

AireOS WLC에서 패킷 캡처 구성

목차

[소개](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[제한 사항](#)

[배경 정보](#)

[구성](#)

[WLC에서 패킷 로깅 활성화](#)

[다음을 확인합니다.](#)

[패킷 로깅 출력을 .pcap 파일로 변환](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 AireOS WLC(Wireless LAN Controller)에서 패킷 덤프를 실행하는 방법에 대해 설명합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC에 대한 CLI(명령줄 인터페이스) 액세스
- Wireshark가 설치된 PC

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- WLC v8.3
- Wireshark v2 이상



참고: 이 기능은 AireOS 버전 4부터 사용할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

제한 사항

패킷 로깅은 WLC의 양방향 CP(Control Plane) - DP(Data Plane) 패킷만 캡처합니다. WLC 데이터 플레인에서 제어 플레인으로/제어 플레인에서 전송되지 않는 패킷(즉, 외부 터널링된 트래픽, DP-CP 삭제 등)은 캡처할 수 없습니다.

CP에서 처리되는 WLC에서 주고받는 트래픽 유형의 예는 다음과 같습니다.

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- 모빌리티 메시지
- CAPWAP 컨트롤
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

클라이언트에서 나가고 들어오는 트래픽은 802.11 관리, 802.1X/EAPOL, ARP, DHCP 및 웹 인증을 제외하고 DP(Data Plane)에서 처리됩니다.

배경 정보

이 방법은 WLC의 CPU 레벨에서 전송 및/또는 수신된 패킷을 16진수 형식으로 표시한 다음 Wireshark를 사용하여 .pcap 파일로 변환합니다. WLC와 RADIUS(Remote Authentication Dial-In User Service) 서버, AP(Access Point) 또는 기타 컨트롤러 간의 통신을 WLC 레벨에서 패킷 캡처를 통해 신속하게 확인해야 하지만 포트 스캔을 수행하기 어려운 경우 유용합니다.

구성

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

WLC에서 패킷 로깅 활성화

1단계. WLC CLI에 로그인합니다.

이 기능에 표시되는 로그의 양과 속도로 인해 콘솔이 아닌 SSH로 WLC에 로그인하는 것이 좋습니다(콘솔보다 출력이 더 빠르므로 SSH가 기본 설정됨).

2단계. 캡처할 트래픽을 제한하려면 ACL(Access Control List)을 적용합니다.

주어진 예에서 캡처는 WLC 관리 인터페이스(IP 주소 172.16.0.34) 및 RADIUS 서버

(172.16.56.153)와 주고받는 트래픽을 보여줍니다.


```
<#root>
```

```
>
```

```
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
```

 **팁:** WLC를 오가는 모든 트래픽을 캡처하려면 SSH 세션을 시작한 호스트에서 오가는 SSH 트래픽을 폐기하는 ACL을 적용하는 것이 좋습니다. 다음은 ACL을 구축하는 데 사용할 수 있는 명령입니다.

```
> 디버그 패킷 로깅 acl ip 1 deny <WLC-IP> <host-IP> tcp 22 any
> 디버그 패킷 로깅 acl ip 2 deny <host-IP> <WLC-IP> tcp any 22
> 디버그 패킷 로깅 acl ip 3 permit any any
```

3단계. Wireshark에서 읽을 수 있는 형식을 구성합니다.

```
<#root>
```

```
>
```

```
debug packet logging format text2pcap
```

4단계. 패킷 로깅 기능을 활성화합니다.

다음 예에서는 100개의 수신/전송 패킷을 캡처하는 방법을 보여 줍니다(1~65535개의 패킷 지원).


```
<#root>
```


```
>
```

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

5단계. 출력을 텍스트 파일에 기록합니다.

 **참고:** 기본적으로 debug packet logging enable 명령을 사용하여 25개의 수신된 패킷만 로깅

 합니다.

 참고: 모든 트래픽 대신 rx 또는 tx를 사용하여 수신 또는 전송된 트래픽만 캡처할 수 있습니다.

패킷 로깅 기능 구성에 대한 자세한 내용은 다음 링크를 참조하십시오.

[Cisco Wireless Controller 컨피그레이션 가이드, 릴리스 8.3, 디버그 기능 사용](#)

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

지정된 명령을 사용하여 패킷 로깅의 현재 컨피그레이션을 확인합니다.

```
<#root>
```

```
>
```

```
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

```

필요한 동작을 재현하여 트래픽을 생성합니다.

다음과 유사한 출력이 나타납니다.

```

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...

```

패킷 로깅에서 ACL 제거

ACL에 의해 적용되는 필터를 비활성화하려면 다음 명령을 사용합니다.

```
<#root>
```

```
>
```

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

```
>
```

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

패킷 로깅 비활성화

ACL을 제거하지 않고 패킷 로깅을 비활성화하려면 다음 명령을 사용합니다.

```
<#root>
```

```
>
```

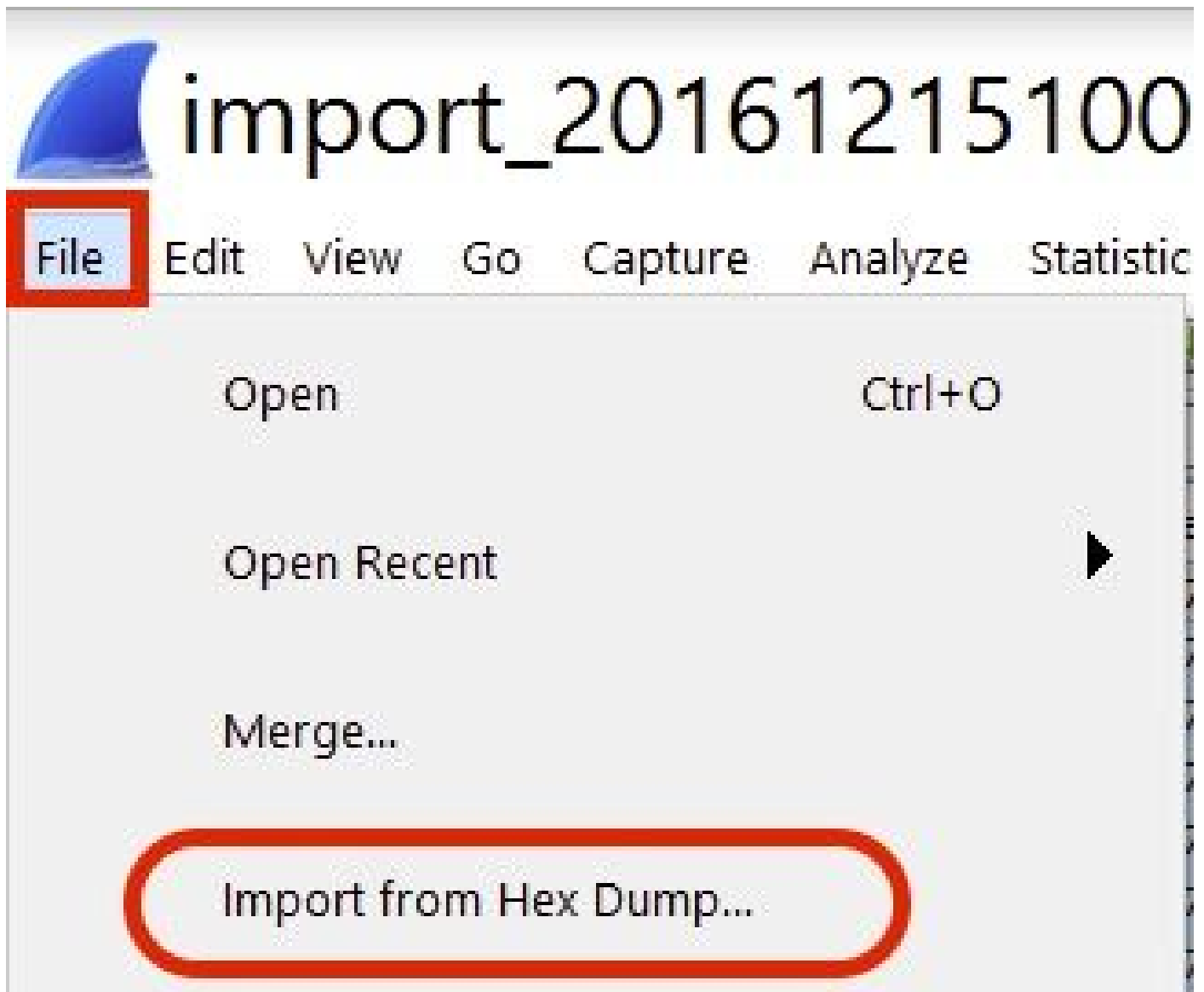
```
debug packet logging disable
```

패킷 로깅 출력을 .pcap 파일로 변환

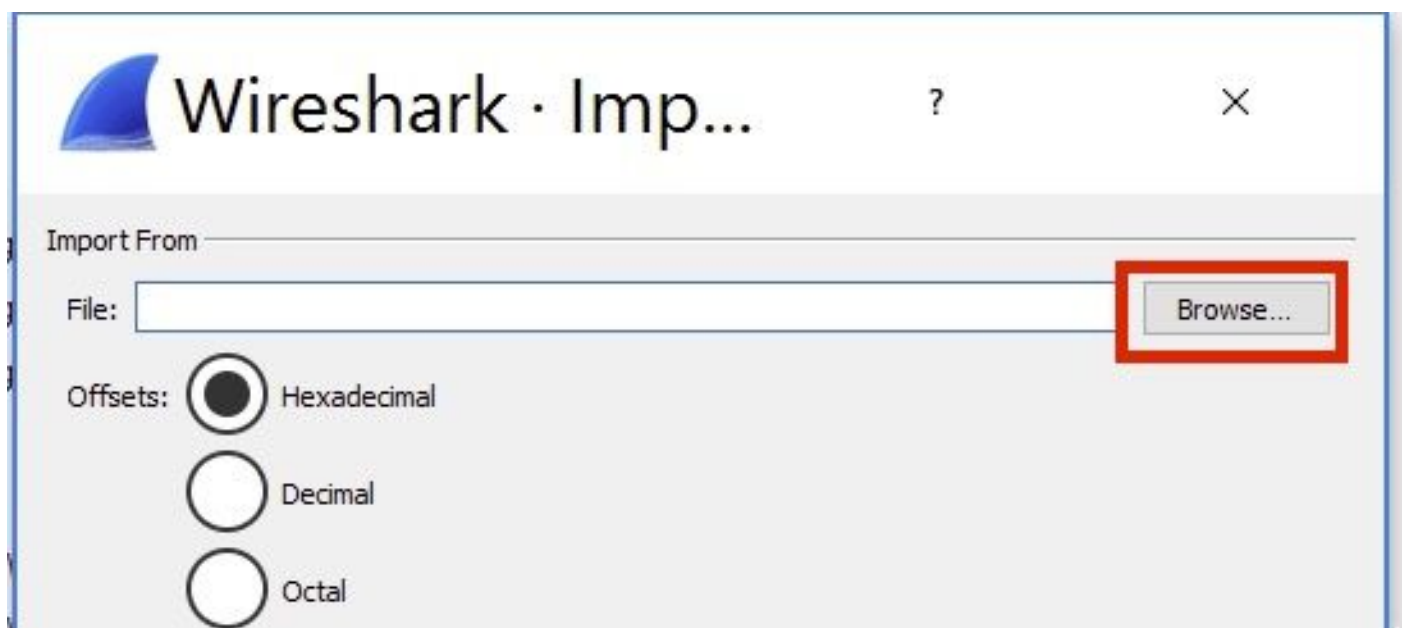
1단계. 출력이 완료되면 수집한 후 텍스트 파일에 저장합니다.

안전한 로그를 수집해야 합니다. 그렇지 않으면 Wireshark가 손상된 패킷을 표시할 수 있습니다.

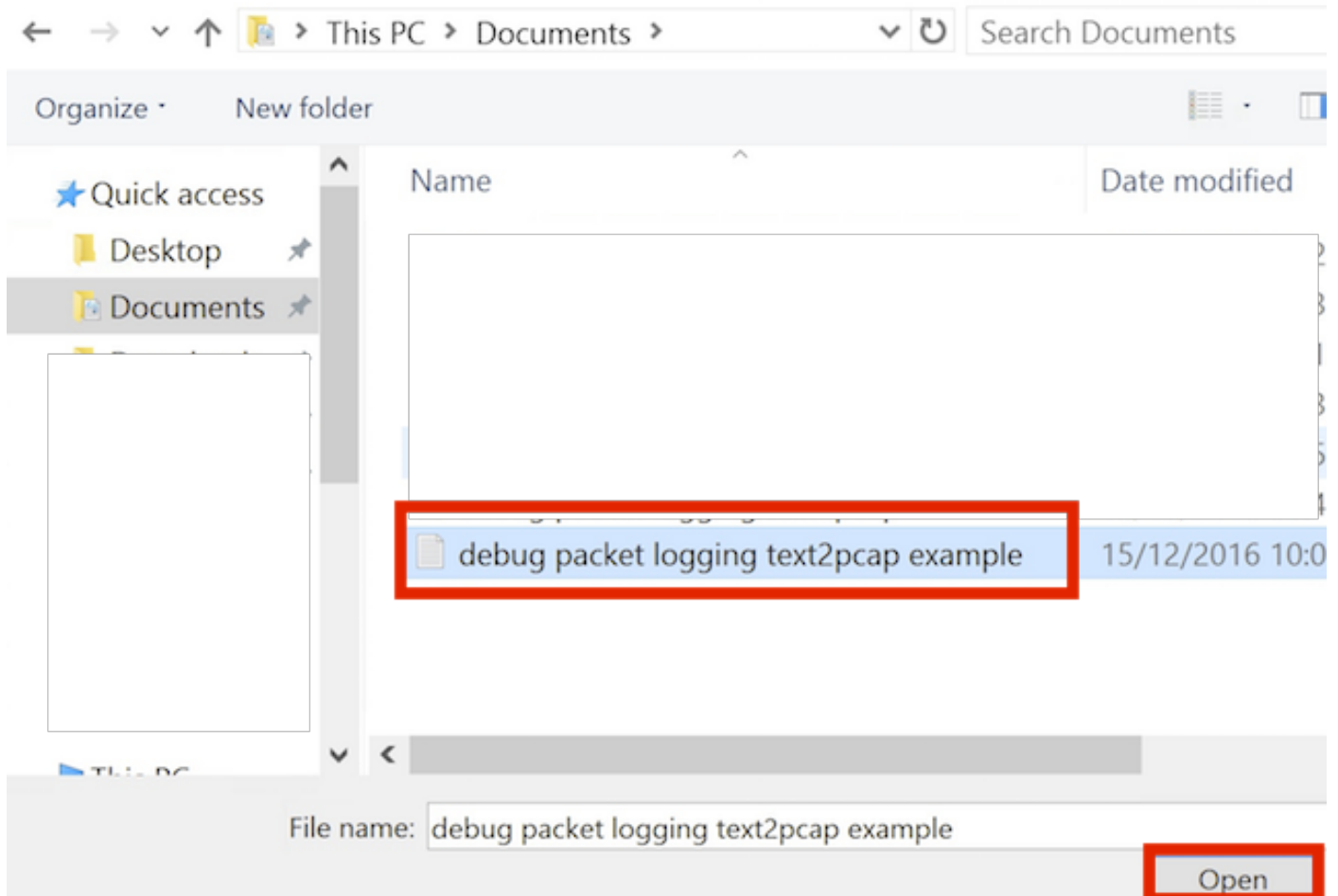
2단계. Wireshark를 열고 File>Import from Hex Dump...로 이동합니다.



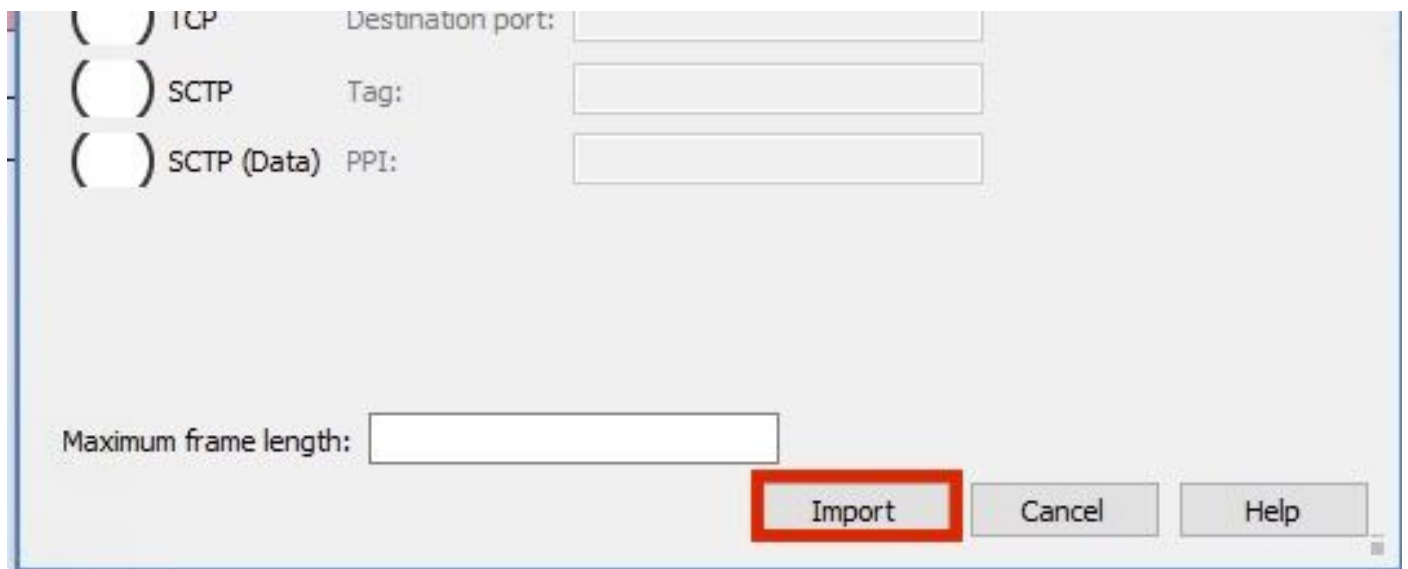
3단계. Browse(찾아보기)를 클릭합니다.



4단계. 패킷 로깅 출력을 저장한 텍스트 파일을 선택합니다.

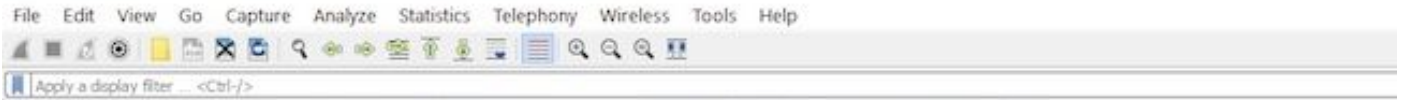


5단계. Import(가져오기)를 클릭합니다.



Wireshark는 파일을 .pcap로 표시합니다.

import_20161215103351_a12316.pcapng



No.	Time	Source	Destination	Protocol	Length	Frame length on the wire	Info
1	0.000000	172.16.0.34	172.16.56.153	RADIUS	310	310	Access-Request(1) (id=10, l=264)
2	0.000001	172.16.56.153	172.16.0.34	RADIUS	169	169	Access-Challenge(11) (id=10, l=123)
3	0.000002	172.16.0.34	172.16.56.153	RADIUS	385	385	Access-Request(1) (id=11, l=339)
4	0.000003	172.16.56.153	172.16.0.34	RADIUS	169	169	Access-Challenge(11) (id=11, l=123)
5	0.000004	172.16.0.34	172.16.56.153	RADIUS	504	504	Access-Request(1) (id=12, l=458)
6	0.000005	172.16.56.153	172.16.0.34	RADIUS	1181	1181	Access-Challenge(11) (id=12, l=1135)
7	0.000006	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=13, l=337)
8	0.000007	172.16.56.153	172.16.0.34	RADIUS	355	355	Access-Challenge(11) (id=13, l=308)
9	0.000008	172.16.0.34	172.16.56.153	RADIUS	973	973	Access-Request(1) (id=14, l=927)
10	0.000009	172.16.56.153	172.16.0.34	RADIUS	228	228	Access-Challenge(11) (id=14, l=182)
11	0.000010	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=15, l=337)
12	0.000011	172.16.56.153	172.16.0.34	RADIUS	206	206	Access-Challenge(11) (id=15, l=160)
13	0.000012	172.16.0.34	172.16.56.153	RADIUS	420	420	Access-Request(1) (id=16, l=374)
14	0.000013	172.16.56.153	172.16.0.34	RADIUS	238	238	Access-Challenge(11) (id=16, l=192)
15	0.000014	172.16.0.34	172.16.56.153	RADIUS	484	484	Access-Request(1) (id=17, l=438)
16	0.000015	172.16.56.153	172.16.0.34	RADIUS	254	254	Access-Challenge(11) (id=17, l=208)
17	0.000016	172.16.0.34	172.16.56.153	RADIUS	420	420	Access-Request(1) (id=18, l=374)
18	0.000017	172.16.56.153	172.16.0.34	RADIUS	206	206	Access-Challenge(11) (id=18, l=160)
19	0.000018	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=19, l=337)
20	0.000019	172.16.56.153	172.16.0.34	RADIUS	307	307	Access-Accept(2) (id=19, l=261)
21	0.000020	172.16.0.34	172.16.56.153	RADIUS	375	375	Accounting-Request(4) (id=154, l=329)
22	0.000021	172.16.56.153	172.16.0.34	RADIUS	66	66	Accounting-Response(5) (id=154, l=20)

```
Frame 1: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0
Ethernet II, Src: CiscoInc_43:ef:40 (e0:89:9d:43:ef:40), Dst: CiscoInc_3f:80:f1 (78:da:6e:3f:80:f1)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2401
Internet Protocol Version 4, Src: 172.16.0.34, Dst: 172.16.56.153
User Datagram Protocol, Src Port: 32774, Dst Port: 1812
RADIUS Protocol
```

```
0000 78 da 6e 3f 80 f1 e0 89 9d 43 ef 40 81 00 09 61  x.n?... .C.@...a
0010 08 00 45 00 01 24 fd 02 00 00 40 11 eb ea ac 10  ..E..$. .@.....
0020 00 22 ac 10 38 99 80 06 07 14 01 10 5a b8 01 0a  ."..8... ..Z...
0030 01 08 da 53 0e b1 50 0a 84 b9 16 8a b3 3b 79 53  ...S..P. ....;yS
0040 aa 67 01 07 75 73 65 72 34 59 03 00 83 06 00 00  .g..user 4Y.....
0050 00 01 1f 13 30 38 2d 37 34 2d 30 32 2d 37 37 2d  ...08-7 4-02-77-
0060 31 33 2d 34 35 1e 1d 30 30 2d 66 65 2d 63 38 2d  13-45..0 0-fe-c8-
0070 32 65 2d 33 62 2d 65 30 3a 63 61 70 74 75 72 65  2e-3b-e0 :capture
0080 31 78 05 06 00 00 00 02 1a 31 00 00 00 09 01 2b  1x..... .l.....+
0090 61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64  audit-se ssion-id
00a0 3d 61 63 31 30 30 30 32 32 30 30 30 30 30 30 33  =ac10002 20000003
00b0 31 35 38 35 32 62 64 62 35 2c 20 35 38 35 32 62  15852bdb 5, 5852b
```

참고: 타임스탬프는 정확하지 않으며 프레임 간의 델타 시간도 정확하지 않습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [AP 패킷 덤프](#)
- [802.11 무선 스니핑의 기본 사항](#)

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.