Convertir volcados de paquetes de punto de acceso para Wireshark

Contenido

Introducción

Este documento describe cómo convertir un volcado de paquetes generado por el punto de acceso COS al formato PCAP para Wireshark como solución alternativa a la limitación de tamaño.

Prerequisites

- Bloc de notas++: disponible sólo en Windows
- Text2pcap instalado: incluido en las instalaciones habituales de Wireshark

Procedimiento

Realizar volcado de paquetes

Capture un volcado de paquetes AP ejecutando el comando debug traffic wired <multiple options> verbose en la línea de comandos de AP. Puede elegir entre varios filtros e interfaces.

Registre la sesión en el terminal.
Tenga cuidado de enviar la menor cantidad de pulsaciones de tecla al hacerlo, cuanto más caracteres imprimibles en el archivo que no pertenecen a la captura en sí, más limpieza que

necesita hacer antes de la conversión.
La manera más fácil de hacerlo es una sesión de consola para el volcado de paquetes, replicar el problema, detener el volcado e inmediatamente finalizar la sesión.

Si está realizando el volcado a través de ssh, utilice un filtro para capturar solamente el tráfico de interés. De lo contrario, la captura contiene los paquetes de sesión ssh.

Refiérase a Troubleshooting de los AP COS para obtener instrucciones completas sobre cómo configurar la captura.

Cuando haya terminado, detenga la captura con el comando undebug all. El archivo resultante tiene el siguiente aspecto:

```
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-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>
```

Limpieza del archivo de salida

Elimine cualquier información que no forme parte del volcado de paquetes en sí. Elimine las líneas que contienen el comando dump, cualquier indicación que contenga el nombre de host (APname#) y cualquier otro mensaje syslog no relacionado presente en el archivo.

Preste especial atención al comando undebug, ya que se puede imprimir antes del contenido de un paquete, como se muestra anteriormente. Después de la limpieza, el archivo resultante tendrá el siguiente aspecto:

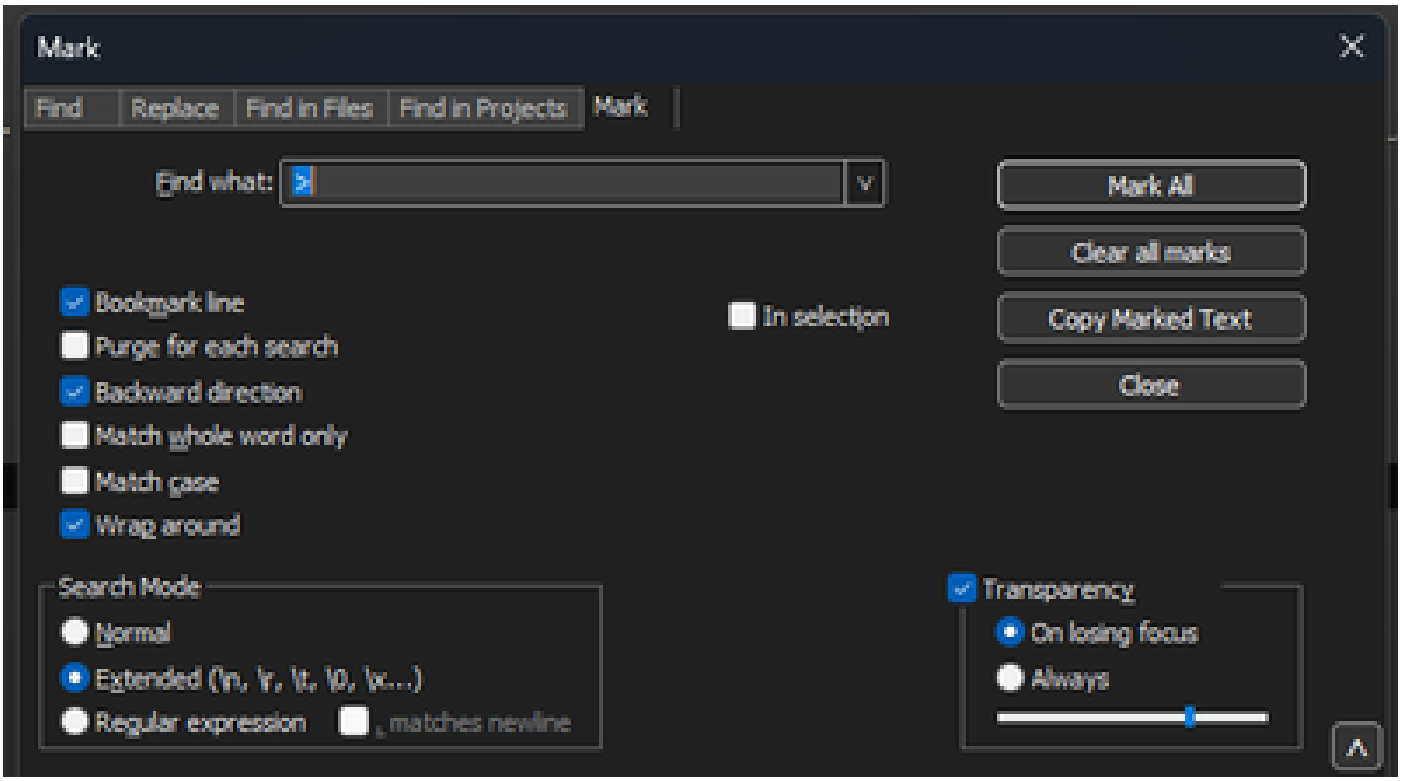
```
22:35:17.1669188 IP CSCO-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656
        0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
        0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
        0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
        0x0030:  7665 7273 696f 6e3d 2231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

Información resumida del paquete de limpieza

El inicio de un nuevo paquete se detecta cuando aparece un nuevo desplazamiento 000000. Text2pcap puede manejar la información de resumen impresa antes de cada paquete, para evitar problemas es mejor eliminarlos.

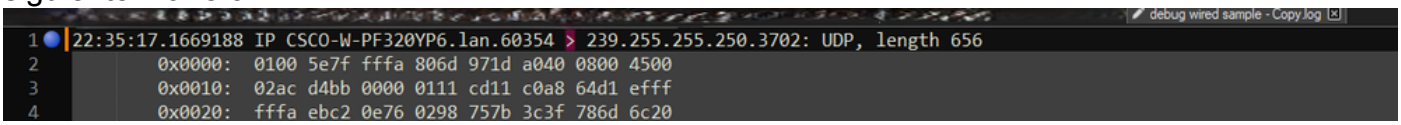
En Notepad++, navegue hasta Buscar>Buscar Y seleccione la pestaña Marcar, asegúrese de que el Modo de búsqueda esté Extendido.

En el campo Find what: ingrese el símbolo > y haga clic en Mark All. Esta acción marca todas las líneas que contienen el símbolo >.



Cuadro de diálogo Marca del Bloc de notas++ con el campo Buscar con el carácter cheurón en su interior.

Después de marcar los encabezados, Notepad++ resalta todas las líneas del documento de la siguiente manera:



Fragmento de volcado de paquetes con línea resaltada que contiene el cheurón.

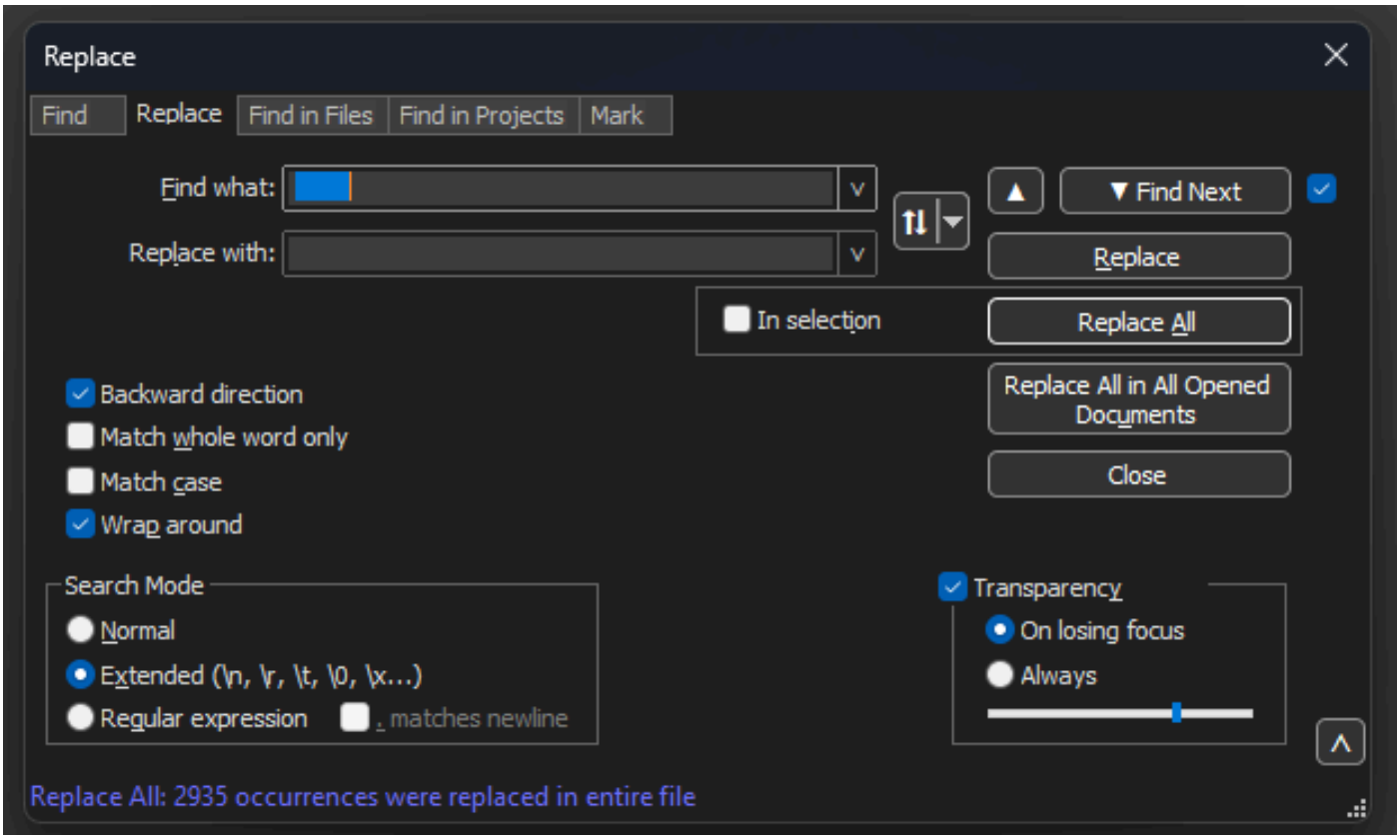
Navegue hasta Buscar>Marcador y haga clic en Eliminar líneas de marcadores. Después de hacerlo, el archivo se ve como este fragmento de código:

```
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
```

Quitar los espacios iniciales y los dos puntos de desplazamiento

Navegue hasta Buscar>Buscar Y seleccione la pestaña Reemplazar, asegúrese de que el modo de búsqueda esté extendido.

En el campo Find what: (Buscar), introduzca 8 espacios en blanco. Deje el campo Reemplazar con: vacío y haga clic en Reemplazar todos. Esto reemplaza los 8 espacios en blanco consecutivos al principio de cada línea con nada, eliminándolos de manera efectiva. El cuadro de diálogo de reemplazo se parece a esta imagen.

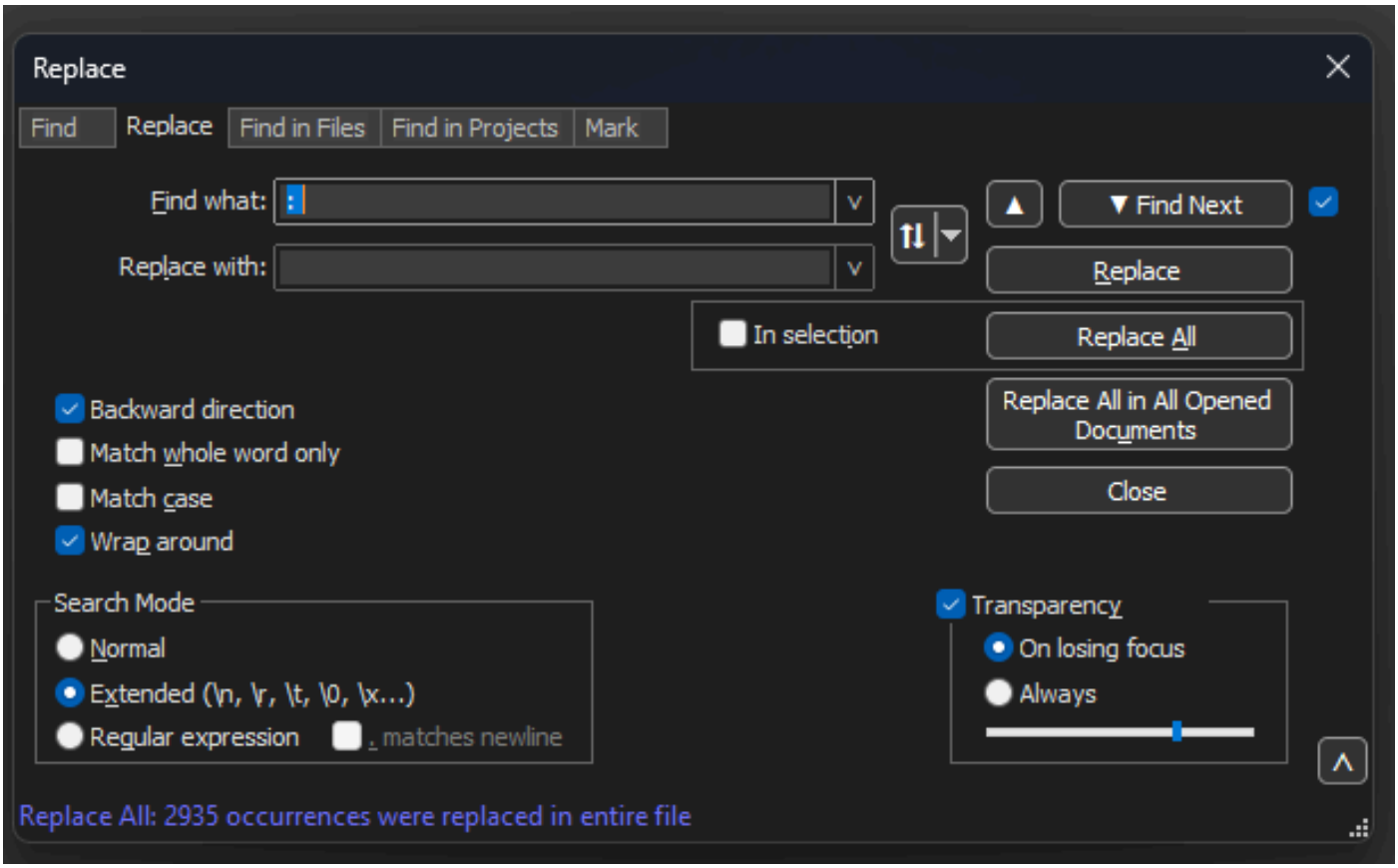


Cuadro de diálogo Reemplazar de Notepad++ con el campo Buscar con 8 espacios.

El archivo resultante después de esta operación se parece a este fragmento de código:

```
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
```

Navegue hasta Buscar>Buscar Y seleccione la pestaña Reemplazar, asegúrese de que el modo de búsqueda esté extendido. Escriba : (observe el espacio en blanco después de los dos puntos) en el campo Buscar:. Deje el campo Reemplazar con: vacío y haga clic en Reemplazar todos. Reemplaza todos los dos puntos y los primeros espacios después del desplazamiento.



Bloc de notas++ Reemplazar por Buscar el campo rellenado por dos puntos y un espacio.

Después de la operación anterior, el archivo de salida resultante tiene el siguiente aspecto:

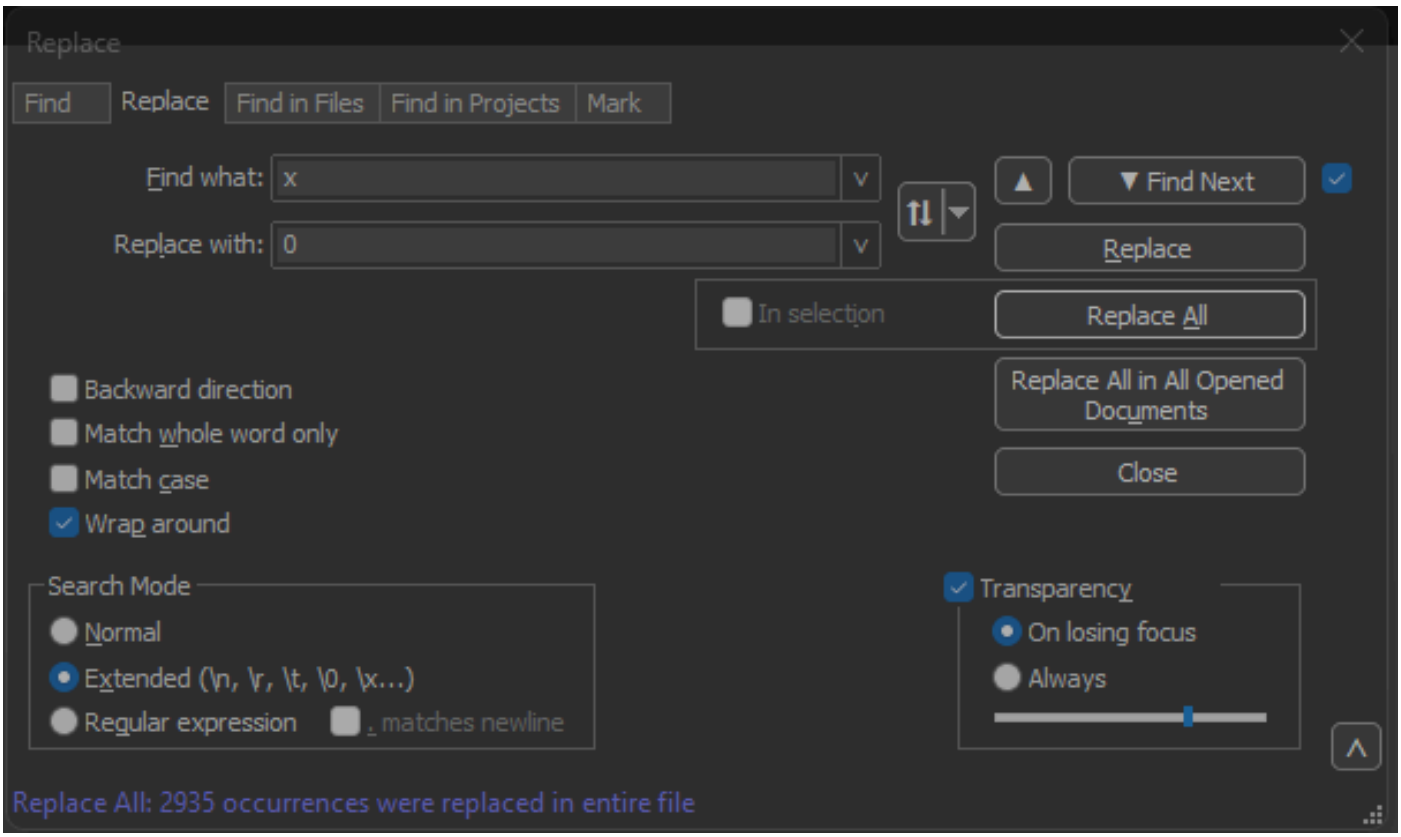
```
0x0000 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060 6d6c 6e73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

Desplazamiento de paquete correcto

Text2pcap espera que el desplazamiento del paquete dentro de cada paquete sea una cadena hexadecimal de 6 caracteres, pero los volcados de paquetes de AP utilizan 0x para simbolizar el desplazamiento en su lugar. Para corregirlo, navegue hasta Buscar>Buscar Y seleccione la pestaña Reemplazar, asegúrese de que el modo de búsqueda esté extendido.

Ingrese x en el campo Find what:. Rellene el campo Reemplazar con: con 0 y haga clic en

Reemplazar todos. Esto reemplaza todas las x dentro del desplazamiento por 0 para que coincidan con el formato de desplazamiento esperado para Text2pcap.



Bloc de notas++ Reemplazar cuadro de diálogo con Buscar el campo rellenado con el carácter x y Reemplazar campo relleno con el carácter 0.

Después de la operación anterior, el archivo de salida resultante tiene el siguiente aspecto:

```
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
```

Bytes de paquete separados

El formato de datos Text2pcap requiere que cada par de valores hexadecimales esté separado por un espacio; un formato incorrecto hace que Text2pcap lea los datos del paquete como un desplazamiento y falle.

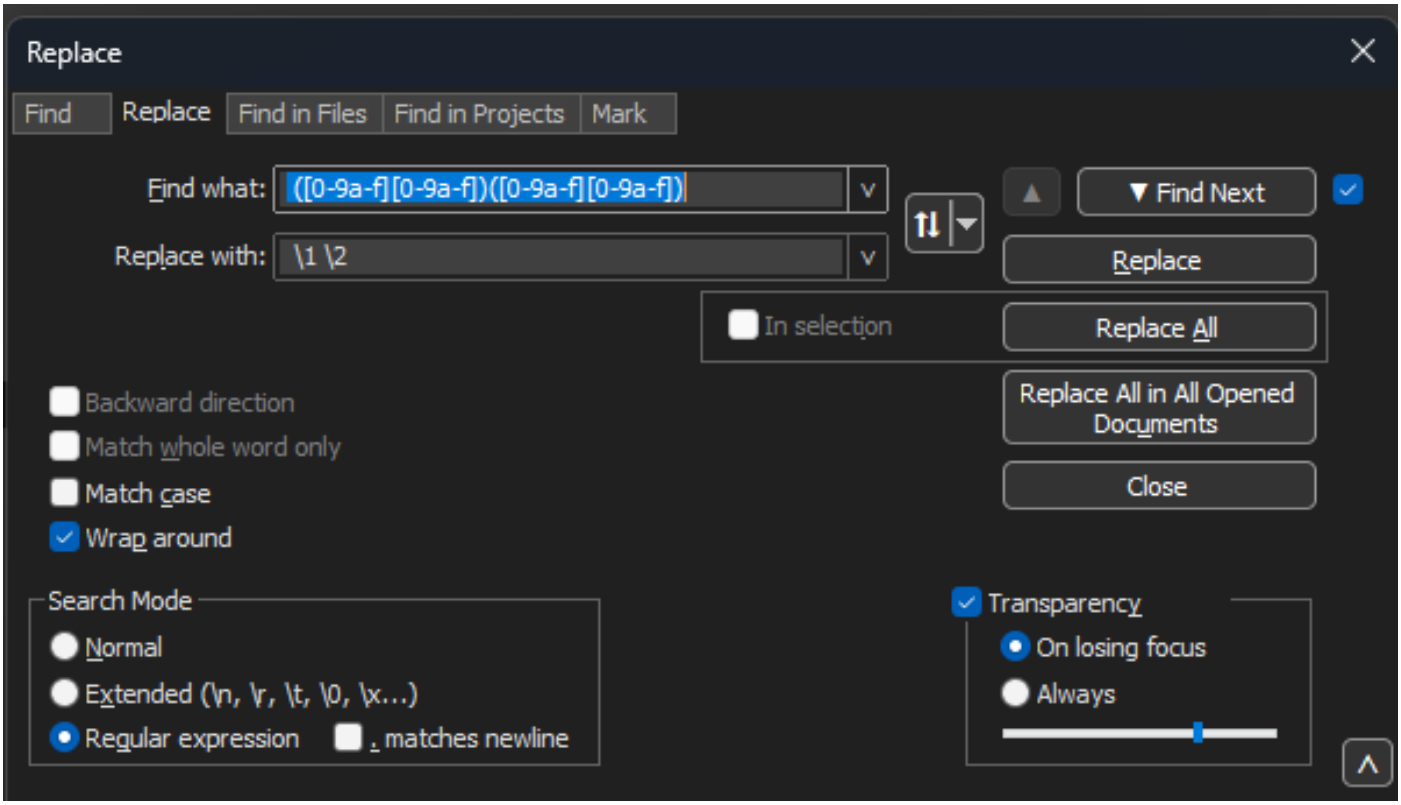
Navegue hasta Buscar>Buscar y seleccione la pestaña Reemplazar, asegúrese de que el modo de búsqueda sea expresión regular.

Escriba ([0-9a-f][0-9a-f])([0-9a-f][0-9a-f]) (observe el espacio inicial) en el campo Buscar:.

Rellene el campo Reemplazar con: con \1 \2 (observe el espacio inicial) y haga clic en Reemplazar todo.

La operación de reemplazo encuentra los bytes hexadecimales del paquete e inserta un espacio entre cada par. El regex coincide con un espacio seguido de un par de dígitos hexadecimales, los guarda en el grupo de captura 1, luego toma el par adyacente de dígitos hexadecimales y los guarda en el grupo de captura 2. La sustitución imprime los espacios necesarios, así como el contenido de cada grupo de captura.

Tarda varios segundos o minutos dependiendo de la duración del archivo. Utiliza una gran cantidad de RAM mientras se ejecuta Si el archivo es grande, tenga paciencia.



Bloc de notas++ Reemplazar (cuadro de diálogo) por buscar lo que se ha rellenado con una expresión regular y el campo Reemplazar (Replace) rellenado con otra expresión regular.

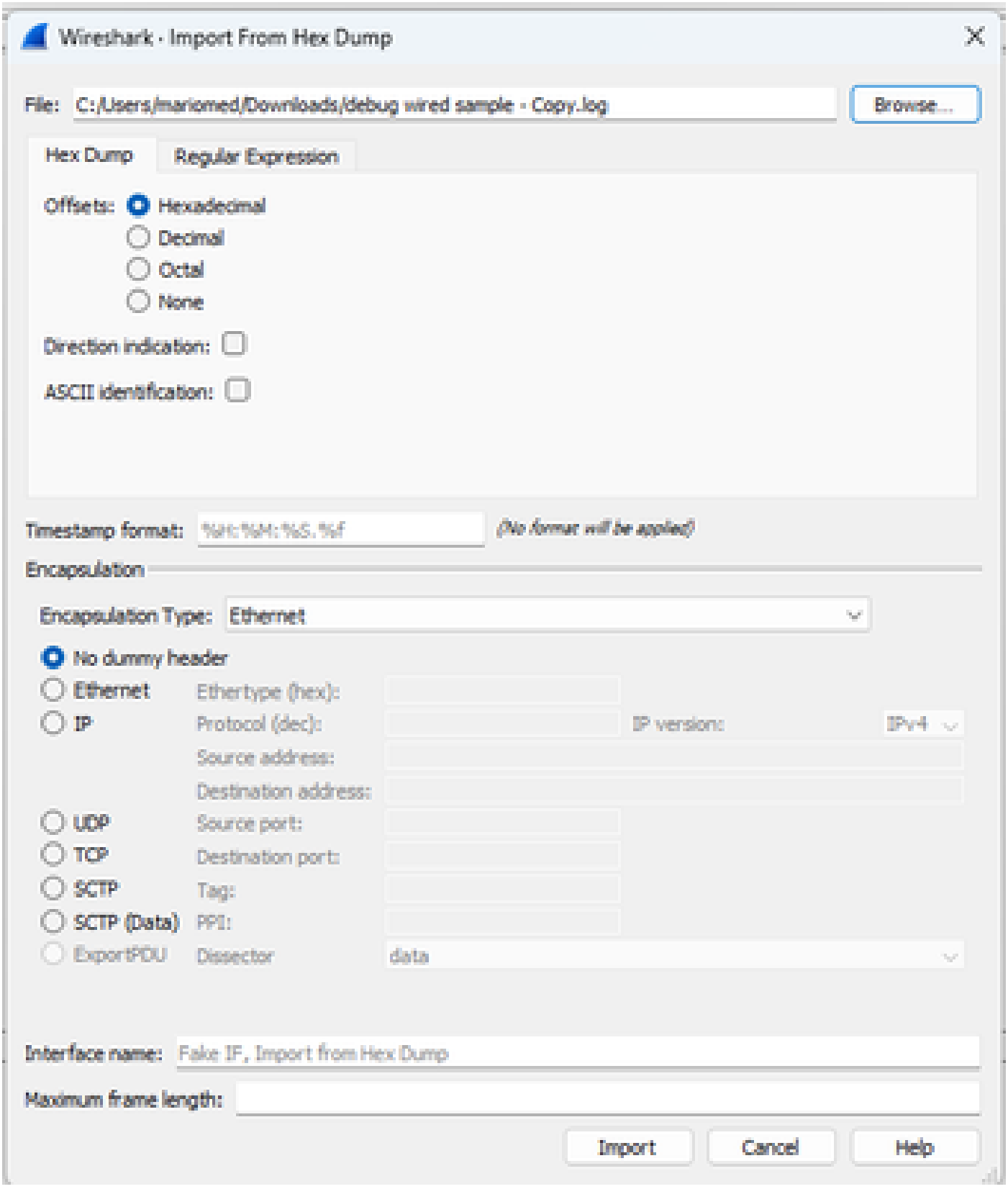
Después de la operación anterior, el archivo de salida resultante se parece a este fragmento de código y está listo para ser convertido por Text2pcap.

```
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
```

Convertir el archivo de texto a PCAP

A través de Wireshark GUI

Para convertir el archivo completo a pcap, abra Wireshark y navegue hasta Archivo>Importar desde volcado hexadecimal, aparecerá un cuadro de diálogo.



Cuadro de diálogo Importar Wireshark

Haga clic en el botón Browse... y seleccione el archivo de texto de volcado. Asegúrese de que el tipo de desplazamiento seleccionado es Hexadecimal, el tipo de encapsulación es Ethernet y se

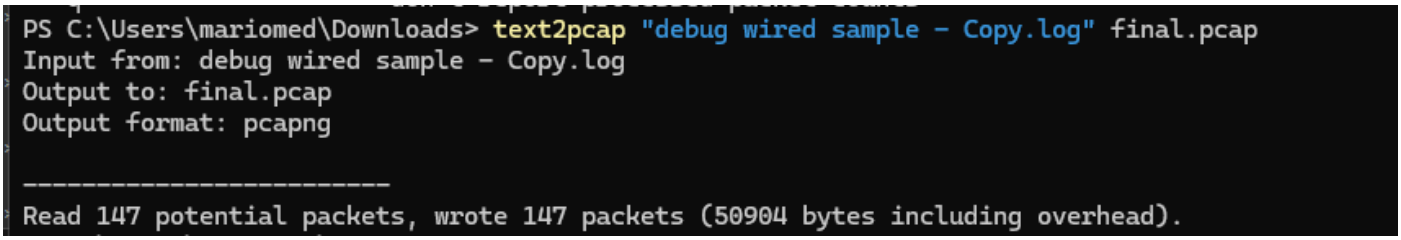
ha seleccionado Ningún encabezado ficticio.

Haga clic en Importar para iniciar el proceso de conversión.

Vía la línea de comandos

Para convertir un archivo de texto en un archivo pcap en la línea de comandos de Windows, ejecute <path to wireshark install folder>\text2pcap.exe <path to text file pcap> <output file path>.

Opcionalmente, puede agregar la carpeta wireshark a su PATH; de lo contrario, tendrá que ejecutar text2pcap haciendo referencia a la ruta completa de text2pcap.exe cada vez que convierta un archivo. Text2pcap.exe se encuentra dentro de la carpeta de instalación de wireshark.



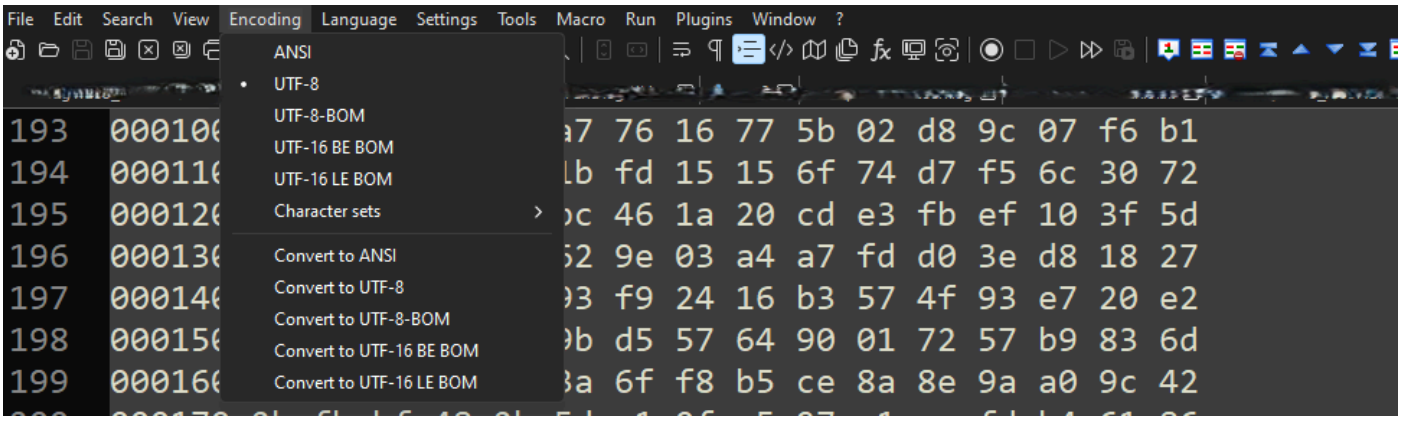
Resultado de la línea de comandos de Windows después de la conversión correcta del volcado de paquetes

Text2pcap también incluye varias opciones de regex para preprocesar el archivo de texto, consulte la página de manual de Text2pcap para obtener más información.

Resolución de problemas

El archivo de texto es correcto pero Text2pcap no puede leer ningún paquete

Text2pcap no puede leer ciertas codificaciones de archivo producidas por emuladores de terminal de uso común (Secure CRT, Putty u otros).
Cambie a una codificación legible por Text2pcap con Notepad++. Vaya a Encoding>UTF-8 y guarde el archivo, luego convierta nuevamente a pcap.



Opciones de menú de codificación del Bloc de notas++.

Desplazamiento incoherente

Este error aparece cuando los bytes de la porción de datos en un paquete no se separan correctamente en pares, esto hace que Text2pcap asuma el inicio de un nuevo paquete y no pueda interpretarlo.
Busque cualquier byte de paquete sin separación o cadenas en medio de un contenido de paquete como el undebug all comando.

Resultado de la línea de comandos de Windows después de intentar convertir un archivo no válido. El desplazamiento incoherente se imprime en el terminal varias veces.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).