Capturer le trafic réseau avec Wireshark

Table des matières

Introduction

Ce document décrit comment capturer le trafic réseau avec Wireshark.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur la sécurité de la couche de DNS Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Parfois, le personnel de l'assistance Cisco Umbrella demande une capture de paquets du trafic Internet circulant entre votre ordinateur et le réseau. La capture permet à la prise en charge d'Umbrella d'analyser le trafic à un niveau bas et d'identifier les problèmes potentiels.

Dans la plupart des cas, il est utile de comparer deux ensembles de captures de paquets illustrant

un scénario de fonctionnement et un scénario de non-fonctionnement.

- Assurez-vous que vous pouvez répliquer le problème et effectuer ces étapes pendant que le problème se produit. Générez une capture de paquets montrant un scénario de non-fonctionnement. Veuillez noter la date et l'heure avec le fuseau horaire afin que ces informations puissent être corrélées avec d'autres données.
- Si possible, répétez ces instructions avec le logiciel Umbrella (et/ou le transfert DNS Umbrella) désactivé. Générez une capture de paquets montrant le scénario de travail. Veuillez noter la date et l'heure avec le fuseau horaire afin que ces informations puissent être corrélées avec d'autres données.

Instructions de Wireshark

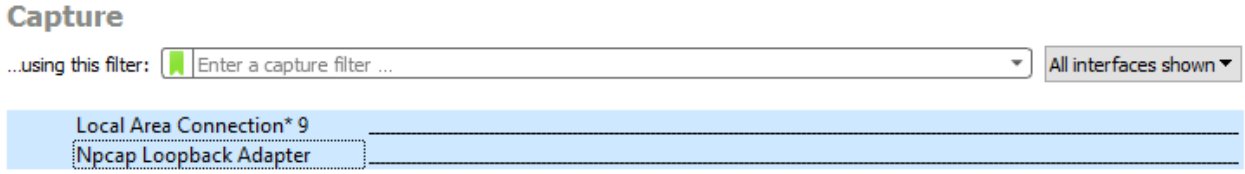
Préparations

1. Téléchargez Wireshark.
2. Déconnectez toutes les connexions réseau inutiles.
    1. Déconnectez les connexions VPN, sauf si elles sont nécessaires pour répliquer le problème.
    2. Utilisez uniquement une connexion filaire ou sans fil et non les deux ensemble.
3. Fermez tous les autres logiciels qui ne sont pas nécessaires pour répliquer le problème.
4. Effacez les cookies et le cache de votre navigateur.
5. Videz votre cache DNS. Sous Windows, avec la commande :

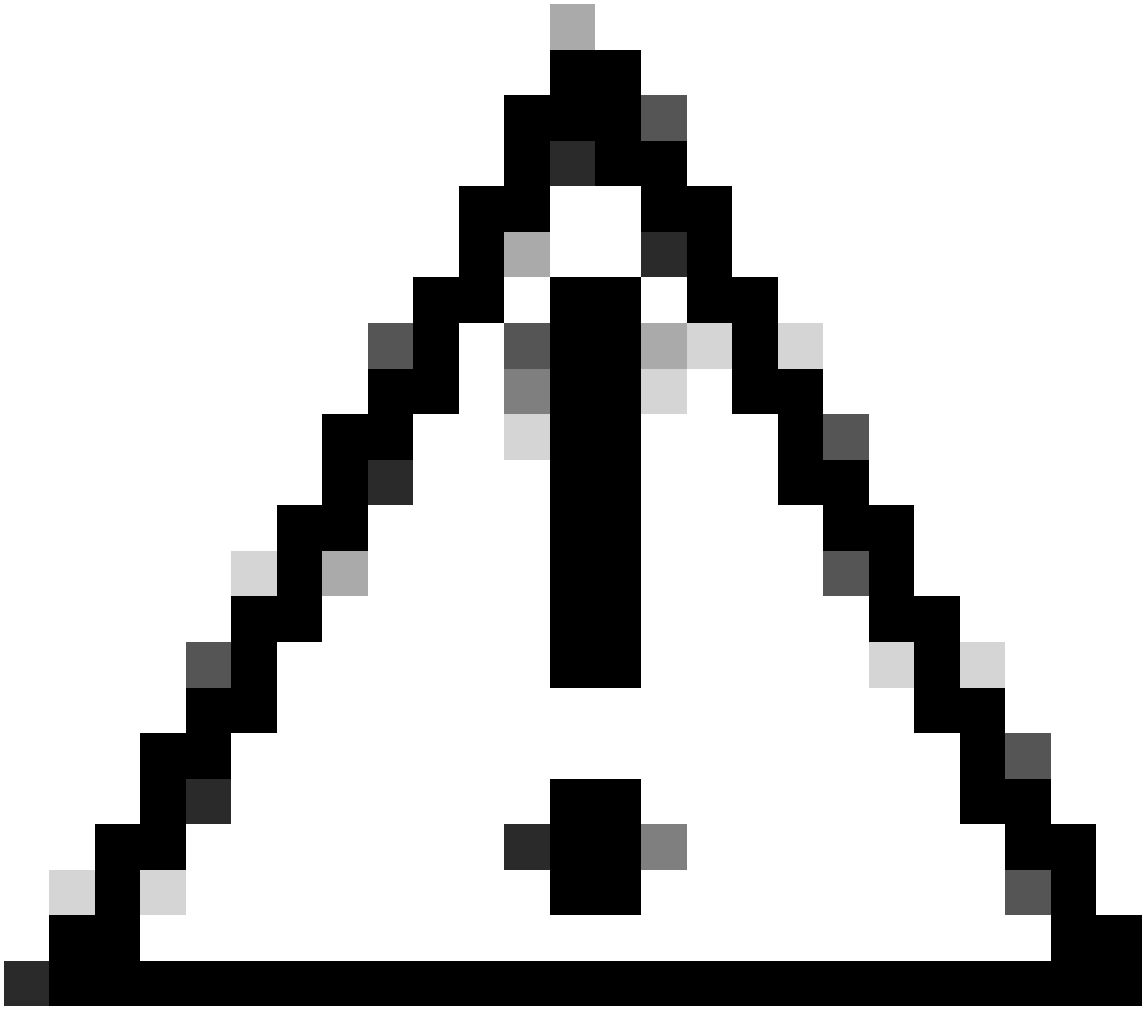
```
ipconfig /flushdns
```

Capture Wireshark de base

1. Lancez Wireshark.
2. Le panneau Capture affiche vos interfaces réseau. Sélectionnez les interfaces appropriées. Vous pouvez sélectionner plusieurs interfaces en utilisant la touche CTRL (Windows) ou la touche CMD (Mac) lors de la sélection.



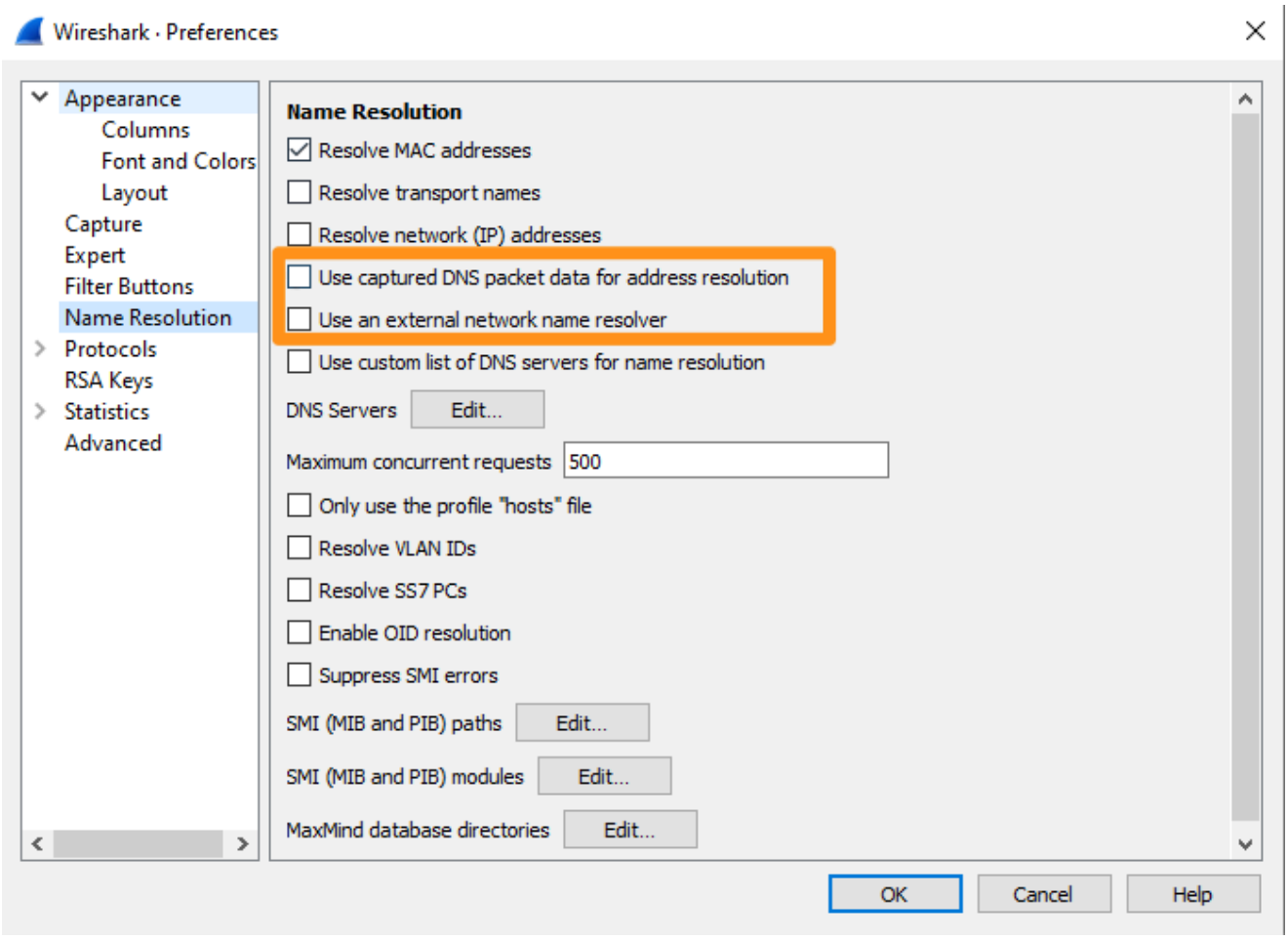
wireshark_1.png



Mise en garde : Il est important de sélectionner la ou les interfaces correctes qui contiennent le trafic réseau. Utilisez la commande "ipconfig" (Windows) ou "ifconfig" (Mac) pour afficher plus de détails sur vos interfaces réseau. Les utilisateurs du client d'itinérance doivent également sélectionner l'adaptateur de bouclage NPCAP OU le bouclage : interfaces lo0 En cas de doute, sélectionnez toutes les interfaces.

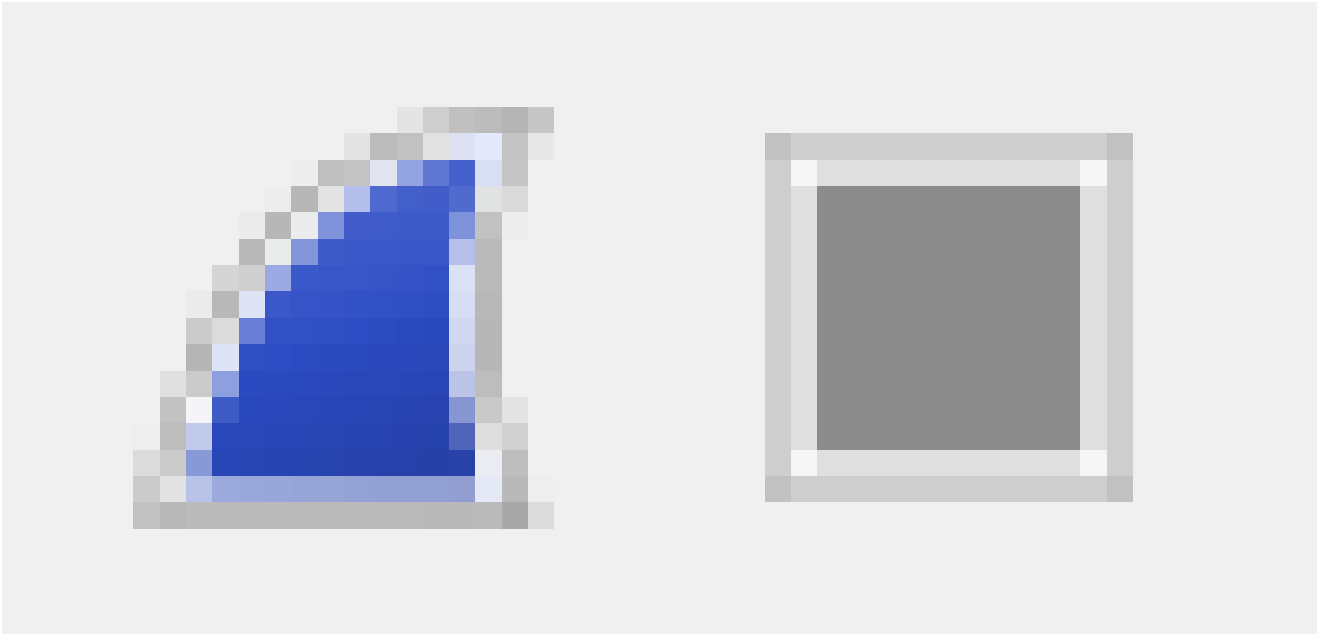
---

3. Assurez-vous que Utiliser les données de paquet DNS capturées pour la résolution d'adresse et Utiliser un programme de résolution de noms de réseau externe ne sont PAS sélectionnés pour garantir que Wireshark n'effectue pas de requêtes DNS, car cela peut compliquer la capture et affecter AnyConnect. Les paramètres sont valides à partir de Wireshark 3.4.9 :



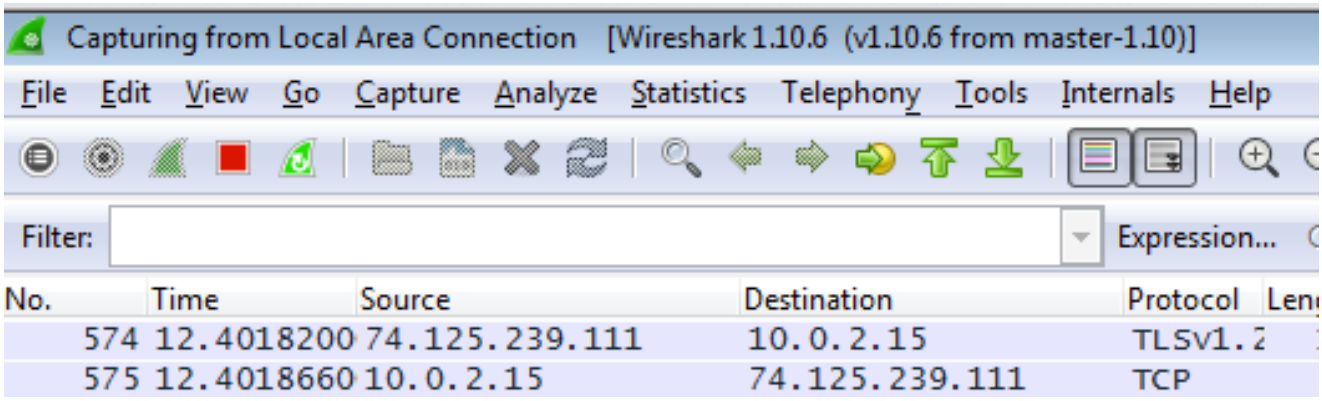
Capture_PNG.png

4. Sélectionnez Capture > Start ou cliquez sur l'icône Blue start.



wireshark_2.png

5. Lorsque Wireshark s’exécute en arrière-plan, répliquez le problème.



wireshark_3.png

6. Une fois le problème entièrement répliqué, sélectionnez Capture > Stop ou utilisez l'icône Stop rouge.
7. Accédez à Fichier > Enregistrer sous et sélectionnez un emplacement pour enregistrer le fichier. Assurez-vous que le fichier est enregistré en tant que type PCAPNG. Le fichier enregistré peut être envoyé à l'assistance Cisco Umbrella pour révision.

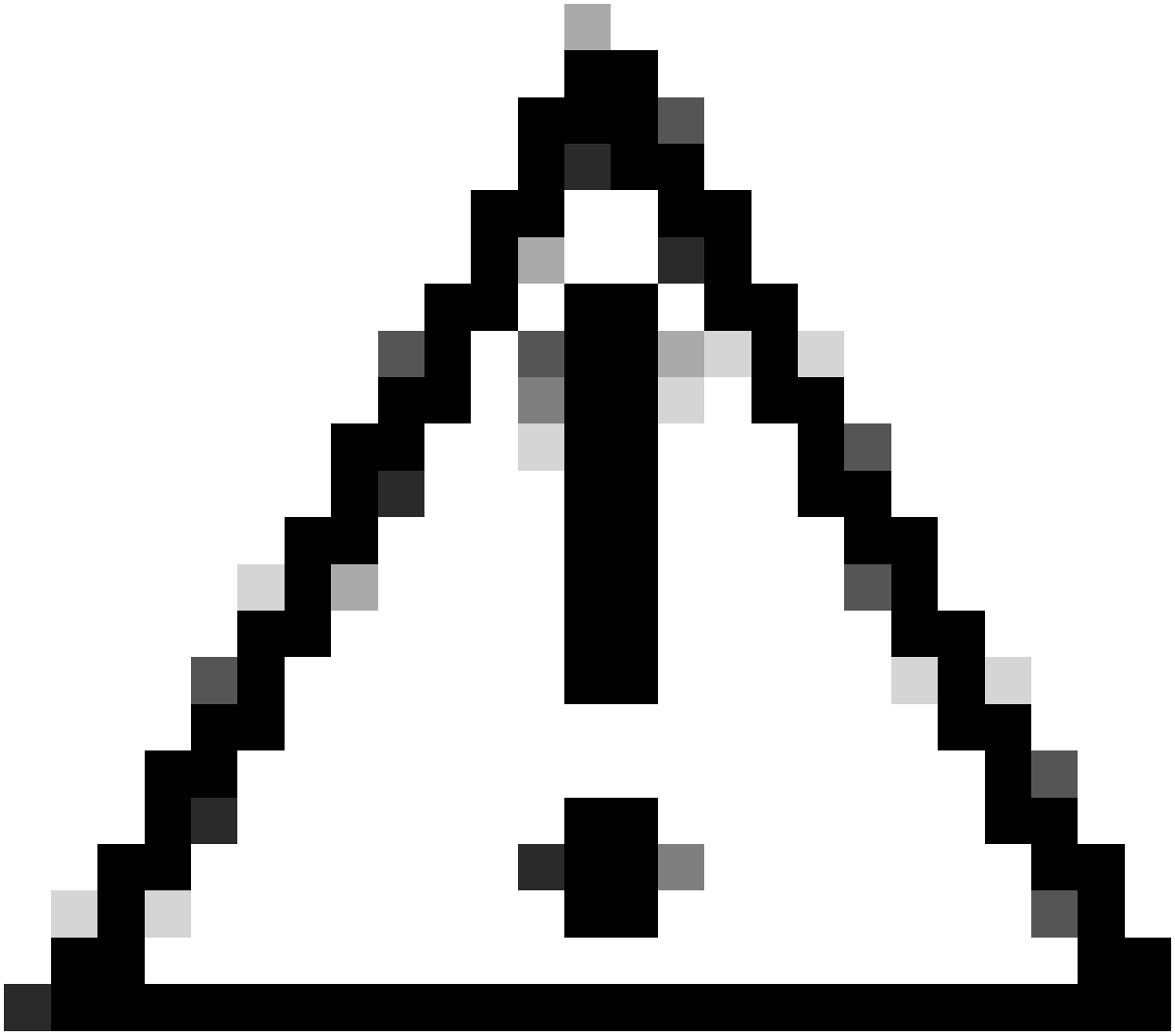
Client d'itinérance - Étapes supplémentaires

D'autres étapes doivent être effectuées pour les utilisateurs autonomes de clients d'itinérance et de modules d'itinérance AnyConnect :

Trafic en boucle

Lorsque vous sélectionnez une interface, vous devez également capturer le trafic sur l’interface de bouclage (127.0.0.1) en plus des autres interfaces réseau. Le proxy DNS du client d'itinérance écoute sur cette interface. Il est donc essentiel de voir le trafic entre le système d'exploitation et le client d'itinérance.

- Fenêtres: Sélectionnez NPCAP Loopback Adapter
- Mac : Sélectionnez Bouclage : lo0



Mise en garde : Les versions Windows plus récentes de Wireshark sont fournies avec le pilote de capture NPCAP, qui prend en charge le pilote de bouclage. Si l'adaptateur de bouclage est manquant, effectuez une mise à jour vers la dernière version de Wireshark ou suivez les instructions de rawcap.exe.

Trafic DNS chiffré

Dans des circonstances normales, le trafic entre le client d'itinérance et Umbrella est chiffré et illisible. Dans certains cas, la prise en charge d'Umbrella peut vous demander de désactiver le cryptage DNS pour afficher le trafic DNS entre le client d'itinérance et le cloud Umbrella. Il existe deux méthodes pour ce faire :

- Créez un bloc de pare-feu local pour UDP 443 à 208.67.220.220 et 208.67.222.222.
- Vous pouvez également créer le fichier en fonction de votre système d'exploitation et de la version du client d'itinérance :
    - Fenêtres:

      ```
      C:\ProgramData\OpenDNS\ERC\force_transparent.flag
      ```

- Windows AnyConnect :

  `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\force_transparent`

- Client sécurisé Windows :

  `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\force_transparent.flag`

- macOS :

  `/Library/Application Support/OpenDNS Roaming Client/force_transparent.flag`

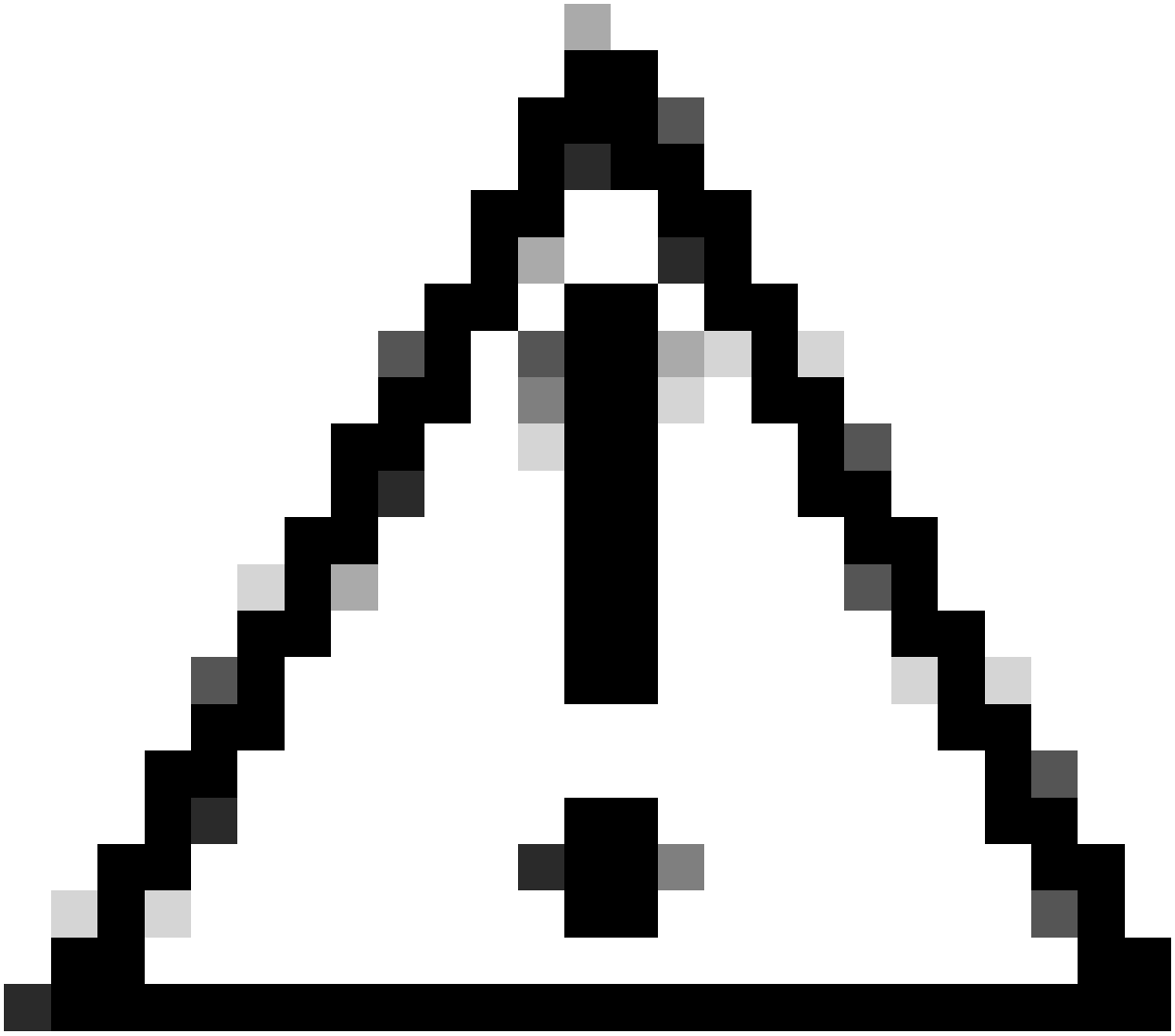
- mac OS AnyConnect :

  `/opt/cisco/anyconnect/umbrella/data/force_transparent.flag`

- mac OS Secure Client :

  `/opt/cisco/secureclient/umbrella/data/force_transparent.flag`

Après avoir effectué cette opération, redémarrez le service ou votre ordinateur.



Mise en garde : Les versions plus récentes de Wireshark sous Windows incluent le pilote de capture NPCAP, qui ne prend pas en charge l'interface VPN Umbrella. Sous Windows, vous devrez peut-être utiliser l'outil rawcap.exe comme alternative.

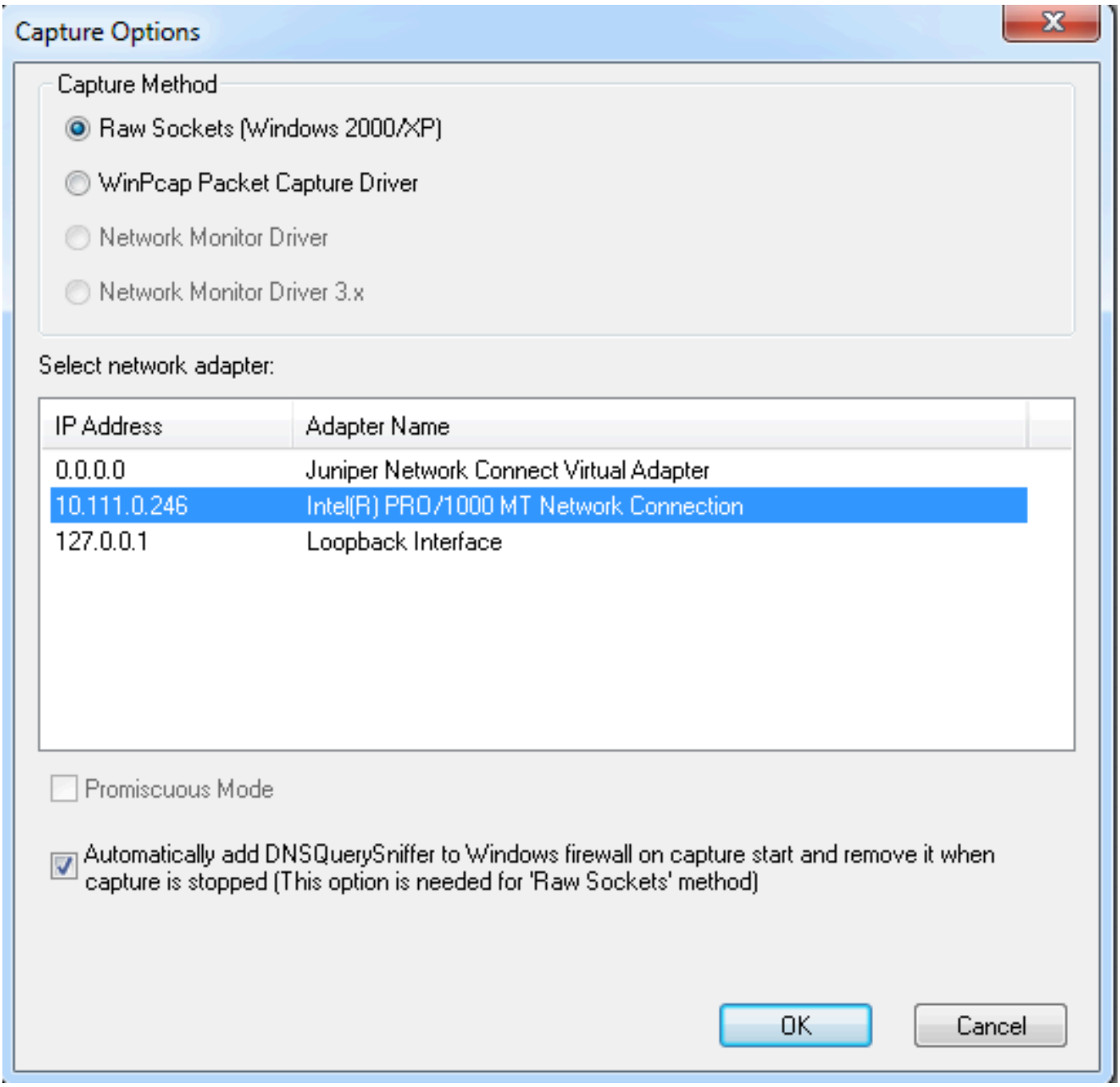
DNSQuerySniffer - Alternative Windows

DNSQuery Sniffer est un analyseur de réseau DNS uniquement pour Windows qui surveille et affiche des tonnes de données utiles. Contrairement à Wireshark ou Rawcap, il est utilisé uniquement pour le DNS et il est beaucoup plus facile d’examiner et d’extraire les informations pertinentes. Cependant, il ne dispose pas des puissants outils de filtrage de Wireshark.

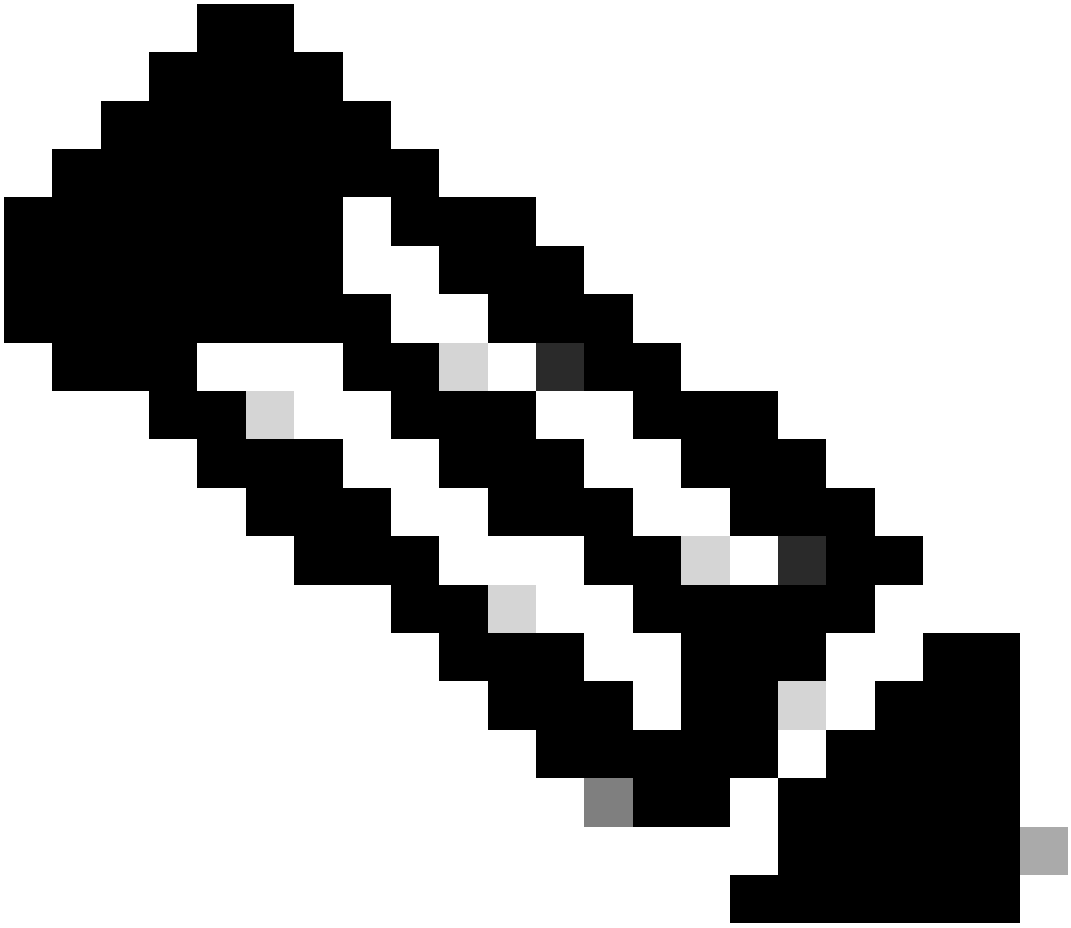
Il s'agit d'un outil léger et facile à utiliser. L'un des avantages de cette méthode est que vous pouvez détecter les paquets lorsque le service client d'itinérance est désactivé, démarrer la capture et afficher chaque requête DNS envoyée par le client d'itinérance à partir du moment où il démarre, plutôt que de démarrer une capture après le démarrage du client d'itinérance.

Il existe deux méthodes de capture :

1. Si vous sélectionnez l'interface réseau normale, vous ne pouvez voir que les requêtes qui figurent dans la liste Domaines internes ou qui n'ont pas transité spécifiquement par le dnscryptproxy.



dns_1.png

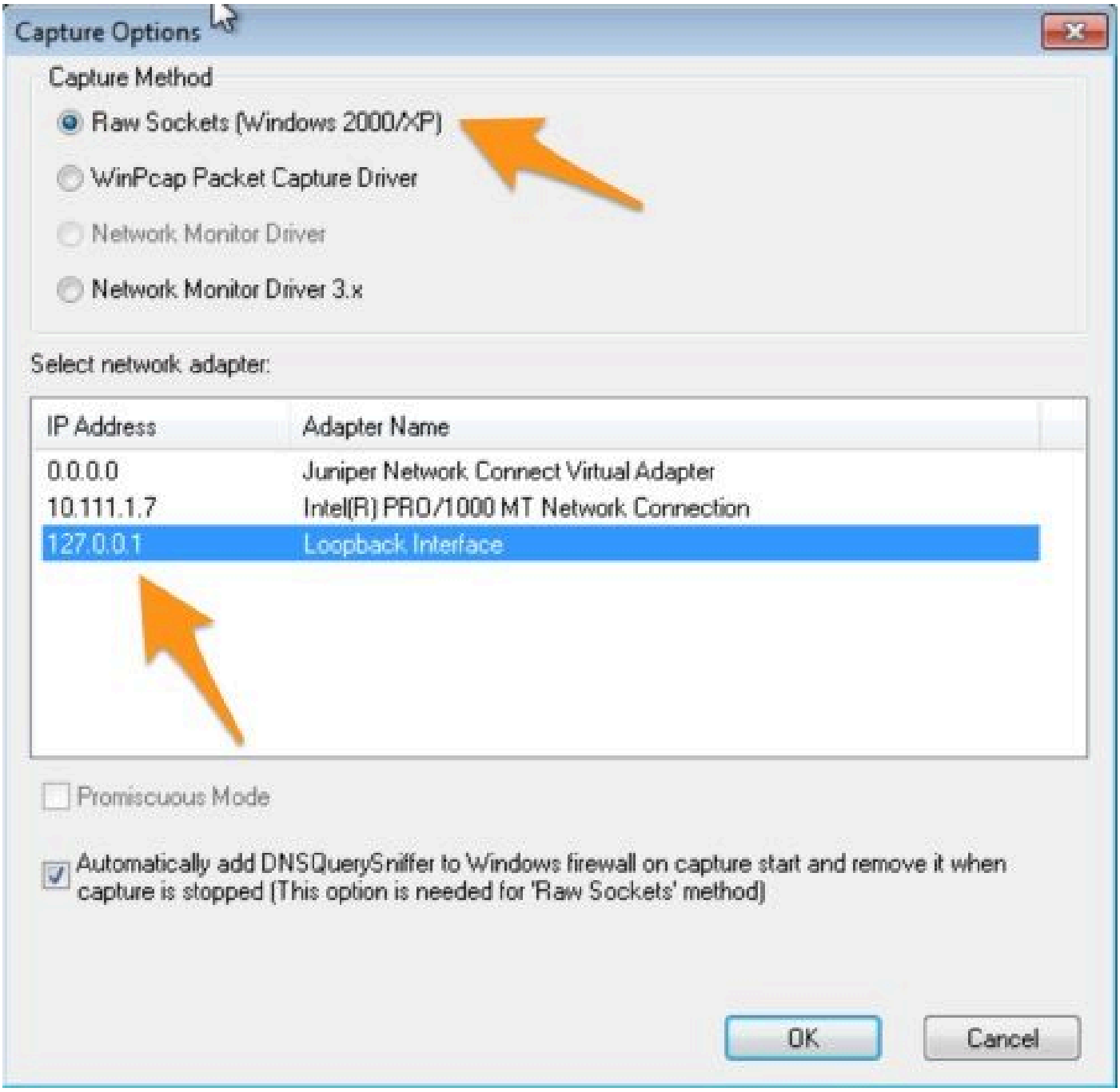


Remarque : Ces colonnes apparaissent tout à droite dans la capture et vous devez faire défiler un peu pour les voir.

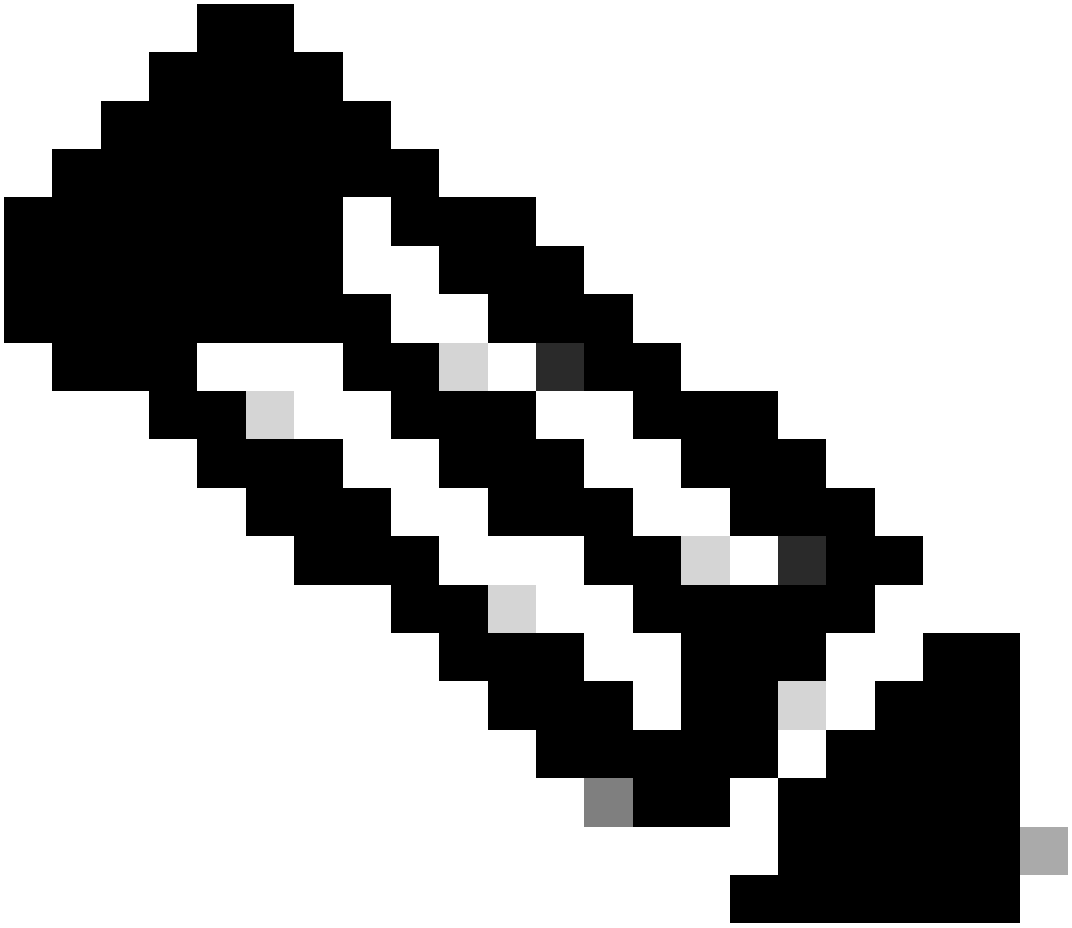
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

Colonnes DNSSniffer

2. Si vous sélectionnez l'interface de bouclage, vous voyez toutes les requêtes DNS qui sont envoyées via le dnscryptproxy, mais vous ne pouvez pas voir la véritable adresse IP de destination pour les domaines sur la liste Domaines internes. Cependant, il affiche toujours la requête et la réponse.


Capture Options
Capture Method
Raw Sockets (Windows 2000/XP)
WinPcap Packet Capture Driver
Network Monitor Driver
Network Monitor Driver 3.x
Select network adapter:
IP Address
Adapter Name
0.0.0.0
Juniper Network Connect Virtual Adapter
10.111.1.7
Intel(R) PRO/1000 MT Network Connection
127.0.0.1
Loopback Interface
Promiscuous Mode
Automatically add DNSQuerySniffer to Windows firewall on capture start and remove it when capture is stopped (This option is needed for 'Raw Sockets' method)
OK
Cancel

dns_2.jpg

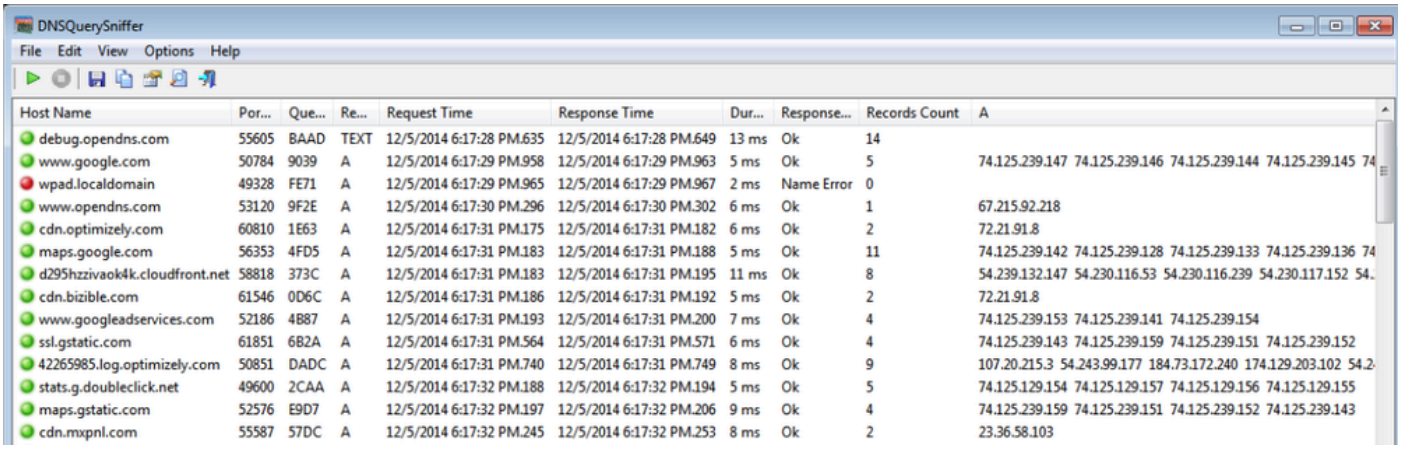


Remarque : Ces colonnes apparaissent à droite dans la capture et vous devez faire défiler la liste pour les voir.

Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

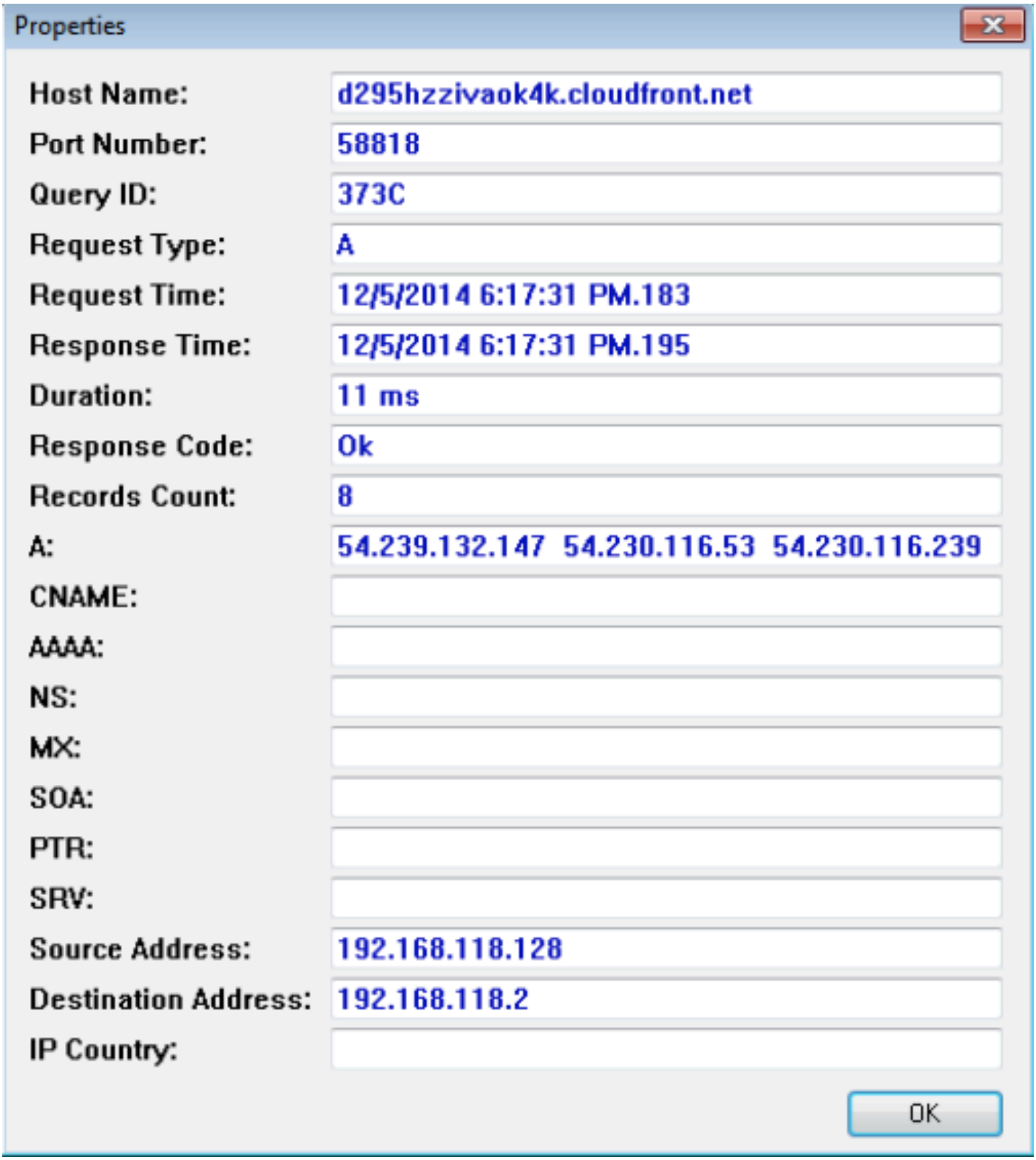
Colonnes DNSSniffer

Les résultats sont les suivants :



dns_3.png

Affichage d'une recherche individuelle :



dns_4.png

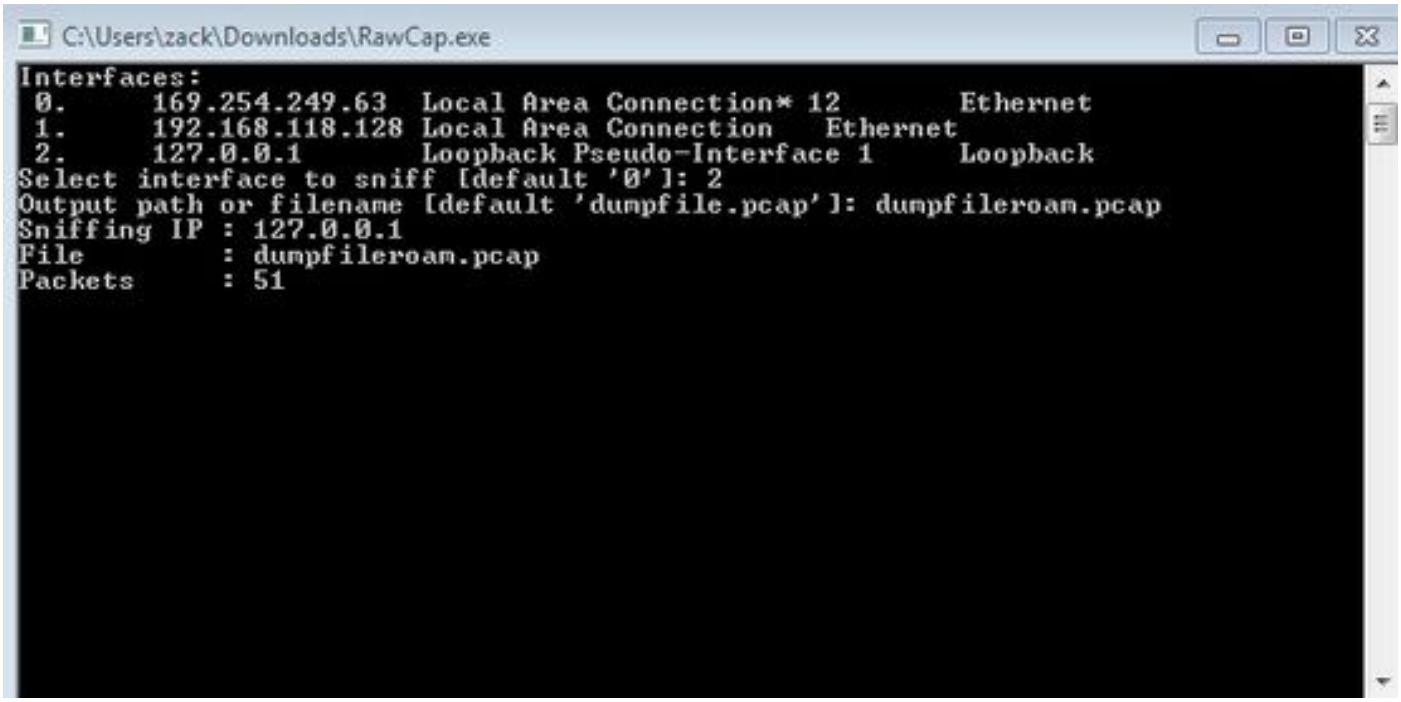
RawCap.exe - Alternative Windows

Dans certaines circonstances, l'interface avec laquelle vous devez travailler n'est pas prise en charge par le pilote de capture de paquets fourni avec Wireshark. Cela peut être un problème pour l'interface de bouclage.

Dans ces cas, nous pouvons utiliser RawCap.exe :

1. Suivez les étapes décrites précédemment dans l'article pour utiliser Wireshark pour capturer le trafic normal.
2. En même temps, exécutez RawCap.exe.
3. Sélectionnez l'interface en spécifiant le numéro de liste correspondant.
4. Spécifiez un nom de fichier de sortie et il disparaît.
5. Sélectionnez Contrôle-C pour arrêter la capture.

Le fichier enregistré est placé dans le dossier à partir duquel vous avez exécuté RawCap.exe :



rawcap_1.jpg

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.