Convertir les paquets vidés du point d'accès pour Wireshark

Table des matières

Introduction

Ce document décrit comment convertir un vidage de paquets généré par un point d'accès COS au format PCAP pour Wireshark comme solution de contournement de la limitation de taille.

Conditions préalables

- Bloc-notes++ - Disponible uniquement sous Windows
- Text2pcap installé - inclus dans les installations régulières de Wireshark

Procédure

Effectuer le vidage des paquets

Capturez un vidage de paquets AP en exécutant la commande debug traffic wired <multiple options> verbose sur la ligne de commande AP. Vous avez le choix entre plusieurs filtres et interfaces.

Consignez la session dans le terminal.
Veillez à envoyer le moins de frappes possibles, car plus le fichier contient de caractères

imprimables qui n'appartiennent pas à la capture elle-même, plus le nettoyage à effectuer avant la conversion est important.
La méthode la plus simple consiste à ouvrir une session en mode console pour le vidage des paquets, à répliquer le problème, à arrêter le vidage et à mettre fin immédiatement à la session.

Si vous effectuez le vidage via ssh, utilisez un filtre pour capturer uniquement le trafic concerné. Sinon, la capture contient les paquets de session ssh.

Référez-vous à Dépanner les AP COS pour des instructions complètes sur la façon de configurer la capture.

Lorsque vous avez terminé, arrêtez la capture avec la commande undebug all. Le fichier résultant ressemble à ceci :

```
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>
```

Nettoyage du fichier de sortie

Supprimez toutes les informations qui ne font pas partie du vidage du paquet lui-même. Supprimez les lignes contenant la commande dump, toute invite contenant le nom d'hôte (APname#) et tout autre message syslog non associé présent dans le fichier.

Soyez particulièrement attentif à la commande undebug, car elle peut être imprimée avant le contenu d'un paquet, comme indiqué ci-dessus. Après le nettoyage, le fichier résultant ressemble

à ceci :

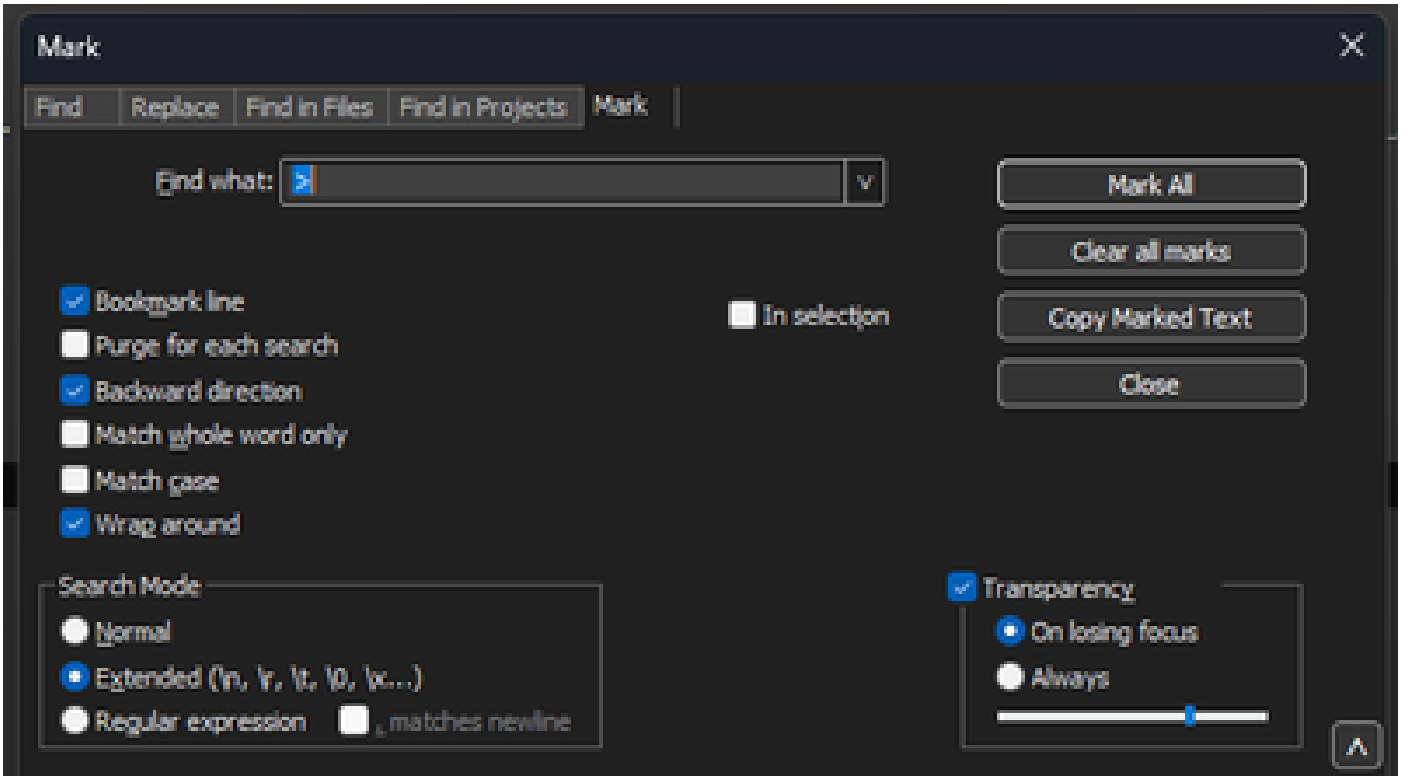
```
22:35:17.1669188 IP CSCO-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656
        0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
        0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
        0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
        0x0030:  7665 7273 696f 6e3d 2231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

Nettoyer les informations récapitulatives des paquets

Le début d'un nouveau paquet est détecté lorsqu'un nouveau décalage 000000 apparaît. Text2pcap peut gérer les informations récapitulatives imprimées avant chaque paquet, afin d'éviter les problèmes, il est préférable de les supprimer.

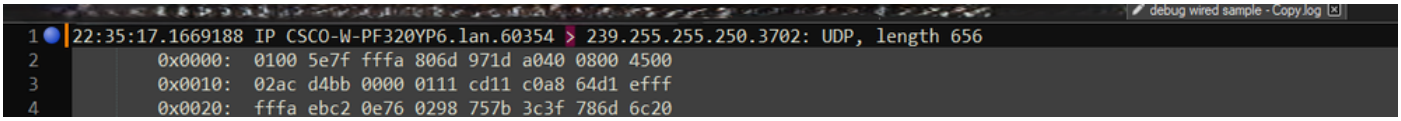
Dans le Bloc-notes++, accédez à Rechercher>Rechercher et sélectionnez l'onglet Marquer, vérifiez que le mode de recherche est Étendu.

Dans le champ Rechercher : saisissez le symbole > et cliquez sur Tout marquer. Cette action crée un signet pour toutes les lignes contenant le symbole >.



Bloc-notes++ boîte de dialogue de marquage avec Trouver ce champ avec le caractère chevron à l'intérieur.

Après avoir marqué les en-têtes, le Bloc-notes++ met en surbrillance toutes les lignes du document comme suit :



Extrait de vidage de paquet avec une ligne en surbrillance qui contient le chevron.

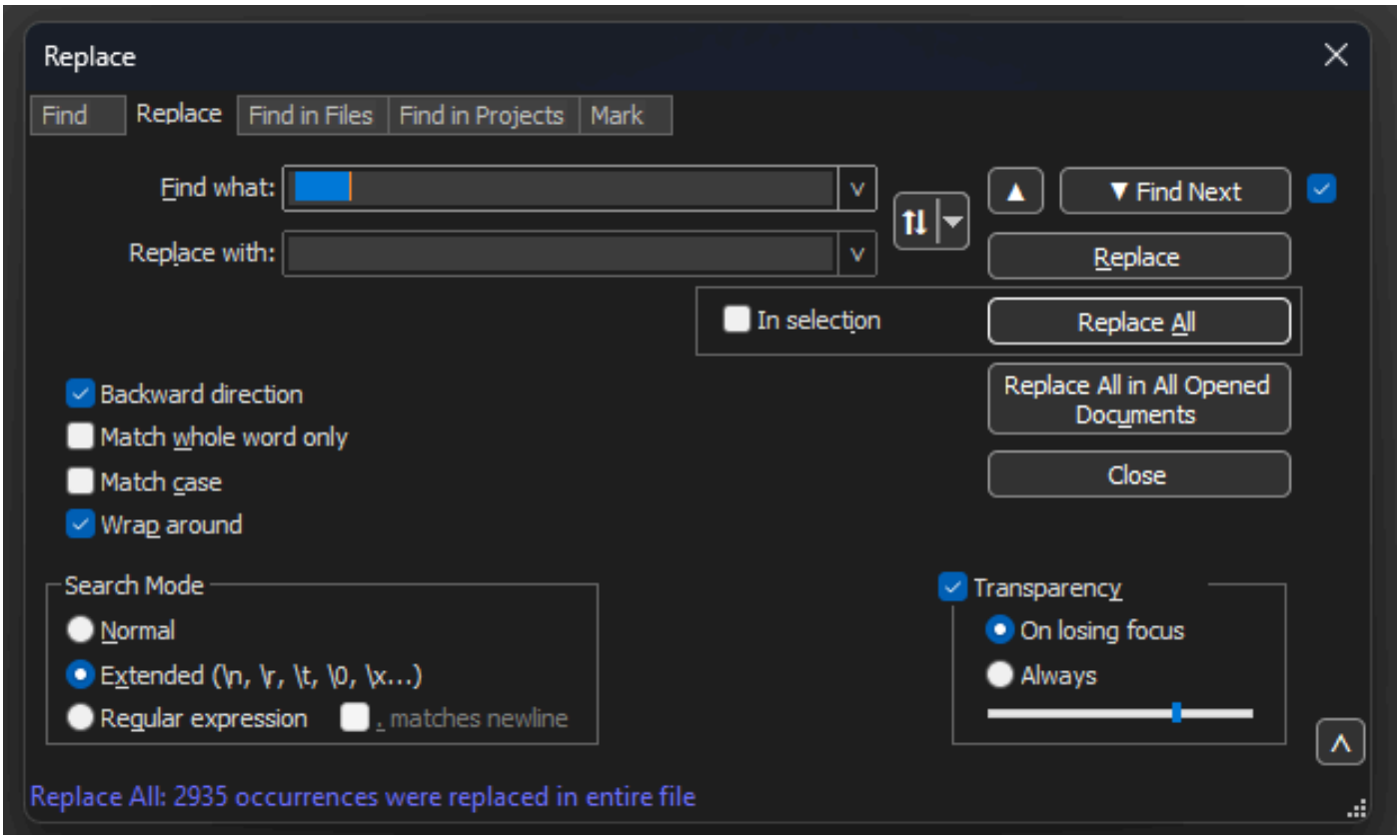
Accédez à Search>Bookmark et cliquez sur Remove bookmarklines. Après cela, le fichier ressemble à l'extrait suivant :

```
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
```

Supprimer les espaces de début et les deux-points décalés

Accédez à Rechercher>Rechercher et sélectionnez l'onglet Remplacer, vérifiez que le mode de recherche est Étendu.

Dans le champ Rechercher : saisissez 8 espaces. Laissez le champ Remplacer par vide et cliquez sur Remplacer tout. Cela remplace les 8 espaces blancs consécutifs au début de chaque ligne par rien, les supprimant ainsi. La boîte de dialogue Remplacer ressemble à cette image.

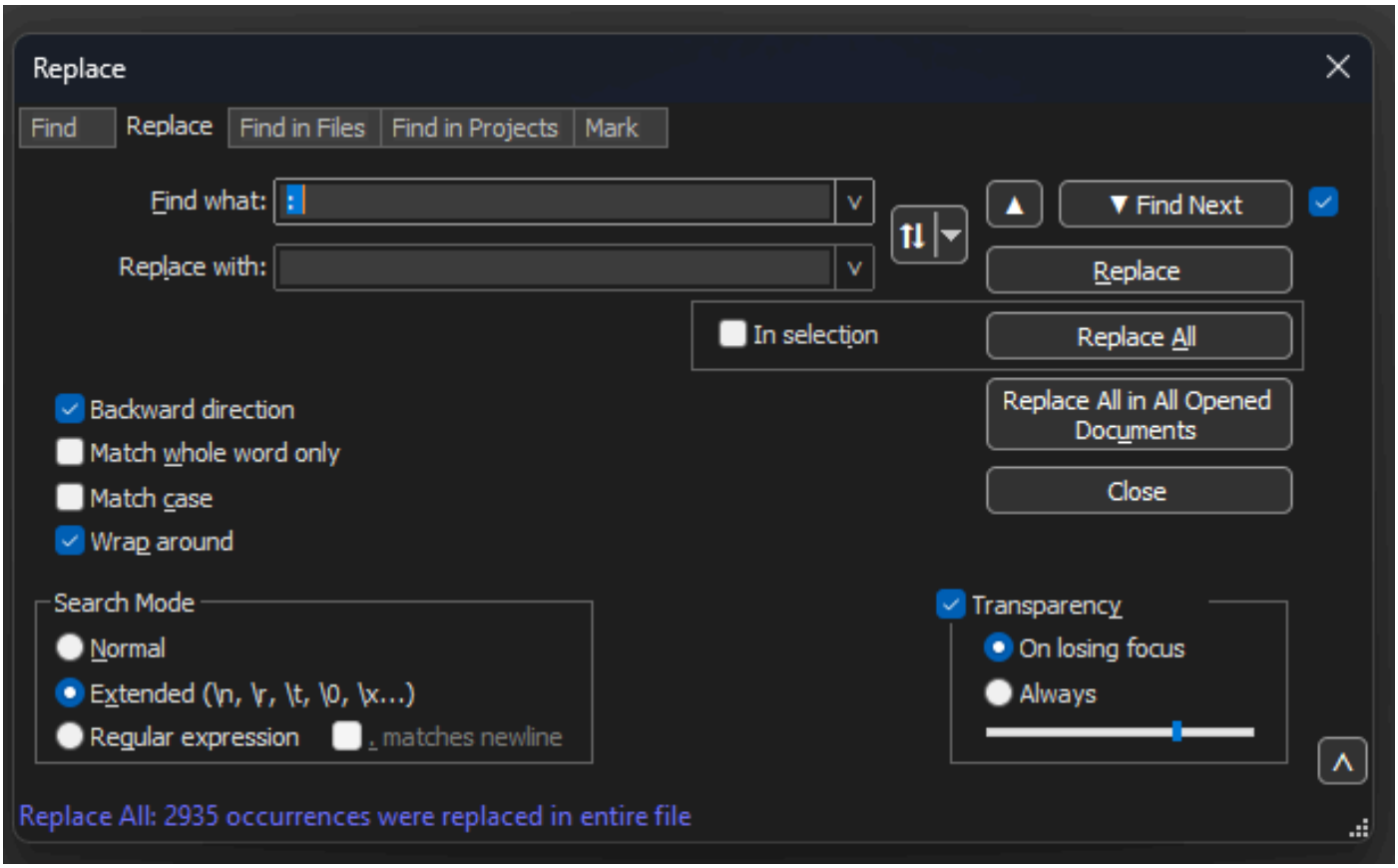


Bloc-notes++ Remplacer boîte de dialogue avec Rechercher ce champ avec 8 espaces.

Le fichier résultant après cette opération ressemble à l'extrait suivant :

```
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
```

Accédez à Rechercher>Rechercher et sélectionnez l'onglet Remplacer, vérifiez que le mode de recherche est Étendu. Saisissez : (notez l'espace vide après les deux-points) dans le champ Rechercher. Laissez le champ Remplacer par vide et cliquez sur Remplacer tout.
Ceci remplace tous les deux-points et les premiers espaces après le décalage.



Bloc-notes++ Remplacer boîte de dialogue avec Rechercher ce champ rempli par un deux-points et un espace.

Après l'opération précédente, le fichier de sortie obtenu ressemble à l'extrait suivant :

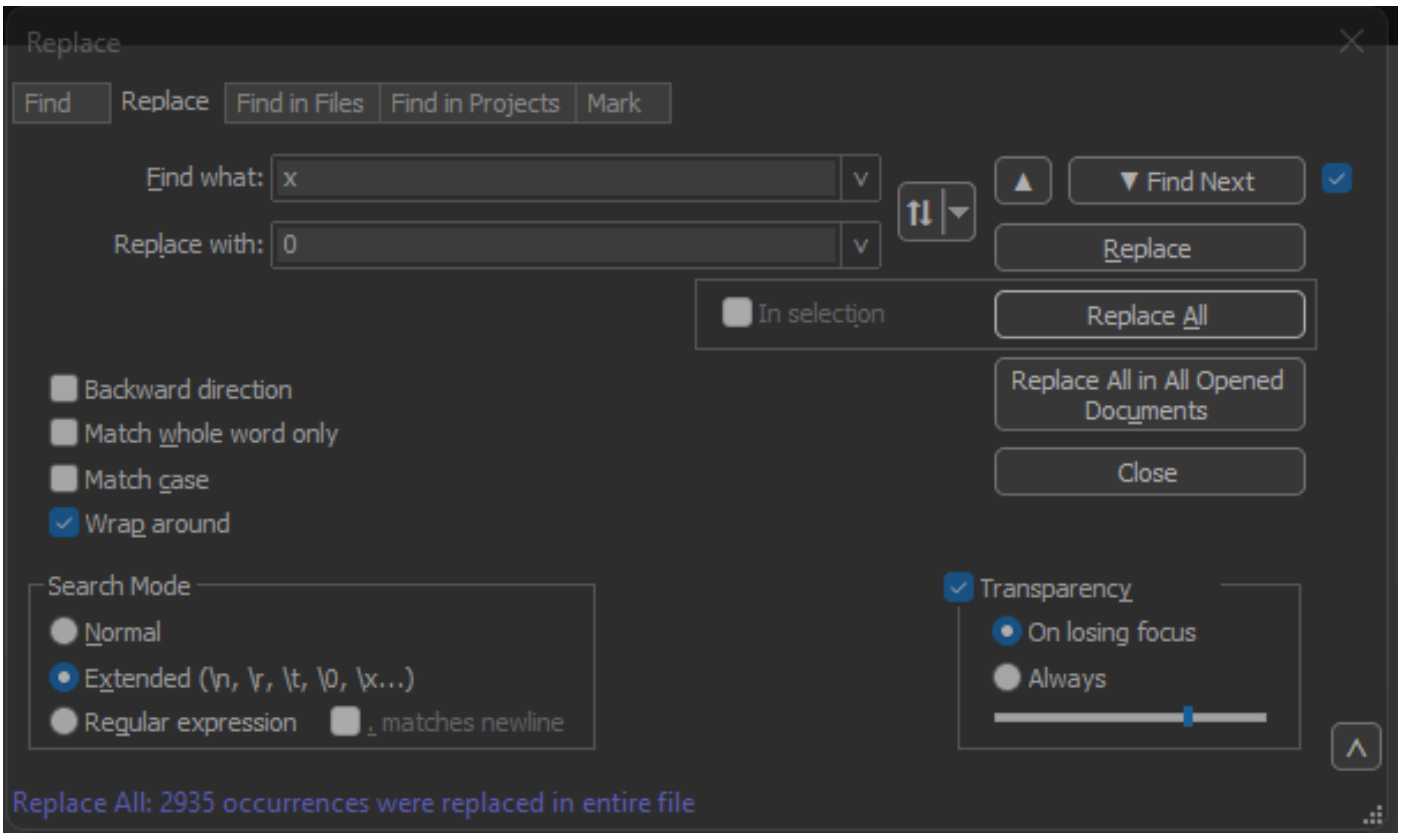
```
0x0000 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060 6d6c 6e73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

Décalage de paquet correct

Text2pcap attend un décalage de paquet à l'intérieur de chaque paquet sous la forme d'une chaîne hexadécimale de 6 caractères, mais les vidages de paquets AP utilisent 0x pour symboliser le décalage à la place. Pour le corriger, accédez à Rechercher>Rechercher et sélectionnez l'onglet Remplacer, vérifiez que le mode de recherche est Étendu.

Saisissez x dans le champ Rechercher. Remplissez le champ Remplacer par : avec 0 et cliquez

sur Remplacer tout. Ceci remplace tout x à l'intérieur du décalage par 0 pour correspondre au format de décalage attendu pour Text2pcap.



Bloc-notes++ Remplacer la boîte de dialogue avec Rechercher le champ rempli avec le caractère x et Remplacer le champ rempli avec le caractère 0.

Après l'opération précédente, le fichier de sortie obtenu ressemble à l'extrait suivant :

```
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
```

Octets de paquet séparés

Le format de données Text2pcap nécessite que chaque paire de valeurs hexadécimales soit séparée par un espace. Un format incorrect entraîne la lecture des données de paquet par Text2pcap en tant que décalage et l'échec.

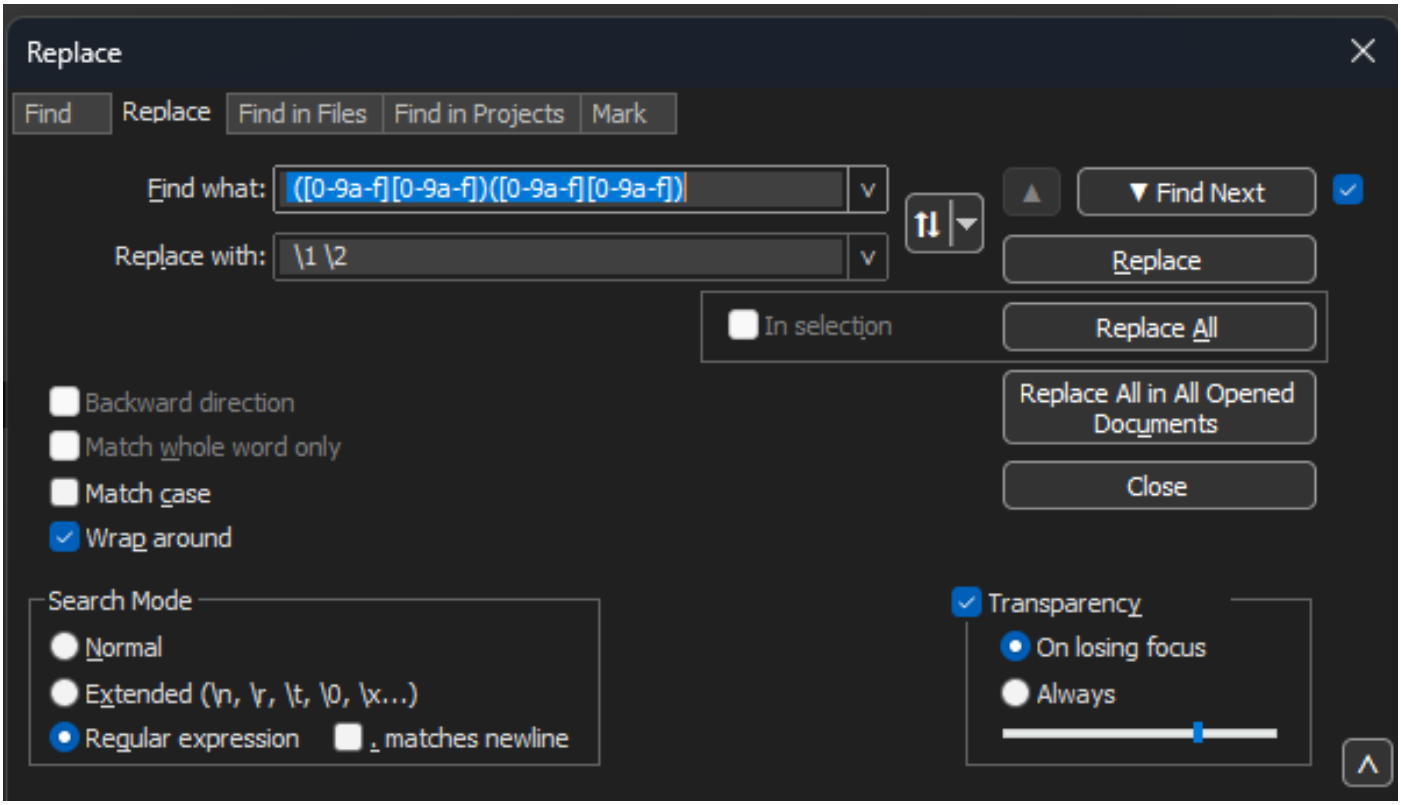
Accédez à Rechercher>Rechercher et sélectionnez l'onglet Remplacer, assurez-vous que le mode de recherche est l'expression régulière.

Saisissez ([0-9a-f][0-9a-f])([0-9a-f][0-9a-f]) (notez l'espace de début) dans le champ Find what:.

Remplissez le champ Remplacer par : par \1 \2 (notez l'espace d'en-tête) et cliquez sur Remplacer tout.

L'opération de remplacement recherche les octets hexadécimaux du paquet et insère un espace entre chaque paire. L'expression régulière correspond à un espace suivi d'une paire de chiffres hexadécimaux, les enregistre sur le groupe de capture 1, puis prend la paire de chiffres hexadécimaux adjacente, les enregistre sur le groupe de capture 2. Le texte de remplacement imprime à la fois les espaces requis et le contenu de chaque groupe de capture.

Cela prend plusieurs secondes ou minutes en fonction de la longueur du fichier. Il utilise beaucoup de mémoire vive lors de l'exécution. Si le fichier est volumineux, soyez patient.



Bloc-notes++ Remplacer la boîte de dialogue avec la recherche de ce qui est rempli avec une expression régulière et le champ Remplacer rempli par une autre expression régulière.

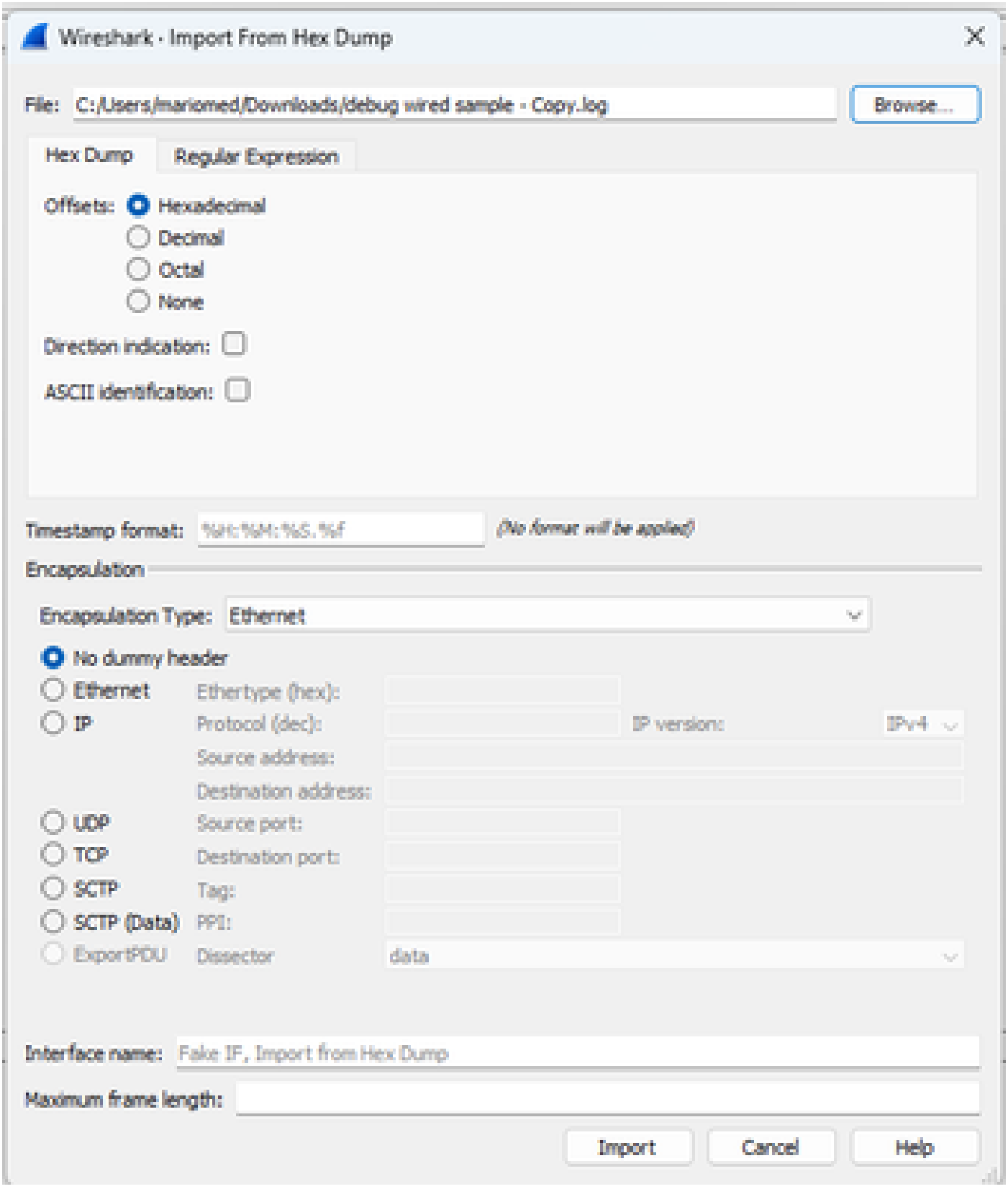
Après l'opération précédente, le fichier de sortie résultant ressemble à cet extrait et est prêt à être converti par Text2pcap.

```
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 le fichier texte en PCAP

Via l'interface graphique Wireshark

Pour convertir le fichier complet en pcap, ouvrez Wireshark et naviguez vers Fichier>Importer à partir de la vidage hexadécimal, une boîte de dialogue s'affiche.



Boîte de dialogue Importation Wireshark

Cliquez sur le bouton Browse... et sélectionnez le fichier texte de vidage. Assurez-vous que le type de décalage sélectionné est hexadécimal, que le type d'encapsulation est Ethernet et

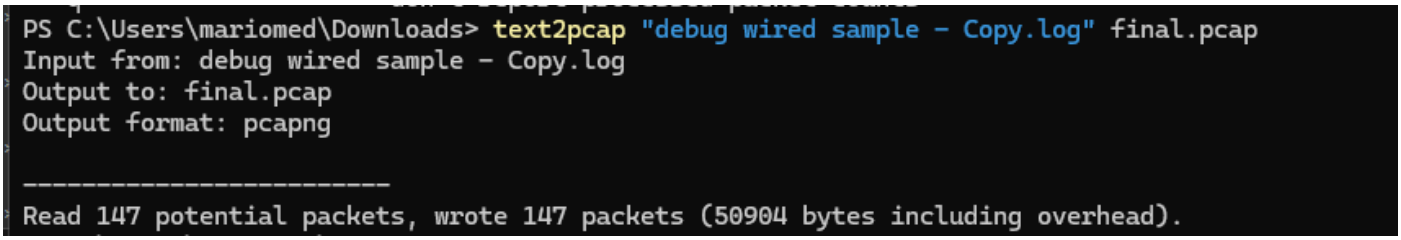
qu'aucun en-tête factice n'est sélectionné.

Cliquez sur Import pour lancer le processus de conversion.

Via la ligne de commande

Pour convertir un fichier texte en fichier pcap dans la ligne de commande Windows, exécutez <chemin d'accès au dossier d'installation de wireshark>\text2pcap.exe <chemin d'accès au fichier texte pcap> <chemin d'accès au fichier de sortie>.

Vous pouvez éventuellement ajouter un dossier wireshark à votre PATH, sinon vous devez exécuter text2pcap en référençant le chemin complet vers le fichier text2pcap.exe chaque fois que vous convertissez un fichier. Text2pcap.exe se trouve dans le dossier d'installation de wireshark.



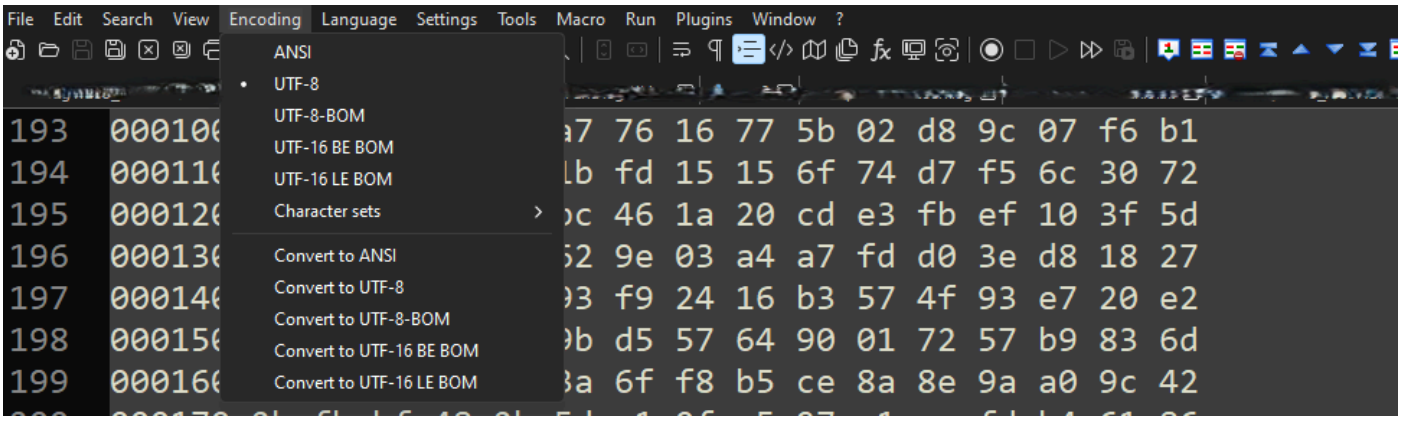
Sortie de la ligne de commande Windows après la conversion réussie du vidage de paquets

Text2pcap inclut également plusieurs options regex pour pré-traiter le fichier texte, veuillez vous reporter à la page de manuel Text2pcap pour plus d'informations.

Dépannage

Le fichier texte est correct, mais Text2pcap ne peut lire aucun paquet

Text2pcap ne peut pas lire certains codages de fichiers produits par les émulateurs de terminal couramment utilisés (Secure CRT, Putty ou autres).
Passez à un codage lisible par Text2pcap avec Notepad++. Accédez à Encoding>UTF-8 et enregistrez le fichier, puis convertissez à nouveau en pcap.



Options du menu Notepad++ encoding.

Décalage incohérent

Cette erreur apparaît lorsque les octets de la partie données d'un paquet ne sont pas correctement séparés en paires, ce qui fait que Text2pcap assume le début d'un nouveau paquet et ne parvient pas à interpréter.
Recherchez des octets de paquets sans séparation ni chaînes au milieu d'un contenu de paquet tel que la undebug all commande.

```
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
```

Sortie de la ligne de commande Windows après la tentative de conversion d'un fichier non valide. Un décalage incohérent est imprimé plusieurs fois sur le terminal.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.