

Konvertieren von Packet Dumps für Access Points für Wireshark

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Vorgehensweise](#)

[Paketausgabe durchführen](#)

[Bereinigung der Ausgabedatei](#)

[Zusammenfassende Informationen zum Cleanup-Paket](#)

[Entfernen von Anfangsräumen und Versatzkollisionen](#)

[Korrekturer Paket-Offset](#)

[Separate Paketbytes](#)

[Konvertieren der Textdatei in PCAP](#)

[Über Wireshark-GUI](#)

[Über Kommandozeile](#)

[Fehlerbehebung](#)

[Textdatei ist korrekt, aber Text2pcap kann keine Pakete lesen](#)

[Inkonsistenter Offset](#)

Einleitung

In diesem Dokument wird beschrieben, wie ein von einem COS-Zugangspunkt generiertes Paketspeicherabbild in das PCAP-Format für Wireshark konvertiert wird, um die Größenbeschränkung zu umgehen.

Voraussetzungen

- Notepad++ - Nur unter Windows verfügbar
- Installierte Text2pcap - in regelmäßigen Installationen von Wireshark enthalten

Vorgehensweise

Paketausgabe durchführen

Erfassen Sie ein AP-Paketdump, indem Sie den Befehl `debug traffic` mit `<multiple options>` ausführliche Informationen auf der AP-Befehlszeile ausführen. Sie können zwischen mehreren Filtern und Schnittstellen wählen.

Protokollieren Sie die Sitzung im Terminal.

Achten Sie darauf, die geringste Anzahl von Tastenanschlägen zu senden, wenn Sie dies tun, die druckbareren Zeichen in der Datei, die nicht zur Erfassung selbst gehören, desto mehr Säuberung müssen Sie vor der Konvertierung tun.

Der einfachste Weg hierfür ist eine Konsolensitzung für das Paket-Dump, um das Problem zu replizieren, das Dump zu stoppen und die Sitzung sofort zu beenden.

Wenn Sie den Dump über SSH durchführen, verwenden Sie einen Filter, um nur den relevanten Datenverkehr zu erfassen. Andernfalls enthält die Erfassung die SSH-Sitzungspakete.

Eine vollständige Anleitung zur Konfiguration der Erfassung finden Sie unter [Troubleshoot COS APs](#).

Wenn Sie fertig sind, stoppen Sie die Erfassung mit dem Befehl `undebug all`. Die resultierende Datei sieht folgendermaßen aus:

```
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>
```

Bereinigung der Ausgabedatei

Entfernen Sie alle Informationen, die nicht Teil des Paket-Dump selbst sind. Löschen Sie die Zeilen, die den Dump-Befehl, eine beliebige Eingabeaufforderung mit dem Hostnamen (APname#) und alle anderen nicht verwandten Syslog-Meldungen in der Datei enthalten.

Achten Sie besonders auf den Befehl `undebug`, da dieser vor dem Paketinhalt wie oben gezeigt

gedruckt werden kann. Nach der Bereinigung sieht die resultierende Datei folgendermaßen aus:

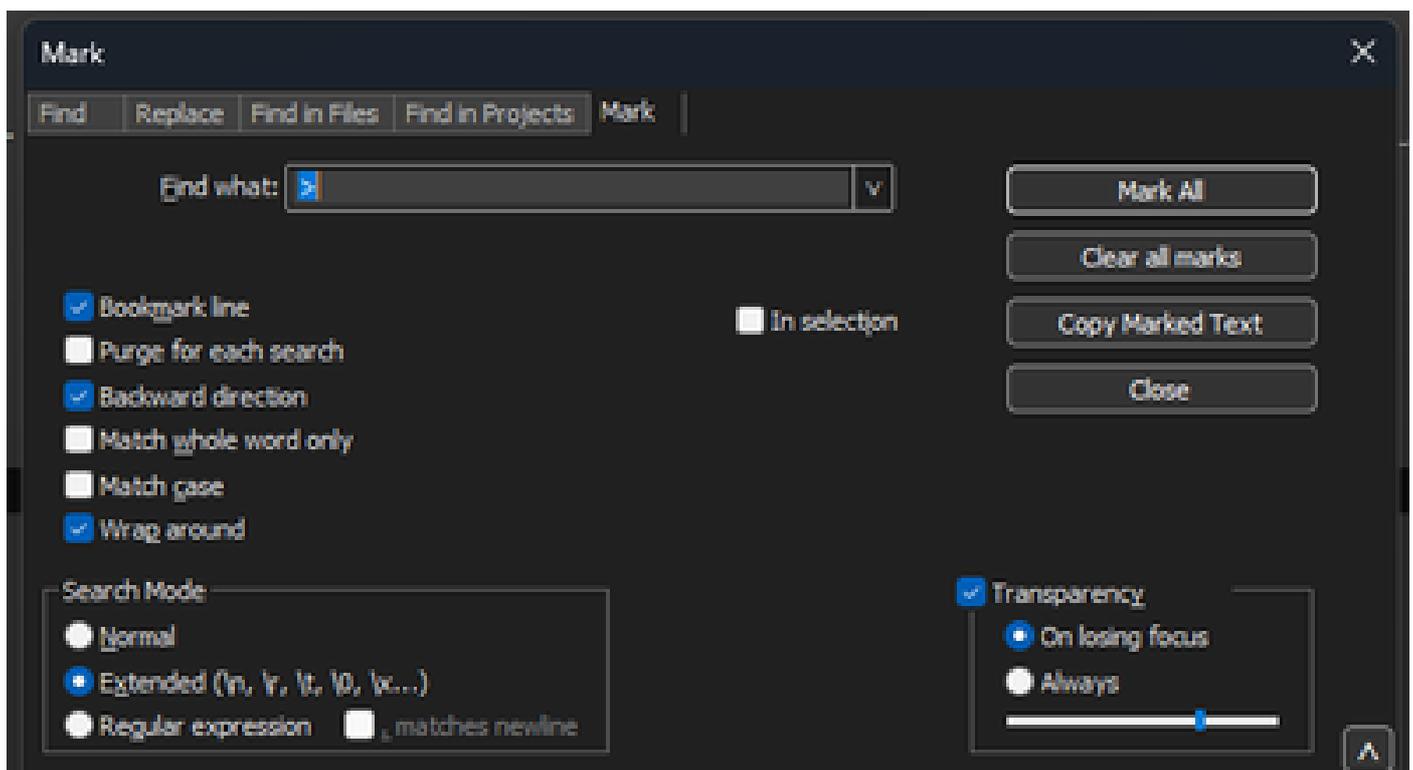
```
22:35:17.1669188 IP CSC0-W-PF320YP6.1an.60354 > 239.255.255.250.3702: UDP, length 656
0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030: 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040: 636f 6469 6e67 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
```

Zusammenfassende Informationen zum Cleanup-Paket

Der Beginn eines neuen Pakets wird erkannt, wenn ein neuer Offset 000000 angezeigt wird. Text2pcap kann die Zusammenfassung Informationen vor jedem Paket gedruckt, um Probleme zu vermeiden ist am besten, sie zu entfernen.

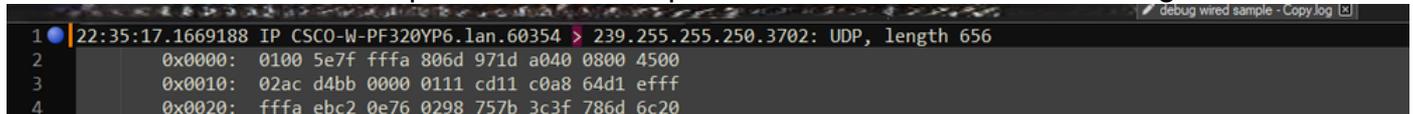
Navigieren Sie im Editor++ zu Suchen>Suchen, und wählen Sie die Registerkarte Markieren aus, um sicherzustellen, dass der Suchmodus Erweitert ist.

Geben Sie im Feld Suchen nach das Symbol ein > und klicken Sie auf Alle markieren. Mit dieser Aktion werden alle Zeilen mit dem Symbol > als Lesezeichen gespeichert.



Notepad++ kennzeichnet das Dialogfeld mit Suchen nach, in dem das Chevron-Zeichen enthalten ist.

Nach dem Markieren der Kopfzeilen hebt Notepad++ alle Dokumentzeilen wie folgt hervor:



```
1 22:35:17.1669188 IP CSCO-W-PF320YP6.1an.60354 > 239.255.255.250: 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
```

Paketausschnitt mit hervorgehobener Linie, die den Chevron enthält.

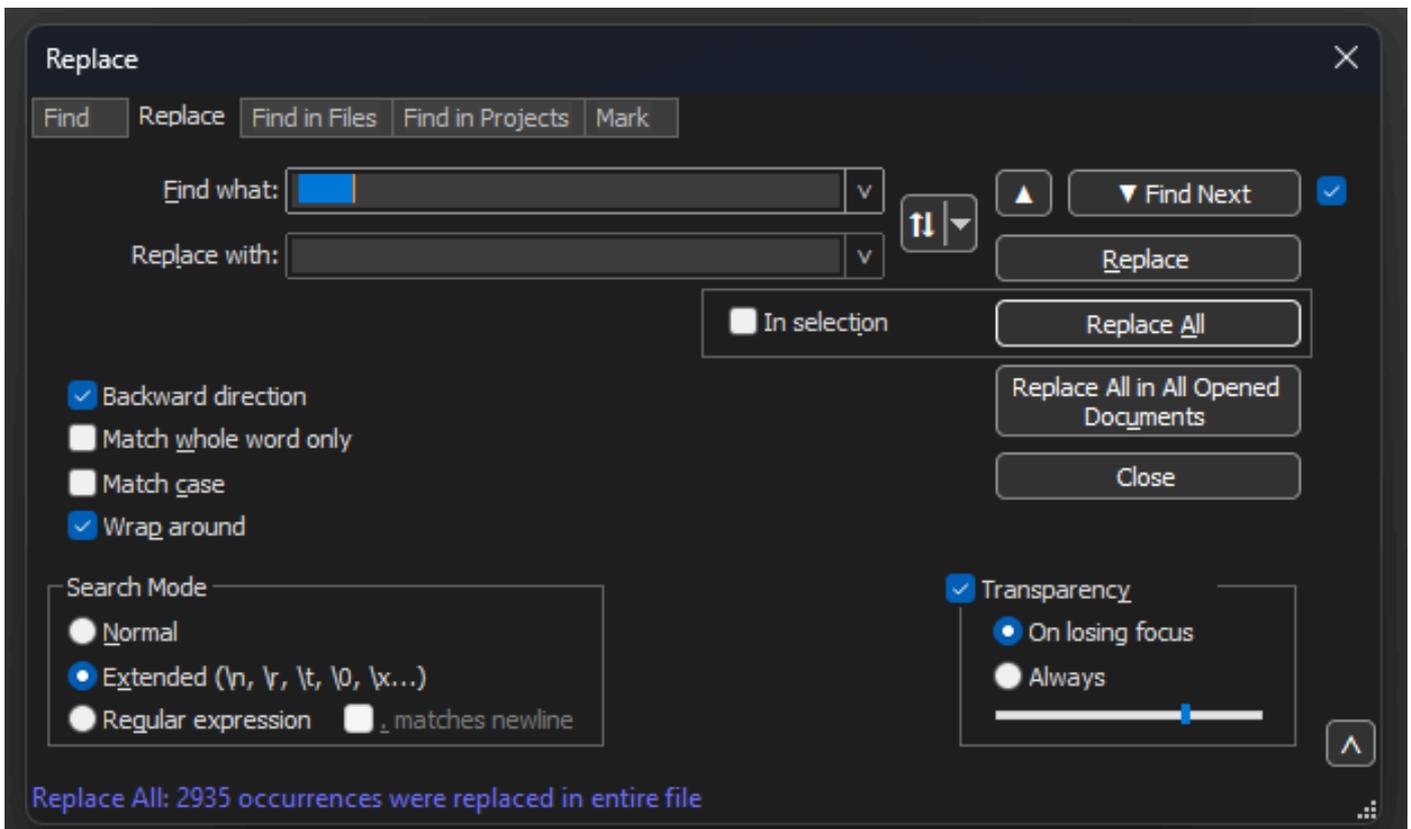
Navigieren Sie zu Suchen>Lesezeichen, und klicken Sie auf Lesezeichen entfernen. Danach sieht die Datei wie dieser Ausschnitt aus:

```
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
```

Entfernen von Anfangsräumen und Versatzkollisionen

Navigieren Sie zu Suchen>Suchen, und wählen Sie die Registerkarte Ersetzen aus, um sicherzustellen, dass der Suchmodus erweitert ist.

Geben Sie im Feld Find what (Suchen nach) 8 Leerzeichen ein. Lassen Sie das Feld Ersetzen durch: leer, und klicken Sie auf Alle ersetzen. Dadurch werden alle acht aufeinander folgenden Leerzeichen am Anfang jeder Zeile durch nichts ersetzt und im Grunde gelöscht. Das Ersetzen-Dialogfeld sieht wie dieses Bild aus.



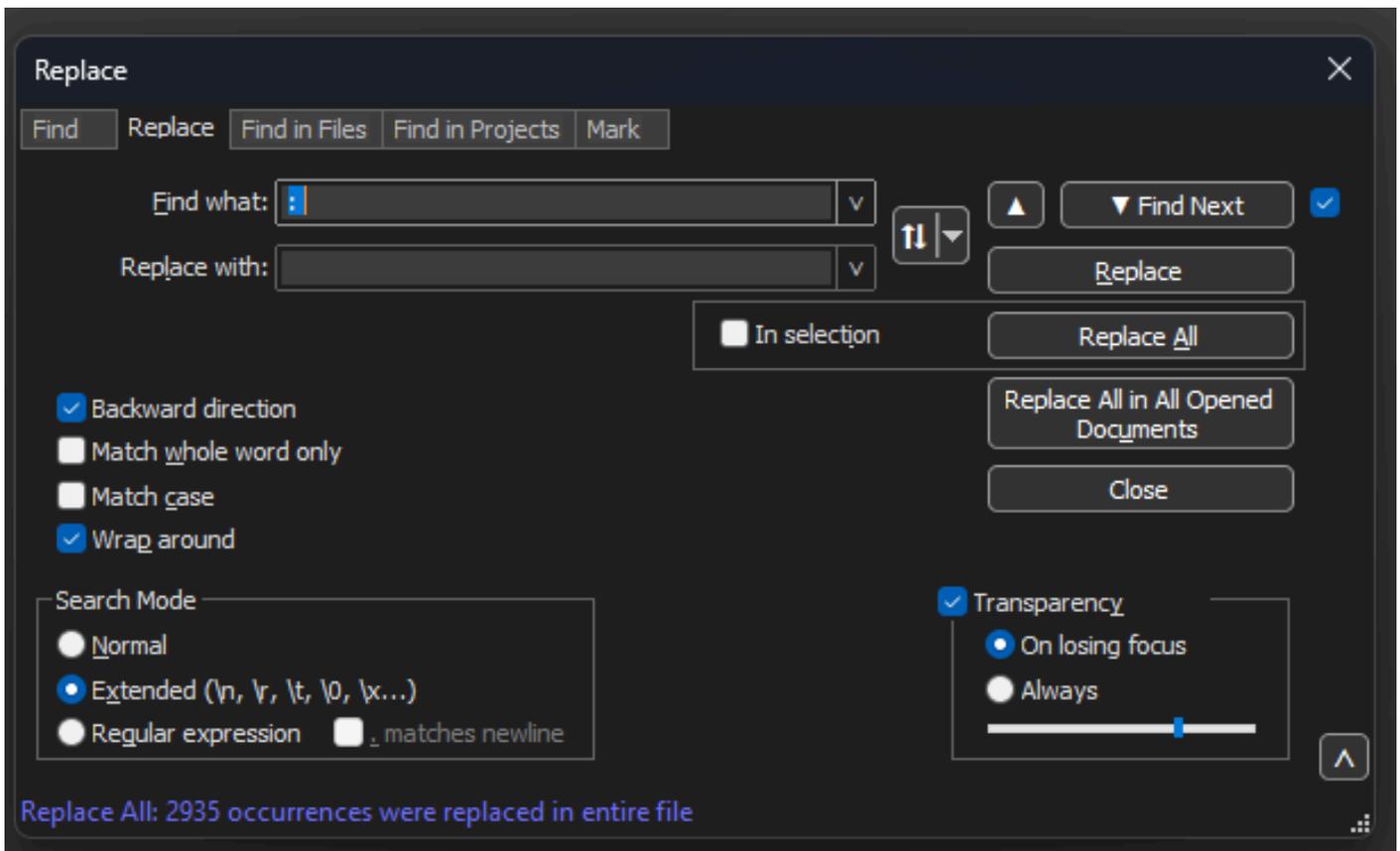
Notepad++ Dialogfeld "Ersetzen" mit "Suchen nach" durch 8 Leerzeichen ersetzen.

Die resultierende Datei nach diesem Vorgang sieht wie dieser Ausschnitt aus:

```
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
```

Navigieren Sie zu Suchen>Suchen, und wählen Sie die Registerkarte Ersetzen aus. Stellen Sie sicher, dass der Suchmodus Erweitert ist. Geben Sie : (beachten Sie die Leerzeichen hinter dem Doppelpunkt) in das Feld Suchen nach: ein. Lassen Sie das Feld Ersetzen durch: leer, und klicken Sie auf Alle ersetzen.

Ersetzt alle Doppelpunkte und ersten Leerzeichen nach dem Versatz.



Notepad++ Ersetzen Sie das Dialogfeld durch Suchen nach einem Feld, das durch einen Doppelpunkt und ein Leerzeichen gefüllt ist.

Nach dem vorherigen Vorgang sieht die Ausgabedatei wie folgt aus:

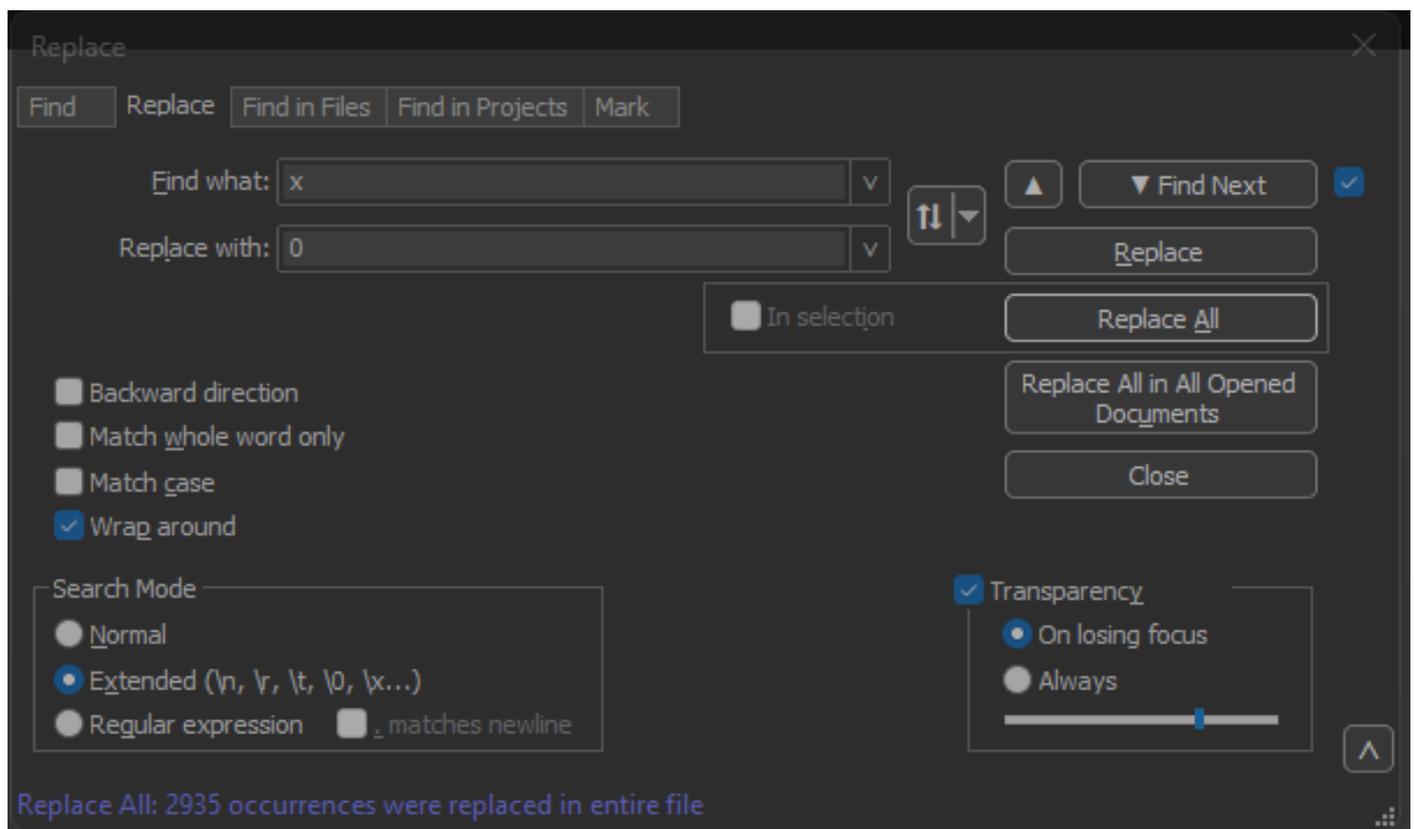
```
0x0000 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060 6d6c 6e73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

Korrektur Paket-Offset

Text2pcap erwartet einen Paket-Offset innerhalb jedes Pakets als sechsstellige Hexadezimalzeichenfolge, aber bei AP-Paket-Dumps wird 0x verwendet, um den Offset zu symbolisieren. Um dies zu korrigieren, navigieren Sie zu Suchen>Suchen, und wählen Sie die Registerkarte Ersetzen aus. Stellen Sie sicher, dass der Suchmodus Erweitert ist.

Geben Sie x in das Feld Suchen nach ein. Füllen Sie das Feld Ersetzen durch: mit 0 aus, und

klicken Sie auf Alle ersetzen. Dadurch wird das gesamte x im Offset durch 0 ersetzt, damit es dem erwarteten Offset-Format für Text2pcap entspricht.



Notepad++ Dialogfeld "Ersetzen" mit "Suchen nach", das mit dem Zeichen "x" ausgefüllt wurde, und "Ersetzen", das mit dem Zeichen "0" ausgefüllt wurde.

Nach dem vorherigen Vorgang sieht die Ausgabedatei wie folgt aus:

```
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
```

Separate Paketbytes

Das Text2pcap-Datenformat erfordert, dass jedes Paar Hex-Werte durch ein Leerzeichen getrennt wird. Bei einer falschen Formatierung werden die Paketdaten von Text2pcap als Offset gelesen, und es treten Fehler auf.

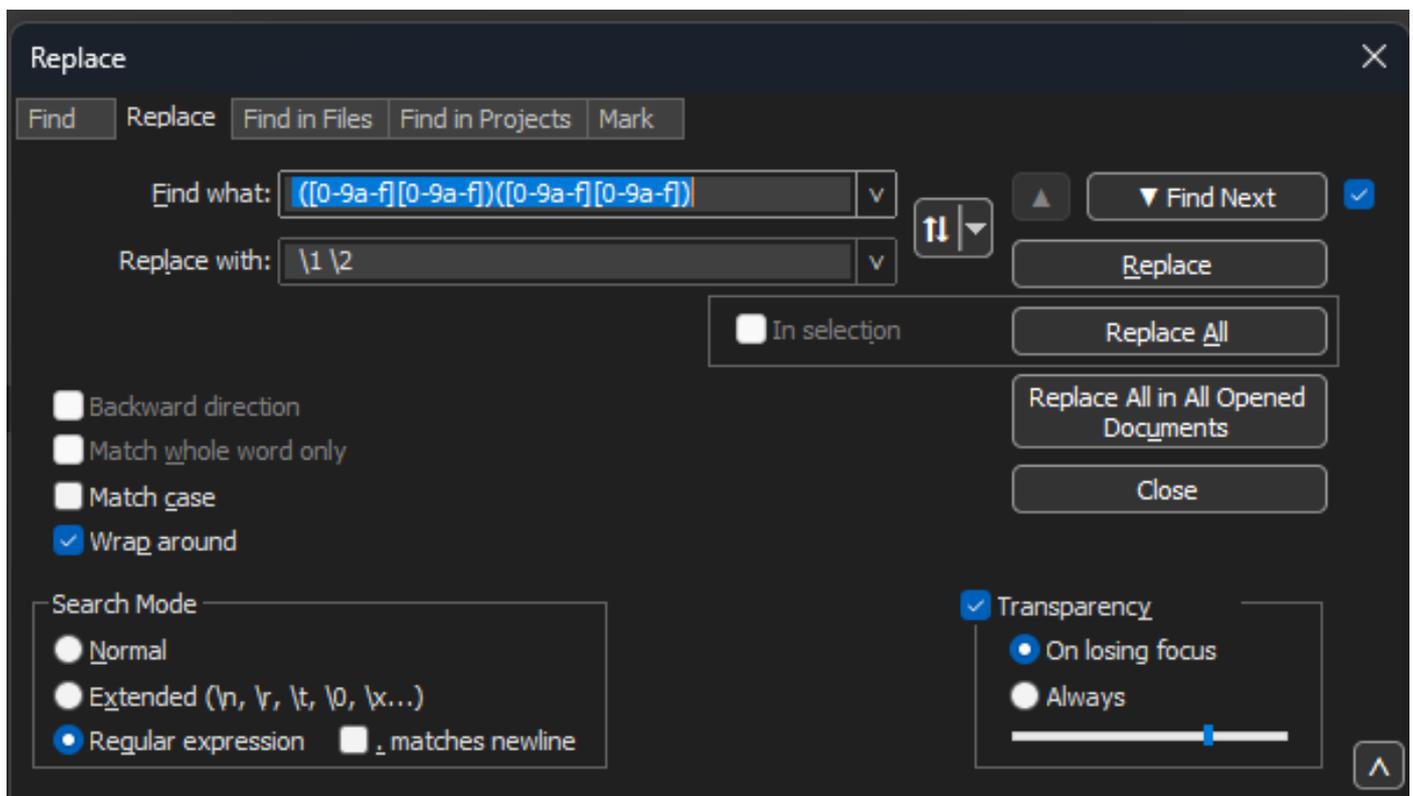
Navigieren Sie zu Suchen>Suchen, und wählen Sie die Registerkarte Ersetzen aus. Stellen Sie sicher, dass der Suchmodus der reguläre Ausdruck ist.

Geben Sie `(([0-9a-f][0-9a-f])([0-9a-f][0-9a-f])` (beachten Sie das Leerzeichen am Anfang) in das Feld Suchen nach: ein.

Füllen Sie das Feld Ersetzen durch: mit `\1 \2` aus (beachten Sie das Leerzeichen am Anfang), und klicken Sie auf Alle ersetzen.

Der Ersetzungsvorgang ermittelt die Hexadezimalbytes des Pakets und fügt zwischen jedem Paar ein Leerzeichen ein. Der reguläre Ausdruck entspricht einem Leerzeichen gefolgt von einem Hexadezimalziffern paar, speichert sie in der Erfassungsgruppe 1, nimmt dann das benachbarte Hexadezimalziffern paar und speichert sie in der Erfassungsgruppe 2. Beim Ersetzen werden sowohl die erforderlichen Leerzeichen als auch der Inhalt jeder Erfassungsgruppe gedruckt.

Je nach Länge der Datei dauert es mehrere Sekunden oder Minuten. Es nutzt viel RAM während der Ausführung. Wenn die Datei groß ist, haben Sie Geduld.



Notepad++ Ersetzen-Dialogfeld mit dem Feld Suchen nach einem regulären Ausdruck und dem Feld Ersetzen, das mit einem anderen regulären Ausdruck gefüllt ist.

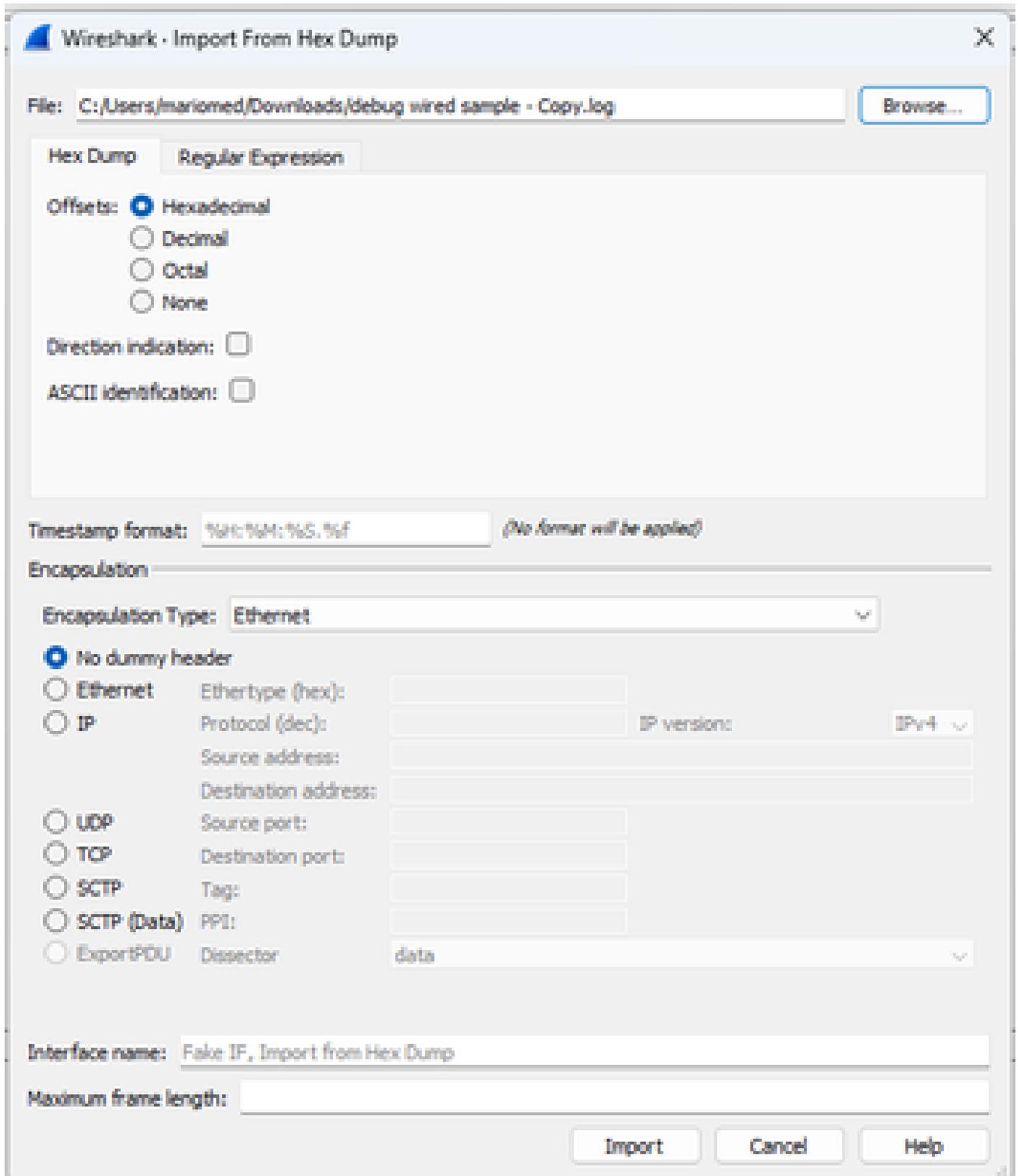
Nach dem vorherigen Vorgang sieht die Ausgabedatei wie dieser Ausschnitt aus und kann von Text2pcap konvertiert werden.

```
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
```

Konvertieren der Textdatei in PCAP

Über Wireshark-GUI

Um die vollständige Datei in pcap zu konvertieren, öffnen Sie Wireshark, und navigieren Sie zu Datei>Aus Hexadezimaldump importieren, ein Dialogfeld wird angezeigt.



Wireshark-Importdialogfeld

Klicken Sie auf die Schaltfläche **Browse...** (Durchsuchen), und wählen Sie die Dump-Textdatei aus. Stellen Sie sicher, dass der ausgewählte Offsetting hexadezimal, der Kapselungstyp Ethernet

ist und kein Dummy-Header ausgewählt ist.

Klicken Sie auf Importieren, um den Konvertierungsvorgang zu starten.

Über Kommandozeile

Um eine Textdatei in eine pcap-Datei in der Windows-Befehlszeile zu konvertieren, führen Sie <Pfad zum wireshark-Installationsordner>\text2pcap.exe <Pfad zur Textdatei pcap> <Ausgabedateipfad> aus.

Sie können optional einen Wireshark-Ordner zu Ihrem PATH hinzufügen. Andernfalls müssen Sie text2pcap ausführen, wobei Sie bei jeder Konvertierung einer Datei den gesamten Pfad zu text2pcap.exe angeben müssen. Text2pcap.exe befindet sich im Installationsordner von Wireshark.

```
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).
```

Windows-Befehlszeilenausgabe nach der erfolgreichen Paketspeicherkonvertierung

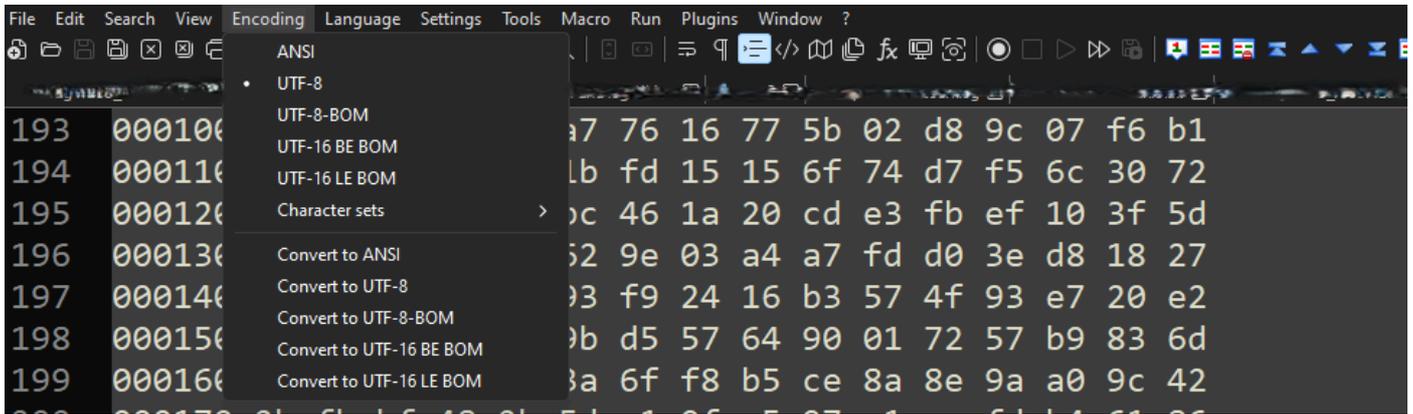
Text2pcap enthält auch mehrere reguläre Optionen, um die Textdatei vorab zu verarbeiten. Weitere Informationen finden Sie auf der [Text2pcap-Handbuchseite](#).

Fehlerbehebung

Textdatei ist korrekt, aber Text2pcap kann keine Pakete lesen

Text2pcap kann bestimmte Dateicodierungen nicht lesen, die von häufig verwendeten Terminal-Emulatoren (Secure CRT, Putty oder andere) erzeugt werden.

Wechseln Sie mit Notepad++ in eine von Text2pcap lesbare Kodierung. Gehen Sie zu Encoding>UTF-8 und speichern Sie die Datei, dann wieder in pcap konvertieren.



Menüoptionen für die Notepad++-Codierung.

Inkonsistenter Offset

Dieser Fehler tritt auf, wenn die Bytes des Datenteils eines Pakets nicht korrekt in Paare aufgeteilt sind. Dies führt dazu, dass Text2pcap den Beginn eines neuen Pakets annimmt und dieses nicht interpretiert.

Suchen Sie in der Mitte eines Paketinhalts nach Paketbytes ohne Separation oder Strings, z. B. mit dem `undebug all` Befehl.

```
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
```

Die Windows-Befehlszeilenausgabe, nachdem versucht wurde, eine ungültige Datei zu konvertieren. Inkonsistenter Offset wird mehrmals auf das Terminal gedruckt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.