Resolución de problemas de paquetes y capturas de DNS en Umbrella Roaming Client

Contenido

Introducción

Este documento describe cómo capturar consultas DNS salientes. El cliente de roaming de Umbrella no tiene actualmente un método para capturar todas las consultas de DNS saliente que realiza. Si necesita capturar DNS, puede utilizar una de estas herramientas.

WireShark - Windows y MacOS admiten la captura de loopback

Wireshark le permite capturar paquetes enviados a la interfaz de loopback local (127.0.0.1), lo que le permite ver las solicitudes DNS enviadas al cliente de roaming de Umbrella, ya sean cifradas o no.

Capturar en todas las interfaces de red activas, especialmente cuando la resolución de DNS local es un factor

Sólo DNS

Si sólo desea ver las solicitudes DNS.

DNS + HTTP

Si sólo desea consultar la solicitud de DNS y HTTP.

Filtrar búsquedas de depuración (sondeos)

Si no está probando explícitamente la comprobación de problemas relacionados con sondeos o problemas con debug.opendns.com, puede filtrar debug.opendns.com escribiendo esto en la barra de filtros:

Para obtener más información sobre cómo aprovechar el potencial de Wireshark, consulte estos recursos:

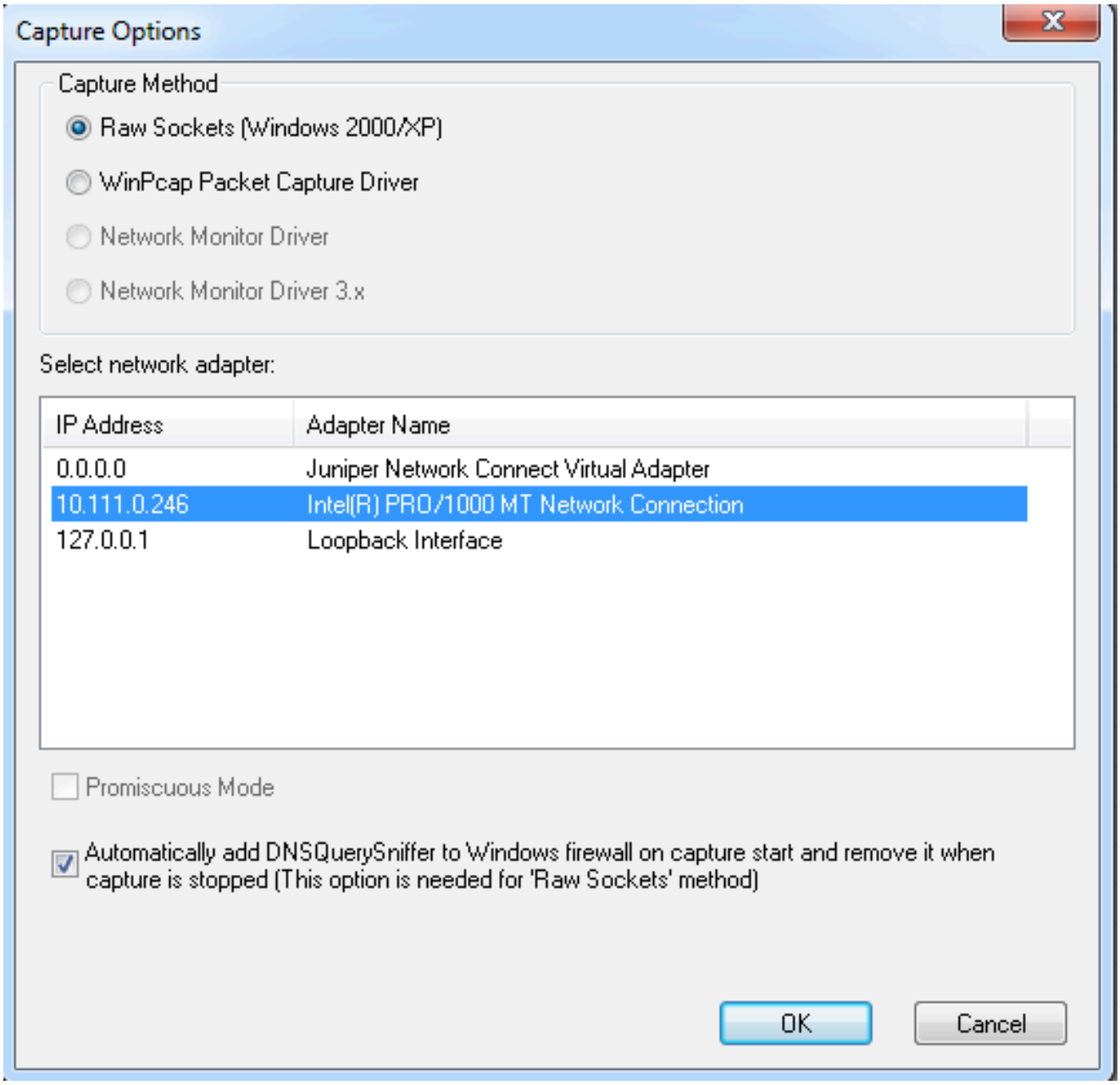
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (Windows)

DNSQuery Sniffer es un sabueso de red solo DNS para Windows que monitorea y muestra toneladas de datos útiles. A diferencia de Wireshark o Rawcap, solo se utiliza para DNS y es mucho más fácil examinar y extraer información relevante. Sin embargo, no cuenta con las potentes herramientas de filtrado de Wireshark.
Se trata de una herramienta ligera y fácil de usar. Una gran ventaja de usar esto es que puede oler paquetes mientras el servicio de cliente de roaming de Umbrella está inhabilitado, iniciar la captura y, de repente, está viendo cada consulta DNS que el cliente de roaming de Umbrella envía desde el momento en que comienza, en lugar de iniciar una captura después de que el cliente de roaming de Umbrella ya haya comenzado.

Existen dos métodos de captura:

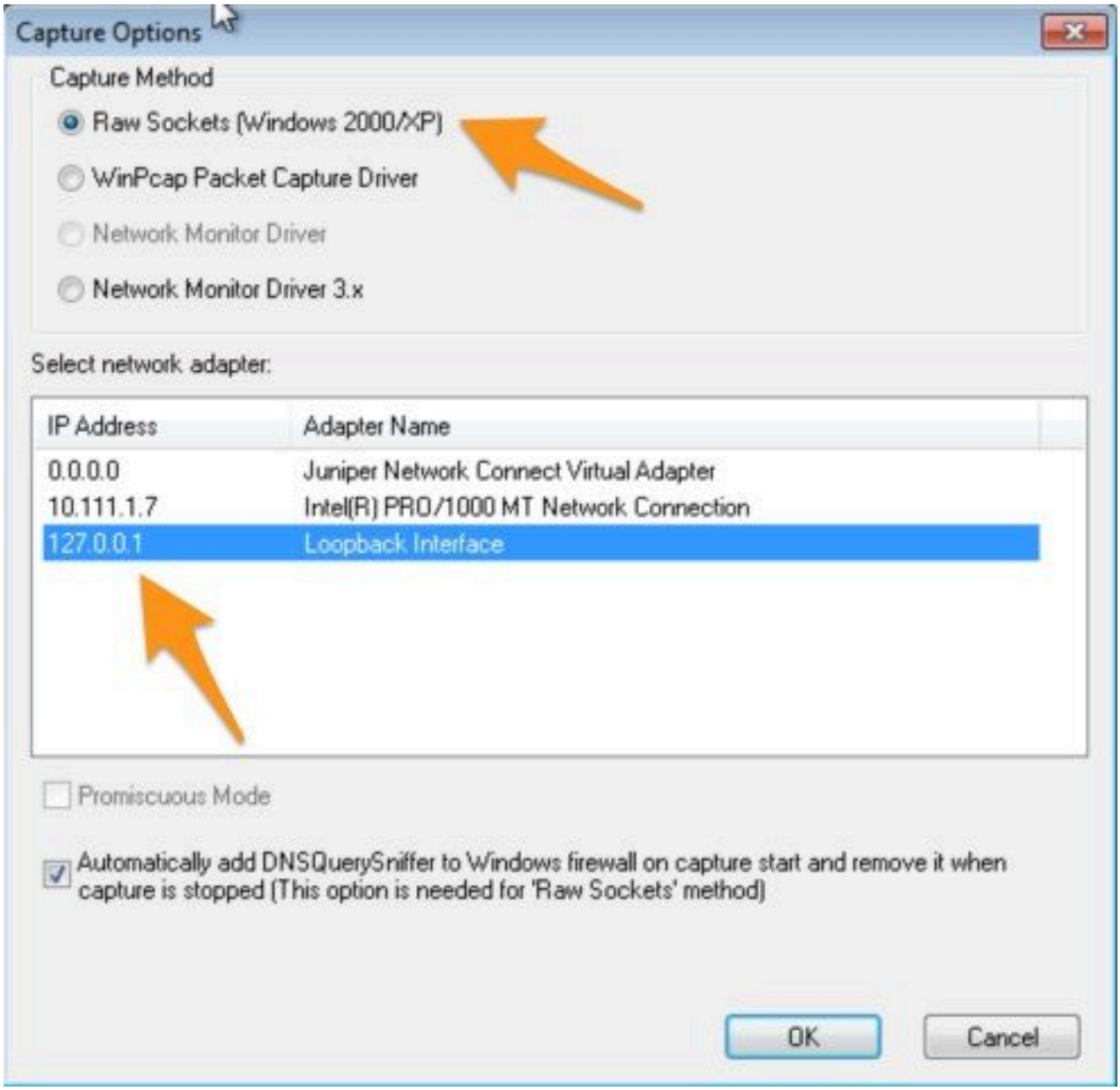
- Método uno: si selecciona la interfaz de red normal, solo se muestran las consultas que se encuentran en la lista Dominios internos o que no pasaron específicamente a través de dnscryptproxy.



Estas columnas aparecen en el extremo derecho de la captura y hay que desplazarse un poco.

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

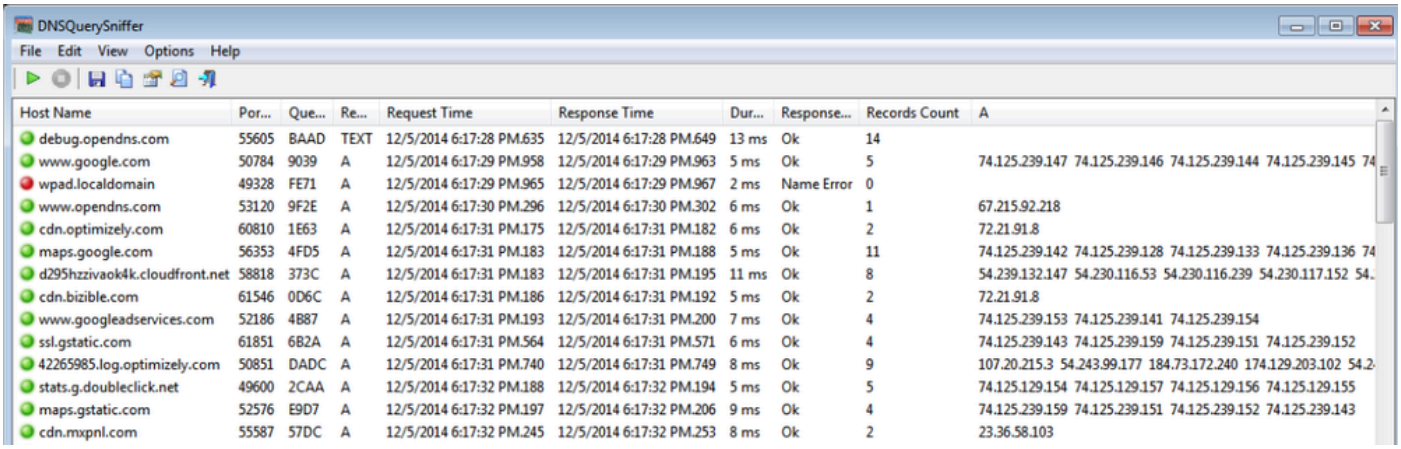
- Método dos: si selecciona la interfaz Loopback, se muestran todas las consultas DNS que se envían a través de dnscryptproxy, pero no se muestra la dirección IP de destino verdadera para los dominios de la lista de dominios internos; sin embargo, se muestran la consulta y la respuesta.



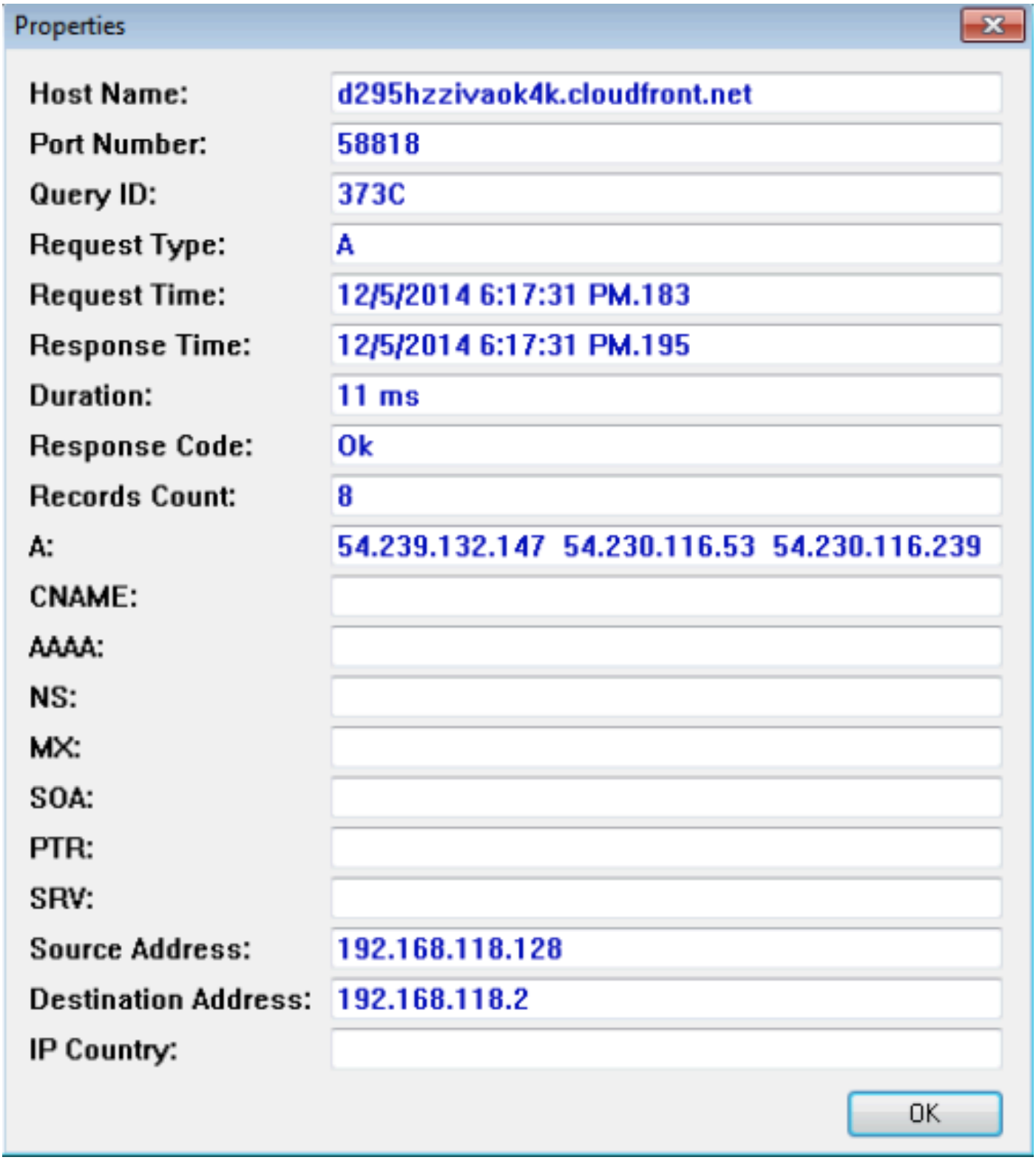
Estas columnas aparecen en el extremo derecho de la captura y hay que desplazarse un poco.

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

Los resultados son los siguientes:



Vista de una búsqueda 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).