Umbrella Roamingクライアントでのパケットおよびキャプチャのトラブルシューティング

内容

はじめに

このドキュメントでは、発信DNSクエリをキャプチャする方法について説明します。Umbrellaローミングクライアントには、現在、発信DNSクエリをすべてキャプチャする方法がありません。DNSをキャプチャする必要がある場合は、次のいずれかのツールを使用できます。

WireShark:WindowsとMacOSの両方がループバックキャプチャをサポート

Wiresharkでは、ローカルループバックインターフェイス(127.0.0.1)に送信されたパケットをキャプチャして、暗号化の有無にかかわらずUmbrellaローミングクライアントに送信されたDNS要求を確認できます。

特にローカルDNS解決が要因の場合は、すべてのアクティブなネットワークインターフェイスでキャプチャします。

DNSのみ

DNS要求のみを確認する場合。

DNS + HTTP

DNS要求とHTTP要求のみを確認する場合。

デバッグ参照（プローブ）をフィルタで除外する

プローブ関連の問題やdebug.opendns.comに関する問題のチェックを明示的にテストしていない場合は、フィルタバーに次のように入力してdebug.opendns.comをフィルタで除外できます。

Wiresharkの機能を活用する方法の詳細については、次のリソースを参照してください。

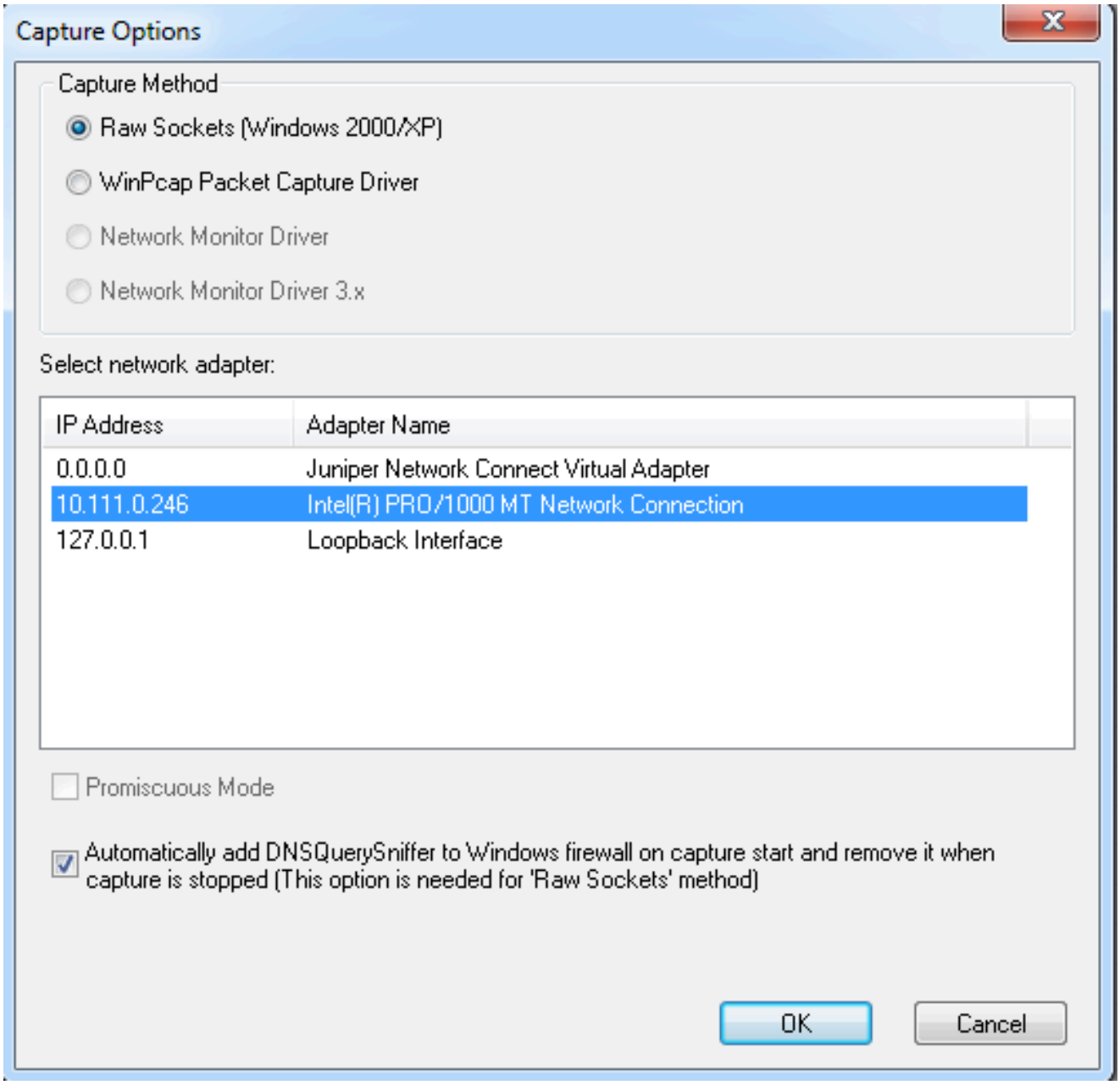
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer(Windows)

DNSQuery Snifferは、大量の有用なデータをモニタおよび表示する、Windows用のDNS専用ネットワークスニファです。WiresharkやRawcapとは異なり、DNSのみに使用され、関連情報の調査と抽出が非常に簡単です。ただし、Wiresharkの強力なフィルタリングツールはありません。
これは軽量で使いやすい道具です。この機能を使用する大きな利点は、Umbrellaローミングクライアントサービスが無効な状態でパケットを傍受し、キャプチャを開始すると、Umbrellaローミングクライアントがすでに開始した後にキャプチャを開始するのではなく、Umbrellaローミングクライアントが開始した時点から送信するすべてのDNSクエリが突然表示されることです。

次の2つのキャプチャ方法があります。

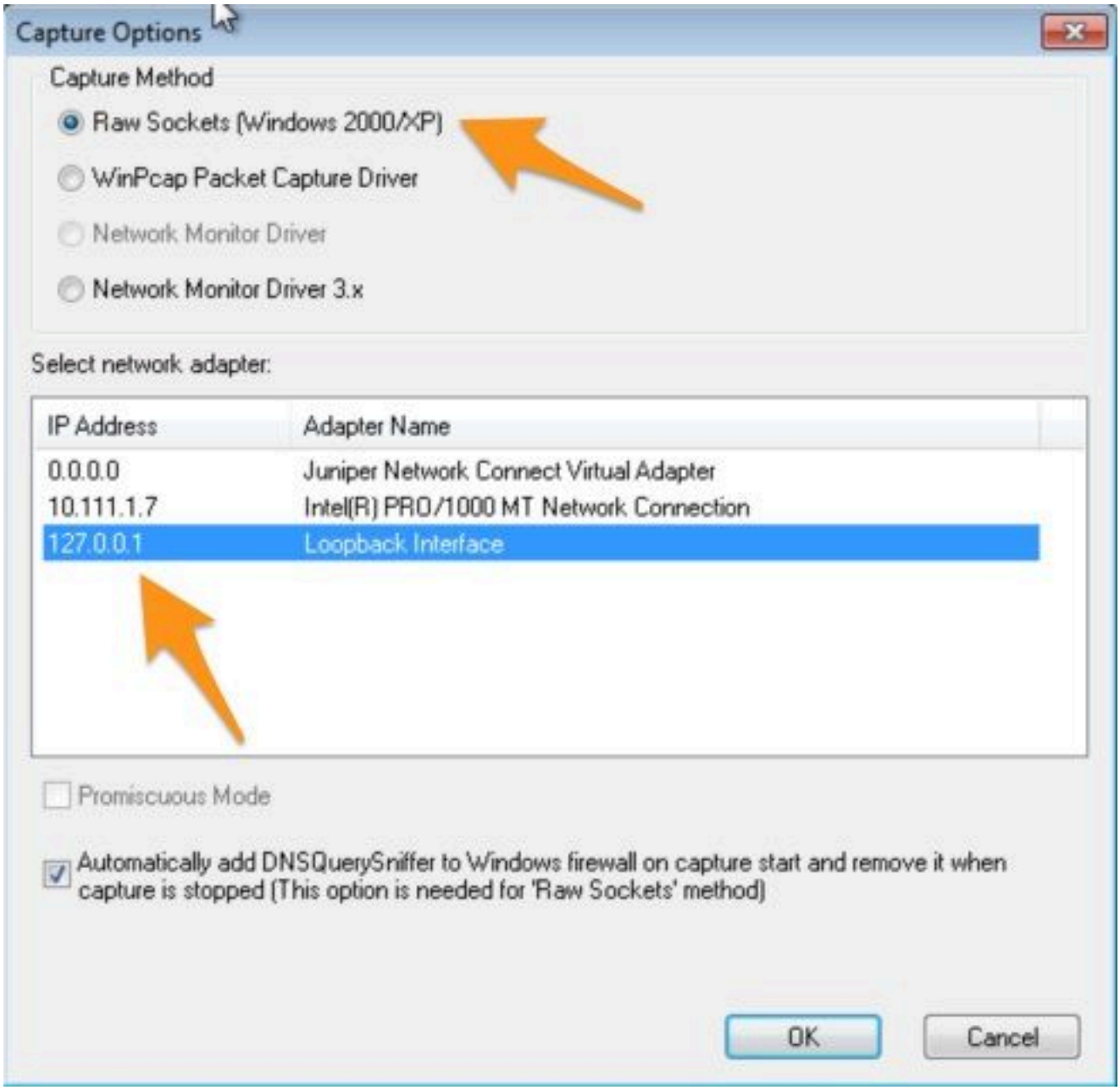
- 方法1：通常のネットワークインターフェイスを選択すると、「内部ドメイン」リストにあるクエリ、または特にdnscryptproxyを通過しなかったクエリだけが表示されます。



これらの列はキャプチャの右端に表示され、かなりスクロールする必要があります。

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

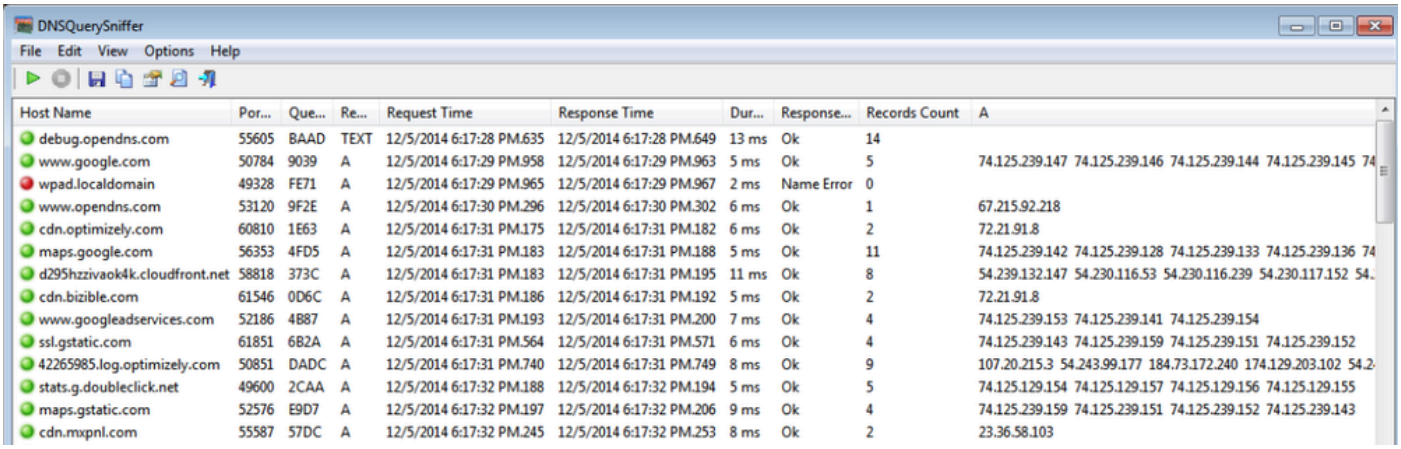
- 方法2：ループバックインターフェイスを選択すると、dnscryptproxyを介して送信されたすべてのDNSクエリーは表示されますが、内部ドメインリストのドメインの実際の宛先IPアドレスは表示されません。ただし、クエリーと応答は表示されます。



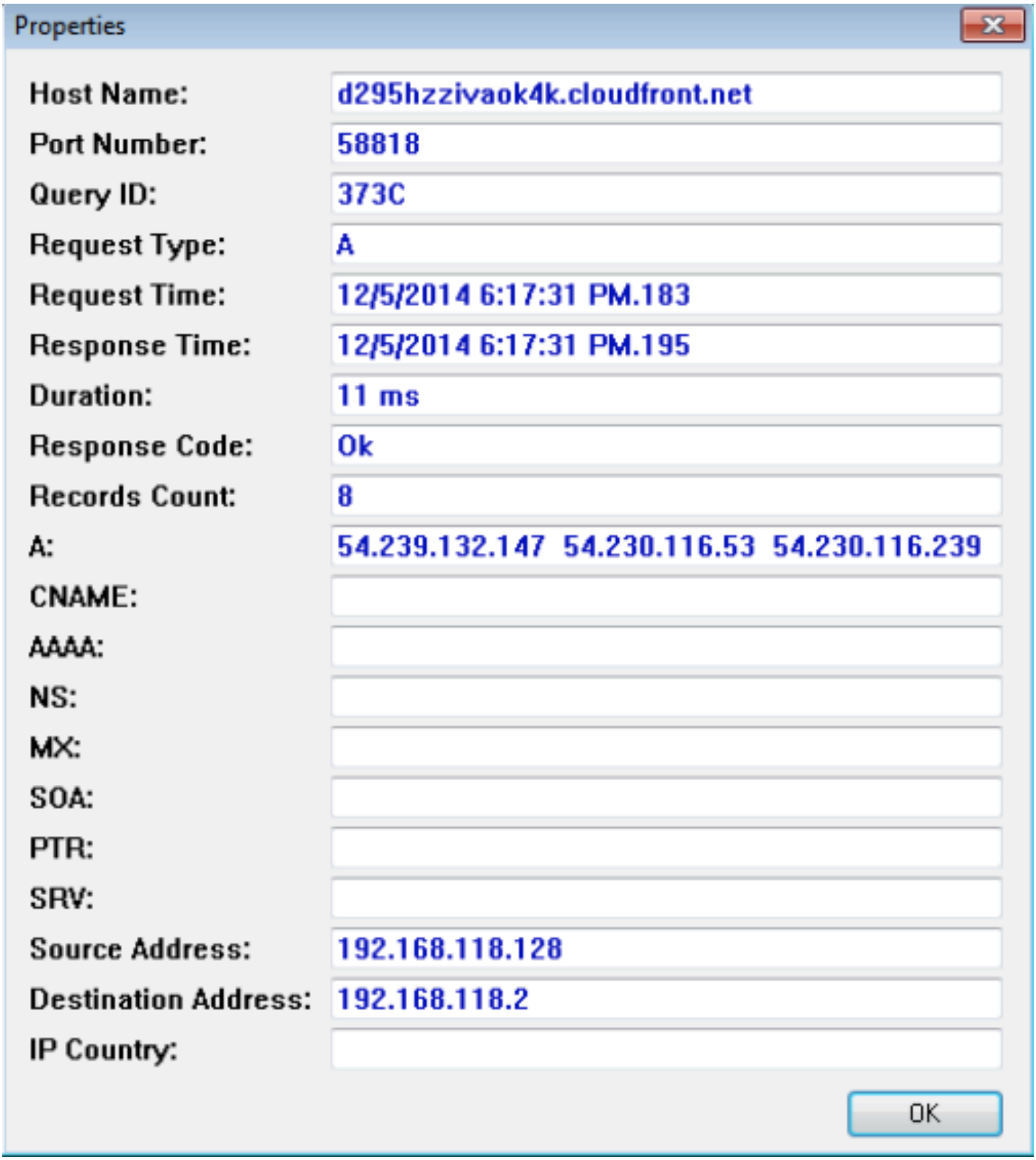
これらの列はキャプチャの右端に表示され、かなりスクロールする必要があります。

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

結果は次のようになります。



個々のルックアップのビュー：


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。