# Gebruik van WirelessShark op een Cisco Business WAP voor pakketanalyse: Uploadbestand

## Doel

Dit artikel legt uit hoe u een Cisco Business Wireless Access Point (WAP) en Wireless Access Point kunt gebruiken om een pakketvastlegging uit te voeren, op te slaan en te uploaden.

## Inleiding

De configuratie verandert, controleert en probleemoplossing is iets waar een netwerkbeheerder vaak mee moet omgaan. Een eenvoudig te gebruiken instrument is van onschatbare waarde. Het doel van dit artikel is om comfortabeler te worden met de basis van pakketvastlegging en hoe een bestand aan Wireless-shark te uploaden. Als u niet bekend bent met dit proces, laten we dan een paar vragen beantwoorden die u misschien al hebt.

Eerst is Wireshark een gratis pakketanalyzer voor iedereen die hun netwerk wil oplossen. Wireshark biedt veel opties voor de opname en het sorteren van verkeer door verschillende parameters. Ga naar Wireshark voor meer informatie over deze opensource-optie.

### Wat is een pakketvastlegging?

Een pakketvastlegging, ook bekend als een PCAP-bestand, is een gereedschap dat kan helpen bij het oplossen van problemen. Het kan elk pakket opnemen dat tussen apparaten in uw netwerk wordt verzonden, in real-time. Het opnemen van pakketten staat u toe om in de details van het netwerkverkeer te graven, dat alles van apparatenontdekking, protocol gesprekken, en mislukte authenticatie kan omvatten. U kunt het pad van specifieke verkeersstroom en elke interactie tussen apparaten op geselecteerde netwerken zien. Deze pakketten kunnen indien nodig worden opgeslagen voor verdere analyse. Het is als een röntgenstraal van de binnenwerking van het netwerk via de overdracht van pakketten.

### Welke typen pakketten kunnen worden opgenomen?

Het WAP-apparaat kan de volgende typen pakketten opslaan:

- 802.11 ontvangen en verzonden pakketten op de radiointerfaces. Packets die worden opgenomen op de radio-interfaces bevatten de header 802.11.

- 802.3 pakketten die op de Ethernet-interface zijn ontvangen en verzonden.

· 802.3 pakketten die op de interne logische interfaces worden ontvangen en verzonden, zoals Virtual Access Point (VAP's) en Wireless Distribution System (WDS) interfaces.

## Hoe kan een pakketvastlegging worden uitgevoerd?

Er zijn twee methoden voor de pakketvastlegging beschikbaar:

1. *Remote Capture Methode* - De opgenomen pakketten worden in realtime opnieuw gericht op een externe computer waarop Wireless-Shark wordt uitgevoerd. U kunt *Stream naar een Remote Host* kiezen om de afstandsopnamemethode te selecteren. Als u de afstandsopnamemethode prefereert, controleer dan Met Wireshark op een WAP voor Packet Analysis: Direct naar Wireless.
2. *Local Capture Methode* - De opgenomen pakketten worden in een bestand op het WAP-apparaat opgeslagen. Het WAP-apparaat kan het bestand naar een TFTP-server (Trivial File Transfer Protocol) overbrengen. Het bestand is opgemaakt in de PCAP-indeling en kan worden onderzocht met behulp van Wireshark. U kunt kiezen *Opslaan op dit apparaat* om de lokale opnamemethode te selecteren.

De focus van dit artikel is om een bestand naar Wireshark te uploaden met de nieuwste Graphical User Interface (GUI). Als u liever een artikel bekijkt dat de oudere GUI voor de lokale opnamemethode gebruikt, controleer dan het configureren van pakketvastlegging om prestaties op een draadloos access point te optimaliseren.

## Wat doe ik met een pakketvastlegging zodra ik het PCAP-bestand heb?

De draadloze pakketvastlegging functie maakt het mogelijk de pakketten op te nemen en op te slaan die door het WAP-apparaat worden ontvangen en verzonden. De opgenomen pakketten kunnen dan door een netwerkprotocolanalyzer worden geanalyseerd om problemen op te lossen of prestaties te optimaliseren. Er zijn veel online toepassingen voor pakketanalyzer van derden beschikbaar. In dit artikel richten we ons op Wireshark.

Wireshark is niet eigendom van of ondersteund door Cisco. Neem voor ondersteuning contact op met Wireshark.

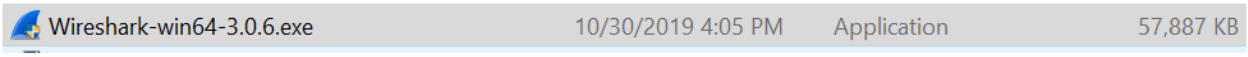
## Apparaten | Software versie

- 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 router | 1.1.0.4

# Download Wireshark

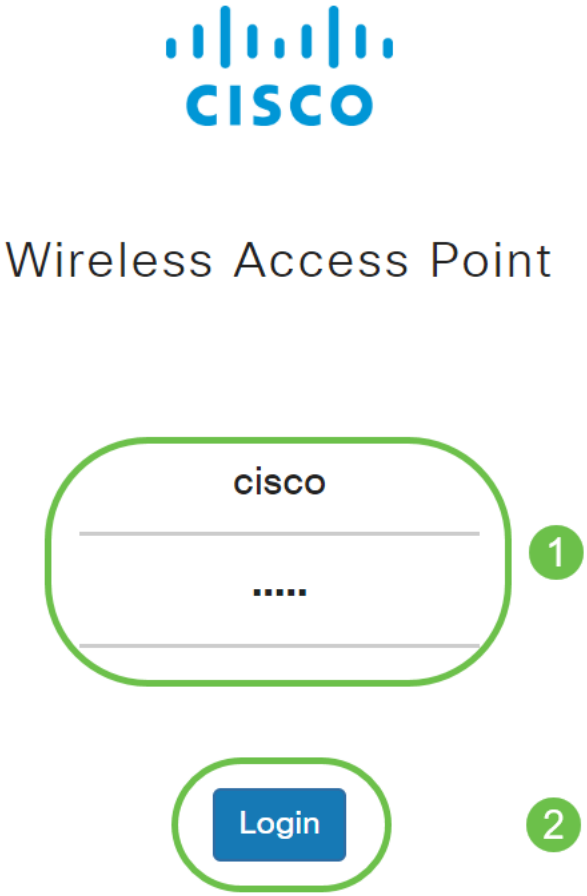
Stap 1. Ga naar de website Wireshark. Klik op **Download (Downloaden).** Selecteer de gewenste versie die u wilt downloaden. De voortgang van de download staat linksonder op het scherm.

Stap 2. Ga naar *downloads* op uw computer en selecteer het bestand Wireless-shark om de toepassing te installeren.




# Inloggen op WAP

Voer in uw webbrowser het IP-adres van de WAP in. Voer je geloofsbrieven in. Als dit de eerste keer is dat u dit apparaat opent of als u een fabrieksreset hebt uitgevoerd, dan zijn de standaardgebruikersnaam en het wachtwoord *Cisco*. Als u instructies nodig hebt over het inloggen, kunt u de stappen in het Access the Web-Based Utility of the Wireless Access Point (WAP) artikel volgen.




# Opslaan van een pakketvastlegging op een pc en uploaden naar draadloos

Stap 1. Navigeer naar **probleemoplossing > Packet Capture**.

Zorg ervoor dat **Save File op dit apparaat** is geselecteerd voor de *Packet Capture Methode*.

Configuratie van deze parameters:

- *Interface* - Voer een type interface in voor de pakketvastlegging:

- *Ethernet* - 802.3 verkeer op de Ethernet-poort.

- *Radio 1 (5 GHz) / Radio 2 (2,4 GHz)* - 802.11 verkeer op de radio-interface.

- *Duur* - Voer de duur in seconden van de opname. Het bereik loopt van 10 tot 3600. De standaard is 60.

- *Max. bestandsgrootte* - Voer de maximaal toegestane grootte in voor het opnamebestand in kilobytes (KB). Het bereik loopt van 64 tot 4096. De standaard is 1024.

Er zijn twee modi voor de pakketvastlegging.

- *Alle draadloze verkeer* - Opname alle draadloze pakketten.

- *Verkeer naar/van deze AP* - Leg de pakketten vast die van AP worden verzonden of door AP worden ontvangen.

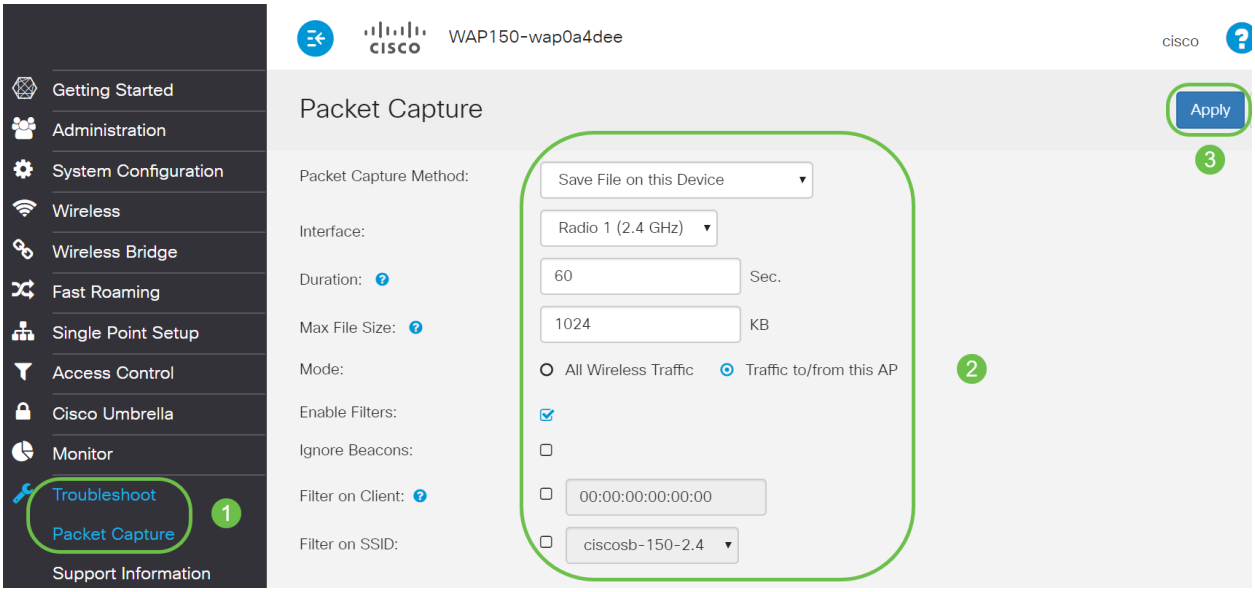
Klik op **Filters inschakelen**. Er zijn drie selectietekens beschikbaar, *negeren bakens, filteren op client* en *filteren op SSID*.

- *Negeren Beacons* - Schakel de opname van 802.11 bakens die door de radio zijn gedetecteerd of verzonden in of uit. Baken-frames zijn uitzendframes die informatie over een netwerk bevatten. Het doel van een baken is het bestaande draadloze netwerk te adverteren. Als u niet op dit type verkeer let, kunt u Afmetingen selecteren.

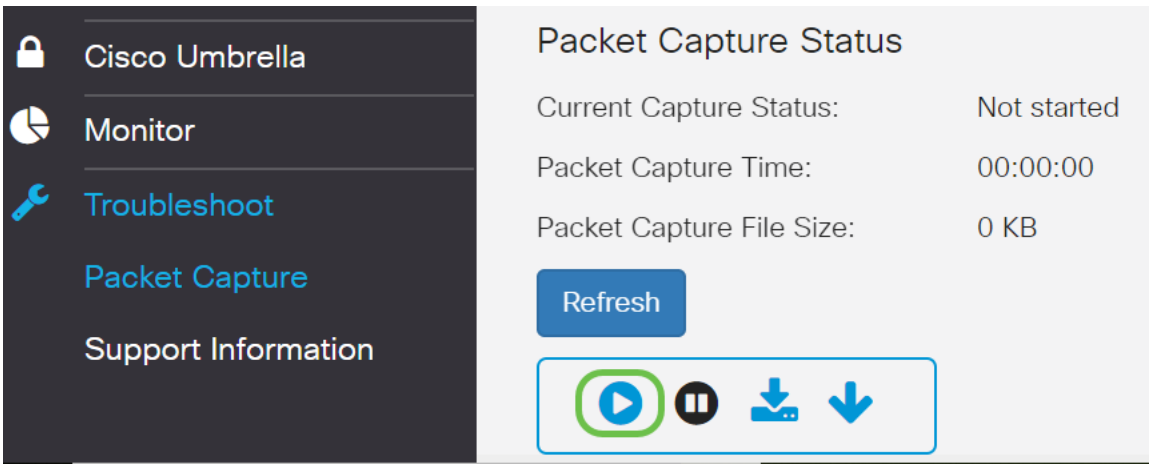
- *Filter op client* - Specificeert het MAC-adres voor de WLAN-clientfilter. Merk op dat het clientfilter alleen actief is als er een opname op een 802.11-interface wordt uitgevoerd.

- *Filter op SSID* - Selecteer een naam van SSID voor de pakketvastlegging.

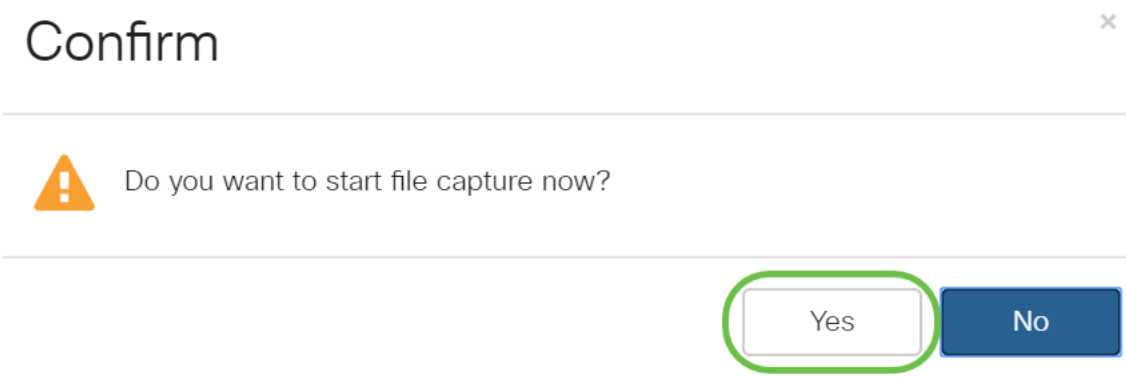
Klik op **Toepassen** om op het opstartbeeld op te slaan.



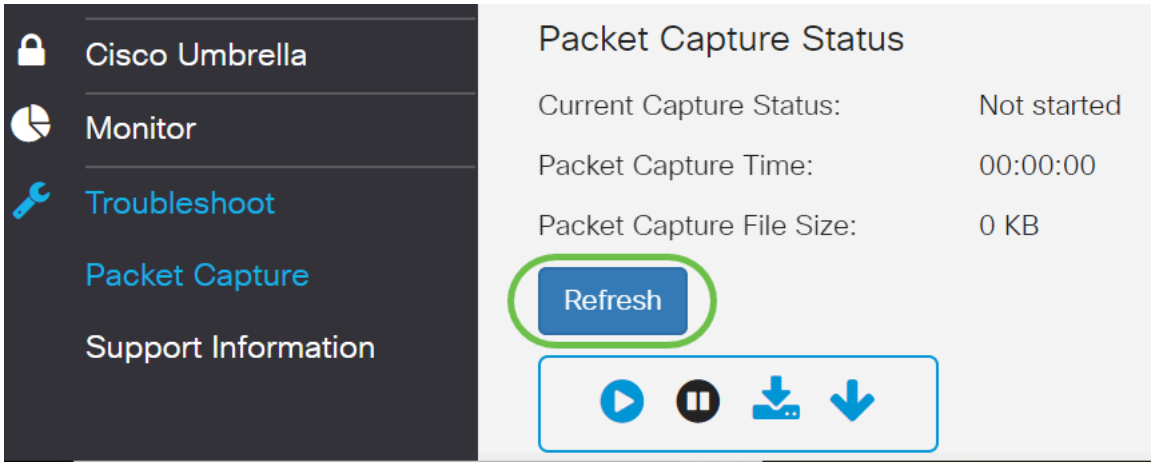

Stap 2. Klik op het pictogram **Start**.



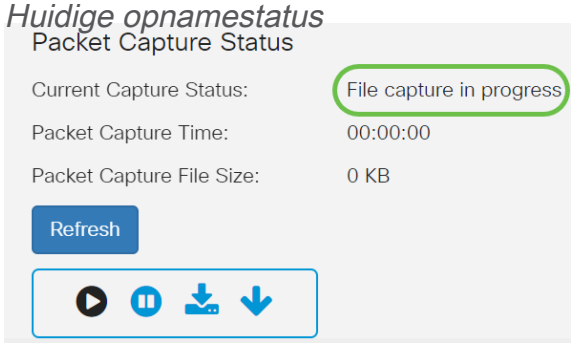

Stap 3. Het pop-upvenster *bevestigen* wordt geopend om de bevestiging te krijgen om het bestand te downloaden, klikt u op **Ja** om het bestand te downloaden.



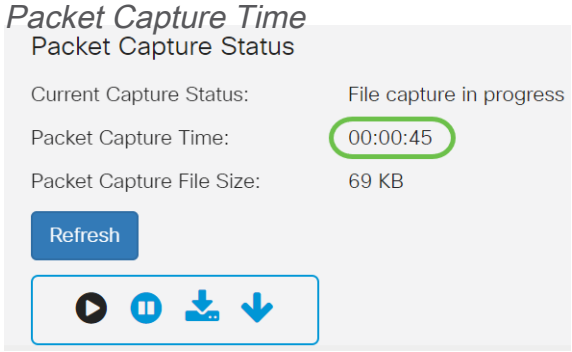

Stap 4. Klik op **Refresh** om de *Packet Capture Status* te verkrijgen die de volgende gegevens bevat:



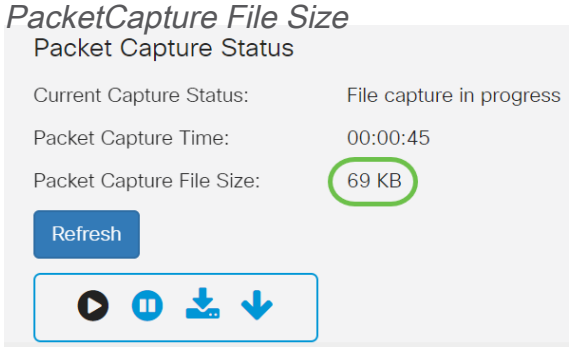

1. *Huidige opnamestatus*



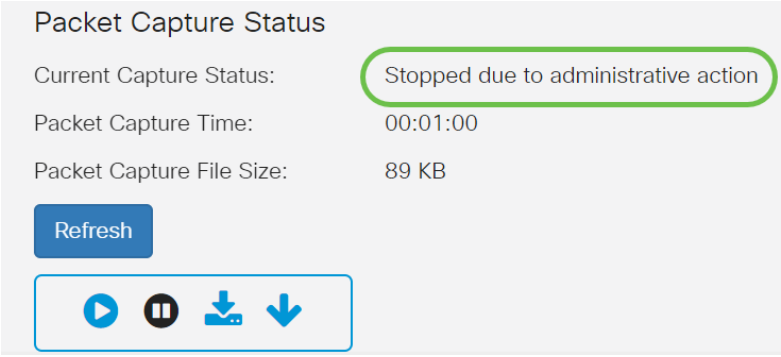

2. *Packet Capture Time*




3. *PacketCapture File Size*

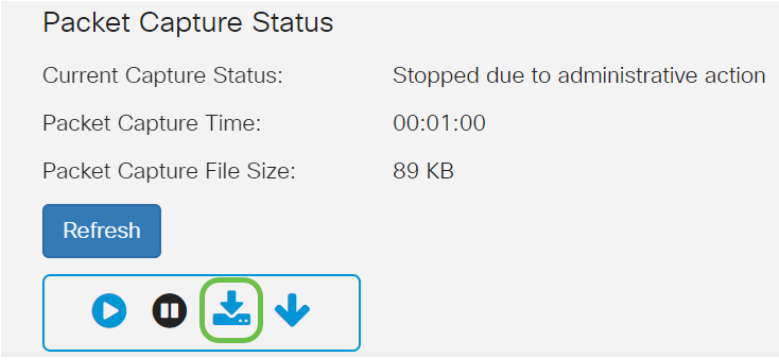



4. In de modus *Packet File Capture*, slaat het WAP-apparaat de opgenomen pakketten op in het systeem met Random Access Memory (RAM). Na activering voert de pakketvastlegging uit tot een van deze gebeurtenissen zich heeft voorgedaan:
   - De opnametijd bereikt de ingestelde duur.
   - Het opnamebestand heeft de maximale grootte.
   - De beheerder stopt de opname.

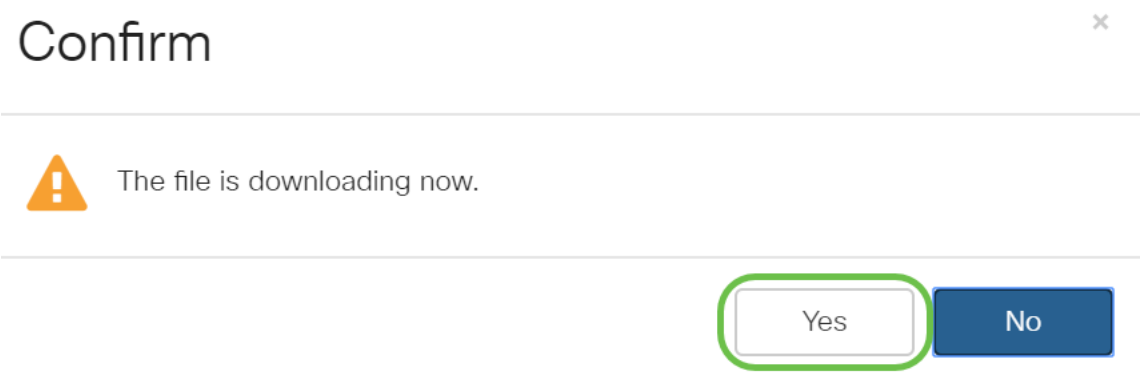



Het pakketvastlegging bestand wordt in het AP opgeslagen totdat u het AP opnieuw start.

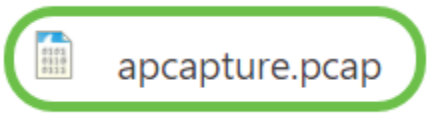
Stap 5. Klik op het pictogram **Download naar dit apparaat** om het recent opgenomen bestand te downloaden.



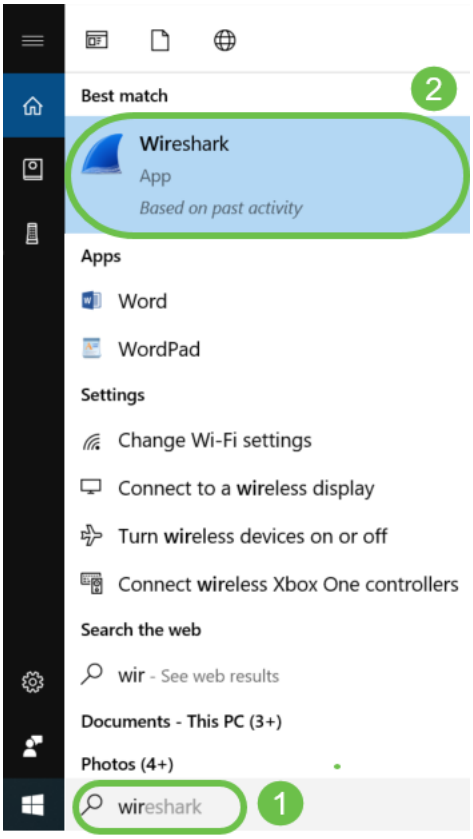

Stap 6. Het pop-upvenster *bevestigen* dat het bestand kan worden gedownload, klikt op **Ja**.



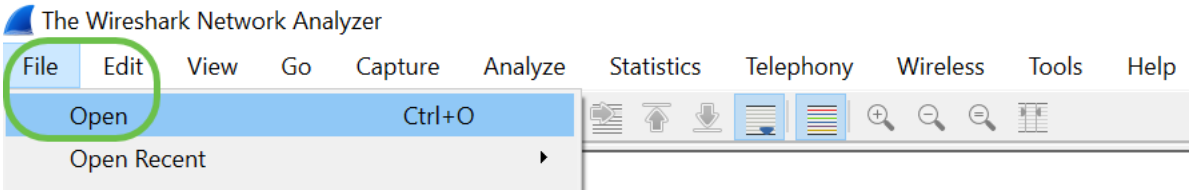

Stap 7. Het bestand met de pakketvastlegging wordt naar uw computer gedownload. In dit voorbeeld is *apshot.pcap* de naam van het bestand.



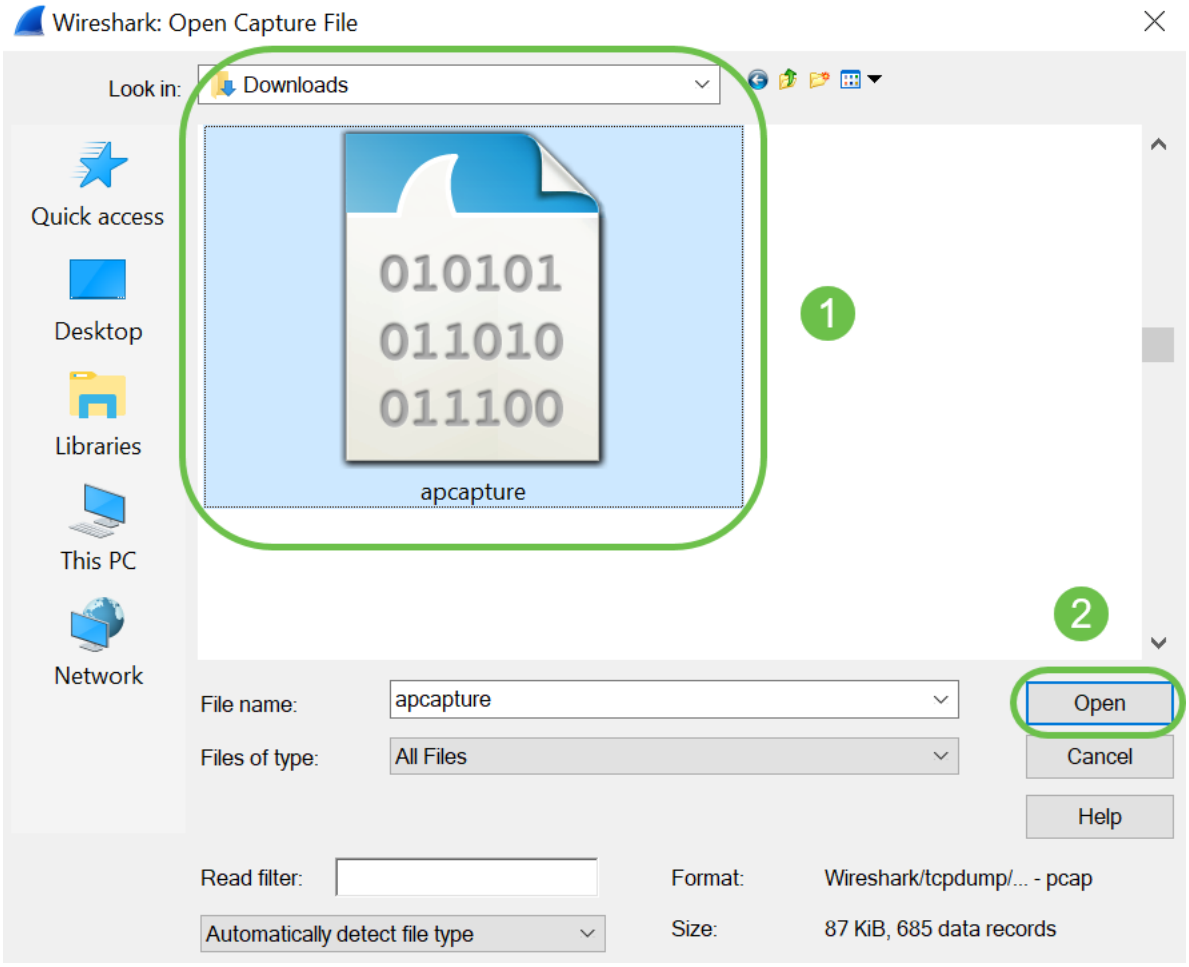

Stap 8. Aangezien Wireless-shark al is gedownload, kan dit worden bereikt door *Wireshark* te typen in de zoekbalk van Microsoft Windows en de toepassing te selecteren wanneer het een optie is.



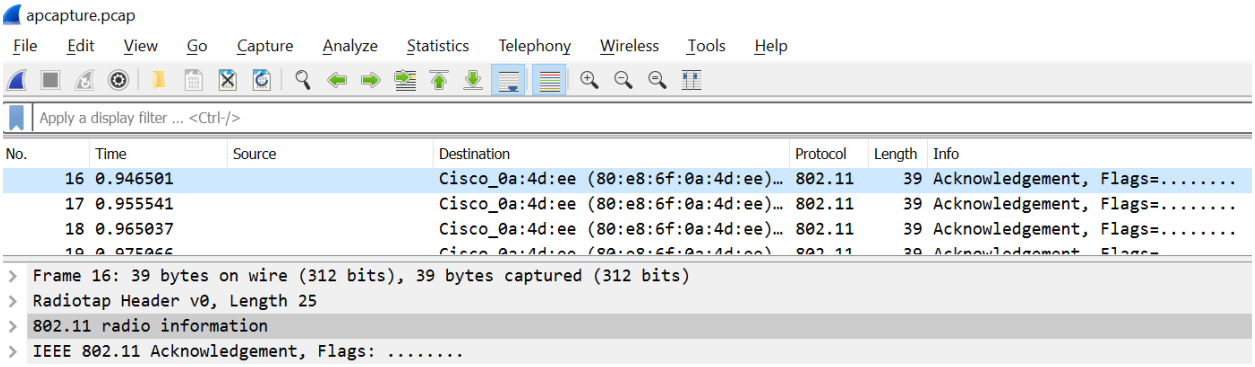

Stap 9. Navigeer naar **Bestand > Openen**.




Stap 10. Blader in het nieuwe pop-upvenster om het bestand, in dit geval, *apshot.pcap* te vinden. Klik op **Openen**.




Stap 1. Het bestand wordt geopend in de applicatie Wireless-shark en u kunt de details van de pakketten zien.




## Conclusie

Wanneer uw pakket wordt opgenomen en geüpload naar Wireshark, kunt u nu beginnen met het analyseren ervan. Weet je niet waar je heen moet? Er zijn genoeg video's en artikelen beschikbaar die u online kunt verkennen. Wat je zoekt, hangt af van de behoeften van je situatie. Dit heb je!