패킷 분석을 위해 Cisco Business WAP에서 Wireshark 사용:파일 업로드

목표

이 문서에서는 Cisco WAP(Business Wireless Access Point) 및 Wireshark를 사용하여 패킷 캡처를 수행, 저장 및 업로드하는 방법에 대해 설명합니다.

소개

구성 변경, 모니터링 및 문제 해결은 네트워크 관리자가 자주 처리해야 하는 작업입니다.간단한 툴을 사용하는 것은 매우 중요합니다!이 문서의 목적은 Wireshark에 파일을 업로드하는 방법과 패킷 캡처의 기본 사항을 보다 쉽게 이해하는 것입니다.이 프로세스에 익숙하지 않은 경우, 이미 알고 계실 수 있는 몇 가지 질문에 답변해 드리겠습니다.

우선, Wireshark는 네트워크 문제를 해결하려는 모든 사용자를 위한 무료 패킷 분석기입니다.Wireshark는 캡처를 위한 다양한 옵션을 제공할 뿐만 아니라 여러 가지 매개 변수를 기준으로 트래픽을 정렬합니다.Wireshark로 이동하여 이 오픈 소스 옵션에 대한 자세한 내용을 확인하십시오.

패킷 캡처란 무엇입니까?

PCAP 파일이라고도 하는 패킷 캡처는 문제 해결에 도움이 될 수 있는 도구입니다.네트워크의 디바이스 간에 전송되는 모든 패킷을 실시간으로 기록할 수 있습니다.패킷을 캡처하면 디바이스 검색, 프로토콜 대화 및 실패한 인증에서 모든 것을 포함할 수 있는 네트워크 트래픽의 세부 정보를 분석할 수 있습니다.특정 트래픽 흐름의 경로와 선택한 네트워크의 디바이스 간 모든 상호 작용을 확인할 수 있습니다.필요에 따라 추가 분석을 위해 이러한 패킷을 저장할 수 있습니다.패킷 전송을 통해 네트워크 내부 작업을 X-ray로 수행하는 것과 같습니다.

캡처할 수 있는 패킷 유형은 무엇입니까?

WAP 디바이스는 다음 유형의 패킷을 캡처할 수 있습니다.

·무선 인터페이스에서 수신 및 전송된 802.11 패킷무선 인터페이스에서 캡처된 패킷에는 802.11 헤더가 포함됩니다.

·이더넷 인터페이스에서 수신 및 전송된 802.3 패킷

·VAP(Virtual Access Point) 및 WDS(Wireless Distribution System) 인터페이스와 같은 내부 논리적 인터페이스에서 수신 및 전송된 802.3 패킷

패킷 캡처를 수행하는 방법은 무엇입니까?

두 가지 패킷 캡처 방법이 있습니다.

1. *원격 캡처 방법* - 캡처된 패킷은 Wireshark를 실행하는 외부 컴퓨터로 실시간으로 리디렉션됩니다.*Stream to a Remote Host(원격 호스트로 스트림)*를 선택하여 원격 캡처 방법을 선택할 수 있습니다.원격 캡처 방법을 선호하는 경우 Using Wireshark on **a WAP for Packet Analysis:Wireshark로 직접 스트리밍합니다**.
2. *로컬 캡처 방법* - 캡처된 패킷은 WAP 디바이스의 파일에 저장됩니다.WAP 디바이스는 파일을 TFTP(Trivial File Transfer Protocol) 서버로 전송할 수 있습니다.파일은 PCAP 형식으로 포맷되어 있으며 Wireshark를 사용하여 검사할 수 있습니다.*이 장치에 파일 저장*을 선택하여 로컬 캡처 방법을 선택할 수 있습니다.

이 문서에서는 최신 GUI(Graphical User Interface)가 포함된 Wireshark에 파일을 업로드하는 데 중점을 둡니다. 로컬 캡처 방법에 이전 GUI를 사용하는 문서를 보려면 **무선 액세스 포인트에서 성능을 최적화하기 위해 패킷 캡처 구성 을** 체크 **아웃합니다**.

PCAP 파일이 있으면 패킷 캡처를 어떻게 해야 합니까?

무선 패킷 캡처 기능을 사용하면 WAP 디바이스에서 수신하여 전송된 패킷을 캡처하고 저장할 수 있습니다.그런 다음 네트워크 프로토콜 분석기가 캡처된 패킷을 분석하여 문제 해결 또는 성능 최적화를 수행할 수 있습니다.온라인으로 제공되는 타사 패킷 분석기 애플리케이션이 많습니다.이 기사에서 우리는 Wireshark에 초점을 맞춥니다.

Wireshark는 Cisco에서 소유하거나 지원하지 않습니다.지원이 필요한 경우 Wireshark **에게 문의하십시오**.

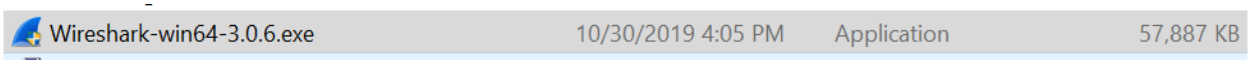
장치 | 소프트웨어 버전

- 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 다운로드

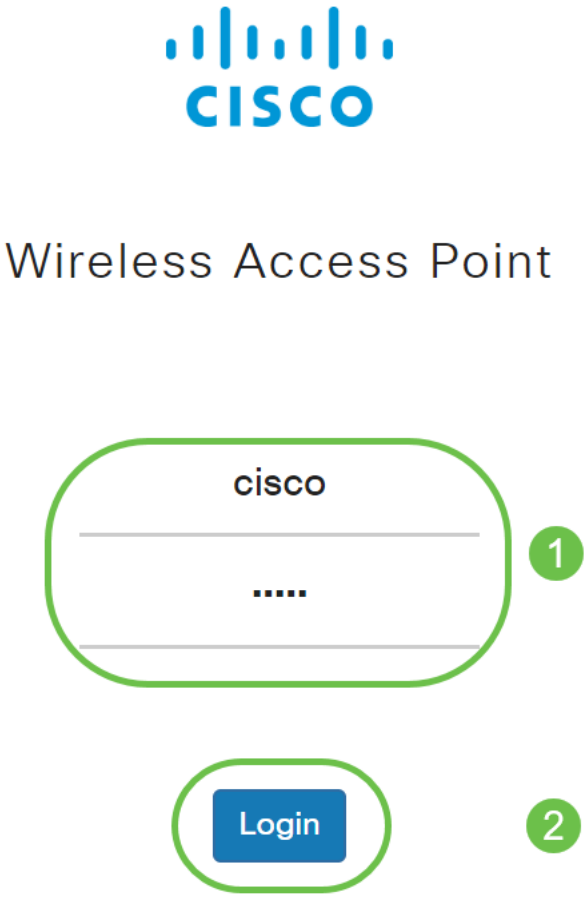
1단계. Wireshark 웹 사이트**로** 이동합니다.Download(다운로드)를 클릭합니다.다운로드할 적절한 버전을 선택합니다.화면 왼쪽 하단에서 다운로드 진행 상황을 확인할 수 있습니다.

2단계. 컴퓨터의 *다운로드*로 이동하여 Wireshark 파일을 선택하여 응용 프로그램을 설치합니다.



WAP에 로그인

웹 브라우저에서 WAP의 IP 주소를 입력합니다.자격 증명을 입력합니다.이 디바이스에 처음 액세스하거나 공장 재설정을 수행한 경우 기본 사용자 이름과 비밀번호는 *cisco*입니다.로그인 방법에 대한 지침이 필요한 경우 WAP(Wireless Access Point) 기사의 웹 기반 유틸리티 액세스 단계를 따를 수 있습니다.



PC에 패킷 캡처 저장 및 Wireshark에 업로드

1단계. Troubleshoot(문제 해결) **> Packet Capture(패킷 캡처)로 이동합니다**.

Packet *Capture Method(패킷 캡처 방법)*에 대해 **Save File on this Device(이 디바이스의 파일 저장)**가 선택되었는지 *확인합니다*.

다음 매개변수를 구성합니다.

·Interface - 패킷 캡처를 위한 캡처 인터페이스 유형을 입력합니다.

·*이더넷* - 이더넷 포트의 802.3 트래픽

·*무선 1(5GHz) / 무선 2(2.4GHz)* - 무선 인터페이스의 802.11 트래픽

·Duration(기간) - 캡처의 시간 기간을 초 단위로 입력합니다.범위는 10~3600입니다.기본값은 60입니다.

·*Max File Size*(최대 파일 크기) - 캡처 파일의 최대 허용 크기(KB)를 입력합니다. 범위는 64~4096입니다.기본값은 1024입니다.

패킷 캡처에는 두 가지 모드가 있습니다.

·*모든 무선 트래픽* - 모든 무선 패킷을 캡처합니다.

·*Traffic to/from this AP* - AP에서 전송되거나 AP에서 수신한 패킷을 캡처합니다.

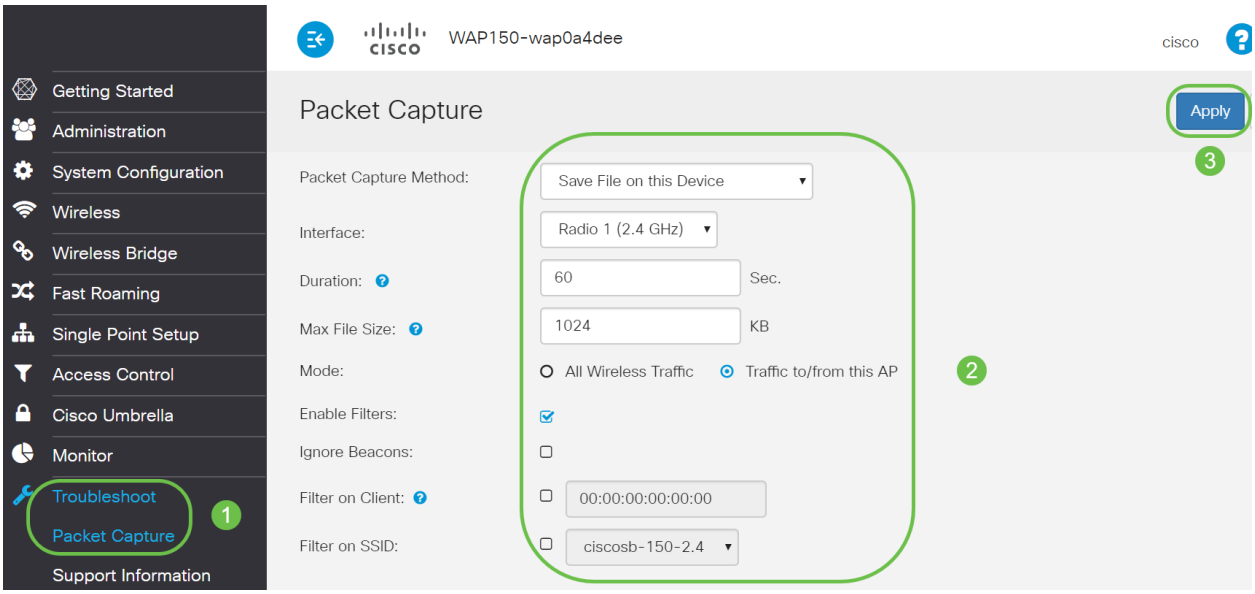
Enable **Filters를 클릭합니다**.사용 가능한 세 가지 확인란은 Ignore Beacons(신호 *무시*), *Filter on Client(클라이언트의 필터)*, SSID*의 Filter(필터)입니다*.

·*신호* 무시 - 무선이 탐지하거나 전송하는 802.11 신호의 캡처를 활성화하거나 비활성화합니다.비컨 프레임은 네트워크에 대한 정보를 전달하는 브로드캐스트 프레임입니다.신호의 목적은 기존 무선 네트워크를 광고하는 것입니다.이 유형의 트래픽을 찾지 않을 경우 신호 무시를 선택할 수 있습니다.

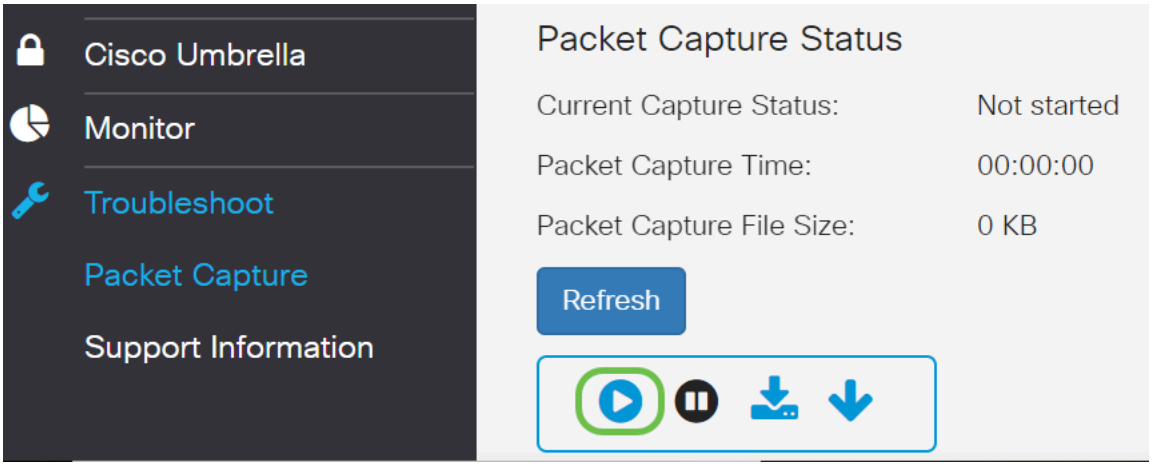
·*Filter on Client* - WLAN 클라이언트 필터의 MAC 주소를 지정합니다.클라이언트 필터는 802.11 인터페이스에서 캡처를 수행할 때만 활성화됩니다.

·*SSID*에서 필터 - 패킷 캡처를 위한 SSID 이름을 선택합니다.

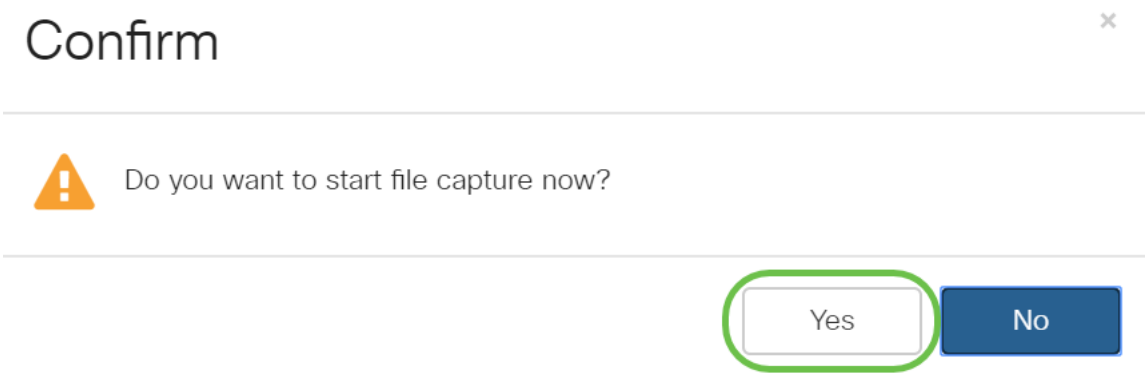
Apply(**적용**)를 클릭하여 Startup Configuration(시작 컨피그레이션)에 저장합니다.



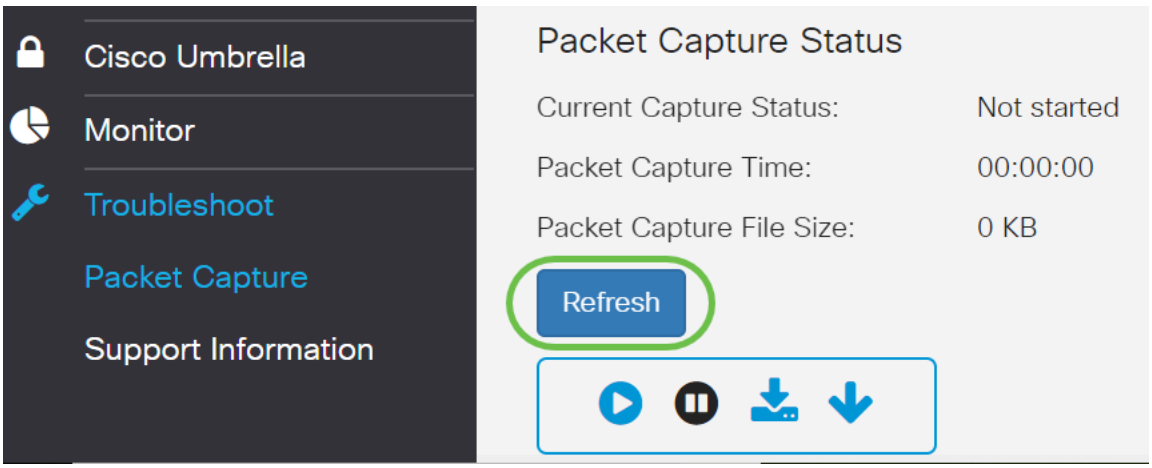
2단계. **캡처 시작** 아이콘**을** 누릅니다.



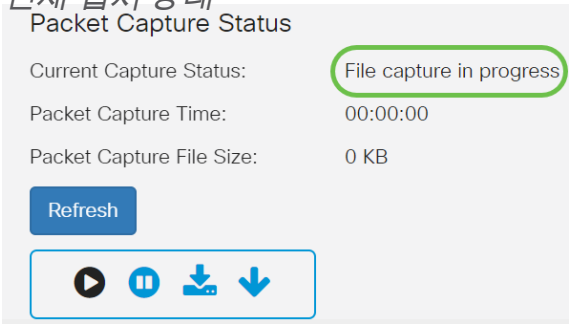
3단계. *확인* 팝업 창이 열리고 파일 다운로드에 대한 확인 메시지가 표시됩니다. **예**를 클릭하여 파일 다운로드를 시작합니다.



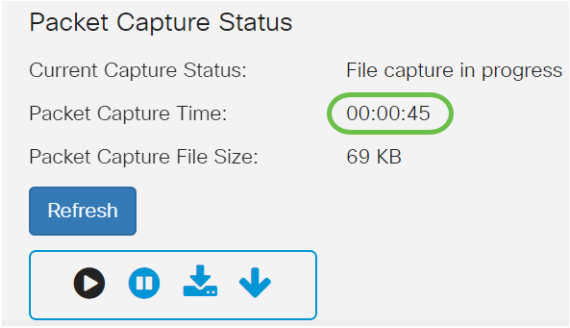
4단계. **Refresh**(새로 고침)를 클릭하여 다음 데이터가 포함된 *Packet Capture Status(패킷 캡처 상태)*를 가져옵니다.



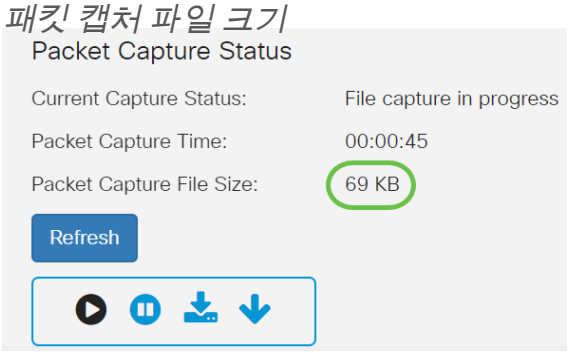
1. *현재 캡처 상태*



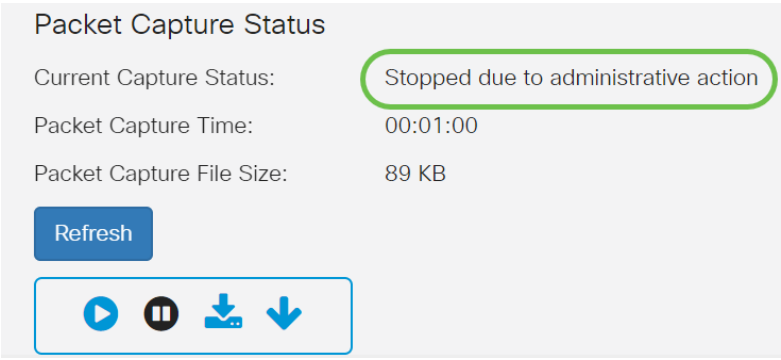
2. *패킷 캡처 시간*



3. *패킷 캡처 파일 크기*

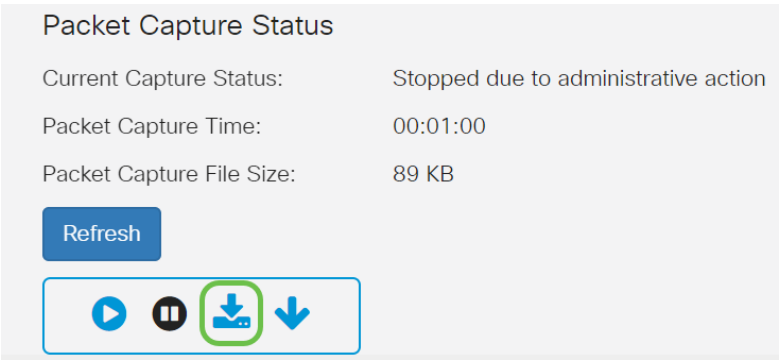


4. Packet *File Capture* 모드에서 WAP 디바이스는 캡처된 패킷을 RAM(Random Access Memory) 파일 시스템에 저장합니다.활성화 시 패킷 캡처는 다음 이벤트 중 하나가 발생할 때까지 진행됩니다.
   ·캡처 시간이 구성된 기간에 도달합니다.
   ·캡처 파일이 최대 크기에 도달했습니다.
   ·관리자가 캡처를 중지합니다.

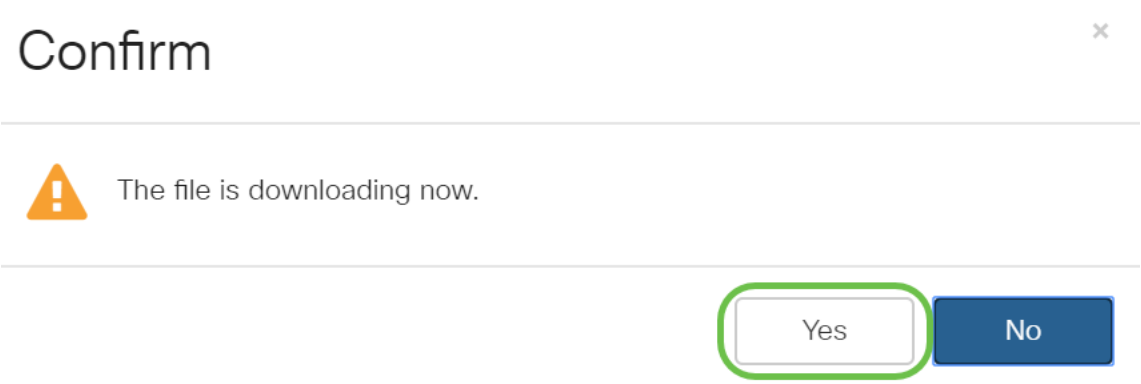


패킷 캡처 파일은 AP를 재부팅할 때까지 AP에 저장됩니다.

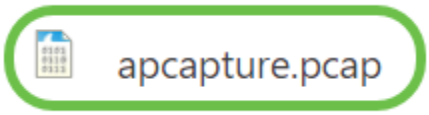
5단계. **Download to this Device(이 디바이스에 다운로드)** 아이콘을 클릭하여 최근에 캡처된 파일을 다운로드합니다.



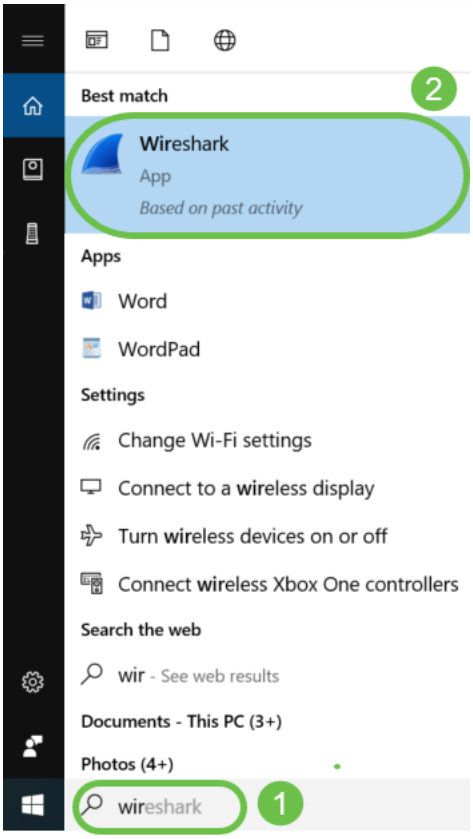
6단계. *확인* 팝업 창이 열리고 파일 다운로드가 확인되고 **예**를 클릭합니다.



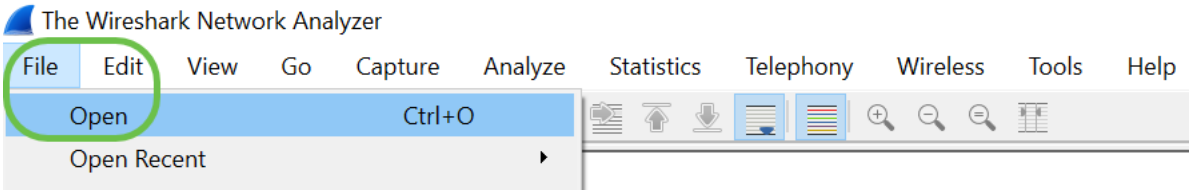
7단계. 패킷 캡처 파일이 컴퓨터에 다운로드됩니다.이 예에서 *apcapture.pcap*은 파일의 이름입니다.



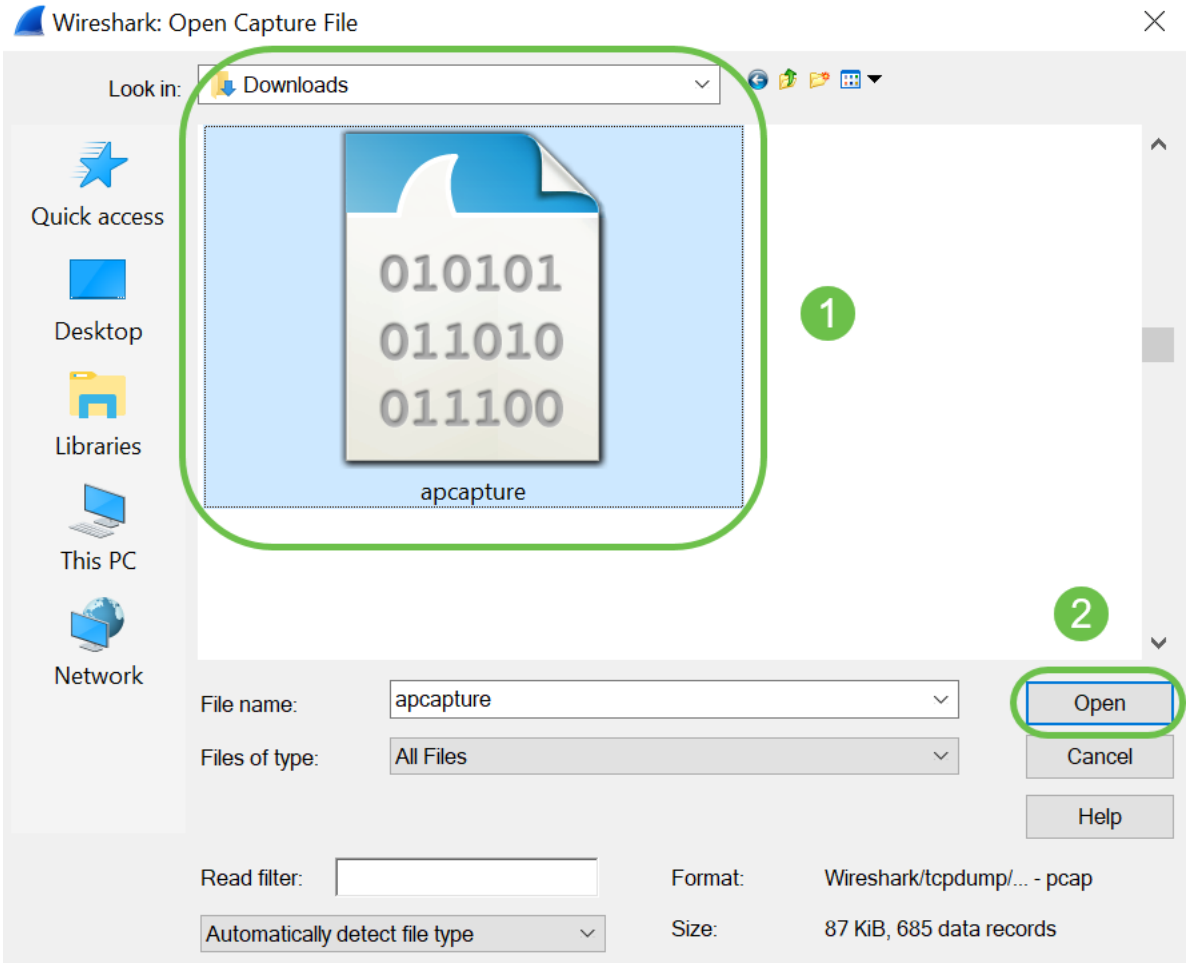
8단계. Wireshark는 이미 다운로드되었으므로 Microsoft Windows의 검색 표시줄*에 Wireshark*를 입력하고 응용 프로그램이 옵션일 때 선택하여 액세스할 수 있습니다.



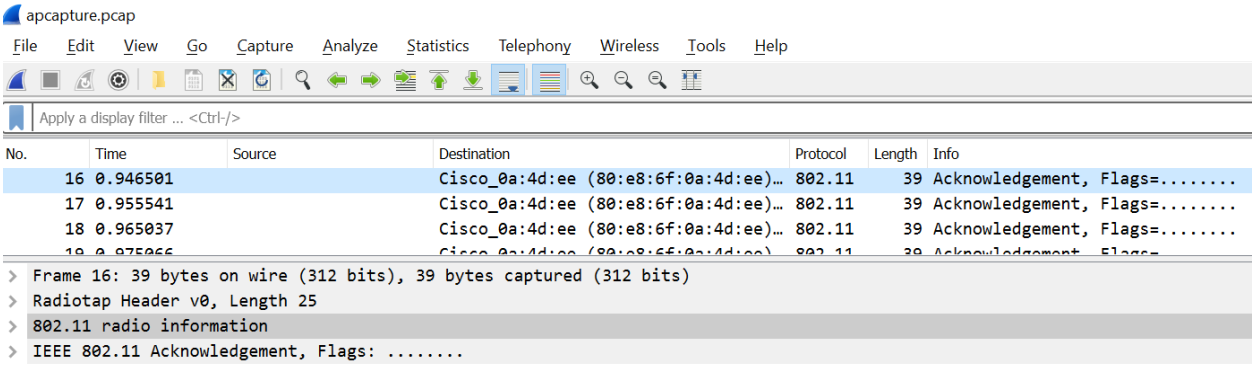
9단계. 파일 > **열기로 이동합니다**.



10단계. 새 팝업 창에서 파일을 찾습니다(이 경우 apcapture.pcap).**열기를 클릭합니다**.



11단계. Wireshark 애플리케이션에서 파일이 *열리고* 패킷의 세부 정보를 볼 수 있습니다.



결론

패킷을 캡처하여 Wireshark에 업로드한 경우 이제 분석을 수행할 수 있습니다.여기서 어디로 가야 할지 잘 모르겠나요?온라인으로 탐색할 수 있는 많은 비디오와 문서가 있습니다.검색하려는 내용은 상황에 따라 달라집니다.네가 알아서 해!