

Verwenden von Wireshark auf einem Cisco Business WAP für die Paketanalyse: Direkter Stream zu Wireshark

Ziel

In diesem Artikel wird erläutert, wie Sie mithilfe eines Cisco Business Wireless Access Point (WAP) eine Paketerfassung des Netzwerkverkehrs durchführen und diesen direkt an Wireshark streamen.

Inhalt

- [Einführung und häufig gestellte Fragen](#)
- [Was ist eine Paketerfassung?](#)
- [Welche Arten von Paketen können erfasst werden?](#)
- [Wie kann eine Paketerfassung auf einem WAP durchgeführt werden?](#)
- [Wo kann ich das Paket streamen?](#)
- [Anwendbare Geräte und Softwareversion](#)
- [Wireshark herunterladen](#)
- [Melden Sie sich beim WAP an.](#)
- [Erläuterung zur Remote-Paketerfassung](#)
- [Streamen einer Erfassung direkt an Wireshark](#)

Einführung und häufig gestellte Fragen

Konfigurationsänderungen, Überwachung und Fehlerbehebung sind häufig ein Thema, mit dem sich Netzwerkadministratoren auseinandersetzen müssen. Ein einfaches Tool zu verwenden ist unschätzbar! In diesem Artikel sollen die Grundlagen der Paketerfassung und das Streaming der Pakete an Wireshark erläutert werden. 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 drahtlos auf den 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 auf einem WAP durchgeführt werden?

Es stehen zwei Methoden zur Paketerfassung zur Verfügung:

1. *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.

Wenn Sie die lokale Erfassungsmethode mit der neuesten Webbenutzeroberfläche bevorzugen, können Sie [mithilfe von Wireshark auf einem WAP für die Paketanalyse](#) auschecken: [Datei hochladen](#).

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](#).

2. *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. Der Vorteil dieser Methode besteht darin, dass die Menge an Paketen, die erfasst werden können, nicht begrenzt ist.

Der Schwerpunkt dieses Artikels ist Stream zu einem Remote-Host, sodass, wenn dies Ihre Präferenz ist, lesen Sie weiter!

Wo kann ich das Paket streamen?

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.

Einige Modelle der Cisco Business WAPs können Pakete in Echtzeit an CloudShark, eine webbasierte Website für Paket-Decoder und -Analyse, senden. Sie ähnelt der Wireshark-Benutzeroberfläche für die Paketanalyse, die viele zusätzliche Optionen mit einem Abonnement enthält. Sie können *Stream to CloudShark* auswählen, um die Remote-Erfassungsmethode auszuwählen. Klicken Sie auf die folgenden Links, um weitere Informationen zu erhalten:

- [CloudShark](#) (ihre offizielle Website)
- [Integration von CloudShark für die Paketanalyse auf einem WAP125 oder WAP581](#)
- [CloudShark-Integration mit WAP571 und WAP571E](#)

Weder Wireshark noch CloudShark sind Eigentum von Cisco oder werden von Cisco unterstützt. Sie sind nur zu Demonstrationszwecken enthalten. Wenden Sie sich für Support an [Wireshark](#) oder [CloudShark](#).

Anwendbare Geräte und Softwareversion

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


Wireshark herunterladen

Schritt 1

Öffnen Sie die [Wireshark](#)-Website. Wählen Sie die entsprechende Version aus. Klicken Sie auf **Download (Herunterladen)**. 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.

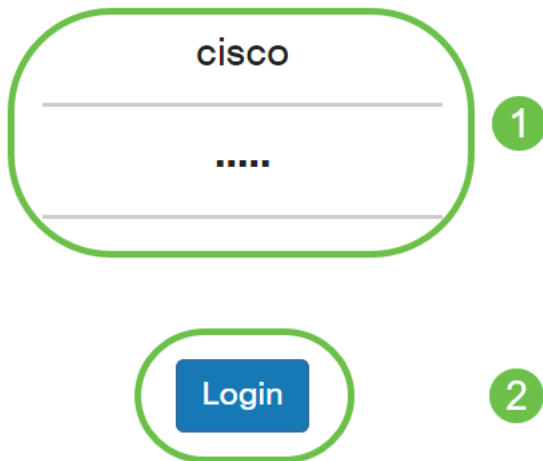
 Wireshark-win64-3.0.6.exe	10/30/2019 4:05 PM	Application	57,887 KB
--------------------------------------------------------------------------------------------------------------	--------------------	-------------	-----------

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.



Wireless Access Point



Erläuterung zur Remote-Paketerfassung

Mit der Funktion zur Paketerfassung per Remote-Zugriff können Sie einen Remote-Port als Zielport für die Paketerfassung festlegen. Diese Funktion arbeitet mit dem Wireshark-Netzwerkanalysetool für Windows zusammen. Ein Paketerfassungsserver wird auf dem WAP-Gerät ausgeführt und sendet die erfassten Pakete über eine TCP-Verbindung (Transmission Control Protocol) an das Wireshark-Tool.

Auf einem Microsoft Windows-Computer mit dem Wireshark-Tool können Sie den erfassten Datenverkehr anzeigen, protokollieren und analysieren. Die Remote-Paketerfassung ist eine Standardfunktion des Wireshark-Tools für Windows.

Obwohl die Remote-Paketerfassung von Linux nicht unterstützt wird, funktioniert das Wireshark-Tool unter Linux und bereits erstellte Erfassungsdateien können angezeigt werden.

Wenn der Remote-Erfassungsmodus verwendet wird, speichert das WAP-Gerät keine erfassten Daten lokal in seinem Dateisystem.

Wenn zwischen dem installierten Wireshark-Computer und dem WAP-Gerät eine Firewall installiert ist, muss Wireshark die Firewall-Richtlinie des Computers durchlaufen dürfen. Die Firewall muss auch so konfiguriert werden, dass der Wireshark-Computer eine TCP-Verbindung zum WAP-Gerät initiieren kann.

Streamen einer Erfassung direkt an Wireshark

Um eine Remote-Erfassung auf einem WAP-Gerät mithilfe der Option *Stream to a Remote Host* (

Stream zu einem Remote-Host) zu initiieren, führen Sie die unten aufgeführten Schritte aus.

Schritt 1

Navigieren Sie auf dem WAP zu **Fehlerbehebung > Paketerfassung**.

Für die *Paketerfassungsmethode*:

1. Wählen Sie **Stream zu einem Remote-Host** aus dem Dropdown-Menü aus.
2. Verwenden Sie im Feld *Remote Capture Port (Remote-Erfassungsport)* den Standard-Port von **2002**, oder geben Sie, wenn Sie einen anderen als den Standard-Port verwenden, die gewünschte Portnummer ein, die für die Verbindung von Wireshark mit dem WAP-Gerät verwendet wird. Der Port-Bereich liegt zwischen 1025 und 65530.
3. Es gibt zwei *Modi* für die Paketerfassung. Wählen Sie aus, was für Ihr Szenario am besten geeignet ist.

·*Gesamter Wireless-Datenverkehr* - Erfassen Sie alle Wireless-Pakete in der Luft.

·*Datenverkehr zu/von diesem AP* - Erfassen Sie das vom WAP oder vom empfangenen WAP gesendete Paket.

4. Aktivieren Sie **Filter aktivieren**.
5. Folgende Optionen stehen zur Auswahl:

·*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, ein bestehendes Wireless-Netzwerk anzukündigen.

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

·*Auf SSID filtern*: Diese Option wird für diesen *Stream zu einer Remote-Host-Option* deaktiviert.

6. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

The screenshot shows the Cisco WAP150 configuration interface for Packet Capture. The interface is titled "Packet Capture" and includes a navigation sidebar on the left. The sidebar has a "Troubleshoot" menu item highlighted with a green circle and the number 1. The "Packet Capture" menu item is also highlighted with a green circle and the number 2. The main content area shows the following settings:

- Packet Capture Method: Stream to a Remote Host (dropdown menu)
- Remote Capture Port: 2002 (text input field)
- Mode: All Wireless Traffic Traffic to/from this AP
- Enable Filters:
- Ignore Beacons:
- Filter on Client: 00:00:00:00:00:00 (text input field)
- Filter on SSID: (dropdown menu)

The "Apply" button is highlighted with a green circle and the number 3. The "Cancel" button is also visible.





Schritt 2

Klicken Sie auf das Symbol **Erfassung starten**.

Packet Capture Status

Current Capture Status:	Not started
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB


Refresh

Schritt 3

Ein Popup-Fenster "*Bestätigen*" wird geöffnet. Klicken Sie auf **Ja**, um die Erfassung zu starten.

Confirm ×

 Are you ready to start remote packet capture?





Schritt 4

Klicken Sie auf die Schaltfläche **Aktualisieren**, um den aktuellen Status zu überprüfen.

Packet Capture Status

Current Capture Status:	Not started
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB

Refresh

Schritt 5

Sie können jetzt sehen, dass der *aktuelle Erfassungsstatus Stream zu einem Remote-Host* ist.

Packet Capture Status

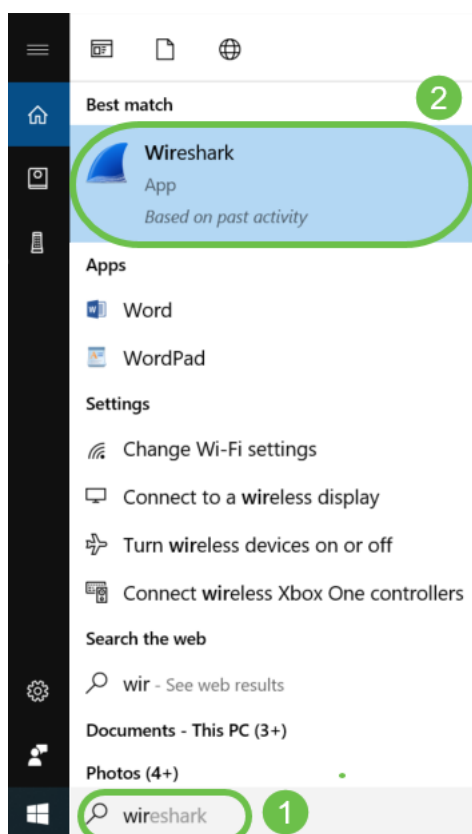
Current Capture Status:	Stream to a Remote Host
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB

Refresh

▶ || ⬇️ ⬇️

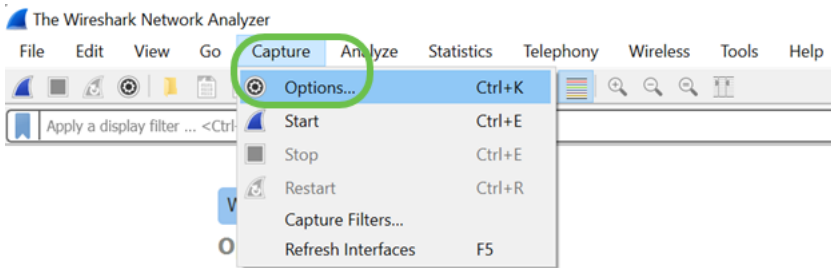
Schritt 6

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.



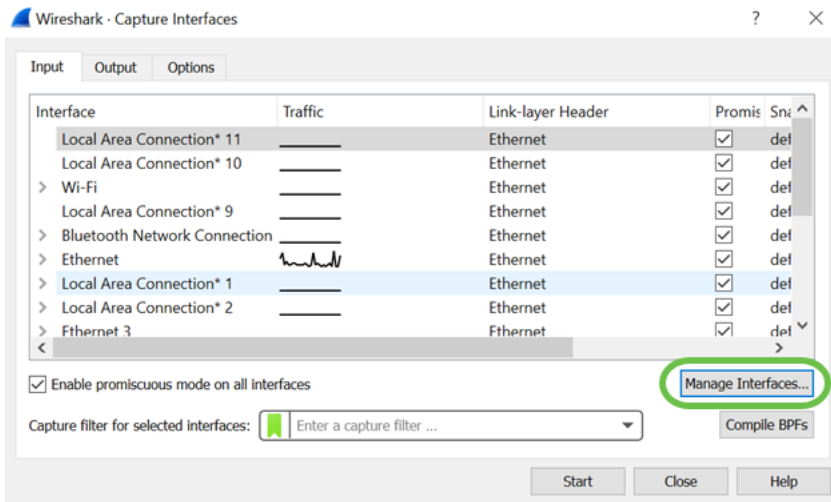
Schritt 7

Navigieren Sie zu **Erfassen > Optionen...**



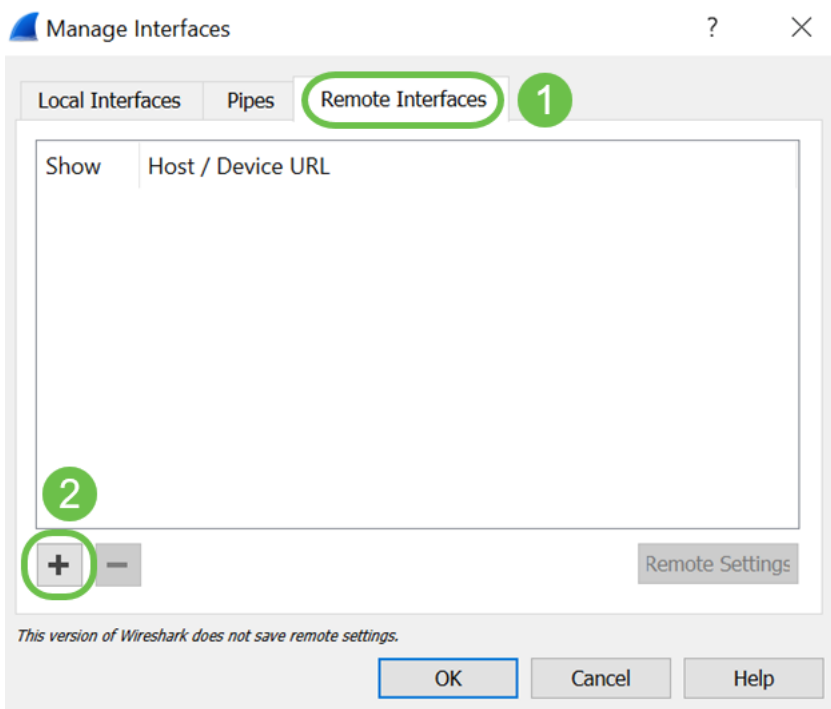
Schritt 8

Klicken Sie im neuen Popup-Fenster *Wireshark - Capture Interfaces (Wireshark - Erfassungsschnittstellen)* auf **Interfaces verwalten...**



Schritt 9

Navigieren Sie im neuen Popup-Fenster *Manage Interfaces (Schnittstellen verwalten)* zu **Remote Interfaces (Remote-Schnittstellen)**, und klicken Sie auf das **Plus-Symbol**, um die Schnittstelle hinzuzufügen.



Schritt 10

Geben Sie im neuen Popup-Fenster "*Remote Interface*" (*Remote-Schnittstelle*) den *Host ein*: IP-Adressdetails (die IP-Adresse des WAP-Geräts, in der Sie die Remote-Erfassung gestartet haben) und *Port*: Nummer (auf WAP für die Remote-Erfassung konfiguriert). In diesem Fall betrug die IP-Adresse des WAP-Geräts 192.168.1.134. Sie können die Option *Null-Authentifizierung* oder *Passwortauthentifizierung* auf Basis Ihrer Einstellungen auswählen. Wenn Sie diese Option auswählen, geben Sie bitte die entsprechenden *Benutzernamen* und *Passwortdetails* ein. Klicken Sie auf **OK**.

Remote Interface ? X

Host: 192.168.1.134

Port: 2002

1

2

Authentication

Null authentication

Password authentication

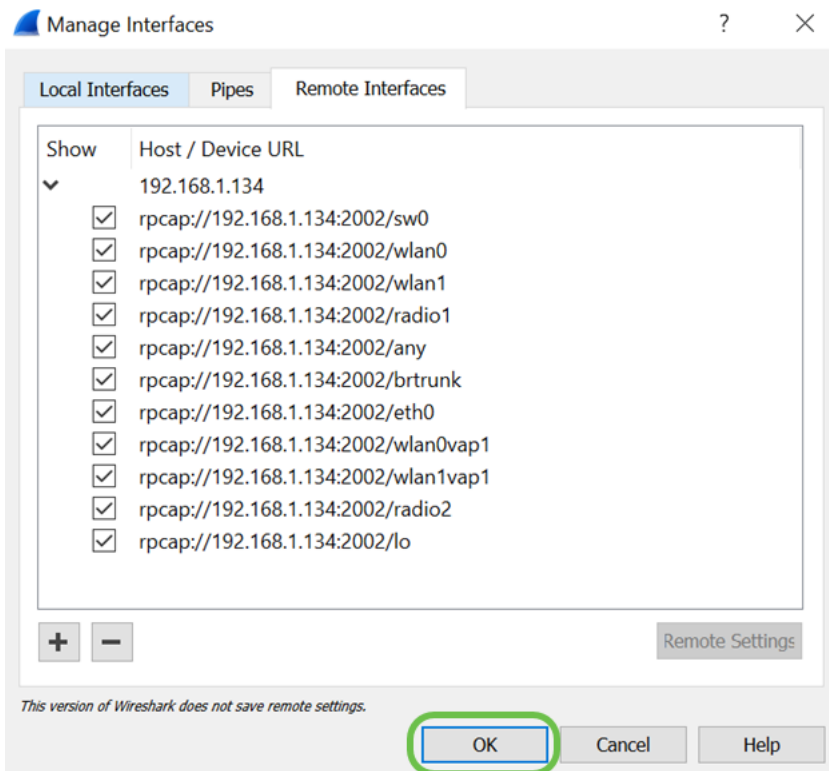
Username:

Password:

3 OK Cancel

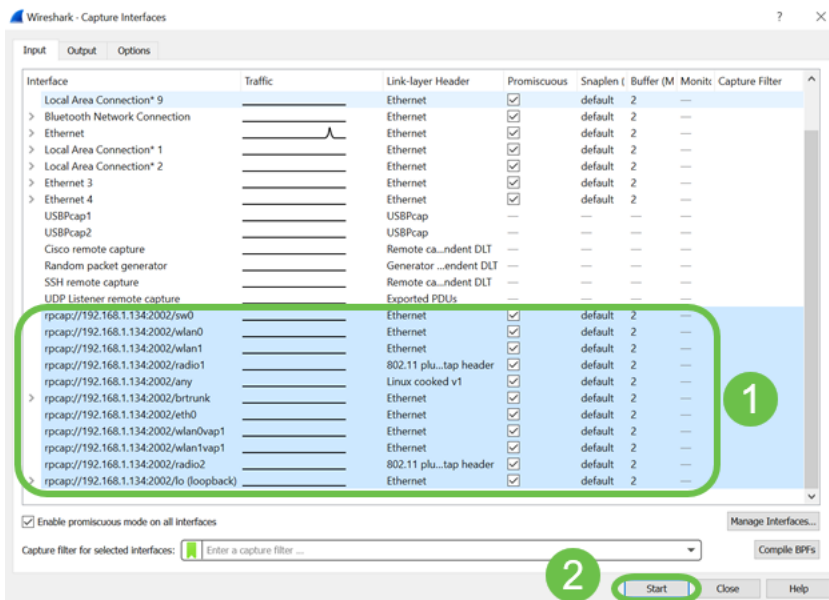
Schritt 11

Unter der Registerkarte *Remote-Schnittstellen* können Sie alle Schnittstellen des Remote-WAP-Geräts sehen. Möglicherweise möchten Sie einige dieser Pakete deaktivieren, um das Volumen der erfassten Pakete zu reduzieren. Wenn Beacon-Pakete angezeigt werden sollen, bleiben die ausgewählten Funkschnittstellen erhalten. Klicken Sie auf **OK**.



Schritt 12

Neu hinzugefügte Schnittstellen spiegeln nun das Fenster *Wireshark - Capture Interfaces* wider. Wählen Sie die Schnittstelle aus, die überwacht werden soll, und klicken Sie auf **Start**, um die Pakete anzuzeigen.



Wenn beim Versuch, die Pakete anzuzeigen, Probleme auftreten, bedeutet dies, dass der Dienst *Remote Packet Capture Protocol* nicht auf Ihrem System funktioniert. Der Remote Packet Capture Protocol-Dienst muss zuerst auf der Zielplattform ausgeführt werden, bevor Wireshark eine Verbindung zu ihm herstellen kann. Weitere Informationen erhalten Sie, wenn Sie auf den Link [Remote Capture Interfaces](#) through Wireshark klicken.

Schritt 13

Klicken Sie auf dem WAP auf das **Symbol Stopp Capture (Erfassung beenden)**, um den

Erfassungsprozess zu stoppen.

Packet Capture Status

Current Capture Status:	Stream to a Remote Host
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB


Refresh

▶ ⏸ ⬇️ ⬇️

Schritt 14

Ein Popup-Fenster *für eine Warnung* wird angezeigt. Klicken Sie auf **OK**, um die Remote-Erfassung zu beenden.

Alert ×

 Stop packet capture.

OK

Sie können die Paketerfassung auch unterbrechen, indem Sie in der Anwendung Wireshark auf die **Stopp**-Schaltfläche klicken.

Schritt 15

Jetzt wird der *aktuelle Erfassungsstatus aufgrund von Verwaltungsaktionen* als *Beendet* angezeigt, und die *Paketerfassungszeit* wird angezeigt, um die Gesamtaufzeichnungsdauer anzuzeigen.

Packet Capture Status

Current Capture Status:	Stopped due to administrative action
Packet Capture Time:	00:02:26
Packet Capture File Size:	0 KB

Refresh

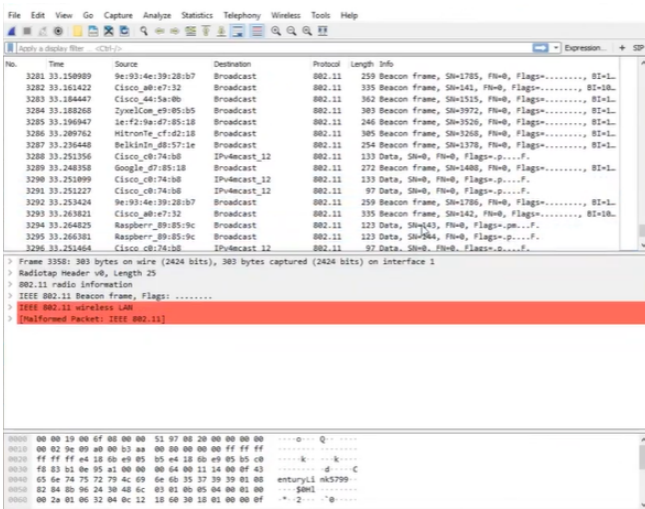
▶ ⏸ ⬇️ ⬇️

Die *Dateigröße für die Paketerfassung* wird als *0 KB* angezeigt. Darüber hinaus funktionieren

Dateidownload-Optionen in diesem Szenario nicht.

Schritt 16

Auf Wireshark können Sie die Paketerfassung anzeigen.



Fazit

Sie können jetzt ein Paket-Stream direkt zu Wireshark übertragen und es direkt 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!