

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

## 内容

---

[はじめに](#)

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

[DNSQuerySniffer\(Windows\)](#)

---

## 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。



Filter:

Development Version  
**WIRESHARK**

The World's Most  
Version 1.9.2 (SVN Rev

## Capture

### Interface List



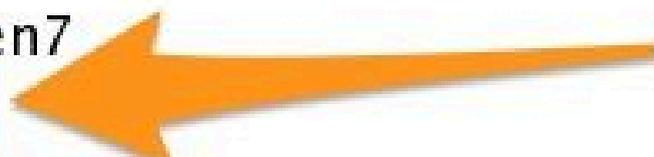
Live list of the capture interfaces  
(counts incoming packets)



### Start

Choose one or more interfaces to capture from, then **Start**

- Thunderbolt Bridge: bridge0
- utun0
- p2p0
- Thunderbolt 1: en6
- Thunderbolt 2: en7
- Loopback: lo0



DNSのみ

DNS要求のみを確認する場合。

Filter: dns

DNS + HTTP

DNS要求とHTTP要求のみを確認する場合。

Filter: dns or http

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。

Filter: dns && not dns contains debug.opendns.com

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。

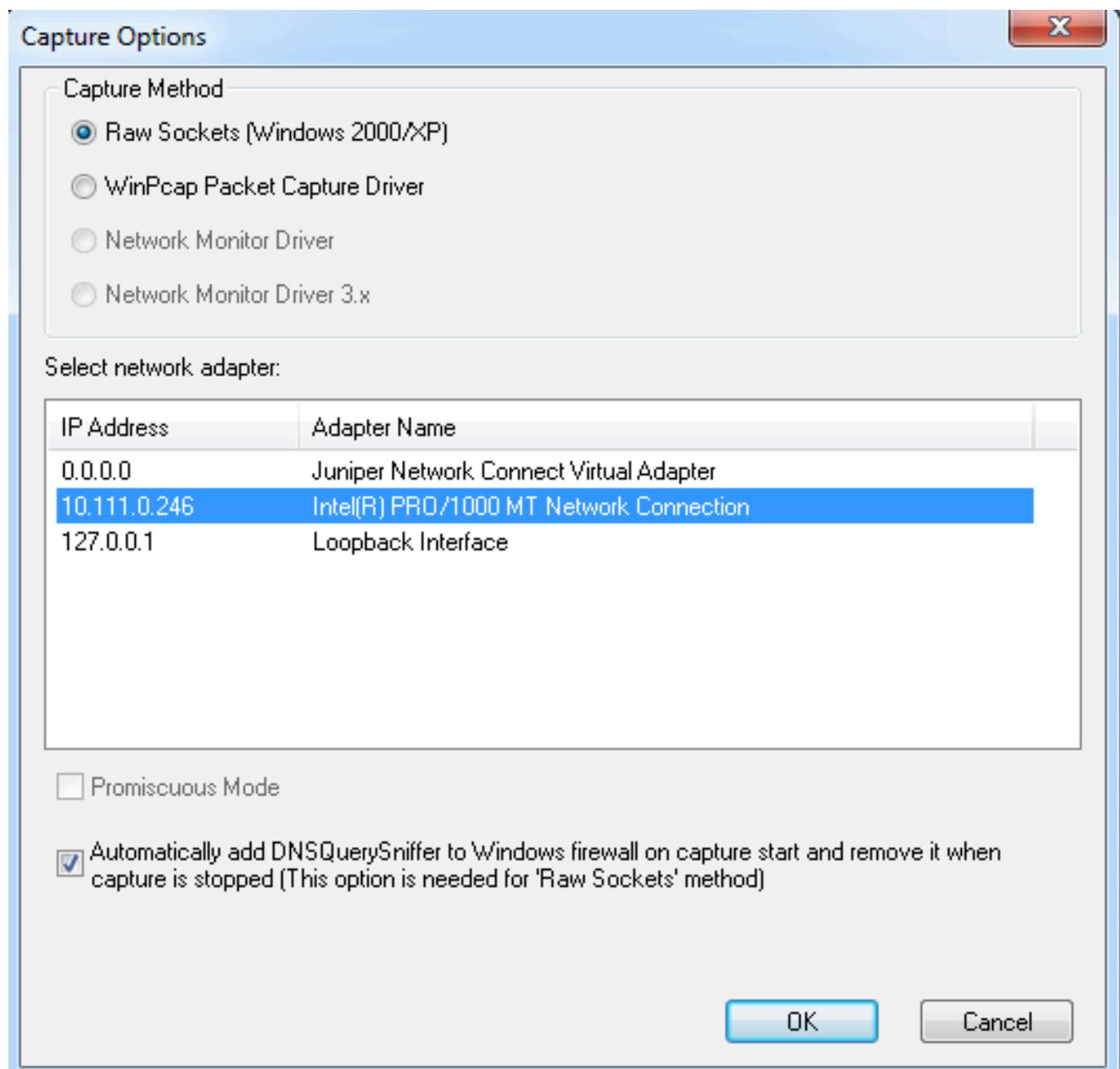
- [http://packetlife.net/media/library/13/Wireshark\\_Display\\_Filters.pdf](http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf)
- <http://wiki.wireshark.org/DisplayFilters>

## 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。

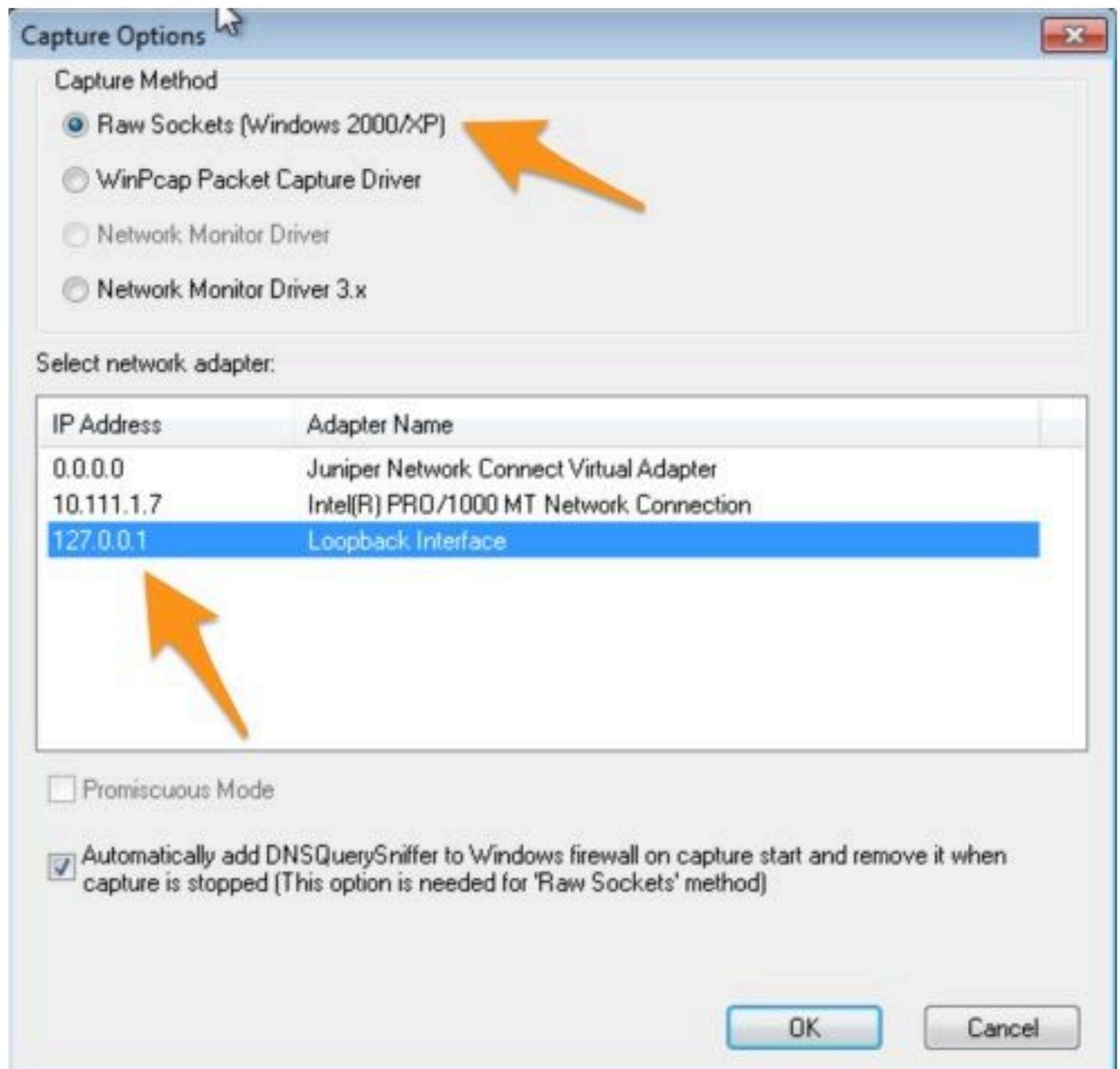
次の2つのキャプチャ方法があります。

- 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。





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
127.0.0.1	127.0.0.1

結果は次のようになります。

Host Name	Port	Queue	Request	Request Time	Response Time	Duration	Response	Records Count	A
debug.opendns.com	55605	BAAD	TEXT	12/5/2014 6:17:28 PM.635	12/5/2014 6:17:28 PM.649	13 ms	Ok	14	
www.google.com	50784	9039	A	12/5/2014 6:17:29 PM.958	12/5/2014 6:17:29 PM.963	5 ms	Ok	5	74.125.239.147 74.125.239.146 74.125.239.144 74.125.239.145 74.125.239.143
wpad.localdomain	49328	FE71	A	12/5/2014 6:17:29 PM.965	12/5/2014 6:17:29 PM.967	2 ms	Name Error	0	
www.opendns.com	53120	9F2E	A	12/5/2014 6:17:30 PM.296	12/5/2014 6:17:30 PM.302	6 ms	Ok	1	67.215.92.218
cdn.optimizely.com	60810	1E63	A	12/5/2014 6:17:31 PM.175	12/5/2014 6:17:31 PM.182	6 ms	Ok	2	72.21.91.8
maps.google.com	56353	4FD5	A	12/5/2014 6:17:31 PM.183	12/5/2014 6:17:31 PM.188	5 ms	Ok	11	74.125.239.142 74.125.239.128 74.125.239.133 74.125.239.136 74.125.239.144 74.125.239.143 74.125.239.145 74.125.239.146 74.125.239.147 74.125.239.148
d295hzzivaok4k.cloudfront.net	58818	373C	A	12/5/2014 6:17:31 PM.183	12/5/2014 6:17:31 PM.195	11 ms	Ok	8	54.239.132.147 54.230.116.53 54.230.116.239 54.230.117.152 54.230.117.151 54.230.117.150 54.230.117.149 54.230.117.148
cdn.bizible.com	61546	0D6C	A	12/5/2014 6:17:31 PM.186	12/5/2014 6:17:31 PM.192	5 ms	Ok	2	72.21.91.8
www.googleadservices.com	52186	4887	A	12/5/2014 6:17:31 PM.193	12/5/2014 6:17:31 PM.200	7 ms	Ok	4	74.125.239.153 74.125.239.141 74.125.239.154
ssl.gstatic.com	61851	6B2A	A	12/5/2014 6:17:31 PM.564	12/5/2014 6:17:31 PM.571	6 ms	Ok	4	74.125.239.143 74.125.239.159 74.125.239.151 74.125.239.152
42265985.log.optimizely.com	50851	DADC	A	12/5/2014 6:17:31 PM.740	12/5/2014 6:17:31 PM.749	8 ms	Ok	9	107.20.215.3 54.243.99.177 184.73.172.240 174.129.203.102 54.243.99.178 54.243.99.179 54.243.99.180 54.243.99.181 54.243.99.182
stats.g.doubleclick.net	49600	2CAA	A	12/5/2014 6:17:32 PM.188	12/5/2014 6:17:32 PM.194	5 ms	Ok	5	74.125.129.154 74.125.129.157 74.125.129.156 74.125.129.155
maps.gstatic.com	52576	E9D7	A	12/5/2014 6:17:32 PM.197	12/5/2014 6:17:32 PM.206	9 ms	Ok	4	74.125.239.159 74.125.239.151 74.125.239.152 74.125.239.143
cdn.mxpnl.com	55587	57DC	A	12/5/2014 6:17:32 PM.245	12/5/2014 6:17:32 PM.253	8 ms	Ok	2	23.36.58.103

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。