Uso di Wireshark su Cisco Business WAP per l'analisi dei pacchetti: Carica file

Obiettivo

In questo articolo viene spiegato come utilizzare un Cisco Business Wireless Access Point (WAP) e Wireshark per eseguire, salvare e caricare un'acquisizione pacchetto.

Introduzione

Le modifiche alla configurazione, il monitoraggio e la risoluzione dei problemi sono problemi che gli amministratori di rete devono affrontare spesso. Avere uno strumento semplice da usare è inestimabile! L'obiettivo di questo articolo è di acquisire familiarità con le nozioni di base sulle acquisizioni dei pacchetti e su come caricare un file in Wireshark. Se non avete familiarità con questo processo, rispondete ad alcune domande che potreste già avere.

Per prima cosa, Wireshark è un analizzatore di pacchetti gratuito per chiunque voglia risolvere i problemi della rete. Wireshark fornisce molte opzioni per l'acquisizione e l'ordinamento del traffico in base a diversi parametri. Visitate Wireshark per i dettagli su questa opzione open-source.

Che cos'è l'acquisizione dei pacchetti?

L'acquisizione di un pacchetto, nota anche come file PCAP, è uno strumento che può essere utile nella risoluzione dei problemi. Può registrare in tempo reale ogni pacchetto inviato tra i dispositivi della rete. L'acquisizione dei pacchetti consente di analizzare i dettagli del traffico di rete, che può includere qualsiasi cosa, dall'individuazione dei dispositivi alle conversazioni di protocollo e all'autenticazione non riuscita. È possibile visualizzare il percorso di un flusso di traffico specifico e ogni interazione tra i dispositivi sulle reti selezionate. Questi pacchetti possono essere salvati per ulteriori analisi, se necessario. È come una radiografia del funzionamento interno della rete tramite il trasferimento di pacchetti.

Quali tipi di pacchetti è possibile acquisire?

Il dispositivo WAP può acquisire i seguenti tipi di pacchetti:

·Pacchetti 802.11 ricevuti e trasmessi su interfacce radio. I pacchetti acquisiti sulle interfacce radio includono l'intestazione 802.11.

·Pacchetti 802.3 ricevuti e trasmessi sull'interfaccia Ethernet.

·Pacchetti 802.3 ricevuti e trasmessi sulle interfacce logiche interne, come i VAP

(Virtual Access Point) e le interfacce WDS (Wireless Distribution System).

In che modo è possibile acquisire un pacchetto?

Sono disponibili due metodi di acquisizione dei pacchetti:

1. *Metodo di acquisizione remota* - I pacchetti acquisiti vengono reindirizzati in tempo reale a un computer esterno che esegue Wireshark. È possibile scegliere *Trasmetti a host remoto* per selezionare il metodo di acquisizione remota. Se si preferisce il metodo di cattura a distanza, utilizzare Wireshark su un WAP per l'analisi dei pacchetti: Flusso diretto a Wireshark.
2. *Local Capture Method* - I pacchetti catturati vengono archiviati in un file sul dispositivo WAP. Il dispositivo WAP può trasferire il file in un server TFTP (Trivial File Transfer Protocol). Il file è formattato in formato PCAP e può essere esaminato utilizzando Wireshark. È possibile scegliere *Salva file sul dispositivo* per selezionare il metodo di acquisizione locale.

In questo articolo viene illustrato come caricare un file in Wireshark con l'interfaccia utente grafica (GUI) più recente. Se si preferisce visualizzare un articolo che utilizza la GUI precedente per il metodo di acquisizione locale, consultare Configurare l'acquisizione dei pacchetti per ottimizzare le prestazioni su un punto di accesso wireless.

Cosa fare con l'acquisizione di un pacchetto una volta ottenuto il file PCAP?

La funzione di acquisizione dei pacchetti wireless consente di acquisire e memorizzare i pacchetti ricevuti e trasmessi dal dispositivo WAP. I pacchetti acquisiti possono quindi essere analizzati da un analizzatore di protocolli di rete per la risoluzione dei problemi o l'ottimizzazione delle prestazioni. Sono disponibili online numerose applicazioni di analisi dei pacchetti di terze parti. In questo articolo, ci concentriamo su Wireshark.

Wireshark non è di proprietà o non è supportato da Cisco. Per assistenza, contattare Wireshark.

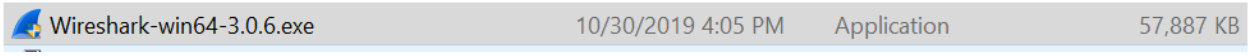
Dispositivi | Versione software

- 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

Scarica Wireshark

Passaggio 1. Accedere al sito Web Wireshark. Fare clic su **Download (Scarica).** Selezionare la versione appropriata da scaricare. In basso a sinistra nella finestra viene visualizzato lo stato del download.

Passaggio 2. Andare in *Download* sul computer e selezionare il file Wireshark per installare la relativa applicazione.



Accedere a WAP

Nel browser Web, immettere l'indirizzo IP del WAP. Immettere le credenziali. Se è la prima volta che accedi a questo dispositivo o hai eseguito una reimpostazione di fabbrica, il nome utente e la password predefiniti sono *cisco*. Per istruzioni su come eseguire l'accesso, seguire la procedura descritta nell'articolo Accesso all'utilità basata sul Web del punto di accesso wireless (WAP).

Salvataggio di un'acquisizione di pacchetti su un PC e caricamento su Wireshark

Passaggio 1. Passare a **Risoluzione dei problemi > Acquisizione pacchetto**.

Verificare che l'opzione **Salva file sul dispositivo** sia selezionata per il *metodo di acquisizione pacchetti*.

Configurare i seguenti parametri:

·*Interface* - Immettere un tipo di interfaccia di acquisizione per l'acquisizione dei pacchetti:

·*Ethernet* - traffico 802.3 sulla porta Ethernet.

·*Radio 1 (5 GHz) / Radio 2 (2,4 GHz)* - traffico 802.11 sull'interfaccia radio.

·*Durata* - Immettere la durata in secondi per l'acquisizione. L'intervallo è compreso tra 10 e 3600. Il valore predefinito è 60.

·*Dimensioni massime file* - Immettere le dimensioni massime consentite per il file di acquisizione in kilobyte (KB). L'intervallo è compreso tra 64 e 4096. Il valore predefinito è 1024.

Sono disponibili due modalità di acquisizione dei pacchetti.

·*All Wireless Traffic* - Acquisisce tutti i pacchetti wireless.

·*Traffico da/verso questo punto di accesso*: cattura i pacchetti inviati dal punto di accesso o ricevuti dal punto di accesso.

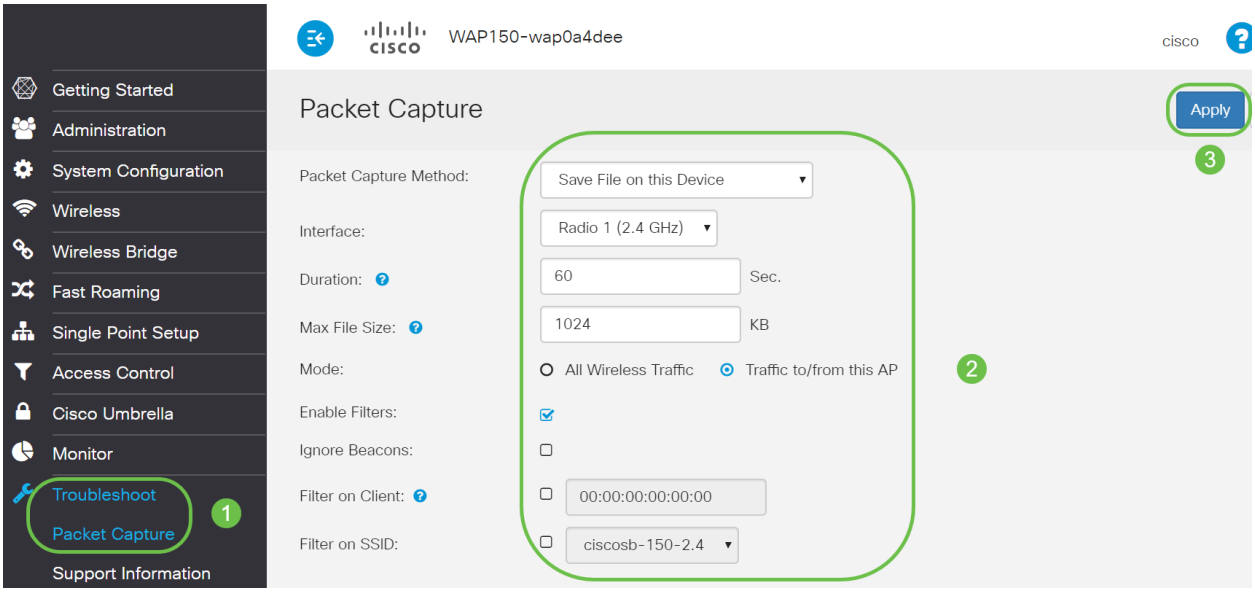
Fare clic su **Abilita filtri**. Sono disponibili tre caselle di controllo: *Ignora beacon, Filtra in base al client* e *Filtra in base al SSID*.

·*Ignora beacon* - Abilita o disabilita la cattura dei beacon 802.11 rilevati o trasmessi dalla radio. I frame beacon sono frame di trasmissione che contengono informazioni relative a una rete. Lo scopo di un beacon è quello di annunciare la rete wireless esistente. Se non si sta cercando questo tipo di traffico, è possibile selezionare Ignora beacon.

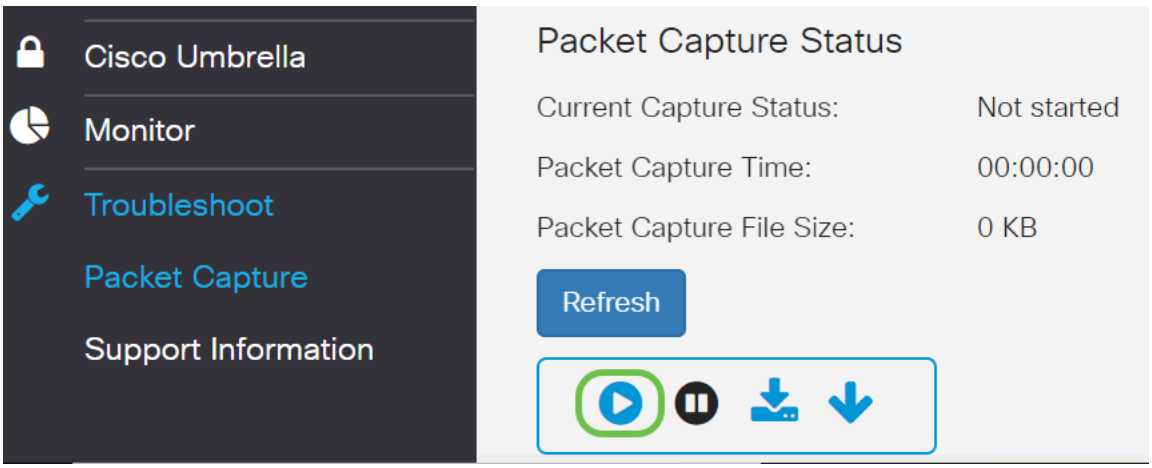
·*Filtro sul client*: per specificare l'indirizzo MAC del filtro client WLAN. Il filtro Client è attivo solo quando si esegue un'acquisizione su un'interfaccia 802.11.

·*Filtro in base a SSID* - Selezionare un nome SSID per l'acquisizione dei pacchetti.

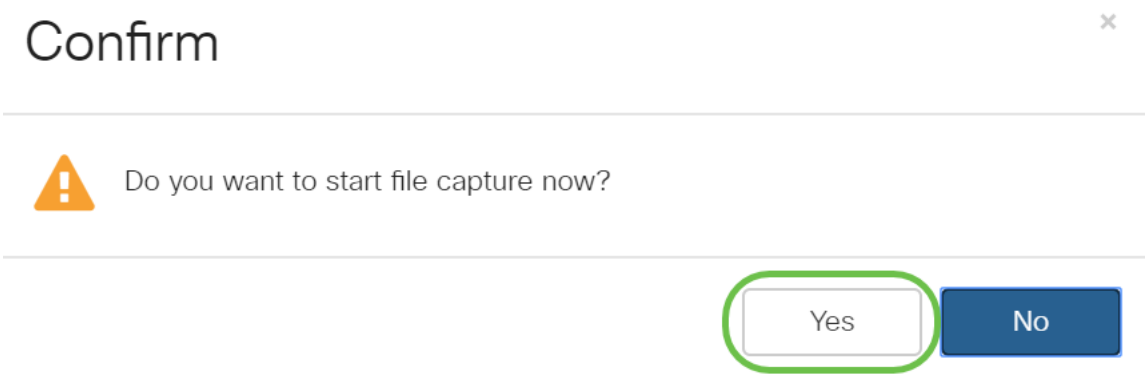
Fare clic su **Apply** (Applica) per salvare il file nella configurazione di avvio.



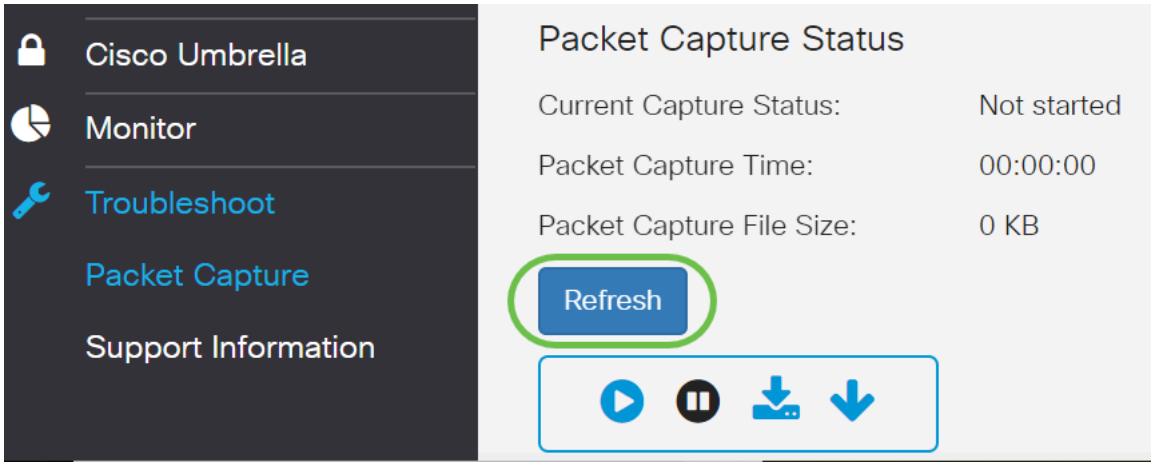
Passaggio 2. Fare clic sull'icona **Avvia acquisizione**.



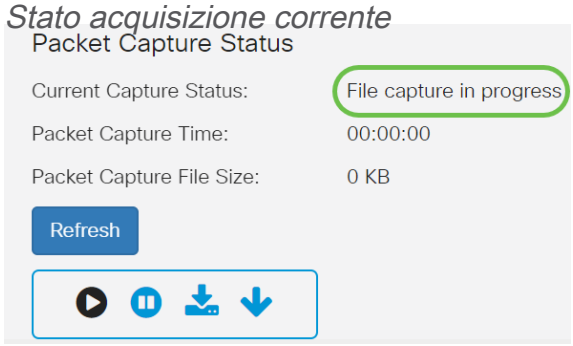
Passaggio 3. Verrà visualizzata una finestra popup di *conferma* per ottenere la conferma del download del file. Fare clic su **Sì** per avviare il download del file.



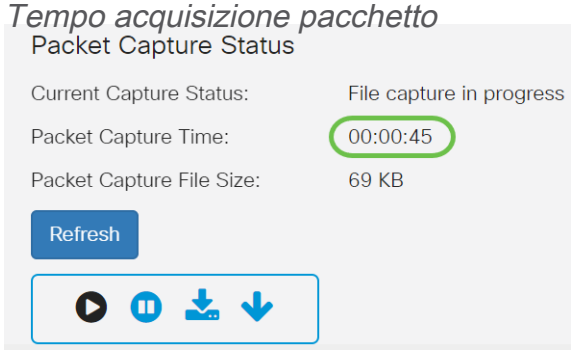
Passaggio 4. Fare clic su **Aggiorna** per ottenere *lo stato di acquisizione* del *pacchetto* contenente i dati seguenti:



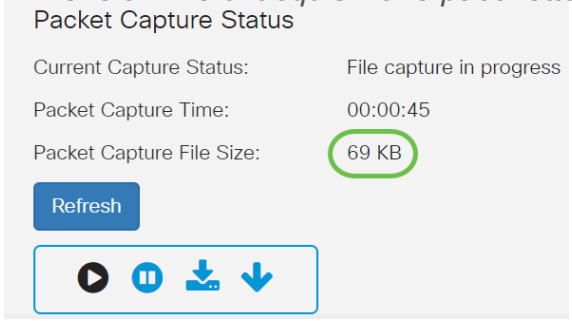
1. *Stato acquisizione corrente*



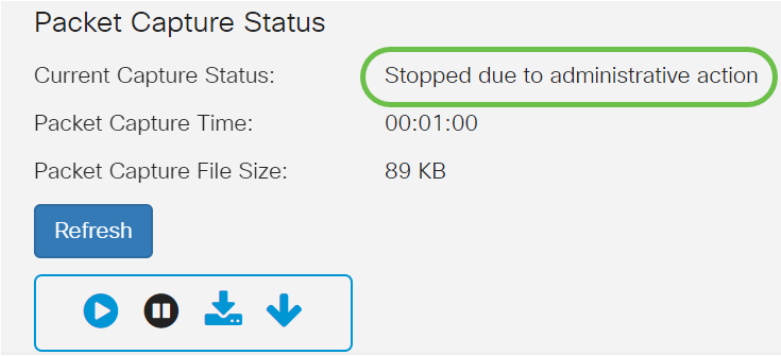
2. *Tempo acquisizione pacchetto*



3. *Dimensioni file di acquisizione pacchetto*

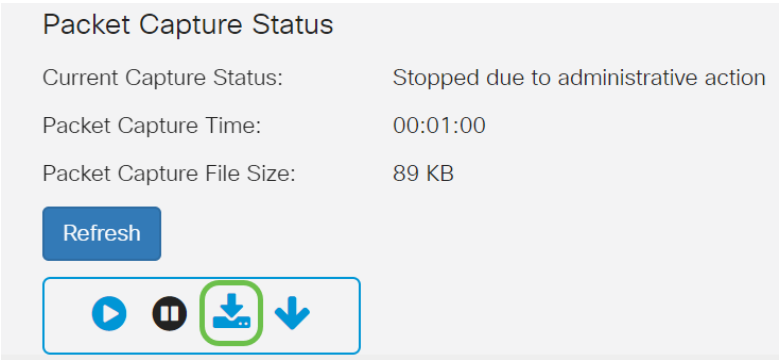


4. In modalità *Packet File Capture*, il dispositivo WAP memorizza i pacchetti acquisiti nel file system RAM (Random Access Memory). Al momento dell'attivazione, l'acquisizione del pacchetto continua finché non si verifica uno dei seguenti eventi:
·Il tempo di acquisizione raggiunge la durata configurata.
·Il file di acquisizione raggiunge le dimensioni massime.
·L'amministratore interrompe la cattura.

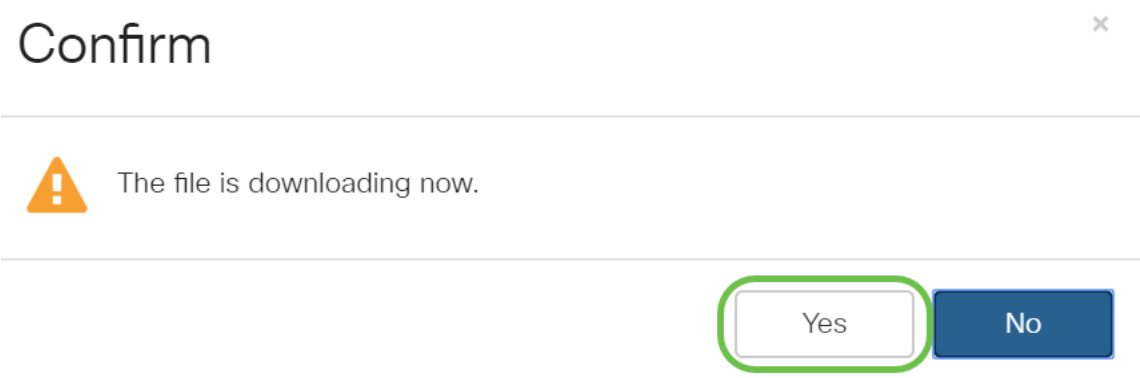


Il file di acquisizione del pacchetto verrà archiviato nell'access point finché non si riavvia l'access point.

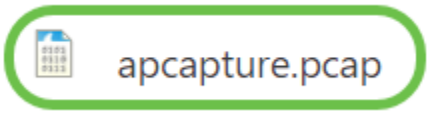
Passaggio 5. Fare clic sull'icona **Scarica su questo dispositivo** per scaricare il file catturato di recente.



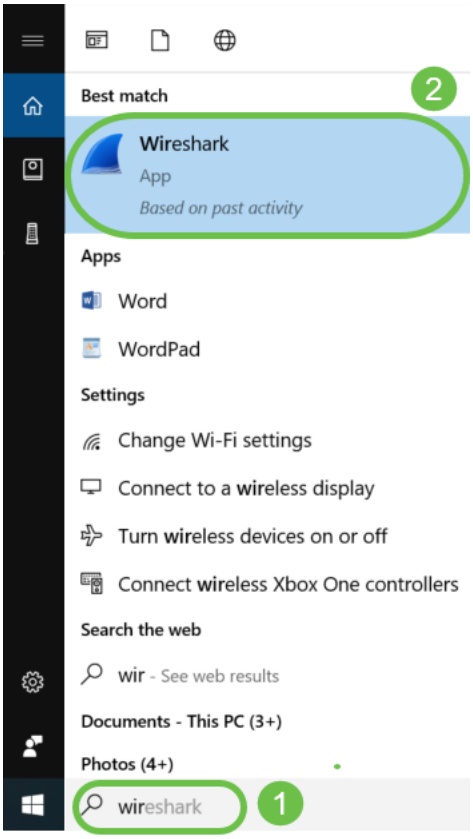
Passaggio 6. Verrà visualizzata una finestra popup di *conferma* per confermare il download del file, fare clic su **Sì**.



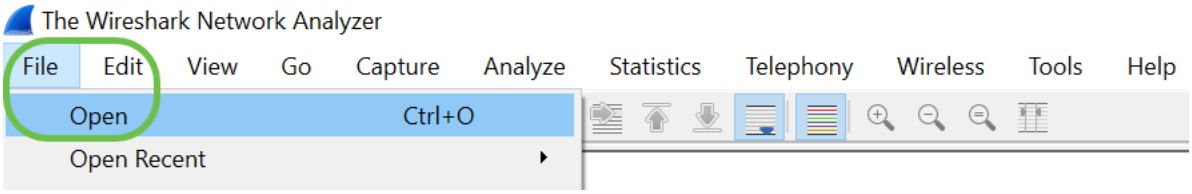
Passaggio 7. Il file di acquisizione dei pacchetti verrà scaricato nel computer. In questo esempio, *apcapture.pcap* è il nome del file.



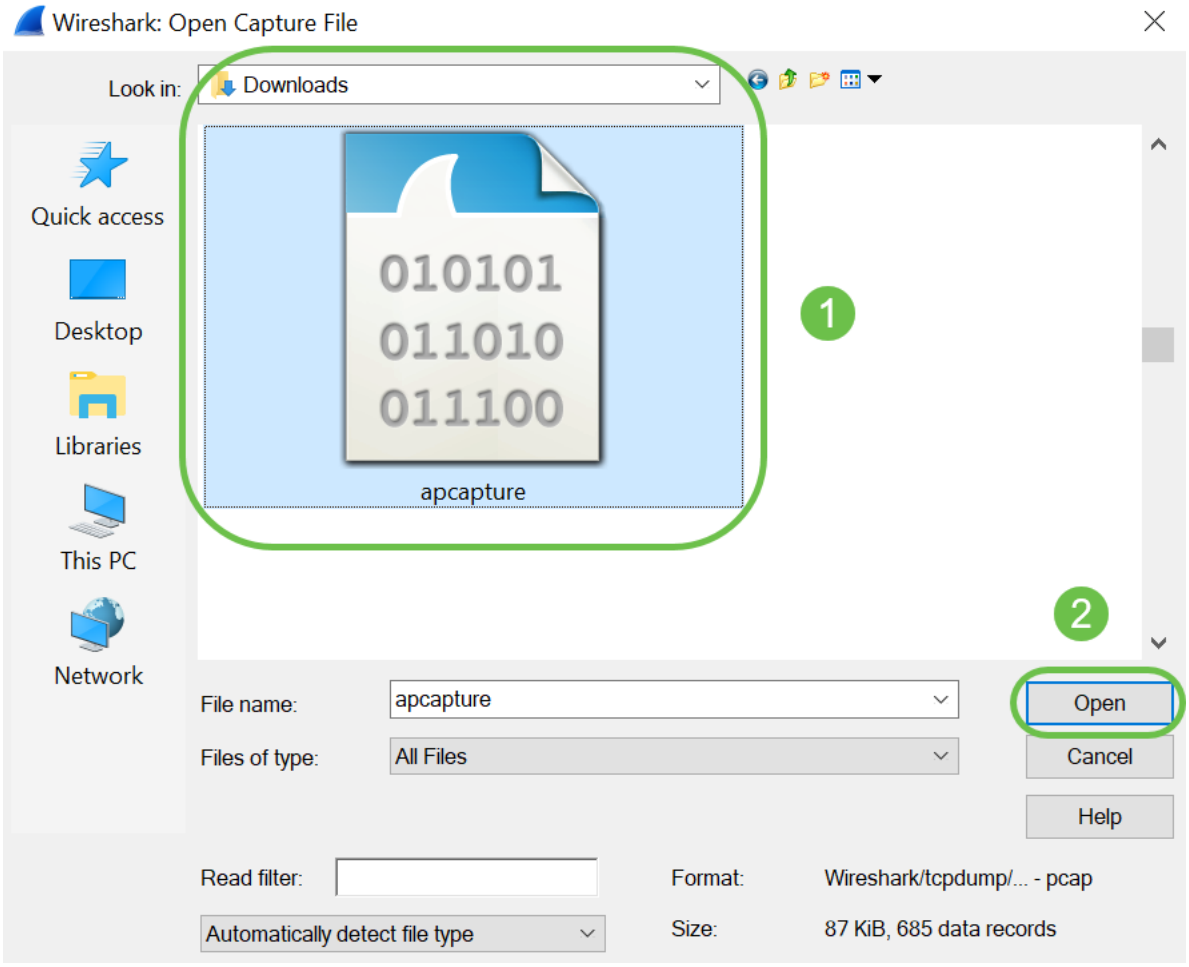
Passaggio 8. Poiché Wireshark è già stato scaricato, è possibile accedervi digitando *Wireshark* nella barra di ricerca di Microsoft Windows e selezionando l'applicazione quando è un'opzione.



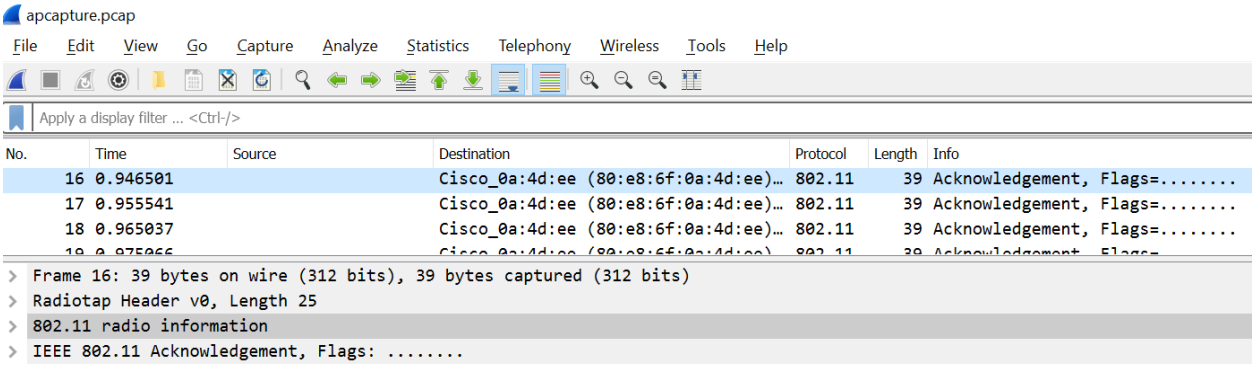
Passaggio 9. Passare a **File > Apri**.



Passaggio 10. Nella nuova finestra popup, individuare il file, in questo caso *apcapture.pcap*. Fare clic su **Apri**.



Passaggio 11. Il file verrà aperto con l'applicazione *Wireshark* e sarà possibile visualizzare i dettagli dei pacchetti.



Conclusioni

Dopo aver acquisito e caricato il pacchetto su Wireshark, è possibile iniziare ad analizzarlo. Non sai dove andare da qui? Ci sono moltissimi video e articoli disponibili online da esplorare. Ciò che cercate dipende dalle esigenze della vostra situazione. Ce l'avete!