Fehlerbehebung bei Paket- und DNS-Erfassungen im Umbrella Roaming Client

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ausgehende DNS-Abfragen erfassen. Der Umbrella-Roaming-Client verfügt derzeit nicht über eine Methode zur Erfassung aller ausgehenden DNS-Abfragen. Wenn Sie DNS erfassen müssen, können Sie eines dieser Tools verwenden.

WireShark - Windows und MacOS unterstützen beide Loopback-Erfassung

Mit Wireshark können Sie Pakete erfassen, die an die lokale Loopback-Schnittstelle (127.0.0.1) gesendet wurden. So können Sie DNS-Anfragen sehen, die verschlüsselt oder unverschlüsselt an den Umbrella-Roaming-Client gesendet wurden.

Erfassung an allen aktiven Netzwerkschnittstellen, insbesondere wenn die lokale DNS-Auflösung eine Rolle spielt

Nur DNS

Wenn Sie nur nach DNS-Anfragen suchen möchten.

DNS + HTTP

Wenn Sie nur die DNS- und HTTP-Anfrage betrachten möchten.

Ausfiltern von Debugsuchvorgängen (Tests)

Wenn Sie die Überprüfung auf Probleme im Zusammenhang mit Datensammlungen oder Probleme mit debug.opendns.com nicht explizit testen, können Sie debug.opendns.com herausfiltern, indem Sie dies in die Filterleiste eingeben:

Weitere Informationen zur optimalen Nutzung von Wireshark finden Sie in den folgenden Ressourcen:

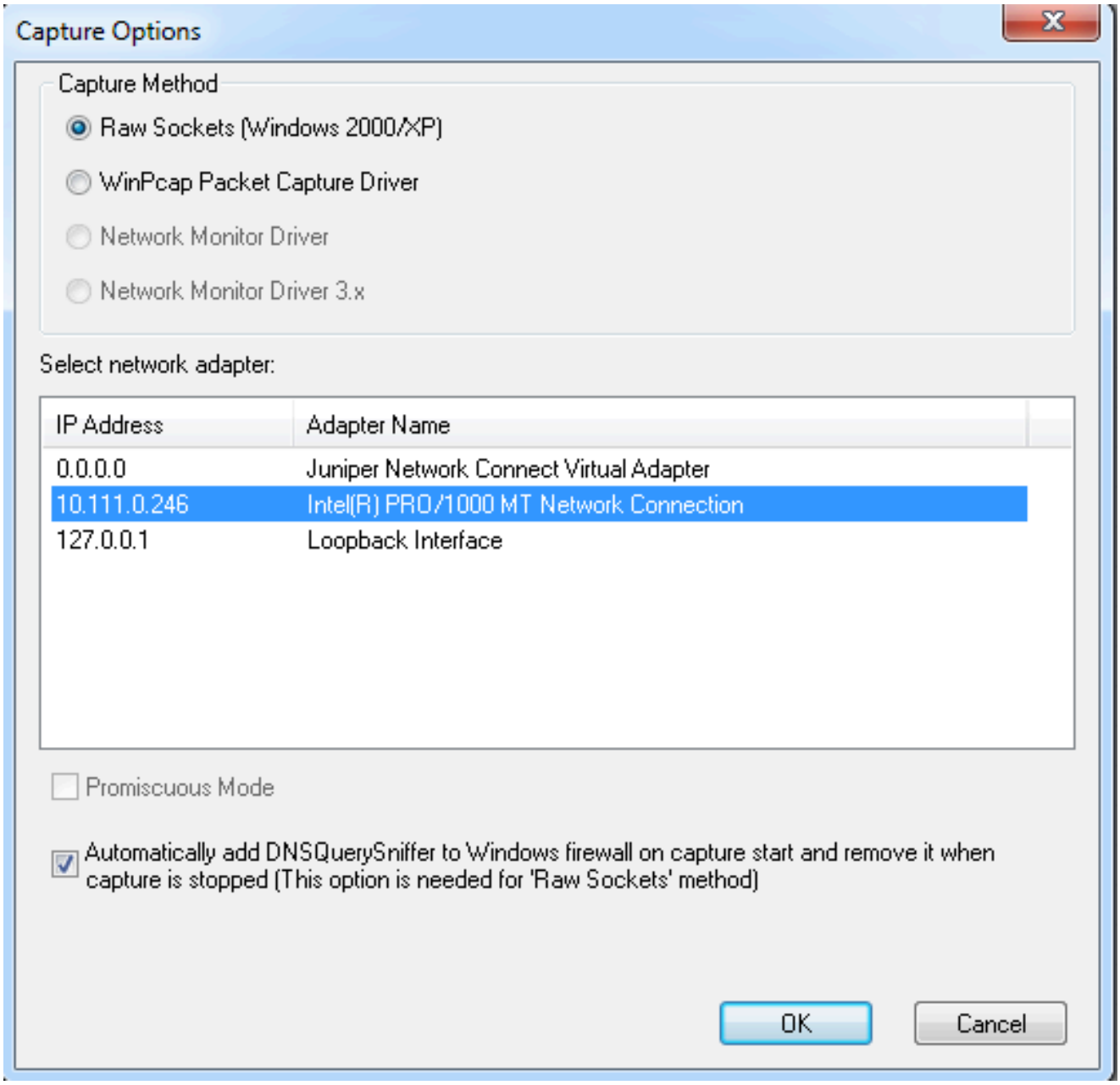
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

DNSQuery Sniffer ist ein reiner DNS-Netzwerk-Sniffer für Windows, der unzählige nützliche Daten überwacht und anzeigt. Im Gegensatz zu Wireshark oder Rawcap wird es nur für DNS verwendet und ist viel einfacher, relevante Informationen zu untersuchen und zu extrahieren. Es verfügt jedoch nicht über die leistungsstarken Filtertools von Wireshark.
Dies ist ein leichtes und benutzerfreundliches Tool. Ein großer Vorteil bei der Verwendung dieser Funktion besteht darin, dass Sie Pakete abhören können, während der Umbrella Roaming Client Service deaktiviert ist, die Erfassung starten und plötzlich jede DNS-Abfrage sehen, die der Umbrella Roaming Client von dem Moment an sendet, als er startet, anstatt eine Erfassung zu starten, nachdem der Umbrella Roaming Client bereits gestartet wurde.

Es gibt zwei Erfassungsmethoden:

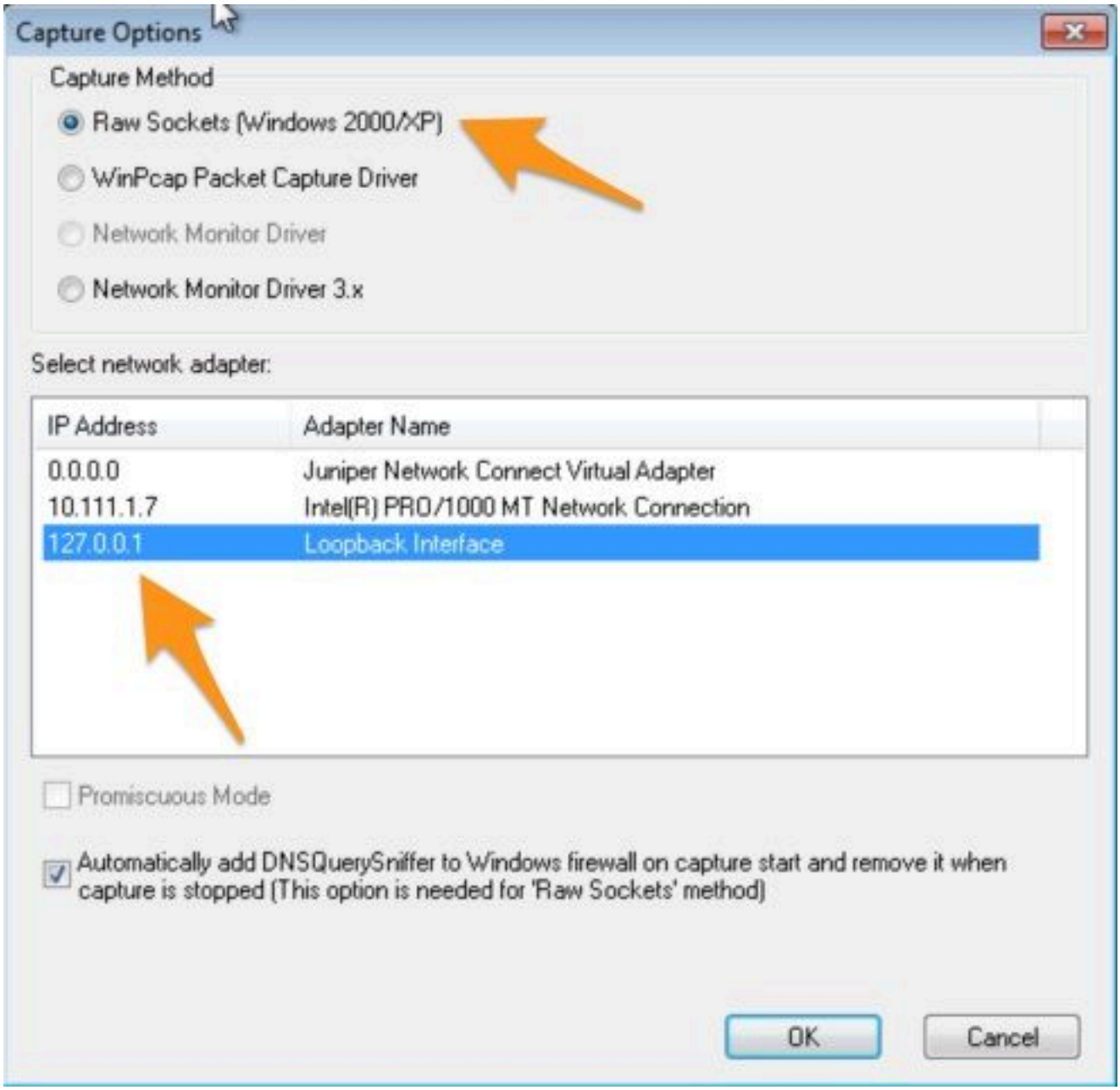
- Methode 1 - Wenn Sie die reguläre Netzwerkschnittstelle auswählen, werden nur Abfragen angezeigt, die sich in der Liste Interne Domänen befinden oder die den dnscryptproxy nicht explizit durchlaufen haben.



Diese Spalten erscheinen ganz rechts in der Aufnahme, und Sie müssen einen Bildlauf durchführen.

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

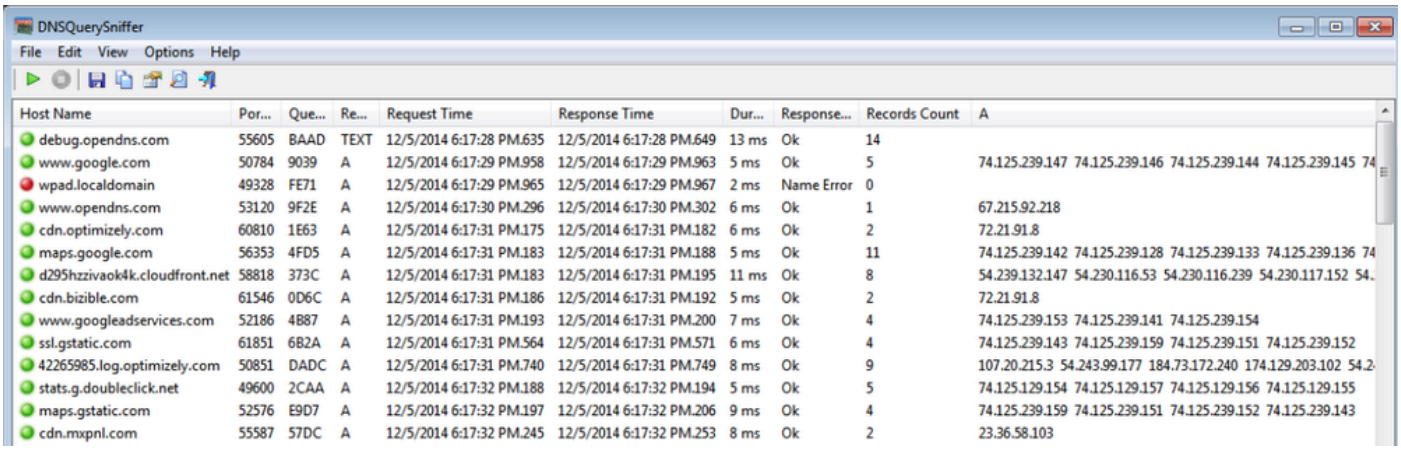
- Methode Zwei: Wenn Sie die Loopback-Schnittstelle auswählen, werden alle DNS-Abfragen angezeigt, die über den dnscryptproxy gesendet werden. Die tatsächliche Ziel-IP-Adresse für Domänen in der Liste Interne Domänen wird jedoch nicht angezeigt. Die Abfrage und die Antwort werden jedoch angezeigt.



Diese Spalten erscheinen ganz rechts in der Aufnahme, und Sie müssen einen Bildlauf durchführen.

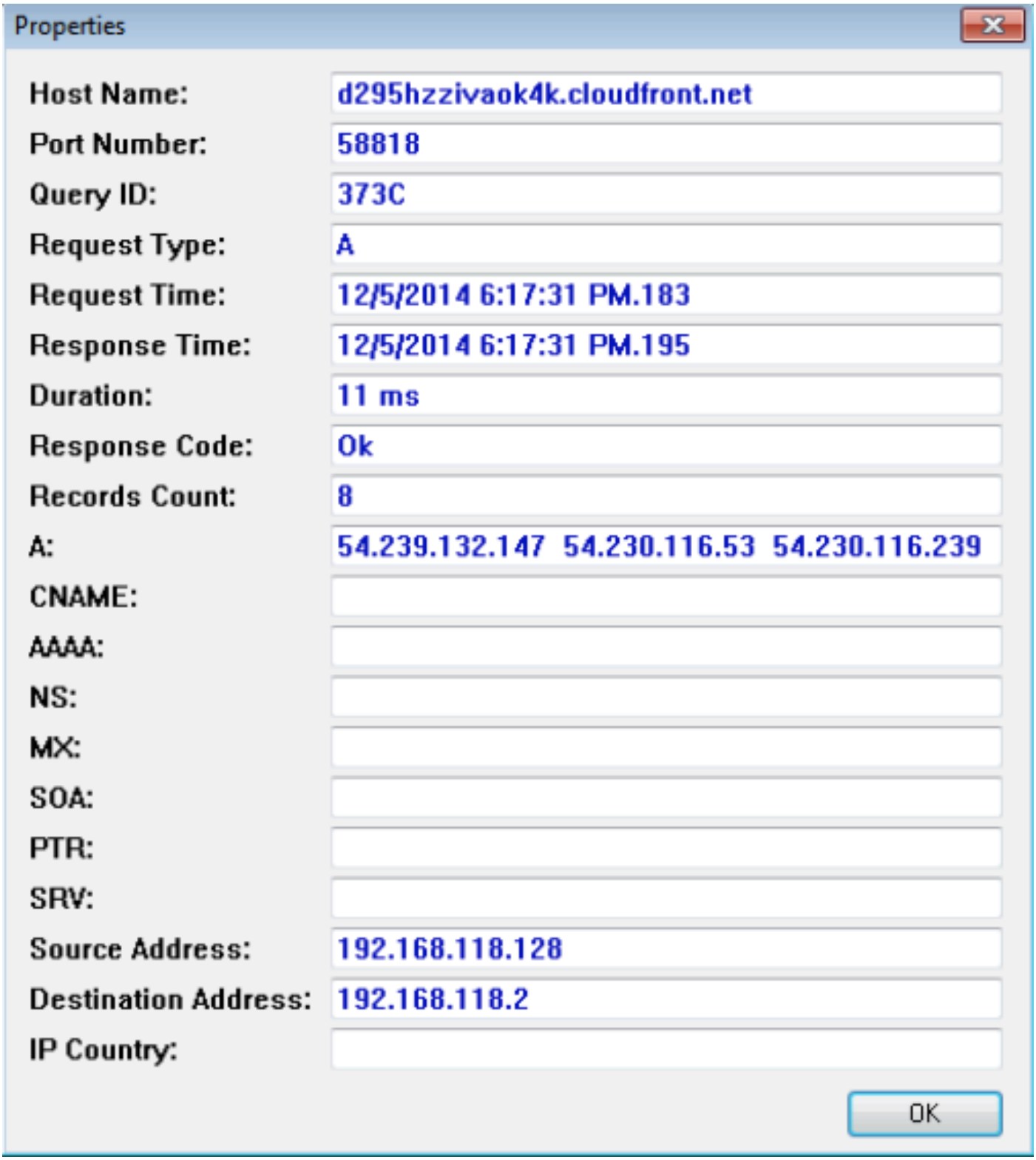
Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

Die Ergebnisse sehen wie folgt aus:



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

Ansicht einer individuellen Suche:


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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.