Problemen oplossen met pakketopnamen en DNS-opnamen in Umbrella Roaming-client

Inhoud

Inleiding

In dit document wordt beschreven hoe u uitgaande DNS-query's kunt vastleggen. De Umbrella-roamingclient heeft momenteel geen methode voor het vastleggen van alle uitgaande DNS-query's die het maakt. Als u DNS wilt vastleggen, kunt u een van deze tools gebruiken.

WireShark - Windows en MacOS ondersteunen beide loopback capture

Met Wireshark kunt u pakketten vastleggen die naar de lokale loopback-interface (127.0.0.1) zijn verzonden, zodat u DNS-verzoeken die naar de Umbrella-roamingclient zijn verzonden, gecodeerd of niet-gecodeerd, kunt zien.

Leg vast op alle actieve netwerkinterfaces, vooral wanneer de lokale DNS-resolutie een factor is

Alleen DNS

Als je alleen maar naar DNS-verzoeken wilt kijken.

DNS + HTTP

Als je alleen wilt kijken naar DNS en HTTP verzoek.

Opzoeken van fouten uitfilteren (probes)

Als u niet expliciet test op problemen of problemen met sonde-gerelateerde problemen met debug.opendns.com, kunt u debug.opendns.com uitfilteren door dit in de filterbalk te typen:

Voor meer informatie over het benutten van de kracht van Wireshark, zie deze bronnen:

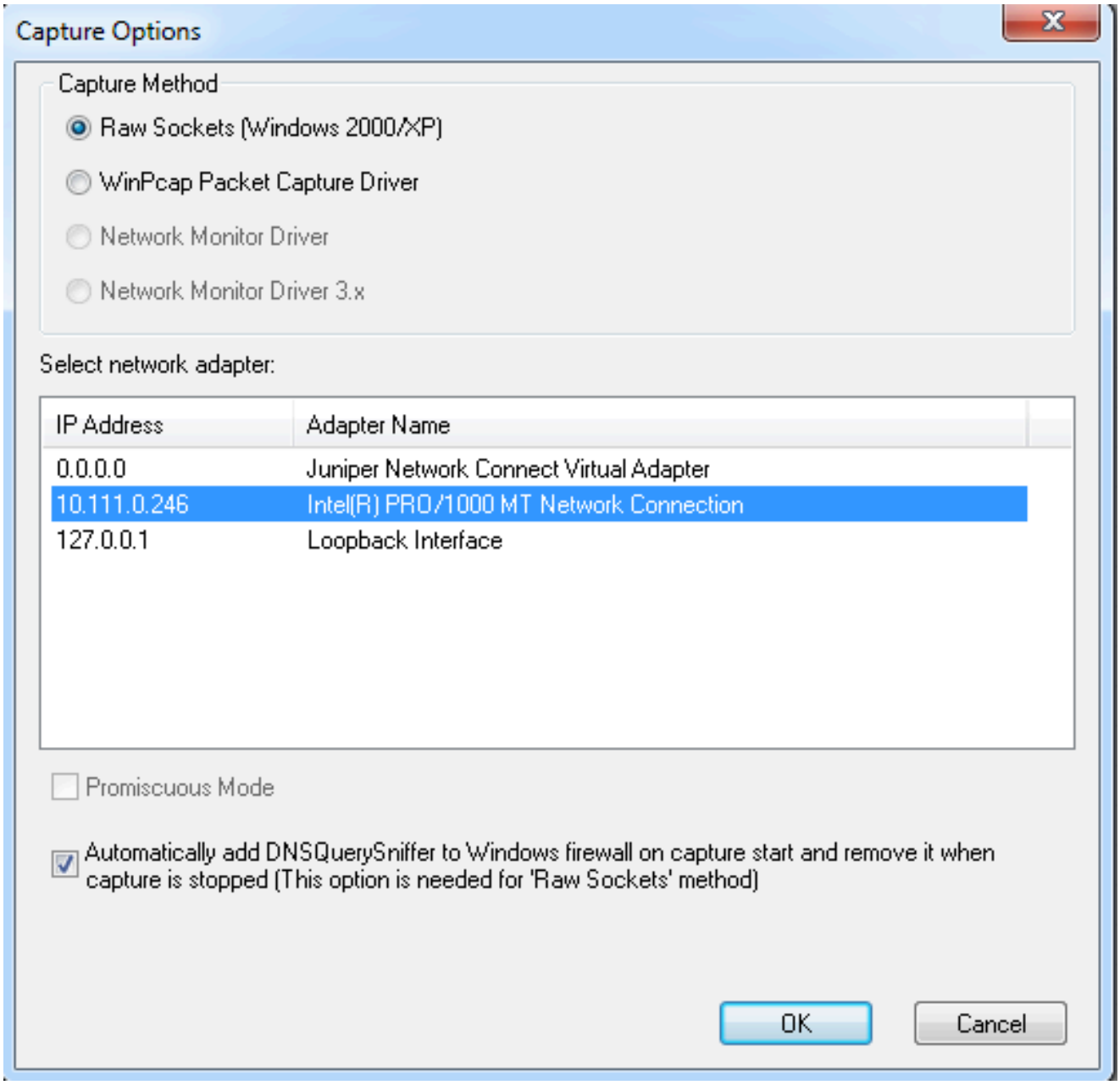
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

DNSQuery Sniffer is een DNS-only netwerksnuiver voor Windows die tonnen nuttige gegevens bewaakt en weergeeft. In tegenstelling tot Wireshark of Rawcap, wordt het alleen gebruikt voor DNS en is het veel gemakkelijker om relevante informatie te onderzoeken en te extraheren. Het heeft echter niet de krachtige filtertools van Wireshark.
Dit is een lichtgewicht en eenvoudig te gebruiken tool. Een groot voordeel van het gebruik hiervan is dat u pakketten kunt snuiven terwijl de Umbrella-roamingclient is uitgeschakeld, de opname kunt starten en plotseling ziet u elke DNS-query die de Umbrella-roamingclient verzendt vanaf het moment dat deze wordt gestart, in plaats van een opname te starten nadat de Umbrella-roamingclient al is gestart.

Er zijn twee vangmethoden:

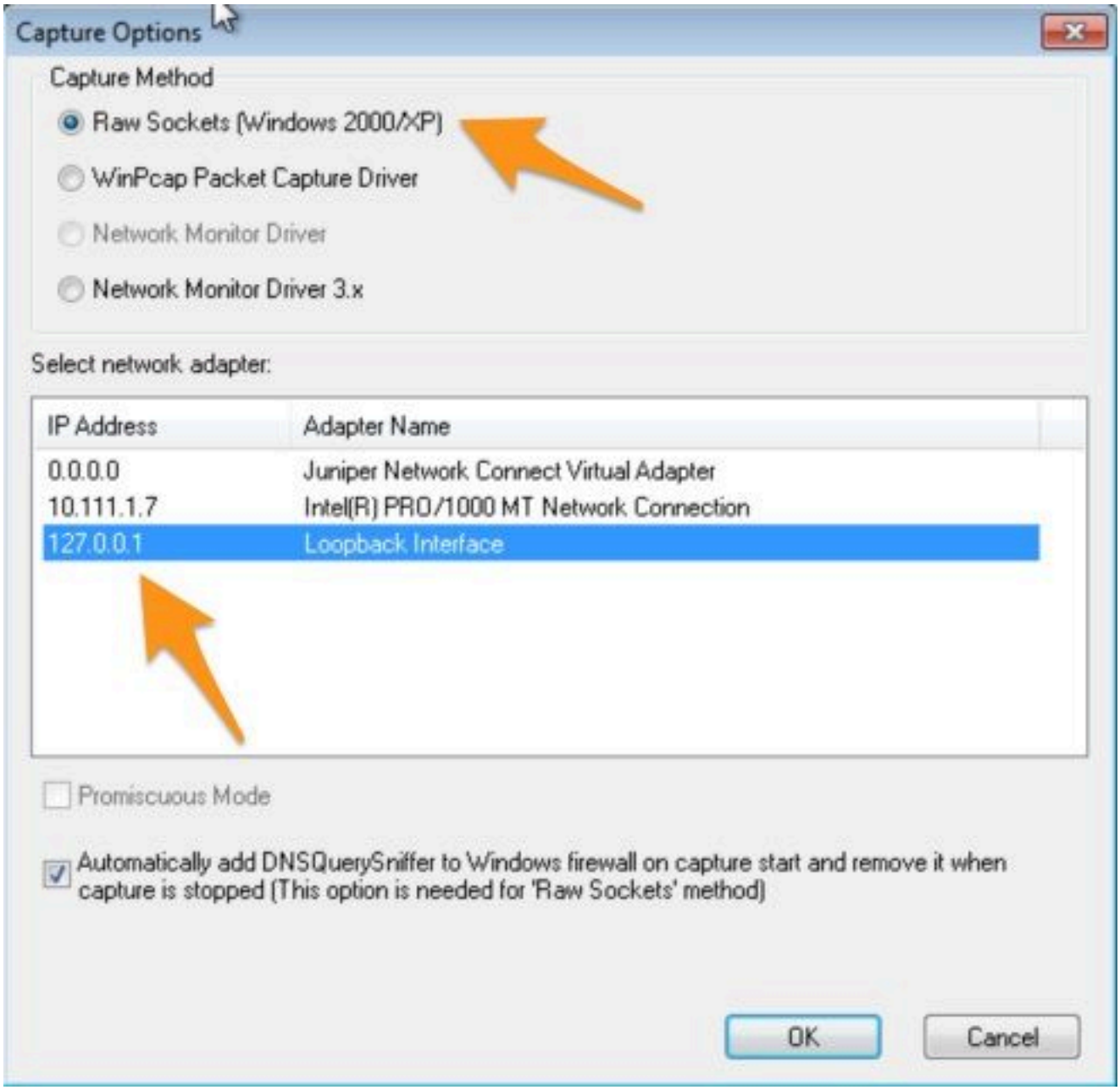
- Methode één: als u de reguliere netwerkinterface selecteert, worden alleen query's weergegeven die in de lijst Interne domeinen staan of die niet specifiek door de encryptieproxy zijn gegaan.



Deze kolommen verschijnen helemaal rechts in de opname en je moet er nogal over scrollen.

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

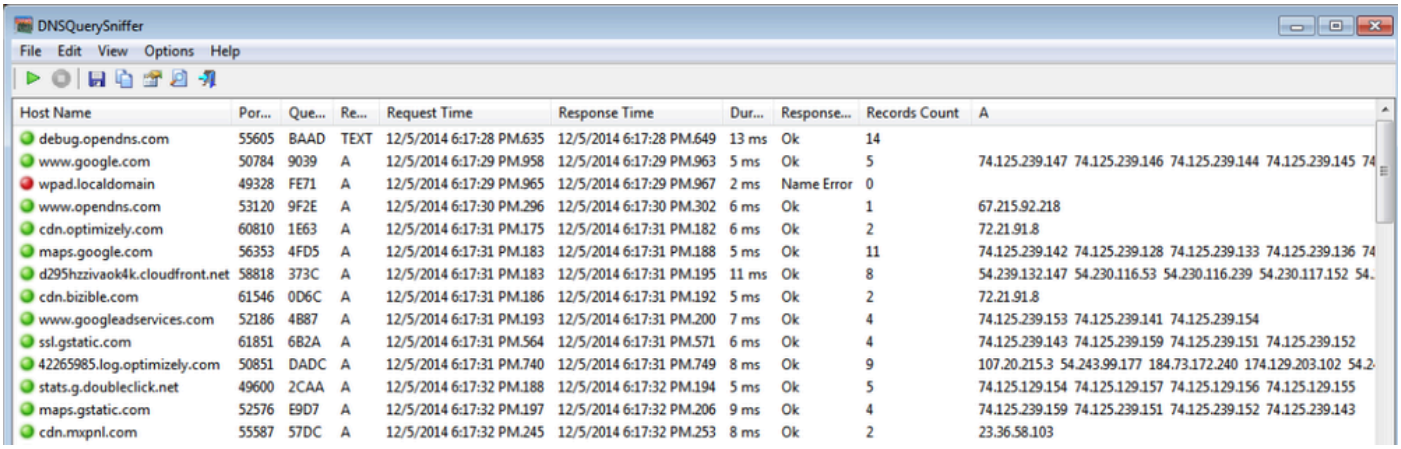
- Methode twee—Als u de Loopback-interface selecteert, worden alle DNS-query's weergegeven die via de encryptieproxy worden verzonden, maar wordt het ware IP-adres van de bestemming voor domeinen in de lijst Interne domeinen niet weergegeven. De query en het antwoord worden echter wel weergegeven.



Deze kolommen verschijnen helemaal rechts in de opname en je moet er nogal over scrollen.

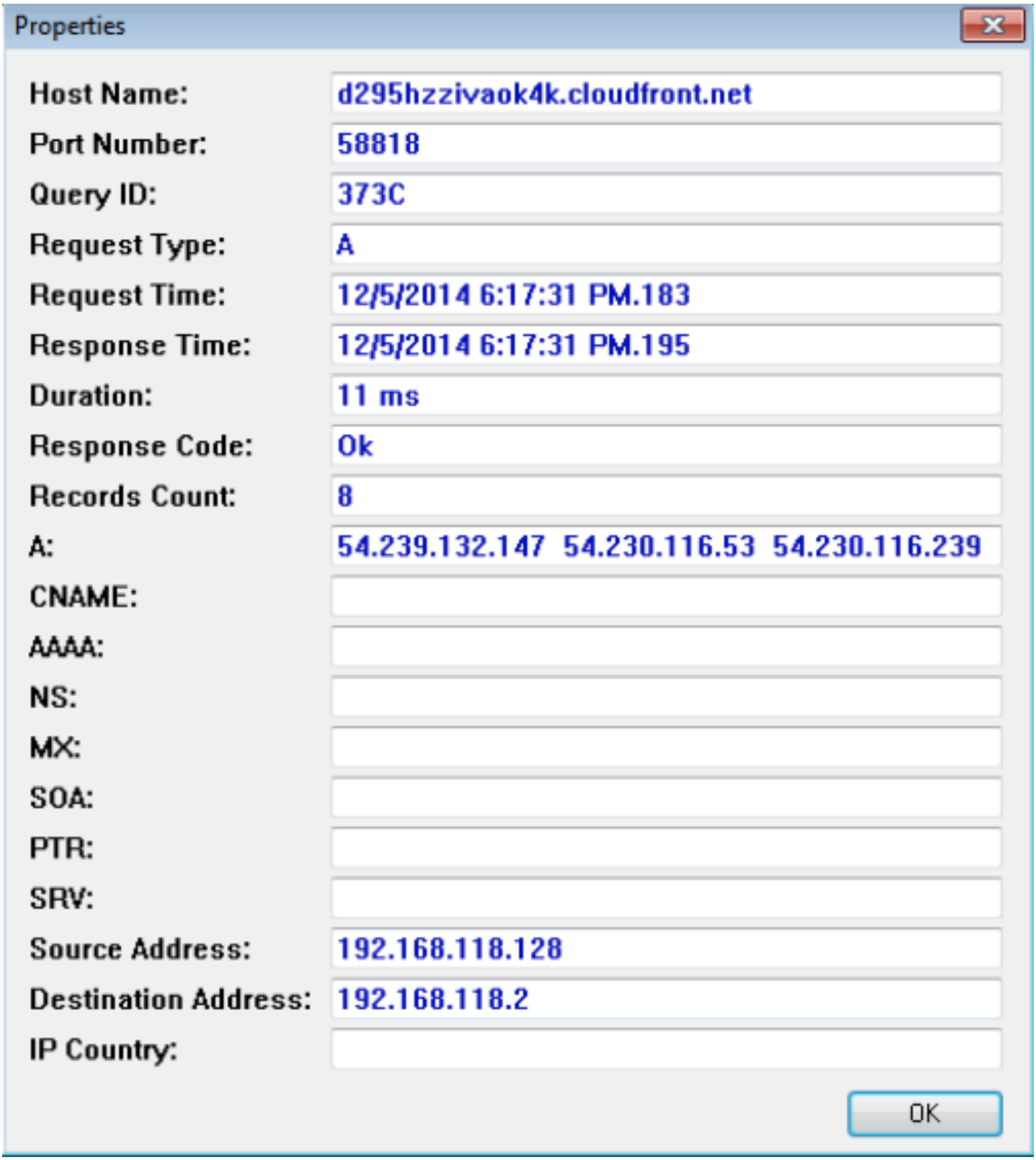
Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

De resultaten zien er als volgt uit:



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

Overzicht van een individuele 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:
OK

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.