Настройте захваты пакета на AireOS WLC

Содержание

Введение

Этот документ описывает, как выполнить пакетный дамп на Контроллере беспроводной локальной сети (WLC) AireOS. Этот метод отображает пакеты, переданные и/или полученные на уровне процессоров WLC в шестнадцатеричном формате, который тогда можно быть преобразован в .pcap файл с Wireshark.

Полезно в случаях, где связь между WLC и сервером Сервиса RADIUS, Точка доступа (AP) или другие контроллеры должны быть проверены в быстром способе с захватом пакета на уровне WLC, но промежуток порта трудно выполнить.

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Доступ интерфейса командной строки (CLI) к WLC, предпочтительно SSH, так как выходные данные быстрее, чем консоль.
- ПК с установленным Wireshark

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WLC v8.3
- Wireshark v2 или позже

Примечание: Эта функция доступна начиная с версии 4 AireOS.

Ограничения

Пакетная регистрация перехватит только двунаправленный Уровень управления (CP) к

пакетам Плоскости данных (DP) в WLC. Те пакеты, которые не переданы от уровня управления к/ота плоскости Данных WLC (т.е. внешний к туннельному трафику привязки, отбрасываниям CP DP и так далее) не будут перехвачены.

Примеры к/ота типов трафика WLC, обработанный в CP :

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS +
- Сообщения мобильности
- Контроль CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Системный журнал
- IAPP

К/от трафика клиент обработан в Плоскости данных (DP) за исключением: управление 802.11, 802.1X/EAPOL, ARP, DHCP и Web-аутентификация.

Настройка

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Включите пакет , входящий в WLC

Шаг 1. Войдите к CLI WLC.

Из-за количества и скорости журналов, что это отображения характеристик рекомендуется войти к WLC SSH а не консолью.

Шаг 2. Примените Список контроля доступа (ACL) для ограничения, какой трафик перехвачен.

В данном примере перехват показывает к/оту трафика интерфейс управления WLC (IP-адрес 172.16.0.34) и сервер 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
```

Совет: Для получения всего к/ота трафика WLC, рекомендуется применить ACL, который сбрасывает от к/ота трафика SSH хост, который инициировал Сеанс SSH. Это

команды, которые можно использовать для построения ACL:

>acl ip 1 регистрации debug packet запрещает <IP WLC> <IP - адрес хоста> tcp 22 любой
>acl ip 2 регистрации debug packet запрещает <IP - адрес хоста> <IP WLC> tcp любые 22
>debug packet, регистрирующий acl ip 3, разрешает любому любого

Шаг 3. Настройте формат, читаемый Wireshark.

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

Шаг 4. . Включите пакетную характеристику входа в систему.

Данный пример показывает, как перехватить 100 полученных/передаваемых пакетов (он поддерживает 1 - 65535 пакетов):

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

Примечание: По умолчанию это только регистрирует 25 полученных пакетов с **logging enable команды debug packet**.

Примечание: Вместо **всего** можно использовать **rx** или **tx** для получения только полученного или передаваемого трафика.

Для получения дальнейшей информации о настройке пакетной характеристики входа в систему консультируются с этой ссылкой:

Руководство конфигурации контроллера беспроводной связи Cisco, выпуск 8.3, Использование средства отладки

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Используйте данную команду для проверки текущей конфигурации пакетной регистрации.

```
> 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
```

Воспроизведите необходимое поведение генерировать трафик.

Появляются выходные данные, подобные этому:

```
> 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
```

Удалите ACL из пакетной регистрации

Для отключения фильтров, примененных использованием ACL эти команды:

```
> 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
```

Отключите пакетную регистрацию

Для отключения пакетной регистрации, не удаляя ACL, просто используют эту команду:

```
> 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
```

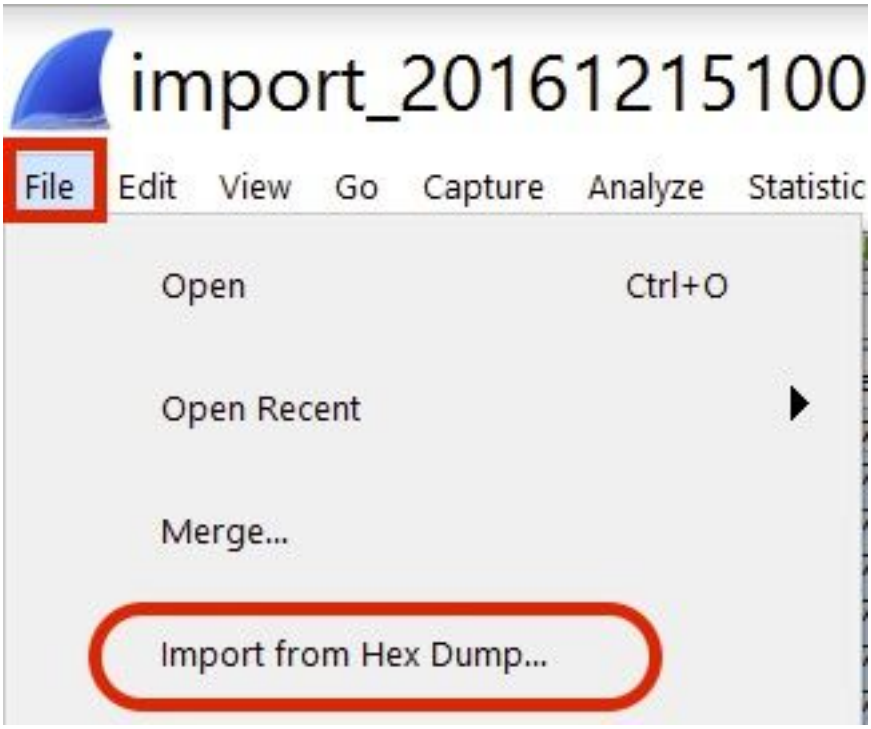
```
    [5]: disabled
    [6]: disabled
IP ACL:
    [1]: permit s=172.16.0.34 d=172.16.56.153 any
    [2]: permit s=172.16.56.153 d=172.16.0.34 any
    [3]: disabled
    [4]: disabled
    [5]: disabled
    [6]: disabled
EoIP-Ethernet ACL:
    [1]: disabled
    [2]: disabled
    [3]: disabled
    [4]: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

Преобразуйте пакетную регистрацию вывода в .pcap файл

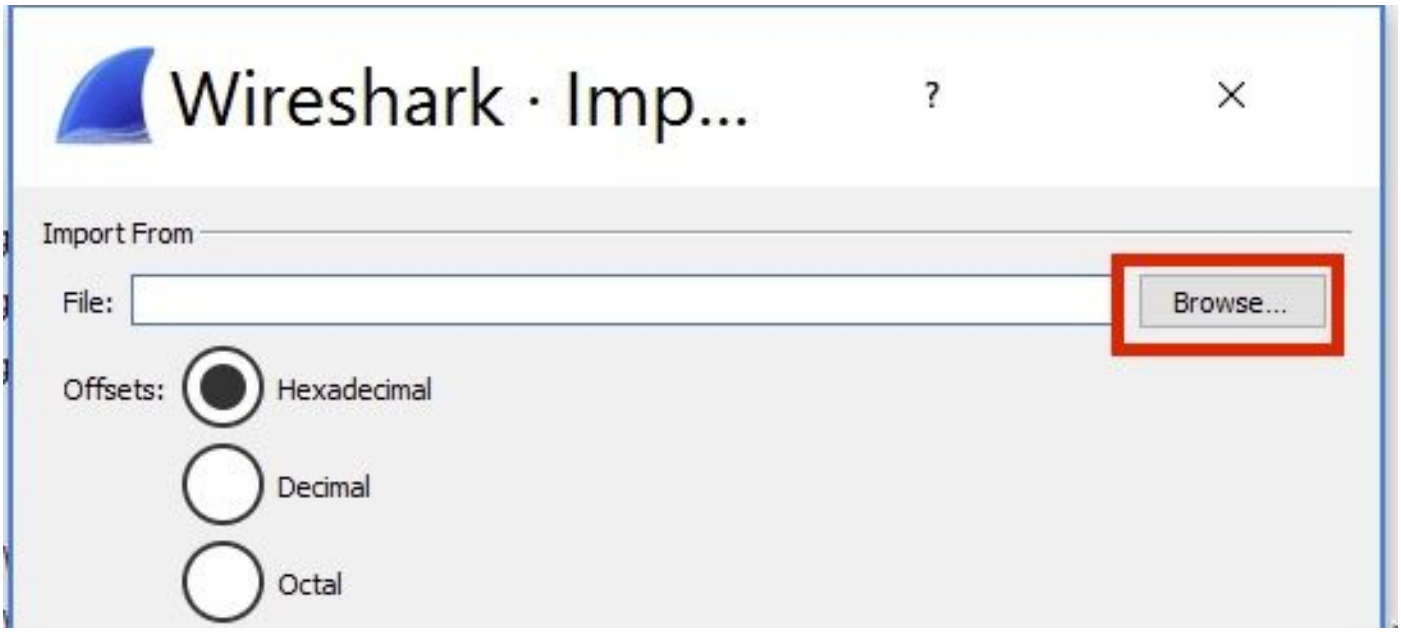
Шаг 1. Как только выходные данные заканчиваются, соберите их и сохраните их к текстовому файлу.

Гарантируйте сбор чистого журнала иначе Wireshark мог бы показать поврежденные пакеты.

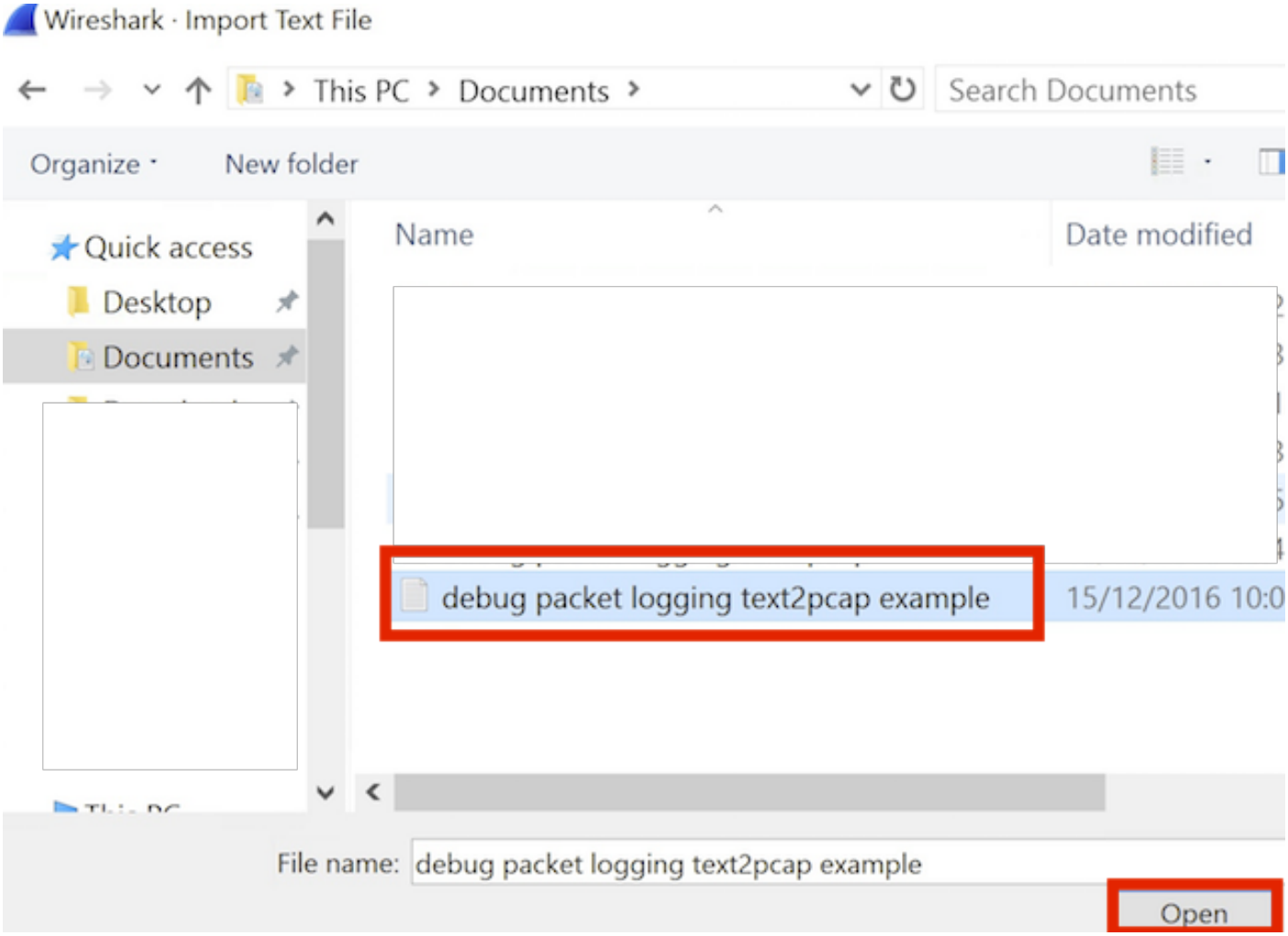
Шаг 2. Открытый Wireshark и перешел к **Файлу> Импорт от Шестнадцатеричного дампа...**



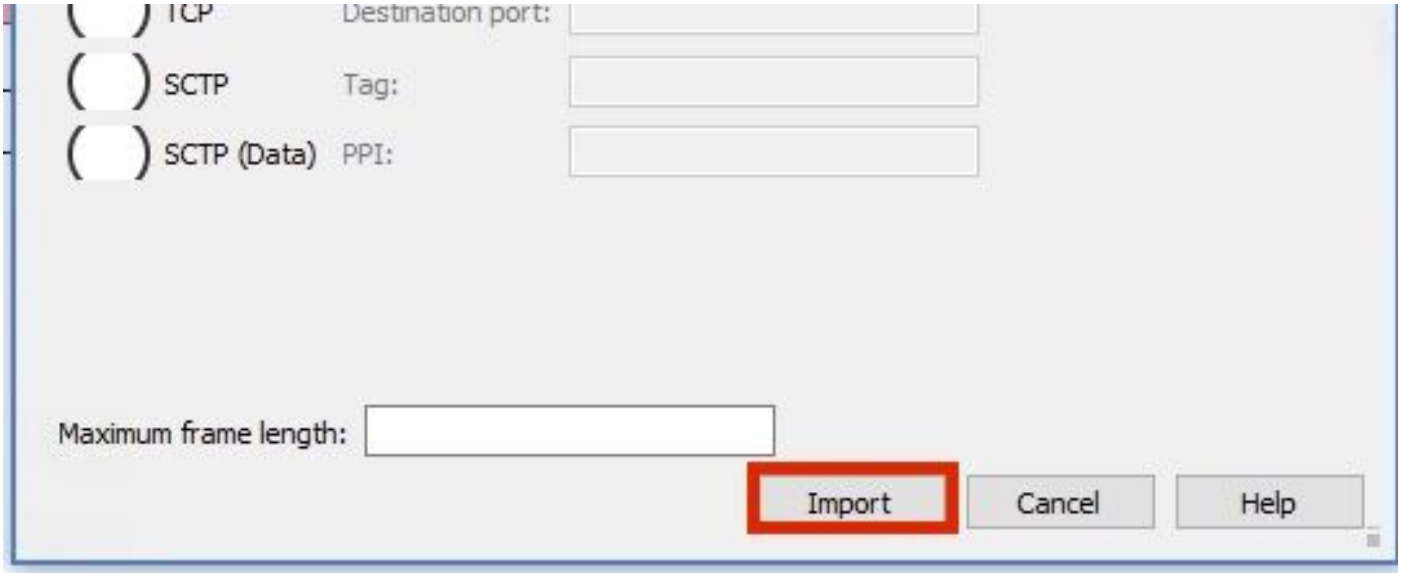
Шаг 3. **Нажмите кнопку Browse.**



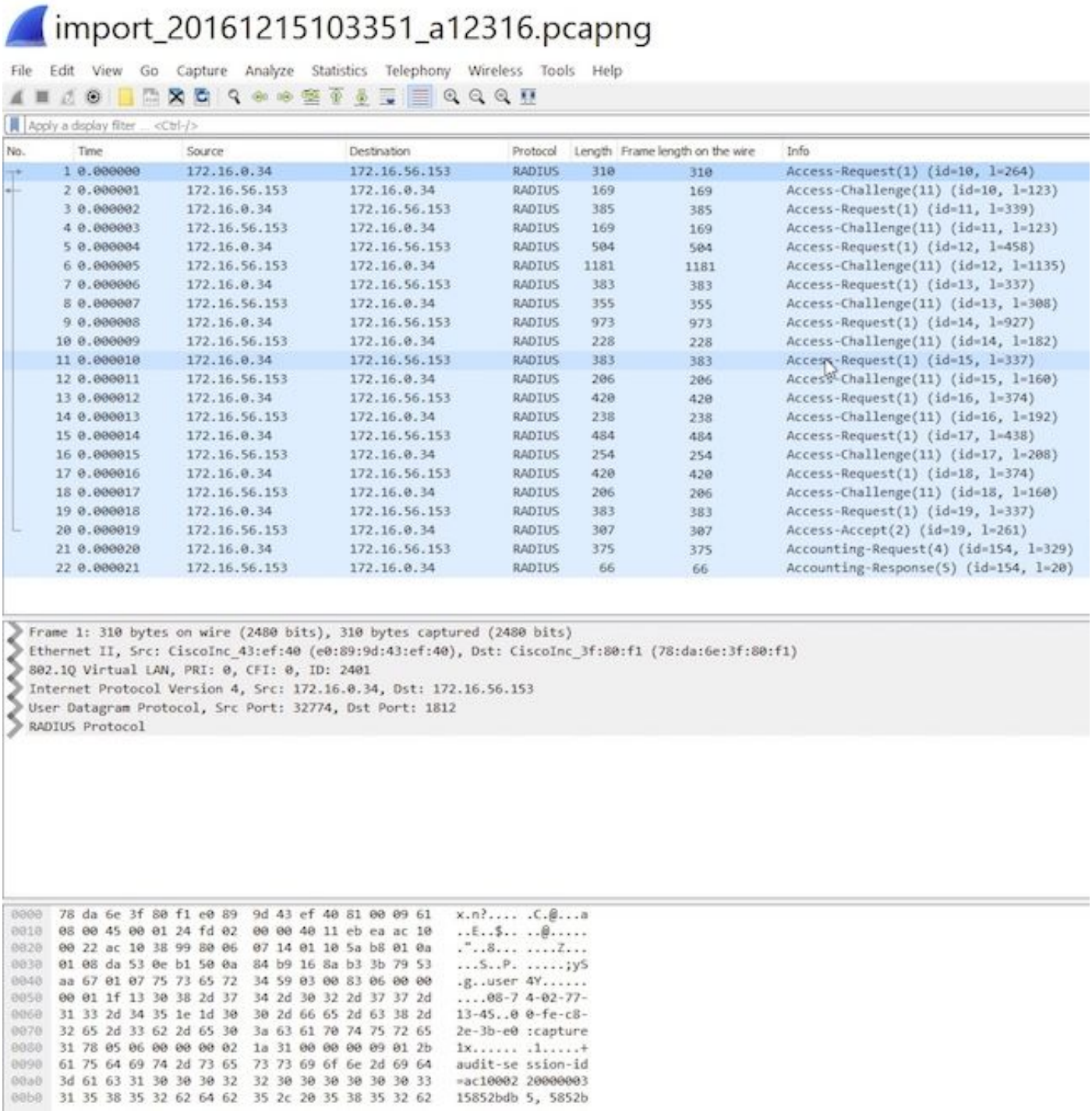
Шаг 4. . Выберите текстовый файл, где вы сохранили пакетную регистрацию вывода.



Шаг 5. . **Нажмите кнопку Import (Импортировать).**



Wireshark показывает файл как .pcap.



Примечание: Знайте, что штампы времени не точны, ни временной промежуток между кадрами.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Пакетный дамп AP
- Основные принципы сниффинга беспроводных сетей 802.11
- Cisco Systems – техническая поддержка и документация