對Umbrella漫遊客戶端中的資料包和DNS捕獲進行故障排除

目錄

[簡介](#)

[WireShark - Windows和MacOS都支援環回捕獲](#)

[DNSQuerySniffer(Windows)](#)

簡介

本文說明如何捕獲出站DNS查詢。Umbrella漫遊客戶端當前沒有捕獲其執行的所有出站DNS查詢的方法。如果需要捕獲DNS，可以使用以下工具之一。

WireShark - Windows和MacOS都支援環回捕獲

Wireshark允許您捕獲傳送到本地環回介面(127.0.0.1)的資料包，因此允許您檢視傳送到Umbrella漫遊客戶端的DNS請求（無論加密或未加密）。

在所有活動網路介面上捕獲，尤其是當本地DNS解析是一個因素時

僅限DNS

如果您只想檢視DNS請求。

DNS + HTTP

如果您只想檢視DNS和HTTP請求，

過濾出調試查詢（探測）

如果您沒有使用debug.opendns.com顯式測試檢查與探測器相關的問題，則可以在過濾欄中鍵入以下內容來過濾debug.opendns.com:

有關利用Wireshark功能的詳細資訊，請參閱以下資源：

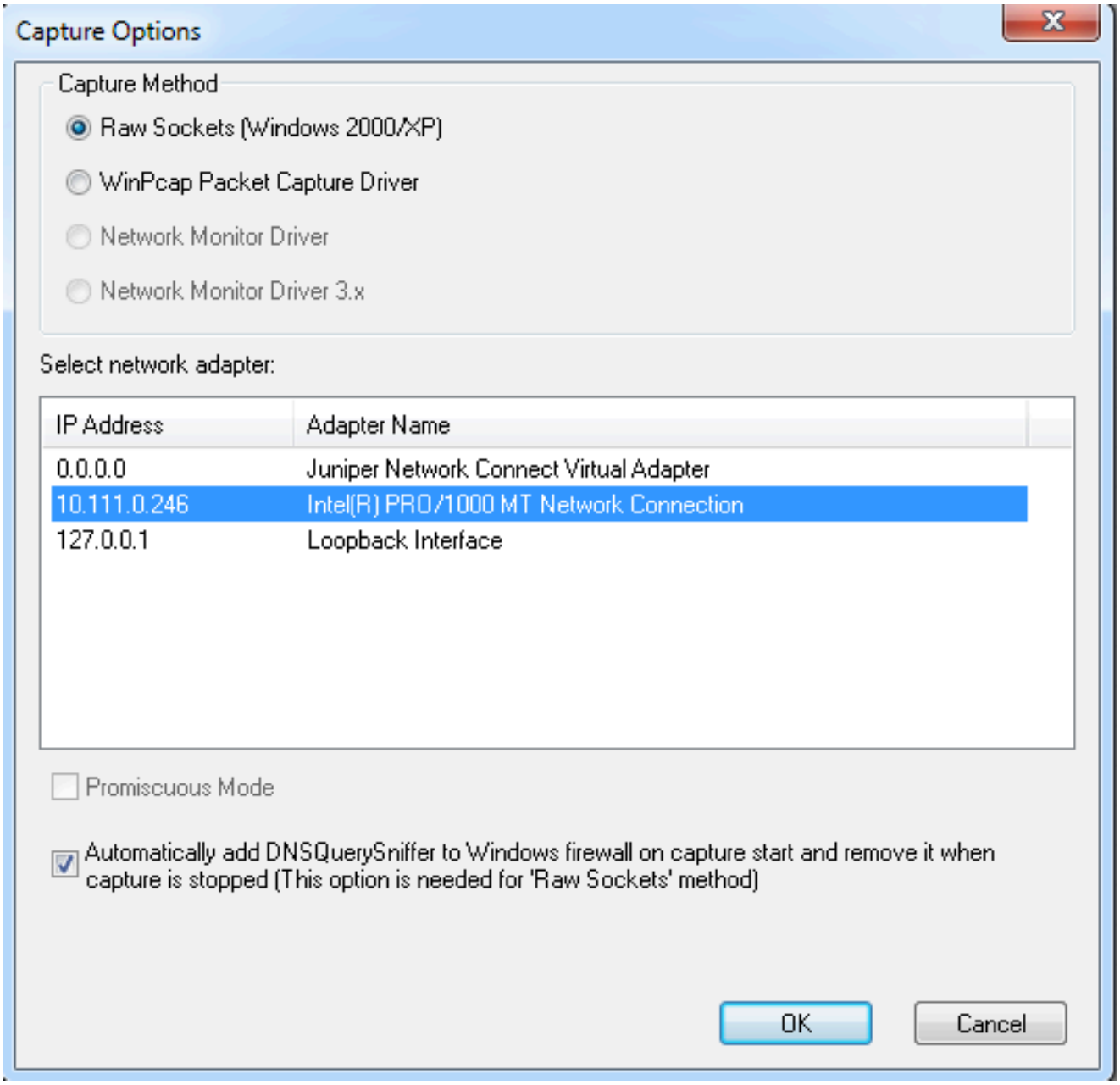
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer(Windows)

DNSQuery嗅探器是用於Windows的僅DNS網路嗅探器，用於監控和顯示大量有用資料。與Wireshark或Rawcap不同，它僅用於DNS，並且更容易檢查和提取相關資訊。但是，它沒有強大的Wireshark過濾工具。
這是一個輕便且易於使用的工具。使用這種方法的巨大優勢是，您可以在Umbrella漫遊客戶端服務禁用時嗅探資料包，開始捕獲，突然您會看到Umbrella漫遊客戶端從啟動時發出的每個DNS查詢，而不是在Umbrella漫遊客戶端已啟動後開始捕獲。

有兩種捕獲方法：

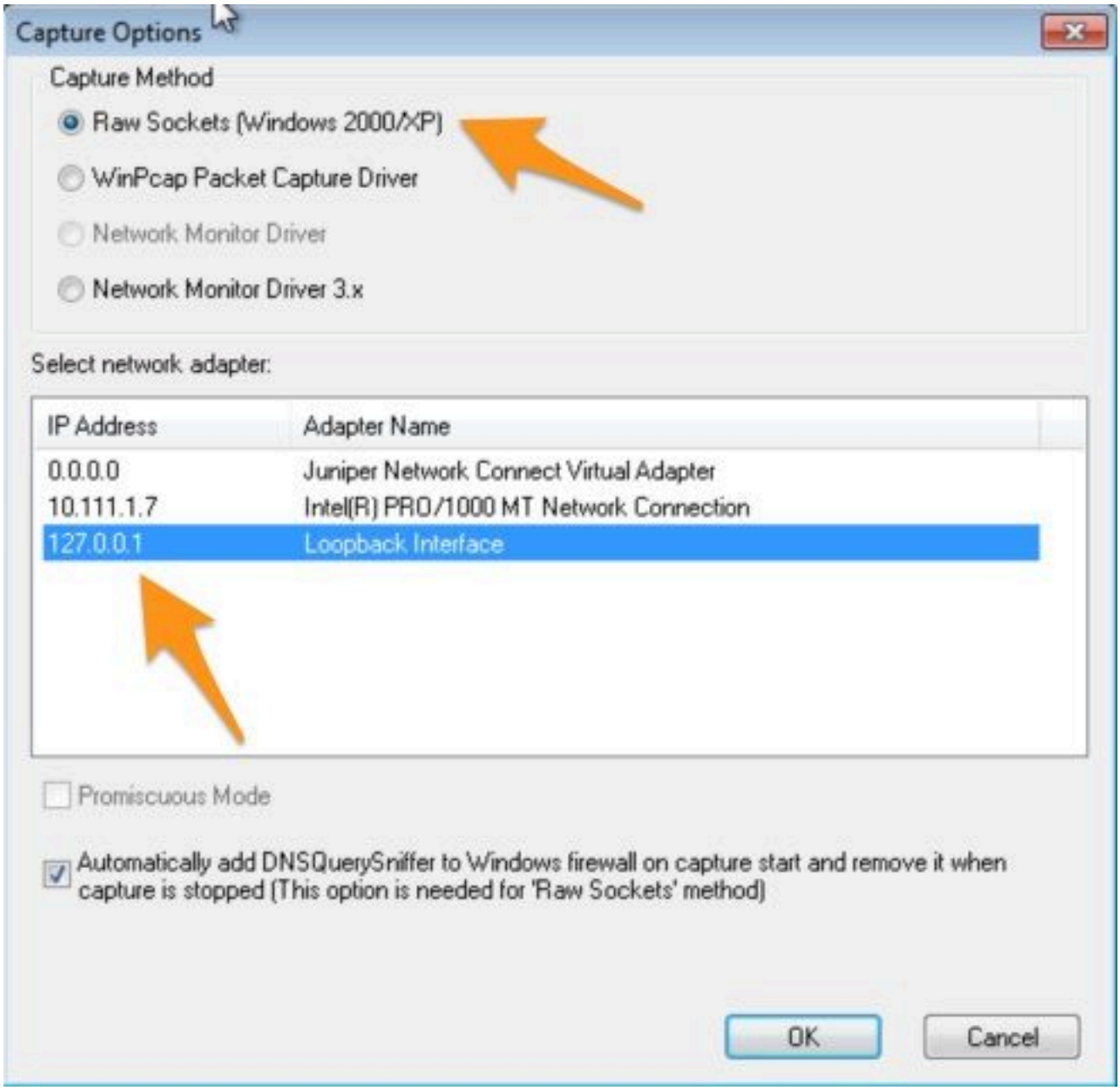
- 方法一 — 如果選擇常規網路介面，則只顯示位於內部域清單上或者未專門通過dnscryptproxy的查詢。



這些列顯示在捕獲中的最右側，您必須滾動相當長的時間。

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

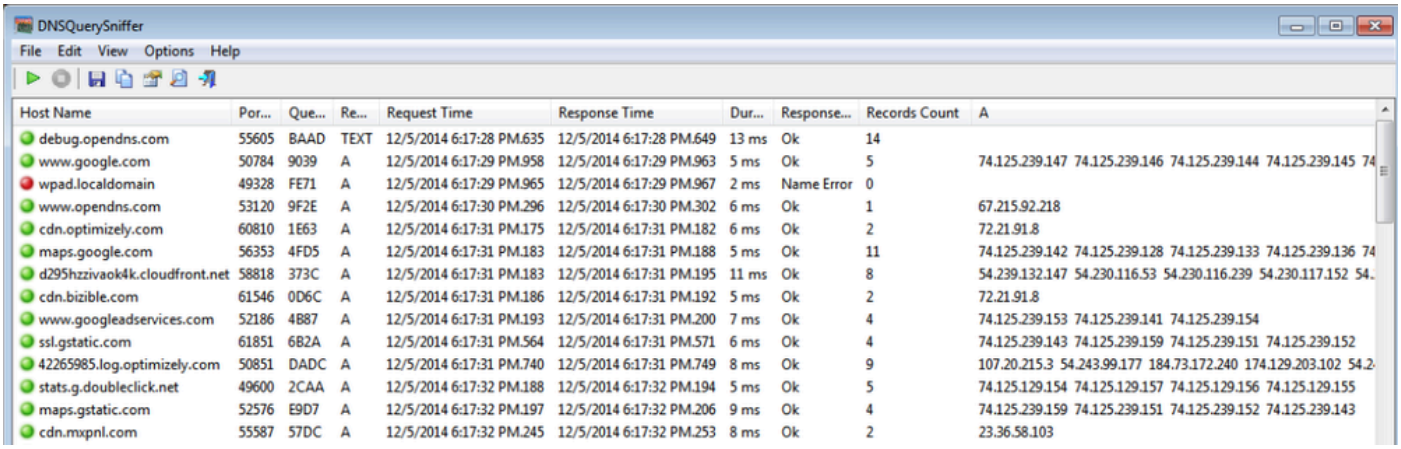
- 方法二 — 如果選擇環回介面，則會顯示通過dnscryptproxy傳送的所有DNS查詢，但不顯示「內部域」清單中域的實際目標IP地址；但是，將顯示查詢和答案。



這些列顯示在捕獲中的最右側，您必須滾動相當長的時間。

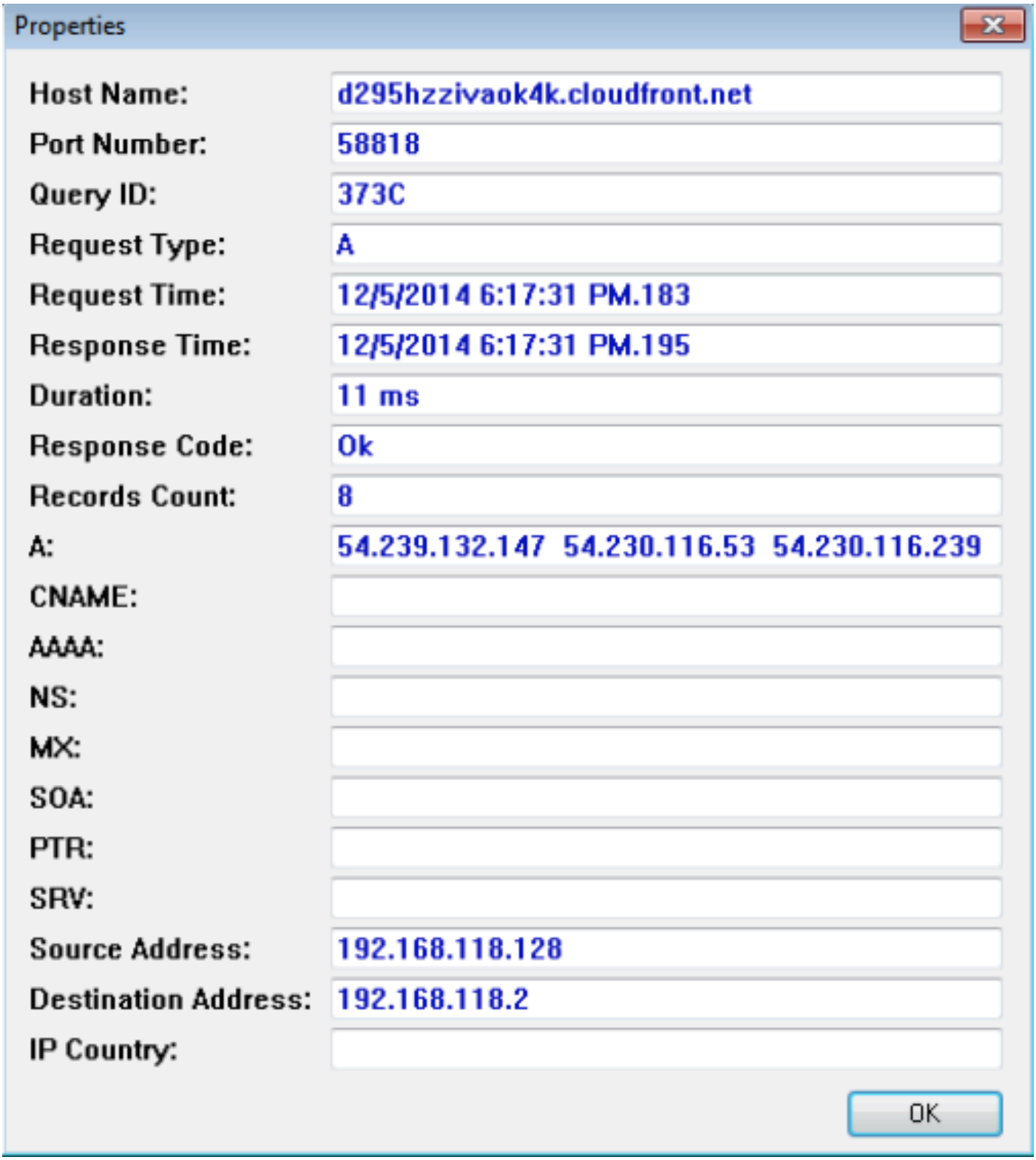
Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

結果如下所示：



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

單個查詢的檢視：


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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。