# Configurazione delle acquisizioni di pacchetti su AireOS WLC

## Sommario



## Introduzione

Questo documento descrive come eseguire un dump di pacchetto su un controller WLC (AireOS Wireless LAN Controller). Questo metodo visualizza i pacchetti inviati e/o ricevuti a livello di CPU del WLC in formato esadecimale, che vengono quindi convertiti in un file .pcap con Wireshark.

Èutile nei casi in cui la comunicazione tra un WLC e un server RADIUS (Remote Authentication Dial-In User Service), un punto di accesso (AP) o altri controller devono essere verificati in modo rapido con un'acquisizione di pacchetti a livello WLC, ma un port-span è difficile da eseguire.

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al WLC dall'interfaccia della riga di comando (CLI), preferibilmente SSH poiché l'output è più veloce della console.
- PC con Wireshark installato

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC v8.3
- Wireshark v2 o successivo

**Nota**: questa funzione è disponibile dalla versione 4 di AireOS.

### Limitazioni

La registrazione dei pacchetti acquisirà solo i pacchetti bidirezionali da Control Plane (CP) a Data Plane (DP) nel WLC. I pacchetti che non vengono inviati dal piano dati WLC al/dal piano di controllo (ad es. traffico esterno verso il tunnel di ancoraggio, cadute DP-CP e così via) non vengono catturati.

Di seguito sono riportati alcuni esempi di tipi di traffico da/verso il WLC elaborati al CCP:

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RAGGIO
- TACACS+
- Messaggi sulla mobilità
- controllo CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

Il traffico da/verso il client viene elaborato nel Data Plane (DP) ad eccezione di: gestione 802.11, autenticazione 802.1X/EAPOL, ARP, DHCP e Web.

# Configurazione

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Abilita registrazione pacchetti in WLC

Passaggio 1. Accedere alla CLI del WLC.

A causa della quantità e della velocità dei log visualizzati da questa funzione, si consiglia di accedere al WLC tramite SSH e non tramite console.

Passaggio 2. Applicare un Access Control List (ACL) per limitare il traffico acquisito.

Nell'esempio riportato, l'acquisizione mostra il traffico da/verso l'interfaccia di gestione del WLC (indirizzo IP 172.16.0.34) e il server RADIUS (172.16.56.153).

```
> debug packet logging acl ip 1 permit 172.16.0.34 172.16.56.153
> debug packet logging acl ip 2 permit 172.16.56.153 172.16.0.34
```

**Suggerimento**: Per acquisire tutto il traffico da/verso il WLC, si consiglia di applicare un ACL

che scarti il traffico SSH da/verso l'host che ha avviato la sessione SSH. Di seguito sono riportati i comandi che è possibile usare per compilare l'ACL:

>debug packet logging acl ip 1 deny <WLC-IP> <host-IP> tcp 22 any
>debug packet logging acl ip 2 deny <host-IP> <WLC-IP> tcp any 2
>debug packet logging acl ip 3 permette qualsiasi

Passaggio 3. Configurare il formato leggibile da Wireshark.

```
> debug packet logging format text2pcap
```

Passaggio 4. Abilitare la funzione di registrazione dei pacchetti.

Nell'esempio viene mostrato come acquisire 100 pacchetti ricevuti/trasmessi (supporta 1 - 65535 pacchetti):

```
> debug packet logging enable all 100
```

Passaggio 5. Registrare l'output in un file di testo.

**Nota: per impostazione predefinita, registra solo 25 pacchetti ricevuti con il comando debug packet logging enable**.

**Nota:** Anziché **tutto,** è possibile utilizzare **rx** o **tx** per acquisire solo il traffico ricevuto o trasmesso.

Per ulteriori dettagli sulla configurazione della funzione di registrazione dei pacchetti, consultare questo collegamento:

Guida alla configurazione di Cisco Wireless Controller, versione 8.3, uso della funzione di debug

# Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Utilizzare il comando specificato per verificare la configurazione corrente della registrazione dei pacchetti.

```
> show debug packet

Status..................................... rx/tx            !!! This means the capture is
active
Number of packets to display..................... 100
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

   Driver ACL:
      [1]: disabled
      [2]: disabled
```

```
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: permit s=172.16.0.34 d=172.16.56.153 any
      [2]: permit s=172.16.56.153 d=172.16.0.34 any
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
```

Riprodurre il comportamento necessario per generare il traffico.

Viene visualizzato un output simile al seguente:

```
rx len=108, encap=unknown, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 5A 69 81 00 00 80 01 78 A7 AC 10 ..E..Zi.....x',.
0020 00 38 AC 10 00 22 03 03 55 B3 00 00 00 00 45 00 .8,.."..U3....E.
0030 00 3E 0B 71 00 00 FE 11 58 C3 AC 10 00 22 AC 10 .>.q..~.XC,.",.
0040 00 38 15 B3 13 88 00 2A 8E DF A8 a1 00 0E 00 0E .8.3...*._(!....
0050 01 00 00 00 00 22 F1 FC 8B E0 18 24 07 00 C4 00 ....."q|.`.$..D.
0060 F4 00 50 1C BF B5 F9 DF EF 59 F7 15 t.P.?5y_oYw.
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
```

```
0010 08 00 45 00 00 28 69 82 40 00 80 06 38 D3 AC 10 ..E..(i.@...8S,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 40 29 50 10 01 01 52 8A 00 00 @)P...R...
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 83 40 00 80 06 38 D2 AC 10 ..E..(i.@...8R,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 41 59 50 10 01 00 51 5B 00 00 AYP...Q[..
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 84 40 00 80 06 38 D1 AC 10 ..E..(i.@...8Q,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 43 19 50 10 01 05 4F 96 00 00 C.P...O...
```

Rimozione di ACL dalla registrazione dei pacchetti

Per disabilitare i filtri applicati dagli ACL, usare questi comandi:

```
> debug packet logging acl ip 1 disable
>debug packet logging acl ip 2 disable
```

**Disabilita registrazione pacchetti**

Per disabilitare la registrazione dei pacchetti senza rimuovere gli ACL, usare questo comando:

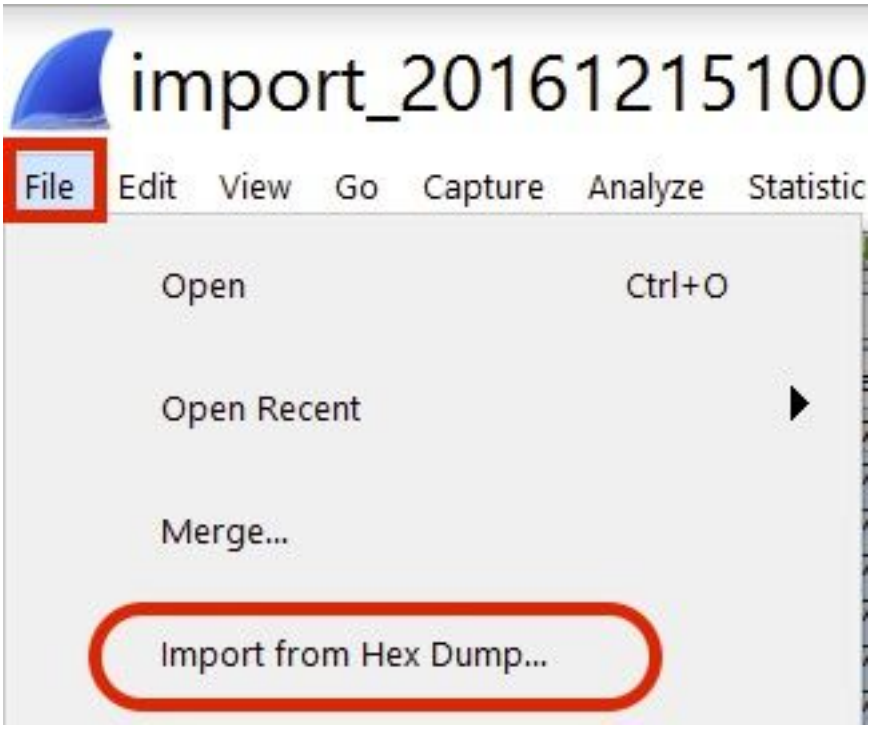
```
> debug packet logging disable
```

# Conversione dell'output di registrazione dei pacchetti in un file con estensione pcap

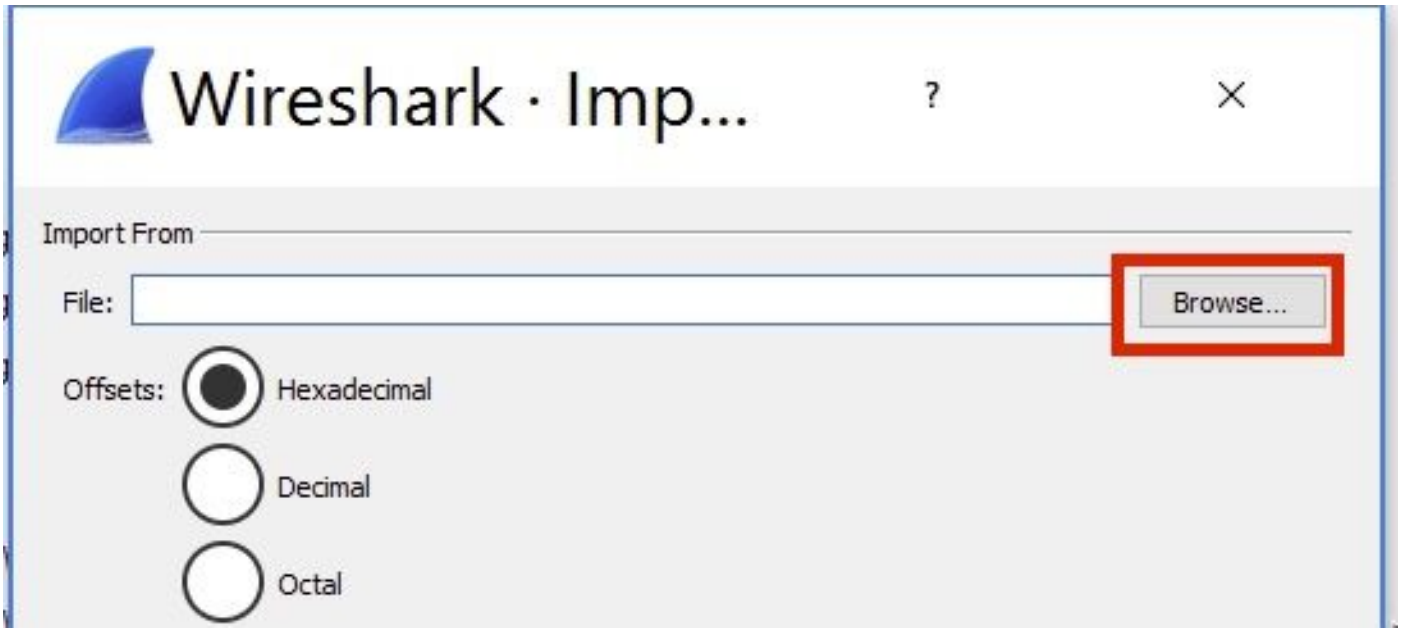
Passaggio 1. Al termine dell'output, raccoglierlo e salvarlo in un file di testo.

Verificare di aver raccolto un log pulito, altrimenti Wireshark potrebbe visualizzare pacchetti danneggiati.

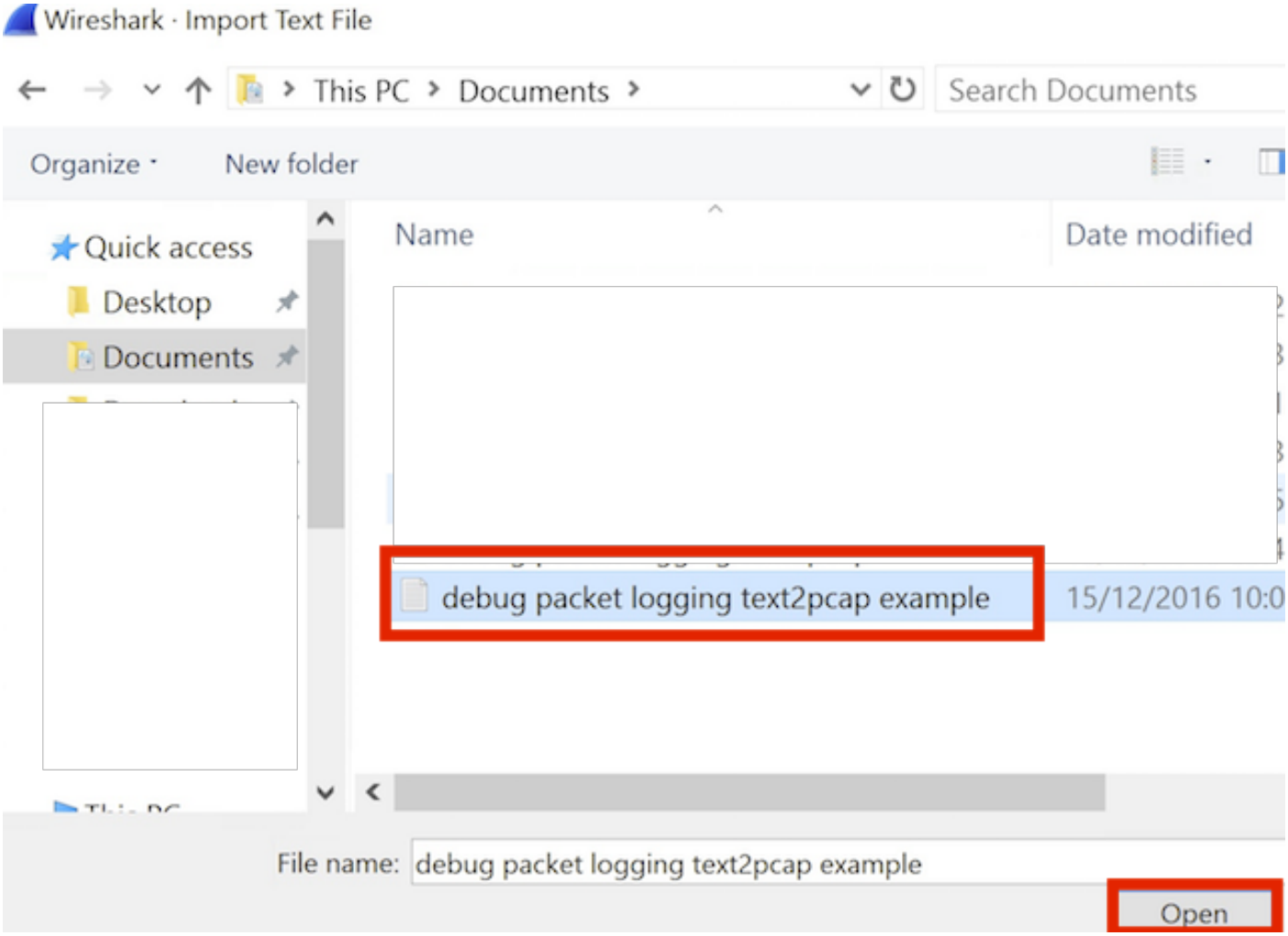
Passaggio 2. Aprire Wireshark e selezionare **File>Import from Hex Dump...**



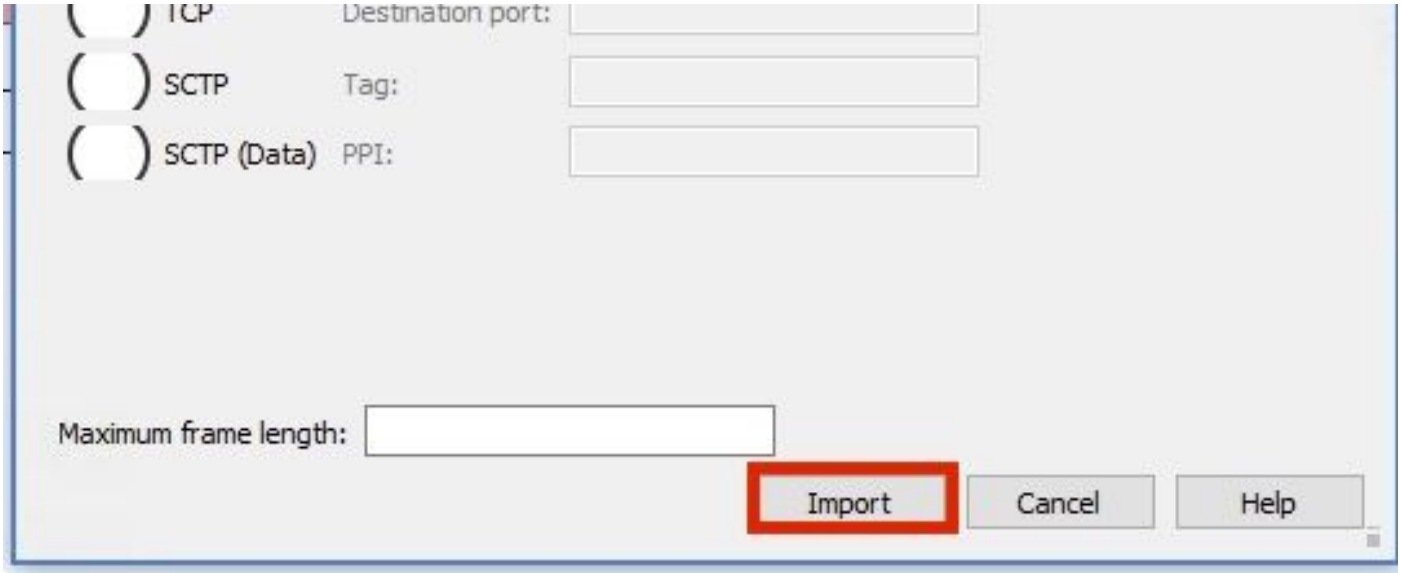

Passaggio 3. Fare clic su **Sfoglia.**



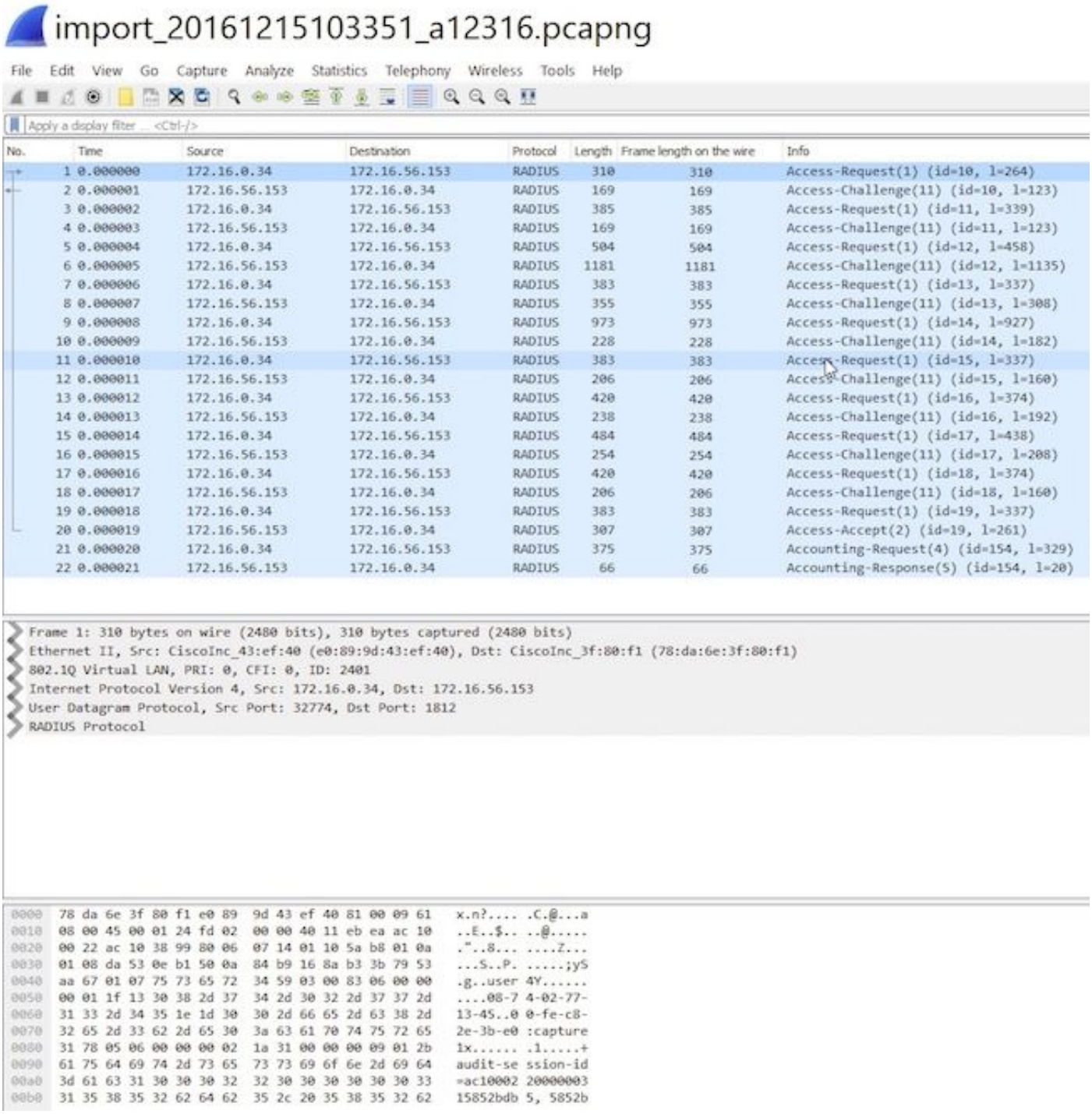

Passaggio 4. Selezionare il file di testo in cui è stato salvato l'output di registrazione dei pacchetti.




Passaggio 5. Fare clic su **Importa.**




Wireshark visualizza il file come .pcap.




**Nota:** Tenere presente che i timestamp non sono accurati né il tempo delta tra i fotogrammi.

# Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

### Informazioni correlate

- Dump pacchetto AP
- Nozioni fondamentali sullo sniffing wireless 802.11
- Documentazione e supporto tecnico – Cisco Systems