

# SD-WAN에 대한 WAN의 패킷 손실 확인 및 식별

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경](#)

[문제 해결 프로세스](#)

[개요 프로세스](#)

[DSCP로 원하는 트래픽 표시](#)

[내장형 캡처로 트래픽 캡처](#)

[Wireshark를 통한 분석](#)

[ESP 시퀀스로 원하는 트래픽 필터링](#)

[관련 정보](#)

## 소개

이 문서에서는 WAN에서 트래픽이 손실되었지만 SD-WAN 에지에서 삭제되지 않은 경우 데이터를 식별하고 수집하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(소프트웨어 정의 WAN)
- 내장형 패킷 캡처 또는 vManage 패킷 캡처
- 와이어샤크
- 마이크로소프트 엑셀

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

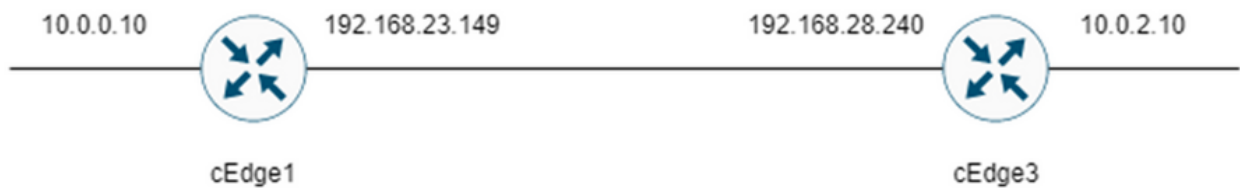
- C8000V 버전 17.03.04
- vManage 버전 20.3.4
- Wireshark 버전 2.6.3

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.

## 배경

이 문제를 해결하기 위해 이 문서에 설명된 단계에서는 특정 트래픽을 DSCP(Differentiated Services Code Point)로 표시하여 원하는 패킷을 식별하는 방법을 보여 줍니다. 이 값은 내부 패킷 헤더에서 IPsec 헤더로 복사되므로 DSCP를 사용하여 트래픽을 식별할 수 있습니다. 원하는 패킷이 식별되면 두 WAN 캡처 전체에서 트래픽을 매칭하여 소스에서 대상으로 트래픽이 전달되도록 하는 방법을 보여 줍니다.

두 개의 단일 라우터 사이트를 사용하여 이 트러블슈팅 기술을 시연합니다. 이 경우 이미지에 표시된 것처럼 100ping의 형태로 ICMP 트래픽이 10.0.0.10에서 10.0.2.10으로 전달됩니다. 이 예시에서는 손실이 없지만, 이것을 식별하기 위한 손실이 있는 경우에 이 동일한 트러블슈팅 기술이 사용됩니다.



## 문제 해결 프로세스

### 개요 프로세스

1. WAN을 통해 추적되는 트래픽의 경우, 일부 미사용 DSCP 값으로 트래픽을 표시하려면 ACL(Access List)(또는 중앙 집중식 정책)이 필요합니다. 이 예에서는 DSCP 27이 사용됩니다.
2. 트래픽이 표시되면 임베디드 패킷 캡처를 사용하여 소스 및 목적지 라우터의 전송 인터페이스에서 패킷을 캡처합니다.

**참고:** 5MB의 데이터 또는 5분의 런타임 제한에도 불구하고 vManage 패킷 캡처를 사용할 수 있습니다.

1. 캡처가 촬영되면 Wireshark에서 열어 봅니다.
2. Wireshark에서 필터를 적용하여 원하는 패킷을 표시한 다음 비교합니다.
3. Microsoft Excel은 정확성을 보장하기 위해 대용량 캡처에 사용됩니다.

### DSCP로 원하는 트래픽 표시

예시와 같은 액세스 목록은 소스 라우터(이 예시의 경우 cEdge1)에 구성되고 표시된 대로 라우터 컨피그레이션의 SD-WAN 부분에 있는 인터페이스에 적용됩니다.

선택적 카운터가 적용되어 트래픽이 예상대로 정책에 도달하는지 확인합니다. `show sdwan policy access-list-counters` 명령으로 확인할 수 있습니다.

```

policy
access-list mark_dscp_27
sequence 10
match
source-ip 10.0.0.10/32
destination-ip 10.0.2.10/32
!
action accept
count MARK_DSCP_27_COUNT (optional counter to verify packets that hit the policy)
set
dscp 27
!
!
!
default-action accept

sdwan
interface GigabitEthernet3
access-list mark_dscp_27 in

```

## 내장형 캡처로 트래픽 캡처

**참고:** Cisco IOS XE에서 임베디드 패킷 캡처를 구성하여 WAN을 통과하는 암호화된 패킷을 캡처하는 방법은 [Embedded Packet Capture for Cisco IOS and Cisco IOS XE Configuration Example](#)으로 이동합니다

**참고:** EPC에 대해 1000PPS rate-limit을 초과할 수 있으므로 ACL을 사용하여 WAN의 EPC를 제한해야 합니다.

예

ACL은 cEdge1 및 cEdge3에서 구성됩니다. 이 예에서는 트래픽이 소스에서 대상으로 가는 방향으로만 확인되기 때문입니다.

**참고:** WAN IP 주소는 캡처를 필터링하는 데 사용됩니다. ACL 필터에 대해 올바른 WAN IP를 식별할 수 있도록 트래픽의 경로를 식별하는 데 사용할 수 있는 여러 출력이 있습니다. 이 출력을 생성하는 데 사용할 수 있는 명령은 **show sdwan app-fwd cflowd flow** 및 **show sdwan policy service path**입니다. 디버그 조건의 [경우 Conditional Packet Trace\(조건부 패킷 추적\)](#)로 이동하십시오.

```

ip access-list extended CAP-Filter
10 permit ip host 192.168.23.149 host 192.168.28.240

```

이 시점에서 두 라우터에서 캡처가 시작되고 오버레이를 통해 100개의 ping이 전송됩니다.

```

#ping vrf 10 10.0.2.10 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.0.2.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

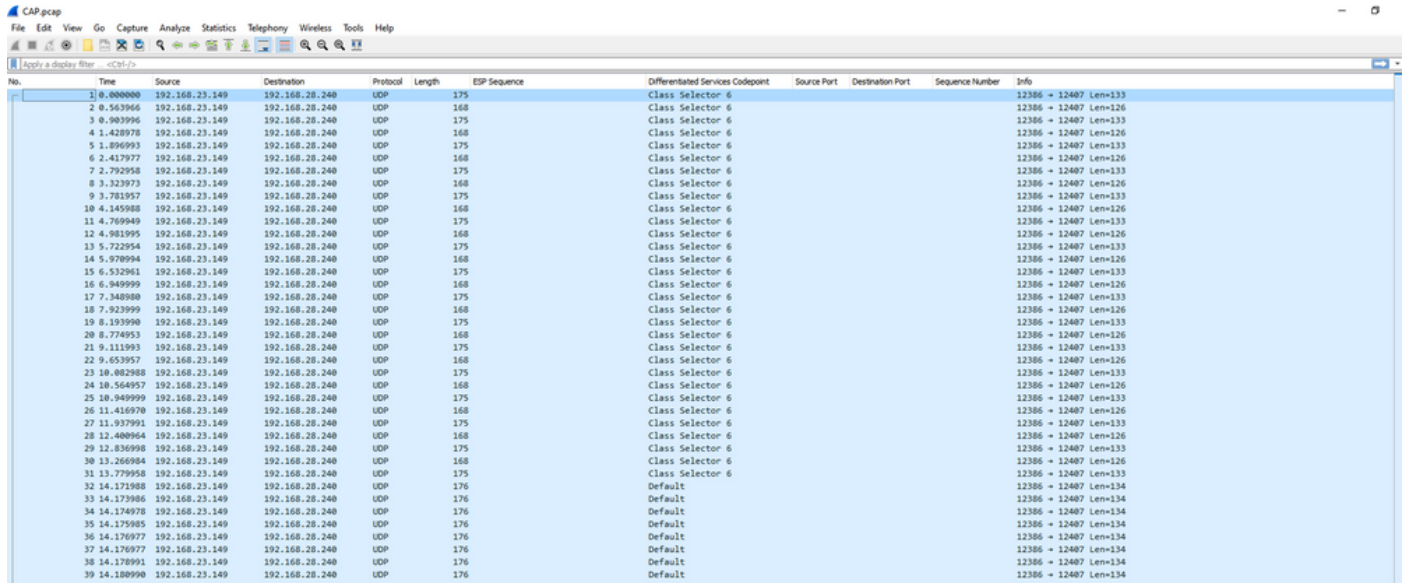
```

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms

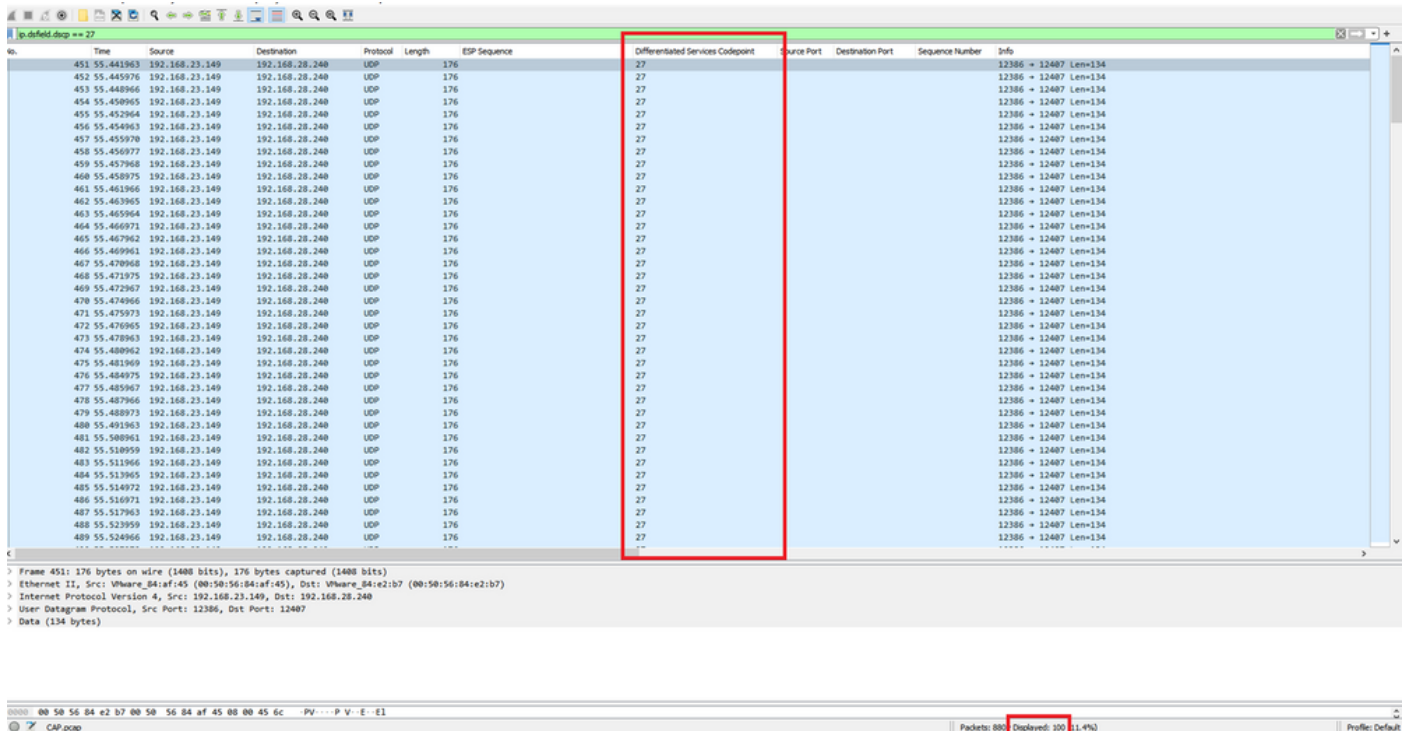
두 라우터에서 캡처가 중지되고 수집되면 이를 보려면 Wireshark에서 해당 캡처를 열어야 합니다.

# Wireshark를 통한 분석

Wireshark에서 cEdge1 캡처가 열리면 모든 트래픽이 암호화되며 어떤 패킷이 전송된 Ping인지 식별하기가 쉽지 않습니다.



이 캡처를 표시 필터 `ip.dsfield.dscp == 27`로 필터링하면 화면 하단에 100개의 패킷만 표시되고 DSCP 열 값에 모두 27이 표시됩니다.



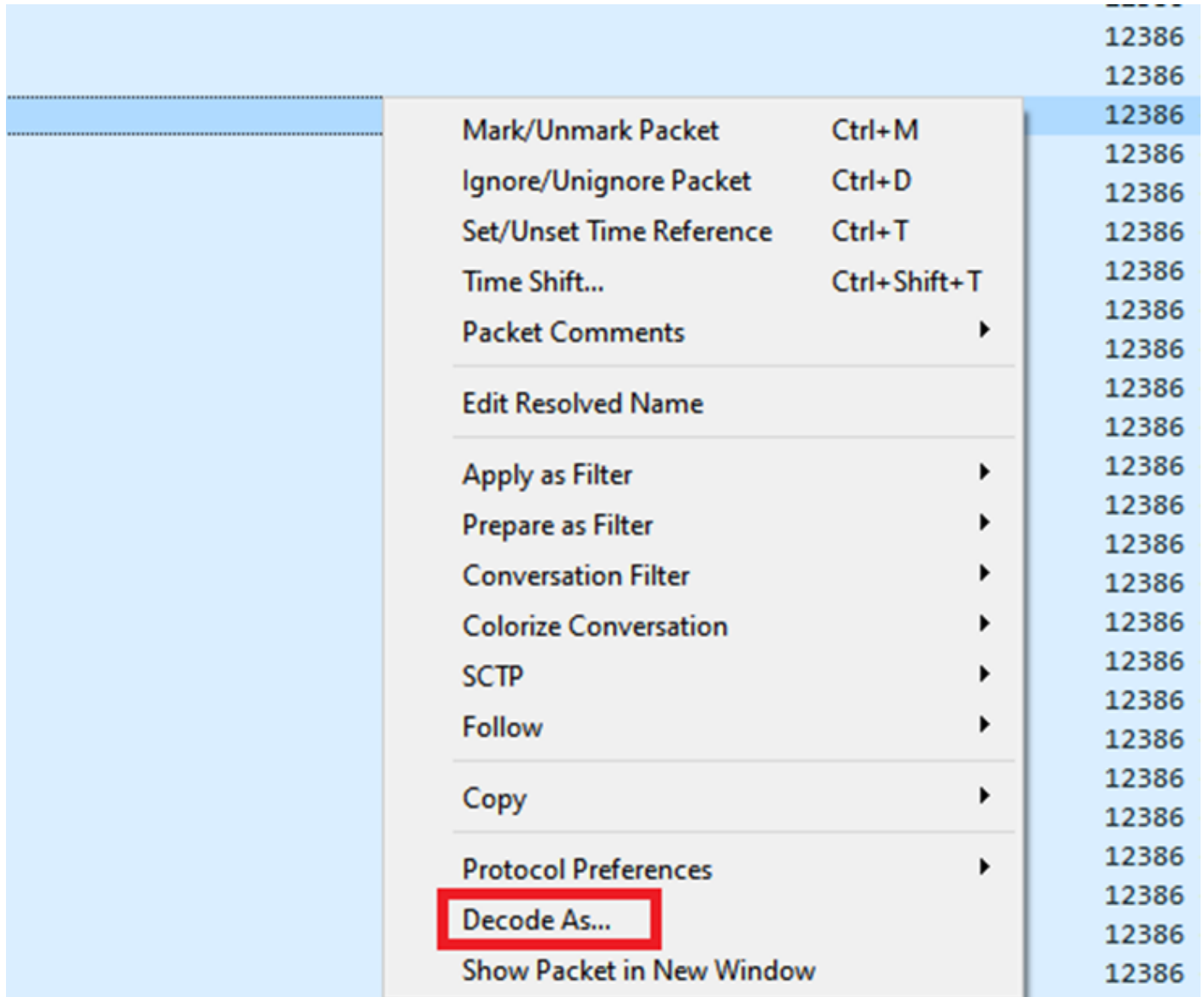
DSCP 값이 WAN에서 유지되는 일부 경우에는 대상 캡처에서 동일한 필터를 사용할 수 있습니다.

DSCP 값이 공용 인터넷 연결에서 지워지는 상황처럼 다른 경우에는 이 작업을 수행할 수 없습니다

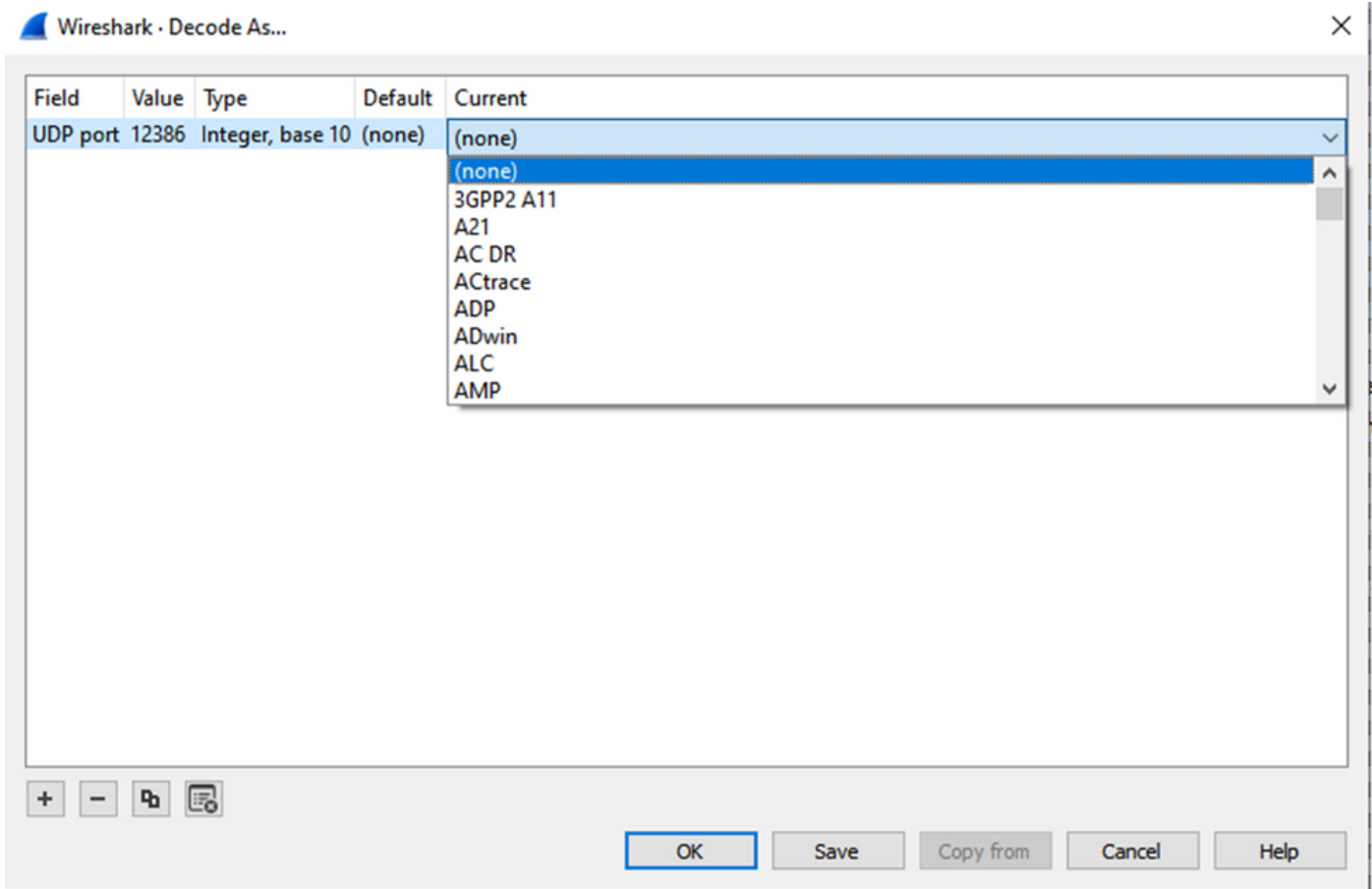
## ESP 시퀀스로 원하는 트래픽 필터링

어떤 경우든 트래픽은 ESP 시퀀스 번호로 식별할 수 있습니다.

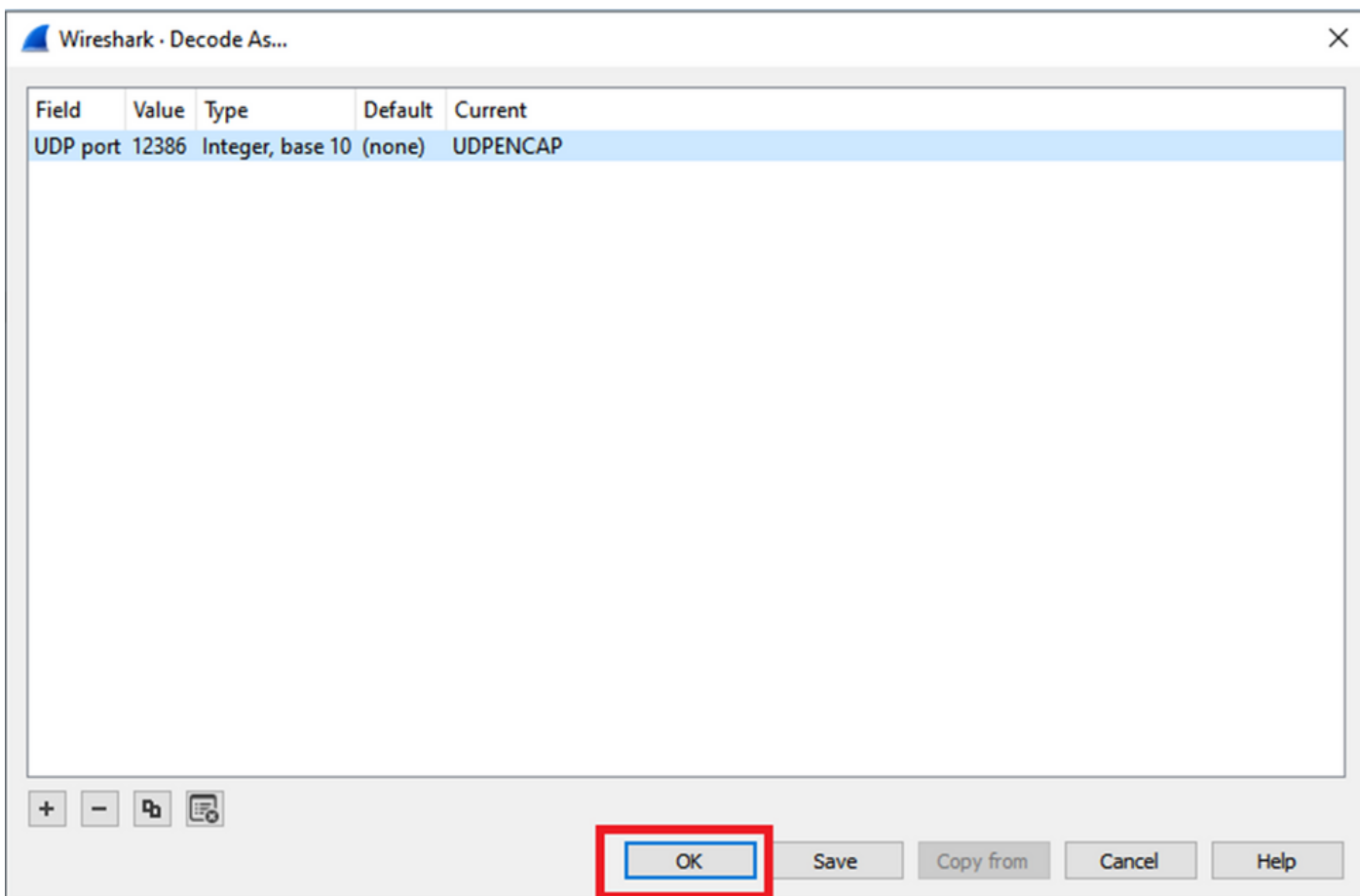
패킷의 ESP 시퀀스 번호를 보려면 마우스 오른쪽 버튼으로 캡처를 클릭하고 표시된 대로 Decode(디코딩)를 선택합니다.



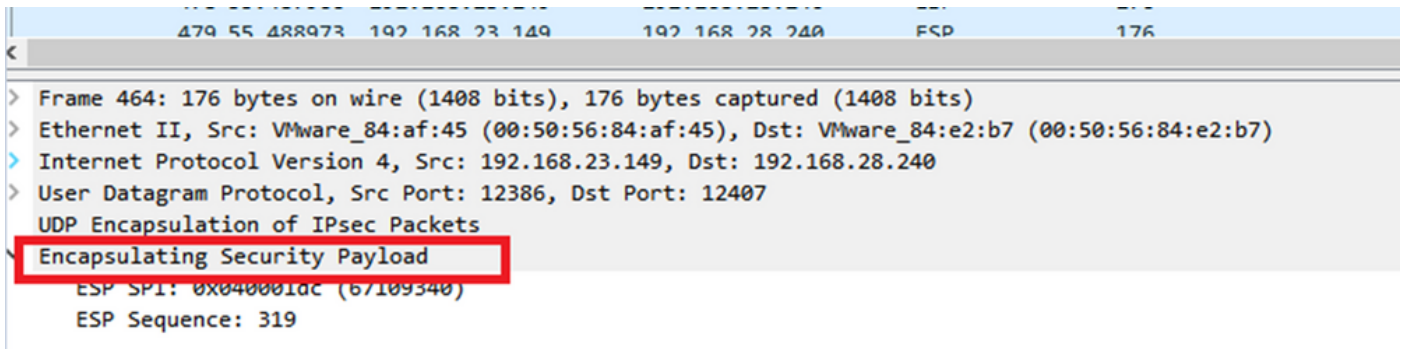
현재 필드 드롭다운 메뉴를 선택하고 해당 필드에 UPENCAP을 입력하거나 드롭다운에서 선택합니다.



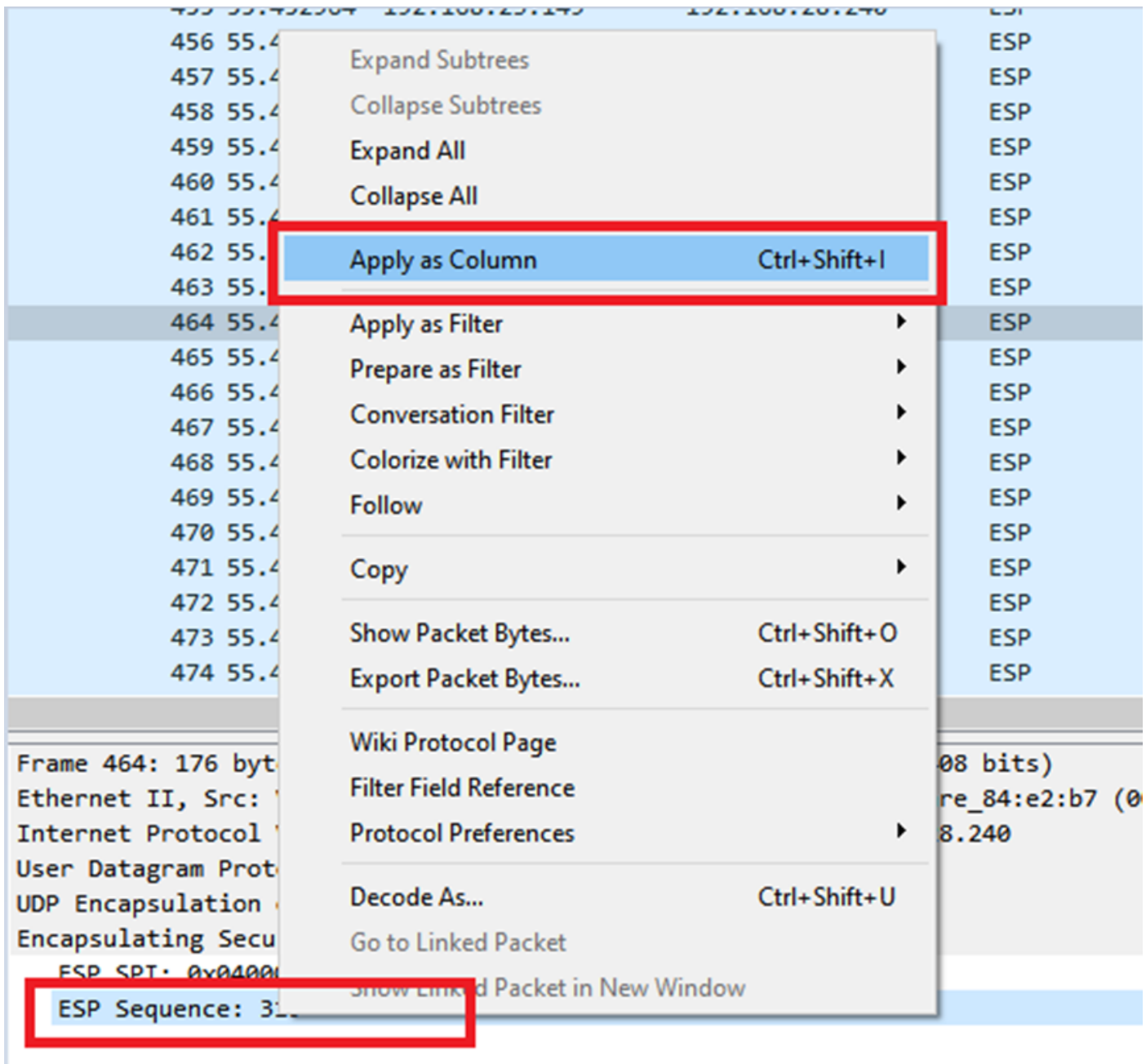
이 작업이 완료되면 **OK(확인)**를 선택합니다.



Wireshark Packet Details(Wireshark 패킷 세부사항) 섹션에서 패킷의 **Encapsulating Security Payload(캡슐화 보안 페이로드)** 부분을 **확장하여 ESP Sequence(ESP 시퀀스)**를 확인합니다.



ESP Sequence(ESP 시퀀스)를 마우스 오른쪽 버튼으로 클릭하고 **apply as column**(다음으로 적용)을 선택하여 ESP 시퀀스가 Wireshark 화면 상단의 Packet List(패킷 목록) 섹션에서 하나의 열로 표시될 수 있도록 합니다.



**참고:** cEdge1의 패킷에 대한 ESP SPI는 0x040001dc입니다. 이는 대상 캡처의 필터에 사용됩니다.



```

> Frame 464: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: VMware_84:af:45 (00:50:56:84:af:45), Dst: VMware_84:e2:b7
> Internet Protocol Version 4, Src: 192.168.23.149, Dst: 192.168.28.240
> User Datagram Protocol, Src Port: 12386, Dst Port: 12407
  UDP Encapsulation of IPsec Packets
    Encapsulating Security Payload

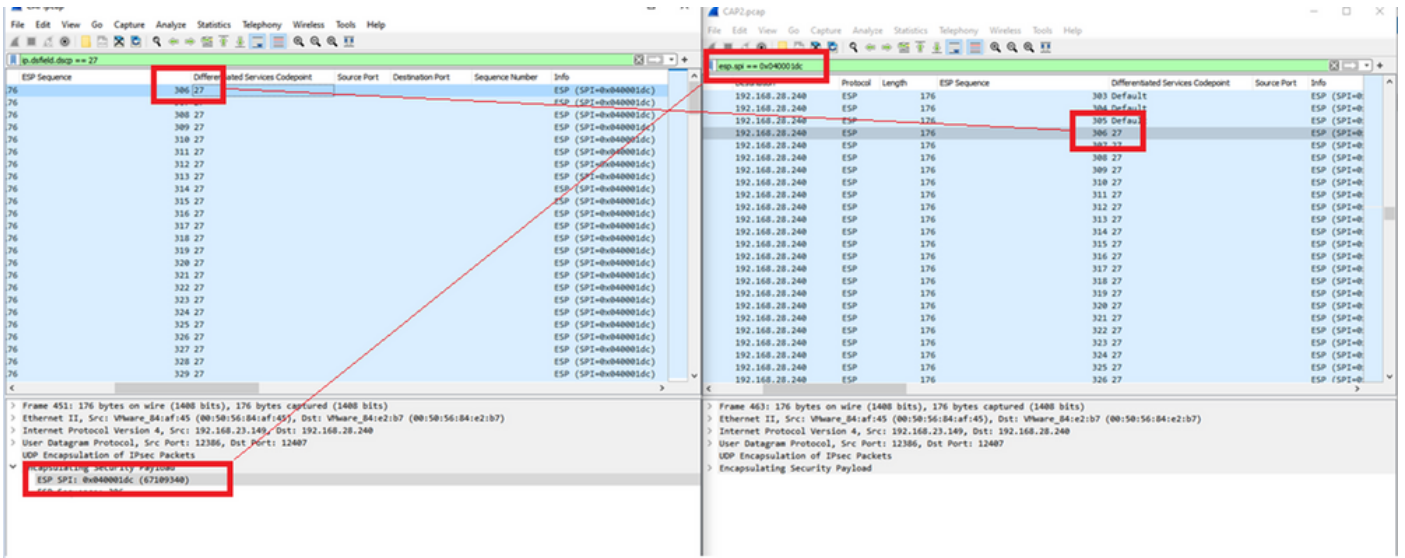
```

**ESP SPI: 0x040001dc (67109340)**  
 ESP Sequence: 319

대상 캡처를 열고, UDPENCAP으로 디코딩하기 위한 단계를 반복하고, 패킷에 ESP 시퀀스 번호를 표시합니다.

패킷에 ESP 시퀀스 번호가 표시되면 첫 번째 캡처의 ESP SPI를 두 번째 캡처의 필터로 사용하여 원하는 트래픽과 일치하는 해당 SPI 내의 트래픽만 표시할 수 있습니다.

둘 다 일치하는 패킷 시퀀스 번호에는 DSCP 27이 표시되어 있습니다.



이 비교는 Wireshark에서 수동으로 수행하거나 Microsoft Excel을 사용하여 비교할 수 있습니다.

Microsoft Excel을 사용하여 비교하려면 두 캡처를 모두 슬라이스하여 두 캡처에 있는 패킷만 포함해야 합니다.

소스 캡처에서, 제1 관련 패킷은 ESP 시퀀스(306)를 가지며 이는 패킷 번호(451)에 대응한다.

No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Different
451	55.441963	192.168.23.149	192.168.28.240	ESP	176	306 27	
452	55.445976	192.168.23.149	192.168.28.240	ESP	176	307 27	
453	55.448966	192.168.23.149	192.168.28.240	ESP	176	308 27	
454	55.450965	192.168.23.149	192.168.28.240	ESP	176	309 27	
455	55.452964	192.168.23.149	192.168.28.240	ESP	176	310 27	
456	55.454963	192.168.23.149	192.168.28.240	ESP	176	311 27	
457	55.455970	192.168.23.149	192.168.28.240	ESP	176	312 27	
458	55.456977	192.168.23.149	192.168.28.240	ESP	176	313 27	

소스 캡처의 마지막 관련 패킷은 ESP 시퀀스 405를 가지며 패킷 번호 550입니다.



548	55.608962	192.168.23.149	192.168.28.240	ESP	176	403 27
549	55.609969	192.168.23.149	192.168.28.240	ESP	176	404 27
550	55.610960	192.168.23.149	192.168.28.240	ESP	176	405 27

목적지 캡처에서, 제1 관련 패킷은 ESP 시퀀스 306을 갖는 소스 캡처에 대응하지만, 이 캡처에서는 패킷 463이다.

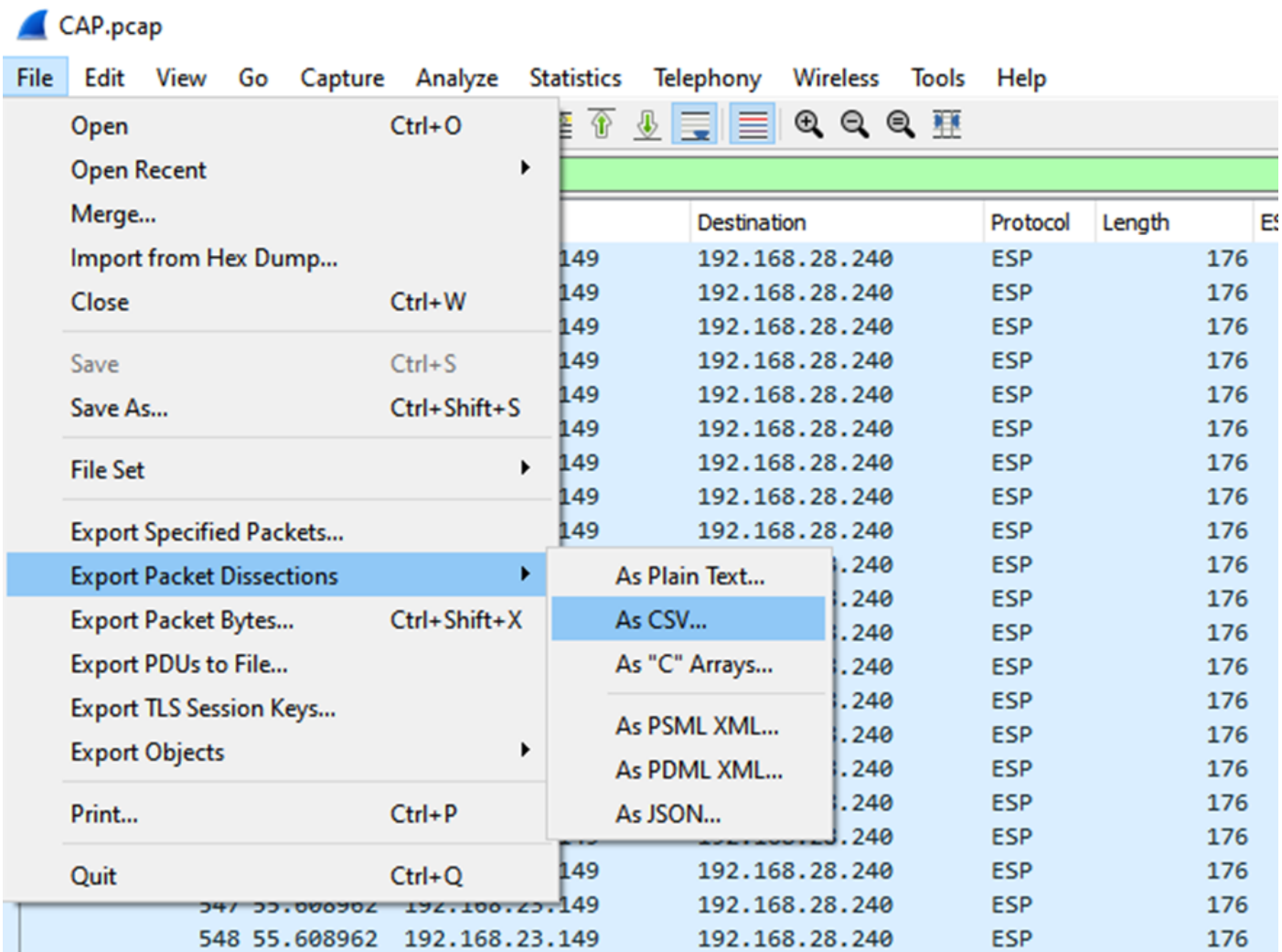
461	60.522028	192.168.23.149	192.168.28.240	ESP	168	407 Class S
462	60.715026	192.168.23.149	192.168.28.240	ESP	175	408 Class S
463	60.999008	192.168.23.149	192.168.28.240	ESP	176	306 27
464	61.003006	192.168.23.149	192.168.28.240	ESP	176	307 27

마지막 관련 패킷은 또한 ESP 시퀀스 405와 함께 존재하며 패킷 564입니다.

560	61.165052	192.168.23.149	192.168.28.240	ESP	176	403 27
561	61.166043	192.168.23.149	192.168.28.240	ESP	176	404 27
562	61.166043	192.168.23.149	192.168.28.240	ESP	176	405 27
563	61.431029	192.168.23.149	192.168.28.240	ESP	168	409 Class S
564	61.584021	192.168.23.149	192.168.28.240	ESP	175	410 Class S

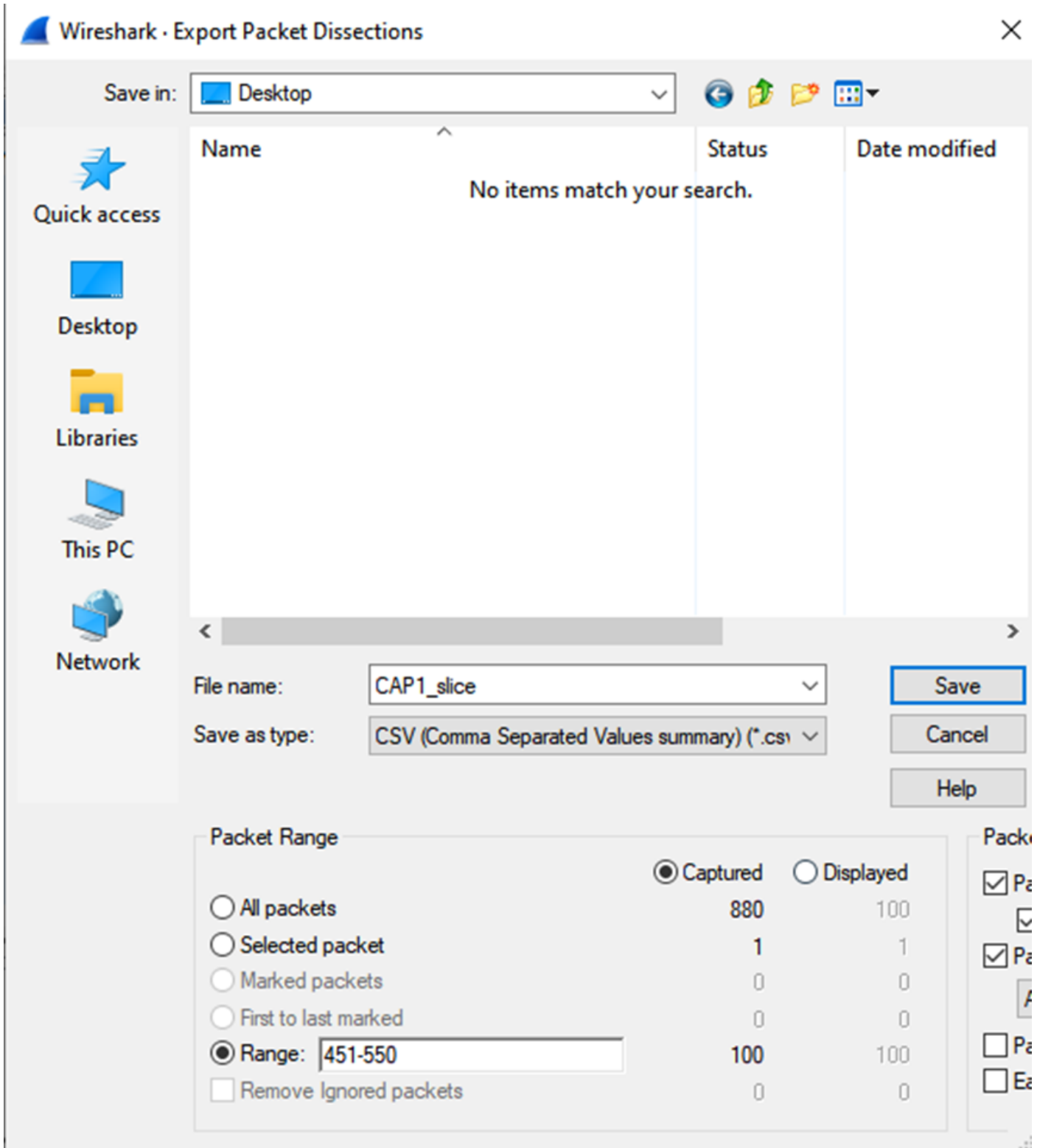
이제 첫 번째 캡처는 관련 패킷만 포함하도록 분할해야 합니다.

File(파일) > Export Packet Dissections(패킷 내보내기) > As CSV...(CSV로)로 이동합니다.

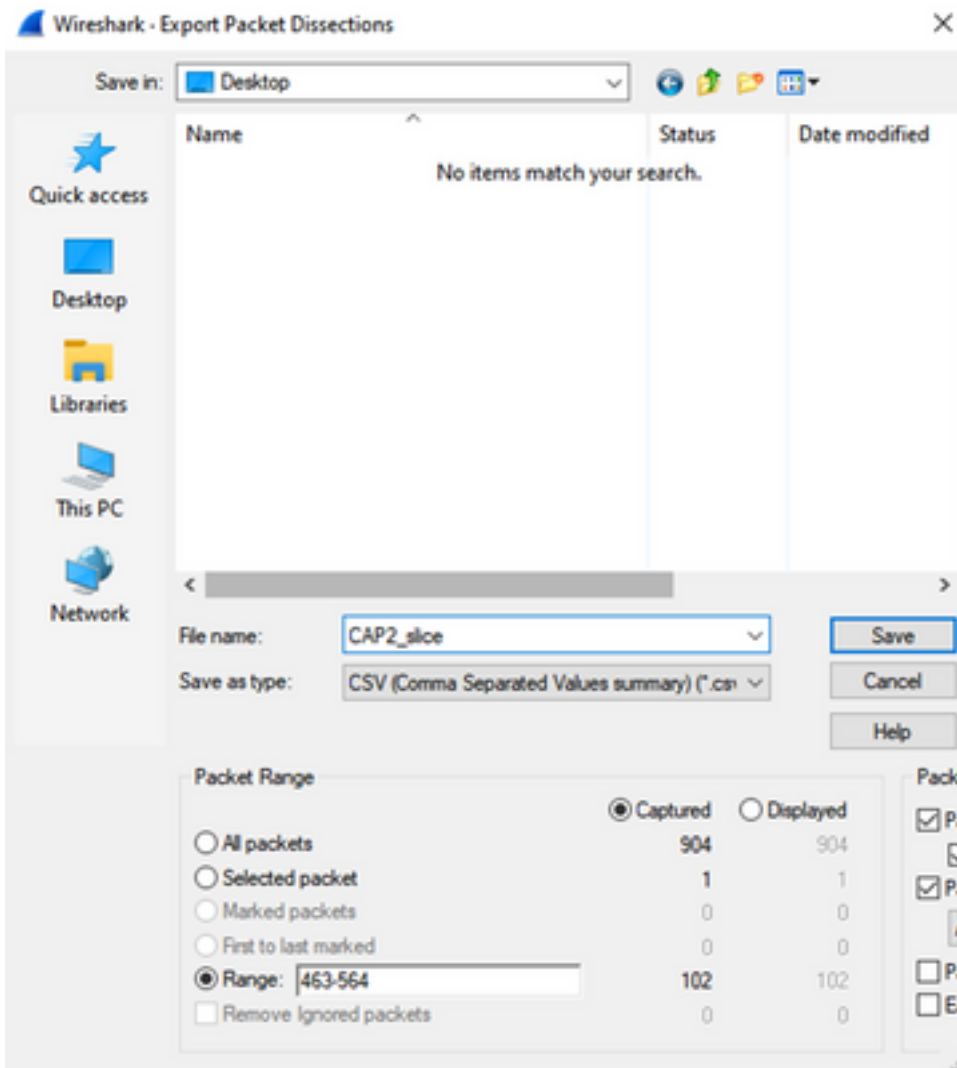


Captured and Range를 선택하고 Range 필드에 첫 번째 관련 패킷부터 마지막 관련 패킷까지의 범위를 입력합니다.

File Name(파일 이름) 필드에 파일 이름을 입력하고 Save(저장)를 클릭합니다.

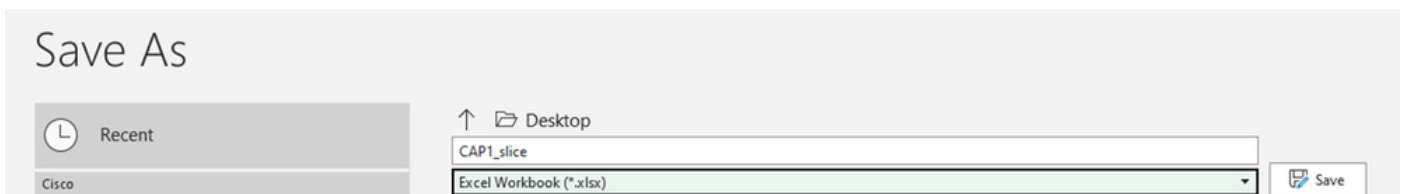


관련 패킷에 대해 캡처 2에서 동일한 프로세스를 반복합니다.

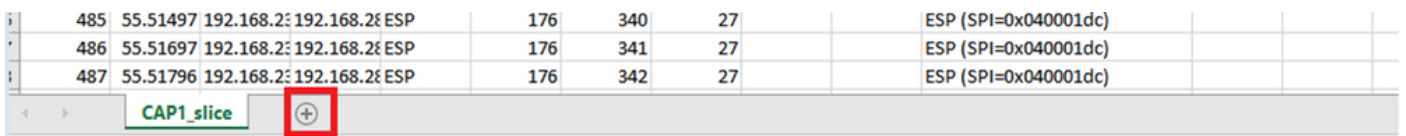


Microsoft Excel에서 두 CSV 파일을 모두 엽니다.

소스 캡처 CSV에서 XLSX 형식으로 저장합니다.



화면 하단에서 + 기호를 선택하여 다른 시트를 추가합니다. 이름을 CAP2\_slice로 지정합니다.



CAP2 CSV 파일을 열고 CTRL + a를 눌러 모두 선택하고 CTRL + c를 눌러 복사합니다.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	No.	Time	Source	Destinatic	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatic	Info	Sequence	Number
2	463	60.99901	192.168.25	192.168.25	ESP	176	306	27			ESP (SPI=0x040001dc)		
3	464	61.00301	192.168.25	192.168.25	ESP	176	307	27			ESP (SPI=0x040001dc)		
4	465	61.00506	192.168.25	192.168.25	ESP	176	308	27			ESP (SPI=0x040001dc)		
5	466	61.00706	192.168.25	192.168.25	ESP	176	309	27			ESP (SPI=0x040001dc)		
6	467	61.00905	192.168.25	192.168.25	ESP	176	310	27			ESP (SPI=0x040001dc)		
7	468	61.01006	192.168.25	192.168.25	ESP	176	311	27			ESP (SPI=0x040001dc)		
8	469	61.01105	192.168.25	192.168.25	ESP	176	312	27			ESP (SPI=0x040001dc)		
9	470	61.01305	192.168.25	192.168.25	ESP	176	313	27			ESP (SPI=0x040001dc)		
10	471	61.01406	192.168.25	192.168.25	ESP	176	314	27			ESP (SPI=0x040001dc)		
11	472	61.01606	192.168.25	192.168.25	ESP	176	315	27			ESP (SPI=0x040001dc)		
12	473	61.01806	192.168.25	192.168.25	ESP	176	316	27			ESP (SPI=0x040001dc)		
13	474	61.02106	192.168.25	192.168.25	ESP	176	317	27			ESP (SPI=0x040001dc)		
14	475	61.02205	192.168.25	192.168.25	ESP	176	318	27			ESP (SPI=0x040001dc)		
15	476	61.02306	192.168.25	192.168.25	ESP	176	319	27			ESP (SPI=0x040001dc)		
16	477	61.02506	192.168.25	192.168.25	ESP	176	320	27			ESP (SPI=0x040001dc)		
17	478	61.02605	192.168.25	192.168.25	ESP	176	321	27			ESP (SPI=0x040001dc)		

CAP1\_slice.xlsx 파일로 이동하고 CAP2\_slice의 두 번째 탭에서 복사된 정보를 셀 A1에 붙여넣습니다(CTRL + v).

Cut Copy Paste Format Painter

Calibri 11 A A B I U Font

Wrap Text Merge & Center Alignment

General \$ % Number

A1

	A	B	C	D	E	F	G	H	I	J	K	L	M
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													
29													
30													
31													
32													
33													
34													
35													
36													
37													
38													



No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination Port	Info	Sequence Number
463	60.99901	192.168.2.2	192.168.2.2	ESP	176	306	27			ESP (SPI=0x040001dc)	
464	61.00301	192.168.2.2	192.168.2.2	ESP	176	307	27			ESP (SPI=0x040001dc)	
465	61.00506	192.168.2.2	192.168.2.2	ESP	176	308	27			ESP (SPI=0x040001dc)	
466	61.00706	192.168.2.2	192.168.2.2	ESP	176	309	27			ESP (SPI=0x040001dc)	
467	61.00905	192.168.2.2	192.168.2.2	ESP	176	310	27			ESP (SPI=0x040001dc)	
468	61.01006	192.168.2.2	192.168.2.2	ESP	176	311	27			ESP (SPI=0x040001dc)	
469	61.01105	192.168.2.2	192.168.2.2	ESP	176	312	27			ESP (SPI=0x040001dc)	
470	61.01305	192.168.2.2	192.168.2.2	ESP	176	313	27			ESP (SPI=0x040001dc)	
471	61.01406	192.168.2.2	192.168.2.2	ESP	176	314	27			ESP (SPI=0x040001dc)	
472	61.01606	192.168.2.2	192.168.2.2	ESP	176	315	27			ESP (SPI=0x040001dc)	
473	61.01806	192.168.2.2	192.168.2.2	ESP	176	316	27			ESP (SPI=0x040001dc)	
474	61.02106	192.168.2.2	192.168.2.2	ESP	176	317	27			ESP (SPI=0x040001dc)	
475	61.02205	192.168.2.2	192.168.2.2	ESP	176	318	27			ESP (SPI=0x040001dc)	
476	61.02306	192.168.2.2	192.168.2.2	ESP	176	319	27			ESP (SPI=0x040001dc)	
477	61.02506	192.168.2.2	192.168.2.2	ESP	176	320	27			ESP (SPI=0x040001dc)	
478	61.02605	192.168.2.2	192.168.2.2	ESP	176	321	27			ESP (SPI=0x040001dc)	
479	61.02805	192.168.2.2	192.168.2.2	ESP	176	322	27			ESP (SPI=0x040001dc)	
480	61.02906	192.168.2.2	192.168.2.2	ESP	176	323	27			ESP (SPI=0x040001dc)	
481	61.02906	192.168.2.2	192.168.2.2	ESP	176	324	27			ESP (SPI=0x040001dc)	
482	61.03005	192.168.2.2	192.168.2.2	ESP	176	325	27			ESP (SPI=0x040001dc)	
483	61.03206	192.168.2.2	192.168.2.2	ESP	176	326	27			ESP (SPI=0x040001dc)	
484	61.03306	192.168.2.2	192.168.2.2	ESP	176	327	27			ESP (SPI=0x040001dc)	
485	61.03505	192.168.2.2	192.168.2.2	ESP	176	328	27			ESP (SPI=0x040001dc)	
486	61.03606	192.168.2.2	192.168.2.2	ESP	176	329	27			ESP (SPI=0x040001dc)	
487	61.03905	192.168.2.2	192.168.2.2	ESP	176	330	27			ESP (SPI=0x040001dc)	
488	61.04105	192.168.2.2	192.168.2.2	ESP	176	331	27			ESP (SPI=0x040001dc)	
489	61.04206	192.168.2.2	192.168.2.2	ESP	176	332	27			ESP (SPI=0x040001dc)	
490	61.04406	192.168.2.2	192.168.2.2	ESP	176	333	27			ESP (SPI=0x040001dc)	
491	61.04606	192.168.2.2	192.168.2.2	ESP	176	334	27			ESP (SPI=0x040001dc)	
492	61.06305	192.168.2.2	192.168.2.2	ESP	176	335	27			ESP (SPI=0x040001dc)	
493	61.06505	192.168.2.2	192.168.2.2	ESP	176	336	27			ESP (SPI=0x040001dc)	
494	61.06705	192.168.2.2	192.168.2.2	ESP	176	337	27			ESP (SPI=0x040001dc)	
495	61.06905	192.168.2.2	192.168.2.2	ESP	176	338	27			ESP (SPI=0x040001dc)	
496	61.07105	192.168.2.2	192.168.2.2	ESP	176	339	27			ESP (SPI=0x040001dc)	
497	61.07105	192.168.2.2	192.168.2.2	ESP	176	340	27			ESP (SPI=0x040001dc)	

CAP1\_slice 시트로 다시 이동하여 COMPARE\_ESP\_SEQUENCE라는 새 열을 만듭니다.

No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination Port	Info	Sequence Number	COMPARE_ESP_SEQUENCE
451	55.44196	192.168.2.2	192.168.2.2	ESP	176	306	27			ESP (SPI=0x040001dc)		
452	55.44598	192.168.2.2	192.168.2.2	ESP	176	307	27			ESP (SPI=0x040001dc)		

ESP 시퀀스 번호가 G열에 있으므로 표시된 대로 VLOOKUP 명령을 작성하여 두 시트를 비교하여 소스의 G열에 있는 모든 것이 대상의 G열에 있는지 확인합니다.

**=IF(ISNA(VLOOKUP(G2,CAP2\_SLICE!G:G,1,FALSE)),"MISSING","PRESENT")**

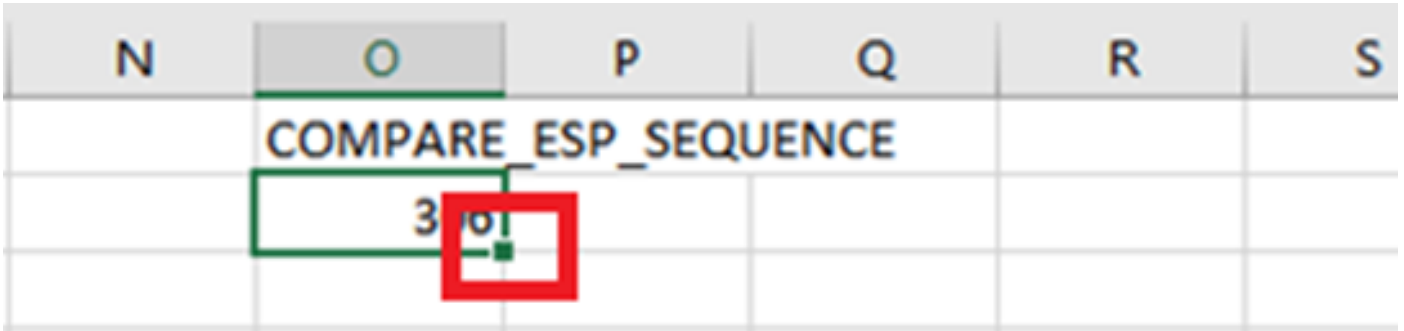
Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination Port	Info	Sequence Number	COMPARE_ESP_SEQUENCE
55.44196	192.168.2.2	192.168.2.2	ESP	176	306	27			ESP (SPI=0x040001dc)		=IF(ISNA(VLOOKUP(G2,CAP2_SLICE!G:G,1,FALSE)),"MISSING","PRESENT")
55.44598	192.168.2.2	192.168.2.2	ESP	176	307	27			ESP (SPI=0x040001dc)		

Enter를 선택하면 PRESENT라는 단어가 표시됩니다. 이는 ESP 시퀀스(306)를 갖는 패킷이 두 번째 시트에 존재함을 의미한다. 이는 패킷이 소스에서 목적지까지 도달했음을 의미하므로 중요합니다.



No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination Info	Sequence Number	COMPARE	ESP_SEQUENCE
451	55.44196	192.168.2.2	192.168.2.2	ESP	176	306	27		ESP (SPI=0x040001dc)		PRESENT	
452	55.44598	192.168.2.2	192.168.2.2	ESP	176	307	27		ESP (SPI=0x040001dc)			

Column O Row 2를 선택하고 해당 셀 주위의 녹색 상자 오른쪽 하단 모서리에 마우스를 놓습니다.

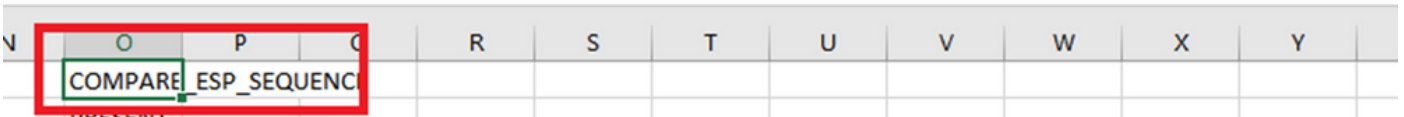
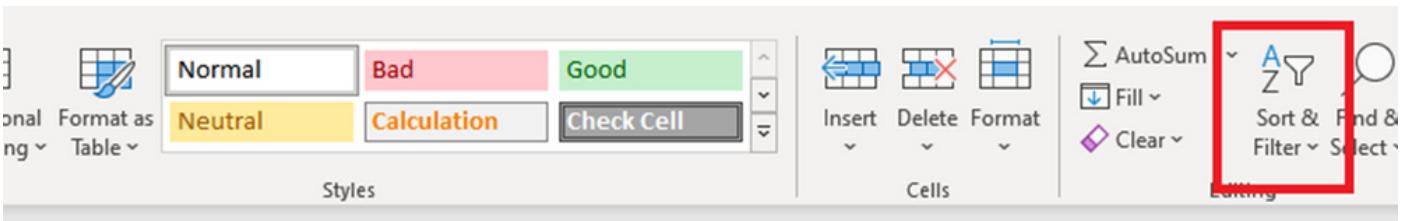


값을 가진 셀의 아래쪽에 이 수식을 복사하려면 마우스 단추를 누른 상태에서 마우스를 끕니다.

=IF(ISNA(VLOOKUP(G2,CAP2\_slice!G:G,1,FALSE)),"MISSING","PRESENT")

Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination Info	Sequence Number	COMPARE	ESP_SEQUENCE
55.44196	192.168.2.2	192.168.2.2	ESP	176	306	27		ESP (SPI=0x040001dc)		PRESENT	
55.44598	192.168.2.2	192.168.2.2	ESP	176	307	27		ESP (SPI=0x040001dc)			
55.44897	192.168.2.2	192.168.2.2	ESP	176	308	27		ESP (SPI=0x040001dc)			
55.45097	192.168.2.2	192.168.2.2	ESP	176	309	27		ESP (SPI=0x040001dc)			
55.45296	192.168.2.2	192.168.2.2	ESP	176	310	27		ESP (SPI=0x040001dc)			
55.45496	192.168.2.2	192.168.2.2	ESP	176	311	27		ESP (SPI=0x040001dc)			
55.45597	192.168.2.2	192.168.2.2	ESP	176	312	27		ESP (SPI=0x040001dc)			
55.45698	192.168.2.2	192.168.2.2	ESP	176	313	27		ESP (SPI=0x040001dc)			
55.45797	192.168.2.2	192.168.2.2	ESP	176	314	27		ESP (SPI=0x040001dc)			
55.45898	192.168.2.2	192.168.2.2	ESP	176	315	27		ESP (SPI=0x040001dc)			
55.46197	192.168.2.2	192.168.2.2	ESP	176	316	27		ESP (SPI=0x040001dc)			
55.46397	192.168.2.2	192.168.2.2	ESP	176	317	27		ESP (SPI=0x040001dc)			
55.46596	192.168.2.2	192.168.2.2	ESP	176	318	27		ESP (SPI=0x040001dc)			
55.46697	192.168.2.2	192.168.2.2	ESP	176	319	27		ESP (SPI=0x040001dc)			
55.46796	192.168.2.2	192.168.2.2	ESP	176	320	27		ESP (SPI=0x040001dc)			
55.46996	192.168.2.2	192.168.2.2	ESP	176	321	27		ESP (SPI=0x040001dc)			
55.47097	192.168.2.2	192.168.2.2	ESP	176	322	27		ESP (SPI=0x040001dc)			
55.60496	192.168.2.2	192.168.2.2	ESP	176	395	27		ESP (SPI=0x040001dc)		PRESENT	
55.60596	192.168.2.2	192.168.2.2	ESP	176	396	27		ESP (SPI=0x040001dc)		PRESENT	
55.60696	192.168.2.2	192.168.2.2	ESP	176	397	27		ESP (SPI=0x040001dc)		PRESENT	
55.60696	192.168.2.2	192.168.2.2	ESP	176	398	27		ESP (SPI=0x040001dc)		PRESENT	
55.60696	192.168.2.2	192.168.2.2	ESP	176	399	27		ESP (SPI=0x040001dc)		PRESENT	
55.60796	192.168.2.2	192.168.2.2	ESP	176	400	27		ESP (SPI=0x040001dc)		PRESENT	
55.60796	192.168.2.2	192.168.2.2	ESP	176	401	27		ESP (SPI=0x040001dc)		PRESENT	
55.60896	192.168.2.2	192.168.2.2	ESP	176	402	27		ESP (SPI=0x040001dc)		PRESENT	
55.60896	192.168.2.2	192.168.2.2	ESP	176	403	27		ESP (SPI=0x040001dc)		PRESENT	
55.60997	192.168.2.2	192.168.2.2	ESP	176	404	27		ESP (SPI=0x040001dc)		PRESENT	
55.61096	192.168.2.2	192.168.2.2	ESP	176	405	27		ESP (SPI=0x040001dc)		PRESENT	

시트 맨 위로 다시 스크롤하여 COMPARE\_ESP\_SEQUENCE를 클릭합니다. 그런 다음 정렬 및 필터를 선택합니다.



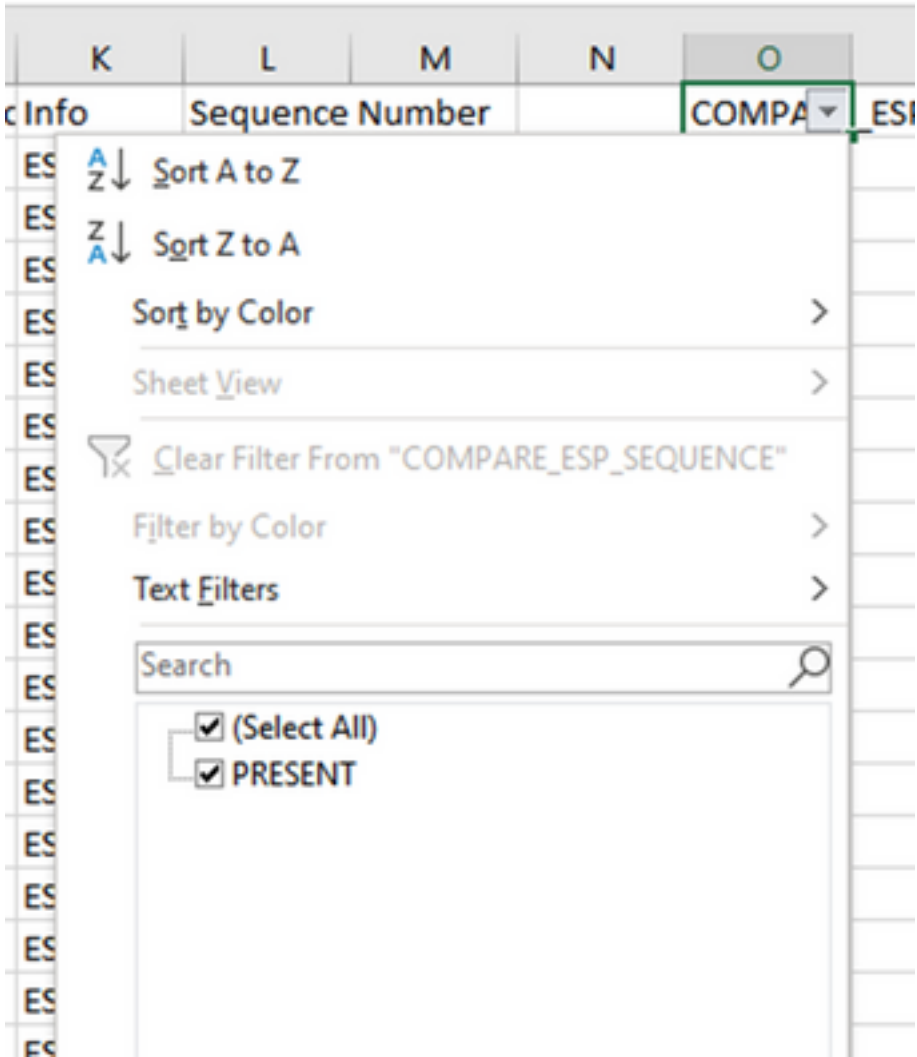
드롭다운 메뉴에서 Filter를 선택합니다.



드롭다운 메뉴가 COMPARE\_ESP\_SEQUENCE 열에 나타납니다.

M	N	O	P
Number		COMPARE ESP_SEQUENCE	
		PRESENT	
		PRESENT	
		PRESENT	

COMPARE\_ESP\_SEQUENCE 제목의 드롭다운 메뉴를 클릭합니다. 이 예에서는 PRESENT 값만 표시됩니다. 즉, 모든 패킷이 두 캡처에 모두 있습니다.




문제가 되는 예를 만들려면 CAP2\_slice에서 10개의 패킷을 삭제하여 일부 누락된 패킷이 없는 테스트에서 이 방법이 어떻게 작동하는지 보여 줍니다.


11	472	61.01806	192.168.2:192.168.2	ESP	176	315	27	ESP (SPI=0x040001dc)
12	473	61.01806	192.168.2:192.168.2	ESP	176	316	27	ESP (SPI=0x040001dc)
13	474	61.02106	192.168.2:192.168.2	ESP	176	317	27	ESP (SPI=0x040001dc)
14	475	61.02205	192.168.2:192.168.2	ESP	176	318	27	ESP (SPI=0x040001dc)
15	476	61.02306	192.168.2:192.168.2	ESP	176	319	27	ESP (SPI=0x040001dc)
16	477	61.02506	192.168.2:192.168.2	ESP	176	320	27	ESP (SPI=0x040001dc)
17	478	61.02605	192.168.2:192.168.2	ESP	176	321	27	ESP (SPI=0x040001dc)
18	479	61.02805	192.168.2:192.168.2	ESP	176	322	27	ESP (SPI=0x040001dc)
19	480	61.02906	192.168.2:192.168.2	ESP	176	323	27	ESP (SPI=0x040001dc)
20	481	61.02906	192.168.2:192.168.2	ESP	176	324	27	ESP (SPI=0x040001dc)
21	482	61.03005	192.168.2:192.168.2	ESP	176	325	27	ESP (SPI=0x040001dc)
22	483	61.03206	192.168.2:192.168.2	ESP	176	326	27	ESP (SPI=0x040001dc)
23	484	61.03306	192.168.2:192.168.2	ESP	176	327	27	ESP (SPI=0x040001dc)
24	485	61.03505	192.168.2:192.168.2	ESP	176	328	27	ESP (SPI=0x040001dc)
25	486	61.03606	192.168.2:192.168.2	ESP	176	329	27	ESP (SPI=0x040001dc)
26	487	61.03905	192.168.2:192.168.2	ESP	176	330	27	ESP (SPI=0x040001dc)
27	488	61.04105	192.168.2:192.168.2	ESP	176	331	27	ESP (SPI=0x040001dc)
28	489	61.04206	192.168.2:192.168.2	ESP	176	332	27	ESP (SPI=0x040001dc)
29	490	61.04406	192.168.2:192.168.2	ESP	176	333	27	ESP (SPI=0x040001dc)
30	491	61.04606	192.168.2:192.168.2	ESP	176	334	27	ESP (SPI=0x040001dc)
31	492	61.06305	192.168.2:192.168.2	ESP	176	335	27	ESP (SPI=0x040001dc)
32	493	61.06505	192.168.2:192.168.2	ESP	176	336	27	ESP (SPI=0x040001dc)
33	494	61.06705	192.168.2:192.168.2	ESP	176	337	27	ESP (SPI=0x040001dc)
34	495	61.06905	192.168.2:192.168.2	ESP	176	338	27	ESP (SPI=0x040001dc)
35	496	61.07105	192.168.2:192.168.2	ESP	176	339	27	ESP (SPI=0x040001dc)
36	497	61.07105	192.168.2:192.168.2	ESP	176	340	27	ESP (SPI=0x040001dc)
37	498	61.07205	192.168.2:192.168.2	ESP	176	341	27	ESP (SPI=0x040001dc)
38	499	61.07605	192.168.2:192.168.2	ESP	176	342	27	ESP (SPI=0x040001dc)


다시 CAP1\_slice 시트로 이동한 다음 10개의 패킷이 누락되었습니다.


Packet No.	Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Length	Offset	Signature	Result
460	55.45898	192.168.2.2	192.168.2.2	ESP	176	315	27		ESP (SPI=0x040001dc)	PRESENT
461	55.46197	192.168.2.2	192.168.2.2	ESP	176	316	27		ESP (SPI=0x040001dc)	PRESENT
462	55.46397	192.168.2.2	192.168.2.2	ESP	176	317	27		ESP (SPI=0x040001dc)	PRESENT
463	55.46596	192.168.2.2	192.168.2.2	ESP	176	318	27		ESP (SPI=0x040001dc)	MISSING
464	55.46697	192.168.2.2	192.168.2.2	ESP	176	319	27		ESP (SPI=0x040001dc)	MISSING
465	55.46796	192.168.2.2	192.168.2.2	ESP	176	320	27		ESP (SPI=0x040001dc)	MISSING
466	55.46996	192.168.2.2	192.168.2.2	ESP	176	321	27		ESP (SPI=0x040001dc)	MISSING
467	55.47097	192.168.2.2	192.168.2.2	ESP	176	322	27		ESP (SPI=0x040001dc)	MISSING
468	55.47198	192.168.2.2	192.168.2.2	ESP	176	323	27		ESP (SPI=0x040001dc)	MISSING
469	55.47297	192.168.2.2	192.168.2.2	ESP	176	324	27		ESP (SPI=0x040001dc)	MISSING
470	55.47497	192.168.2.2	192.168.2.2	ESP	176	325	27		ESP (SPI=0x040001dc)	MISSING
471	55.47597	192.168.2.2	192.168.2.2	ESP	176	326	27		ESP (SPI=0x040001dc)	MISSING
472	55.47697	192.168.2.2	192.168.2.2	ESP	176	327	27		ESP (SPI=0x040001dc)	MISSING
473	55.47896	192.168.2.2	192.168.2.2	ESP	176	328	27		ESP (SPI=0x040001dc)	PRESENT
474	55.48096	192.168.2.2	192.168.2.2	ESP	176	329	27		ESP (SPI=0x040001dc)	PRESENT

COMPARE\_ESP\_SEQUENCE 열에서 드롭다운 메뉴가 선택된 경우 누락된 패킷도 표시됩니다. MISSING 패킷만 보려면 이 옵션을 전환할 수 있습니다.


K	L	M	N	O
Info	Sequence Number			COMPA 

 Sort A to Z


 Sort Z to A


Sort by Color 


---

Sheet View 


---

 Clear Filter From "COMPARE\_ESP\_SEQUENCE"

Filter by Color 

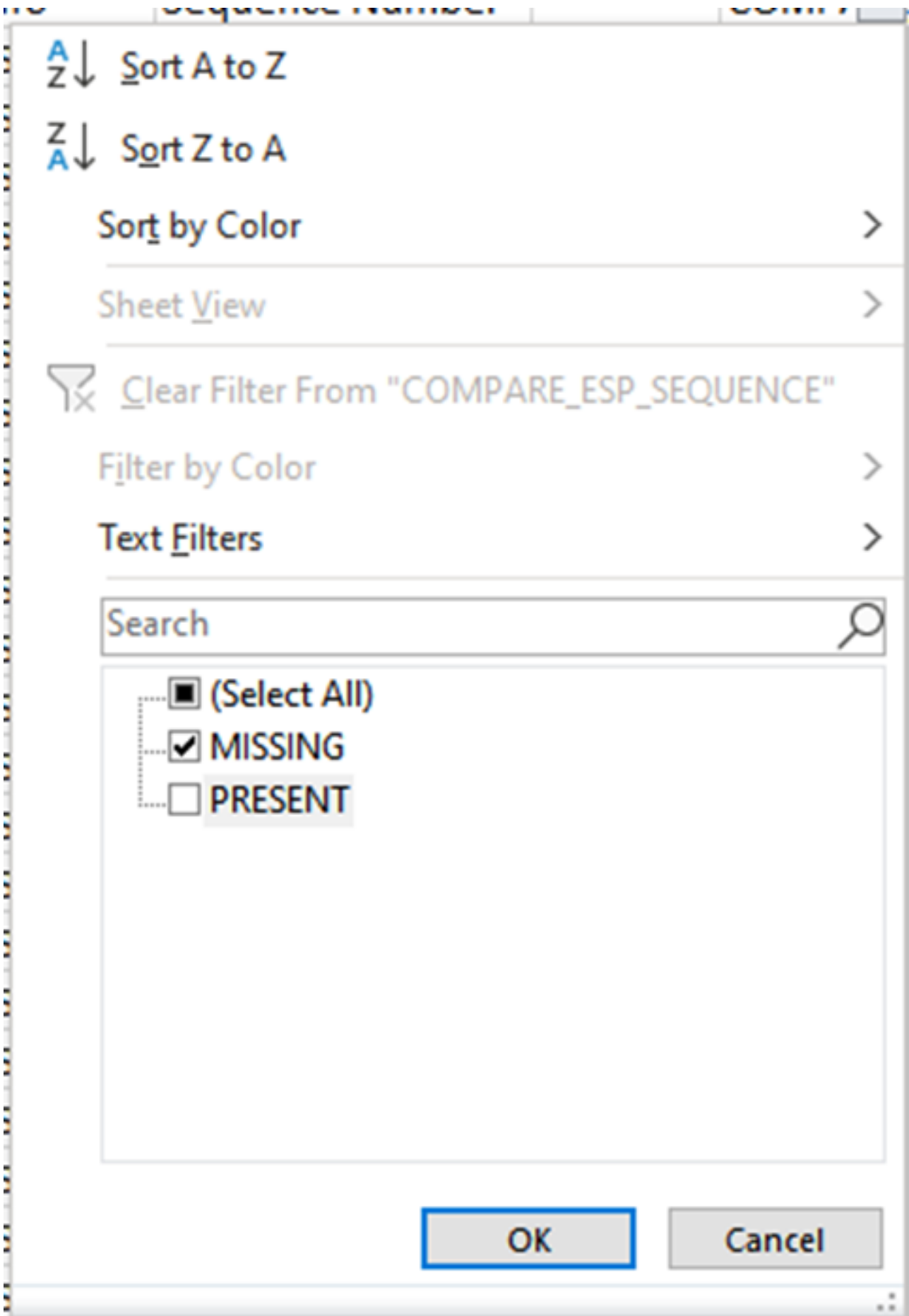
Text Filters 

---

Search 

- (Select All)
- MISSING
- PRESENT

OK Cancel



이제 누락된 패킷만 Excel 시트에 표시됩니다.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination	Info	Sequence Number			COMPACT	ESP_SEQUENCE
4	463	55.46596	192.168.2.2	192.168.2.2	ESP	176	318	27			ESP (SPI=0x040001dc)					MISSING
5	464	55.46697	192.168.2.2	192.168.2.2	ESP	176	319	27			ESP (SPI=0x040001dc)					MISSING
6	465	55.46796	192.168.2.2	192.168.2.2	ESP	176	320	27			ESP (SPI=0x040001dc)					MISSING
7	466	55.46996	192.168.2.2	192.168.2.2	ESP	176	321	27			ESP (SPI=0x040001dc)					MISSING
8	467	55.47097	192.168.2.2	192.168.2.2	ESP	176	322	27			ESP (SPI=0x040001dc)					MISSING
9	468	55.47198	192.168.2.2	192.168.2.2	ESP	176	323	27			ESP (SPI=0x040001dc)					MISSING
0	469	55.47297	192.168.2.2	192.168.2.2	ESP	176	324	27			ESP (SPI=0x040001dc)					MISSING
1	470	55.47497	192.168.2.2	192.168.2.2	ESP	176	325	27			ESP (SPI=0x040001dc)					MISSING
2	471	55.47597	192.168.2.2	192.168.2.2	ESP	176	326	27			ESP (SPI=0x040001dc)					MISSING
3	472	55.47697	192.168.2.2	192.168.2.2	ESP	176	327	27			ESP (SPI=0x040001dc)					MISSING
12																
13																

## 관련 정보

- [Cisco 임베디드 패킷 캡처](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.