패킷 분석을 위해 Cisco Business WAP에서 Wireshark 사용:Wireshark로 직접 스트리밍

목표

이 문서에서는 Cisco WAP(Business Wireless Access Point)를 사용하여 네트워크 트래픽의 패킷 캡처를 수행하고 이를 Wireshark에 직접 스트리밍하는 방법에 대해 설명합니다.

목차

소개 및 FAQ

구성 변경, 모니터링 및 문제 해결은 네트워크 관리자가 자주 처리해야 하는 작업입니다.간단한 툴을 사용하는 것은 매우 중요합니다!이 문서의 목적은 패킷 캡처의 기본 사항과 Wireshark로 패킷을 스트리밍하는 방법을 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 무선으로 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

WAP에서 패킷 캡처를 수행하는 방법은 무엇입니까?

두 가지 패킷 캡처 방법이 있습니다.

1. *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.

최신 UI(Web User Interface)가 포함된 로컬 캡처 방법을 선호하는 경우 패킷 분석을 위한 WAP에서 Wireshark 사용:파일을 업로드합니다.

로컬 캡처 방법에 이전 GUI를 사용하는 문서를 보려면 무선 액세스 포인트에서 성능을 최적화하기 위해 패킷 캡처 구성 을 체크 아웃합니다.

2. *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.이 방법의 장점은 캡처할 수 있는 패킷의 볼륨에 제한이 없다는 것입니다.

이 문서의 핵심은 원격 호스트로 스트리밍하는 것이므로 원하는 경우 계속 읽어 보십시오!

패킷은 어디서 스트림합니까?

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.

일부 Cisco Business WAP 모델은 웹 기반 패킷 디코더 및 분석기 사이트인 CloudShark에 실시간으로 패킷을 전송할 수 있습니다.이는 서브스크립션과 함께 많은 추가 옵션을 포함하는 패킷 분석을 위한 Wireshark User Interface(UI)와 유사합니다.원격 캡처 방법을 선택하려면 Stream to CloudShark를 선택할 수 있습니다.자세한 내용을 보려면 다음 링크를 클릭하십시오.

- CloudShark(공식 웹 사이트)
- WAP125 또는 WAP581에서 패킷 분석을 위한 CloudShark 통합
- WAP571 및 WAP571E와 CloudShark 통합

Wireshark나 CloudShark는 모두 Cisco에서 소유하거나 지원하지 않습니다.데모 용도로만 포함되어 있습니다.지원이 필요한 경우 Wireshark 또는 CloudShark에 문의하십시오.

적용 가능한 장치 및 소프트웨어 버전

- WAP125 버전 1.0.2.0
- WAP150 버전 1.1.1.0
- WAP121 버전 1.0.6.8
- WAP361 버전 1.1.1.0
- WAP581 버전 1.0.2.0

- WAP571 버전 1.1.0.4
- WAP571E 버전 1.1.0.4

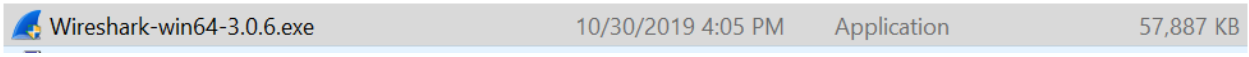
Wireshark 다운로드

1단계

Wireshark 웹 사이트로 이동합니다.적절한 버전을 선택합니다.Download(다운로드)를 클릭합니다.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.

원격 패킷 캡처 설명

Remote Packet Capture(원격 패킷 캡처) 기능을 사용하면 원격 포트를 패킷 캡처의 대상 포트로 지

정할 수 있습니다.이 기능은 Windows용 Wireshark 네트워크 분석기 도구와 함께 작동합니다.패킷 캡처 서버는 WAP 디바이스에서 실행되며 TCP(Transmission Control Protocol) 연결을 통해 캡처된 패킷을 Wireshark 툴에 전송합니다.

Wireshark 툴을 실행하는 Microsoft Windows 컴퓨터를 사용하면 캡처된 트래픽을 표시, 로깅 및 분석할 수 있습니다.원격 패킷 캡처 기능은 Windows용 Wireshark 툴의 표준 기능입니다.

Linux에서는 원격 패킷 캡처를 지원하지 않지만 Wireshark 툴은 Linux에서 작동하며 이미 생성된 캡처 파일을 볼 수 있습니다.

원격 캡처 모드를 사용 중인 경우 WAP 디바이스는 캡처된 데이터를 파일 시스템에 로컬로 저장하지 않습니다.

Wireshark가 설치된 컴퓨터와 WAP 디바이스 간에 방화벽이 설치된 경우 Wireshark가 컴퓨터의 방화벽 정책을 통과하도록 허용해야 합니다.또한 Wireshark 컴퓨터가 WAP 디바이스에 대한 TCP 연결을 시작할 수 있도록 방화벽을 구성해야 합니다.

Wireshark로 캡처 직접 스트리밍

Stream to a Remote Host 옵션을 사용하여 WAP 디바이스*에서* 원격 캡처를 시작하려면 아래 나열된 단계를 수행합니다.

1단계

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

패킷 *캡처 방법*:

1. 드롭다운 메뉴**에서 Stream to a Remote Host(원격 호스트로** 스트림)를 선택합니다.
2. *Remote Capture Port(원격 캡처 포트*) 필드에서 **2002**의 기본 포트를 사용하거나, 기본값 이외의 포트를 사용하는 경우 Wireshark를 WAP 디바이스에 연결하는 데 사용되는 원하는 포트 번호를 입력합니다.포트 범위는 1025~65530입니다.
3. 패킷 캡처 옵션에는 두 *가지 모드*가 있습니다.시나리오에 가장 적합한 항목을 선택합니다.

·*모든 무선 트래픽* - 무선 패킷을 모두 캡처합니다.

·*이 AP*에서 *오가는 트래픽* - 수신된 AP 또는 AP에서 전송된 패킷을 캡처합니다.

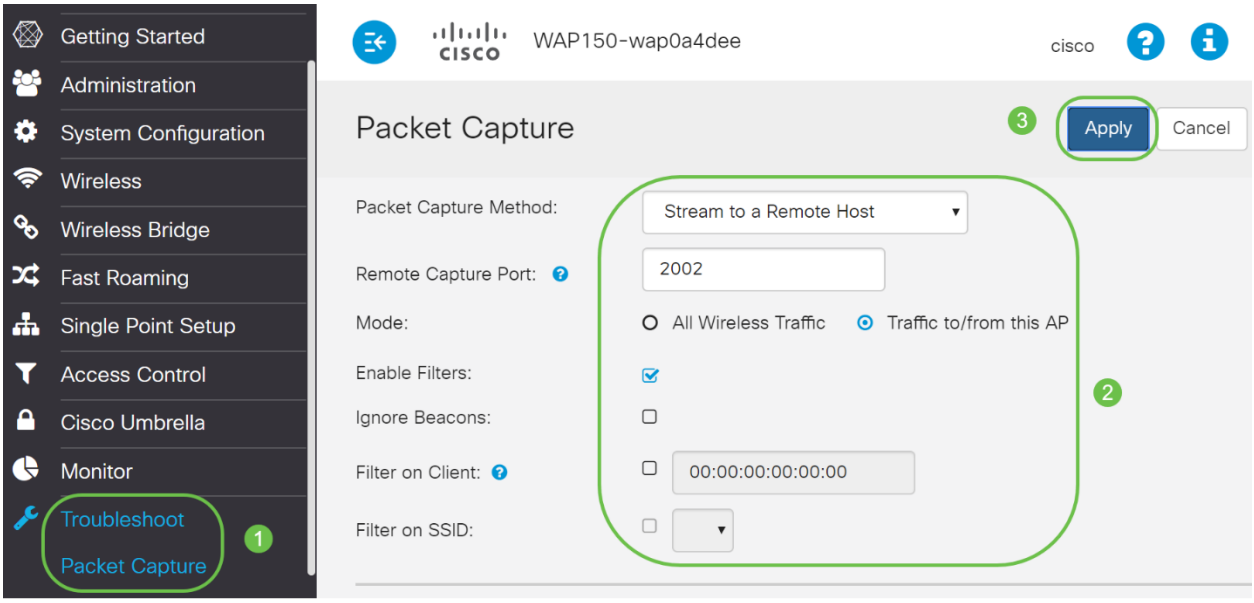
4. Enable **Filters(필터 활성화)를 선택합니다**.
5. 다음 옵션 중에서 선택합니다.

·*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.

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

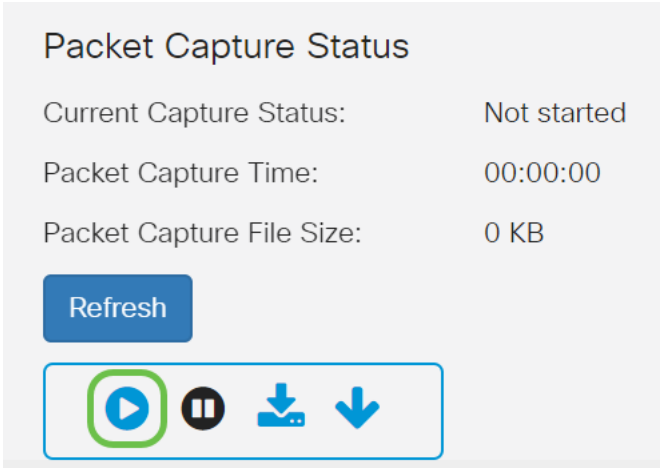
·*SSID*에서 필터 - 이 *Stream to a Remote Host* 옵션에 대해 이 *옵션이 회색으로* 표시됩니다.

6. **적용**을 클릭하여 설정을 저장합니다.



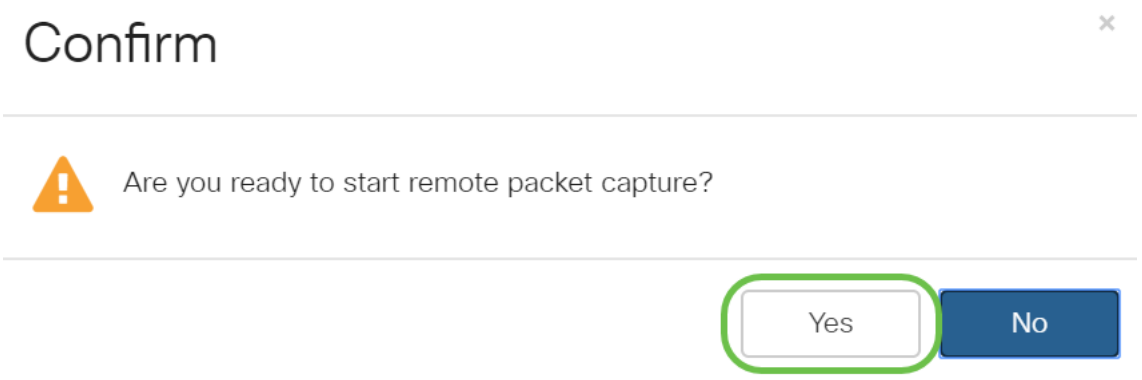
2단계

캡처 시작 아이콘을 클릭합니다.



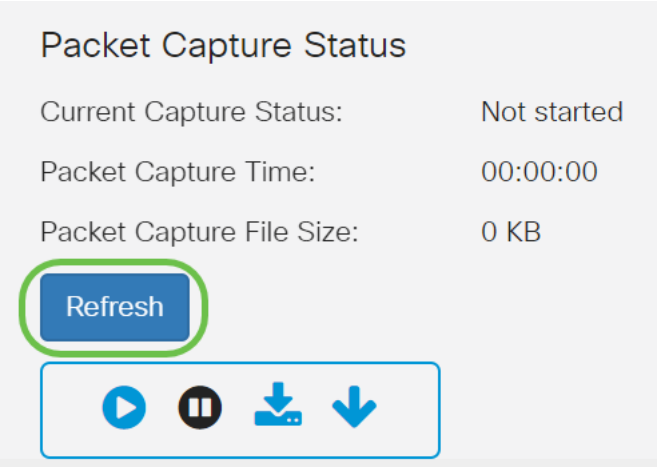
3단계

확인 팝업 창이 열립니다.Yes(**예**)를 클릭하여 캡처를 시작합니다.



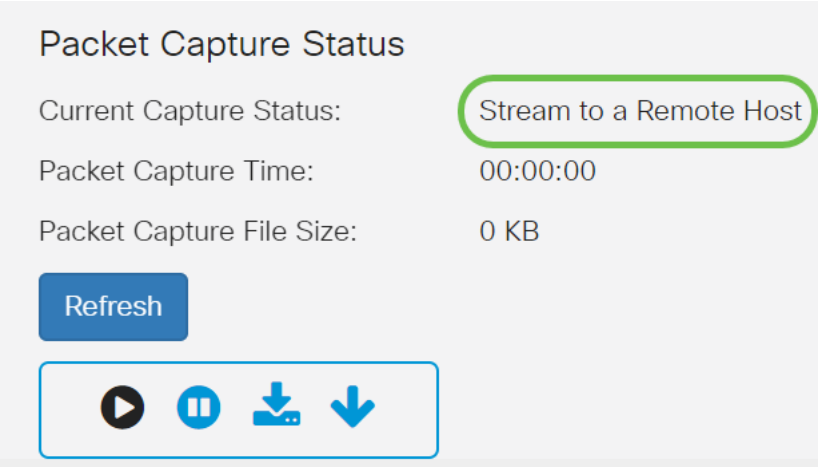
4단계

Refresh(새로 **고침**) 버튼을 클릭하여 현재 상태를 확인합니다.



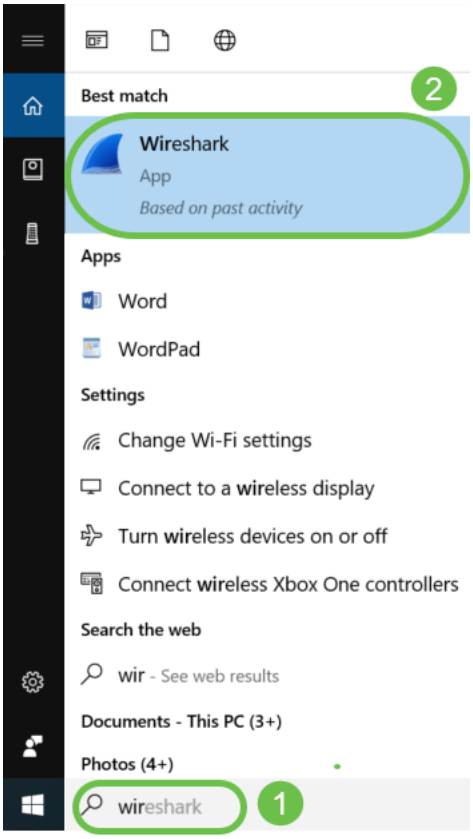
5단계

이제 에서 Current *Capture Status(현재 캡처 상태)*가 *Stream to a Remote Host(원격 호스트로 스트림)*가 될 *것임을 확인할 수 있습니다*.



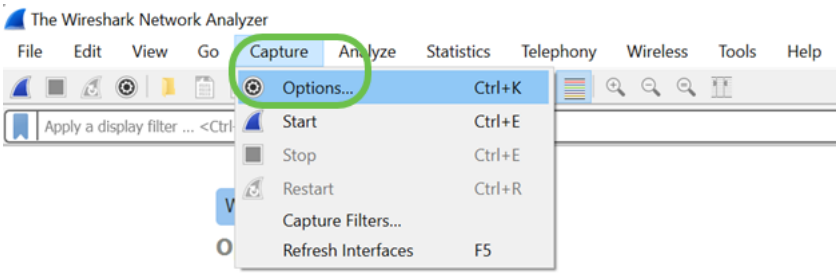
6단계

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



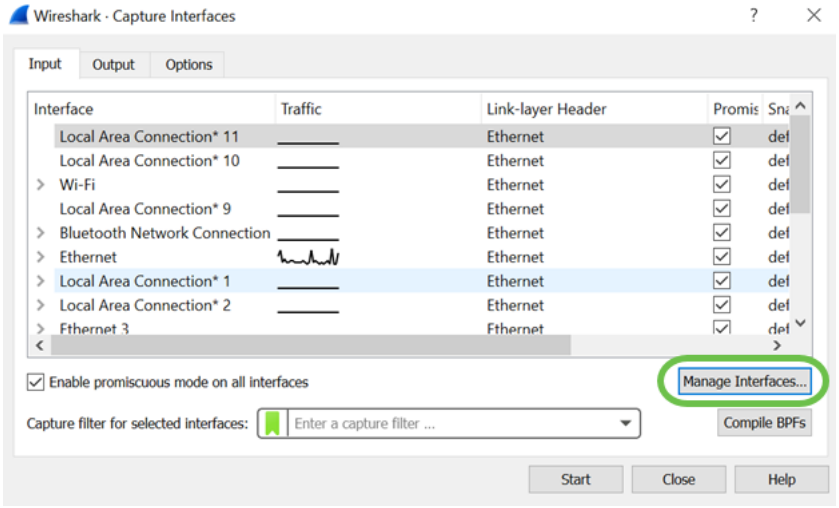
7단계

Capture(**캡처**) > Options(**옵션**)로 이동합니다.



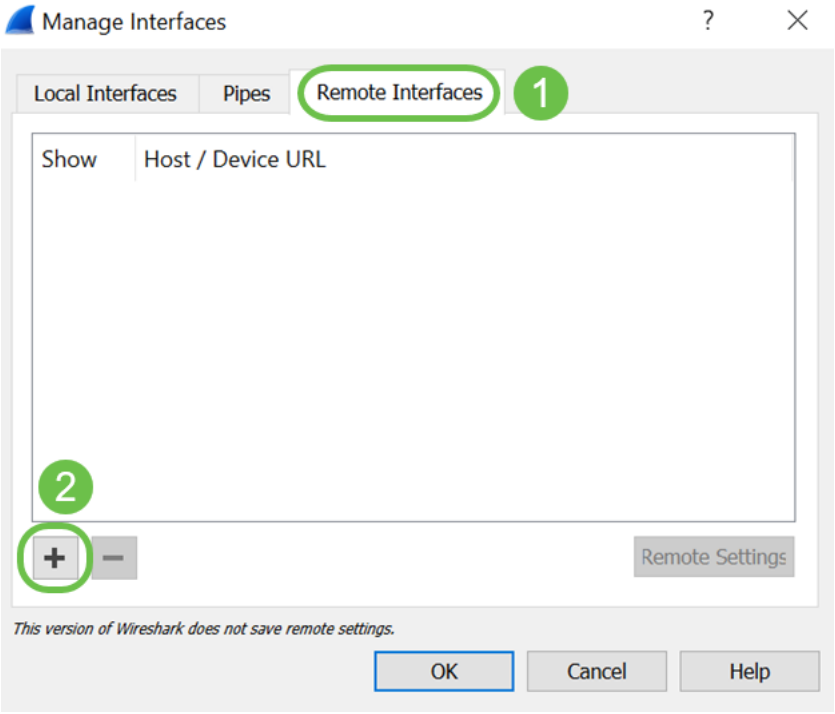
8단계

새 팝업 Wireshark - *Capture Interfaces* 창에서 **Manage Interfaces**..를 클릭합니다.



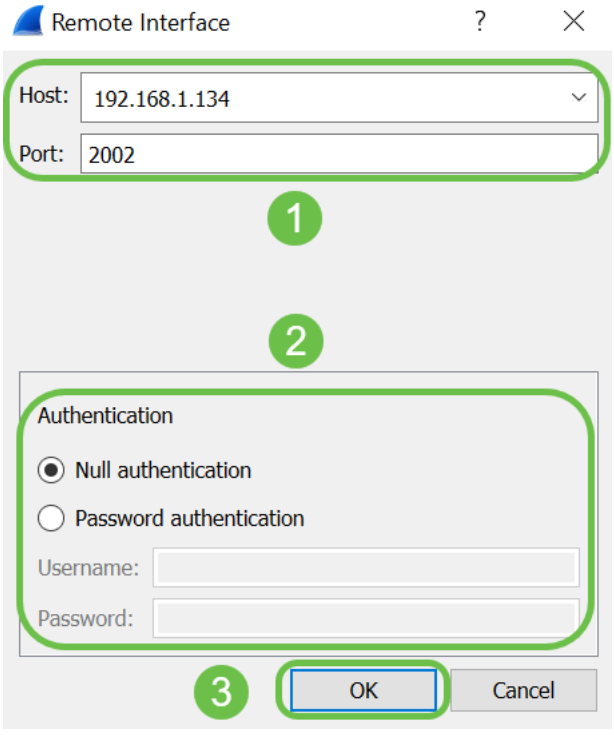
9단계

새 *Manage Interfaces* 팝업 창에서 **Remote Interfaces**로 이동하고 **더하기 아이콘**을 클릭하여 인터페이스를 추가합니다.



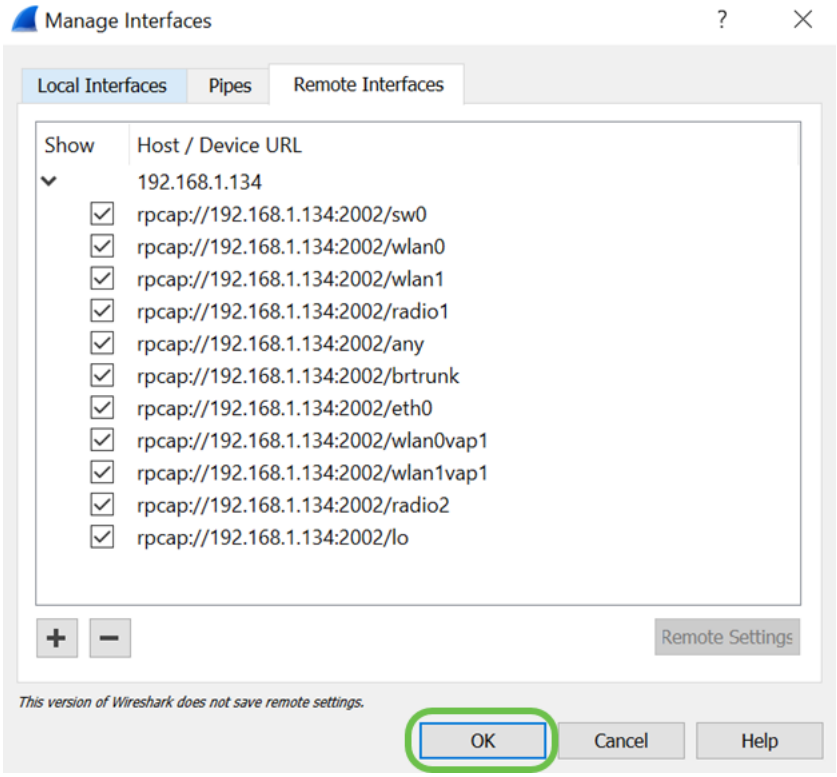
10단계

새 *Remote Interface* 팝업 창에서 *Host*를 입력합니다.IP 주소 세부 정보(원격 캡처를 시작한 WAP 디바이스 IP) 및 *포트:*번호(원격 캡처를 위해 WAP에 구성) 이 경우 WAP 장치 IP는 192.168.1.134입니다. 설정을 기반으로 *Null 인증* 또는 *비밀번호 인증* 옵션을 선택할 수 있습니다 .Password authentication(비밀번호 인증)을 선택한 경우 이에 따라 *Username(사용자 이름)* 및 *Password(비밀번호)* 세부사항을 입력하십시오.**확인**을 **클릭합니다**.



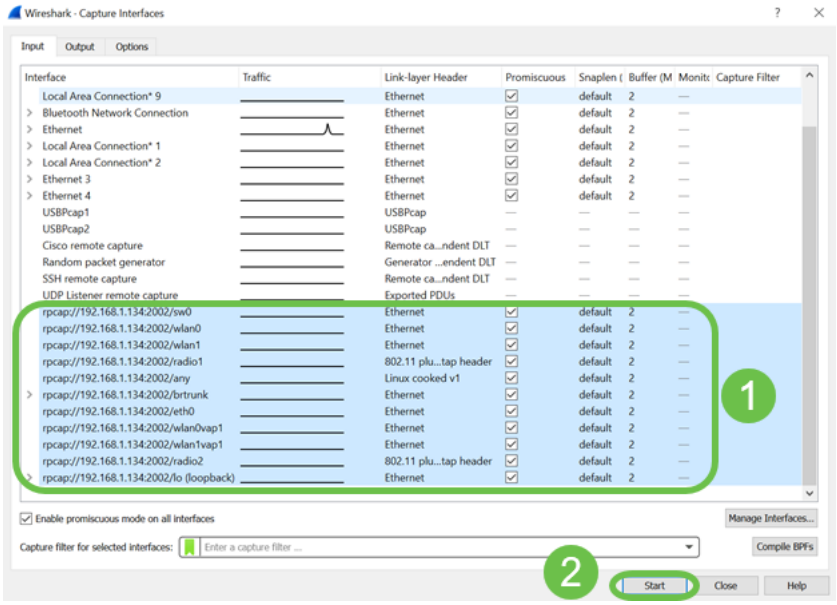
11단계

Remote Interfaces 탭에서 원격 WAP 디바이스의 모든 인터페이스를 볼 수 있습니다.캡처된 패킷의 볼륨을 줄이기 위해 이들 중 일부만 선택 취소할 수 있습니다.신호 패킷을 보려면 라디오 인터페이스를 선택한 상태로 둡니다.**확인**을 **클릭합니다**.



12단계

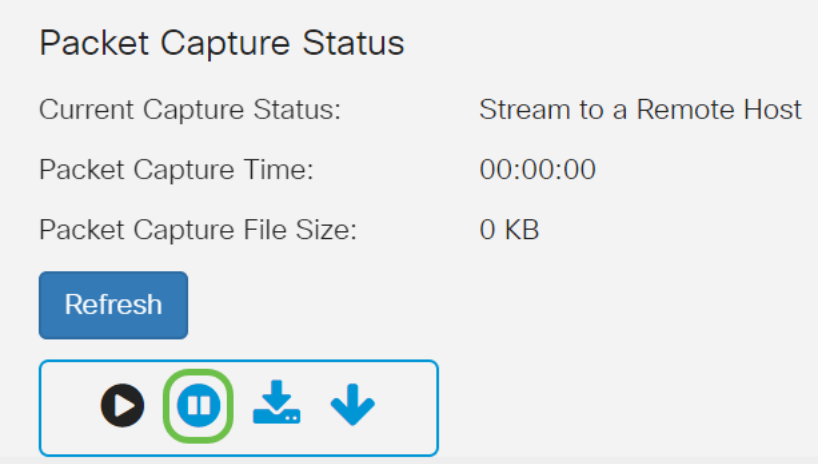
이제 새로 추가된 인터페이스는 Wireshark - *Capture Interfaces* 창*에* 반영됩니다.모니터링할 인터페이스를 선택하고 **Start**(시작)를 클릭하여 패킷을 확인합니다.



패킷을 보려고 할 때 문제가 발생하면 *원격 패킷 캡처 프로토콜* 서비스가 시스템에서 작동하지 않습니다.Wireshark가 대상 플랫폼에 연결하려면 먼저 대상 플랫폼에서 원격 패킷 캡처 프로토콜 서비스를 실행해야 합니다.자세한 내용을 보려면 Wireshark를 통해 *Remote Capture Interfaces* 링크를 클릭합니다.

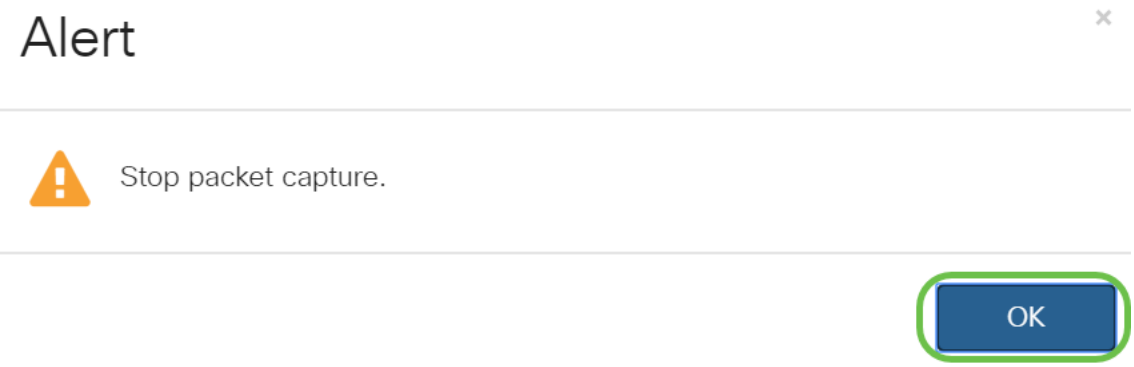
13단계

WAP에서 캡처 **중지 아이콘**을 클릭하여 캡처 프로세스를 중지합니다.



14단계

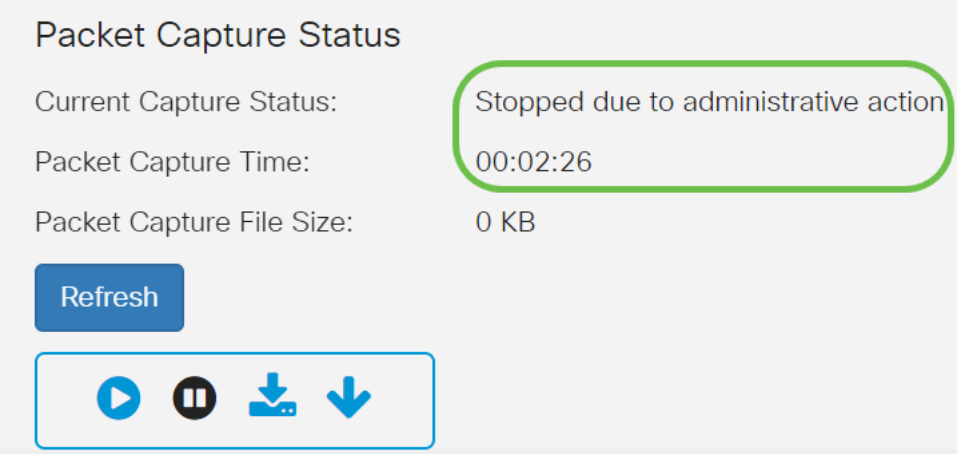
Alert 팝업 창이 나타납니다.OK(**확인**)를 클릭하여 원격 캡처를 중지합니다.



Wireshark 애플리케이션에서 **Stop** 버튼을 클릭하여 패킷 캡처를 중지할 수도 있습니다.

15단계

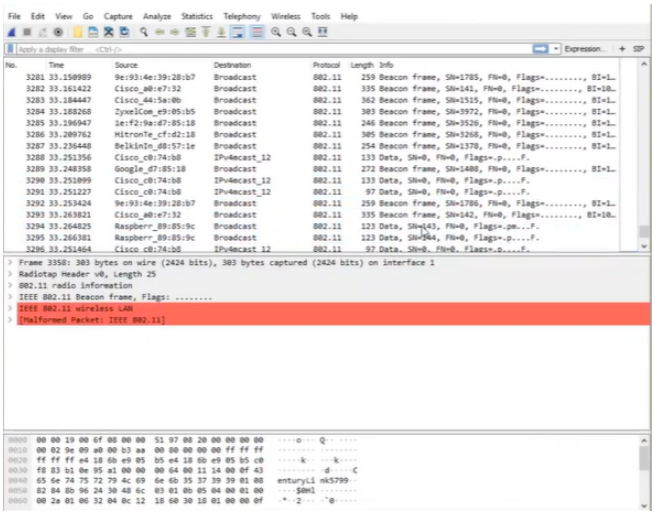
이제 *Current Capture Status(현재 캡처 상태)*가 *관리 작업으로 인해 Stopped(중지됨)*로 표시되고, *Packet Capture Time(패킷 캡처 시간)*이 반영되어 총 캡처 기간이 표시됩니다.



Packet *Capture File Size(패킷 캡처 파일 크기)*가 *0KB로 표시됩니다*.또한 이 시나리오에서는 파일 다운로드 옵션이 작동하지 않습니다.

16단계

Wireshark에서 패킷 캡처를 볼 수 있습니다.



결론

이제 Wireshark로 패킷을 직접 스트리밍할 수 있는 기술을 보유하고 있으며, 이를 분석하여 작업을 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!