Converter Despejos de Pacote de Ponto de Acesso para o Wireshark

Contents

Introdução

Este documento descreve como converter um dump de pacote gerado pelo Ponto de Acesso COS para o formato PCAP para o Wireshark como uma solução alternativa para a limitação de tamanho.

Pré-requisitos

- Notepad++ - Disponível apenas no Windows
- Text2pcap instalado - incluído nas instalações regulares do Wireshark

Procedimento

Executar despejo de pacote

Capture um dump de pacote AP executando o comando debug traffic wired <multiple options> verbose na linha de comando do AP. Você pode escolher entre vários filtros e interfaces.

Registre a sessão no terminal.
Tenha cuidado para enviar a menor quantidade de teclas digitadas ao fazer isso, quanto mais

caracteres imprimíveis no arquivo que não pertencem à captura em si, mais limpeza você precisa fazer antes da conversão.
A maneira mais fácil de fazer isso é uma sessão de console para o dump de pacote, replicar o problema, parar o dump e imediatamente terminar a sessão.

Se você estiver executando o dump via ssh, use um filtro para capturar apenas o tráfego de interesse. Caso contrário, a captura contém os pacotes de sessão ssh.

Consulte Troubleshooting de COS APs para obter instruções completas sobre como configurar a captura.

Quando terminar, interrompa a captura com o comando undebug all. O arquivo resultante terá esta aparência:

```
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>
```

Limpeza do Arquivo de Saída

Remova todas as informações que não façam parte do próprio dump do pacote. Exclua as linhas que contêm o comando dump, qualquer prompt que contenha o nome do host (APname#) e qualquer outra mensagem de syslog não relacionada presente no arquivo.

Preste atenção especial ao comando undebug, pois ele pode ser impresso antes do conteúdo de um pacote, como mostrado acima. Após a limpeza, o arquivo resultante terá a seguinte

aparência:

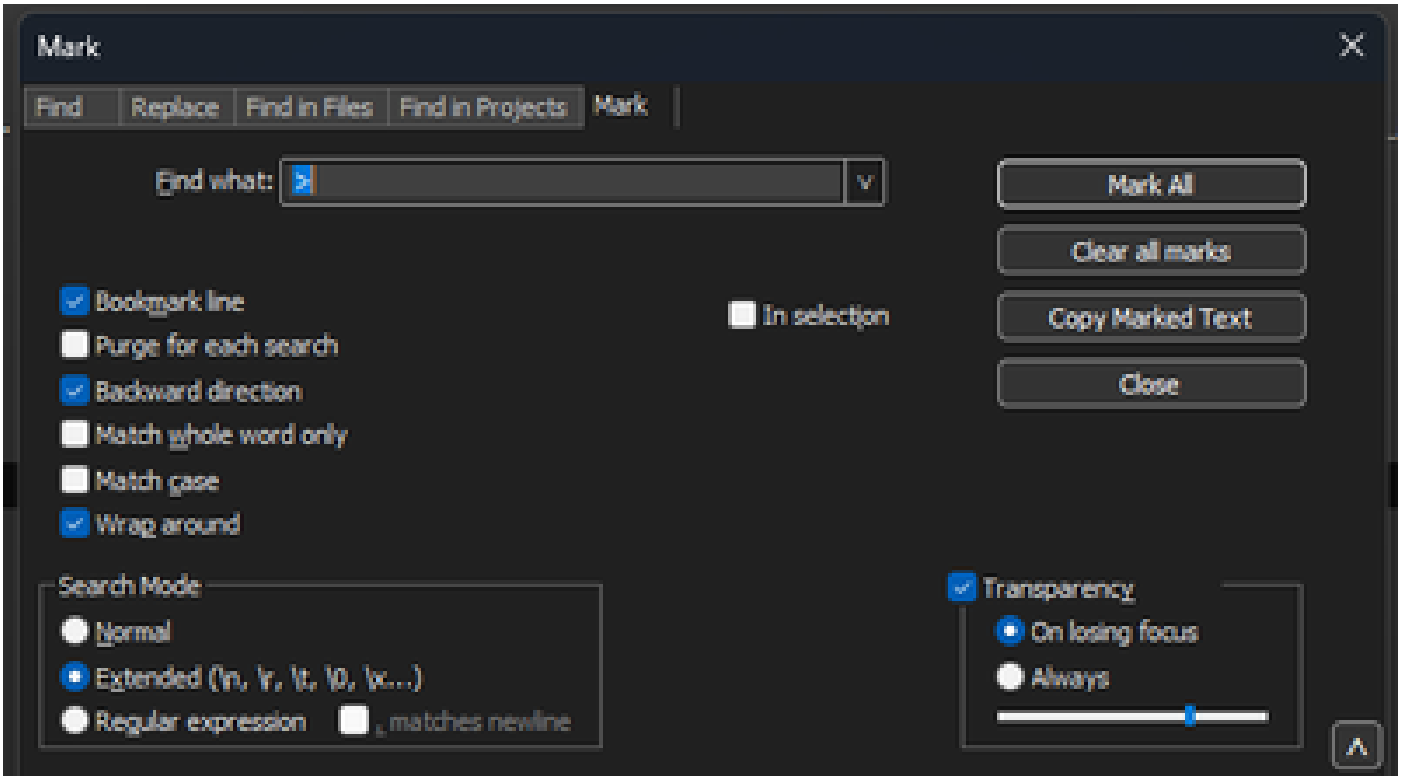
```
22:35:17.1669188 IP CSCO-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656
        0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
        0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
        0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
        0x0030:  7665 7273 696f 6e3d 2231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

Informações de resumo do pacote de limpeza

O início de um novo pacote é detectado quando um novo 000000 de deslocamento é exibido. Text2pcap pode lidar com as informações de resumo impressas antes de cada pacote, para evitar problemas é melhor removê-los.

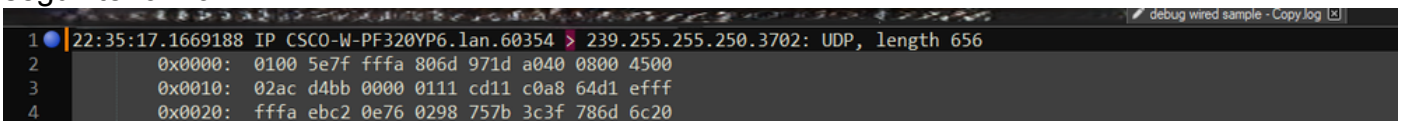
No Bloco de Notas++ navegue para Pesquisar>Localizar E selecione a guia Marcar, certifique-se de que o Modo de Pesquisa seja Estendido.

No campo Localizar:, insira o símbolo > e clique em Marcar tudo. Essa ação marca todas as linhas que contêm o símbolo >.



O Bloco de Notas++ marca a caixa de diálogo com o campo Localizar com o caractere de divisa dentro.

Depois de marcar os cabeçalhos, o Bloco de Notas++ realça todas as linhas do documento da seguinte forma:



Trecho de despejo de pacote com linha realçada que contém a divisa.

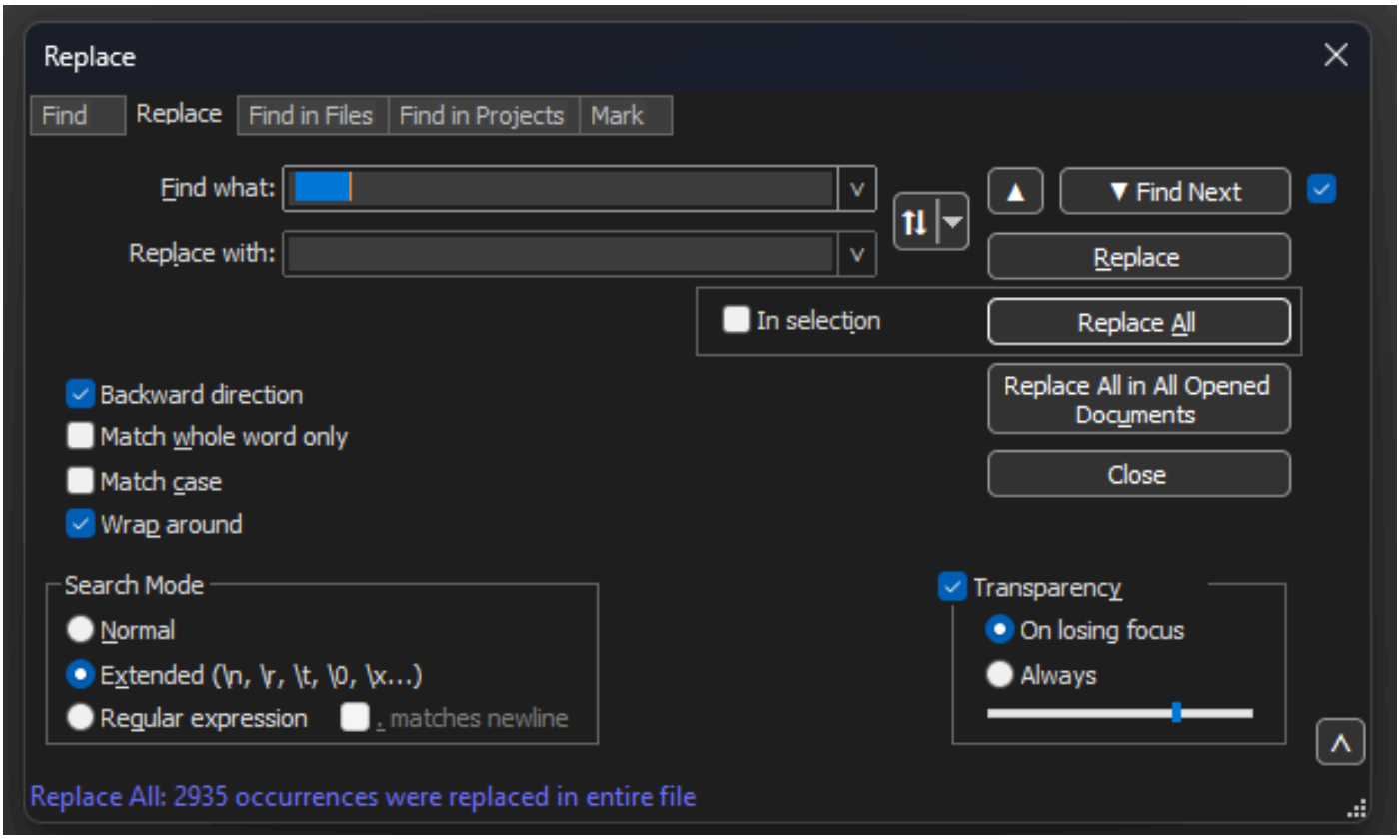
Navegue até Search>Bookmark e clique em Remove bookmarked lines. Depois de fazer isso, o arquivo se parecerá com este snippet:

```
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
```

Remover espaços iniciais e dois pontos de deslocamento

Navegue para Pesquisar>Localizar E selecione a guia Substituir, verifique se o Modo de pesquisa é Estendido.

No campo Localizar:, insira 8 espaços em branco. Deixe o campo Replace with: vazio e clique em Replace all. Isso substitui todos os 8 espaços em branco consecutivos no início de cada linha por nada, excluindo-os efetivamente. A caixa de diálogo de substituição se parece com esta imagem.

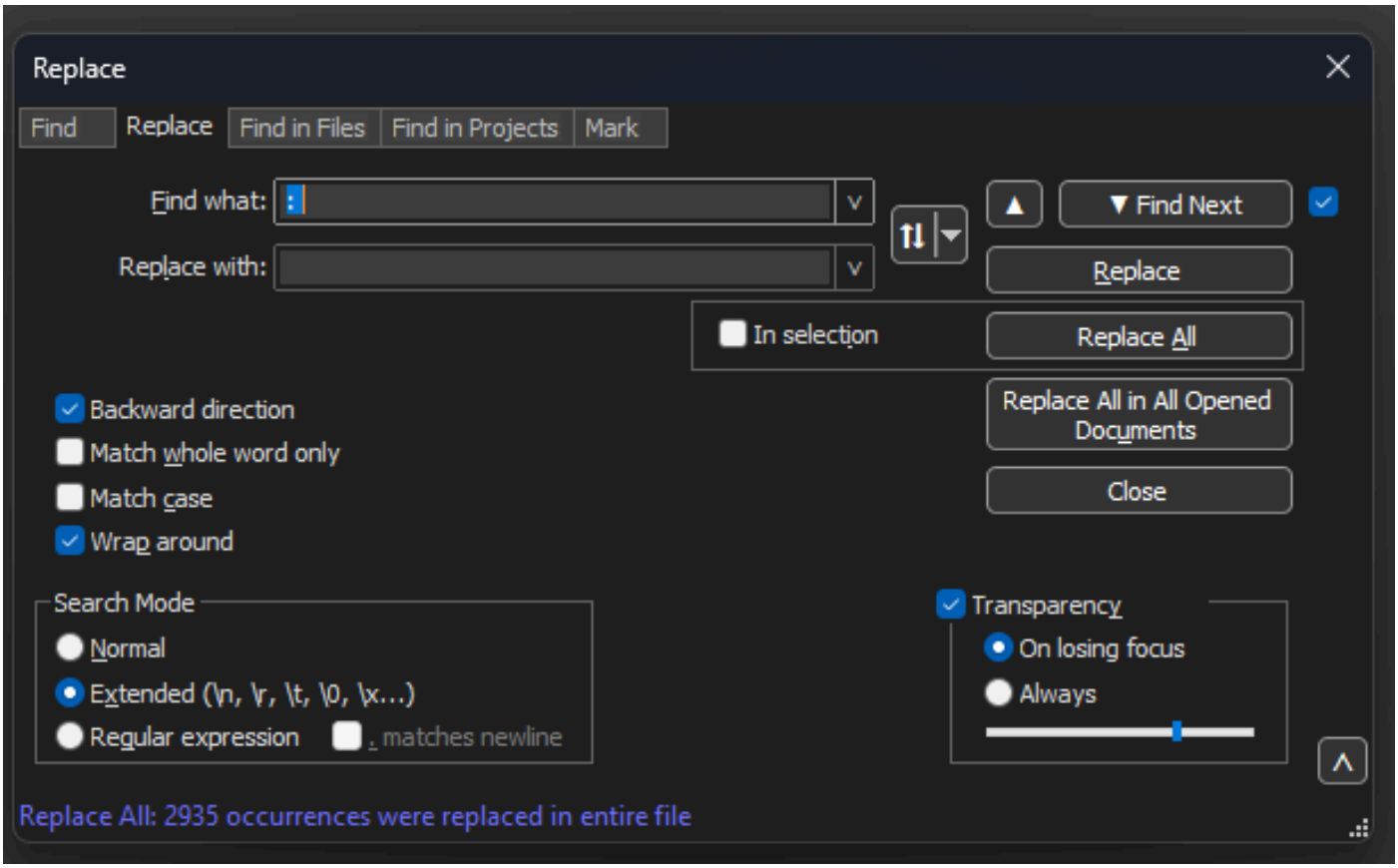


Bloco de notas++ caixa de diálogo Substituir com o campo Localizar com 8 espaços.

O arquivo resultante após esta operação se parece com este snippet:

```
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 para Pesquisar>Localizar E selecione a guia Substituir, verifique se o Modo de pesquisa está estendido. Digite : (observe o espaço em branco após os dois-pontos) no campo Localizar o que:. Deixe o campo Replace with: vazio e clique em Replace all.
Substitui todos os dois pontos e os primeiros espaços após o deslocamento.



Bloco de Notas++ caixa de diálogo Substituir com o campo Localizar preenchido por dois-pontos e um espaço.

Após a operação anterior, o arquivo de saída resultante se parece com este snippet:

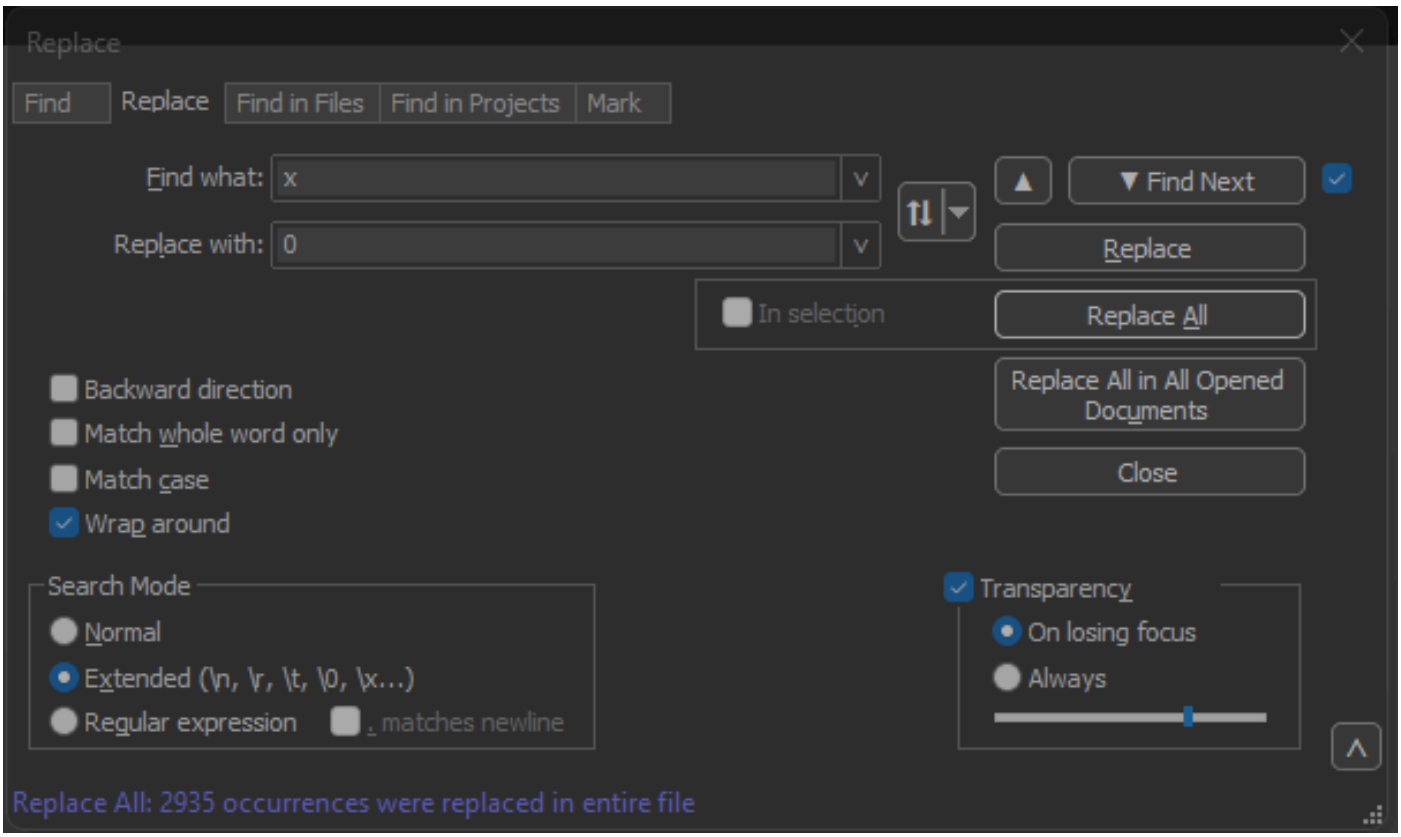
```
0x0000 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060 6d6c 6e73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

Deslocamento de pacote correto

Text2pcap espera o deslocamento de pacote dentro de cada pacote como uma string hexadecimal de 6 caracteres, mas os dumps de pacote AP usam 0x para simbolizar o deslocamento. Para corrigi-lo, navegue até Pesquisar>Localizar E selecione a guia Substituir, verifique se o Modo de pesquisa é Estendido.

Digite x no campo Localizar o que:. Preencha o campo Substituir por: com 0 e clique em Substituir

tudo. Isso substitui todo o x dentro do deslocamento por 0 para corresponder ao formato de deslocamento esperado para Text2pcap.



Bloco de Notas++ caixa de diálogo Substituir com o campo Localizar preenchido com o caractere x e campo Substituir preenchido com o caractere 0.

Após a operação anterior, o arquivo de saída resultante se parece com este snippet:

```
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 pacotes separados

O formato de dados Text2pcap requer que cada par de valores hexadecimais seja separado por um espaço; um formato incorreto faz com que Text2pcap leia dados de pacotes como um deslocamento e falhe.

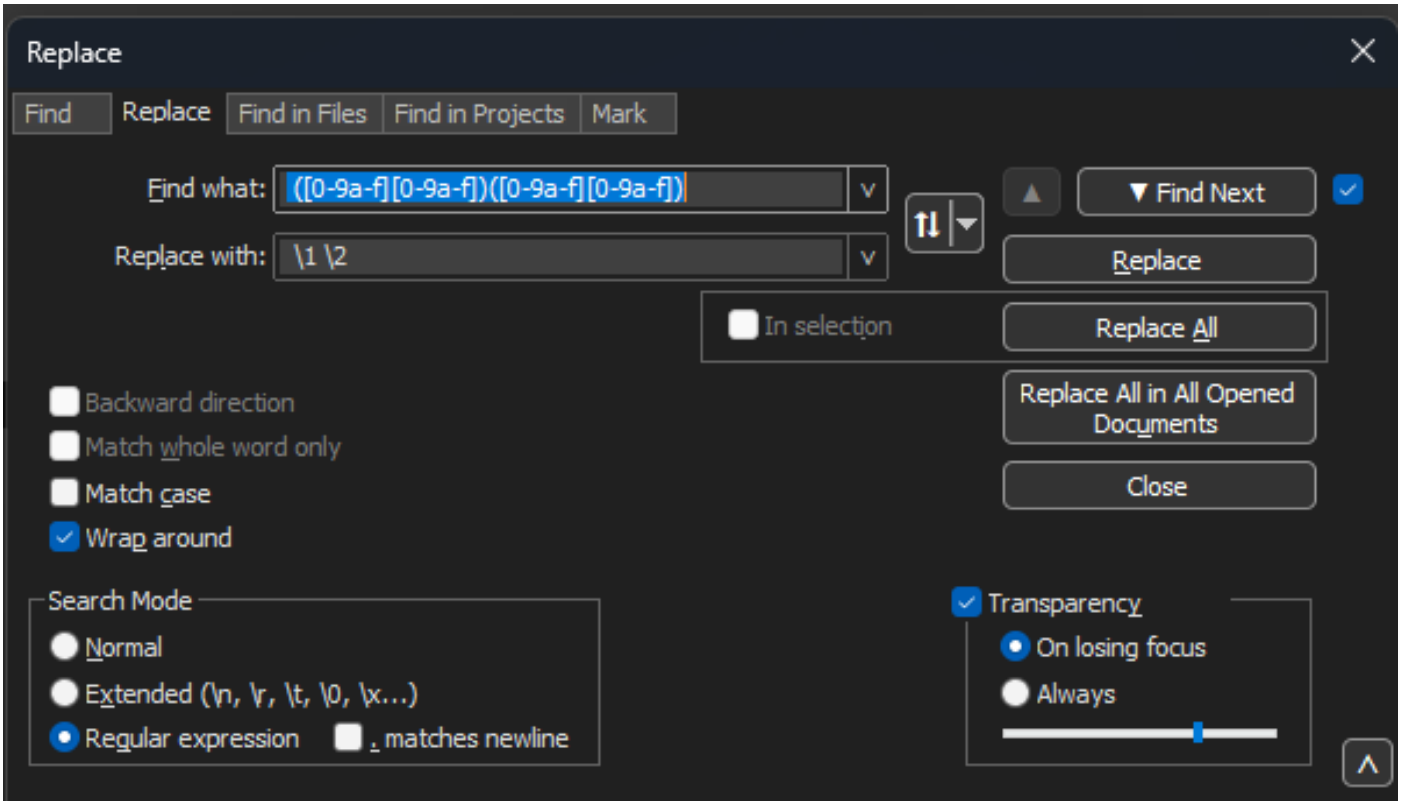
Navegue para Pesquisar>Localizar e selecione a guia Substituir, verifique se o Modo de pesquisa é Expressão regular.

Insira ([0-9a-f][0-9a-f])([0-9a-f][0-9a-f]) (observe o espaço à esquerda) no campo Localizar:.

Preencha o campo Substituir por: com \1 \2 (observe o espaço à esquerda) e clique em Substituir tudo.

A operação de substituição localiza os bytes hexadecimais do pacote e insere um espaço entre cada par. O regex corresponde a um espaço seguido por um par de dígitos hexadecimais, salva-os no grupo de captura 1, em seguida, pega o par adjacente de dígitos hexadecimais, salva-os no grupo de captura 2. A substituição imprime os espaços necessários, bem como o conteúdo de cada grupo de captura.

Leva vários segundos ou minutos, dependendo do comprimento do arquivo. Ele utiliza muita RAM durante a execução. Se o arquivo for grande, seja paciente.



Bloco de Notas++ caixa de diálogo Substituir com o comando localizar o que foi preenchido com uma expressão regular e o campo Substituir preenchido por outra expressão regular.

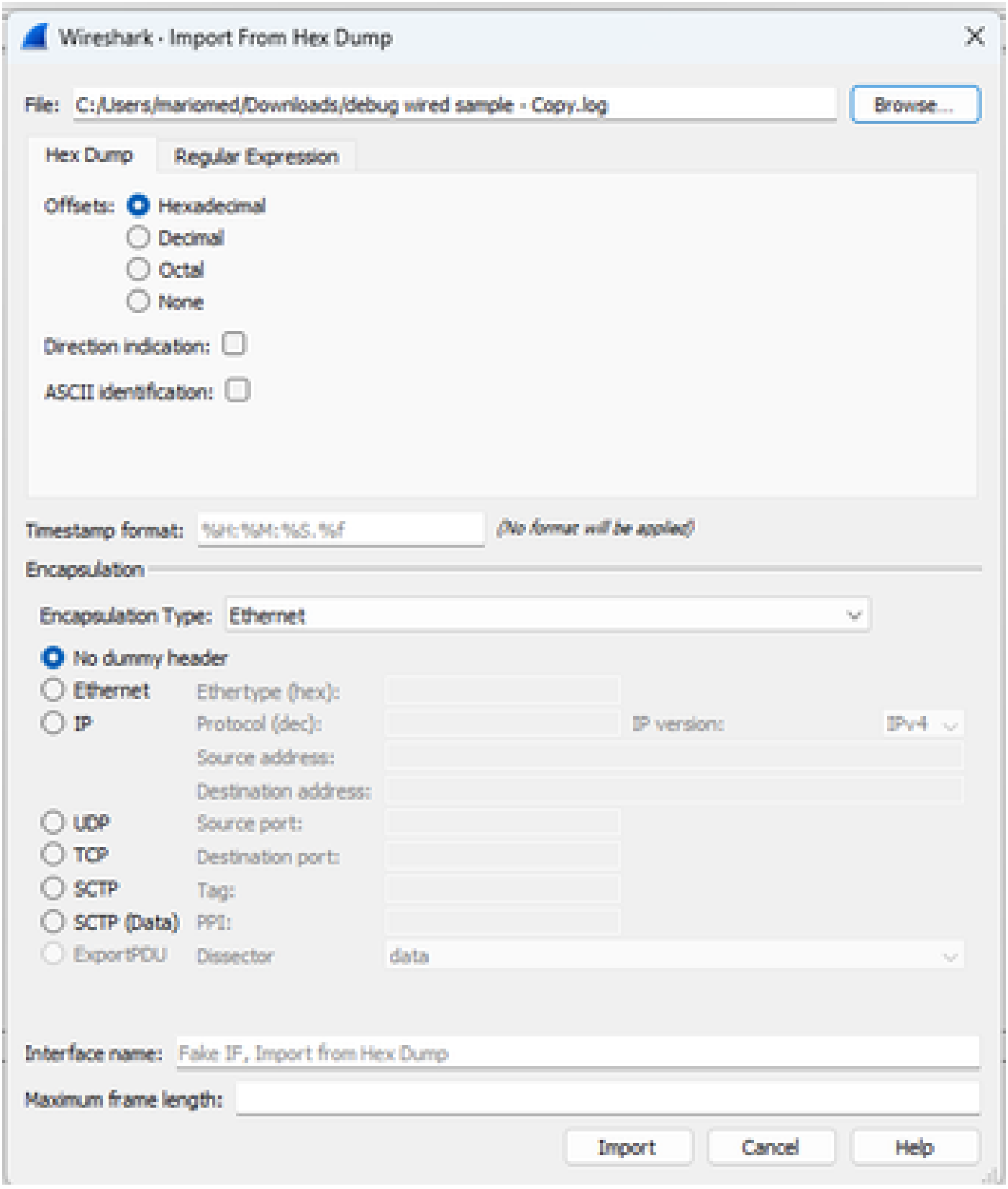
Após a operação anterior, o arquivo de saída resultante se parece com este snippet e está pronto para ser convertido por Text2pcap.

```
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
```

Converter o arquivo de texto em PCAP

Via GUI do Wireshark

Para converter o arquivo completo em pcap, abra o Wireshark e navegue para File>Import from hex dump, uma caixa de diálogo é exibida.



Caixa de diálogo de importação do Wireshark

Clique no botão Browse... e selecione o arquivo de texto de dump. Certifique-se de que o tipo de deslocamento selecionado seja Hexadecimal, que o tipo de encapsulamento seja Ethernet e que

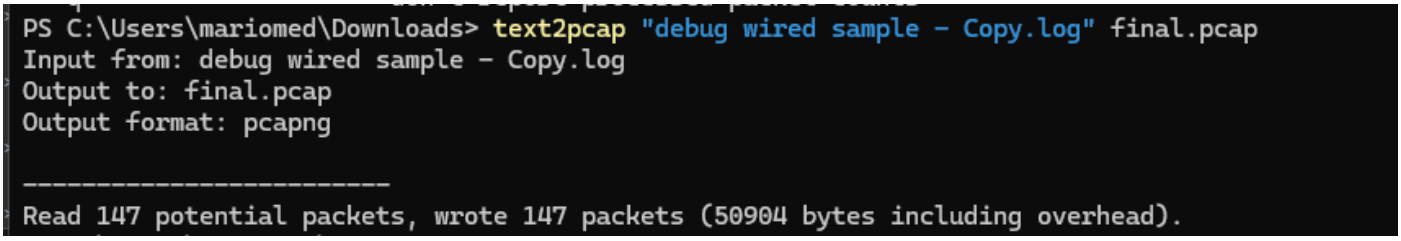
Nenhum cabeçalho fictício esteja selecionado.

Clique em Importar para iniciar o processo de conversão.

Via linha de comando

Para converter um arquivo de texto em um arquivo pcap na linha de comando do Windows, execute <path to wireshark install folder>\text2pcap.exe <path to text file pcap> <output file path>.

Opcionalmente, você pode adicionar a pasta do Wireshark ao seu PATH, caso contrário, você precisa executar text2pcap referenciando o caminho inteiro para o text2pcap.exe toda vez que converter um arquivo. Text2pcap.exe está localizado dentro da pasta de instalação do Wireshark.



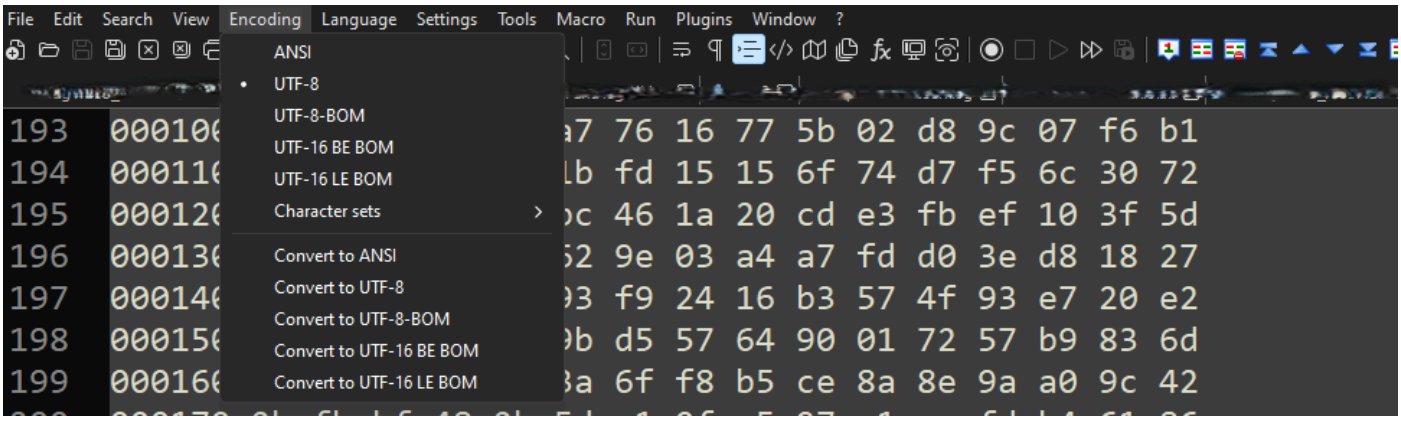
Saída da linha de comando do Windows após a conversão bem-sucedida do despejo de pacotes

Text2pcap também inclui várias opções regex para pré-processar o arquivo de texto, consulte a página de manual Text2pcap para obter mais informações.

Troubleshooting

O arquivo de texto está correto, mas Text2pcap não pode ler nenhum pacote

Text2pcap não pode ler certas codificações de arquivo produzidas por emuladores de terminal comumente usados (Secure CRT, Putty ou outros).
Altere para uma codificação legível por Text2pcap com o Notepad++. Vá para Encoding>UTF-8 e salve o arquivo, em seguida, converta para pcap novamente.



Opções do menu de codificação do Notepad++.

Deslocamento Inconsistente

Esse erro aparece quando os bytes da parte de dados em um pacote não estão separados corretamente em pares, fazendo com que Text2pcap assuma o início de um novo pacote e falhe na interpretação.
Procure qualquer byte de pacote sem separação ou strings no meio de um conteúdo de pacote, como o 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
```

Saída da linha de comando do Windows após tentativa de conversão de arquivo inválido. O deslocamento inconsistente é impresso no terminal várias vezes.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.