在思科企業WAP上使用Wireshark進行資料包分析：上傳檔案

目標

本文說明如何使用思科企業無線存取點(WAP)和Wireshark執行、儲存和上傳封包擷取。

簡介

配置更改、監控和故障排除是網路管理員必須經常解決的問題。擁有簡單的工具非常寶貴！本文的目標是更熟悉封包擷取的基礎知識以及如何將檔案上傳到Wireshark。如果您不熟悉此過程，讓我們回答您可能已經遇到的一些問題。

首先，Wireshark是免費的包分析器，適合任何想要排除網路故障的人。Wireshark為捕獲提供了許多選項，並按幾個不同的引數對流量進行排序。請前往Wireshark，瞭解有關此開源選項的詳細資訊。

什麼是資料包捕獲？

資料包捕獲（也稱為PCAP檔案）是一種有助於進行故障排除的工具。它可以即時記錄網路中裝置之間傳送的每個資料包。通過捕獲資料包，您可以深入瞭解網路流量的詳細資訊，這些資訊可能包括裝置發現、協定對話和失敗身份驗證等所有內容。您可以看到特定流量的路徑以及選定網路上裝置之間的每次互動。可以根據需要儲存這些資料包以供進一步分析。它就像通過資料包傳輸來檢視網路內部運作情況的X光片。

可以捕獲哪些型別的資料包？

WAP裝置可以捕獲以下型別的資料包：

·在無線電介面上接收和傳輸的802.11資料包。在無線電介面上捕獲的資料包包括802.11報頭。

·在乙太網介面上接收和傳輸的802.3資料包。

·在內部邏輯介面(例如虛擬接入點(VAP)和無線分佈系統(WDS)介面)上接收和傳輸的802.3資料包。

如何執行資料包捕獲？

有兩種資料包捕獲方法可用：

1. *遠端捕獲*方法 — 捕獲的資料包被即時重定向到運行Wireshark的外部電腦。您可以選擇*Stream to a Remote Host*以選擇遠端捕獲方法。如果您更喜歡遠端捕獲方法，請檢視在

WAP上使用Wireshark進行資料包分析：直接流向Wireshark。

2. *本地捕獲方法* — 捕獲的資料包儲存在WAP裝置上的檔案中。WAP裝置可將檔案傳輸到簡單式檔案傳輸協定(TFTP)伺服器。檔案採用PCAP格式，可以使用Wireshark檢查。您可以選擇*Save File on this Device*以選擇本地捕獲方法。

本文的重點是將具有最新圖形使用者介面(GUI)的檔案上傳到Wireshark。 如果您更喜歡檢視使用舊版GUI進行本地捕獲方法的文章，請選中Configure Packet Capture to Optimize Performance on a Wireless Access Point。

在具有PCAP檔案後，如何處理資料包捕獲？

無線分組捕獲功能能夠捕獲和儲存由WAP裝置接收和傳輸的分組。捕獲的資料包隨後可由網路協定分析器進行分析，以進行故障排除或效能最佳化。許多第三方資料包分析器應用程式都可以線上使用。本文重點介紹Wireshark。

Wireshark不是思科的所有者或支持者。如需支援，請聯絡 Wireshark。

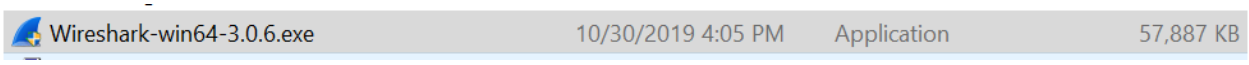
裝置 |軟體版本

- 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

下載Wireshark

步驟1.訪問Wireshark網站。按一下「**Download**」。選擇要下載的相應版本。您將在螢幕左下角看到下載進度。

步驟2.轉到*您電腦上的Downloads*，然後選擇Wireshark檔案以安裝其應用程式。



登入到WAP

在Web瀏覽器中，輸入WAP的IP地址。輸入您的憑據。如果您是第一次訪問此裝置或進行了出廠重置，則預設使用者名稱和密碼為*cisco*。如果您需要有關如何登入的說明，可以按照無線接入點(WAP)文章訪問基於Web的實用程式中的步驟操作。

在PC上儲存資料包捕獲並上傳到Wireshark

步驟1.導覽至**Troubleshoot > Packet Capture**。

確保為*Packet Capture Method*選擇了**Save File on this Device**。

配置以下引數：

·*Interface* — 輸入封包擷取的擷取介面型別：

·*Ethernet* — 乙太網埠上的802.3流量。

·*無線電1(5 GHz)/無線電2(2.4 GHz)* — 無線電介面上的802.11流量。

·*Duration* — 輸入捕獲的持續時間（秒）。範圍為10到3600。預設值為60。

·*Max File Size* — 輸入捕獲檔案允許的最大大小(KB)。 範圍為64至4096。預設值為1024。

封包擷取有兩種模式。

·*All Wireless Traffic* — 捕獲所有無線資料包。

·*傳入/傳出此AP的流量* — 捕獲從AP傳送或由AP接收的資料包。

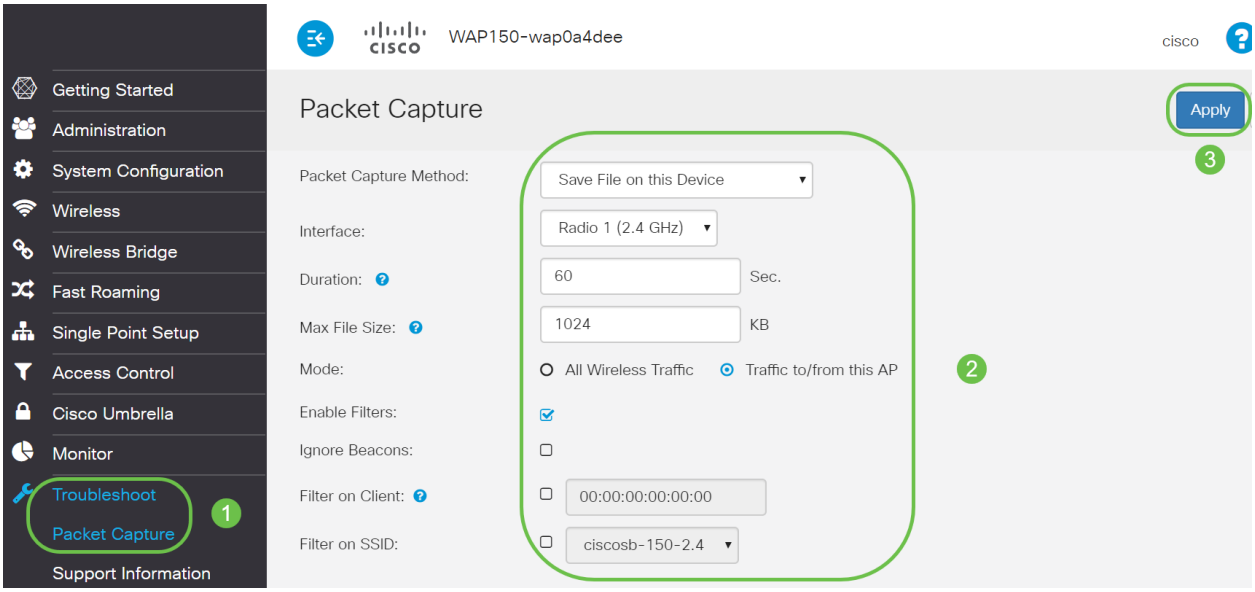
按一下「**Enable Filters**」。有三個覈取方塊可用：*Ignore Beacons*、*Filter on Client*和*Filter on SSID*。

·*Ignore Beacons* — 啟用或停用對無線電偵測或傳輸的802.11信標進行擷取。信標幀是承載關於網路的資訊的廣播幀。信標的目的是通告現有的無線網路。如果您不查詢此類流量，則可以選擇Ignore Beacons。

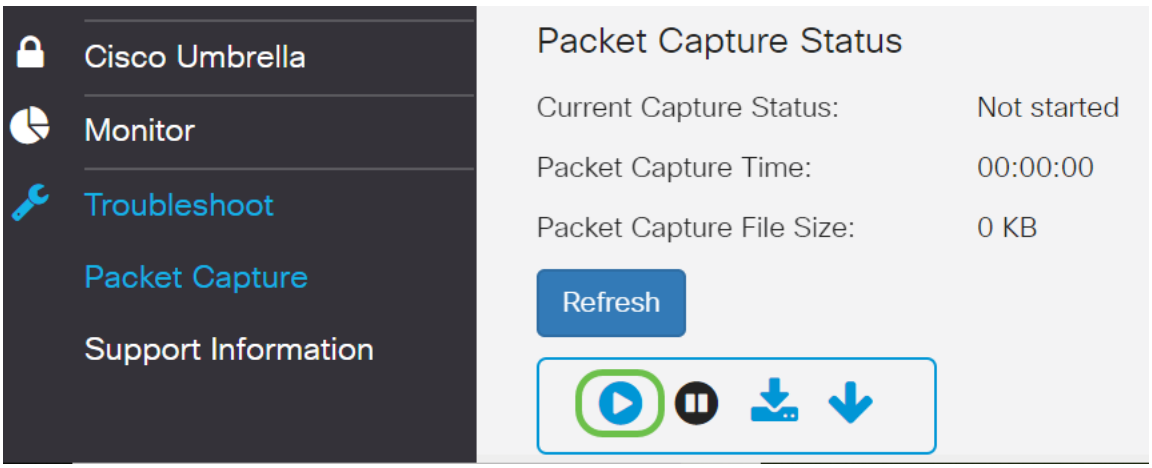
·*Filter on Client* — 指定WLAN客戶端過濾器的MAC地址。請注意，僅當在802.11介面上執行捕獲時，客戶端過濾器才處於活動狀態。

·*SSID過濾* — 選擇資料包捕獲的SSID名稱。

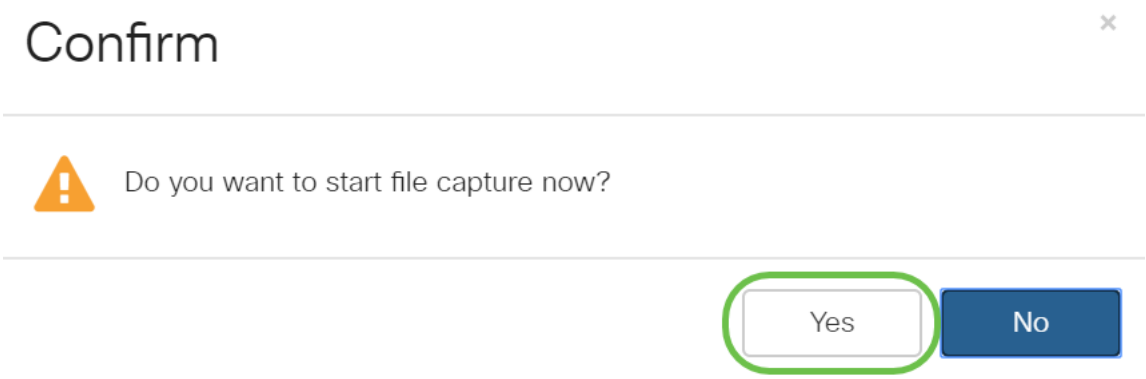
按一下「**Apply**」以儲存到「Startup Configuration」中。



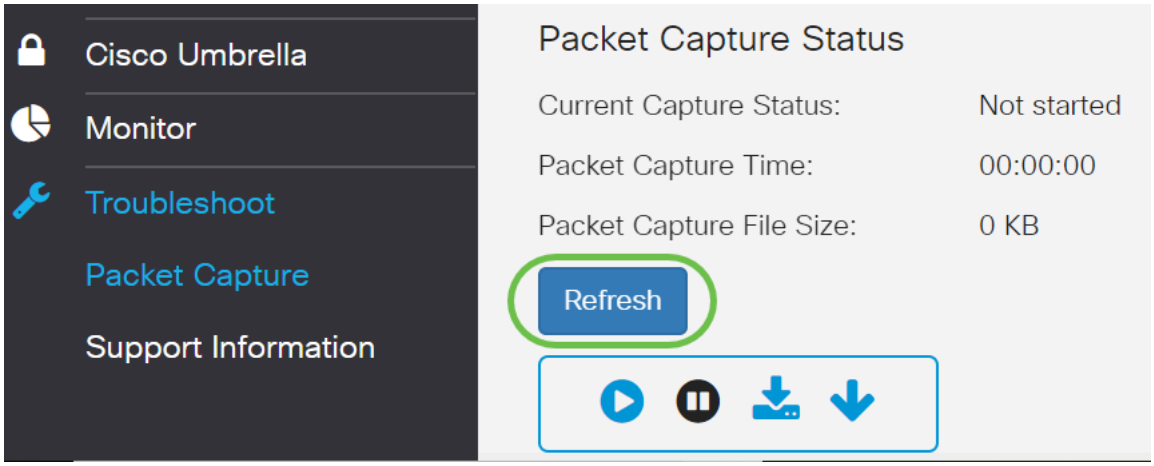
步驟2.按一下**Start Capture**圖標。



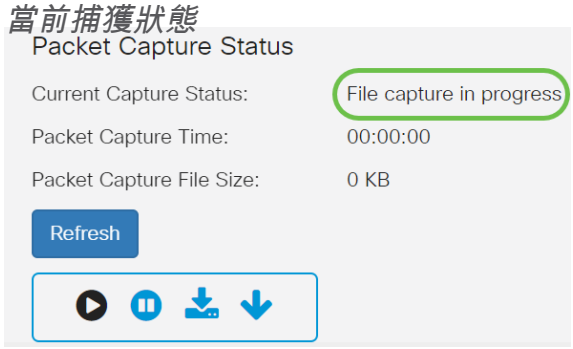
步驟3.將開啟*Confirm*彈出視窗獲取下載檔案的確認，然後點選**Yes**開始下載檔案。



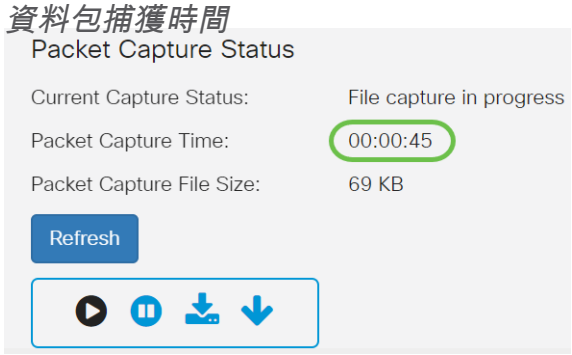
步驟4.按一下**Refresh**以獲取*Packet Capture Status*，其中包含下列資料：



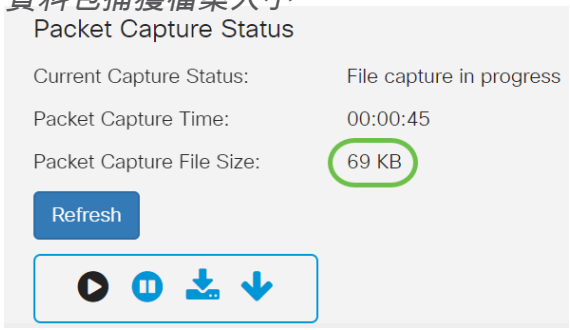
1. *當前捕獲狀態*



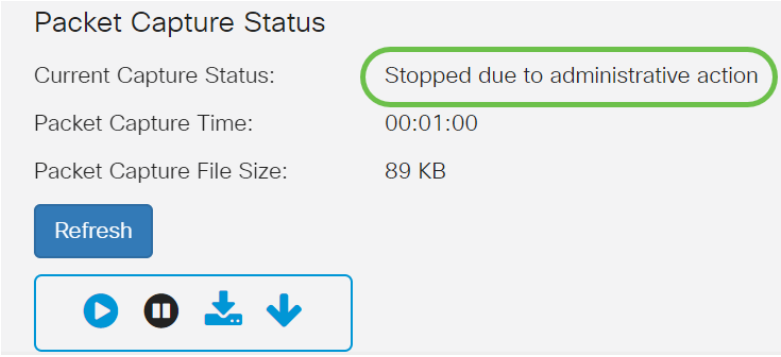
2. *資料包捕獲時間*



3. *資料包捕獲檔案大小*

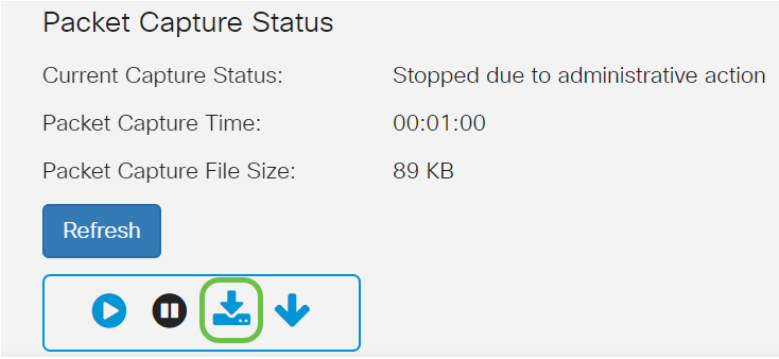


4. 在*封包檔案擷取*模式下，WAP裝置會將擷取的封包儲存在隨機存取記憶體(RAM)檔案系統中。啟用後，資料包捕獲繼續進行，直到發生以下事件之一：
   ·捕獲時間達到配置的持續時間。
   ·捕獲檔案達到其最大大小。
   ·管理員停止捕獲。

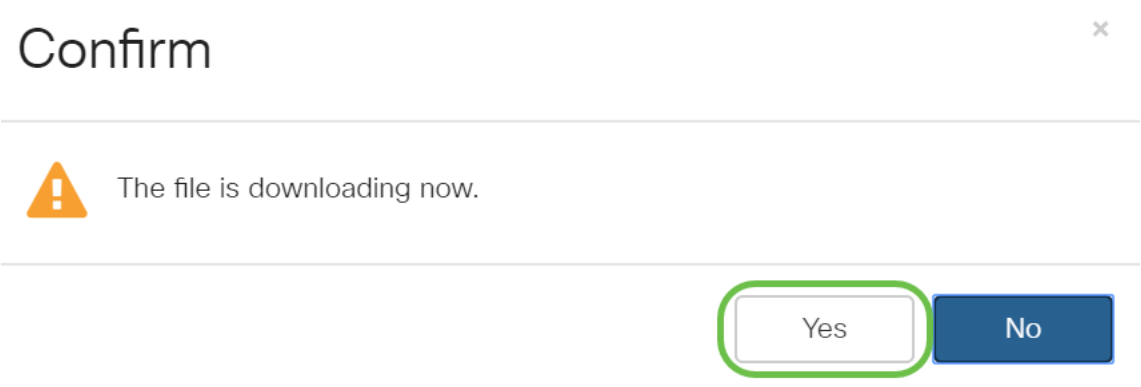


資料包捕獲檔案將儲存在AP中，直到您重新啟動AP。

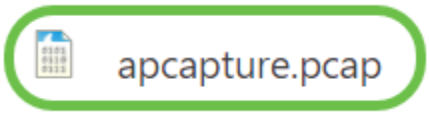
步驟5.按一下**Download to this Device**圖示下載最近擷取的檔案。



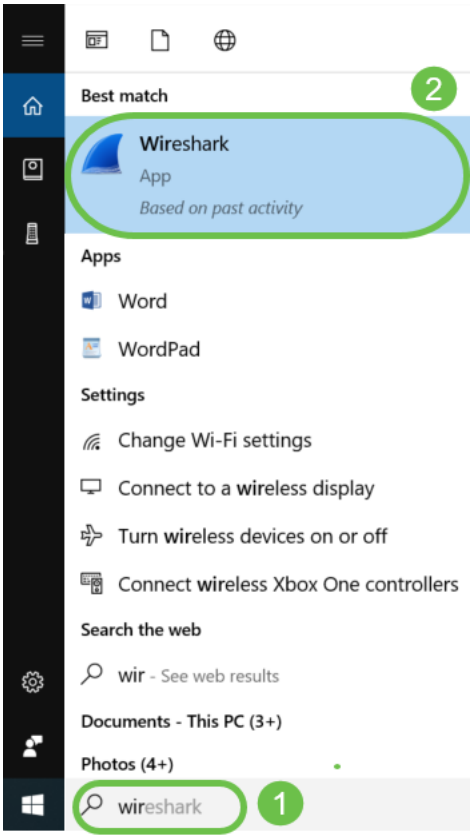
步驟6.將開啟*Confirm*彈出視窗以確認檔案下載，然後按一下**Yes**。



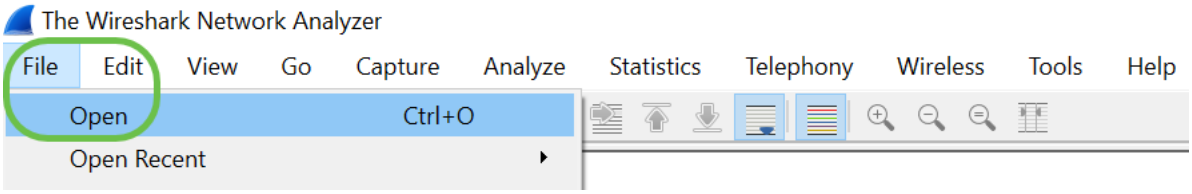
步驟7.資料包捕獲檔案將下載到您的電腦。在本示例中，*apcapture.pcap*是檔案的名稱。



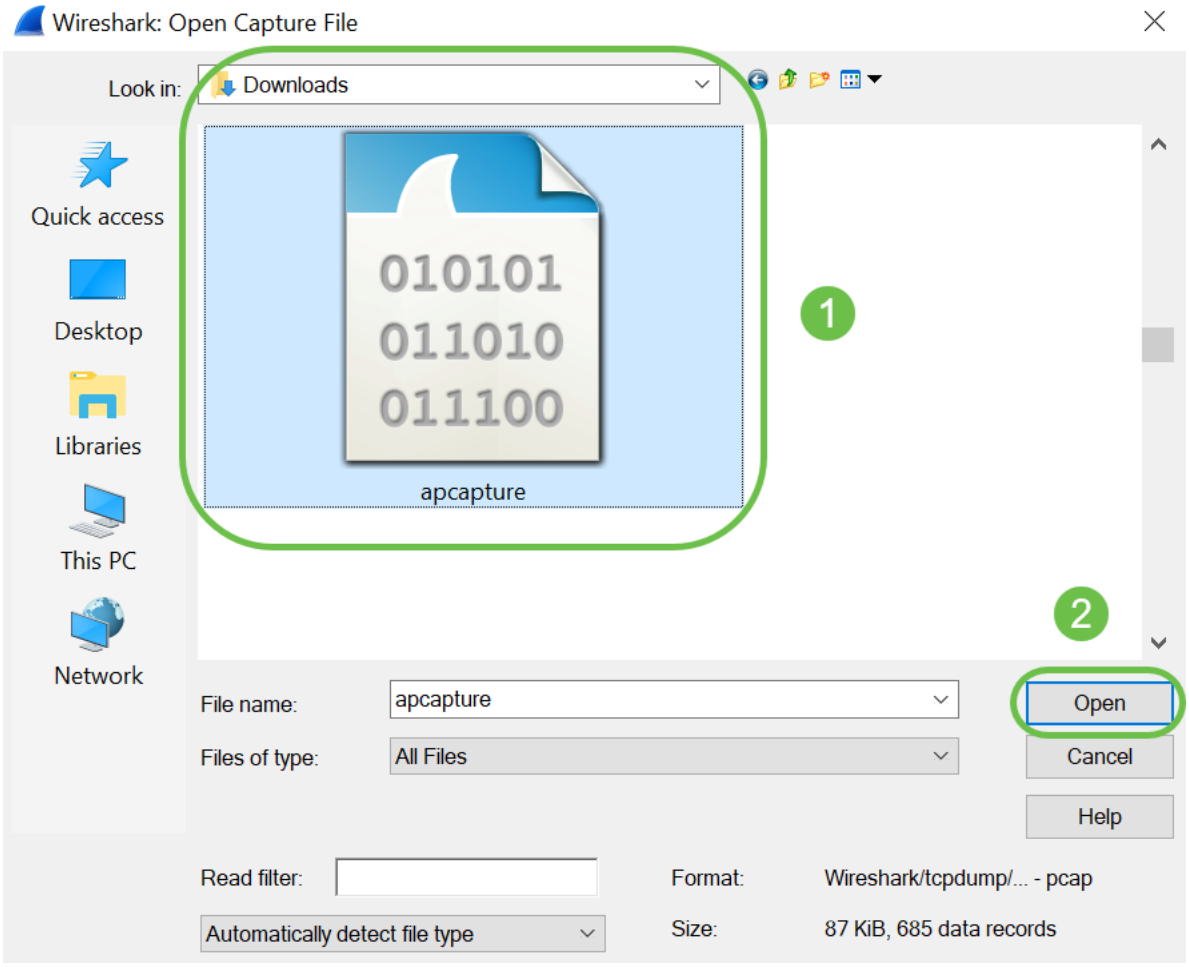
步驟8.由於Wireshark已下載，因此可以通過在Microsoft Windows的搜尋欄中鍵入*Wireshark*並選擇應用程式作為選項來訪問它。



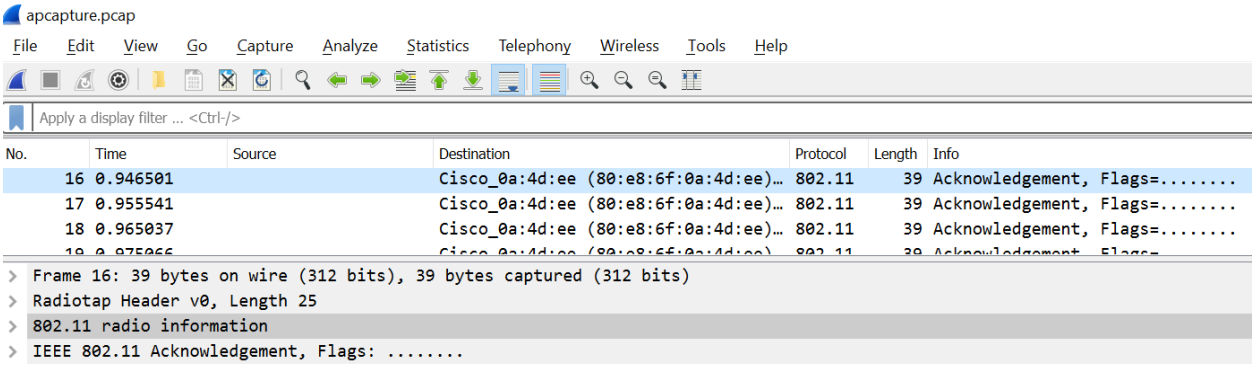
步驟9.導覽至**File > Open**。



步驟10.在新快顯視窗上，瀏覽以找到檔案(在本案例中為*apcapture.pcap*)。按一下「**Open**」。



步驟11。檔案將會在*Wireshark*應用程式上開啟，您會看到封包的詳細資訊。



結論

您的資料包已捕獲並上傳到Wireshark，現在您可以開始分析它。不知道從這裡往哪裡走？網上有大量的影片和文章可供探索。您搜尋的內容取決於您的具體情況。你有這個！