Dépannage des captures de paquets et DNS dans le client d’itinérance Umbrella

Table des matières

Introduction

WireShark - Windows et MacOS prennent tous deux en charge la capture en mode bouclé

DNSQuerySniffer (Windows)

Introduction

Ce document décrit comment capturer des requêtes DNS sortantes. Le client d'itinérance Umbrella ne dispose pas actuellement d'une méthode pour capturer toutes les requêtes DNS sortantes qu'il effectue. Si vous avez besoin de capturer DNS, vous pouvez utiliser l'un de ces outils.

WireShark - Windows et MacOS prennent tous deux en charge la capture en mode bouclé

Wireshark vous permet de capturer les paquets envoyés à l’interface de bouclage locale (127.0.0.1), ce qui vous permet de voir les requêtes DNS envoyées au client d’itinérance Umbrella, qu’elles soient chiffrées ou non.

Capture sur toutes les interfaces réseau actives, en particulier lorsque la résolution DNS locale est un facteur

DNS uniquement

Si vous voulez seulement regarder les requêtes DNS.

DNS + HTTP

Si vous souhaitez uniquement examiner les requêtes DNS et HTTP.

Filtrer les recherches de débogage (sondes)

Si vous ne testez pas explicitement la recherche de problèmes liés aux sondes ou de problèmes avec debug.opendns.com, vous pouvez filtrer debug.opendns.com en tapant ceci dans la barre de filtre :

Pour plus d'informations sur l'exploitation de la puissance de Wireshark, consultez ces ressources :

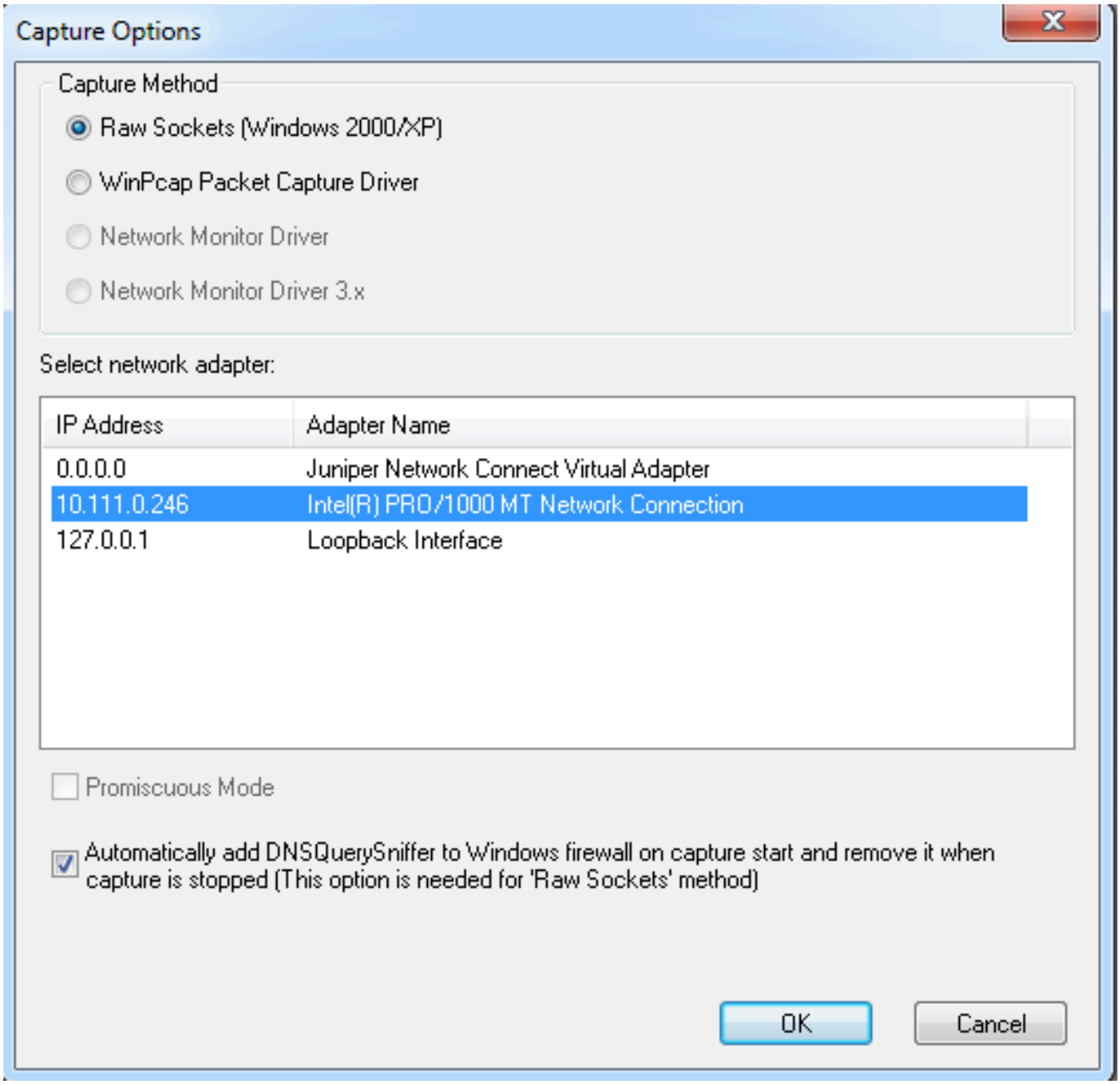
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

DNSQuery Sniffer est un analyseur de réseau uniquement DNS 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 des 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 principaux avantages de cette méthode est que vous pouvez renifler des paquets lorsque le service client d'itinérance Umbrella est désactivé, démarrer la capture et soudainement vous voyez chaque requête DNS que le client d'itinérance Umbrella envoie à partir du moment où il démarre, plutôt que de démarrer une capture après que le client d'itinérance Umbrella a déjà démarré.

Il existe deux méthodes de capture :

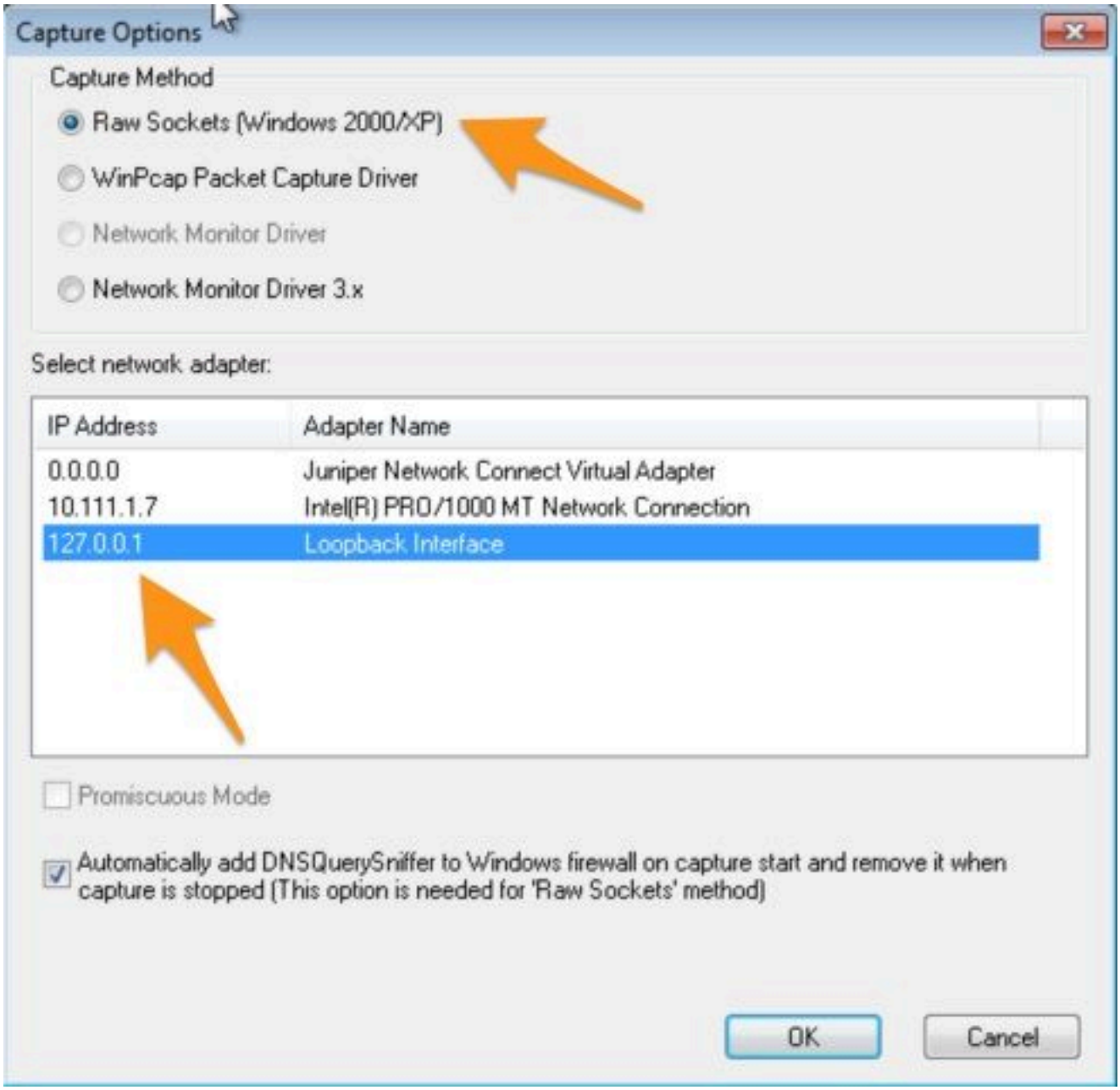
- Méthode 1 : si vous sélectionnez l'interface réseau normale, seules les requêtes qui figurent dans la liste Domaines internes ou qui n'ont pas transité spécifiquement par le dnscryptproxy sont affichées.



Ces colonnes apparaissent à l'extrême droite de la capture et vous devez faire défiler un peu.

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

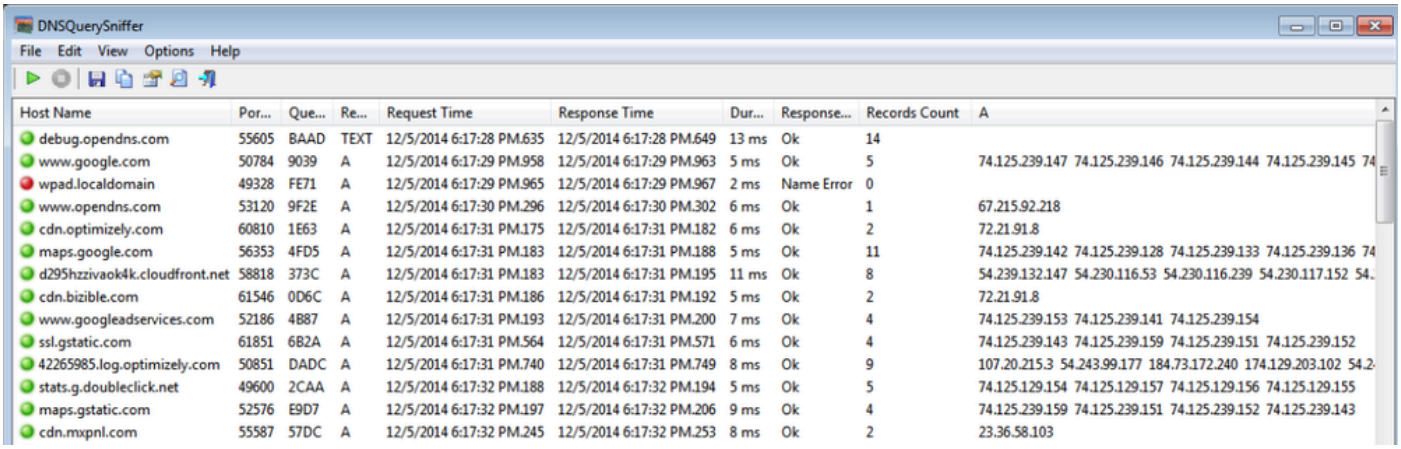
- Méthode 2 : si vous sélectionnez l'interface de bouclage, toutes les requêtes DNS envoyées via le serveur dnscryptproxy sont affichées, mais l'adresse IP de destination réelle pour les domaines de la liste Domaines internes n'est pas affichée ; toutefois, la requête et la réponse sont affichées.



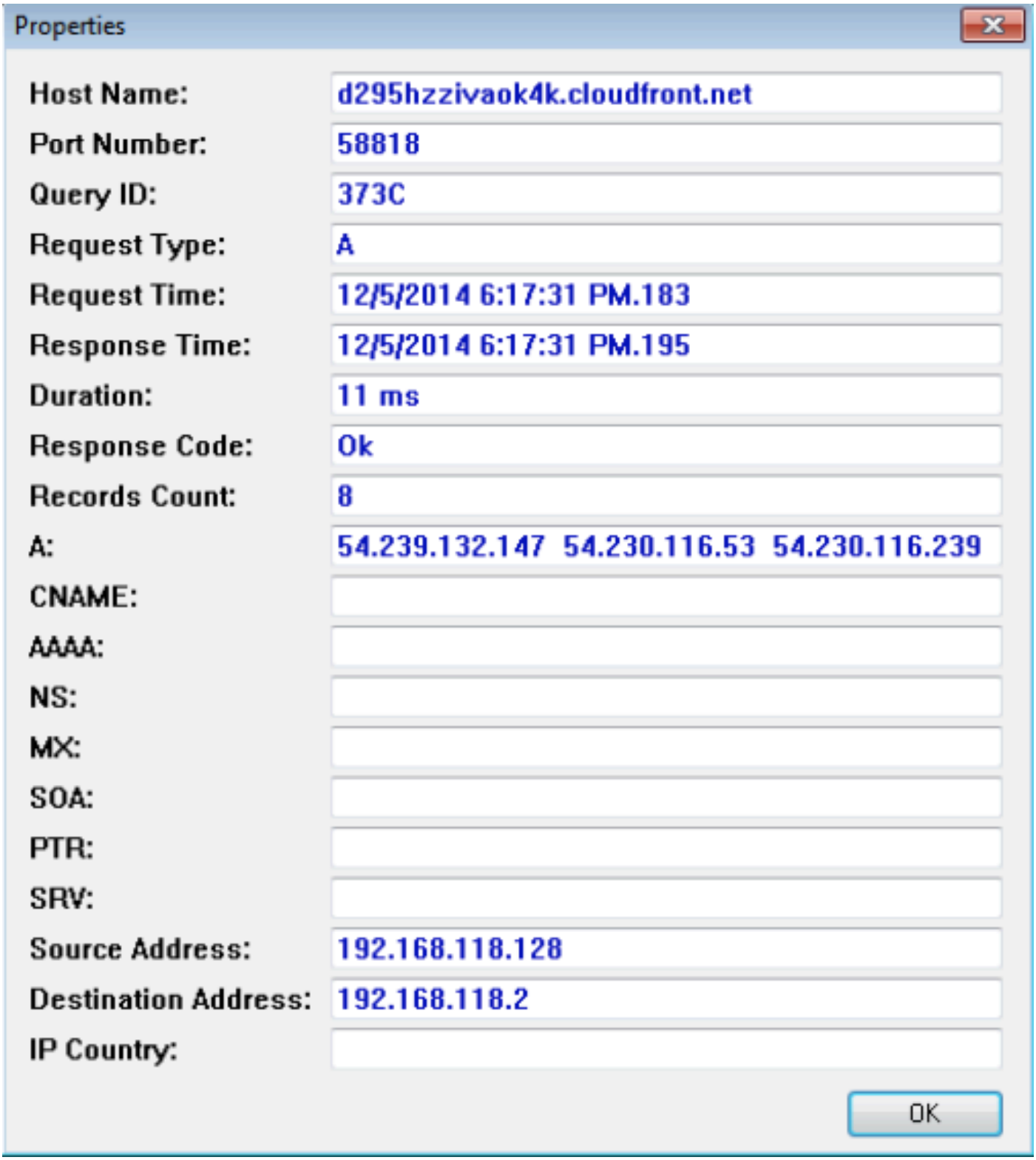
Ces colonnes apparaissent à l'extrême droite de la capture et vous devez faire défiler un peu.

Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

Les résultats sont les suivants :



Affichage d'une recherche individuelle :


Properties
Host Name:
d295hzzivaok4k.cloudfront.net
Port Number:
58818
Query ID:
373C
Request Type:
A
Request Time:
12/5/2014 6:17:31 PM.183
Response Time:
12/5/2014 6:17:31 PM.195
Duration:
11 ms
Response Code:
Ok
Records Count:
8
A:
54.239.132.147 54.230.116.53 54.230.116.239
CNAME:
AAAA:
NS:
MX:
SOA:
PTR:
SRV:
Source Address:
192.168.118.128
Destination Address:
192.168.118.2
IP Country:
OK

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.