

Controleer en identificeer pakketverlies in het WAN voor SD-WAN

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Proces voor probleemoplossing](#)

[Overzicht proces](#)

[Markeer het gewenste verkeer met DSCP](#)

[Leg het verkeer vast met de ingesloten vastlegging](#)

[Analyse via Wireshark](#)

[Filter het gewenste verkeer op ESP Sequence](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u gegevens kunt identificeren en verzamelen wanneer het verkeer over het WAN is kwijtgeraakt, maar er geen dalingen worden gezien op de SD-WAN Edge.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)
- Ingesloten pakketvastlegging voor vManager-pakketvastlegging
- draadhaai
- Microsoft Excel

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C800V versie 17.03.04
- vManager versie 20.3.4
- Wireshark versie 2.6.3

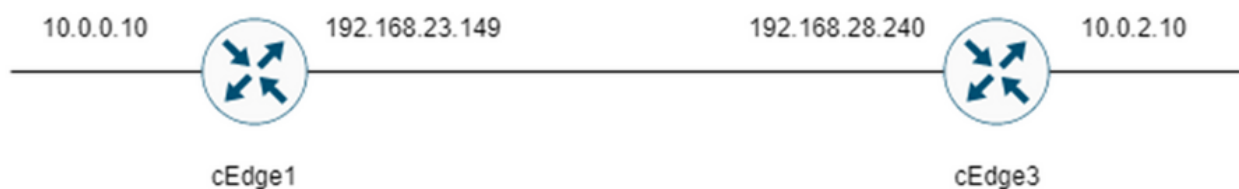
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrond

Om bij deze uitdaging te helpen, tonen de stappen die in dit document worden beschreven hoe u specifiek verkeer kunt markeren met gedifferentieerde services code point (DSCP) om te helpen de gewenste pakketten te identificeren. DSCP kan worden gebruikt om het verkeer te identificeren aangezien deze waarde van de binnen pakketheader aan de kopbal IPsec wordt gekopieerd. Zodra de gewenste pakketten worden geïdentificeerd, toont het hoe te om het verkeer over twee WAN aan te passen vangt om verkeer te verzekeren dat van bron tot bestemming wordt gemaakt.

Twee enige routerplaatsen worden gebruikt om deze probleemoplossingstechniek aan te tonen. In dit geval, ICMP verkeer van 10.0.0.10 tot 10.0.2.10 in de vorm van 100 pings zoals getoond in het beeld. Er is geen verlies in dit voorbeeld maar deze zelfde probleemoplossingstechniek wordt gebruikt in het geval waar er een verlies is om het te identificeren.



Proces voor probleemoplossing

Overzicht proces

1. Voor het verkeer dat over WAN wordt overgetrokken, is een Toegangslijst (ACL) (of gecentraliseerd beleid) nodig om verkeer met wat ongebruikte DSCP-waarde te markeren. In dit voorbeeld wordt DSCP 27 gebruikt.
2. Zodra het verkeer wordt gemarkeerd, wordt de ingesloten pakketvastlegging gebruikt om de pakketten op de transportinterface van de bron en de bestemmingsrouter op te nemen.

Opmerking: vManager-pakketvastlegging kan ook worden gebruikt, hoewel er een beperking is van 5 MB aan gegevens of 5 minuten looptijd.

1. Nadat de opnamen zijn genomen, open ze in Wireshark om te bekijken.
2. De filter wordt toegepast in Wireshark om te tonen welke pakketten worden gewenst en dan worden zij vergeleken.
3. Microsoft Excel wordt gebruikt voor grote opnamen om nauwkeurigheid te garanderen.

Markeer het gewenste verkeer met DSCP

Een toegangslijst zoals het voorbeeld wordt geconfigureerd op de bronrouter (cEdge1 in dit voorbeeld) en toegepast op de interface in het SD-WAN-gedeelte van de routerconfiguratie zoals getoond.

Een optionele teller wordt toegepast om te verifiëren dat het verkeer het beleid raakt zoals verwacht. Dit kan worden gecontroleerd met de opdracht **tonen sdwan beleid access-list-tellers**.

```
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
```

Leg het verkeer vast met de ingesloten vastlegging

Opmerking: hoe u een ingesloten pakketopname in Cisco IOS XE configureert om de versleutelde pakketten op te nemen die via het WAN worden verzonden, naar het [voorbeeld Ingesloten pakketvastlegging voor Cisco IOS en Cisco IOS XE Configuration](#)

Opmerking: er moet een ACL worden gebruikt om de EPC op het WAN te beperken, aangezien er meer dan de 1000 PPS-snelheidslimiet voor de EPC zou kunnen zijn.

Voorbeeld

Een ACL wordt geconfigureerd op cEdge1 en cEdge3 omdat verkeer alleen is geselecteerd in de richting van bron naar bestemming in dit voorbeeld.

Opmerking: de WAN IP-adressen worden gebruikt om de opname te filteren. Er zijn meerdere uitgangen die kunnen worden gebruikt om het pad dat het verkeer neemt te identificeren, zodat de juiste WAN IP's kunnen worden geïdentificeerd voor het ACL-filter. De opdrachten die kunnen worden gebruikt om deze uitvoer te genereren zijn de **show sdwan app-fwd cflowd flows** en **toon sdwan policy service path**. Blader naar [Conditional Packet Trace](#) om de debug-voorwaarde te controleren.

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

Op dit punt worden de opnamen gestart op beide routers en worden 100 pings over de overlay verzonden.

```
#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

Nadat de opnamen zijn gestopt en van beide routers zijn verzameld, moeten ze worden geopend in Wireshark om ze te kunnen bekijken.

Analyse via Wireshark

Als de cEdge1-opname eenmaal is geopend in Wireshark, wordt gezien dat al het verkeer is versleuteld en het is niet eenvoudig te ontcijferen welke pakketten de pings zijn die zijn verzonden.

No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Differentiated Services Codepoint	Source Port	Destination Port	Sequence Number	Info
1	0.000000	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
2	0.563966	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
3	0.983996	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
4	1.423978	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
5	1.896993	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
6	2.417977	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
7	2.792958	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
8	3.323973	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
9	3.781957	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
10	4.145988	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
11	4.769949	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
12	4.981995	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
13	5.722954	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
14	5.978994	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
15	6.532961	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
16	6.949999	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
17	7.348980	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
18	7.923999	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
19	8.193990	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
20	8.774953	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
21	9.111993	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
22	9.653957	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
23	10.682988	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
24	10.564957	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
25	10.949999	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
26	11.416970	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
27	11.937991	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
28	12.488984	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
29	12.836998	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
30	13.266984	192.168.23.149	192.168.28.240	UDP	168		Class Selector 6			12386	12407 Len=126
31	13.779958	192.168.23.149	192.168.28.240	UDP	175		Class Selector 6			12386	12407 Len=133
32	14.171988	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
33	14.173986	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
34	14.174978	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
35	14.175985	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
36	14.176977	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
37	14.176977	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
38	14.178991	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134
39	14.188990	192.168.23.149	192.168.28.240	UDP	176		Default			12386	12407 Len=134

Filter deze opname met een weergavefilter `ip.dsfield.dscp == 27`, men ziet dat er slechts 100 pakketten worden weergegeven aan de onderkant van het scherm en men ziet dat de DSCP kolom waarde allen 27 toont.

No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Differentiated Services Codepoint	Source Port	Destination Port	Sequence Number	Info
451	55.441963	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
452	55.445976	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
453	55.448966	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
454	55.450965	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
455	55.452964	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
456	55.454963	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
457	55.456970	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
458	55.458977	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
459	55.460984	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
460	55.462991	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
461	55.464998	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
462	55.466997	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
463	55.468996	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
464	55.470995	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
465	55.472994	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
466	55.474993	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
467	55.476992	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
468	55.478991	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
469	55.480990	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
470	55.482989	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
471	55.484988	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
472	55.486987	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
473	55.488986	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
474	55.490985	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
475	55.492984	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
476	55.494983	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
477	55.496982	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
478	55.498981	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
479	55.500980	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
480	55.502979	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
481	55.504978	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
482	55.506977	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
483	55.508976	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
484	55.510975	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
485	55.512974	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
486	55.514973	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
487	55.516972	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
488	55.518971	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134
489	55.520970	192.168.23.149	192.168.28.240	UDP	176	27	27	12386	12407	Len=134	12386 → 12407 Len=134

> Frame 451: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) on interface 0
 > Ethernet II, Src: VMware_B4:af:45 (00:50:56:04:af:45), Dst: VMware_B4:e2:b7 (00:50:56:04: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
 > Data (134 bytes)

0000 00 50 56 04 e2 b7 00 50 56 04 af 45 08 00 45 0c -PV- P V E E1
 CAP.pcap Packets: 880 Displayed: 200 (1.4%) Profile: Default

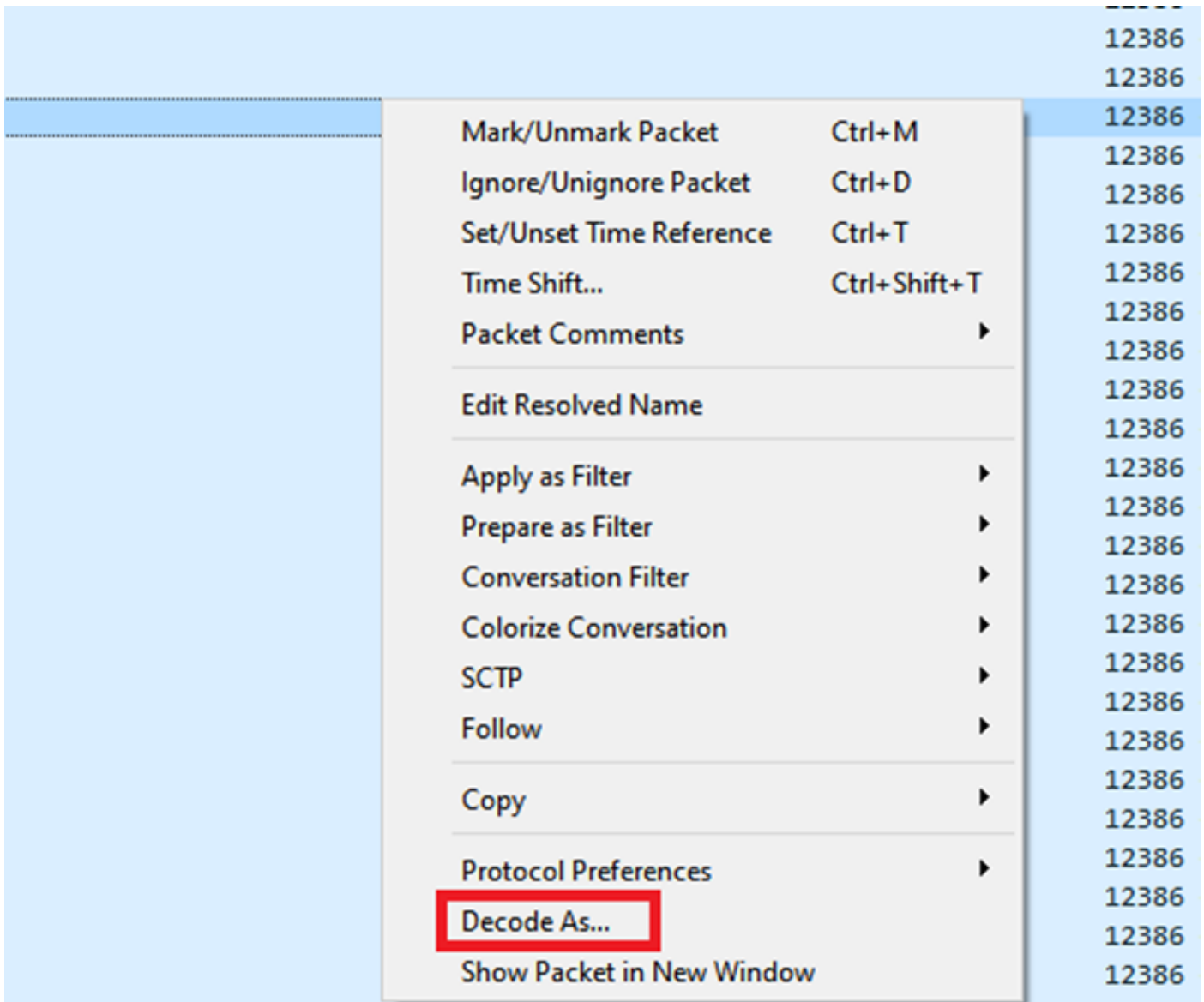
In sommige gevallen waarin DSCP-waarde over het WAN wordt behouden, kan dezelfde filter op de doelopname worden gebruikt.

In andere gevallen is dit niet mogelijk, zoals een situatie waarin DSCP-waarde via een openbare internetverbinding wordt gewist.

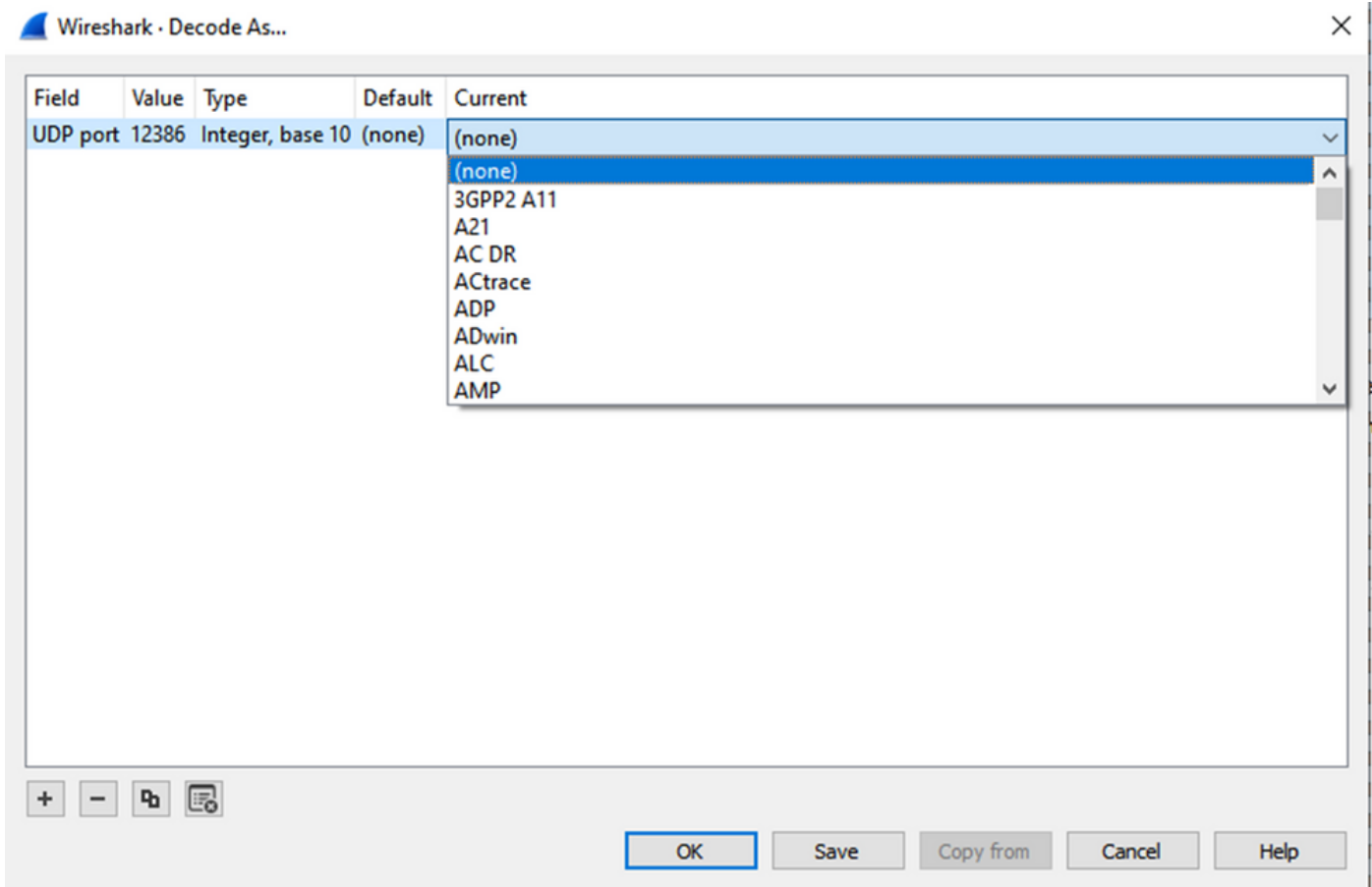
Filter het gewenste verkeer op ESP Sequence

In beide gevallen kan het verkeer worden geïdentificeerd met de ESP-volnummers.

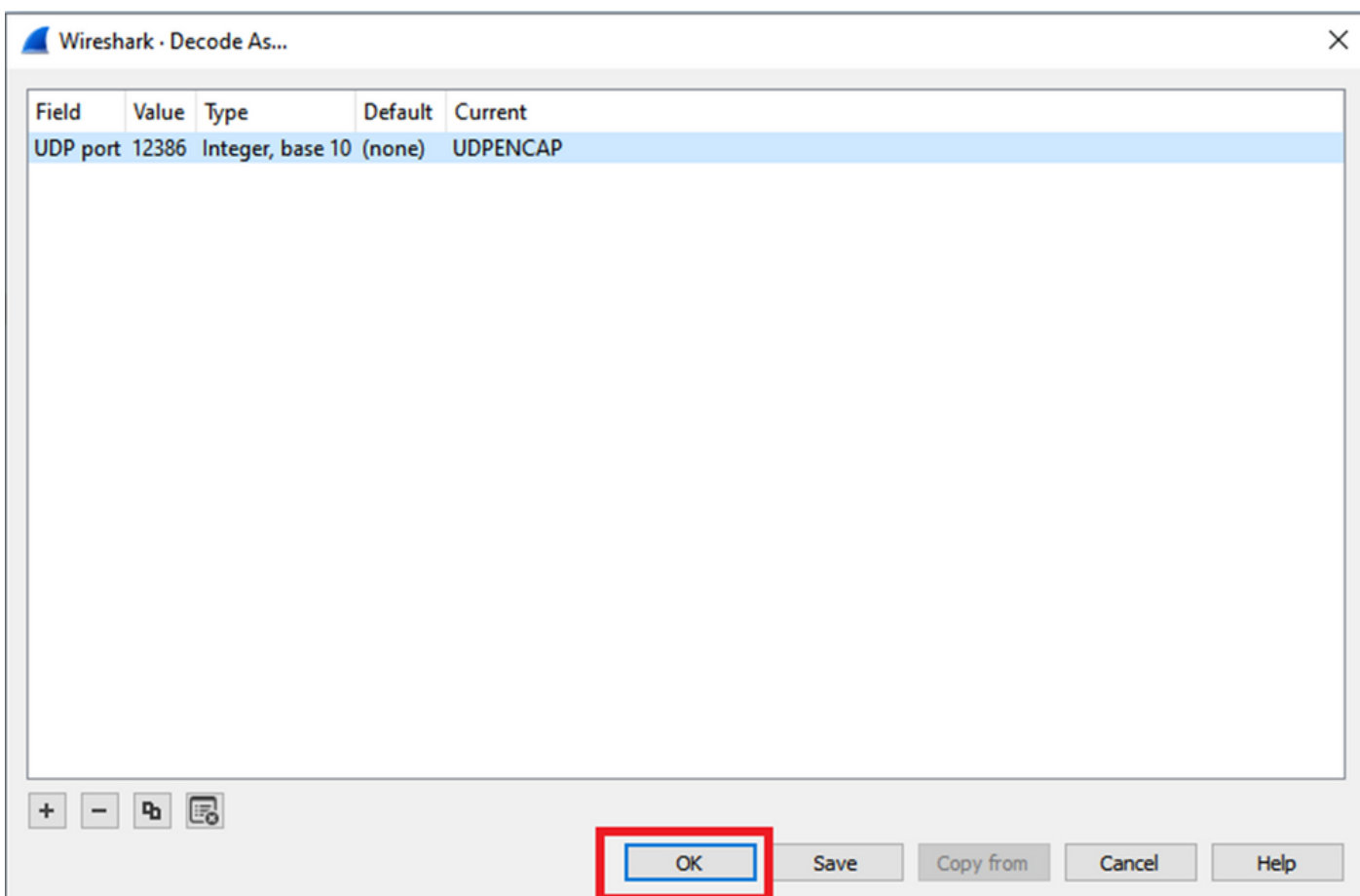
Om de ESP opeenvolgingsaantallen in het pakket te zien, klik op de opname met de rechtermuisknop en kies **Decoderen** zoals getoond.



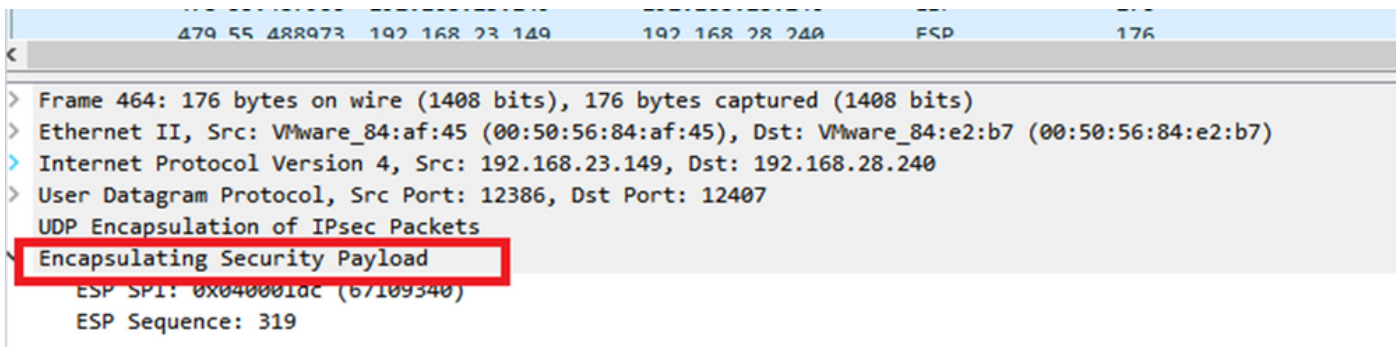
Selecteer het vervolgkeuzemenu **Huidige** veld en selecteer in dat veldtype **UDPENCAP** of selecteer het in de vervolgkeuzelijst.



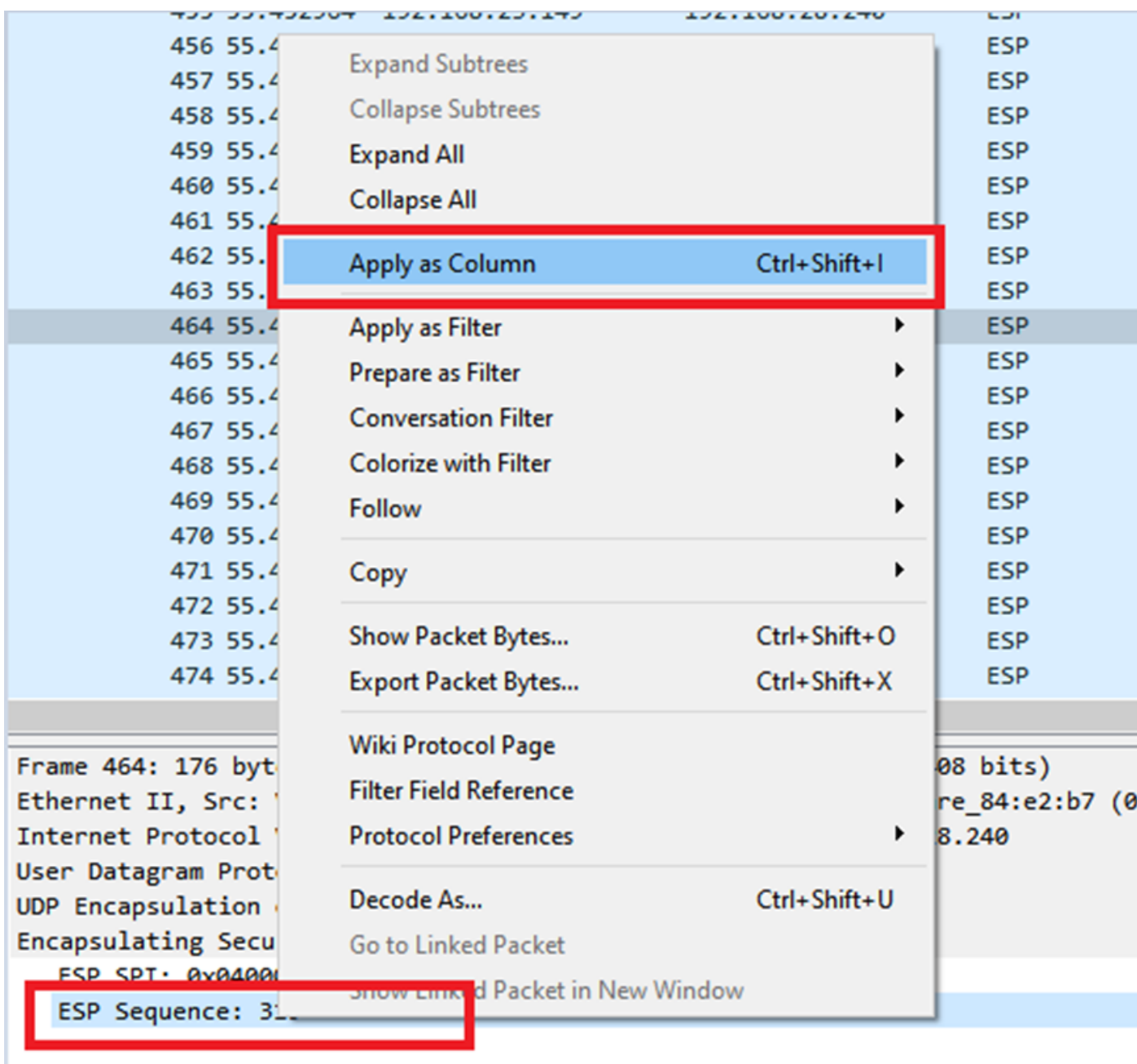
Selecteer **OK** zodra dit is voltooid.



Vouw in het gedeelte Wireshark Packet Details het gedeelte **Encapsulating Security payload** van het pakket uit om **ESP Sequence** te zien.



Klik met de rechtermuisknop op **ESP Sequence** en kies **toepassen als kolom** zodat de ESP Sequence kan worden gezien als een kolom in de sectie Packet List op het bovenste gedeelte van het Wireshark-scherm.



Opmerking: de ESP SPI voor de pakketten op cEdge1 is **0x040001dc**. Dit wordt gebruikt voor een filter op de doelopname.


```

> 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

```

Open de doelopname, herhaal de stappen om te decoderen als **UDPENCAP**, en toon de ESP Sequence nummers in de pakketten.

Zodra de pakketten het ESP volgnummer weergeven, kan de ESP SPI van de eerste opname worden gebruikt als filter op de tweede opname om alleen het verkeer binnen die SPI weer te geven die overeenkomt met het gewenste verkeer.

Bericht dat de aantallen van de pakkeopeenvolging die allebei aanpassen DSCP 27 duidelijk hebben.

The image displays two Wireshark windows side-by-side. The left window shows a packet list with columns for 'ESP Sequence', 'Differentiated Services Codepoint', 'Source Port', 'Destination Port', and 'Sequence Number'. A red box highlights the value '306 27' in the 'Differentiated Services Codepoint' column for the first packet. The right window shows a filter 'esp spi == 0x040001dc' applied to the capture. Below the filter, a table lists ESP packets with columns for 'Protocol', 'Length', 'ESP Sequence', and 'Differentiated Services Codepoint'. A red box highlights the value '306 27' in the 'Differentiated Services Codepoint' column for the first packet in this filtered view. Both windows show detailed packet information for the selected packets, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and UDP Encapsulation of IPsec Packets.

Deze vergelijking kan handmatig worden uitgevoerd in Wireshark of Microsoft Excel kan worden gebruikt om deze vergelijking te doen.

Om Microsoft Excel te gebruiken om te vergelijken, is het noodzakelijk om beide opnamen te snijden om alleen pakketten te bevatten die in beide opnamen zijn.

In de bronopname heeft het eerste relevante pakket ESP-reeks 306 en die correspondeert met pakketnummer 451.

Wireshark interface showing a packet list for the filter 'ip.dsfield.dscp == 27'. The table below represents the data shown in the interface.

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

Het laatste relevante pakket in de bronopname heeft ESP-reeks 405 en is pakketnummer 550.

Wireshark interface showing packets 548, 549, and 550. The table below represents the data shown in the interface.

548	55.600962	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

In de bestemmingsopname komt het eerste relevante pakket overeen met de bronopname met ESP-reeks 306, maar in deze opname is pakket 463.

Wireshark interface showing packets 461, 462, 463, and 464. The table below represents the data shown in the interface.

461	60.522028	192.168.23.149	192.168.28.240	ESP	168		407 Class Se
462	60.715026	192.168.23.149	192.168.28.240	ESP	175		408 Class Se
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

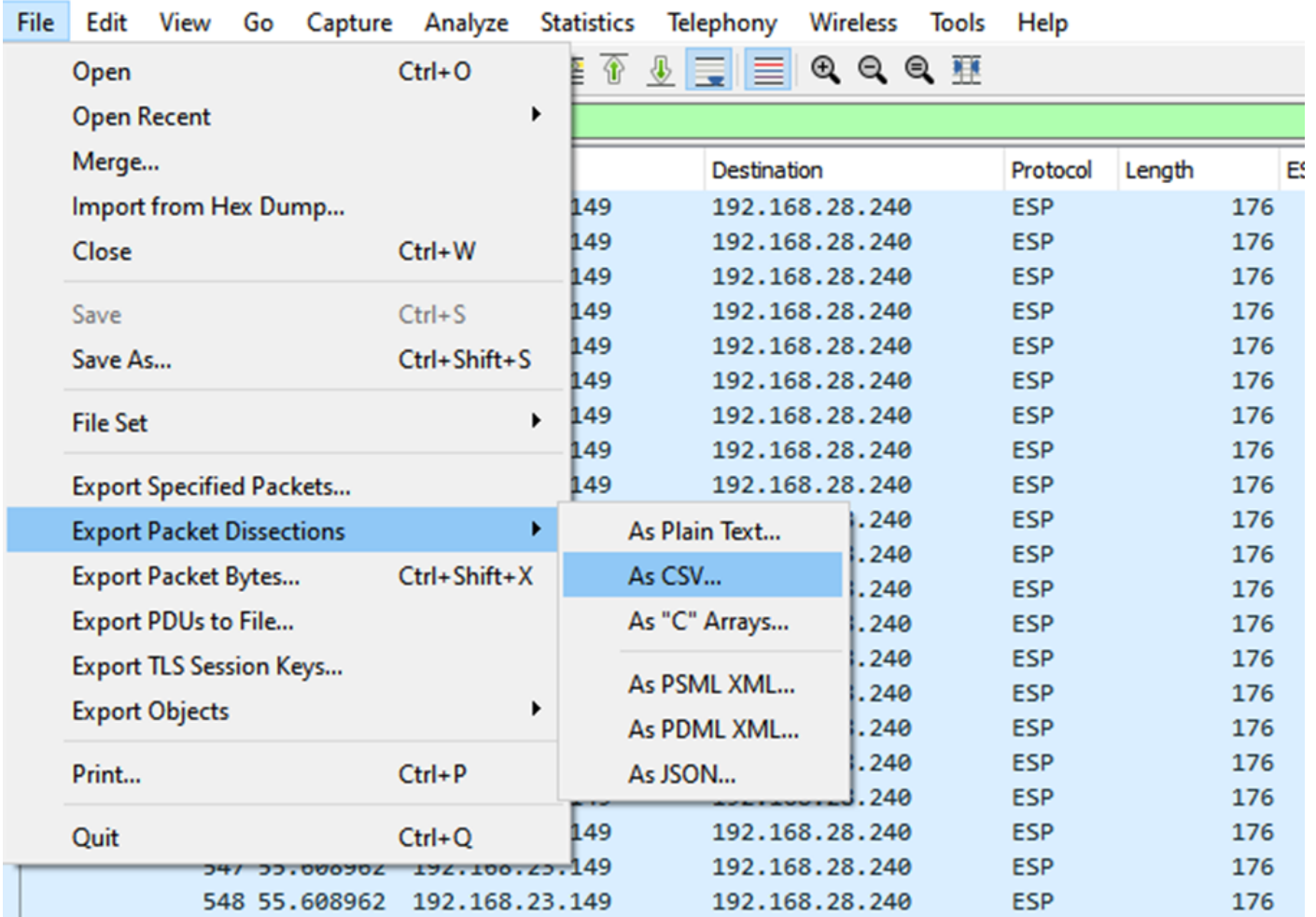
Het laatste relevante pakket is ook aanwezig met ESP Sequence 405 en het is pakket 564.

Wireshark interface showing packets 560, 561, 562, 563, and 564. The table below represents the data shown in the interface.

560	61.165052	192.168.23.149	192.168.28.240	ESP	176		405 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 Se
564	61.584021	192.168.23.149	192.168.28.240	ESP	175		410 Class Se

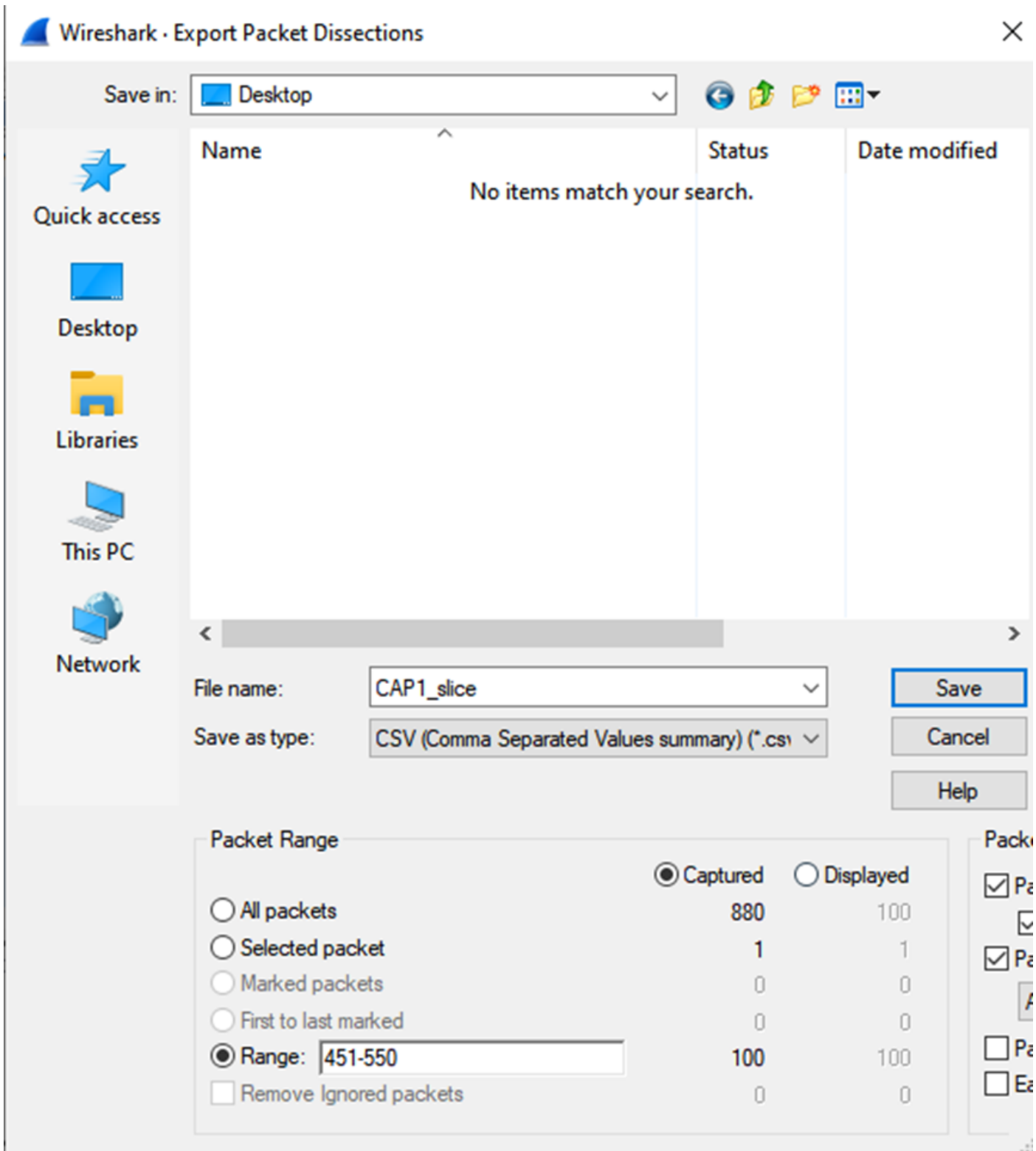
De eerste opname moet nu worden gesneden om alleen relevante pakketten te bevatten.

Navigeer naar **Bestand > Packet Dissections exporteren > Als CSV...**

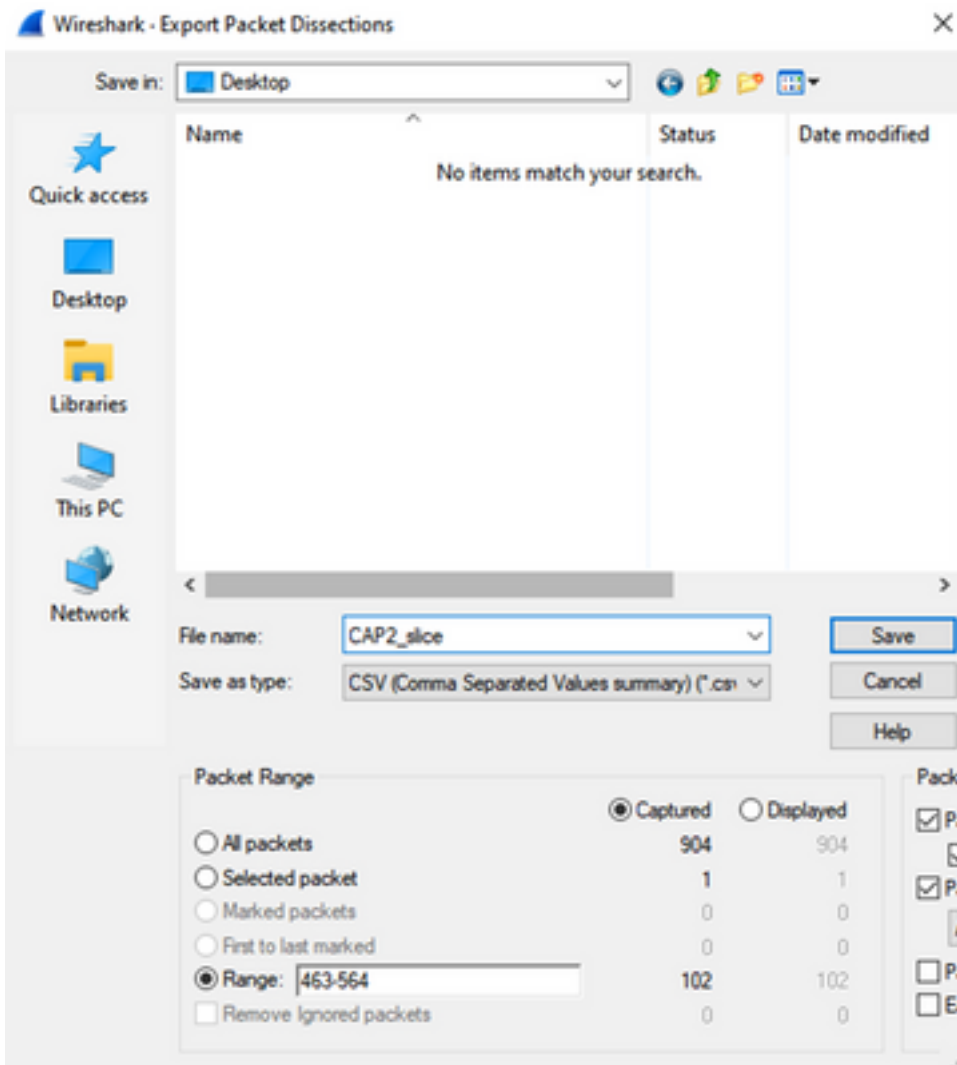


Selecteer **Opgenomen** en **Bereik** en typ in het veld **Bereik** het bereik van het eerste relevante pakket tot het laatste relevante pakket.

Voer een bestandsnaam in het veld **Bestandsnaam in** en klik op **Opslaan**.

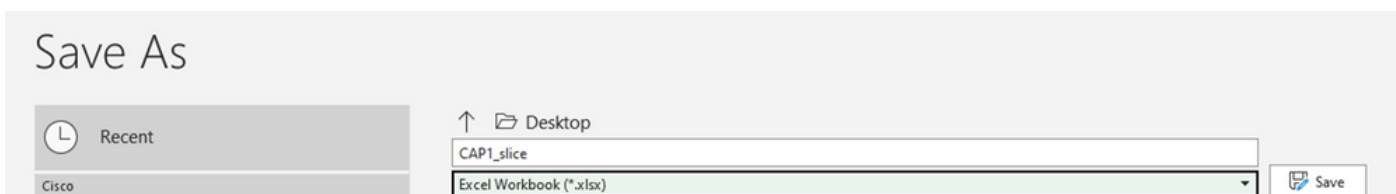


Herhaal hetzelfde proces bij opname 2 voor de desbetreffende pakketten.

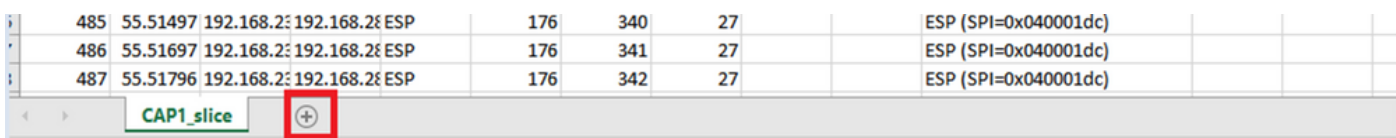


Open beide CSV-bestanden in Microsoft Excel.

Leg op de bron **CSV vast**, behalve als **XLSX formaat**.



Selecteer onder in het scherm het symbool + om een ander vel toe te voegen. Noem het **CAP2_slice**



Open het **CAP2 CSV**-bestand en druk op **CTRL + a** om alle bestanden te selecteren en op **CTRL + c** om het te kopiëren.

	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	192.168.253	192.168.253	ESP	176	306	27			ESP (SPI=0x040001dc)		
3	464	61.00301	192.168.253	192.168.253	ESP	176	307	27			ESP (SPI=0x040001dc)		
4	465	61.00506	192.168.253	192.168.253	ESP	176	308	27			ESP (SPI=0x040001dc)		
5	466	61.00706	192.168.253	192.168.253	ESP	176	309	27			ESP (SPI=0x040001dc)		
6	467	61.00905	192.168.253	192.168.253	ESP	176	310	27			ESP (SPI=0x040001dc)		
7	468	61.01006	192.168.253	192.168.253	ESP	176	311	27			ESP (SPI=0x040001dc)		
8	469	61.01105	192.168.253	192.168.253	ESP	176	312	27			ESP (SPI=0x040001dc)		
9	470	61.01305	192.168.253	192.168.253	ESP	176	313	27			ESP (SPI=0x040001dc)		
10	471	61.01406	192.168.253	192.168.253	ESP	176	314	27			ESP (SPI=0x040001dc)		
11	472	61.01606	192.168.253	192.168.253	ESP	176	315	27			ESP (SPI=0x040001dc)		
12	473	61.01806	192.168.253	192.168.253	ESP	176	316	27			ESP (SPI=0x040001dc)		
13	474	61.02106	192.168.253	192.168.253	ESP	176	317	27			ESP (SPI=0x040001dc)		
14	475	61.02205	192.168.253	192.168.253	ESP	176	318	27			ESP (SPI=0x040001dc)		
15	476	61.02306	192.168.253	192.168.253	ESP	176	319	27			ESP (SPI=0x040001dc)		
16	477	61.02506	192.168.253	192.168.253	ESP	176	320	27			ESP (SPI=0x040001dc)		
17	478	61.02605	192.168.253	192.168.253	ESP	176	321	27			ESP (SPI=0x040001dc)		

Navigeer naar het bestand **CAP1_slice.xlsx** en plak op het tweede tabblad voor CAP2_slice (CTRL + v) de gekopieerde informatie in de cel A1.

Cut
Copy
Format Painter

Calibri 11 A A
B I U

Wrap Text
Merge & Center

General
\$ %

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													

1	No.	Time	Source	Destinatic	Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic	Info	Sequence N
2	463	60.99901	192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=0x040001dc)	
3	464	61.00301	192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=0x040001dc)	
4	465	61.00506	192.168.2	192.168.2	ESP	176	308	27			ESP (SPI=0x040001dc)	
5	466	61.00706	192.168.2	192.168.2	ESP	176	309	27			ESP (SPI=0x040001dc)	
6	467	61.00905	192.168.2	192.168.2	ESP	176	310	27			ESP (SPI=0x040001dc)	
7	468	61.01006	192.168.2	192.168.2	ESP	176	311	27			ESP (SPI=0x040001dc)	
8	469	61.01105	192.168.2	192.168.2	ESP	176	312	27			ESP (SPI=0x040001dc)	
9	470	61.01305	192.168.2	192.168.2	ESP	176	313	27			ESP (SPI=0x040001dc)	
10	471	61.01406	192.168.2	192.168.2	ESP	176	314	27			ESP (SPI=0x040001dc)	
11	472	61.01606	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	61.07305	192.168.2	192.168.2	ESP	176	341	27			ESP (SPI=0x040001dc)	

Navigeer terug naar **CAP1_slice** sheet en maak een nieuwe kolom genaamd **Compare_ESP_SEQUENCE**.

1	No.	Time	Source	Destinatic	Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic	Info	Sequence Number	COMPARE_ESP_SEQUENCE
2	451	55.44196	192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=0x040001dc)		
3	452	55.44598	192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=0x040001dc)		
4	453	55.44807	192.168.2	192.168.2	ESP	176	308	27			ESP (SPI=0x040001dc)		

Aangezien het ESP-volnummer in kolom G staat, stel een VLOOKUP-opdracht samen zoals getoond om de twee bladen te vergelijken om ervoor te zorgen dat alles in kolom G op de bron in kolom G op de bestemming is.

=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"ONTBREEKT","AANWEZIG")

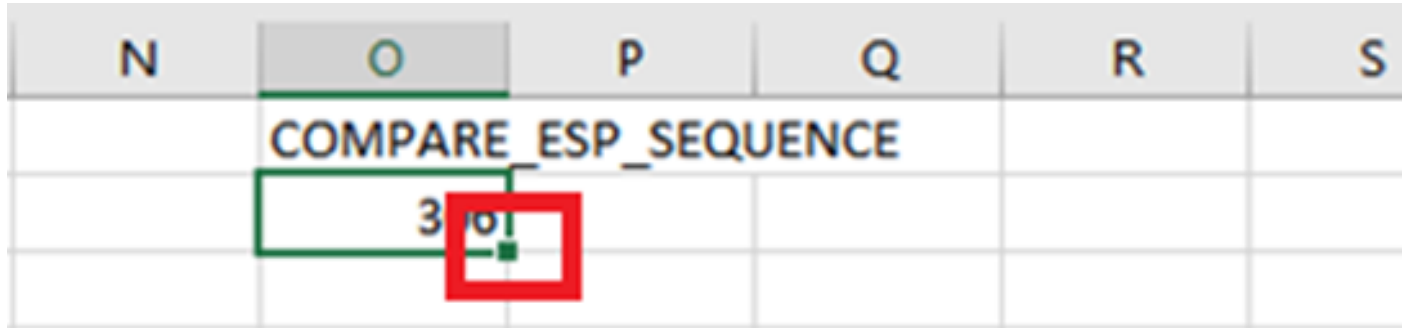
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Time	Source	Destinatic	Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic	Info	Sequence Number			COMPARE	ESP_SEQUENCE								
55.44196	192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=0x040001dc)				=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"MISSING","PRESENT")									
55.44598	192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=0x040001dc)													

Nadat ENTER is geselecteerd wordt het woord **PRESENT** weergegeven. Dit betekent dat het pakket met ESP Sequence **306** in het tweede blad aanwezig is. Dit is belangrijk omdat het

betekent dat het pakket het van de bron naar de bestemming maakte.

No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Differentiated	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)			

Selecteer Kolom O Rij 2 en zweef rechtsonder in het groene vak rond die cel.

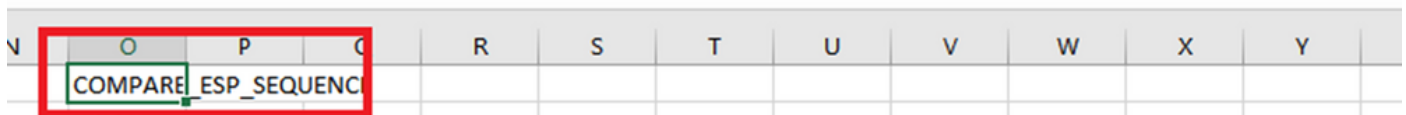
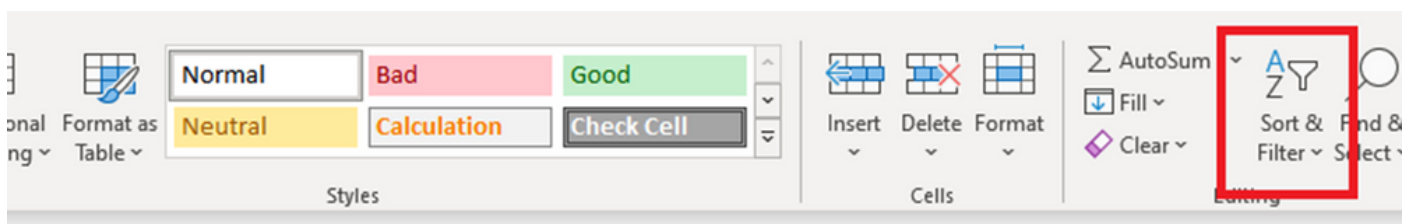


Selecteer en houd de muis ingedrukt om deze formule naar de onderkant van de cellen met waarden te kopiëren.

=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)), "MISSING", "PRESENT")

Time	Source	Destination	Protocol	Length	ESP Sequence	Differentiated	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)			
55.50297	192.168.2.2	192.168.2.2	ESP	176	324	27		ESP (SPI=0x040001dc)		PRESENT	
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	
55.60796	192.168.2.2	192.168.2.2	ESP	176	398	27		ESP (SPI=0x040001dc)		PRESENT	
55.60896	192.168.2.2	192.168.2.2	ESP	176	399	27		ESP (SPI=0x040001dc)		PRESENT	
55.60996	192.168.2.2	192.168.2.2	ESP	176	400	27		ESP (SPI=0x040001dc)		PRESENT	
55.61096	192.168.2.2	192.168.2.2	ESP	176	401	27		ESP (SPI=0x040001dc)		PRESENT	
55.61196	192.168.2.2	192.168.2.2	ESP	176	402	27		ESP (SPI=0x040001dc)		PRESENT	
55.61296	192.168.2.2	192.168.2.2	ESP	176	403	27		ESP (SPI=0x040001dc)		PRESENT	
55.61396	192.168.2.2	192.168.2.2	ESP	176	404	27		ESP (SPI=0x040001dc)		PRESENT	
55.61496	192.168.2.2	192.168.2.2	ESP	176	405	27		ESP (SPI=0x040001dc)		PRESENT	

Scroll terug naar de bovenkant van het blad en klik op **Compare_ESP_SEQUENCE**. Selecteer vervolgens **Sorteren en filteren**.



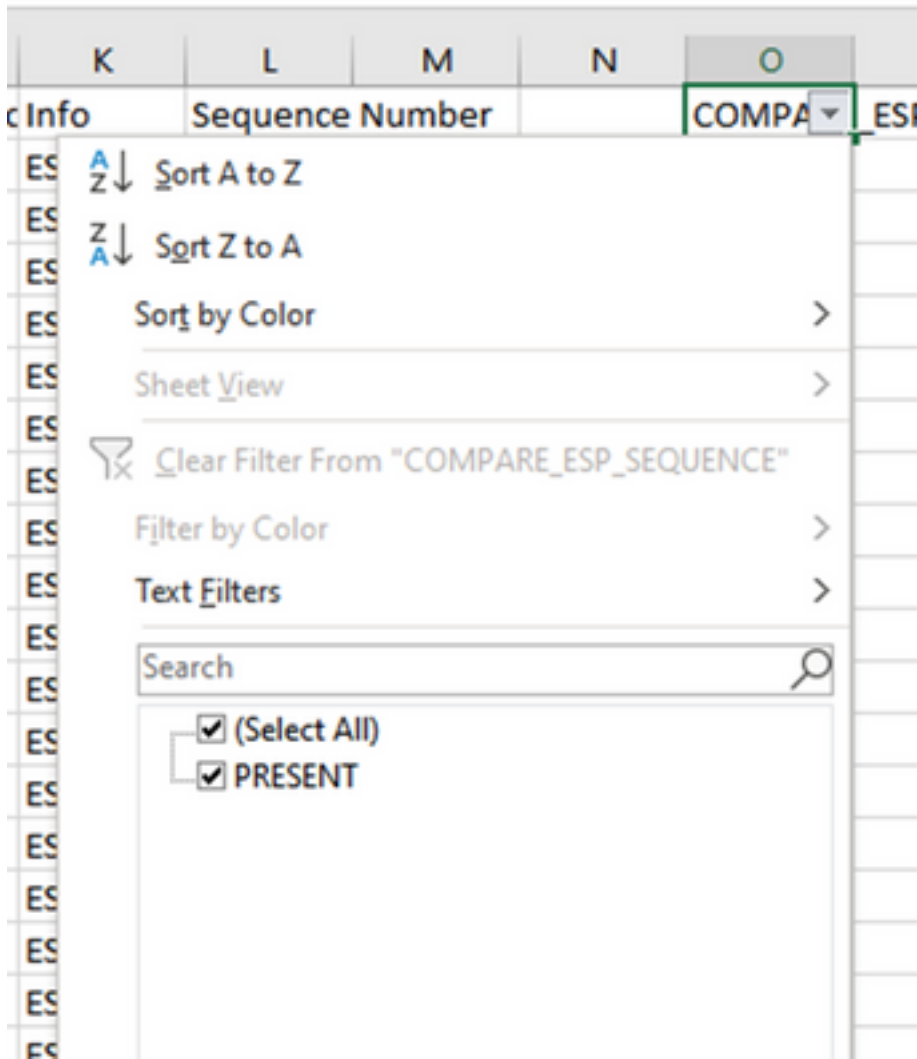
Kies **Filter** in het uitrolmenu.



Er verschijnt een vervolgkeuzemenu in de kolom **Compare_ESP_SEQUENCE**.

M	N	O	P
Number		COMPARISON	ESP_SEQUENCE
		PRESENT	
		PRESENT	
		PRESENT	

Klik op het vervolgkeuzemenu in de kop **VERGELIJKEN_ESP_SEQUENCE**. Merk op dat in dit voorbeeld, de enige getoonde waarde **AANWEZIG** is. Dit betekent dat alle pakketten aanwezig zijn in beide opnamen.




Om een problematisch voorbeeld te creëren, verwijder 10 pakketten van de CAP2_slice, om aan te tonen hoe dit zou werken in een test waar sommige gemiste pakketten ontbreken.


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)


Navigeer terug naar **CAP1_slice** sheet en nu wordt gezien dat er 10 pakketten ontbreken.


Seq	Time	Src	Dest	Protocol	Len	Off	Len	Off	Protocol	Present
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


Wanneer het dropdown menu is geselecteerd in de kolom **Compare_ESP_SEQUENCE**, zien we nu dat er ook **ONTBREKENDE** pakketten zijn. Dit kan worden omgeschakeld om alleen de **ONTBREKENDE** pakketten te bekijken.


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"

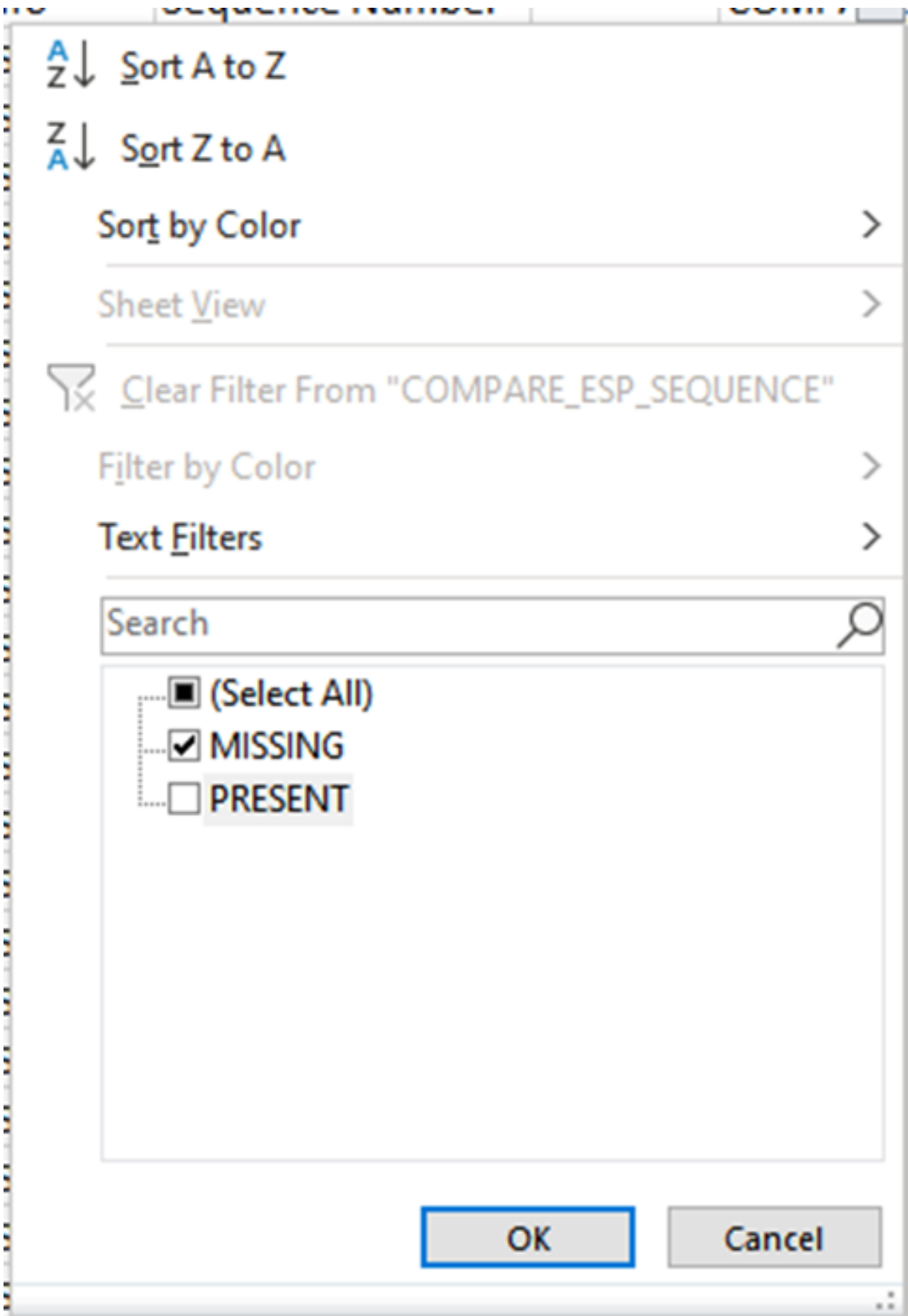
Filter by Color 

Text Filters 

Search 

- (Select All)
- MISSING
- PRESENT

OK Cancel



Nu worden alleen de ontbrekende pakketten getoond in het Excel-blad.

	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	192.168.2	ESP	176	318	27			ESP (SPI=0x040001dc)					MISSING
5	464	55.46697	192.168.2	192.168.2	ESP	176	319	27			ESP (SPI=0x040001dc)					MISSING
6	465	55.46796	192.168.2	192.168.2	ESP	176	320	27			ESP (SPI=0x040001dc)					MISSING
7	466	55.46996	192.168.2	192.168.2	ESP	176	321	27			ESP (SPI=0x040001dc)					MISSING
8	467	55.47097	192.168.2	192.168.2	ESP	176	322	27			ESP (SPI=0x040001dc)					MISSING
9	468	55.47198	192.168.2	192.168.2	ESP	176	323	27			ESP (SPI=0x040001dc)					MISSING
0	469	55.47297	192.168.2	192.168.2	ESP	176	324	27			ESP (SPI=0x040001dc)					MISSING
1	470	55.47497	192.168.2	192.168.2	ESP	176	325	27			ESP (SPI=0x040001dc)					MISSING
2	471	55.47597	192.168.2	192.168.2	ESP	176	326	27			ESP (SPI=0x040001dc)					MISSING
3	472	55.47697	192.168.2	192.168.2	ESP	176	327	27			ESP (SPI=0x040001dc)					MISSING
12																
13																

Gerelateerde informatie

- [Cisco ingesloten pakketvastlegging](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.