Solucionar problemas de captura de pacotes e DNS no cliente Umbrella Roaming

Contents

Introdução

Este documento descreve como capturar consultas de DNS de saída. O cliente de roaming Umbrella atualmente não tem um método para capturar todas as consultas DNS de saída que ele faz. Se precisar capturar DNS, você pode usar uma dessas ferramentas.

WireShark - Windows e MacOS suportam captura de loopback

O Wireshark permite capturar pacotes enviados para a interface de loopback local (127.0.0.1), permitindo assim que você veja solicitações DNS enviadas ao cliente de roaming Umbrella criptografadas ou não.

Capturar todas as interfaces de rede ativas, especialmente quando a resolução de DNS local é um fator

Somente DNS

Se quiser apenas examinar as solicitações DNS.

DNS + HTTP

Se você quiser apenas examinar solicitações DNS e HTTP.

Filtrar pesquisas de depuração (sondas)

Se você não estiver testando explicitamente a verificação de problemas relacionados à sonda ou de problemas com debug.opendns.com, poderá filtrar debug.opendns.com digitando isso na barra de filtro:

Para obter mais informações sobre como aproveitar o poder do Wireshark, consulte estes recursos:

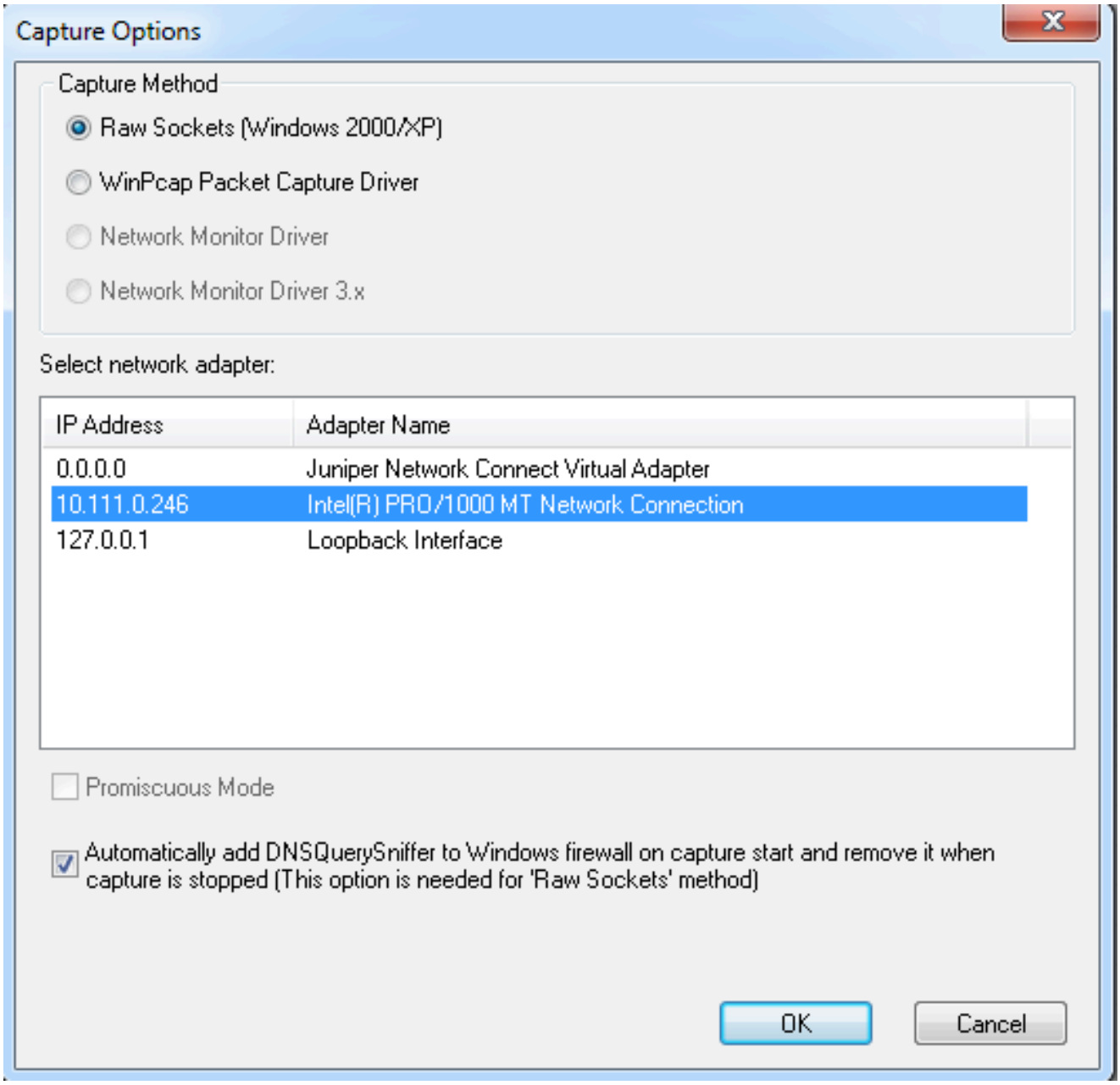
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

O DNSQuery Sniffer é um sniffer de rede apenas para DNS para Windows que monitora e exibe toneladas de dados úteis. Ao contrário do Wireshark ou Rawcap, ele é usado apenas para DNS e é muito mais fácil de examinar e extrair informações relevantes. No entanto, ele não tem as ferramentas de filtragem poderosas do Wireshark.
Esta é uma ferramenta leve e fácil de usar. Uma grande vantagem de usar isso é que você pode farejar pacotes enquanto o serviço cliente de roaming Umbrella está desabilitado, iniciar a captura e, de repente, você está vendo cada consulta DNS que o cliente de roaming Umbrella envia a partir do momento em que ele começa, em vez de iniciar uma captura depois que o cliente de roaming Umbrella já começou.

Há dois métodos de captura:

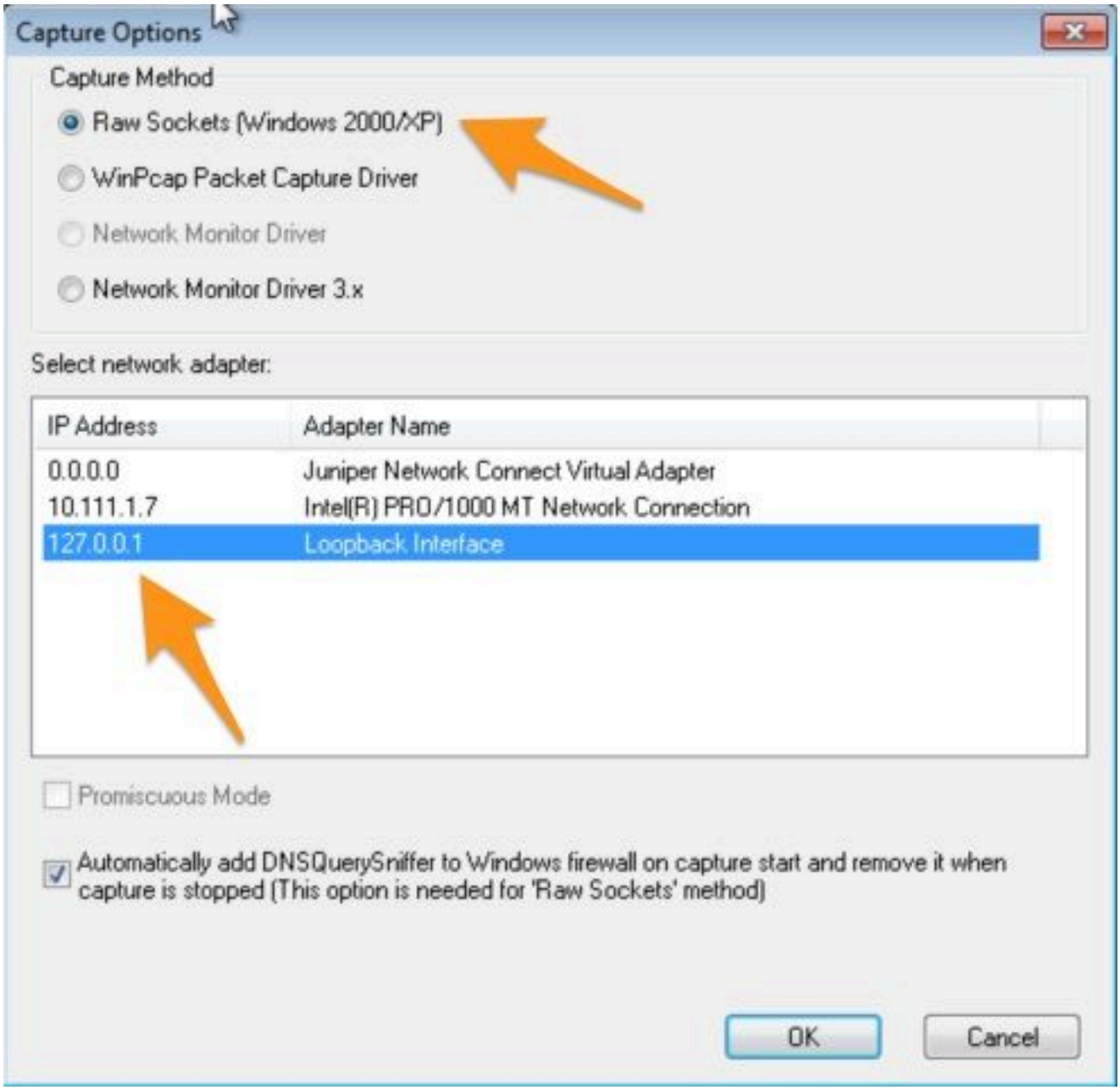
- Método um — Se você selecionar a interface de rede regular, somente as consultas que estão na lista Domínios internos ou que não passaram especificamente pelo dnscryptproxy serão mostradas.



Essas colunas aparecem na extrema direita na captura e você tem que rolar por cima um pouco.

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

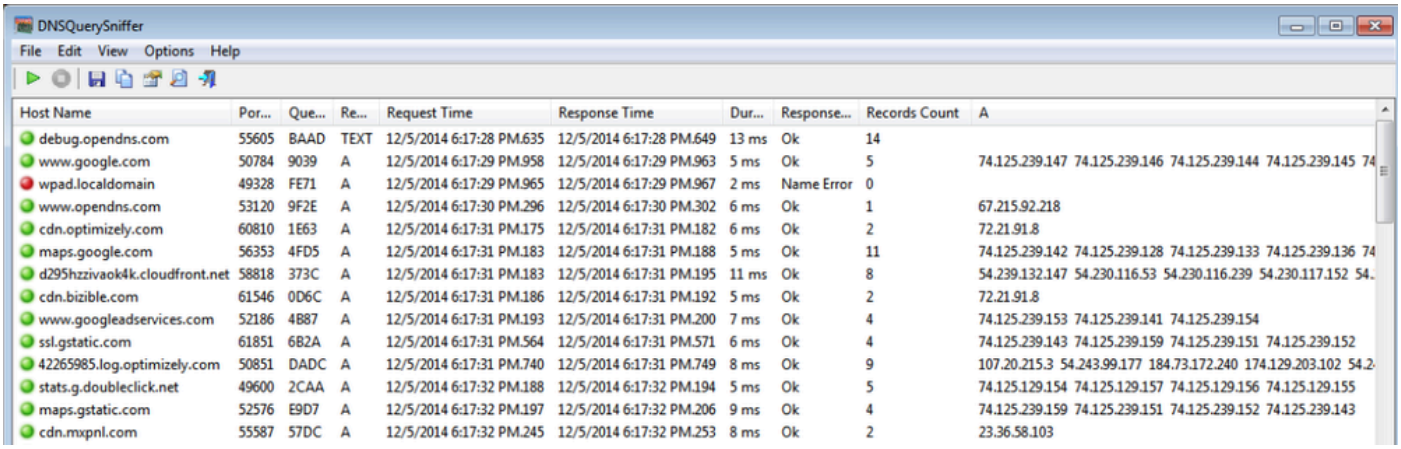
- Método dois — Se você selecionar a interface de loopback, todas as consultas de DNS enviadas através do dnscryptproxy serão mostradas, mas o endereço IP de destino verdadeiro para domínios na lista Domínios internos não será mostrado; no entanto, a consulta e a resposta são exibidas.



Essas colunas aparecem na extrema direita na captura e você tem que rolar por cima um pouco.

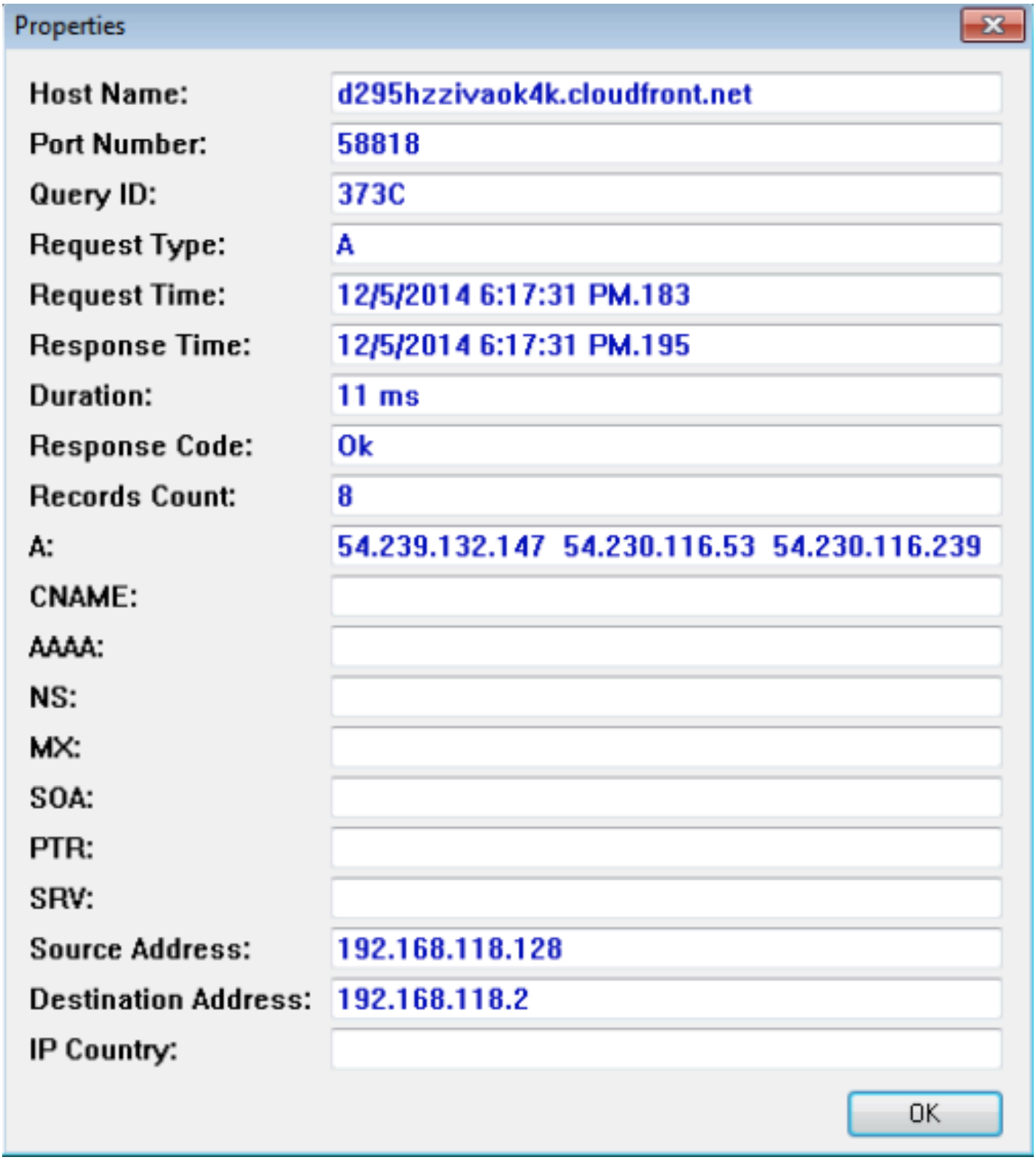
Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

Os resultados se parecem com:



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

Exibição de uma pesquisa individual:


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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.