Converti dump pacchetti access point per Wireshark

Sommario

Introduzione

In questo documento viene descritto come convertire un dump di pacchetti generato da COS Access Point nel formato PCAP per Wireshark per risolvere il problema della limitazione delle dimensioni.

Prerequisiti

- Notepad++ - Disponibile solo in Windows
- Text2pcap installato - incluso nelle installazioni regolari di Wireshark

Procedura

Esegui dump pacchetti

Acquisire un dump di pacchetto AP eseguendo il comando debug traffic wired <multiple options> verbose sulla riga di comando del punto di accesso. È possibile scegliere tra più filtri e interfacce.

Registrare la sessione nel terminale.
Prestare attenzione a inviare la minore quantità di pressioni di tasti durante questa operazione,

maggiore sarà il numero di caratteri stampabili nel file che non appartengono all'acquisizione stessa e maggiore sarà la pulizia da eseguire prima della conversione.
Il modo più semplice per farlo è una sessione console per il dump del pacchetto, replicare il problema, arrestare il dump e terminare immediatamente la sessione.

Se si sta eseguendo il dump tramite ssh, usare un filtro per catturare solo il traffico di interesse. In caso contrario, l'acquisizione contiene i pacchetti della sessione ssh.

Per istruzioni complete su come configurare l'acquisizione, fare riferimento alla sezione Risoluzione dei problemi dei punti di accesso COS.

Al termine, arrestare la cattura con il comando undebug all. Il file risultante sarà simile al seguente:

```
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 CSCO-W-PF32OYP6.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>
```

Pulizia file di output

Rimuovere tutte le informazioni che non fanno parte del dump del pacchetto stesso. Eliminare le righe contenenti il comando dump, qualsiasi prompt contenente il nome host (APname#) e qualsiasi altro messaggio syslog non correlato presente nel file.

Prestare particolare attenzione al comando undebug perché può essere stampato prima del contenuto di un pacchetto, come mostrato sopra. Dopo la pulizia, il file risultante sarà simile al

seguente:

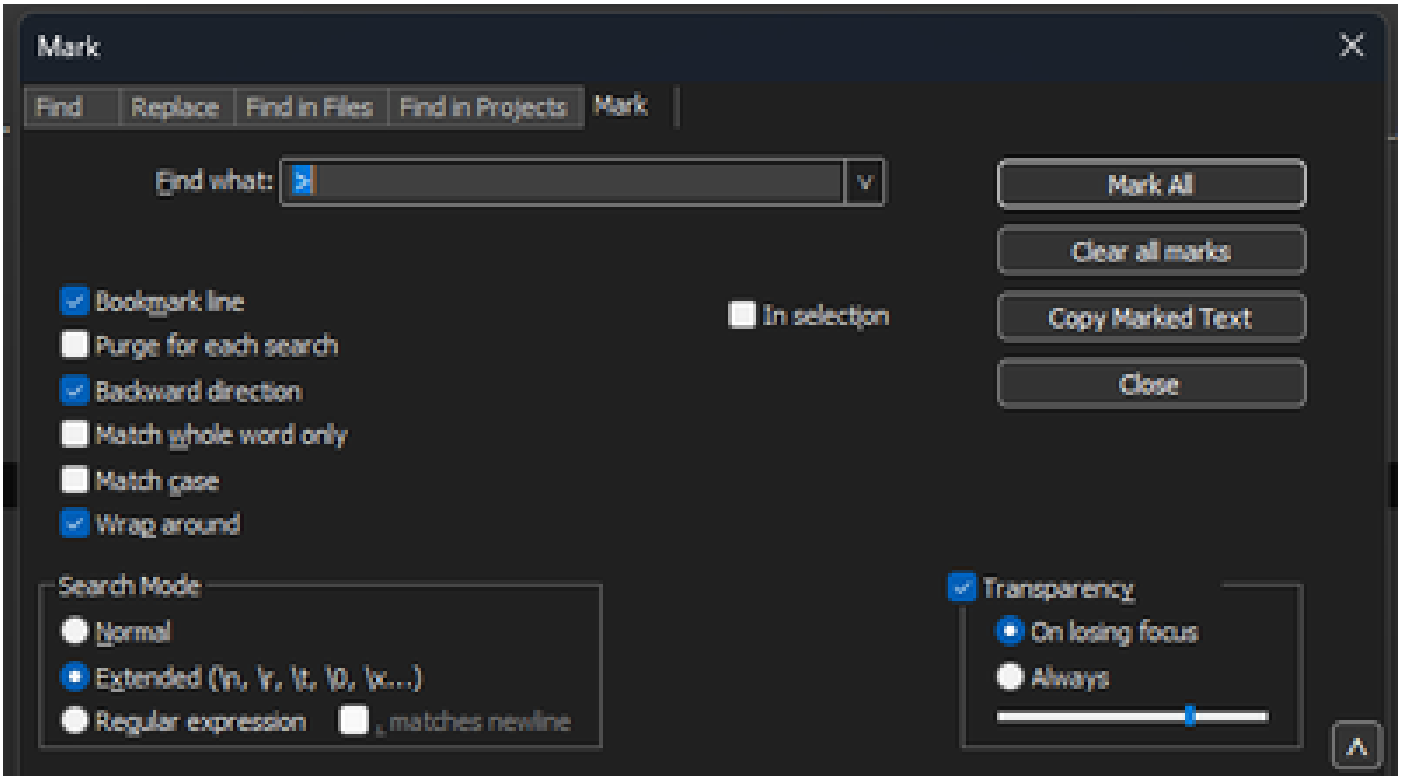
```
22:35:17.1669188 IP CSCO-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656
        0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
        0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
        0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
        0x0030:  7665 7273 696f 6e3d 2231 2e30 2220 656e
        0x0040:  636f 6469 6e67 3d22 7574 662d 3822 3f3e
<truncated>
        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
```

Informazioni di riepilogo sul pacchetto di pulizia

Quando viene visualizzato un nuovo valore di offset, viene rilevato l'inizio di un nuovo pacchetto. Text2pcap può gestire le informazioni di riepilogo stampate prima di ogni pacchetto, per evitare problemi è meglio rimuoverli.

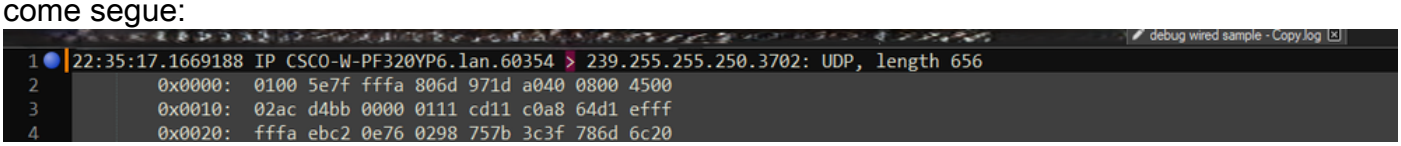
In Blocco note++ passare a Cerca>Trova e selezionare la scheda Contrassegna, assicurarsi che la modalità di ricerca sia Estesa.

Nel campo Trova: immettere il simbolo > e fare clic su Segna tutto. Questa azione consente di aggiungere un segnalibro a tutte le righe contenenti il simbolo >.



Blocco note++ con il campo Trova contenente il carattere virgolette acute.

Dopo aver contrassegnato le intestazioni, Blocco note+ evidenzia tutte le righe del documento come segue:



Frammento di dump del pacchetto con riga evidenziata contenente le virgolette acute.

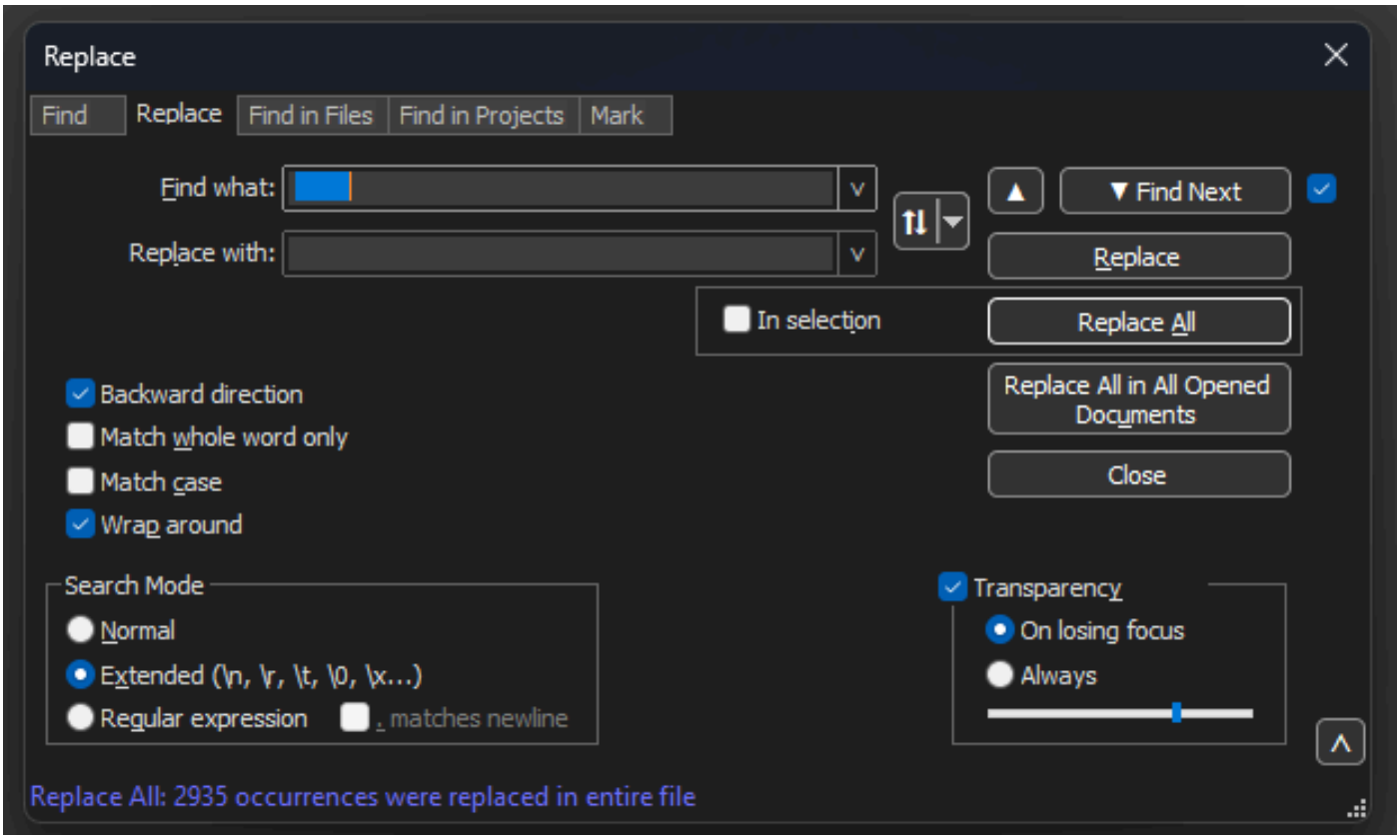
Passare a Ricerca>Segnalibro e fare clic su Rimuovi righe con segnalibro. Il file avrà quindi l'aspetto del frammento seguente:

```
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
```

Rimuovere gli spazi iniziali e i due punti di offset

Passare a Ricerca>Trova e selezionare la scheda Sostituisci, accertarsi che la modalità di ricerca sia Estesa.

Nel campo Trova: immettere 8 spazi vuoti. Lasciare vuoto il campo Sostituisci con: e fare clic su Sostituisci tutto. Questo sostituisce tutti gli 8 spazi vuoti consecutivi all'inizio di ogni riga con nulla, eliminandoli di fatto. La finestra di dialogo Sostituisci è simile a questa immagine.

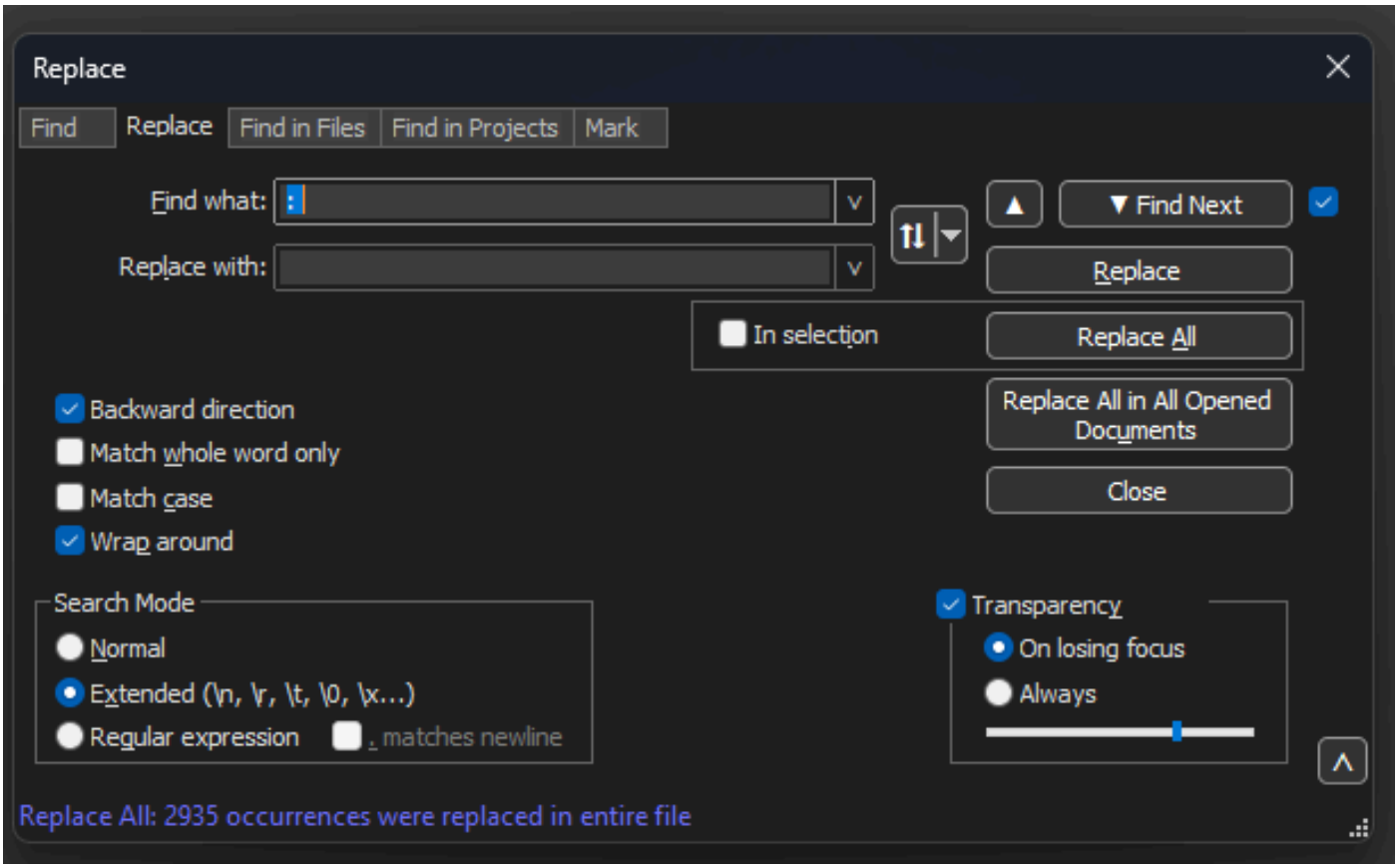


Blocco note++ Finestra di dialogo Sostituisci con il campo Trova con 8 spazi.

Il file risultante dopo questa operazione sarà simile al seguente frammento di codice:

```
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
```

Passare a Ricerca>Trova e selezionare la scheda Sostituisci, accertarsi che la modalità di ricerca sia Estesa. Immettere : (notare lo spazio vuoto dopo i due punti) nel campo Trova:. Lasciare vuoto il campo Sostituisci con: e fare clic su Sostituisci tutto.
Verranno sostituiti tutti i due punti e i primi spazi dopo l'offset.



Blocco note++ Finestra di dialogo Sostituisci con il campo Trova riempito da due punti e uno spazio.

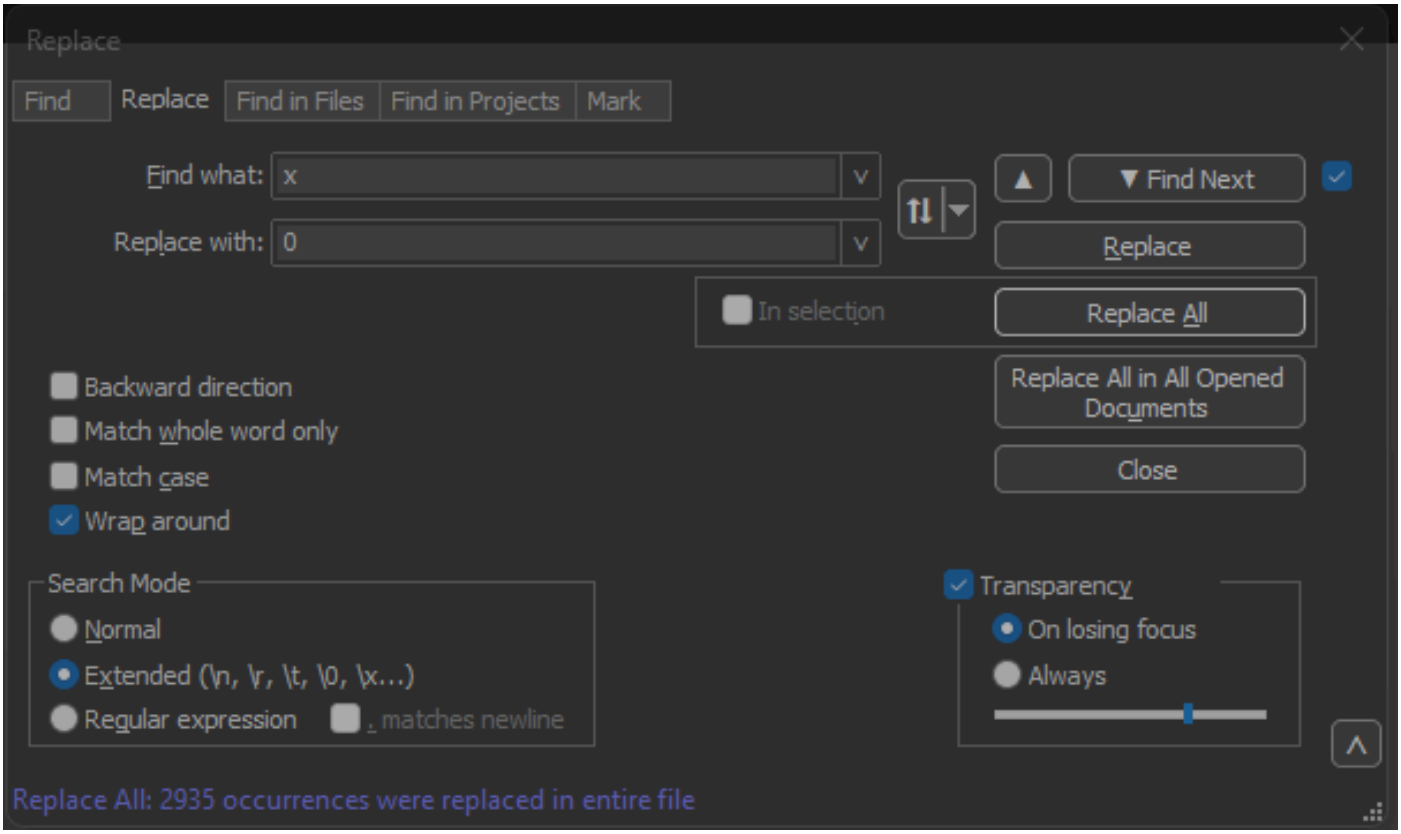
Dopo l'operazione precedente, il file di output risultante sarà simile al seguente frammento di codice:

```
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
```

Offset pacchetto corretto

Text2pcap prevede l'offset del pacchetto all'interno di ogni pacchetto come una stringa esadecimale di 6 caratteri, ma i dump di pacchetti AP utilizzano 0x per simbolizzare invece l'offset. Per correggere il problema, selezionare Cerca>Trova e selezionare la scheda Sostituisci, accertarsi che la modalità di ricerca sia Estesa.

Immettere x nel campo Trova:. Riempire il campo Sostituisci con: con 0 e fare clic su Sostituisci tutto. In questo modo, tutte le x all'interno dell'offset verranno sostituite con 0 in modo da corrispondere al formato di offset previsto per Text2pcap.



Blocco note++ Finestra di dialogo Sostituisci con il campo Trova contenente il carattere x e il campo Sostituisci contenente il carattere 0.

Dopo l'operazione precedente, il file di output risultante sarà simile al seguente frammento di codice:

```
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
```

Byte pacchetti separati

Il formato di dati Text2pcap richiede che ogni coppia di valori esadecimali sia separata da uno spazio. Se il formato non è corretto, Text2pcap legge i dati del pacchetto come offset e ha esito

negativo.

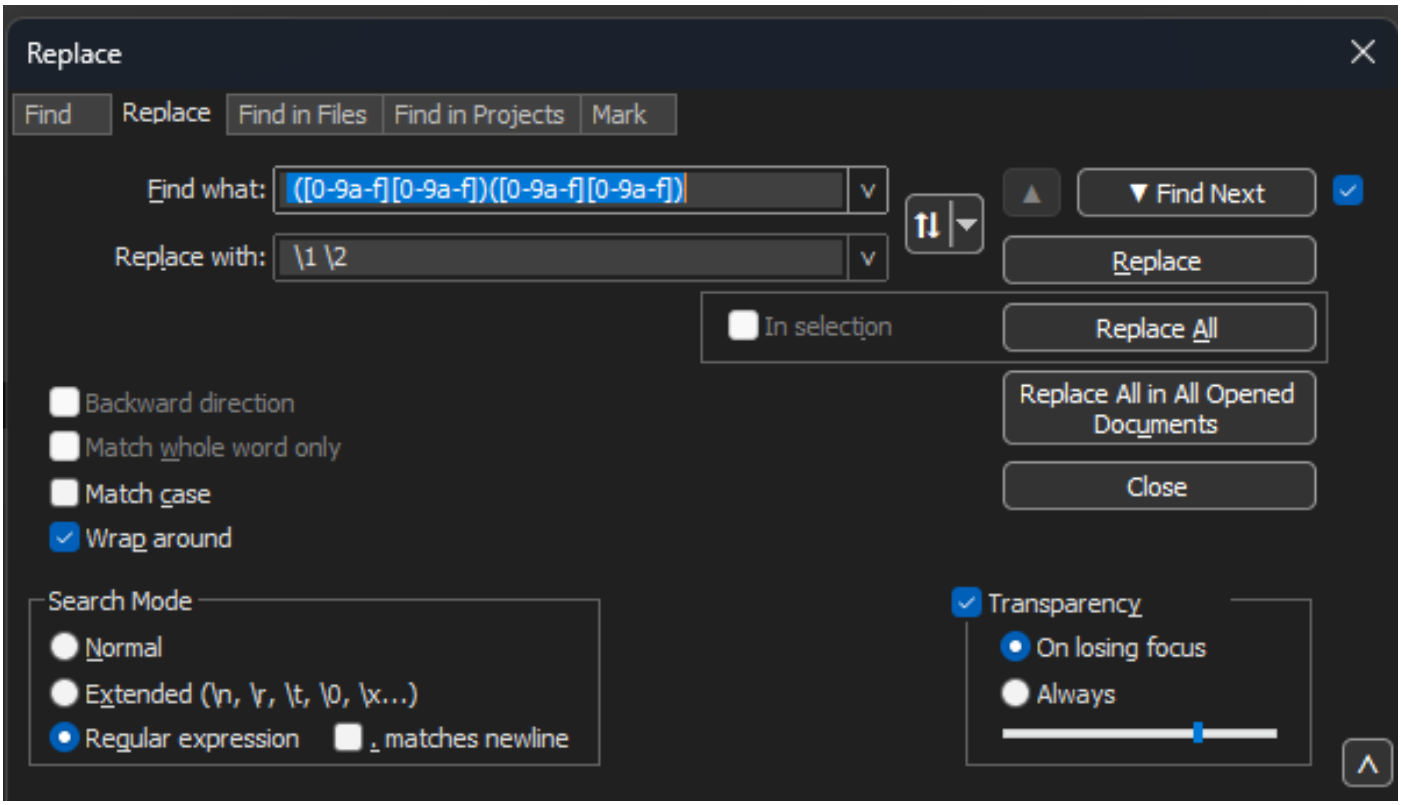
Passare a Ricerca>Trova e selezionare la scheda Sostituisci, assicurandosi che la modalità di ricerca sia Espressione regolare.

Immettere ([0-9a-f][0-9a-f])([0-9a-f][0-9a-f]) (notare lo spazio iniziale) nel campo Trova:.

Riempire il campo Sostituisci con: con \1 \2 (notare lo spazio iniziale) e fare clic su Sostituisci tutto.

L'operazione replace trova i byte esadecimali del pacchetto e inserisce uno spazio tra ogni coppia. Il regex corrisponde a uno spazio seguito da una coppia di cifre esadecimali, le salva nel gruppo di acquisizione 1, quindi prende la coppia di cifre esadecimali adiacente e le salva nel gruppo di acquisizione 2. La sostituzione stampa sia gli spazi richiesti che il contenuto di ciascun gruppo di acquisizione.

Sono necessari più secondi o minuti a seconda della lunghezza del file. Utilizza molta RAM durante l'esecuzione Se il file è di grandi dimensioni, attendere.



Blocco note++ Finestra di dialogo Sostituisci con la finestra di dialogo Trova contenente un'espressione regolare e il campo Sostituisci contenente un'altra espressione regolare.

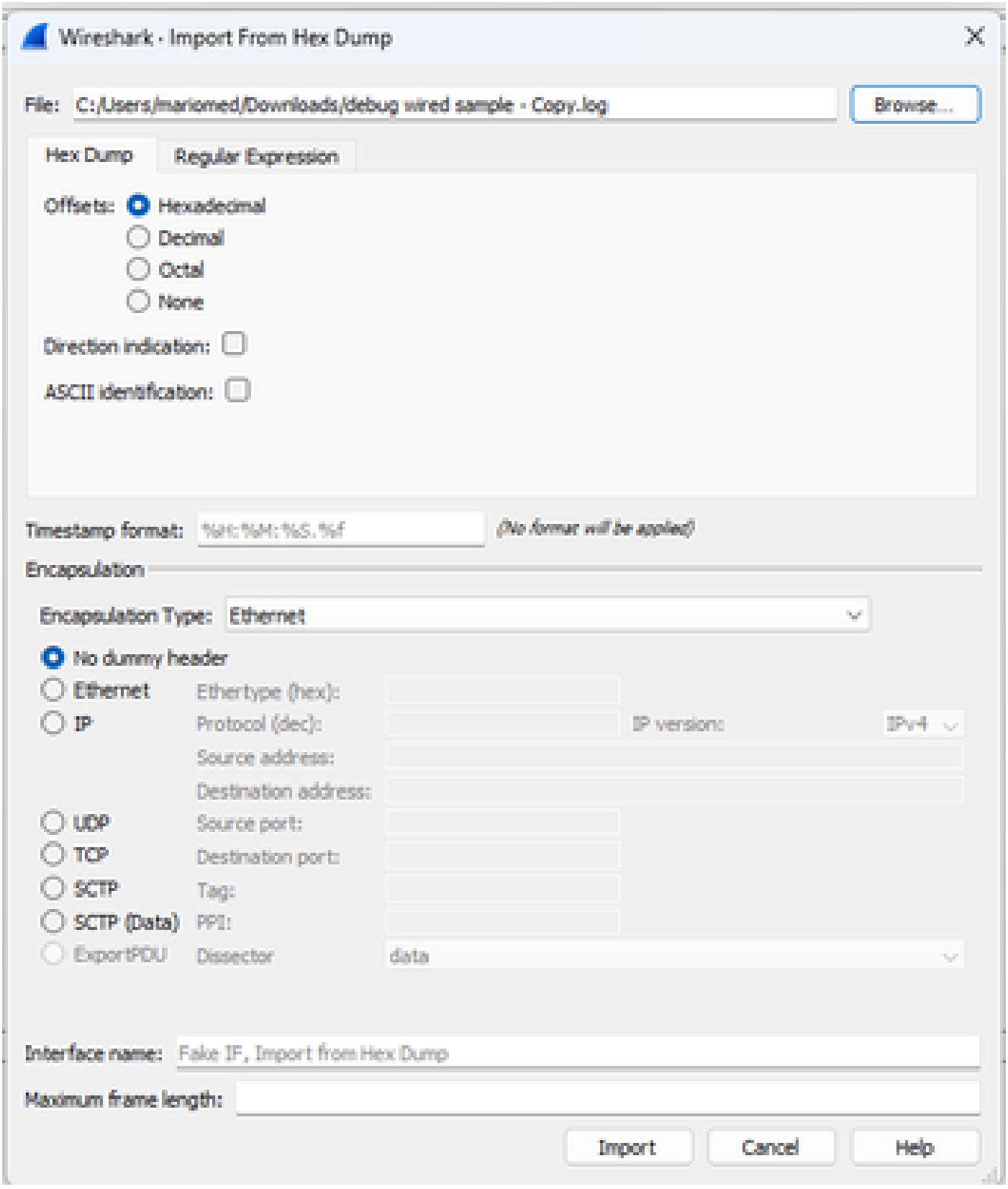
Dopo l'operazione precedente, il file di output risultante avrà l'aspetto di questo frammento ed è pronto per essere convertito da Text2pcap.

```
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
```

Converti il file di testo in PCAP

GUI Via Wireshark

Per convertire il file completo in pcap, aprire Wireshark e selezionare File>Import from hex dump, viene visualizzata una finestra di dialogo.



Finestra di dialogo Importazione wireshark

Fare clic sul pulsante Sfoglia e selezionare il file di testo di dump. Verificare che il tipo di offset selezionato sia Esadecimale, che il tipo di incapsulamento sia Ethernet e che non sia selezionata

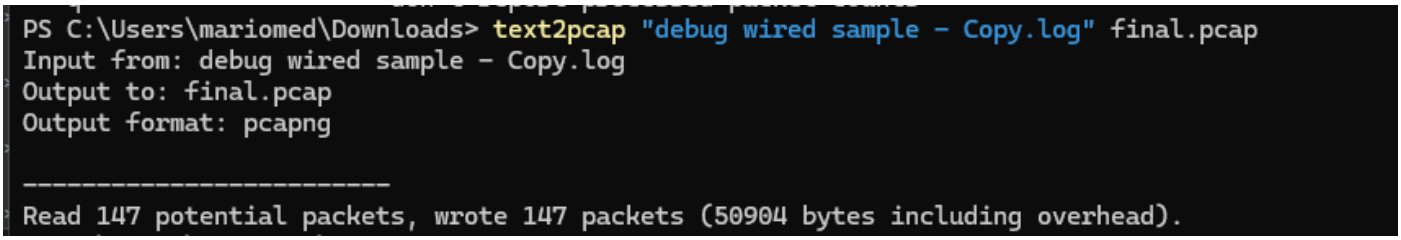
alcuna intestazione fittizia.

Fare clic su Importa per avviare il processo di conversione.

Tramite riga di comando

Per convertire un file di testo in un file pcap nella riga di comando di Windows, eseguire <percorso cartella di installazione wireshark>\text2pcap.exe <percorso file di testo pcap> <percorso file di output>.

Se lo si desidera, è possibile aggiungere la cartella wireshark al PATH. In caso contrario, è necessario eseguire text2pcap facendo riferimento all'intero percorso al file text2pcap.exe ogni volta che si converte un file. Text2pcap.exe si trova nella cartella di installazione di wireshark.



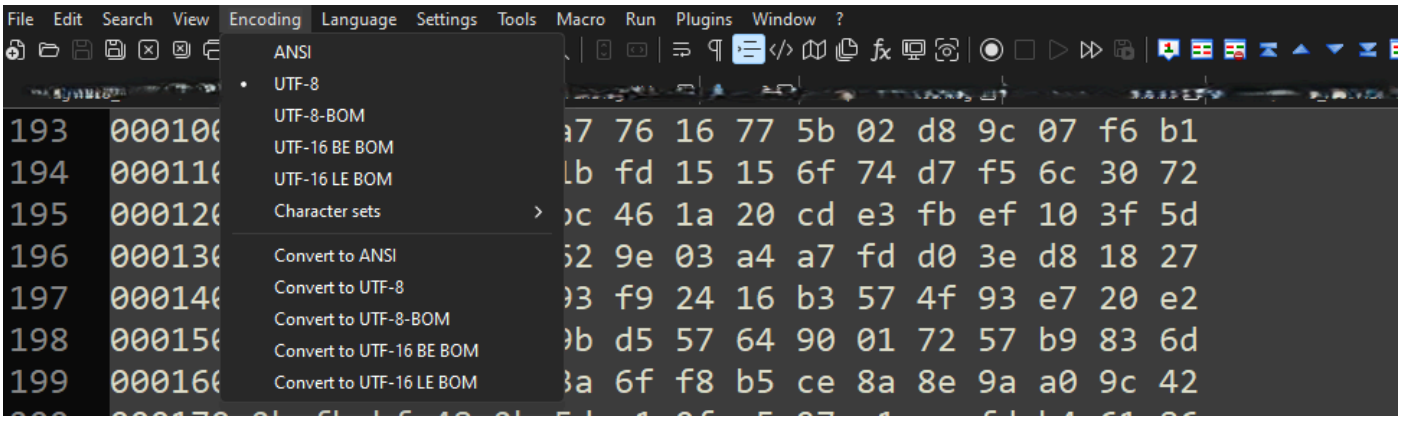
Output della riga di comando di Windows dopo la corretta conversione del dump del pacchetto

Text2pcap include anche più opzioni regex per pre-elaborare il file di testo, fare riferimento alla pagina del manuale Text2pcap per ulteriori informazioni.

Risoluzione dei problemi

Il file di testo è corretto ma Text2pcap non è in grado di leggere alcun pacchetto

Text2pcap non è in grado di leggere alcune codifiche di file prodotte dagli emulatori di terminale comunemente utilizzati (Secure CRT, Putty o altri).
Passare a una codifica leggibile da Text2pcap con Blocco note++. Andare a Encoding>UTF-8 e salvare il file, quindi convertire nuovamente in pcap.



Opzioni del menu di codifica Blocco note++.

Offset non coerente

Questo errore viene visualizzato quando i byte della parte di dati di un pacchetto non sono separati correttamente in coppie. In questo modo, Text2pcap considera l'inizio di un nuovo pacchetto e non riesce a interpretarlo.
Cercare tutti i byte dei pacchetti senza separazione o le stringhe all'interno del contenuto, ad esempio il undebug all comando.

```
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
```

Output della riga di comando di Windows dopo il tentativo di conversione di un file non valido. L'offset non coerente viene stampato sul terminale più volte.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).