

# Converteren van access point pakketdumps voor Wireshark

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Procedure](#)

[Packet Dump uitvoeren](#)

[Opschonen van uitvoerbestanden](#)

[Samenvatting van pakketinformatie opschonen](#)

[Startspaties en offset-dubbelpunten verwijderen](#)

[Correcte pakketoffset](#)

[Afzonderlijke pakketbytes](#)

[Het Tekstbestand converteren naar PCAP](#)

[Via Wireshark GUI](#)

[Via opdrachtregel](#)

[Probleemoplossing](#)

[Tekstbestand is correct maar Text2pcap kan geen pakketten lezen](#)

[Inconsistente offset](#)

---

## Inleiding

Dit document beschrijft hoe u een door COS Access Point gegenereerd pakketdump naar PCAP-indeling voor Wireshark kunt converteren als tijdelijke oplossing voor de groottebeperking.

## Voorwaarden

- Kladblok++ - Alleen beschikbaar voor Windows
- Text2pcap geïnstalleerd - inbegrepen op regelmatige installaties van Wireshark

## Procedure

### Packet Dump uitvoeren

Leg een AP-pakketdump vast door de opdracht debug verkeer bekabeld <meervoudige opties> breedspakig op de AP-opdrachtregel uit te voeren. U kunt kiezen tussen meerdere filters en interfaces.

Log de sessie in de terminal.

Zorg ervoor dat de minste hoeveelheid toetsaanslagen wordt verzonden als u dit doet, zodat de

meer afdrubare tekens in het bestand die niet bij de opname zelf horen, beter worden schoongemaakt voordat de conversie wordt uitgevoerd.

De gemakkelijkste manier om het te doen is een consolesessie voor de pakketdump, repliceer het probleem, stop de dump en onmiddellijk beëindigen van de sessie.

Als u de stortplaats via ssh uitvoert gebruik een filter om alleen het verkeer van belang te vangen. Anders bevat de opname de SSH-sessiepakketten.

Raadpleeg [Probleemoplossing van COS-AP's](#) voor volledige instructies over hoe de opname te configureren.

Wanneer u klaar bent, stopt u de opname met de opdracht `undebug all`. Het resulterende bestand ziet er als volgt uit:

```
AP-9105>en
Password:
AP-9105#debug traffic wired udp
  capture capture packets in pcap file
  verbose Verbose Output
  <cr>
AP-9105#debug traffic wired udp verbose
AP-9105#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
22:35:17.1669188 IP CSC0-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656
    0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
    0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
    0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
    0x0030:  7665 7273 696f 6e3d 2231 2e30 2220 656e
    0x0040:  636f 6469 6e67 3d22 7574 662d 3822 3f3e
<truncated>
undebug 0x0070:  444c 4e41 444f 432f 312e 3530 2050 6c61
    0x0080:  7469 6e75 6d2f 312e 302e 342e 320d 0a4d
    0x0090:  414e 3a20 2273 7364 703a 6469 7363 6f76
    0x00a0:  6572 220d 0a53 543a 2073 7364 703a 616c
all     0x00b0:  6c0d 0a4d 583a 2033 0d0a 0d0a
<truncated>
tcpdump: pcap_loop: error reading dump file: Interrupted system call
All possible debugging has been turned off
<end of file>
```

## Opschonen van uitvoerbestanden

Verwijder alle informatie die geen deel uitmaakt van de pakketstortplaats zelf. Verwijdert de lijnen die de opdracht dump bevatten, elke prompt die de hostnaam (APname#) bevat en alle andere niet-verwante syslog-berichten die in het bestand aanwezig zijn.

Besteed speciale aandacht aan het `undebug` bevel aangezien het vóór een pakketinhoud zoals hierboven getoond kan worden gedrukt. Na de opschonen ziet het resulterende bestand er als

volgt uit:

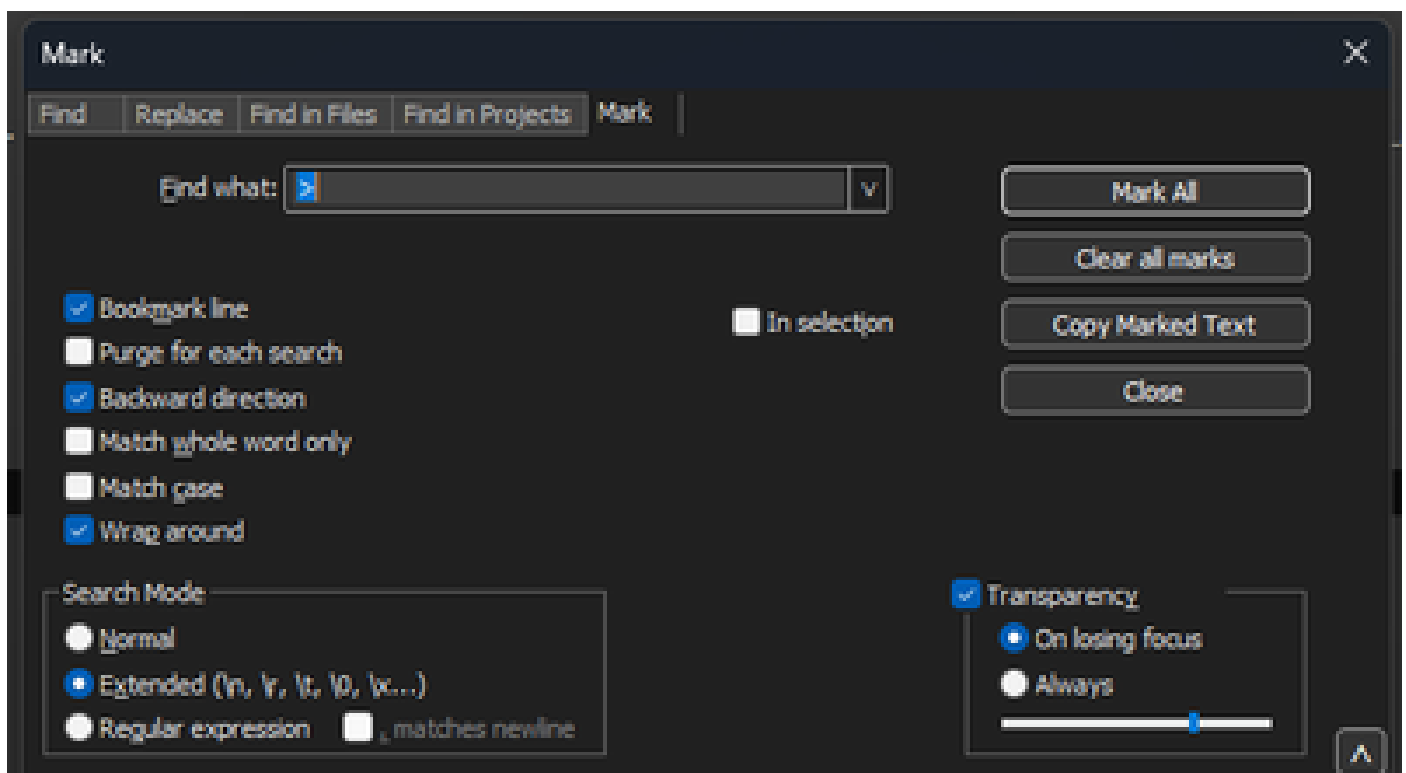
```
22:35:17.1669188 IP CSC0-W-PF320YP6.1an.60354 > 239.255.255.250.3702: UDP, length 656
 0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
 0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
 0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
 0x0030: 7665 7273 696f 6e3d 2231 2e30 2220 656e
 0x0040: 636f 6469 6e67 3d22 7574 662d 3822 3f3e
<truncated>
 0x0070: 444c 4e41 444f 432f 312e 3530 2050 6c61
 0x0080: 7469 6e75 6d2f 312e 302e 342e 320d 0a4d
 0x0090: 414e 3a20 2273 7364 703a 6469 7363 6f76
 0x00a0: 6572 220d 0a53 543a 2073 7364 703a 616c
 0x00b0: 6c0d 0a4d 583a 2033 0d0a 0d0a
```

## Samenvatting van pakketinformatie opschonen

Het begin van een nieuw pakket wordt gedetecteerd wanneer er een nieuwe offset 000000 verschijnt. Text2pcap kan de summierende informatie behandelen die voor elk pakket wordt afgedrukt, om problemen te vermijden is best om ze te verwijderen.

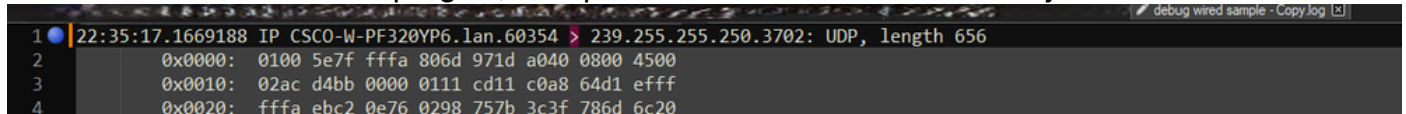
Ga in Kladblok++ naar Zoeken>Zoeken en selecteer het tabblad Markeren, om er zeker van te zijn dat de zoekmodus uitgebreid is.

Typ in het veld Wat zoeken: voer het symbool in > en klik op Alles markeren. Deze actie beschrijft alle regels met het > symbool.



Kladblok++ markeren dialogovenster met Zoeken naar welk veld met het chevron-teken erin.

Na het markeren van de kopregels, Notepad++ benadrukt alle documentlijnen als dit:



```
1 22:35:17.1669188 IP CSCO-W-PF320YP6.1an.60354 > 239.255.255.250.3702: UDP, length 656
2 0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
3 0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
4 0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
```

Packet dump snippet met gemarkeerde lijn die de chevron bevat.

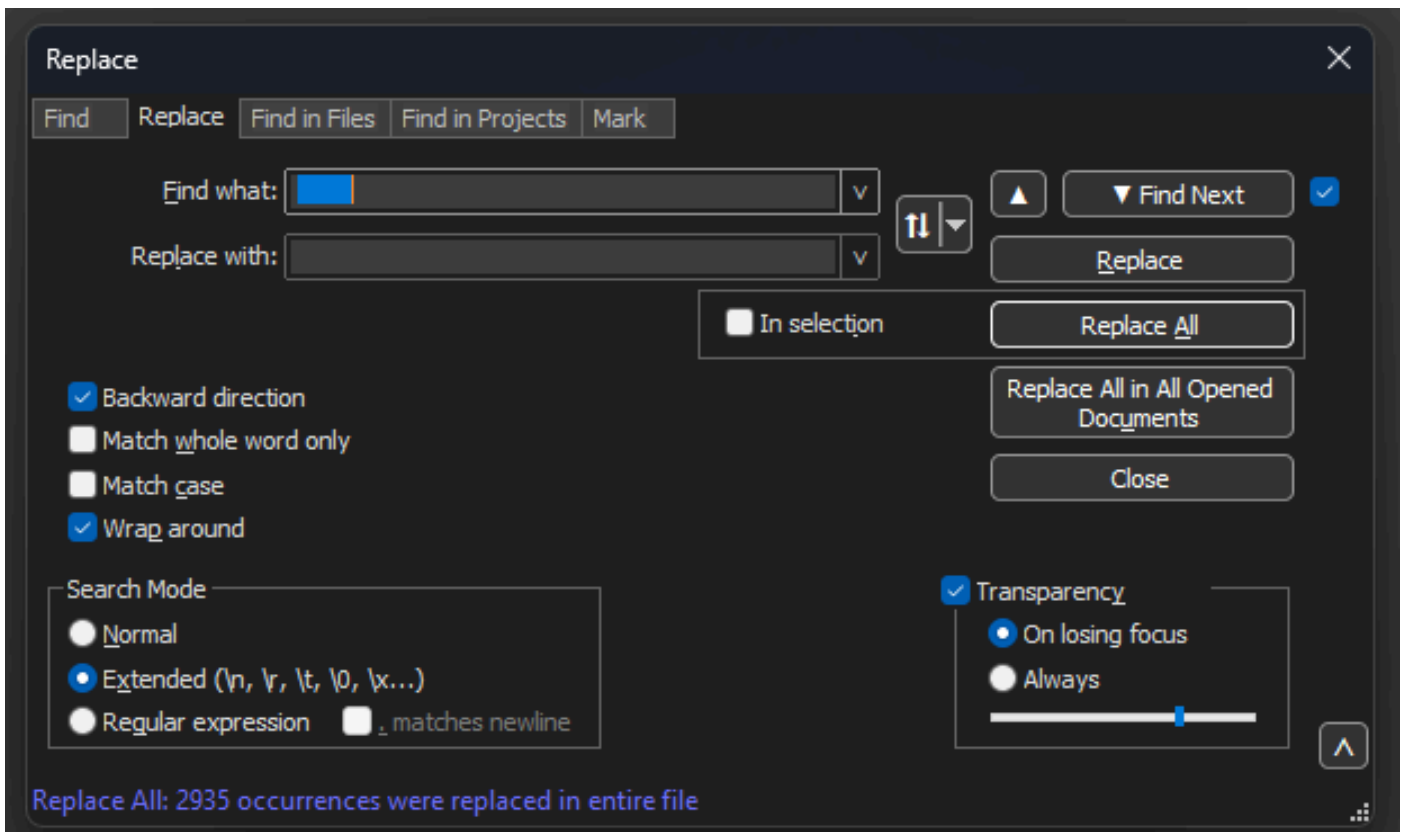
Navigeer naar Zoeken>Bladwijzer en klik op Bladwijzers verwijderen. Daarna ziet het bestand er zo uit als dit fragment:

```
0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030: 7665 7273 696f 6e3d 2231 2e30 2220 656e
```

## Startspaties en offset-dubbelpunten verwijderen

Navigeer naar Zoeken>Zoeken en selecteer het tabblad Vervangen, om er zeker van te zijn dat de zoekmodus is uitgebreid.

In het veld Zoeken wat: voer 8 spaties in. Laat het veld Vervangen met: veld leeg en klik op Alles vervangen. Dit vervangt alle 8 opeenvolgende witte ruimten aan het begin van elke lijn met niets, effectief hen wissen. Het dialoogvenster Vervangen ziet er precies zo uit als deze afbeelding.

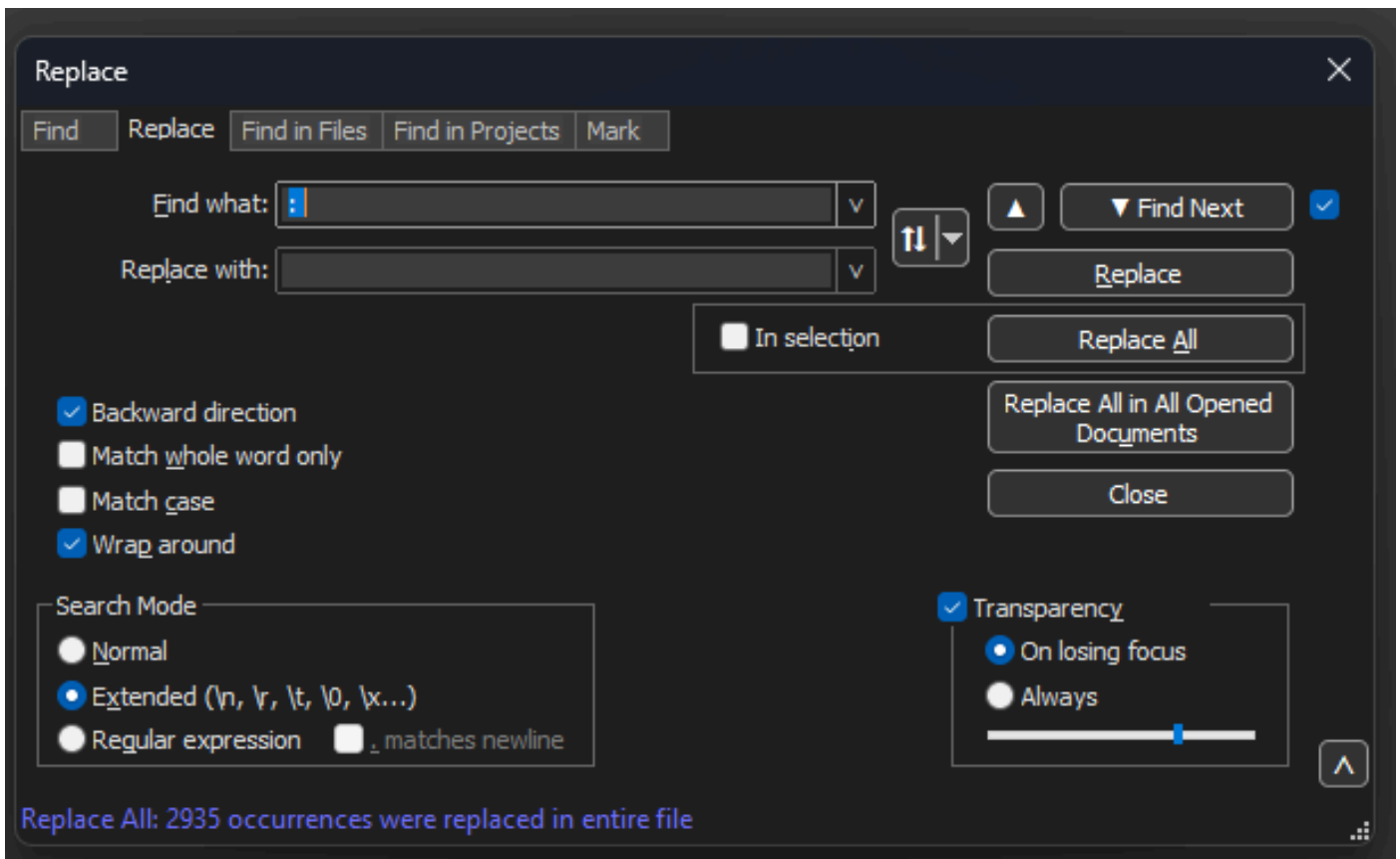


Kladblok++ Dialogvenster vervangen met Zoeken naar welk veld met 8 spaties.

Het resulterende bestand na deze bewerking ziet er zo uit als dit fragment:

```
0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030:  7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040:  636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050:  3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060:  6d6c 6e73 3a73 6f61 703d 2268 7474 703a
0x0070:  2f2f 7777 772e 7733 2e6f 7267 2f32 3030
```

Navigeer naar Zoeken>Zoeken en selecteer het tabblad Vervangen, om er zeker van te zijn dat de zoekmodus uitgebreid is. Geef op : (merk de lege ruimte na de dubbele punt op) in het veld Zoeken wat:. Laat het veld Vervangen met: veld leeg en klik op Alles vervangen. Dit vervangt alle dubbele punten en eerste spaties na de offset.



Kladblok++ Dialogvenster vervangen met Zoeken naar welk veld gevuld is met een dubbele punt en een spatie.

Na de vorige bewerking ziet het resulterende uitvoerbestand er als volgt uit:

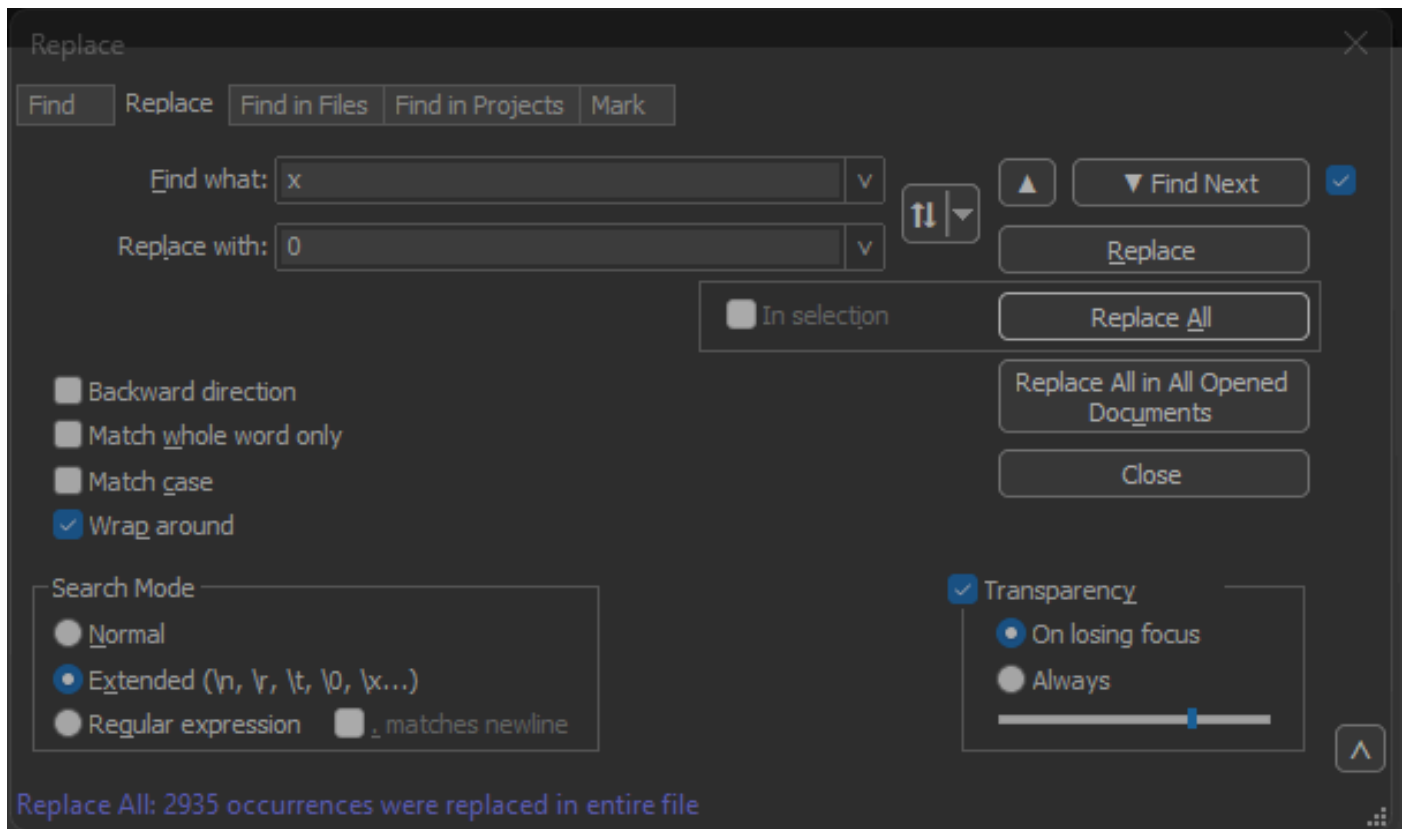
```
0x0000 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060 6d6c 6e73 3a73 6f61 703d 2268 7474 703a
0x0070 2f2f 7777 772e 7733 2e6f 7267 2f32 3030
```

## Correcte pakketoffset

Text2pcap verwacht pakketoffset in elk pakket als een 6-karakter hex-string, maar AP-pakketdumps gebruiken 0x om de offset in plaats daarvan te symboliseren. Als u de fout wilt corrigeren, gaat u naar Zoeken>Zoeken en selecteert u het tabblad Vervangen. Controleer of de zoekmodus is uitgebreid.

Typ x in het veld Wat zoeken:. Vul het veld Vervangen met: veld met 0 en klik op Alles vervangen.

Dit vervangt alle x binnen de offset door 0 om het verwachte offset-formaat voor Text2pcap aan te passen.



Kladblok++ Dialoogvenster vervangen met Vondst welk veld gevuld was met het teken x en Veld vervangen met het teken 0.

Na de vorige bewerking ziet het resulterende uitvoerbestand er als volgt uit:

```
000000 0100 5e7f fffa 806d 971d a040 0800 4500
000010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
000020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
000030 7665 7273 696f 6e3d 2231 2e30 2220 656e
000040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
000050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
```

## Afzonderlijke pakketbytes

Text2pcap-dataformaat vereist dat elk paar hexuitdraai door een spatie van elkaar wordt gescheiden, een onjuist formaat zorgt ervoor dat Text2pcap pakketgegevens als een offset leest en mislukt.

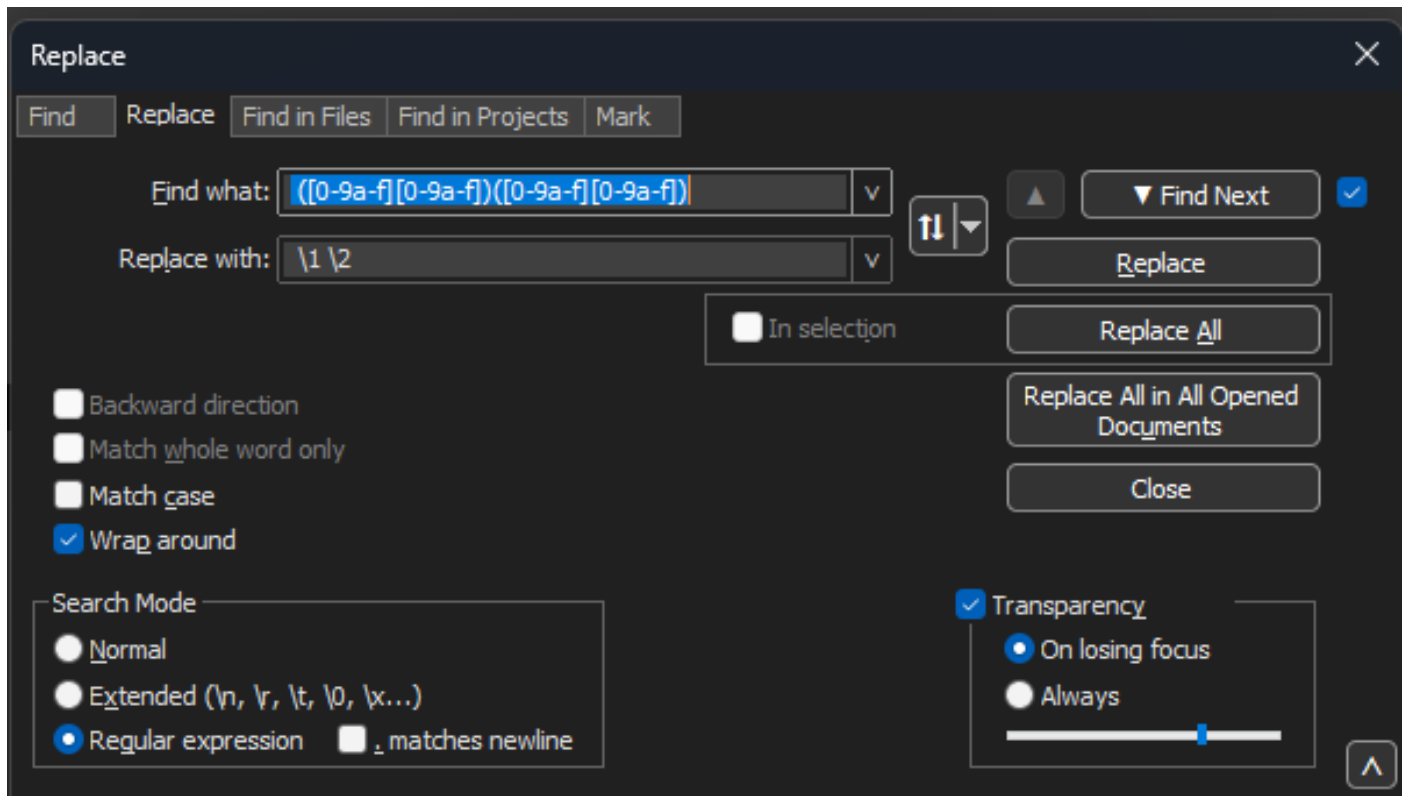
Navigeer naar Zoeken>Zoek en selecteer het tabblad Vervangen, zodat de zoekmodus reguliere expressie is.

Voer `(([0-9a-f][0-9a-f])([0-9a-f][0-9a-f])` (let op de ruimte aan de voorkant) in op het veld Zoeken wat:.

Vul het veld Vervangen met: veld met `\1 \2` (merk de ruimte aan het begin op) en klik op Alles vervangen.

Vervang de operatie vindt de hexuitdraai bytes van het pakket en plaatst een ruimte tussen elk paar. De regex komt overeen met een ruimte gevolgd door een hexuitdraaicijfpaar, slaat ze op opnamegroep 1, neemt vervolgens het aangrenzende paar hexuitdraaicijfers, slaat ze op opnamegroep 2. De vervanging drukt zowel vereiste ruimtes als de inhoud van elke opnamegroep af.

Dit duurt meerdere seconden of minuten, afhankelijk van de lengte van het bestand. Het maakt gebruik van veel RAM tijdens het uitvoeren Als het bestand groot is, wees geduldig.



Kladblok++ Vervang het dialoogvenster met de zoekfunctie die met een reguliere expressie is gevuld en het veld Vervangen die met een andere reguliere expressie is gevuld.

Na de vorige handeling ziet het resulterende uitvoerbestand er precies zo uit als dit fragment en kan het worden geconverteerd door Text2pcap.

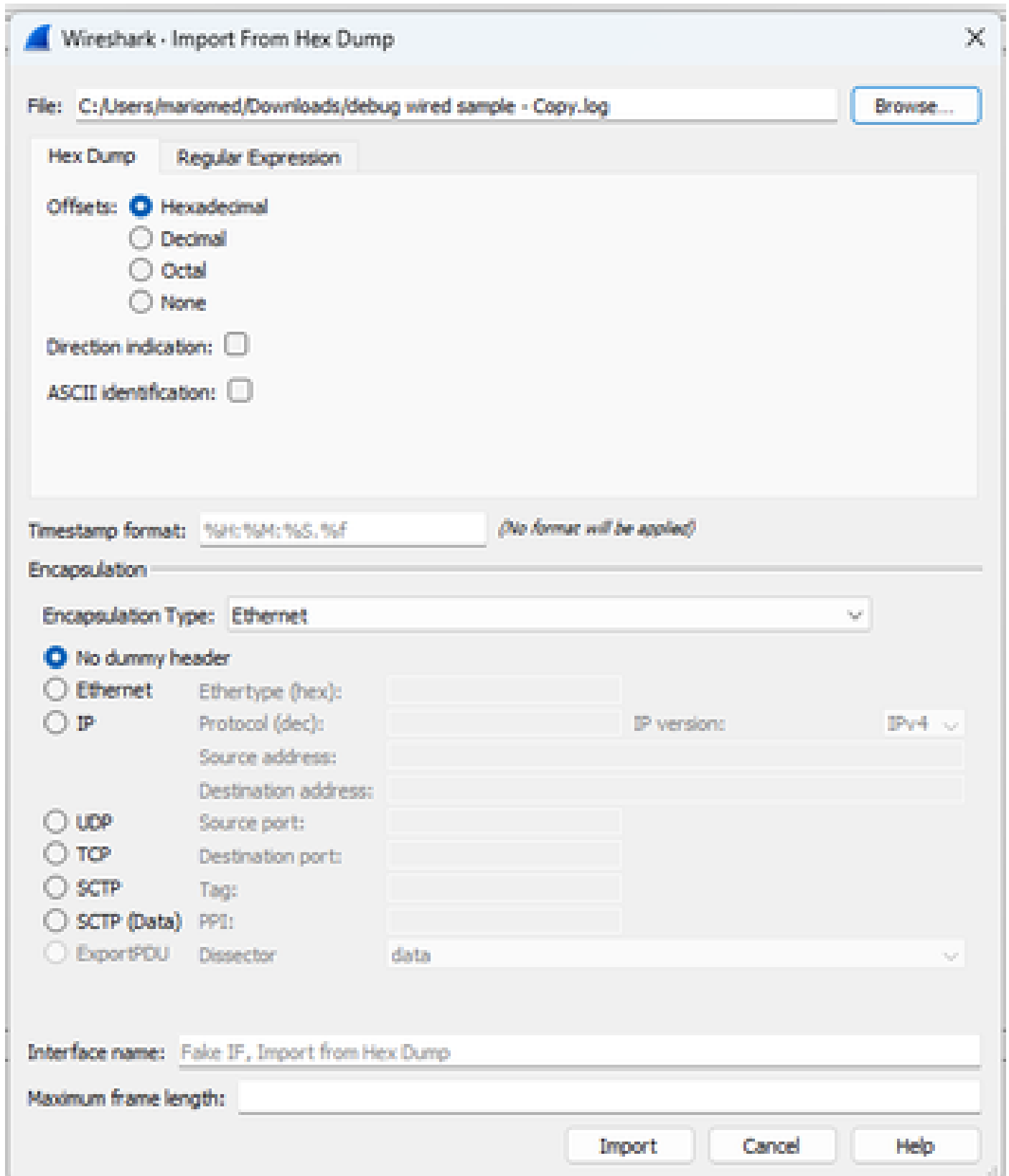


```
000000 01 00 5e 7f ff fa 80 6d 97 1d a0 40 08 00 45 00
000010 02 ac d4 bb 00 00 01 11 cd 11 c0 a8 64 d1 ef ff
000020 ff fa eb c2 0e 76 02 98 75 7b 3c 3f 78 6d 6c 20
000030 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e
000040 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e
000050 3c 73 6f 61 70 3a 45 6e 76 65 6c 6f 70 65 20 78
000060 6d 6c 6e 73 3a 73 6f 61 70 3d 22 68 74 74 70 3a
000070 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30
000080 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f
000090 70 65 22 20 78 6d 6c 6e 73 3a 77 73 61 3d 22 68
```

## Het Tekstbestand converteren naar PCAP

### Via Wireshark GUI

Om het volledige bestand naar pcap te converteren, Wireshark te openen en naar Bestand>Importeren vanaf hex dump te navigeren, verschijnt een dialoogvenster.



Dialogvenster voor importeren van draadloze haaien

Klik op de knop Bladeren... en selecteer het tekstbestand met de dump. Zorg ervoor dat het geselecteerde offset-type hexadecimaal is, insluitingstype Ethernet is en er geen dummyheader is

geselecteerd.

Klik op Importeren om het conversieproces te starten.

## Via opdrachtregel

Als u een tekstbestand in een pcap-bestand in de opdrachtregel van Windows wilt converteren, voert u <path to wireshark install folder>text2pcap.exe <path to text file pcap> <path van uitvoerbestand> uit.

U kunt naar keuze wireshark map aan uw PAD toevoegen, anders moet u text2pcap uitvoeren met verwijzing naar het gehele pad naar text2pcap.exe telkens als u een bestand converteert.

Text2pcap.exe wordt gevestigd binnen de wireshark installatiemap.

```
PS C:\Users\mariomed\Downloads> text2pcap "debug wired sample - Copy.log" final.pcap
Input from: debug wired sample - Copy.log
Output to: final.pcap
Output format: pcapng

-----
Read 147 potential packets, wrote 147 packets (50904 bytes including overhead).
```

Uitvoer van Windows-opdrachtregel na de succesvolle pakketdump-conversie

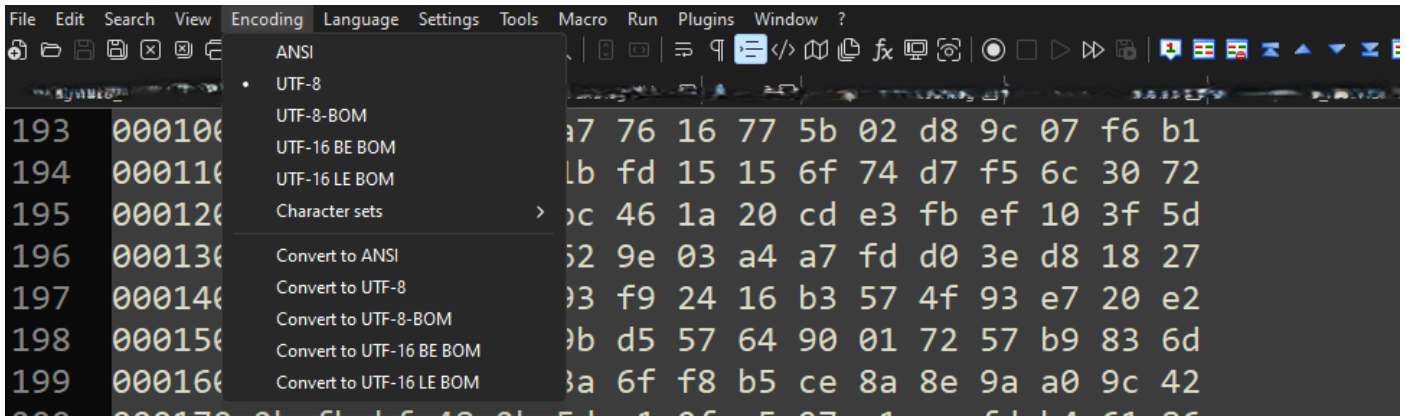
Text2pcap bevat ook meerdere regex-opties om het tekstbestand vooraf te verwerken, raadpleeg de [Text2pcap handleiding pagina](#) voor meer informatie.

## Probleemoplossing

### Tekstbestand is correct maar Text2pcap kan geen pakketten lezen

Text2pcap kan bepaalde bestandencoderingen niet lezen die door terminalemulators worden geproduceerd die vaak worden gebruikt (Secure CRT, Putty of anderen).

Verandering in een coderende leesbaar door Text2pcap met Kladblok++. Ga naar Encoding>UTF-8 en sla het bestand op, en converteer vervolgens nogmaals naar pcap.



Kladblok++ coderingsmenu-opties.

## Inconsistente offset

Deze fout verschijnt wanneer de bytes van het gegevensgedeelte op een pakket niet correct in paren worden gescheiden, dit veroorzaakt Text2pcap om het begin van een nieuw pakket te veronderstellen en er niet in slaagt om te interpreteren.

Zoek naar pakketbytes zonder scheiding of koorden in het midden van een pakketinhoud zoals de undebug all opdracht.

```
C:\Users\mariomed>text2pcap "C:\Users\mariomed\Downloads\debug wired sample - Copy.log" output.pcap
Input from: C:\Users\mariomed\Downloads\debug wired sample - Copy.log
Output to: output.pcap
Output format: pcapng
** (text2pcap:81244) 10:30:46.781149 [(none) MESSAGE] -- Inconsistent offset. Expecting 75, got 80. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.781712 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782136 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782446 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782599 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782748 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782891 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783033 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783169 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783319 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783456 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
```

*Uitvoer van Windows-opdrachtregel na ongeldig bestand wordt geprobeerd te converteren. Inconsistente offset wordt meerdere malen op de terminal afgedrukt.*

## 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.