パケット分析のためのCisco Business WAPでのWiresharkの使用：ファイルのアップロード

目的

この記事では、Cisco Business Wireless Access Point(WAP)およびWiresharkを使用してパケットキャプチャを実行、保存、およびアップロードする方法について説明します。

概要

設定の変更、モニタリング、およびトラブルシューティングは、ネットワーク管理者が頻繁に対処する必要があります。簡単なツールを使用することは非常に貴重です！この記事の目的は、パケットキャプチャの基本と、Wiresharkにファイルをアップロードする方法について、さらに理解を深めることです。このプロセスに精通していない場合は、すでに質問に答えましょう。

まず最初に、Wiresharkは、ネットワークのトラブルシューティングを検討しているすべてのユーザに対する無料パケットアナライザです。Wiresharkには、キャプチャに関する多くのオプションが用意されており、複数の異なるパラメータでトラフィックをソートできます。このオープンソースオプションの詳細については、Wiresharkに進んでください。

パケットキャプチャとは何ですか。

パケットキャプチャ（PCAPファイルとも呼ばれる）は、トラブルシューティングに役立つツールです。ネットワーク内のデバイス間で送信されるすべてのパケットをリアルタイムで記録できます。パケットをキャプチャすると、ネットワークトラフィックの詳細を調べることができます。これには、デバイスの検出、プロトコルの会話、および認証の失敗などすべてが含まれます。特定のトラフィックフローのパスと、選択したネットワーク上のデバイス間のすべてのインタラクションを確認できます。これらのパケットは、必要に応じてさらに分析するために保存できます。これは、パケットの転送を介したネットワークの内部の動作のX線のようなものです。

どのような種類のパケットをキャプチャできますか。

WAPデバイスは、次のタイプのパケットをキャプチャできます。

・無線インターフェイスで送受信された802.11パケット。無線インターフェイスでキャプチャされたパケットには、802.11ヘッダーが含まれます。

・イーサネットインターフェイスで送受信される802.3パケット。

・仮想アクセスポイント(VAP)やWireless Distribution System(WDS)インターフェイス

などの内部論理インターフェイスで送受信される802.3パケット。

パケットキャプチャを実行する方法はどれか？

パケットキャプチャには、次の2つの方法があります。

1. *リモートキャプチャ方法*：キャプチャされたパケットは、Wiresharkを実行している外部コンピュータにリアルタイムでリダイレクトされます。リモート・キャプチャ方法を選択するには、*[Stream to a Remote Host]*を選択できます。リモートキャプチャ方式を使用する場合は、「パケット分析**のためのWAPでのWiresharkの使用：Wiresharkに直接ストリーミングします**。
2. *ローカルキャプチャ方法*：キャプチャされたパケットは、WAPデバイス上のファイルに保存されます。WAPデバイスは、トリビアルファイル転送プロトコル(TFTP)サーバにファイルを転送できます。ファイルはPCAP形式でフォーマットされ、Wiresharkを使用して調べることができます。*[このデバイスにファイルを保存]を選択して、ローカルキャプチャ方式を選択できます。*

この記事では、最新のグラフィカルユーザインターフェイス(GUI)を備えたWiresharkにファイルをアップロードします。 ローカルキャプチャ方式に古いGUIを使用する記事を表示する場合は、「ワイヤレスアクセスポイントのパフォーマンスを最適化するためのパケットキャプチャの設定」を参照してください。

PCAPファイルを取得したら、パケットキャプチャをどのように行いますか。

ワイヤレスパケットキャプチャ機能は、WAPデバイスで送受信されたパケットをキャプチャして保存することを可能にします。キャプチャされたパケットは、トラブルシューティングまたはパフォーマンス最適化のためにネットワークプロトコルアナライザで分析できます。オンラインで利用できるサードパーティ製パケットアナライザアプリケーションは数多くあります。この記事では、Wiresharkについて説明します。

Wiresharkは、シスコが所有またはサポートしていません。サポートについては、Wiresharkにお問い合 **わせください**。

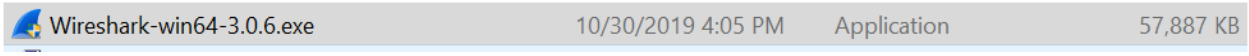
Devices |ソフトウェアバージョン

- 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のダウンロード

ステップ1:WiresharkのWebサイト**に移動**します。[Download] をクリックします。ダウンロードする適切なバージョンを選択します。画面左下にダウンロードの進行状況が表示されます。

ステップ2：コンピュータのダウンロード*に移動*し、Wiresharkファイルを選択してそのアプリケーションをインストールします。



WAPにログインします

Webブラウザで、WAPのIPアドレスを入力します。認証情報を入力してください。このデバイスに初めてアクセスした場合、または工場出荷時のリセットを行った場合、デフォルトのユーザ名とパスワードは*cisco*です。ログイン方法の説明が必要な場合は、**Wireless Access Point (WAP)のWebベースのユーティリティへのアクセスに関する記事の手順に従ってく**ださい。

PCでのパケットキャプチャの保存とWiresharkへのアップロード

ステップ1:[Troubleshoot] > **[Packet Capture]に移動します。**

[パケットキャプチャ**方法]で[このデバイスのファイ**ルを保存]が選択されていることを*確認してください。*

次のパラメータを設定します。

・ *Interface* – パケットキャプチャのキャプチャインターフェイスタイプを入力します。

・ *Ethernet* : イーサネットポート上の802.3トラフィック。

・ *無線1(5 GHz)/無線2(2.4 GHz)* - 802.11トラフィックを無線インターフェイスで伝送します。

・ *Duration* – キャプチャの時間 (秒) を入力します。範囲は 10 ~ 3600 です。デフォルト値は 60 です。

・ *Max File Size* : キャプチャファイルの最大許容サイズ(KB)を入力します。 範囲は 64 ~ 4096 です。デフォルト値は 1024 です。

パケットキャプチャには2つのモードがあります。

・ *All Wireless Traffic* : すべての無線パケットをキャプチャします。

・ *このAPとの間のトラフィック*:APから送信されたパケット、またはAPで受信されたパケットをキャプチャします。

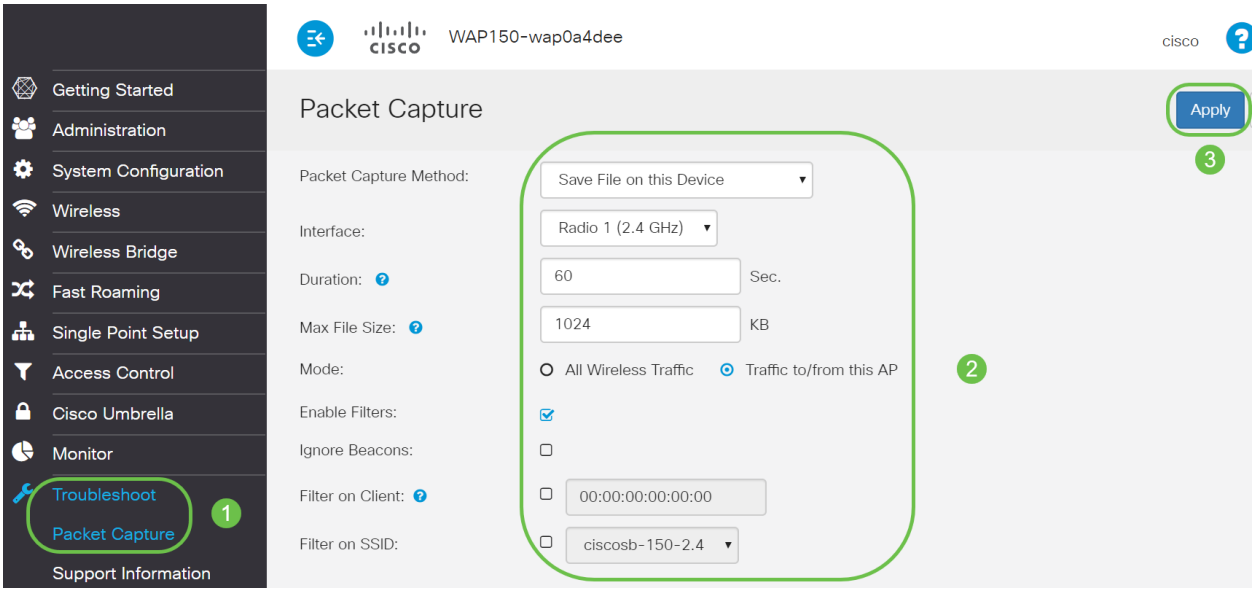
[フィルタを有効**にする]をクリックします**。[ビーコンを無視(Ignore Beacons)]、[クライアント*でフィルタ(Filter on Client)]、および[SSIDでフィルタ(Filter on SSID)]の3つのチェックボックスがあります*。

・ *ビーコンを無視する* : 無線で検出または送信された802.11ビーコンのキャプチャを有効または無効にします。ビーコンフレームは、ネットワークに関する情報を伝送するブロードキャストフレームです。ビーコンの目的は、既存のワイヤレスネットワークをアドバタイズすることです。このタイプのトラフィックを探していない場合は、[ビーコンを無視]を選択できます。

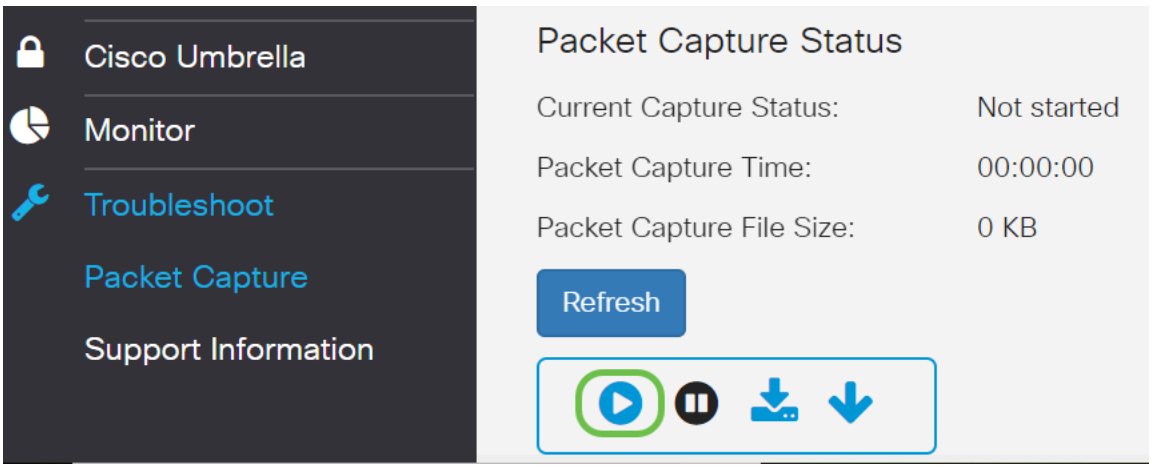
・ *Filter on Client*:WLANクライアントフィルタのMACアドレスを指定します。クライアントフィルタがアクティブになるのは、802.11インターフェイスでキャプチャが実行された場合だけです。

・ *Filter on SSID* : パケットキャプチャのSSID名を選択します。

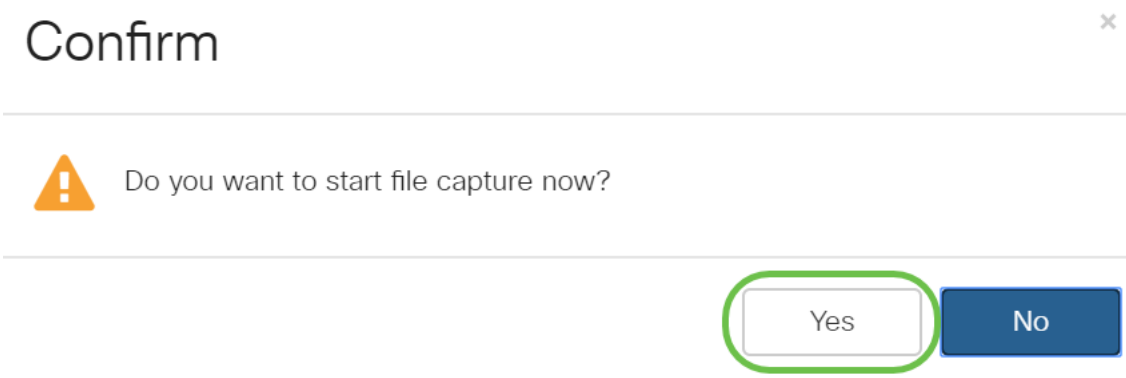
[Apply]をクリックし、スタートアップコンフィギュレーションに保存します。



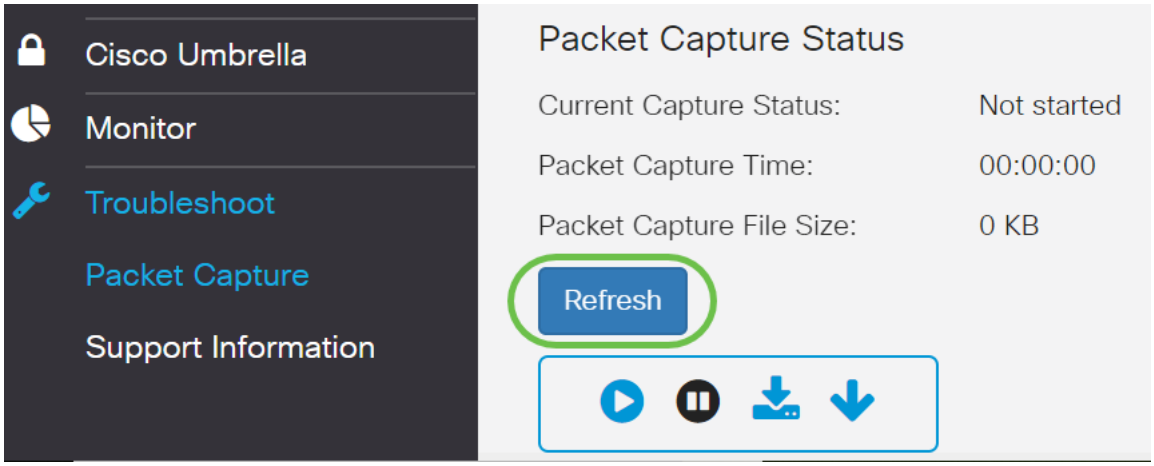
ステップ2:[Start Capture]アイコンをクリックします。



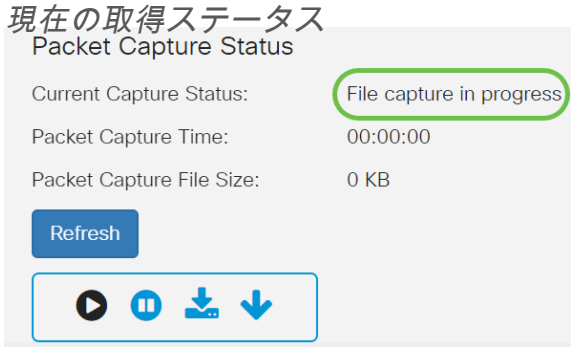
ステップ3:[*Confirm*]ポップアップウィンドウが開き、ファイルのダウンロードを確認できます。[**Yes**]をクリックしてファイルのダウンロードを開始します。



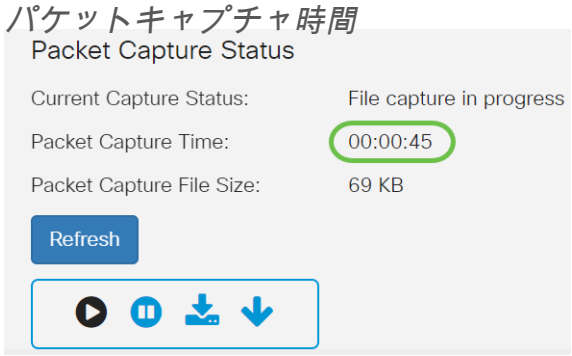
ステップ4:[Refresh]をクリックし、次のデータを含む*[Packet Capture Status]*を取得します。



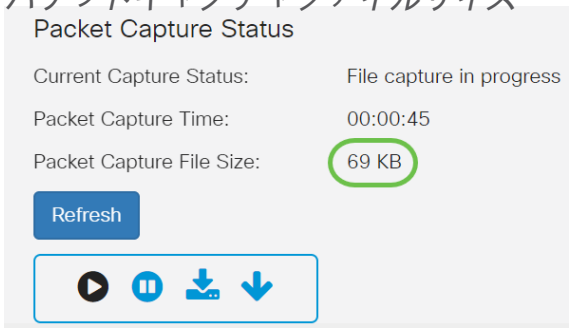
1. *現在の取得ステータス*



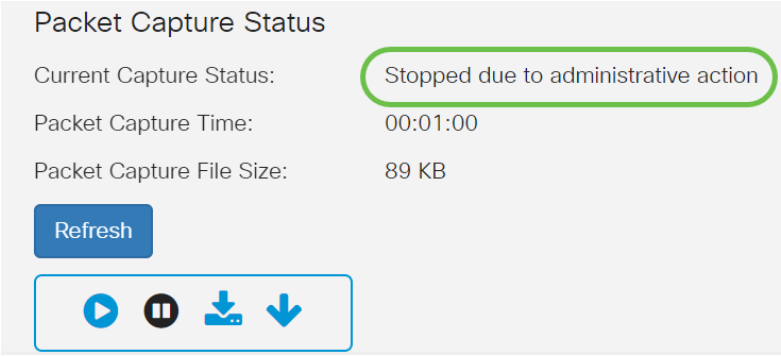
2. *パケットキャプチャ時間*



3. *パケットキャプチャファイルサイズ*

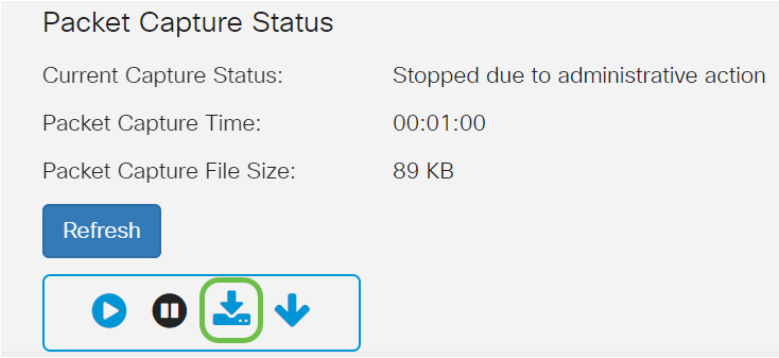


4. パケットファイル取り込みモードでは、WAPデバイスは取り込んだパケットをランダムアクセスメモリ(RAM)ファイルシステムに格納します。アクティブ化されると、次のいずれかのイベントが発生するまでパケットキャプチャが続行されます。
   - キャプチャ時間が設定された期間に達します。
   - キャプチャファイルが最大サイズに達します。
   - 管理者がキャプチャを停止します。

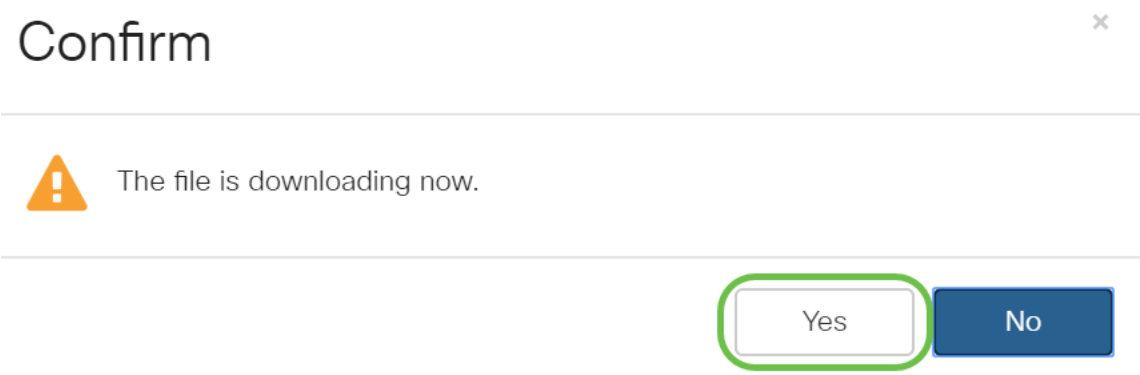


パケットキャプチャファイルは、APをリブートするまでAPに保存されます。

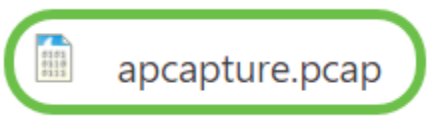
ステップ5:[Download to **this Device]アイコンをクリックして**、最近キャプチャしたファイルをダウンロードします。



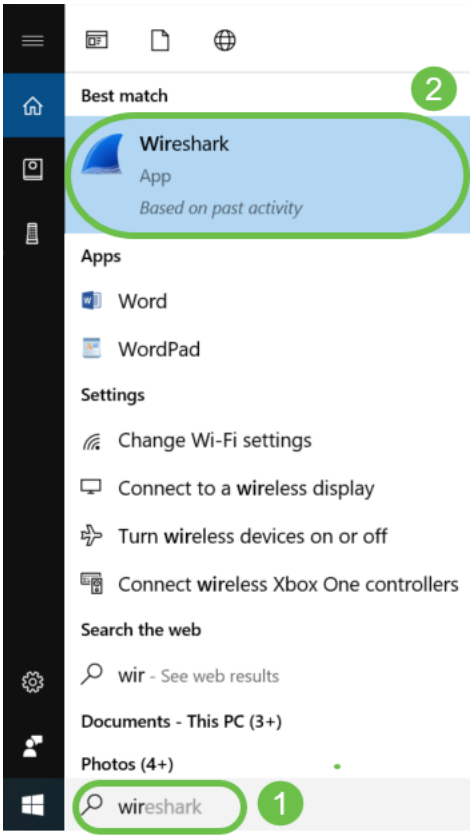
ステップ6:[Confirm]ポップアップウィンドウが開き、ファイルのダウンロードを確認できます。[Yes]をクリック**します**。



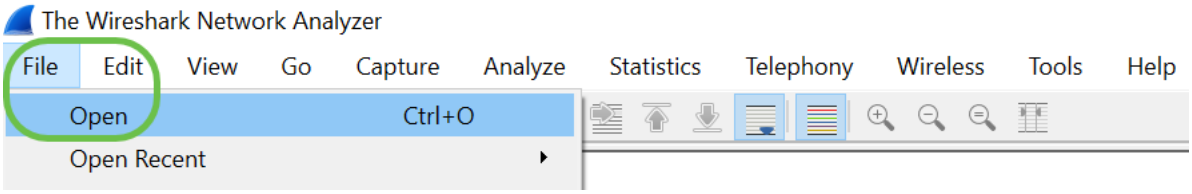
ステップ7：パケットキャプチャファイルがコンピュータにダウンロードされます。この例では、*apcapture.pcap*はファイルの名前です。



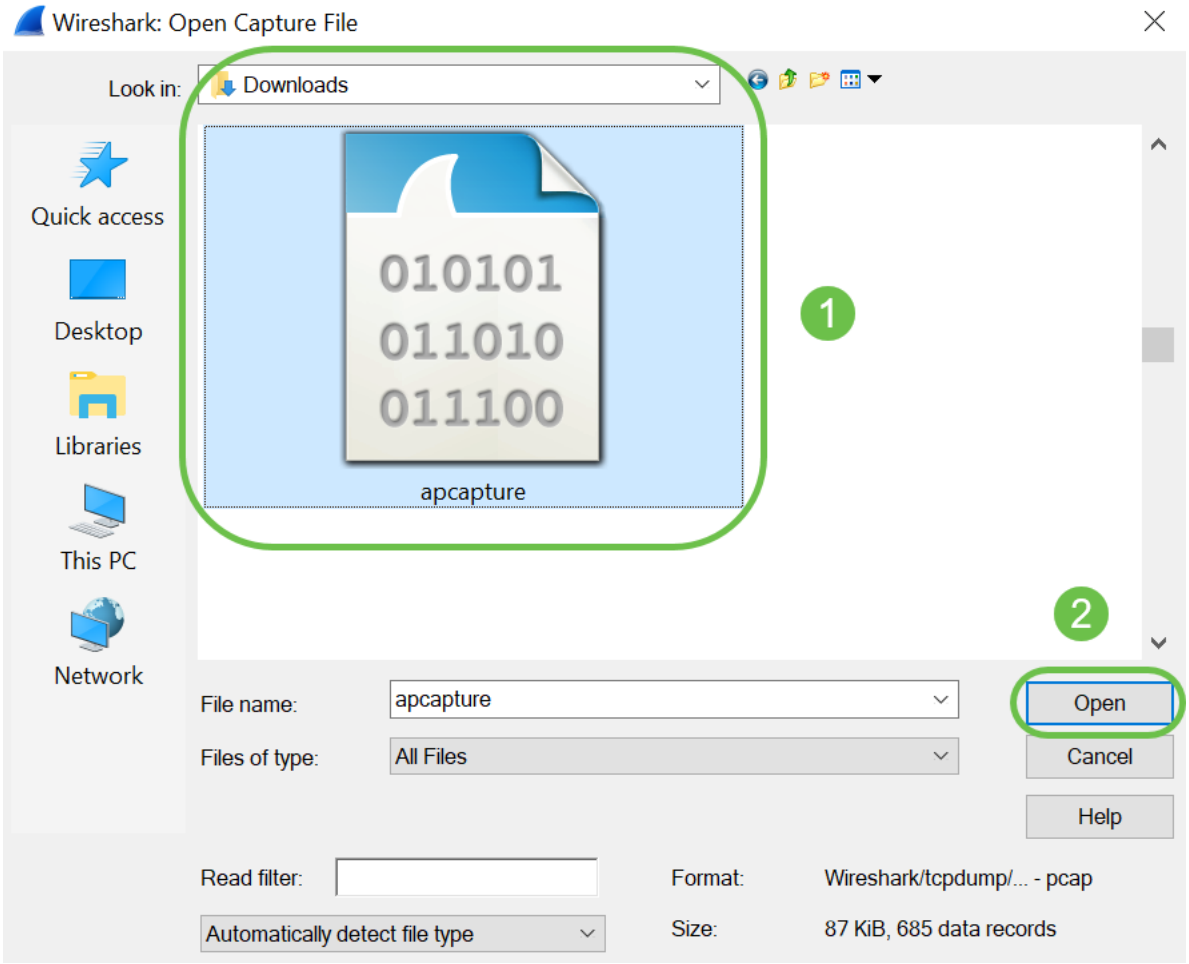
ステップ8:Wiresharkはすでにダウンロードされているため、Microsoft Windowsの検索バーに*Wireshark*と入力し、*オプションが表示されたらアプリケーションを選択してアクセスできます。*



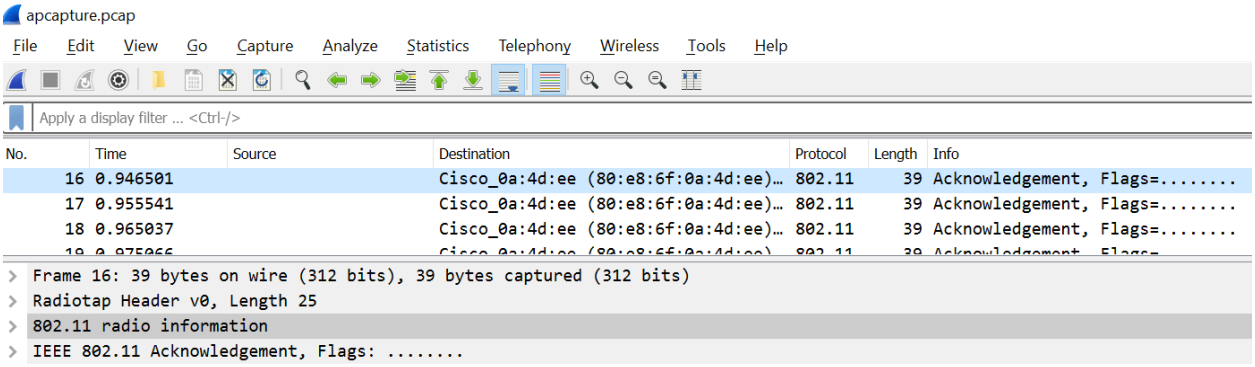
ステップ9:[ファイル] > [開く]に移動します。



ステップ10：新しいポップアップウィンドウで、ファイル(この場合は*apcapture.pcap*)を参照します。[Open] をクリックします。



ステップ11：ファイルが*Wireshark*アプリケーションで開き、パケットの詳細を表示できます。



結論

パケットがキャプチャされ、Wiresharkにアップロードされました。これで、パケットの分析を行うことができます。ここからどこに行けばいいのか分からないのか？オンラインで閲覧できる動画や記事は多数あります。検索する内容は、状況のニーズによって異なります。これだ！