在思科业务WAP上使用Wireshark进行数据包分析：上载文件

目标

本文介绍如何使用思科业务无线接入点(WAP)和Wireshark执行、保存和上传数据包捕获。

简介

配置更改、监控和故障排除是网络管理员必须经常处理的问题。使用简单的工具非常宝贵！本文的目标是更轻松地了解数据包捕获的基本信息以及如何将文件上传到Wireshark。如果您不熟悉此流程，让我们回答您可能已经提出的一些问题。

首先，Wireshark是一款免费的数据包分析器，适用于任何想要排除网络故障的人。Wireshark提供了许多捕获选项，以及按多个不同参数对流量进行分类。转到Wireshark，了解此开源选项的详细信息。

什么是数据包捕获？

数据包捕获（也称为PCAP文件）是有助于排除故障的工具。它可以实时记录网络中设备之间发送的每个数据包。通过捕获数据包，您可以深入了解网络流量的详细信息，其中可能包括从设备发现、协议会话和失败的身份验证等所有内容。您可以看到特定流量的路径以及所选网络上设备之间的每次交互。可根据需要保存这些数据包以进行进一步分析。它就像通过数据包传输来检查网络内部运作的X光。

可以捕获哪些类型的数据包？

WAP设备可以捕获以下类型的数据包：

·在无线电接口上接收和传输的802.11个数据包。在无线电接口上捕获的数据包包括802.11报头。

·在以太网接口上接收和传输的802.3数据包。

·在内部逻辑接口(如虚拟接入点(VAP)和无线分布系统(WDS)接口)上接收和传输的802.3数据包。

数据包捕获的方式是什么？

有两种数据包捕获方法可用：

1. *远程捕获方法* — 捕获的数据包会实时重定向到运行Wireshark的外部计算机。可以选择

*Stream to a Remote Host*以选择远程捕获方法。如果您更喜欢远程捕获方法，请选中**在WAP上使用Wireshark进行数据包分析：直接流到Wireshark**。

2. *本地捕获方法* — 捕获的数据包存储在WAP设备上的文件中。WAP设备可以将文件传输到简单文件传输协议(TFTP)服务器。文件采用PCAP格式，可以使用Wireshark进行检查。可以选择"*在此设备上保存*文件"以选择本地捕获方法。

本文的重点是将文件上传到Wireshark，其中包含最新的图形用户界面(GUI)。 如果您喜欢查看使用旧GUI进行本地捕获方法的文章，请选中**配置数据包捕获以优化无线接入点的性能**。

拥有PCAP文件后，如何处理数据包捕获？

无线分组捕获功能可捕获和存储由WAP设备接收和传输的分组。然后，网络协议分析器可以分析捕获的数据包，以便进行故障排除或性能优化。有许多第三方数据包分析器应用程序可在线使用。在本文中，我们重点介绍Wireshark。

思科不拥有或支持Wireshark。如需支持，请与 Wireshark联系。

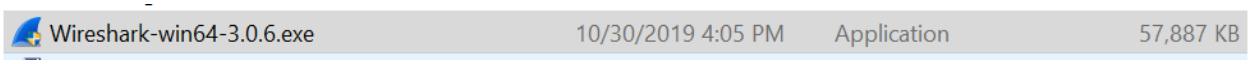
设备 |软件版本

- 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

下载Wireshark

步骤1.转到Wireshark网站。单击 **Download**。选择要下载的适当版本。您将在屏幕左下角看到下载进度。

步骤2.转到计算*机*上的"下载"并选择Wireshark文件以安装其应用程序。



登录WAP

在Web浏览器中，输入WAP的IP地址。输入您的凭证。如果这是您首次访问此设备或您执行了出厂重置，则默认用户名和密码为*cisco*。如果需要有关如何登录的说明，可以按照**访问无线接入点(WAP)的基于Web的实用程序(Access the Web-based Utility)一文中的步骤**操作。

在PC上保存数据包捕获并上传到Wireshark

步骤1.导航至Troubleshoot **> Packet Capture**。

确保为**数据包捕获方法选**择“在此设备*上保存文件*”。

配置以下参数：

·*接口* — 输入数据包捕获的捕获接口类型：

·*以太网* — 以太网端口上的802.3流量。

·*无线电1(5 GHz)/无线电2(2.4 GHz)* — 无线电接口上的802.11流量。

·*持续时间* — 输入捕获的时间持续时间（以秒为单位）。范围从 10 至 3600。默认值为 60。

·*最大文件大小* — 输入捕获文件允许的最大大小(以千字节(KB)为单位)。 范围从 64 至 4096。默认值为 1024。

数据包捕获有两种模式。

·*所有无线流量* — 捕获所有无线数据包。

·*进出此AP的流量* — 捕获从AP发送或AP接收的数据包。

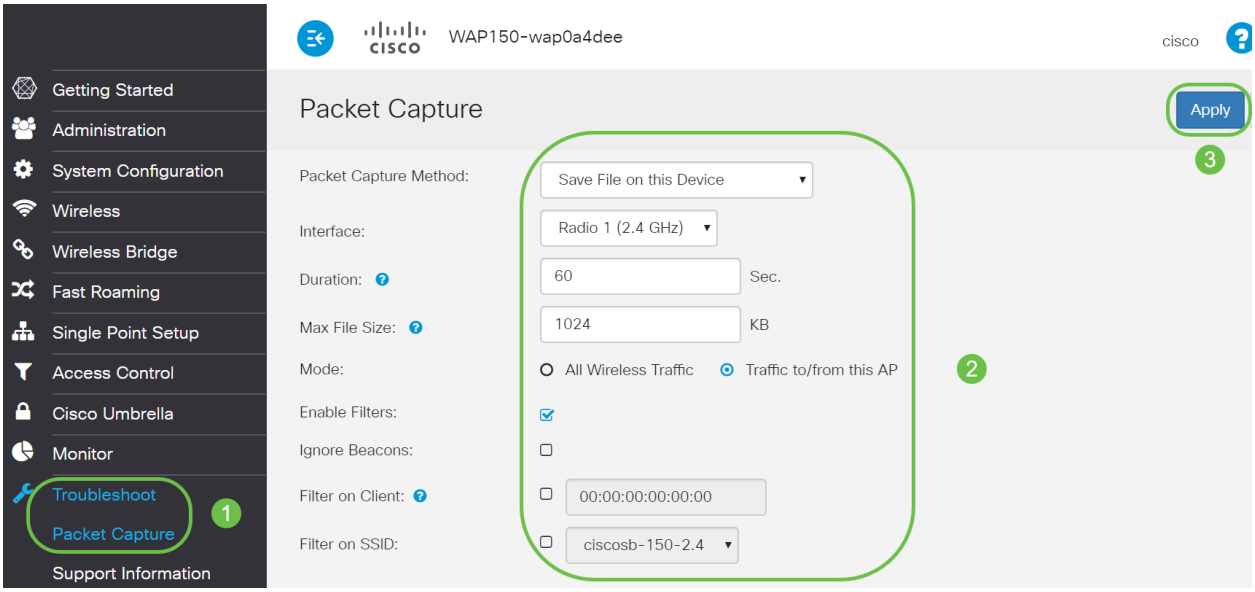
单击“**Enable Filters(启用过滤器)**”。有三个复选框可用：*忽略信标*、*客户端过滤*器和*SSID过滤器*。

·*忽略信标* — 启用或禁用捕获无线电检测或传输的802.11信标。信标帧是传送有关网络信息的广播帧。信标的目的是通告现有无线网络。如果不查找此类型的流量，可以选择忽略信标。

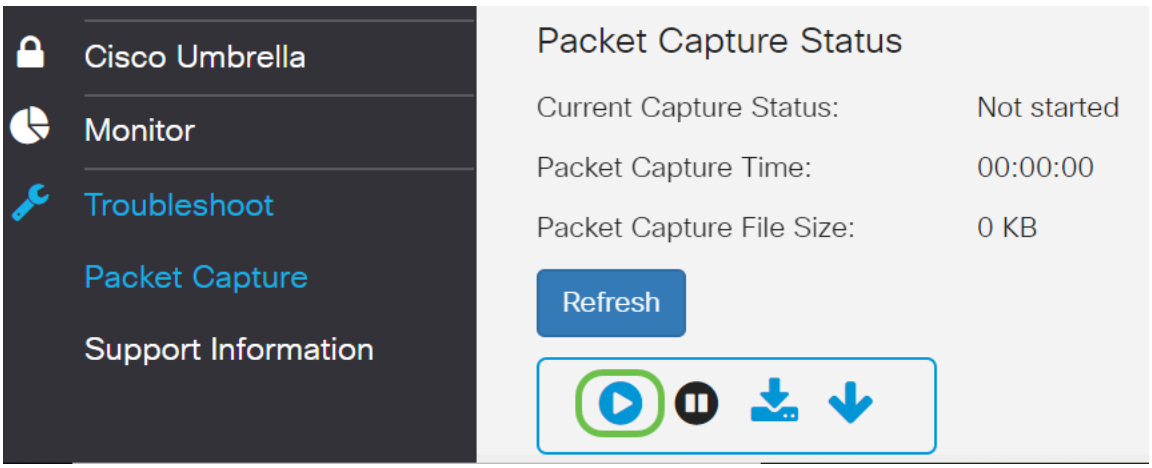
·*Filter on Client* — 指定WLAN客户端过滤器的MAC地址。请注意，仅当在802.11接口上执行捕获时，客户端过滤器才处于活动状态。

·*SSID过滤器* — 为数据包捕获选择SSID名称。

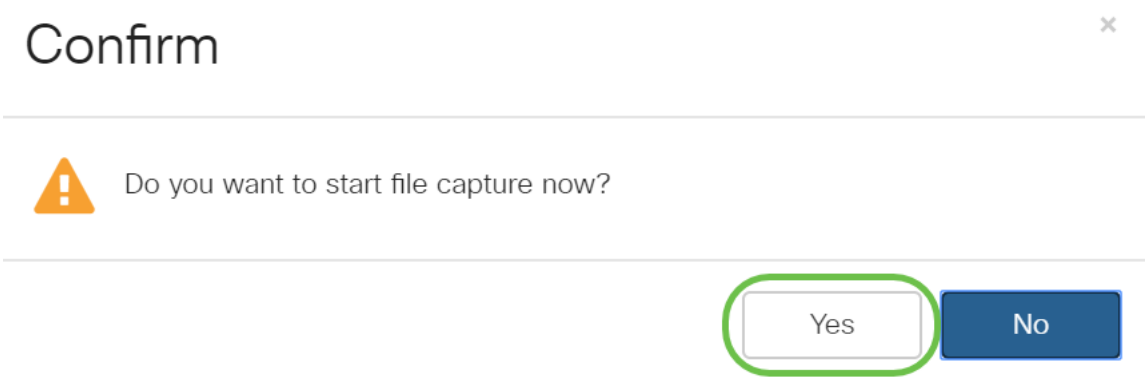
单击**Apply**保存到“Startup Configuration”。



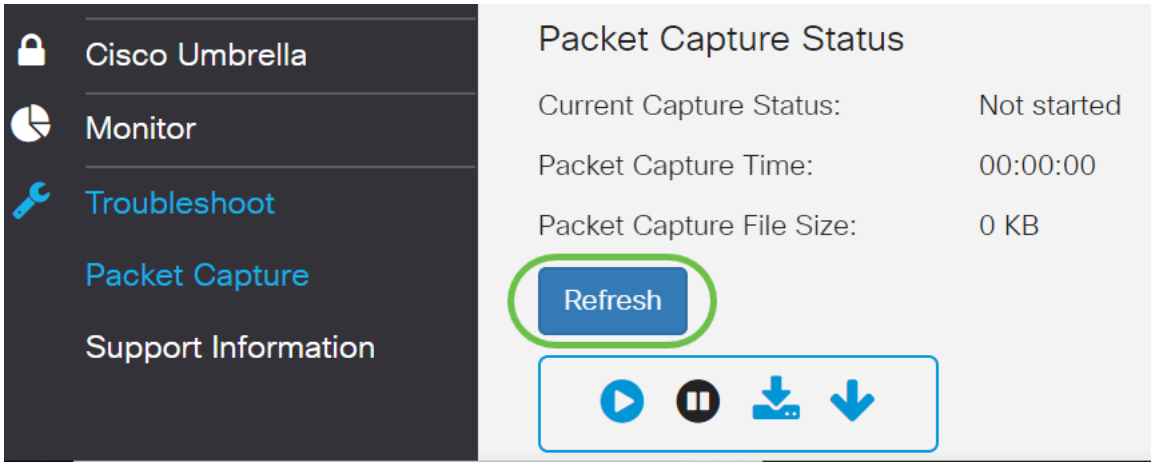
步骤2.单击“开始**捕获**”图标。



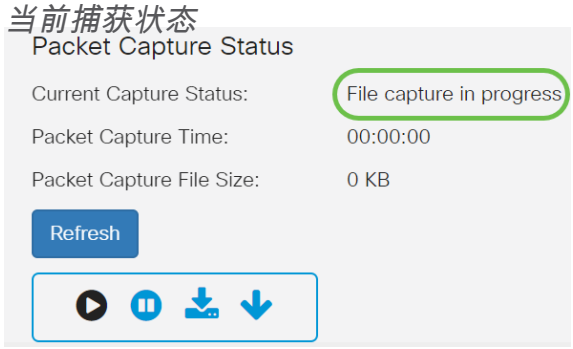
步骤3.将打*开*“确认”弹出窗口以获取下载文件的确认，单击“**是**”开始下载文件。



步骤4.单击“**刷新**”以获*取包含以*下数据的数据包捕获状态：

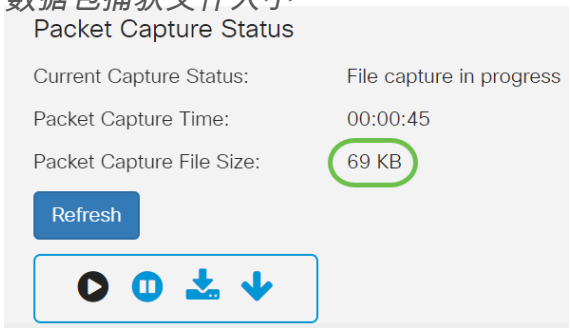


1. *当前捕获状态*

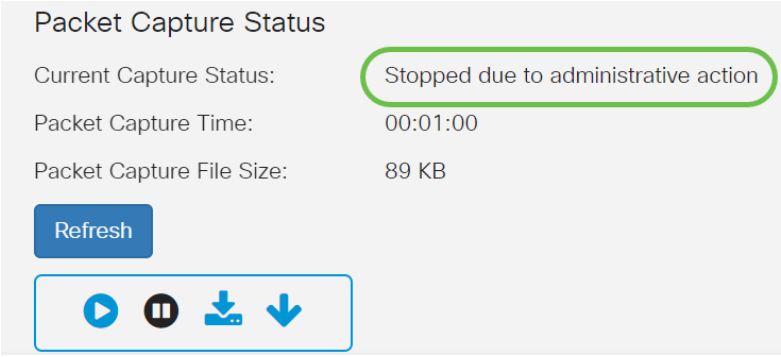


2. *数据包捕获时间*

3. *数据包捕获文件大小*

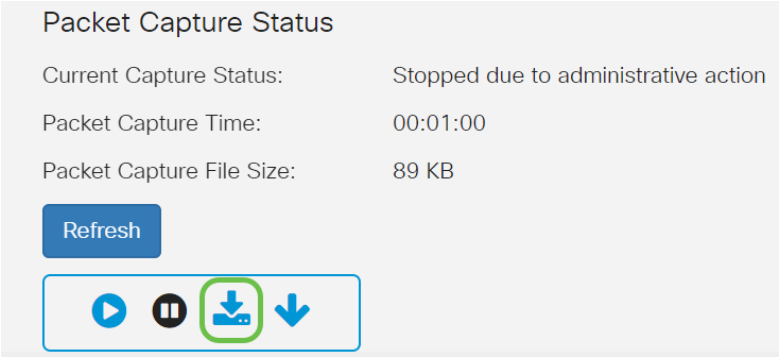


4. 在数*据包文件捕*获模式下，WAP设备将捕获的数据包存储在随机访问内存(RAM)文件系统中。激活后，数据包捕获将继续，直到发生以下事件之一：
·捕获时间达到配置的持续时间。
·捕获文件达到其最大大小。
·管理员停止捕获。

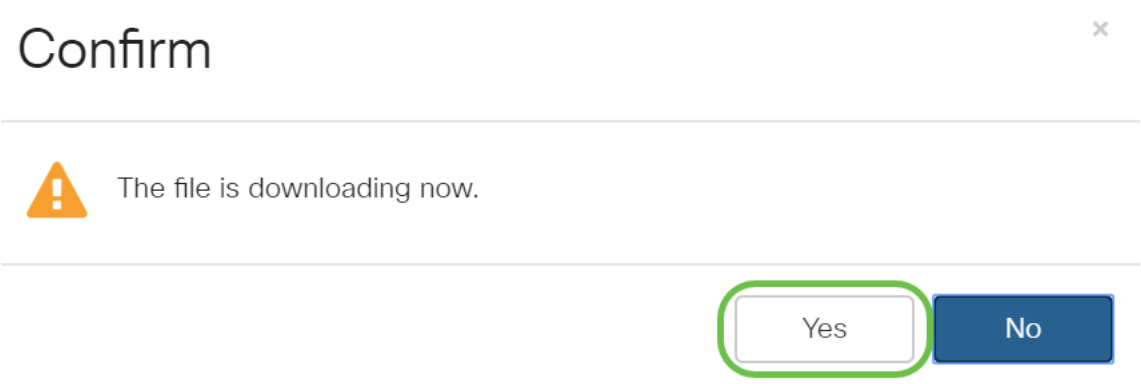


数据包捕获文件将存储在AP中，直到您重新启动AP。

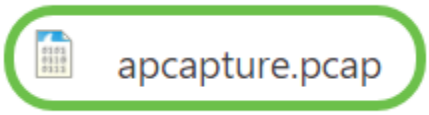
步骤5.单击“下载到**此设备”图**标下载最近捕获的文件。



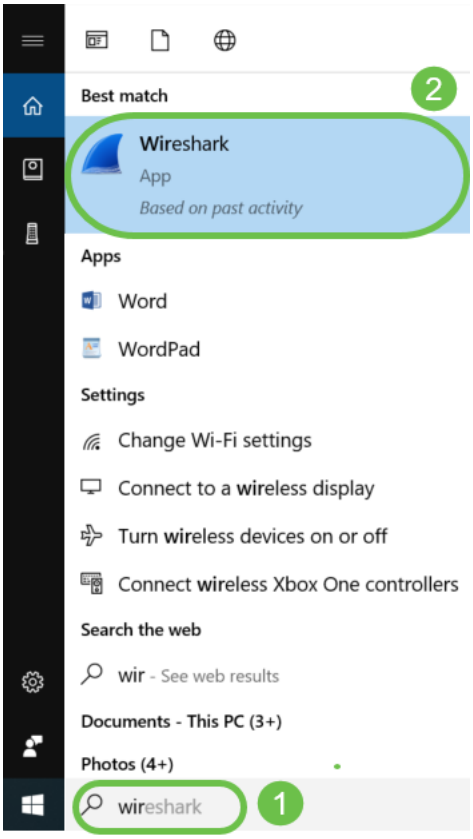
步骤6.将打*开*“确认”弹出窗口以确认文件下载，单击“**是”**。



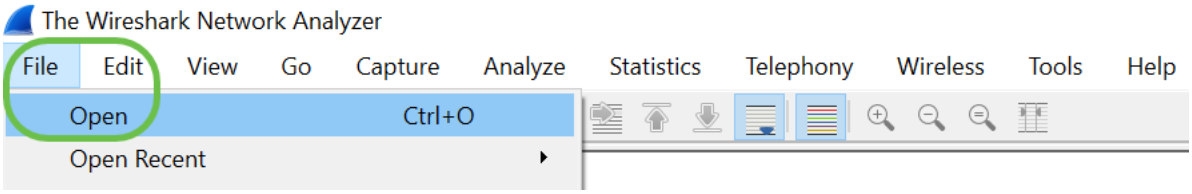
步骤7.数据包捕获文件将下载到您的计算机。在本示例中，*apcapture.pcap*是文件的名称。



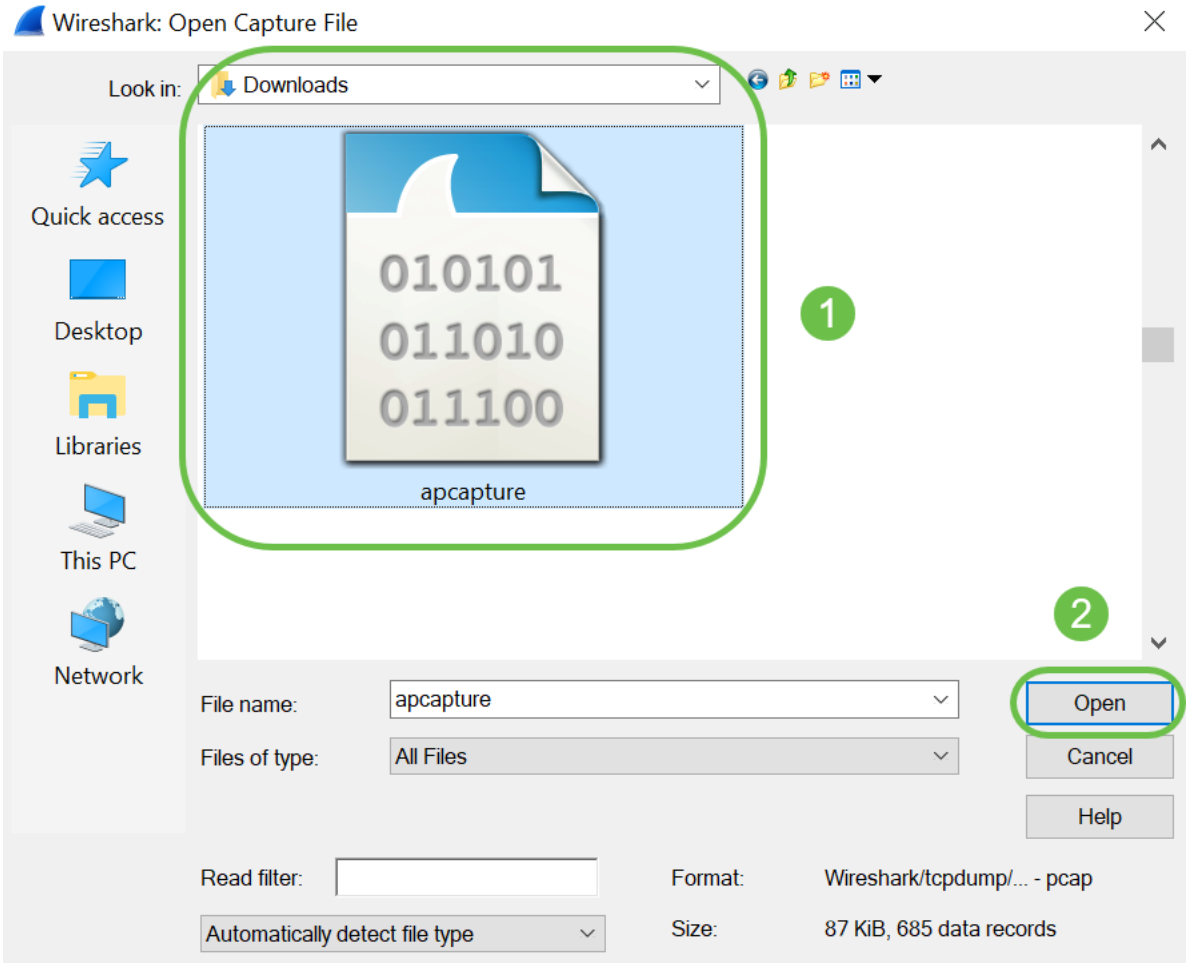
步骤8.由于Wireshark已下载，因此可以在Microsoft Windows的搜索栏中键入*Wireshark*，然后选择应用程序（当它是选项时）来访问它。



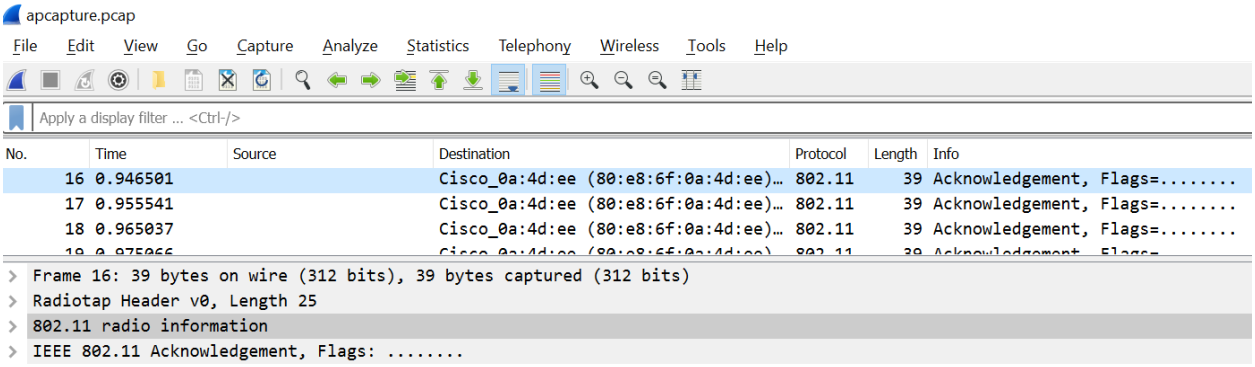
步骤9.导航至“文件”**>“打开”**。



步骤10.在新的弹出窗口上，浏览以查找文件(在本例中为*apcapture.pcap*)。单击 **Open**（打开）。



步骤11.文件将在Wireshark应用程序上打开，您将能够查看数据包的详细信息。



结论

您的数据包已捕获并上传到Wireshark，现在可以开始分析它了。不确定该从这里去哪里？有大量视频和文章可供在线浏览。您搜索的内容取决于您的情况需求。你有这个！