排除Umbrella漫游客户端中的数据包和DNS捕获故障

目录

简介

本文档介绍如何捕获出站DNS查询。Umbrella漫游客户端当前没有捕获其执行的所有出站DNS查询的方法。如果需要捕获DNS，可以使用以下工具之一。

WireShark - Windows和MacOS都支持环回捕获

Wireshark允许您捕获发送到本地环回接口(127.0.0.1)的数据包，因此，您可以查看发送到Umbrella漫游客户端的DNS请求，无论加密还是未加密。

在所有活动网络接口上捕获，尤其是当本地DNS解析是一个因素时

仅DNS

如果您只想查看DNS请求。

DNS + HTTP

如果只想查看DNS和HTTP请求。

过滤出调试查找（探测器）

如果您没有使用debug.opendns.com显式测试检查探测相关问题或问题，则可以通过在过滤栏中键入以下内容来过滤debug.opendns.com:

有关利用Wireshark功能的详细信息，请参阅以下资源：

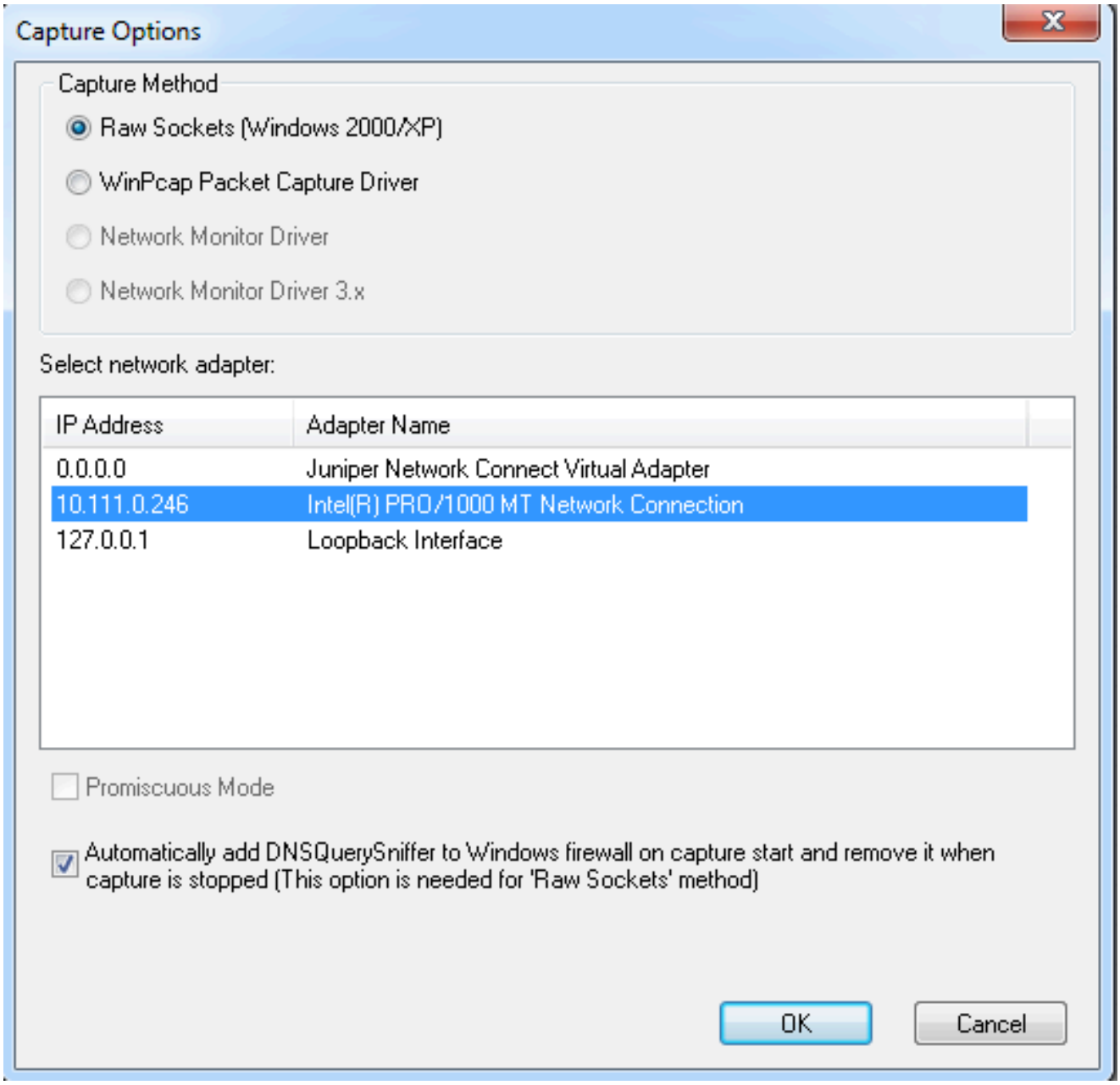
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer(Windows)

DNSQuery Sniffer是Windows的仅DNS网络嗅探器，用于监控和显示大量有用数据。与Wireshark或Rawcap不同，它仅用于DNS，并且更容易检查和提取相关信息。但是，它没有Wireshark的强大过滤工具。
这是一个轻巧且易于使用的工具。使用此功能的一个巨大优势是，您可以在Umbrella漫游客户端服务禁用时嗅探数据包，开始捕获，然后突然看到Umbrella漫游客户端从启动时发出的每个DNS查询，而不是在Umbrella漫游客户端已启动后开始捕获。

有两种捕获方法：

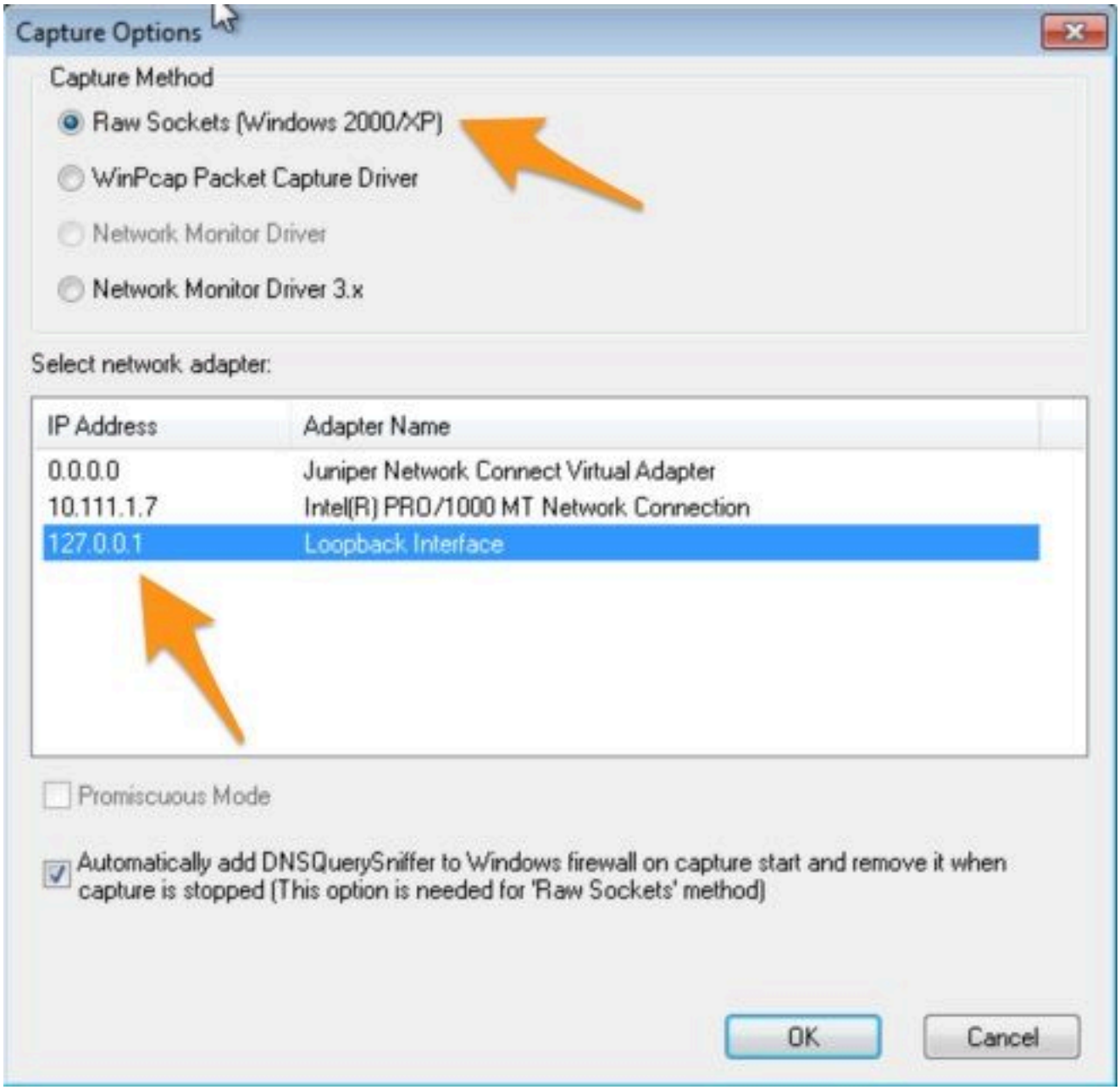
- 方法一 — 如果选择常规网络接口，则仅显示位于内部域列表上或未专门通过dnscryptproxy的查询。



这些列显示在捕获的最右侧，您必须滚动相当多的地方。

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

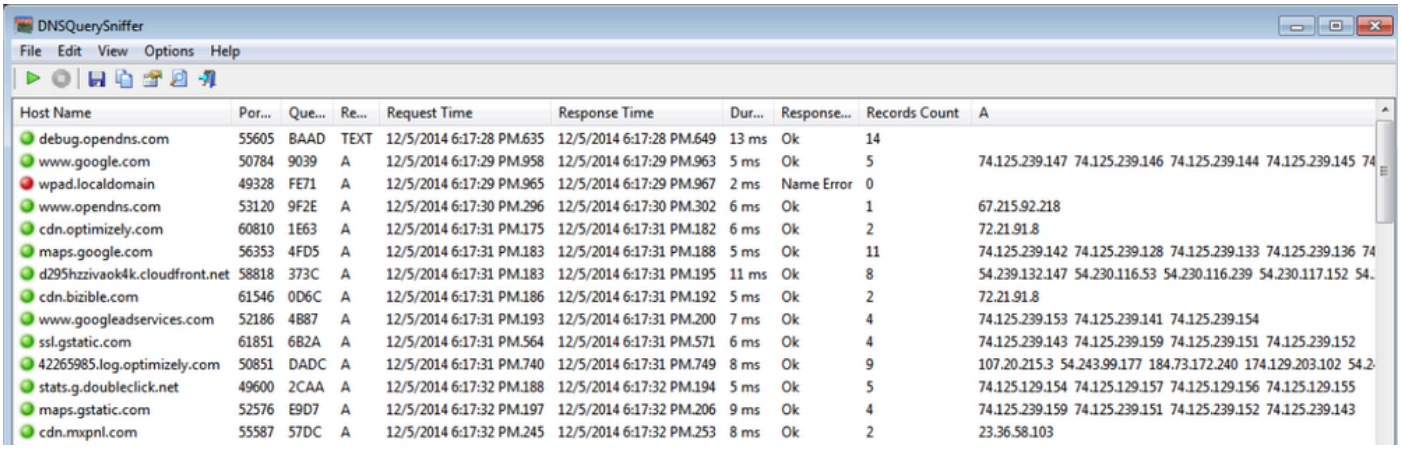
- 方法二 — 如果选择环回接口，则显示通过dnscryptproxy发送的所有DNS查询，但不显示Internal Domains列表中域的实际目标IP地址；但是，会显示查询和答案。



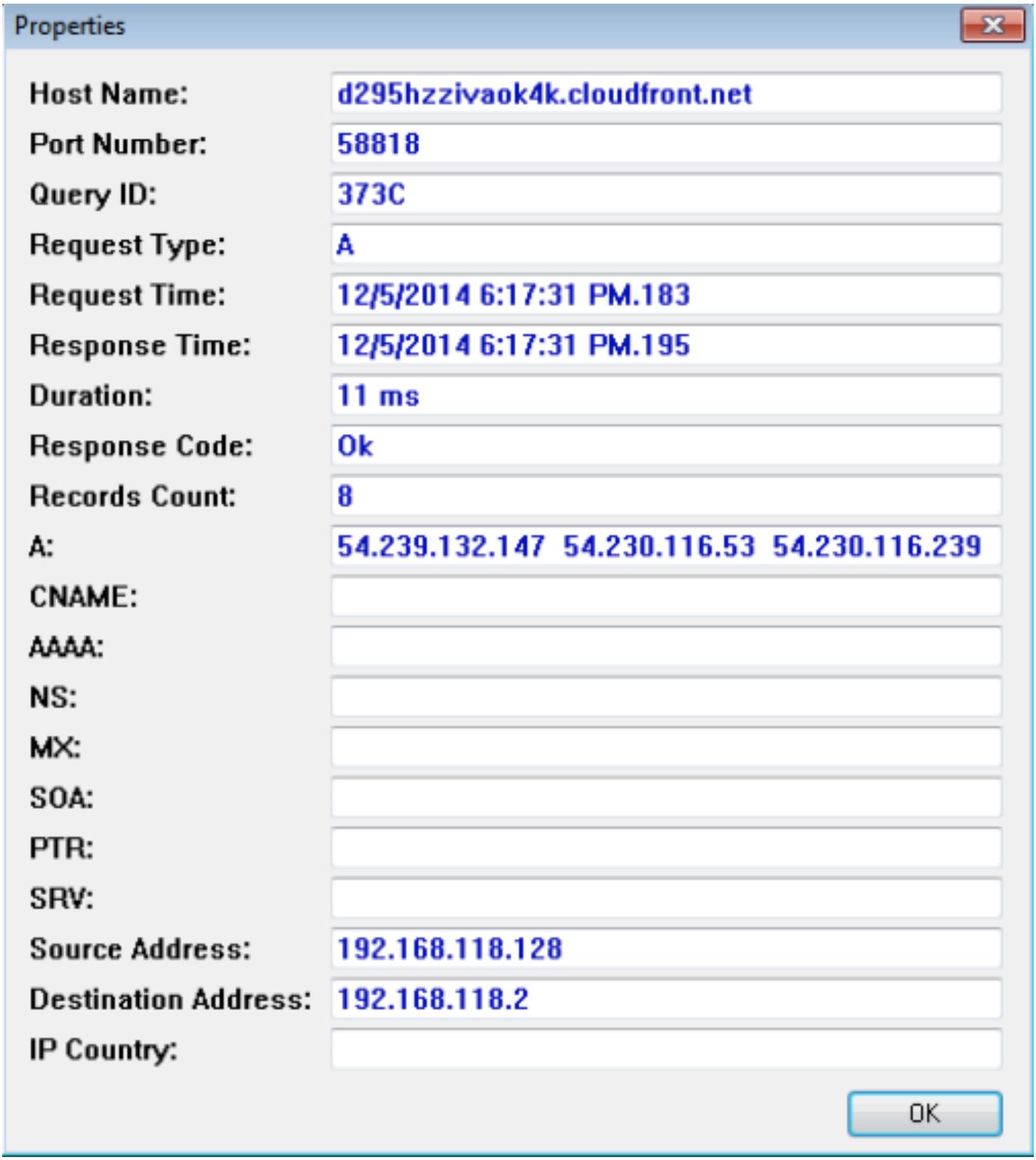
这些列显示在捕获的最右侧，您必须滚动相当多的地方。

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

结果如下：



单个查找的视图：


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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。