

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

## Contenido

---

[Introducción](#)

[WireShark - Windows y MacOS admiten la captura de loopback](#)

[DNSQuerySniffer \(Windows\)](#)

---

## 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

The screenshot shows the Wireshark application window. The title bar reads "The V". The menu bar includes "File", "Edit", "View", "Go", "Capture", "Analyze", "Statistics", and "Tools". The toolbar contains icons for menu, refresh, capture, display filter, packet list, packet bytes, packet details, packet raw, search, and back. Below the toolbar is a "Filter:" input field. The main area has a blue header "Capture" and a sub-header "Interface List". Under "Interface List" is a description: "Live list of the capture interfaces (counts incoming packets)". Below that is a "Start" button with a red circle icon and the text "Choose one or more interfaces to capture from, then **Start**". A list of interfaces is shown below, each with a checkbox and a small icon: "Thunderbolt Bridge: bridge0", "utun0", "p2p0", "Thunderbolt 1: en6", "Thunderbolt 2: en7", and "Loopback: lo0". The "Loopback: lo0" entry is highlighted with an orange box, and a large orange arrow points to it from the right.

Development Version  
**WIRESHARK**

The World's Most  
Version 1.9.2 (SVN Rev

## Capture

### Interface List

Live list of the capture interfaces  
(counts incoming packets)

### Start

Choose one or more interfaces to capture from, then **Start**

- Thunderbolt Bridge: bridge0
- utun0
- p2p0
- Thunderbolt 1: en6
- Thunderbolt 2: en7
- Loopback: lo0

Sólo DNS

Si sólo desea ver las solicitudes DNS.

Filter: `dns`

DNS + HTTP

Si sólo desea consultar la solicitud de DNS y HTTP.

Filter: `dns or 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:

Filter: `dns && not dns contains debug.opendns.com`

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

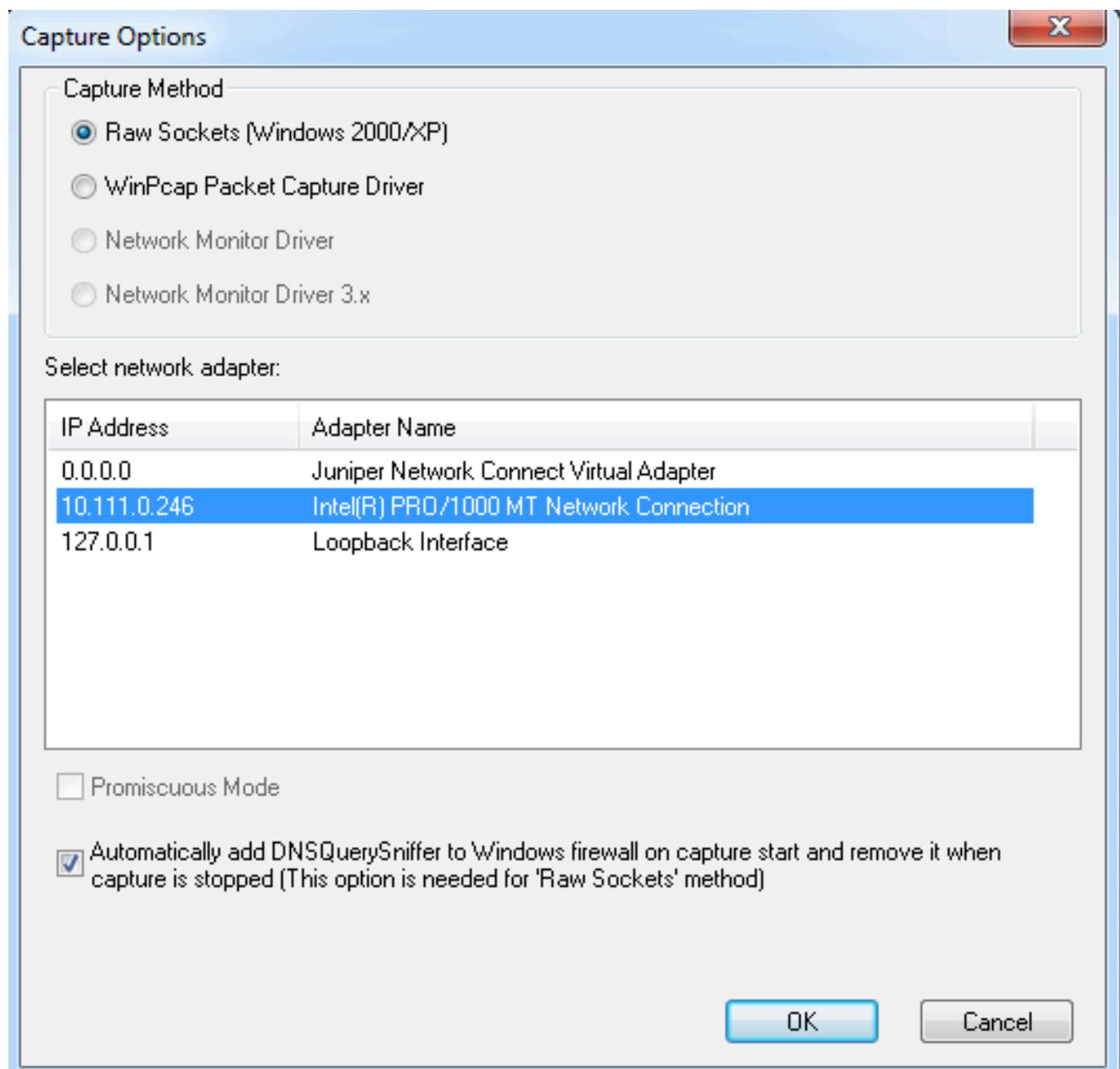
## DNSQuerySniffer (Windows)

[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.

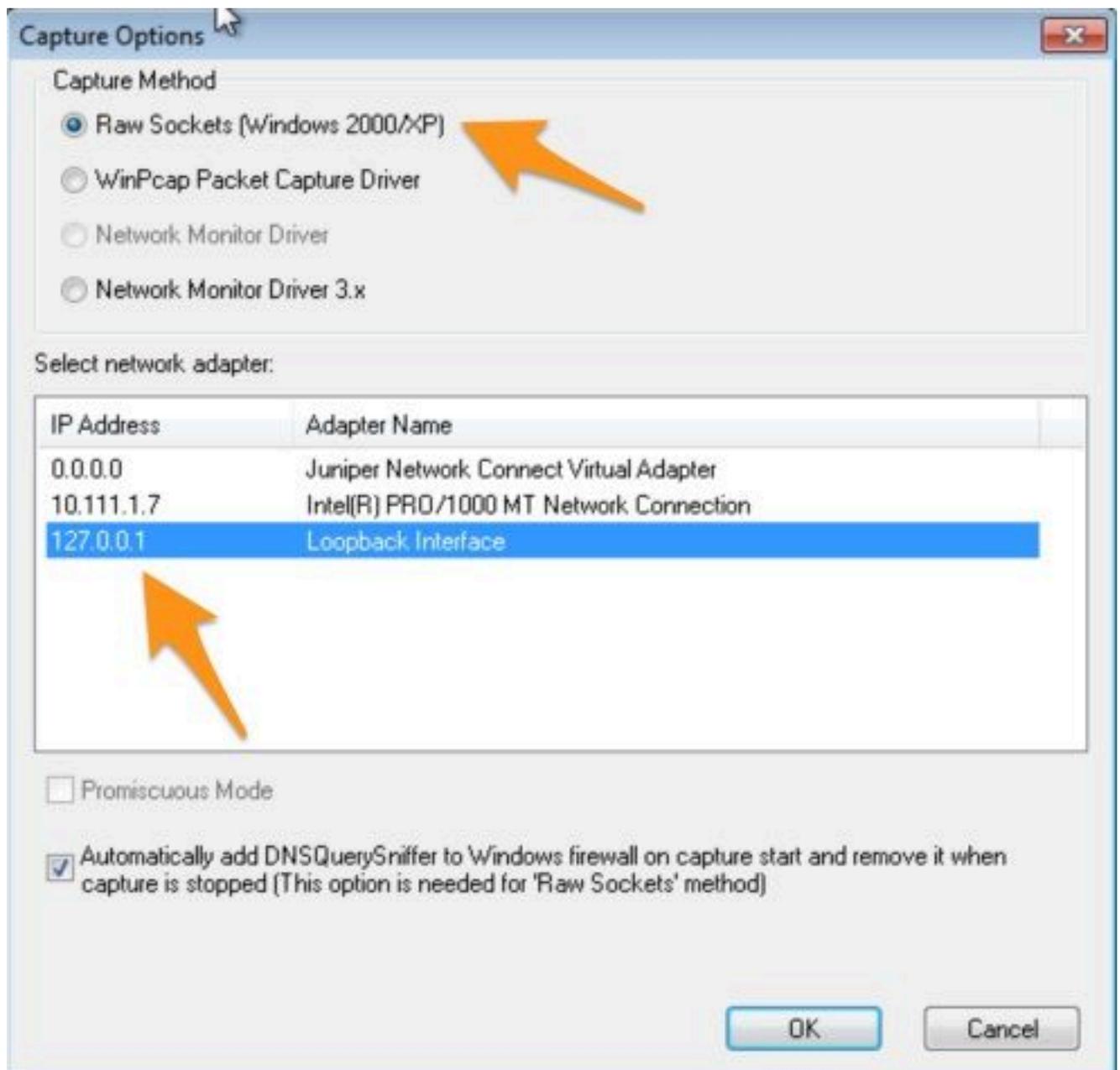
Existen dos métodos de captura:

- 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.





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
127.0.0.1	127.0.0.1

Los resultados son los siguientes:

Host Name	Port	Queue	Request	Request Time	Response Time	Duration	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 74.125.239.143
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 74.125.239.143
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 54.230.117.151
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	4887	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 54.230.117.151
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

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).