Troubleshoot Packet and DNS Captures in Umbrella Roaming Client

Contents

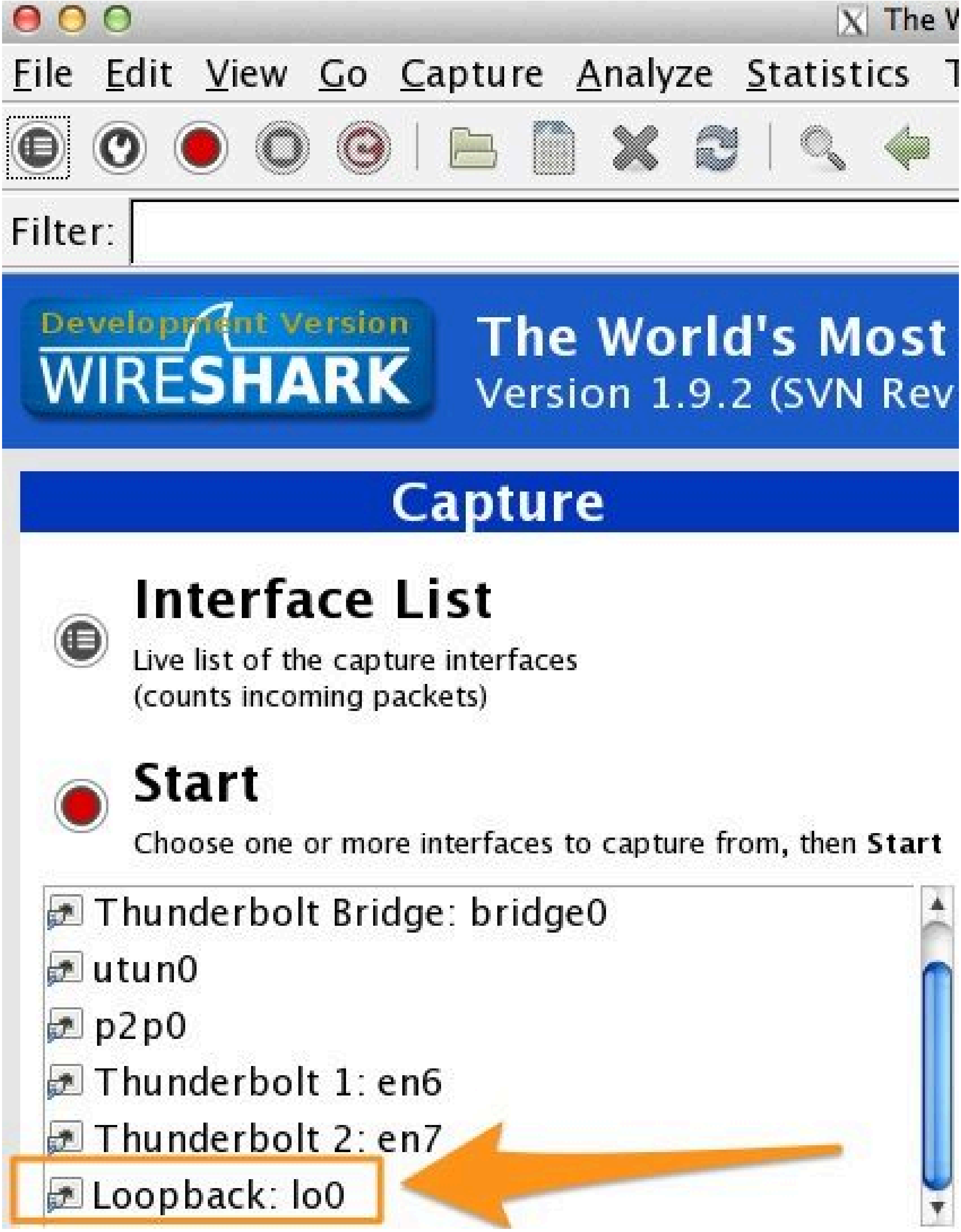
Introduction

This document describes how to capture outbound DNS queries. The Umbrella roaming client doesn’t currently have a method for capturing all the outbound DNS queries it makes. If you need to capture DNS, you can use one of these tools.

WireShark - Windows and MacOS both support loopback capture

Wireshark allows you to capture packets sent to the local loopback interface (127.0.0.1), therefor allowing you to see DNS requests sent to the Umbrella roaming client whether encrypted or unencrypted.

Capture on all active network interfaces especially when local DNS resolution is a factor



File Edit View Go Capture Analyze Statistics

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

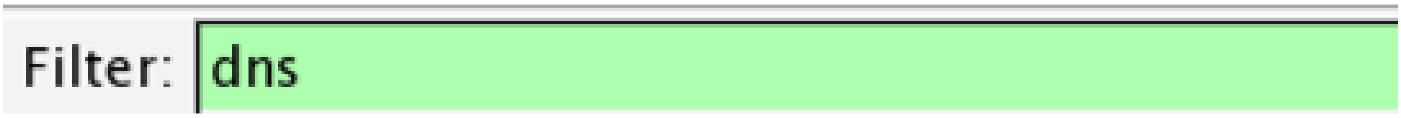
Thunderbolt 1: en6

Thunderbolt 2: en7

Loopback: lo0

DNS Only

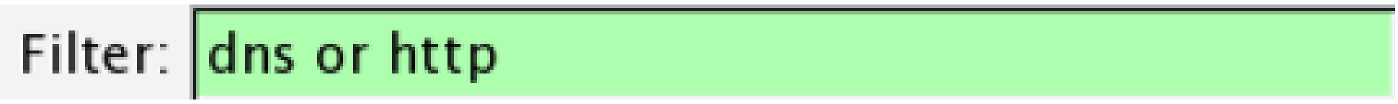
If you only want to look at DNS requests.



Filter: dns

DNS + HTTP

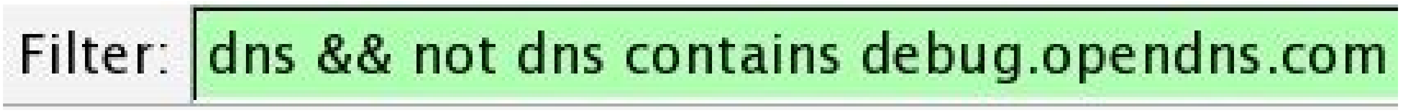
If you only want to look at DNS and HTTP request.



Filter: dns or http

Filter out debug lookups (probes)

If you are not explicitly testing checking for probe-related issues or issues with debug.opendns.com, you can filter out debug.opendns.com by typing this in the filter bar:



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

For more information about harnessing the power of Wireshark, see these resources:

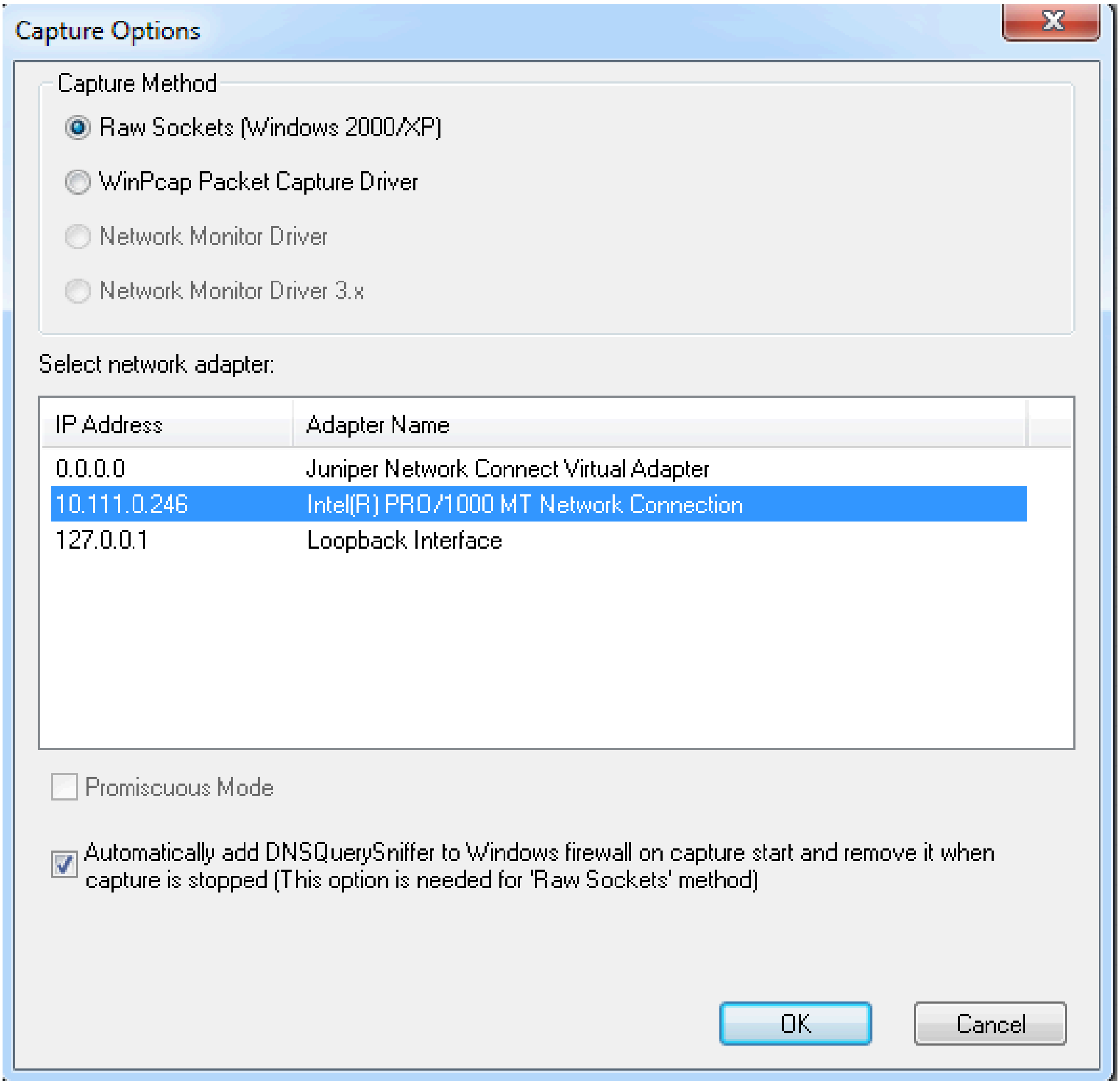
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

DNSQuery Sniffer is a DNS-only network sniffer for Windows which monitors and displays tons of useful data. Unlike Wireshark or Rawcap, it’s only used for DNS, and is much easier to examine and extract relevant information. However, it does not have the powerful filtering tools of Wireshark.
This is a lightweight and easy-to-use tool. A huge advantage to using this is that you can sniff packets while the Umbrella roaming client service is disabled, start the capture, and suddenly you are seeing every DNS query that the Umbrella roaming client sends from the moment it starts, rather than starting a capture after the Umbrella roaming client has already started.

There are two capture methods:

- **Method One**—If you select the regular network interface, only queries that are on the Internal Domains list or that did not specifically go through the dnscryptproxy are shown.



Capture Options

Capture Method

● Raw Sockets (Windows 2000/XP)

○ WinPcap Packet Capture Driver

○ Network Monitor Driver

○ Network Monitor Driver 3.x

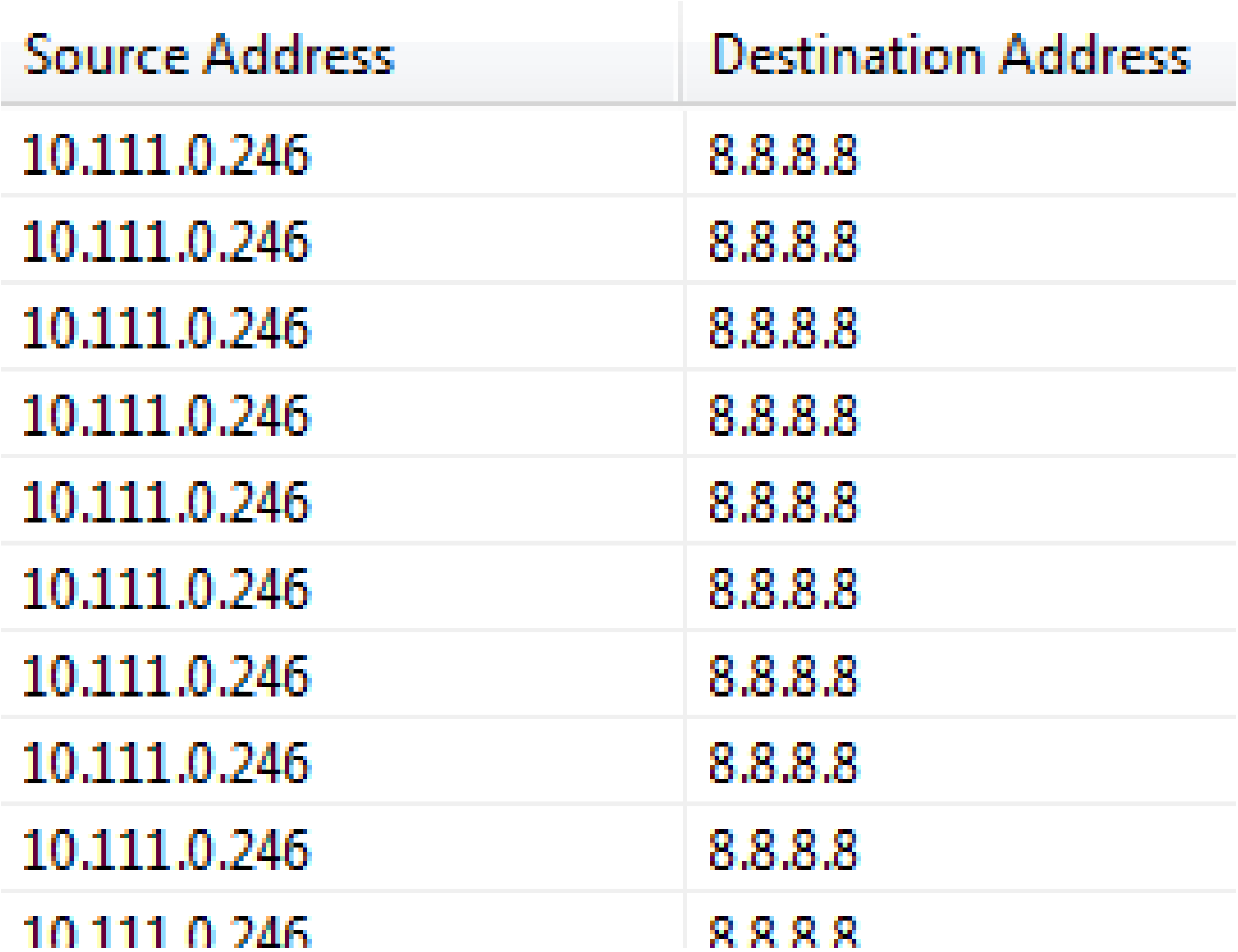
Select network adapter:

IP Address	Adapter Name
0.0.0.0	Juniper Network Connect Virtual Adapter
10.111.0.246	Intel(R) PRO/1000 MT Network Connection
127.0.0.1	Loopback Interface

□ Promiscuous Mode

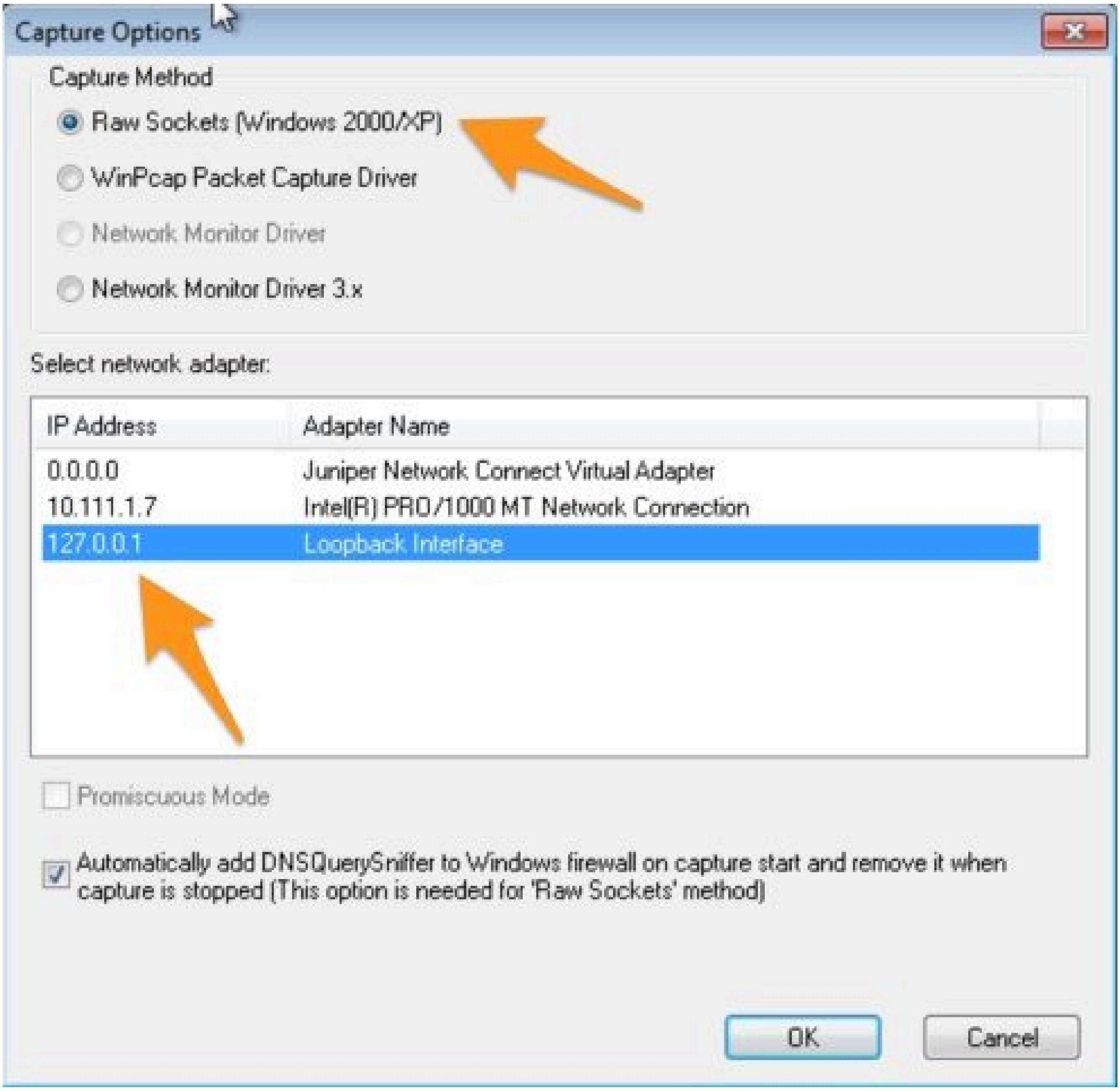
☑ Automatically add DNSQuerySniffer to Windows firewall on capture start and remove it when capture is stopped (This option is needed for 'Raw Sockets' method)

These columns appear on the far right in the capture and you have to scroll over quite a bit.



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

- **Method Two**—If you select the Loopback interface, all DNS queries that are sent through the dnscryptproxy are shown, but the true destination IP address for domains on the Internal Domains list are not shown; however, the query and answer are displayed.


Capture Options

Capture Method

● Raw Sockets (Windows 2000/XP)

○ WinPcap Packet Capture Driver

○ Network Monitor Driver

○ Network Monitor Driver 3.x

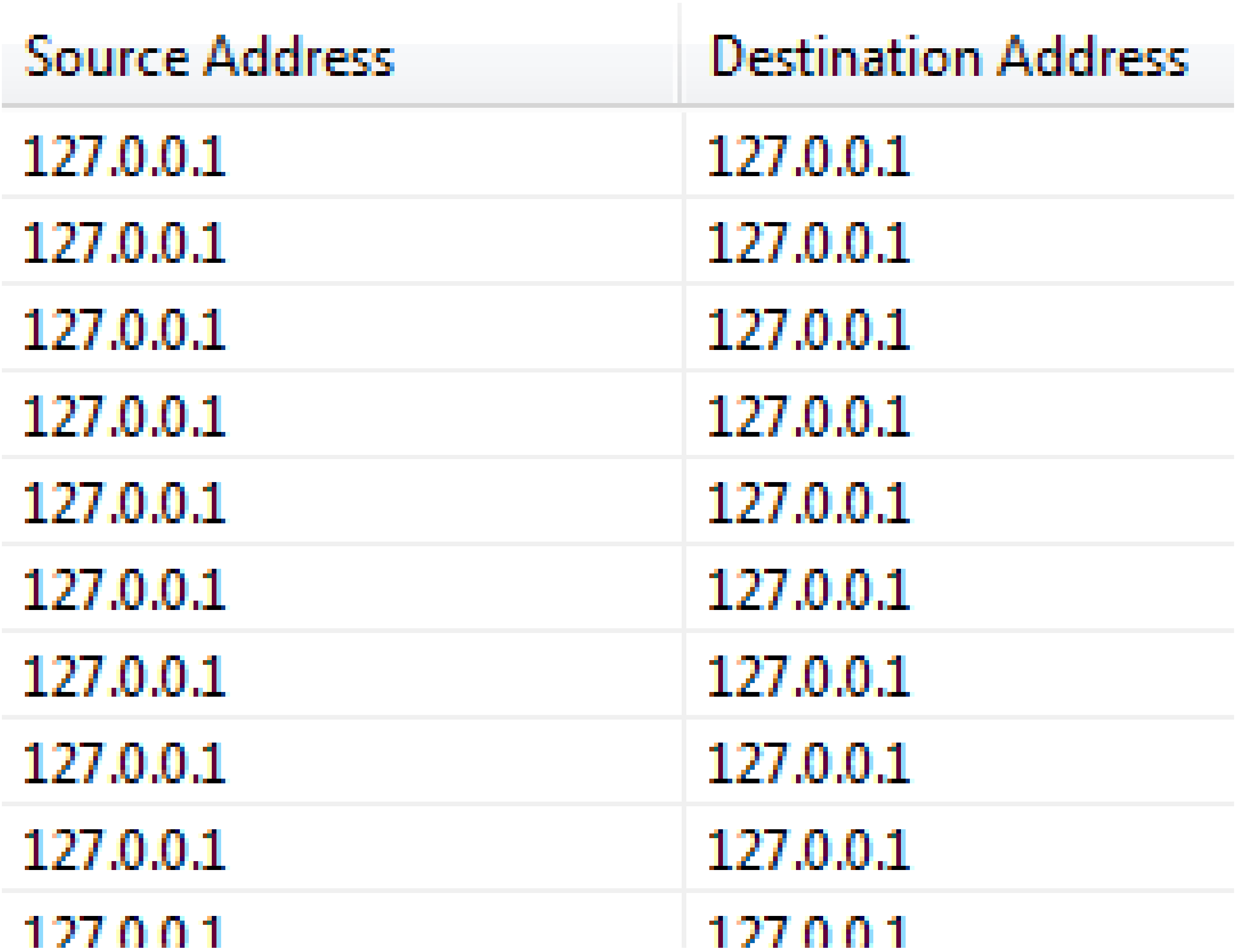
Select network adapter:

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

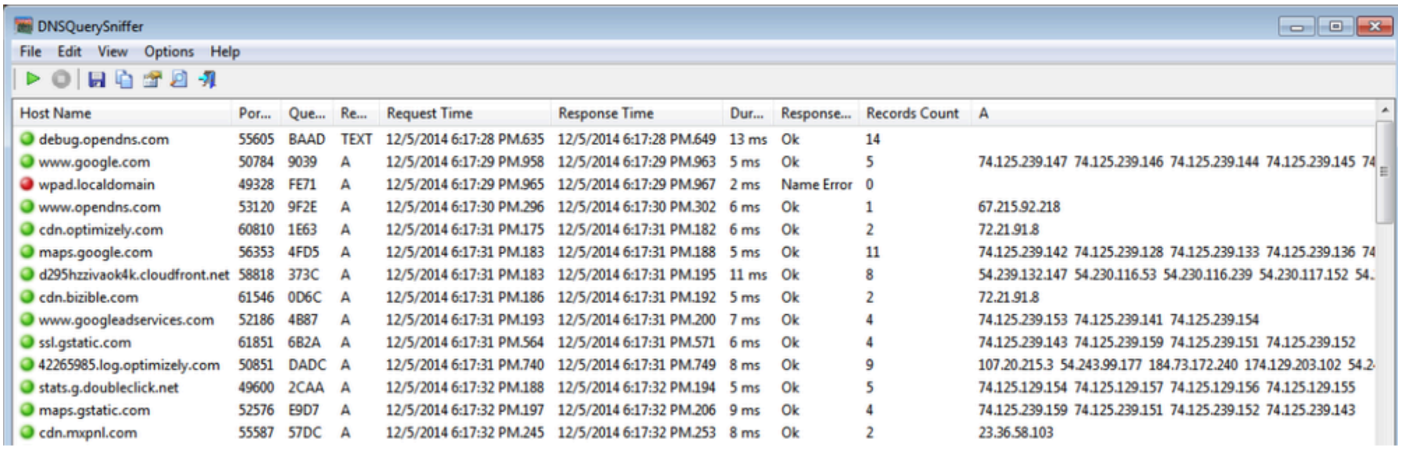
☑ Automatically add DNSQuerySniffer to Windows firewall on capture start and remove it when capture is stopped (This option is needed for 'Raw Sockets' method)

These columns appear on the far right in the capture and you have to scroll over quite a bit.



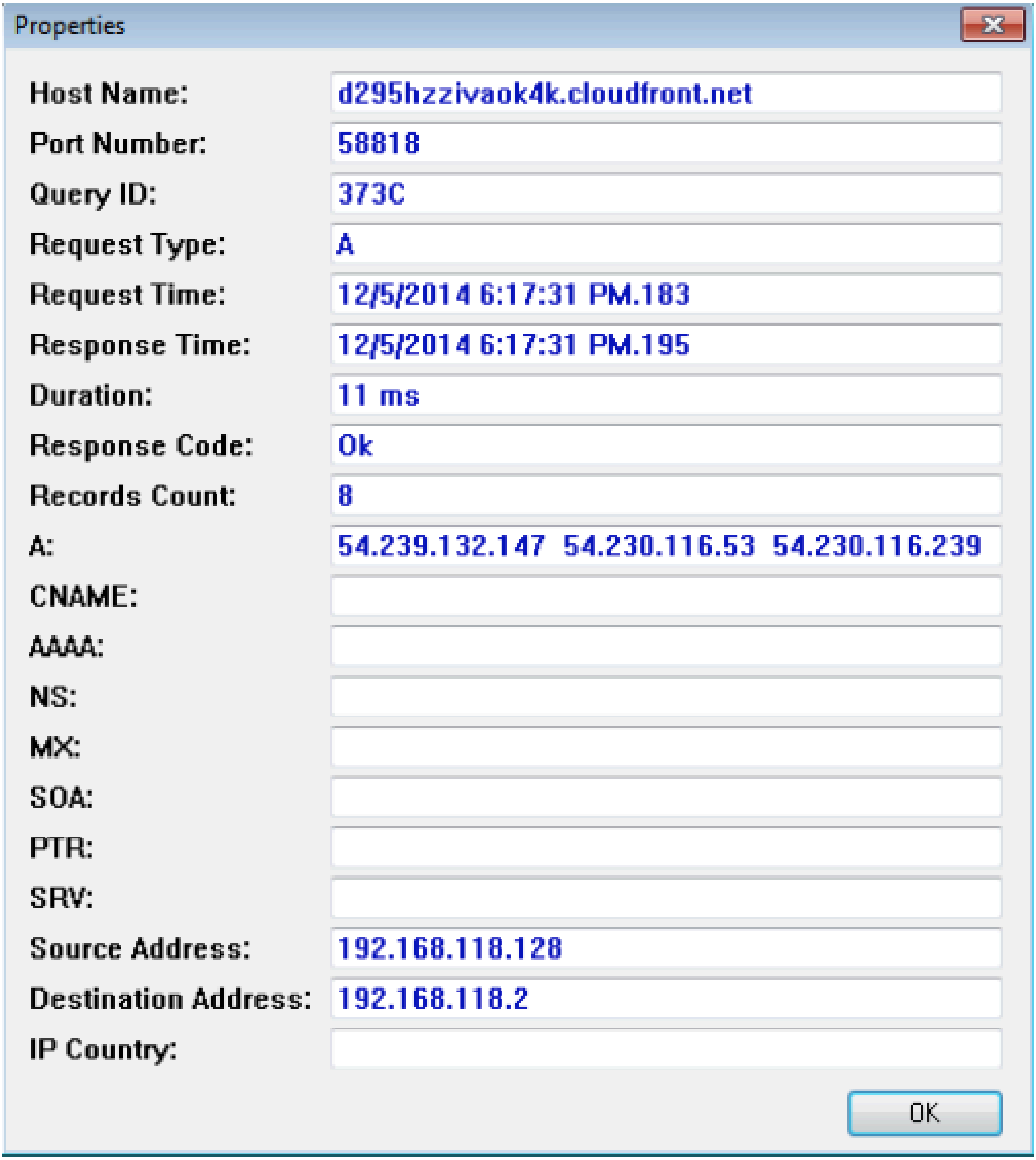
Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

The results look like this:



Host Name	Por...	Que...	Re...	Request Time	Response Time	Dur...	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
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
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.
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	4B87	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 54.2
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

View of an individual lookup:



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:	