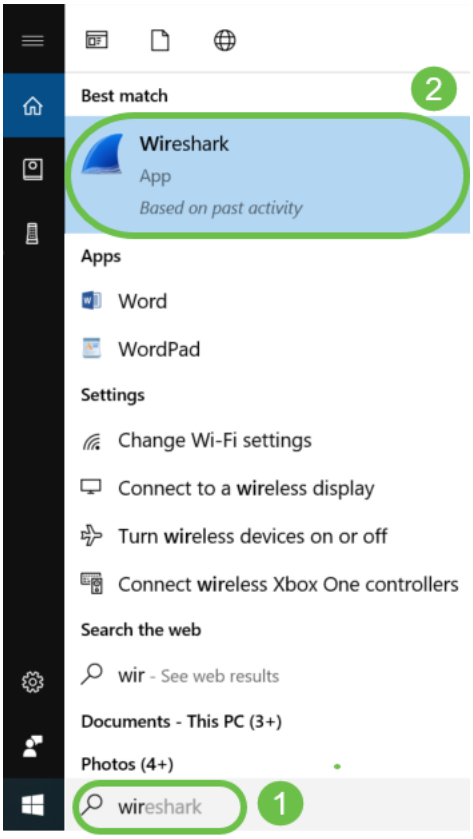

Schritt 6: Ein Popup-Fenster *Bestätigen* wird geöffnet, um den Download der Datei zu bestätigen. Klicken Sie auf **Ja**.



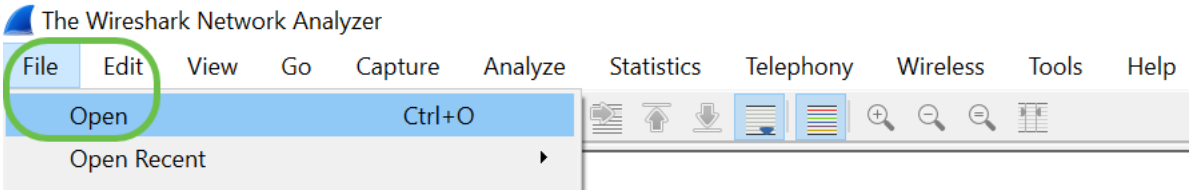

Schritt 7: Die Paketerfassungsdatei wird auf Ihren Computer heruntergeladen. In diesem Beispiel ist *apcapture.pcap* der Name der Datei.



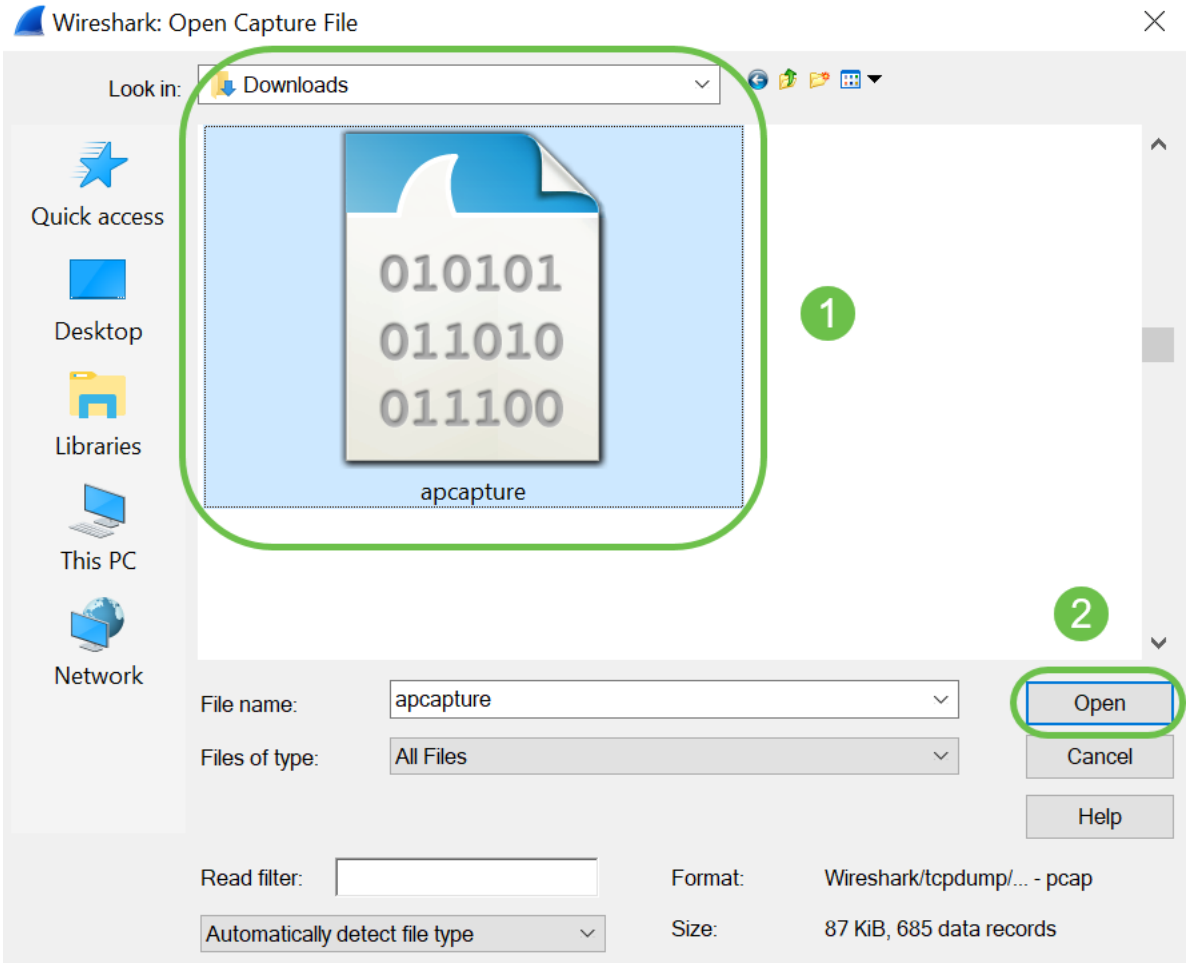

Schritt 8: Da Wireshark bereits heruntergeladen wurde, können Sie auf das Programm zugreifen, indem Sie *Wireshark* in der Suchleiste von Microsoft Windows eingeben und die Anwendung auswählen, wenn es eine Option ist.



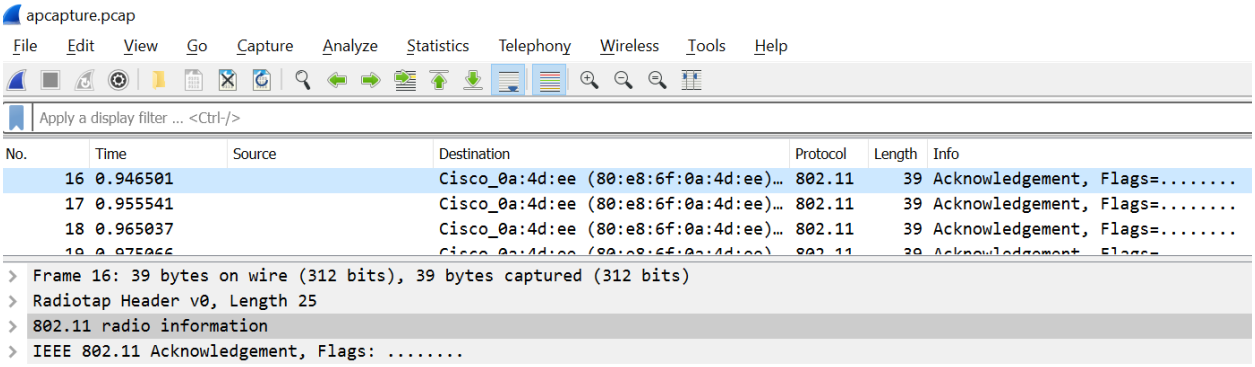

Schritt 9: Navigieren Sie zu **Datei > Öffnen**.




Schritt 10: Suchen Sie im neuen Popup-Fenster nach der Datei, in diesem Fall *apcapture.pcap*. Klicken Sie auf **Öffnen**.




Schritt 11: Die Datei wird in der *Wireshark*-Anwendung geöffnet, und Sie können die Details der Pakete sehen.




## Fazit

Sie lassen Ihr Paket erfassen und in Wireshark hochladen, und Sie können es jetzt auch analysieren. Nicht sicher, wohin Sie von hier gehen sollen? Es gibt viele Videos und Artikel online zu erkunden. Was Sie suchen, hängt von den Bedürfnissen Ihrer Situation ab. Du hast das!