Configurar capturas de pacote de informação em AireOS WLC

Índice

Introdução

Este original descreve como executar uma descarga do pacote em um Wireless LAN Controller(WLC) de AireOS. Este método indica os pacotes enviados e/ou recebido a nível CPU do WLC encantar dentro o formato, que seja traduzido então a um arquivo .pcap com o Wireshark.

É útil nos casos onde uma comunicação entre um WLC e um server do Remote Authentication Dial-In User Service (RADIUS), um Access Point (AP) ou outros controladores precisa de ser verificada em uma maneira rápida com uma captura de pacote de informação a nível WLC mas um porta-período é duro de executar.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso do comando line interface(cli) ao WLC, preferivelmente SSH desde que a saída é mais rápida do que o console.
- O PC com Wireshark instalou

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC v8.3
- Wireshark v2 ou mais tarde

Note: Esta característica está disponível desde a versão 4 de AireOS.

Limitações

O registro do pacote capturará somente o plano bidirecional do controle (CP) aos pacotes do plano dos dados (DP) no WLC. Aqueles pacotes que não são enviados dos dados WLC aplanam para/desde o plano do controle (isto é estrangeiro para ancorar e assim por diante o tráfego em túnel, as gotas DP-CP) não serão capturados.

Os exemplos dos tipos de tráfego para/desde o WLC processados no CP são:

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP:
- NTP
- RADIUS
- TACACS+
- Mensagens da mobilidade
- Controle CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

O tráfego para/desde o cliente é processado no plano dos dados (DP) à exceção de: Gerenciamento do 802.11, 802.1X/EAPOL, ARP, DHCP e autenticação da Web.

Configurar

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Permita o pacote que entra o WLC

Etapa 1. Início de uma sessão ao CLI do WLC.

Devido à quantidade e à velocidade dos logs que estes exibições de recursos é recomendado entrar ao WLC pelo SSH e não pelo console.

Etapa 2. Aplique um Access Control List (ACL) para limitar que tráfego é capturado.

No exemplo dado a captação mostra o tráfego para/desde a interface de gerenciamento do WLC (endereço IP 172.16.0.34) e o servidor 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
```

Dica: Para capturar todo o tráfego para/desde o WLC recomenda-se aplicar um ACL que

rejeite o tráfego SSH para/desde o host que iniciou a sessão SSH. Estes são os comandos que você pode usar para construir o ACL:

>debugar o pacote que registra acl IP 1 negam o <host-IP> tcp 22 <WLC-IP>
>debugar o pacote que registra acl IP 2 negam ao <host-IP> <WLC-IP> tcp quaisquer 22
>debugar o pacote registrando a licença acl IP 3 alguma

Etapa 3. Configurar o formato legível por Wireshark.

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

Etapa 4. Permita recursos de registro do pacote.

Este exemplo mostra como capturar 100 recebidos/pacotes transmitido (apoia 1 - 65535 pacotes):

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

Nota: À revelia, registra somente 25 pacotes recebidos com o comando debug o **registro do pacote que permite**.

Note: Em vez de **tudo** você pode usar o **RX** ou o **TX** para capturar tráfego somente recebido ou transmitido.

Para uns detalhes mais adicionais sobre configurar recursos de registro do pacote consulte este link:

Guia de configuração de controle do Cisco Wireless, liberação 8.3, usando a facilidade debugar

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Use o comando dado verificar a configuração atual do registro do pacote.

```
> 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
```

Reproduza o comportamento necessário para gerar o tráfego.

Uma saída similar a esta aparece:

```
> 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
```

Remova os ACL do registro do pacote

A fim desabilitar os filtros aplicados pelos ACL use estes comandos:

```
> 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
```

Desabilite o registro do pacote

A fim desabilitar o pacote que registra sem remover os ACL use simplesmente este comando:

```
> 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
```

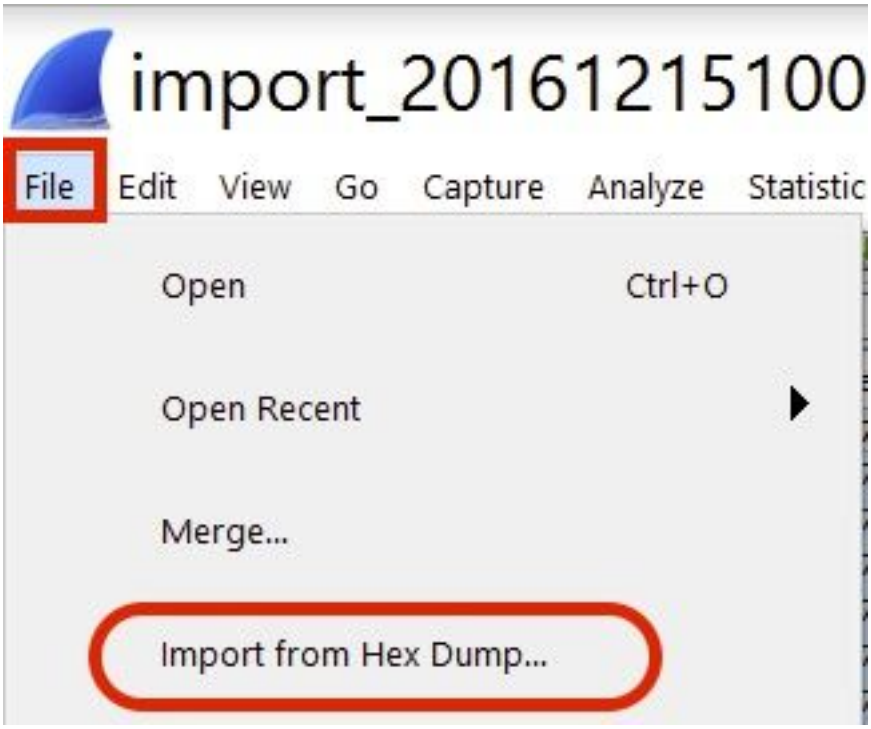
```
    [4]: disabled
    [5]: disabled
    [6]: disabled
  Ethernet ACL:
    [1]: disabled
    [2]: disabled
    [3]: disabled
    [4]: disabled
    [5]: disabled
    [6]: disabled
  IP ACL:
    [1]: permit s=172.16.0.34 d=172.16.56.153 any
    [2]: permit s=172.16.56.153 d=172.16.0.34 any
    [3]: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

Converta saídas de registro do pacote a um arquivo .pcap

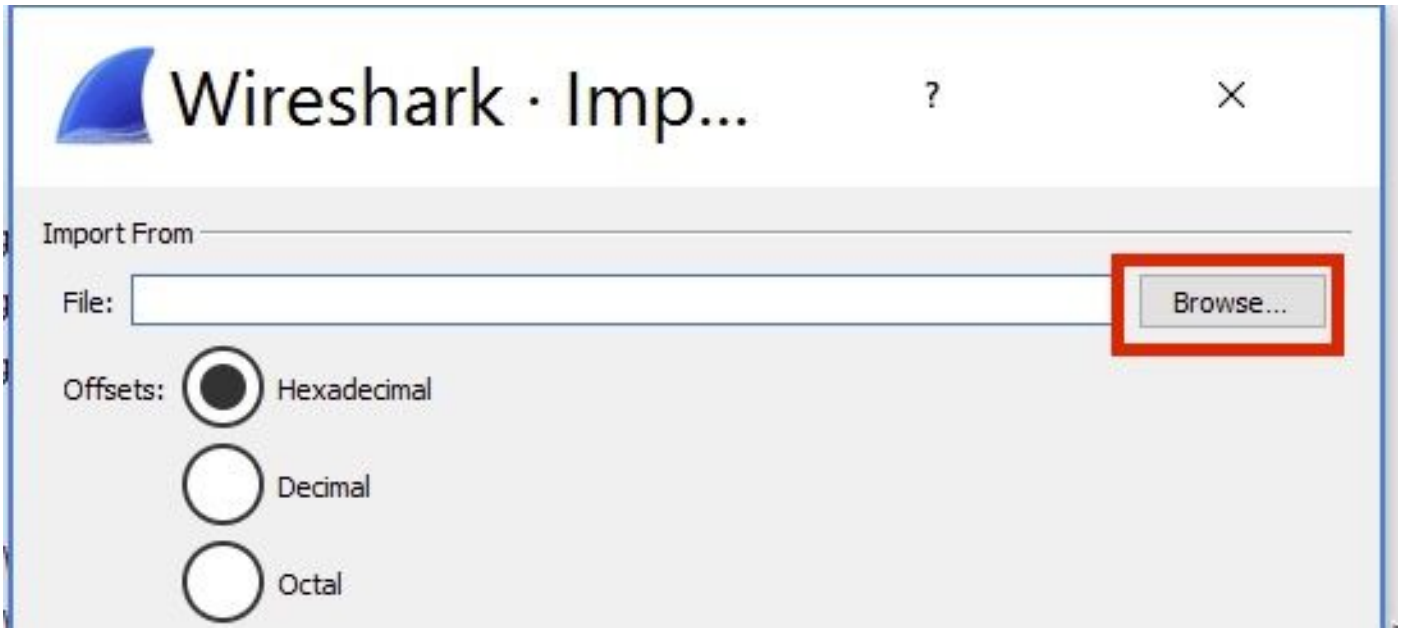
Etapa 1. Uma vez que a saída termina, recolha-a e salvar à um arquivo de texto.

Assegure que você recolhe um log limpo, se não Wireshark pôde mostrar pacotes corrupto.

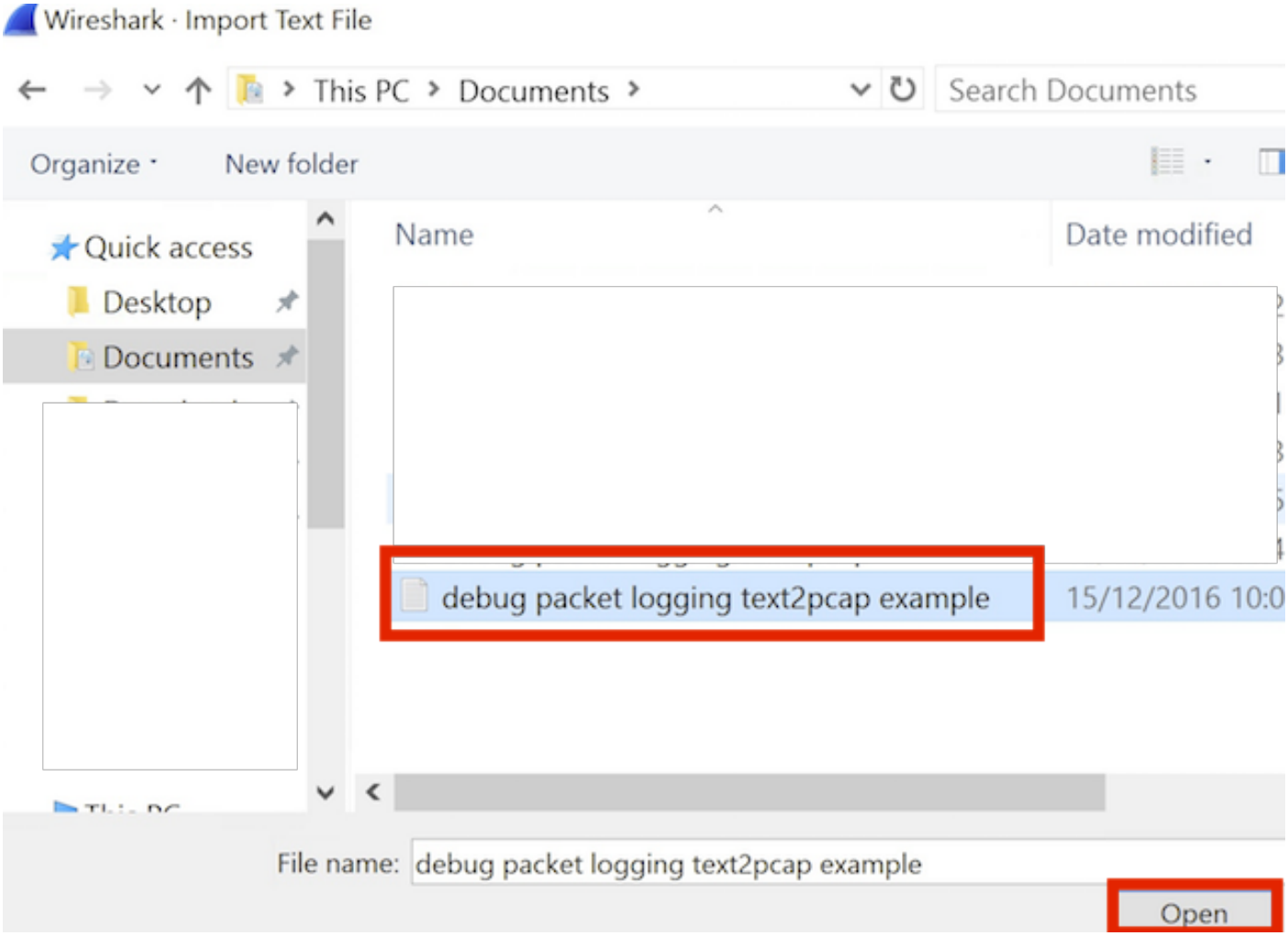
Etapa 2. Abra Wireshark e navegue **para arquivar o >Import da cópia parcial da memória de HEX...**



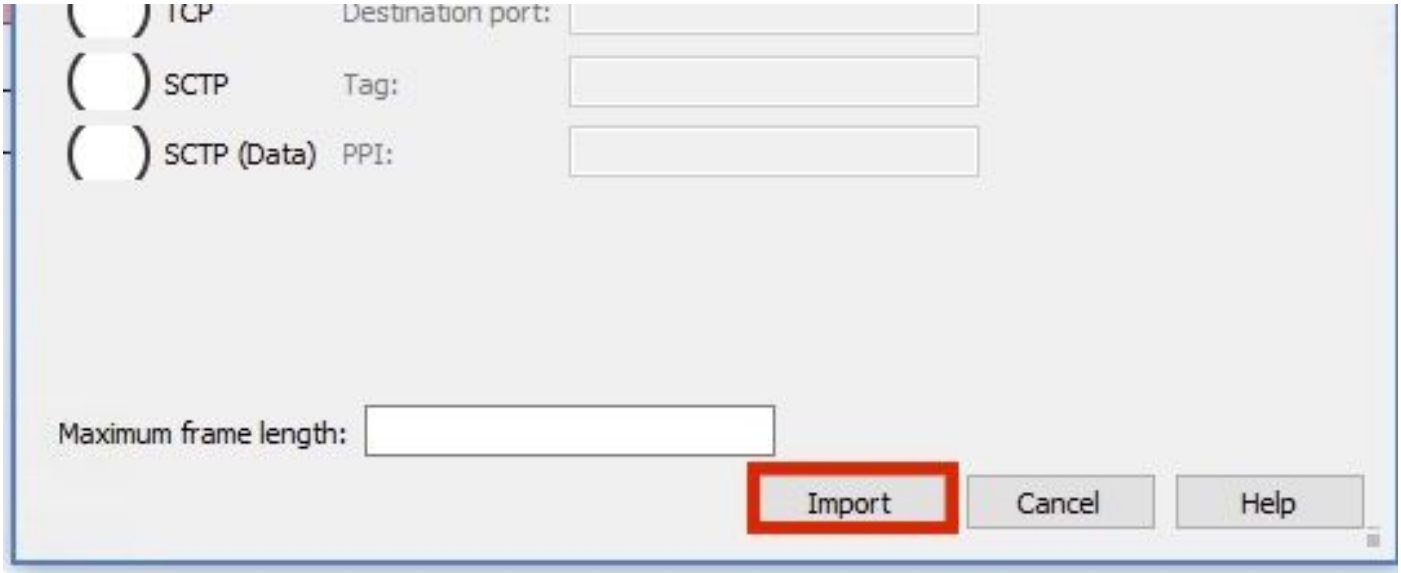
Etapa 3. O clique **consulta.**



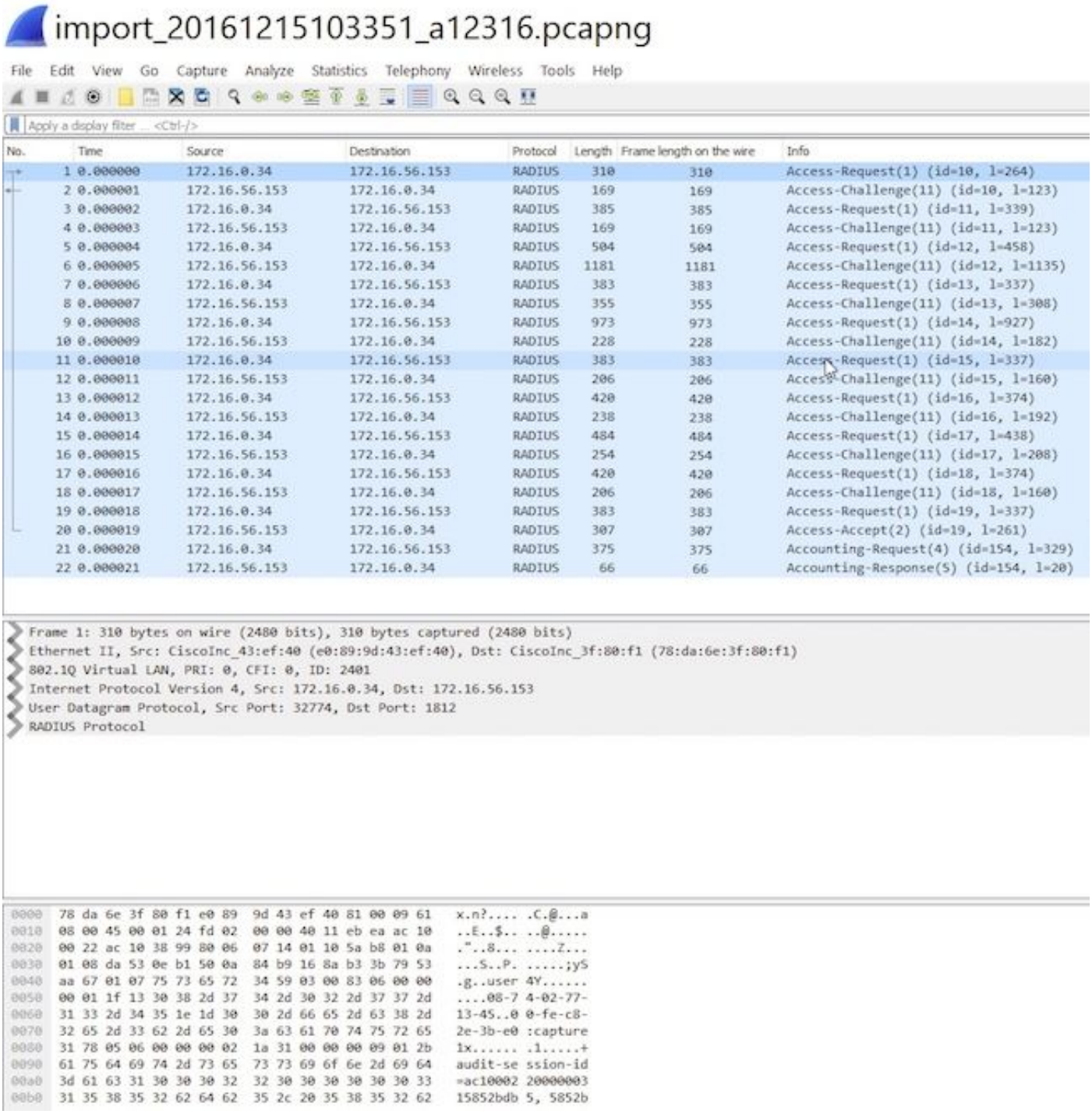
Etapa 4. Selecione o arquivo de texto onde você salvar as saídas de registro do pacote.



Etapa 5. **Importação do** clique.



Wireshark mostra o arquivo como .pcap.



Note: Esteja ciente que os selos de tempo não são exatos nem o tempo delta entre os quadros.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Descarga do pacote AP
- Fundamentos do sniffing wireless do 802.11

- Suporte Técnico e Documentação - Cisco Systems