أستكشاف أخطاء الحزمة وحزم DNS وإصلاحها في Umbrella Roaming Client

المحتويات

المقدمة

يوضح هذا المستند كيفية التقاط استعلامات DNS الصادرة. العميل Umbrella المتجول حاليا طريقة لالتقاط كافة استعلامات DNS الصادرة التي يقوم بها. إذا احتجت إلى التقاط DNS، يمكنك إستخدام إحدى هذه الأدوات.

التقاط الاسترجاع لنظامي Windows و MacOS لكل من مدعي - WireShark

يسمح لك Wireshark بالتقاط الحزم المرسلة إلى واجهة الاسترجاع المحلية (127.0.0.1)، وبالتالي السماح لك برؤية طلبات DNS المرسلة إلى عميل Umbrella المتجول سواء كانت مشفرة أو غير مشفرة.

الالتقاط على جميع واجهات الشبكة النشطة خاصة عندما يكون تحليل DNS المحلي عاما

DNS فقط

إذا كنت تريد فقط النظر في طلبات DNS.

DNS + HTTP

إذا كنت تريد فقط النظر في طلب DNS و HTTP.

تصفية عمليات بحث تصحيح الأخطاء (المسابر)

إذا لم تكن تختبر فحص المشاكل المتعلقة بالمسابر بشكل صريح باستخدام debug.opendns.com، فيمكنك تصفية debug.opendns.com بكتابة هذا في شريط التصفية:

لمزيد من المعلومات حول إستخدام قوة Wireshark، راجع هذه المصادر:

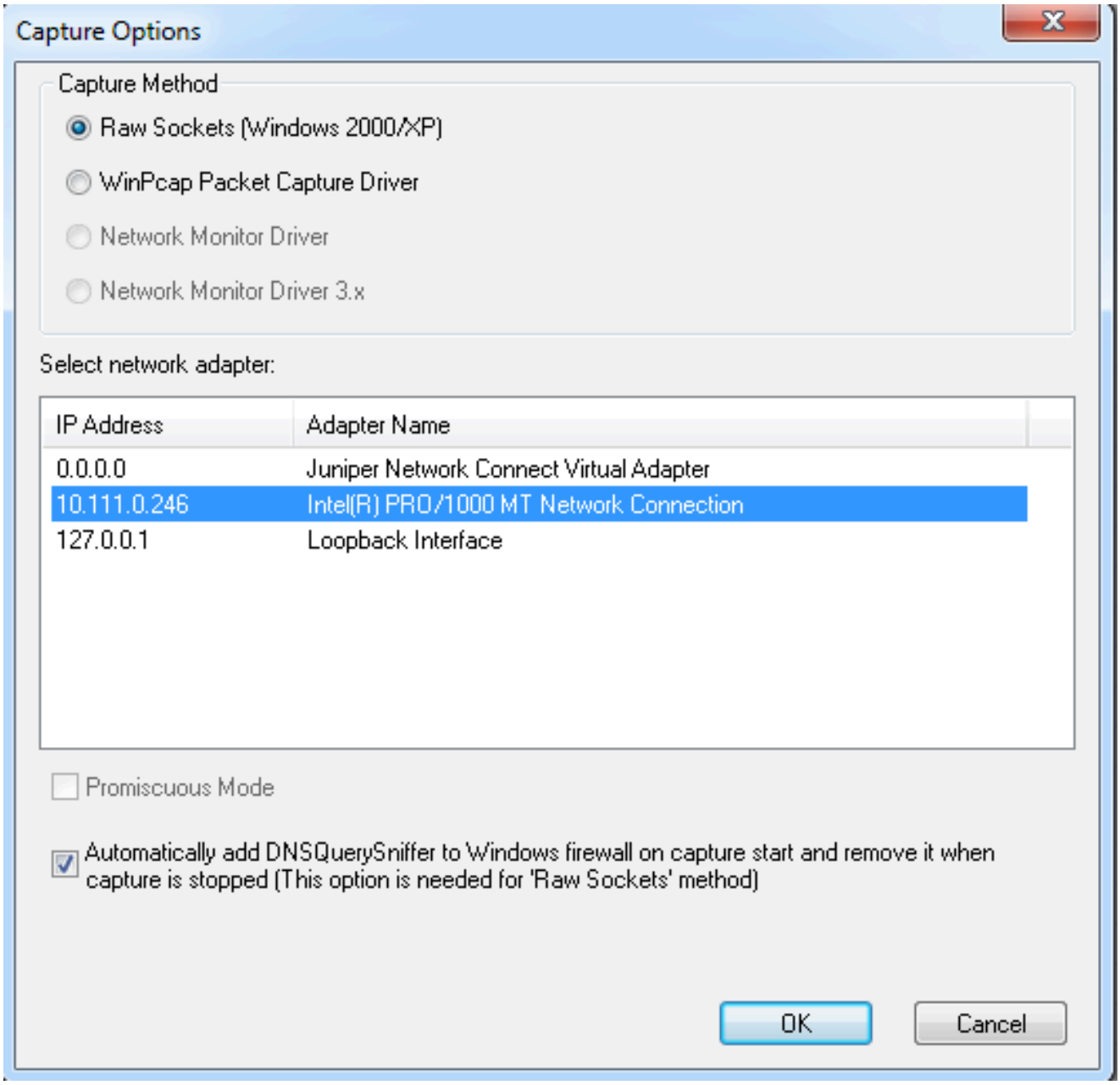
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

DNSQuery Sniffer وه sniffer خاص بشبكة DNS ل Windows والذي يراقب ويعرض أطنان من البيانات المفيدة. على عكس Wireshark أو Rawcap، فإنها تستخدم فقط من أجل DNS، وهي أسهل بكثير لفحص واستخلاص المعلومات ذات الصلة. إلا أنها لا تمتلك أدوات التصفية القوية التي يتمتع بها موقع Wireshark.
هذه أداة خفيفة الوزن وسهلة الاستخدام. ميزة كبيرة لاستخدام هذا الخيار هي أنه يمكنك التقاط الحزم أثناء تعطيل خدمة Umbrella Roaming Client (عميل حماية التجول)، وبدء عملية الالتقاط، وفجأة تشاهد كل استعلام DNS يرسله عميل Umbrella المتجول من اللحظة التي يبدأ فيها، بدلا من بدء عملية الالتقاط بعد بدء تشغيل عميل Umbrella المتجول بالفعل.

هناك طريقتان للالتقاط:

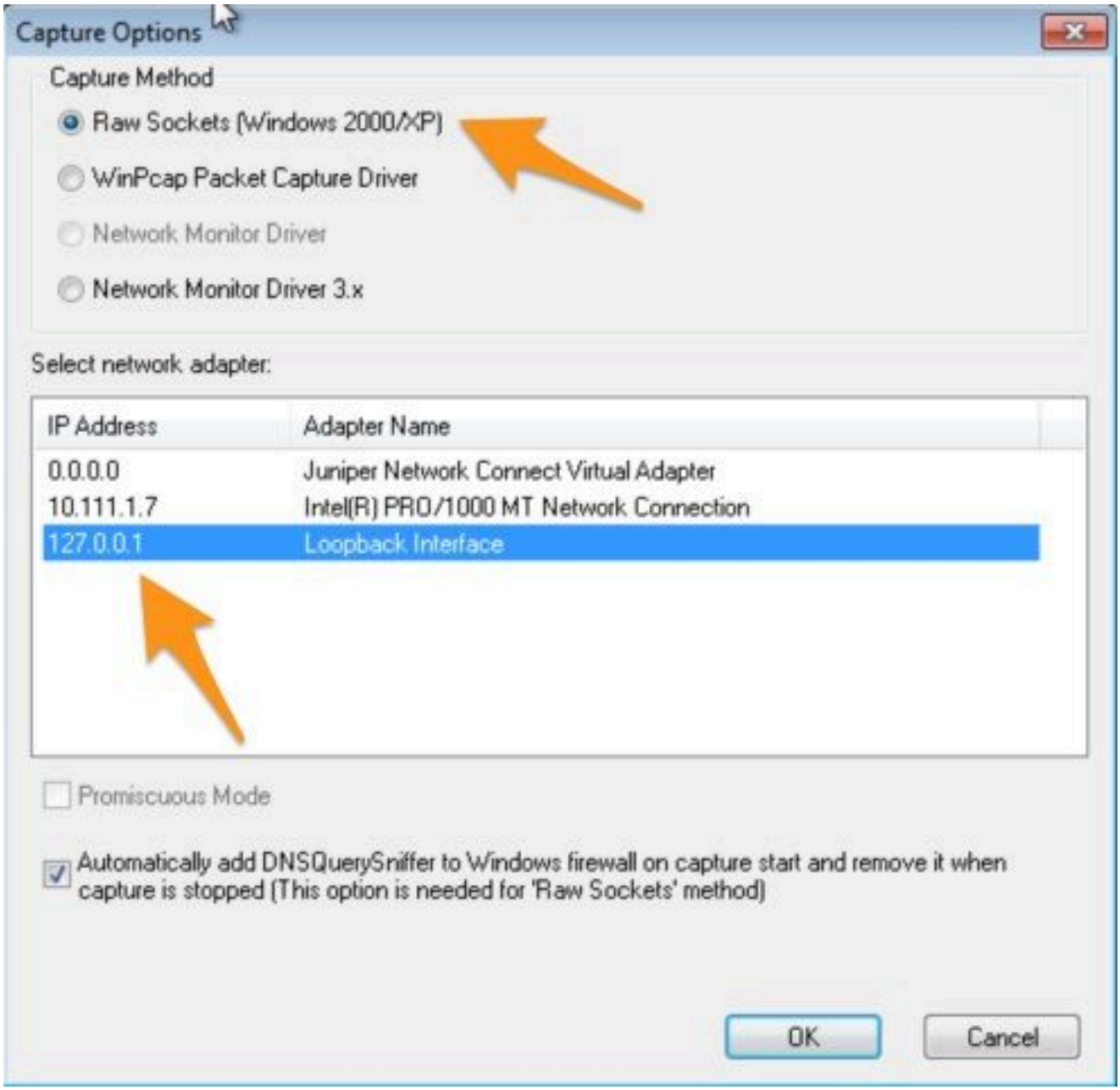
- الطريقة One—إذا قمت بتحديد واجهة الشبكة العادية، سيتم عرض الاستعلامات الموجودة في قائمة المجالات الداخلية فقط أو التي لم تمر تحديدا عبر dnscryptproxy.



تظهر هذه الأعمدة في أقصى اليمين في الالتقاط وعليك التمرير فوق القليل جدا.

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

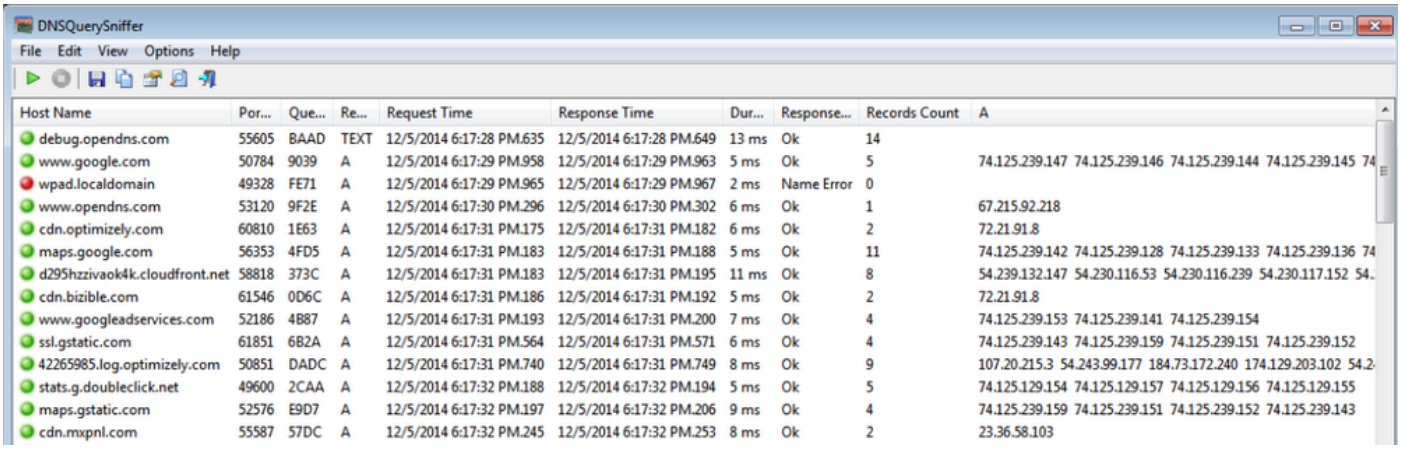
- الطريقة الثانية—إذا قمت بتحديد واجهة الاسترجاع، يتم عرض جميع استعلامات DNS التي يتم إرسالها من خلال dnscryptproxy، ولكن لا يتم عرض عنوان IP الوجهة الحقيقي للمجالات في قائمة المجالات الداخلية؛ ومع ذلك، يتم عرض الاستعلام والإجابة.



تظهر هذه الأعمدة في أقصى اليمين في الالتقاط وعليك التمرير فوق القليل جدا.

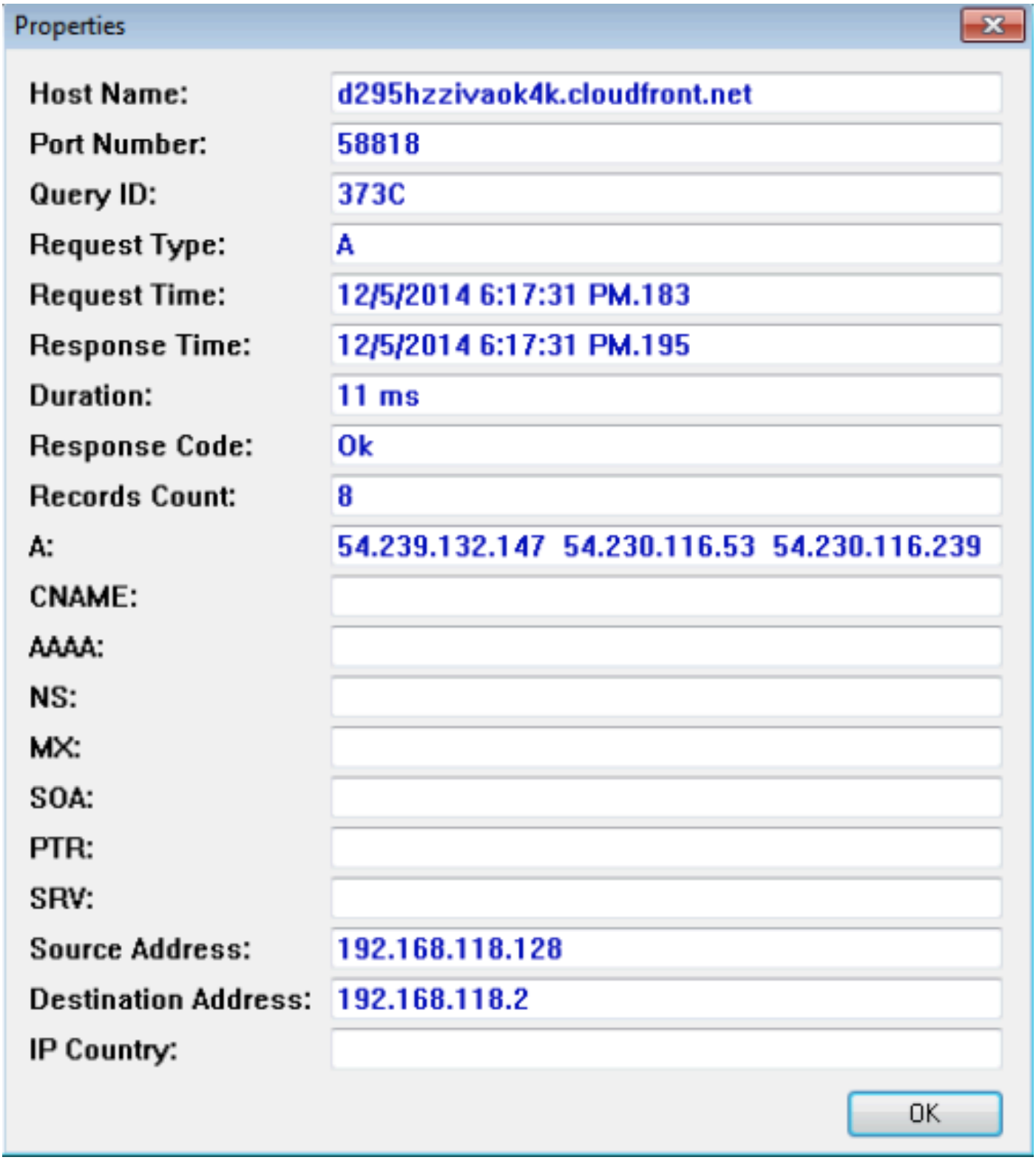
Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

النتائج تبدو كما يلي:



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

عرض البحث الفردي:


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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).