Captura de tráfico de red con Wireshark

Contenido

Introducción

Este documento describe cómo capturar el tráfico de red con Wireshark.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Umbrella DNS Layer Security.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

En ocasiones, el personal de Cisco Umbrella Support solicita una captura de paquetes del tráfico de Internet que fluye entre el ordenador y la red. La captura permite al soporte de Umbrella analizar el tráfico a un nivel bajo e identificar posibles problemas.

En la mayoría de los casos, es útil comparar dos conjuntos de capturas de paquetes que

muestran un escenario de funcionamiento y otro de no funcionamiento.

- Asegúrese de que puede replicar el problema y completar estos pasos mientras se produce el problema. Genere una captura de paquetes que muestre un escenario de no funcionamiento. Tenga en cuenta la fecha y la hora con la zona horaria para que esta información se pueda correlacionar con otros datos.
- Si es posible, repita estas instrucciones con el software Umbrella (o el reenvío de DNS de Umbrella) deshabilitado. Genere una captura de paquetes que muestre el escenario de trabajo. Tenga en cuenta la fecha y la hora con la zona horaria para que esta información se pueda correlacionar con otros datos.

Instrucciones de Wireshark

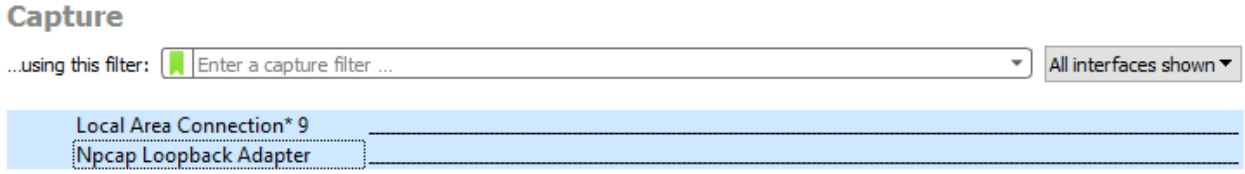
Preparativos

1. Descargue Wireshark.
2. Desconecte las conexiones de red innecesarias.
    1. Desconecte las conexiones VPN a menos que sean necesarias para replicar el problema.
    2. Utilice únicamente conexiones por cable o inalámbricas y no ambas a la vez.
3. Cierre cualquier otro software que no sea necesario para replicar el problema.
4. Borre las cookies y la caché de su navegador.
5. Vaciar la caché DNS. En Windows con el comando:

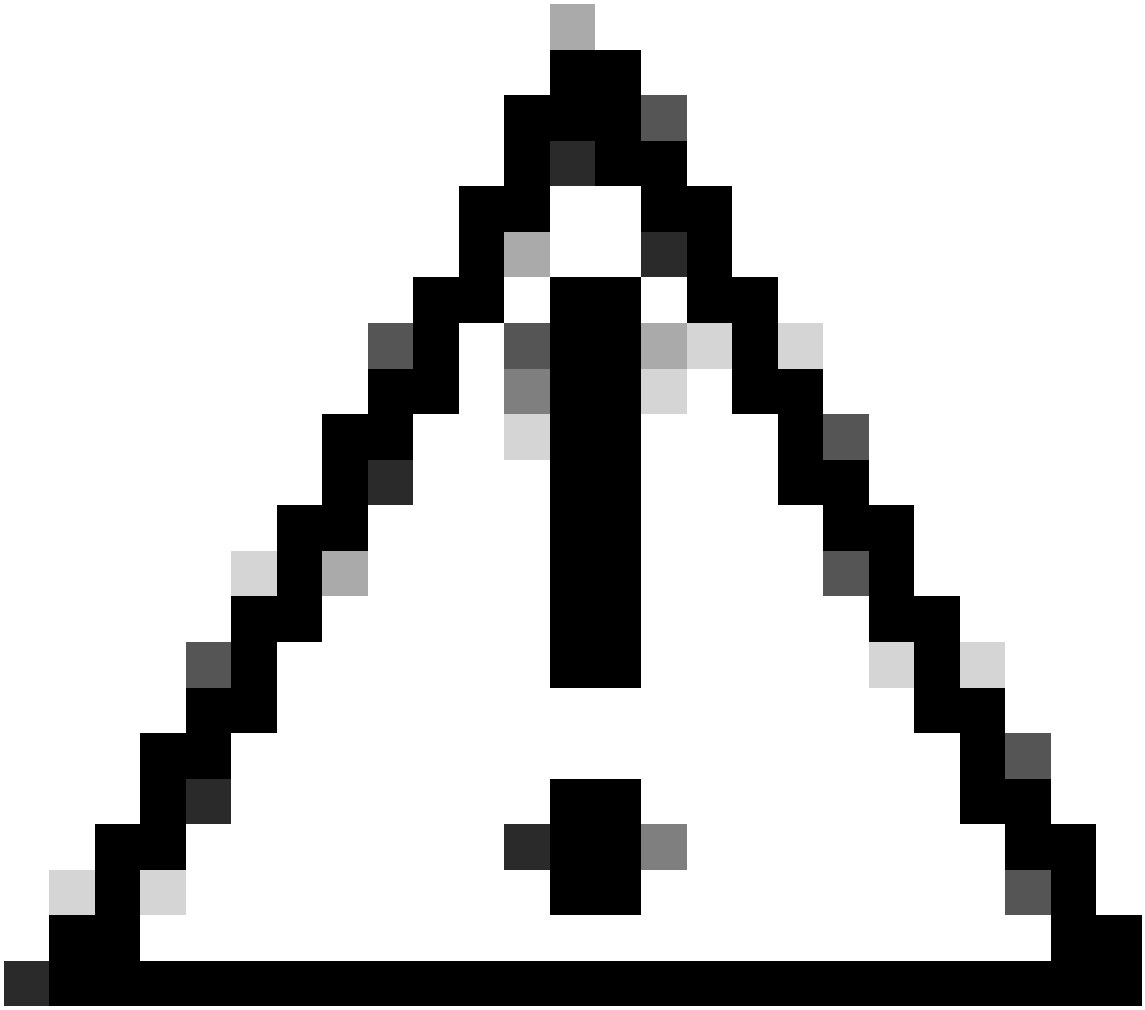
```
ipconfig /flushdns
```

Captura básica de Wireshark

1. Inicie Wireshark.
2. El panel Capturar muestra las interfaces de red. Seleccione las interfaces relevantes. Se pueden seleccionar varias interfaces mediante la tecla CTRL (Windows) o la tecla CMD (Mac) mientras se selecciona.

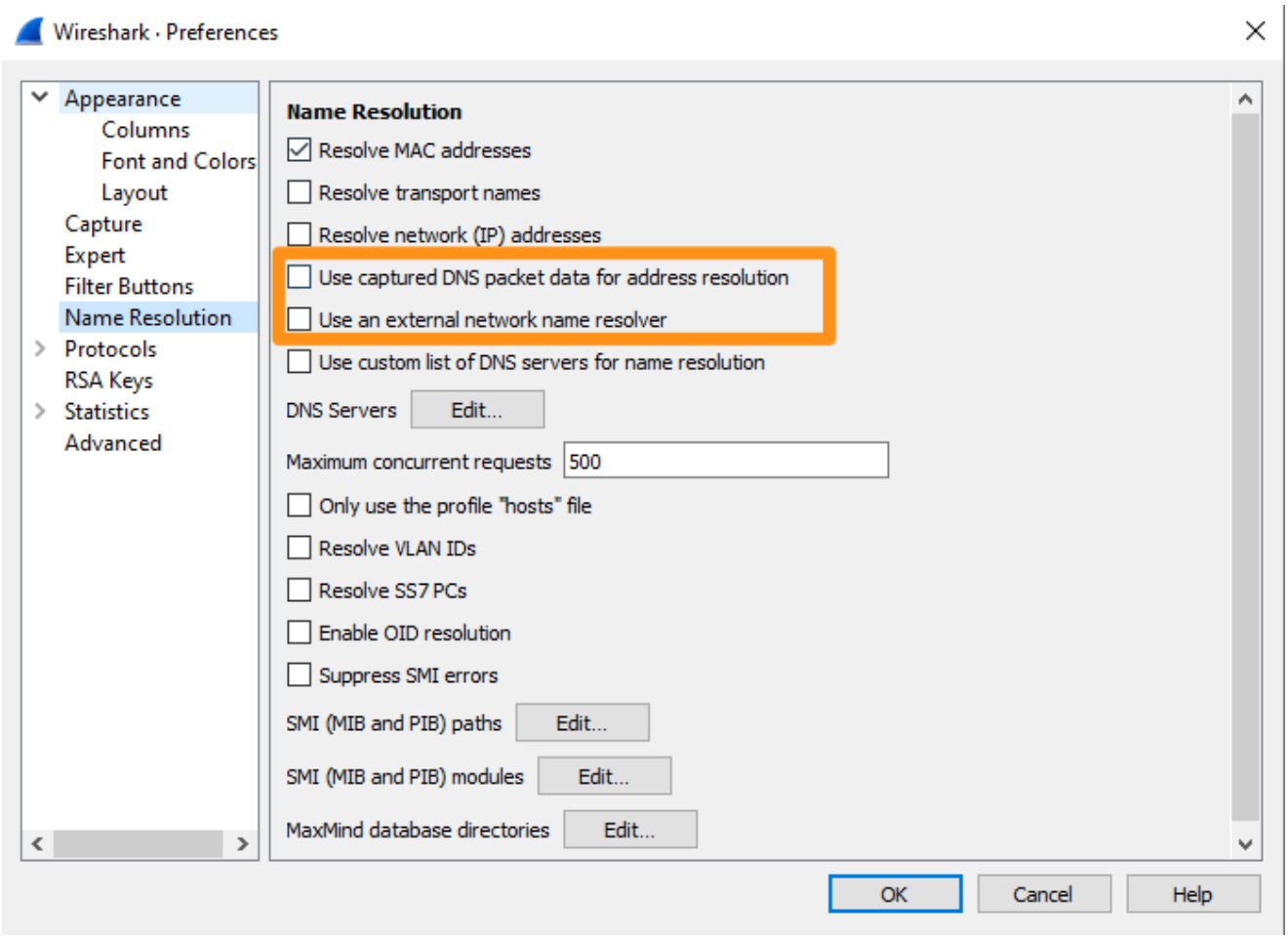


wireshark_1.png



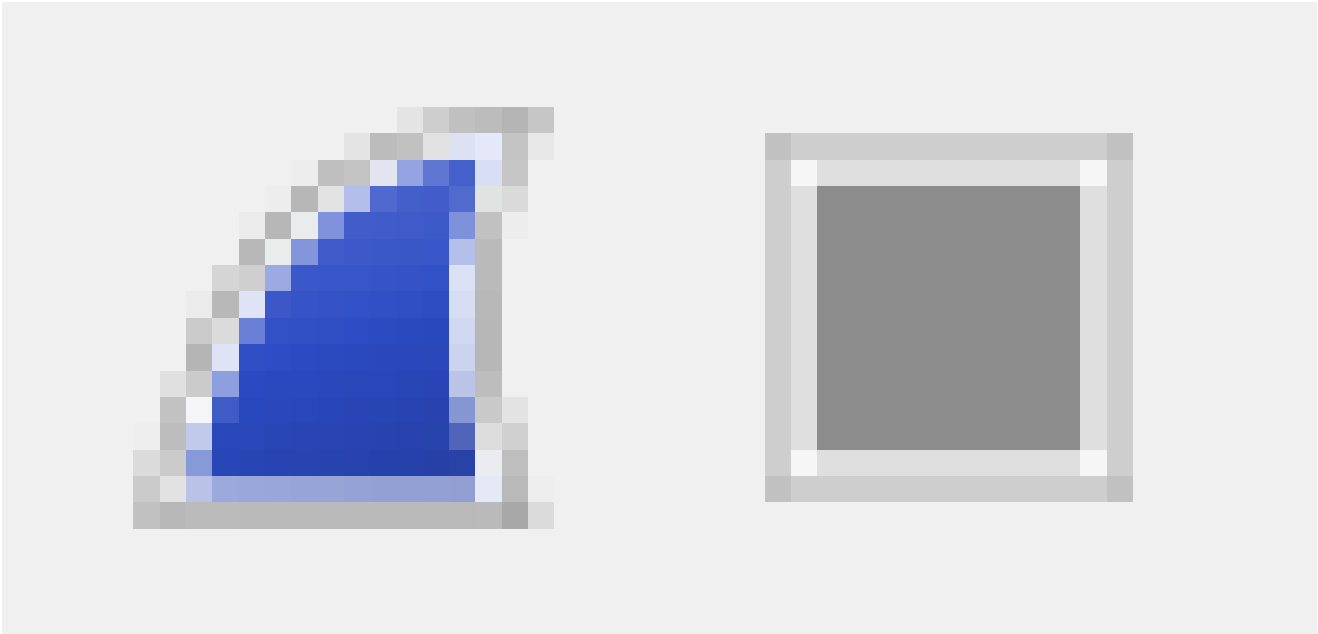
Precaución: Es importante seleccionar las interfaces correctas que contienen tráfico de red. Utilice el comando "ipconfig" (Windows) o el comando "ifconfig" (Mac) para ver más detalles sobre las interfaces de red. Los usuarios del cliente de roaming deben seleccionar adicionalmente el adaptador de loopback NPCAP O loopback: lo0 interfaces. En caso de duda, seleccione todas las interfaces.

3. Asegúrese de que las opciones Usar datos de paquetes DNS capturados para la resolución de direcciones y Usar una resolución de nombres de red externa estén seleccionadas NO para asegurarse de que Wireshark no realiza consultas DNS, ya que esto puede complicar la captura y afectar a AnyConnect. La configuración es válida a partir de Wireshark 3.4.9:



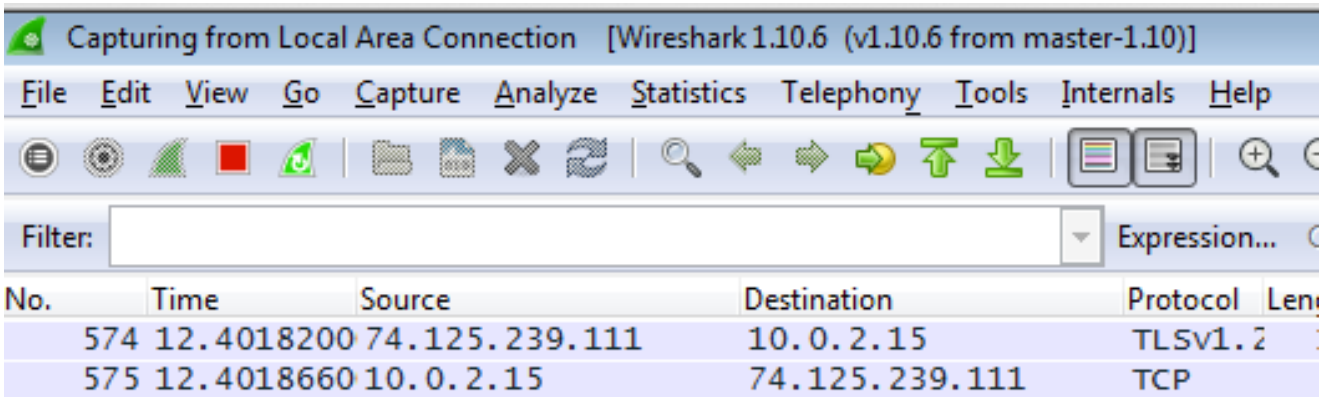
Capture_PNG.png

4. Seleccione Capture > Start o seleccione el icono de inicio azul.



wireshark_2.png

5. Mientras Wireshark se ejecuta en segundo plano, replique el problema.



wireshark_3.png

6. Una vez que el problema se haya replicado completamente, seleccione Capture > Stop o utilice el icono rojo Stop.
7. Navegue hasta Archivo > Guardar como y seleccione un lugar para guardar el archivo. Asegúrese de que el archivo se guarda como un tipo PCAPNG. El archivo guardado se puede enviar a soporte técnico de Cisco Umbrella para su revisión.

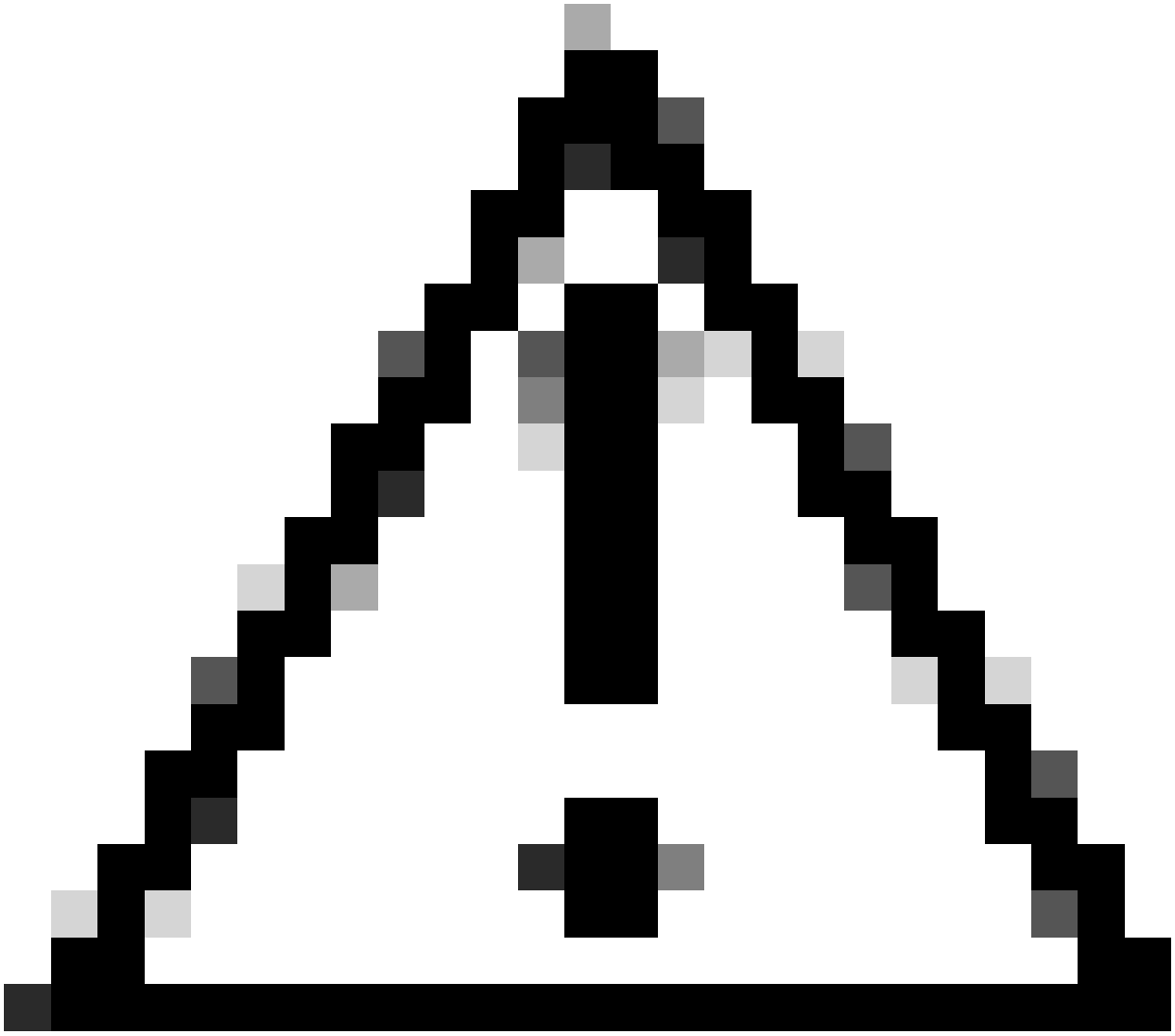
Cliente de roaming: pasos adicionales

Hay pasos adicionales que deben completarse para los usuarios independientes del cliente de roaming y del módulo de roaming de AnyConnect:

Tráfico de loopback

Al seleccionar una interfaz, también debe capturar el tráfico en la interfaz de loopback (127.0.0.1) además de otras interfaces de red. El proxy DNS del cliente de roaming escucha en esta interfaz, por lo que es vital ver el tráfico que circula entre el sistema operativo y el cliente de roaming.

- Windows: Seleccione NPCAP Loopback Adapter
- Mac: Seleccione Loopback: lo0



Precaución: Las versiones más recientes de Wireshark para Windows incluyen el controlador de captura NPCAP, que admite el controlador de loopback. Si falta el adaptador de loopback, actualice a la última versión de Wireshark o siga las instrucciones de rawcap.exe.

Tráfico DNS cifrado

En circunstancias normales, el tráfico entre el cliente de roaming y Umbrella está cifrado y no es legible por las personas. En algunos casos, la compatibilidad con Umbrella puede solicitar que desactive el cifrado DNS para ver el tráfico DNS entre el cliente de roaming y la nube de Umbrella. Hay dos métodos para hacer esto:

- Cree un bloque de firewall local para UDP 443 a 208.67.220.220 y 208.67.222.222.
- O bien, cree el archivo en función de su sistema operativo y de la versión del cliente de roaming:
    - Windows:

```
C:\ProgramData\OpenDNS\ERC\force_transparent.flag
```

- Windows AnyConnect:

  `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\force_transparent`

- Cliente seguro de Windows:

  `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\force_transparent.flag`

- macOS:

  `/Library/Application Support/OpenDNS Roaming Client/force_transparent.flag`

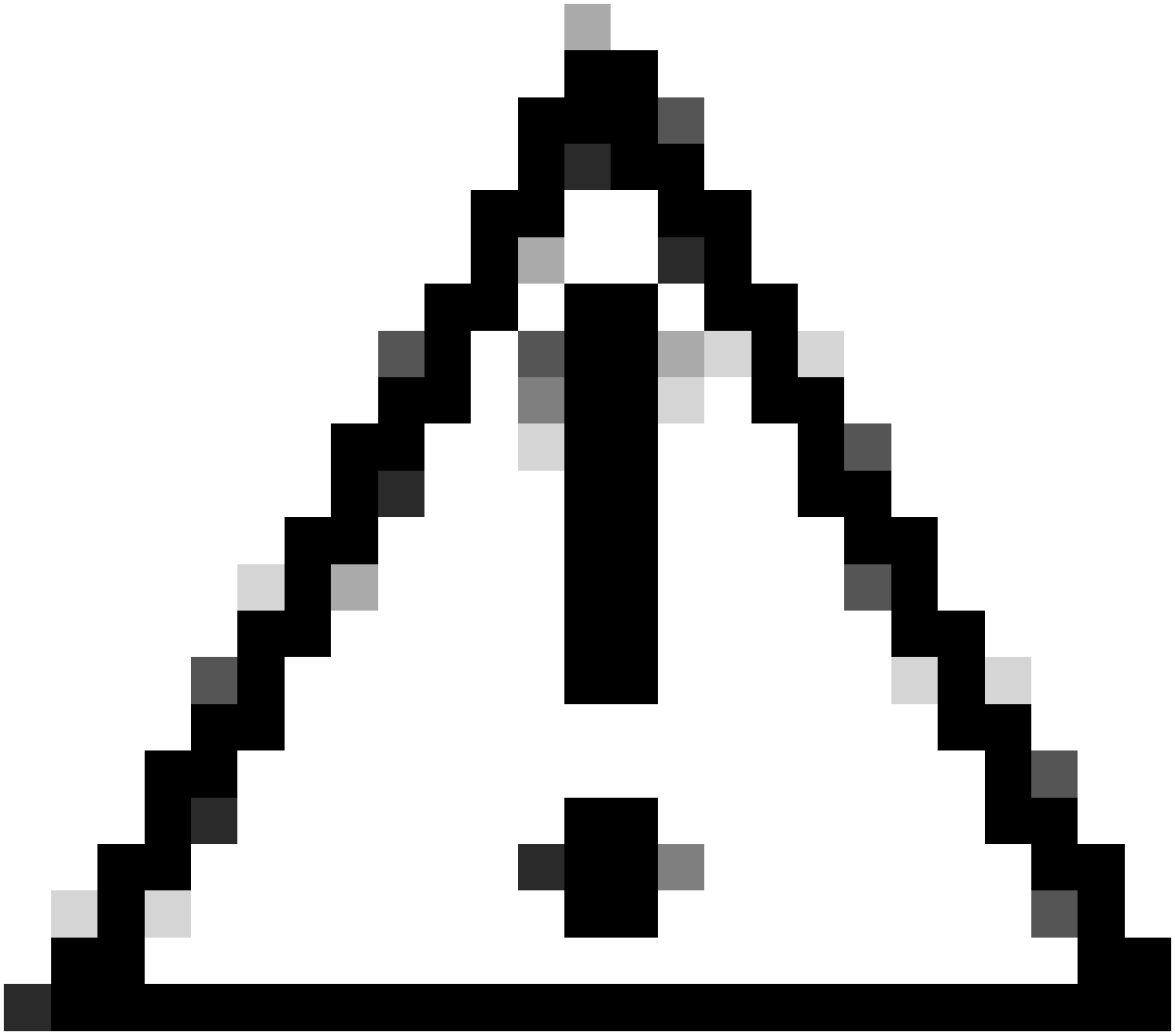
- Mac OS AnyConnect:

  `/opt/cisco/anyconnect/umbrella/data/force_transparent.flag`

- Mac OS Secure Client:

  `/opt/cisco/secureclient/umbrella/data/force_transparent.flag`

Después de hacer esto, reinicie el servicio o el equipo.



Precaución: Las versiones más recientes de Wireshark en Windows incluyen el controlador de captura NPCAP , que no es compatible con la interfaz VPN de Umbrella. En Windows, puede que necesite utilizar la herramienta rawcap.exe como alternativa.

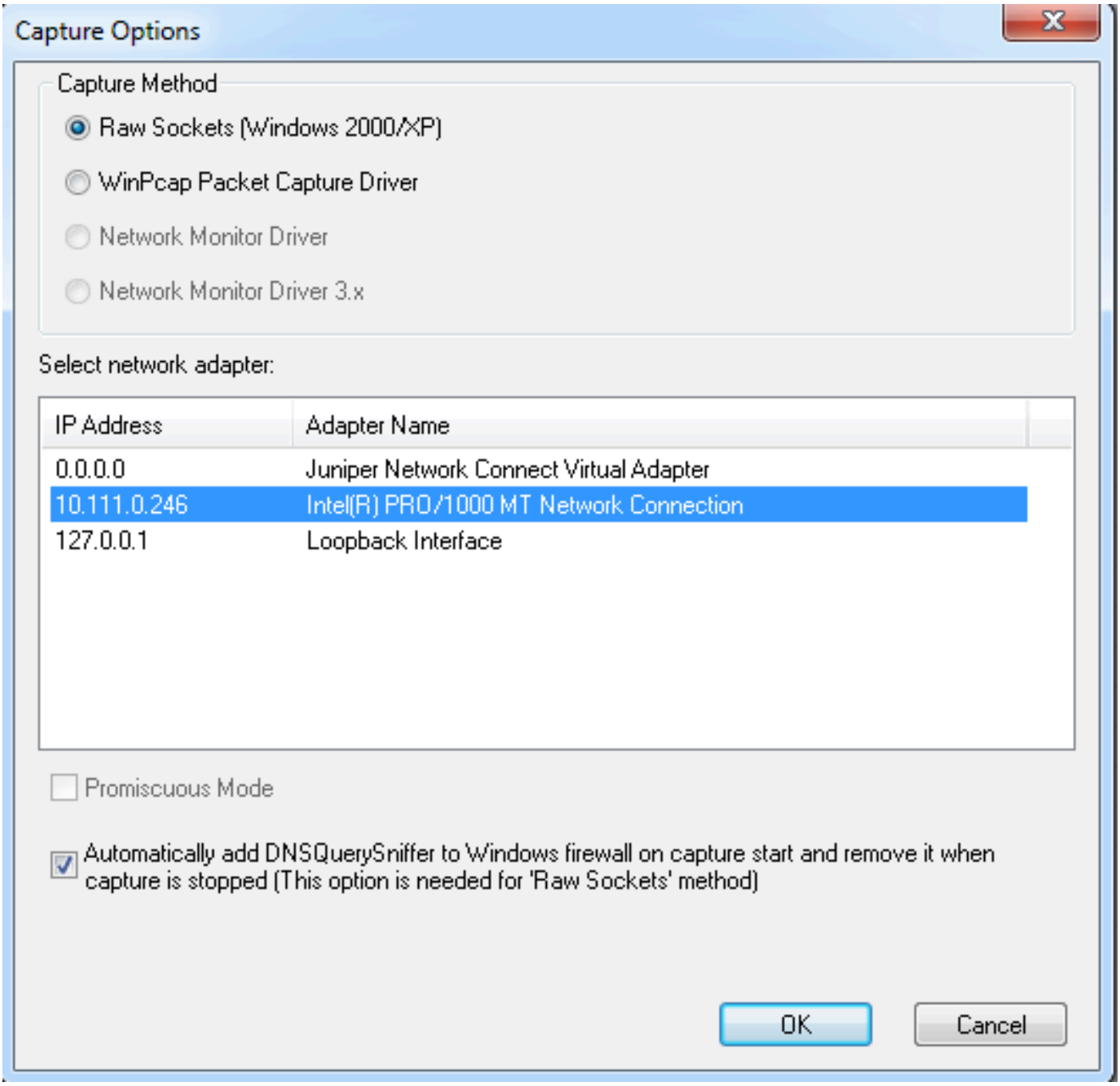
DNSQuerySniffer: alternativa de Windows

DNSQuery Sniffer es un rastreador de red solo DNS para Windows que supervisa 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.

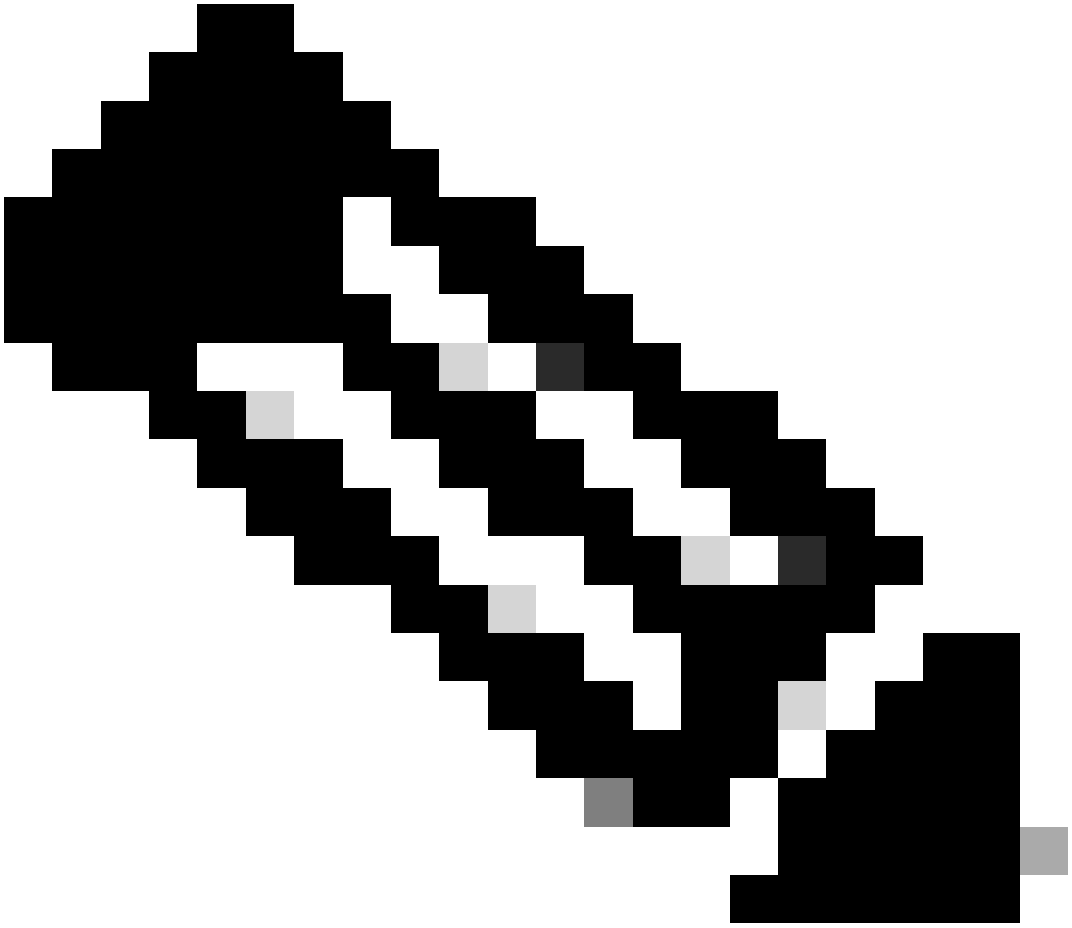
Se trata de una herramienta ligera y fácil de usar. Una ventaja de utilizar esto es que puede olfatear paquetes mientras el servicio Roaming Client está inhabilitado, iniciar la captura y puede ver cada consulta DNS que el cliente Roaming envía desde el momento en que se inicia en lugar de iniciar una captura después de que el cliente Roaming ya se haya iniciado.

Existen dos métodos de captura:

1. Si selecciona la interfaz de red normal, sólo podrá ver las consultas que se encuentren en la lista Dominios internos o que no hayan pasado específicamente a través de dnscryptproxy.



dns_1.png

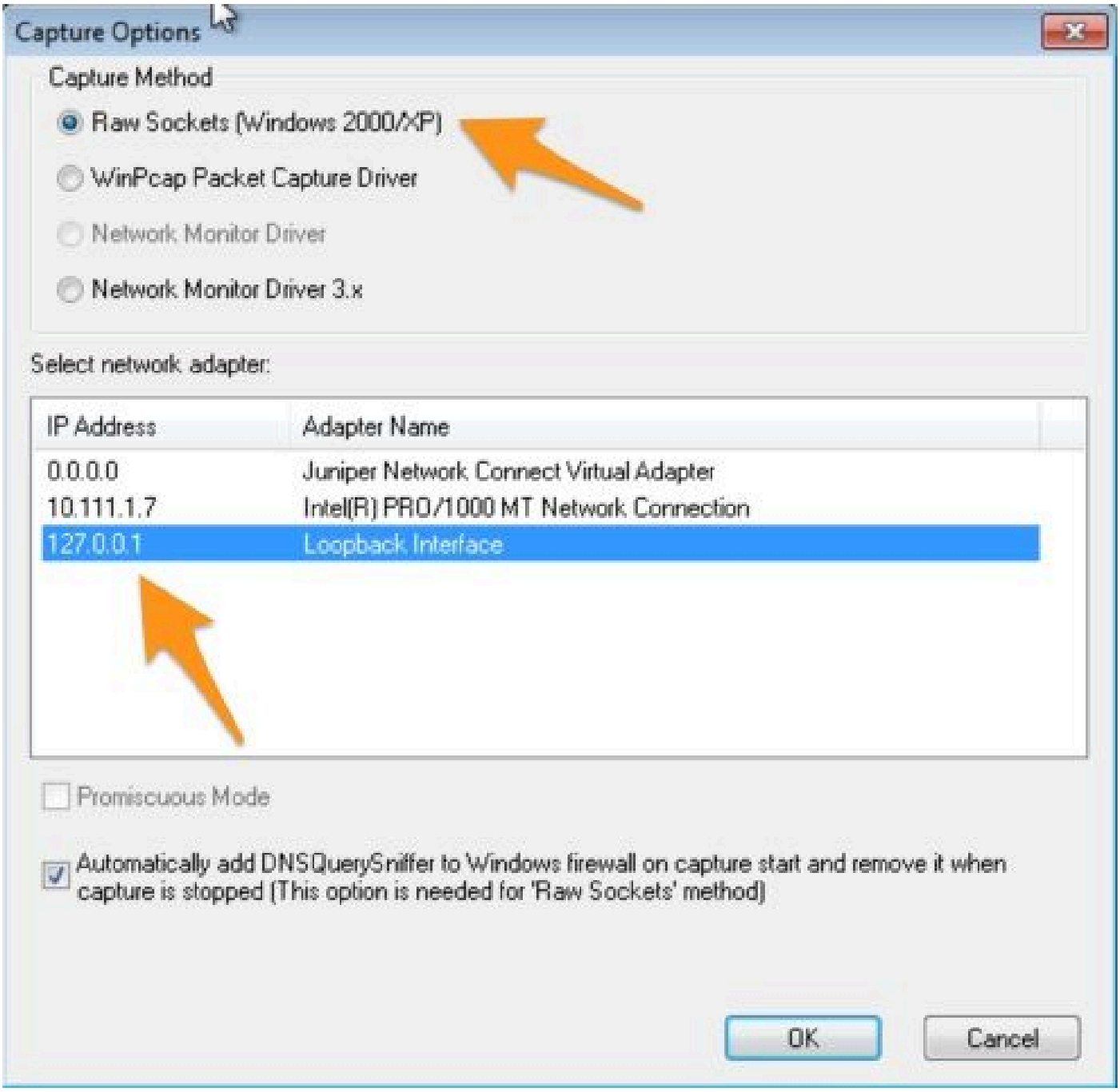


Nota: Estas columnas aparecen a la derecha de la captura y hay que desplazarse un poco para verlas.

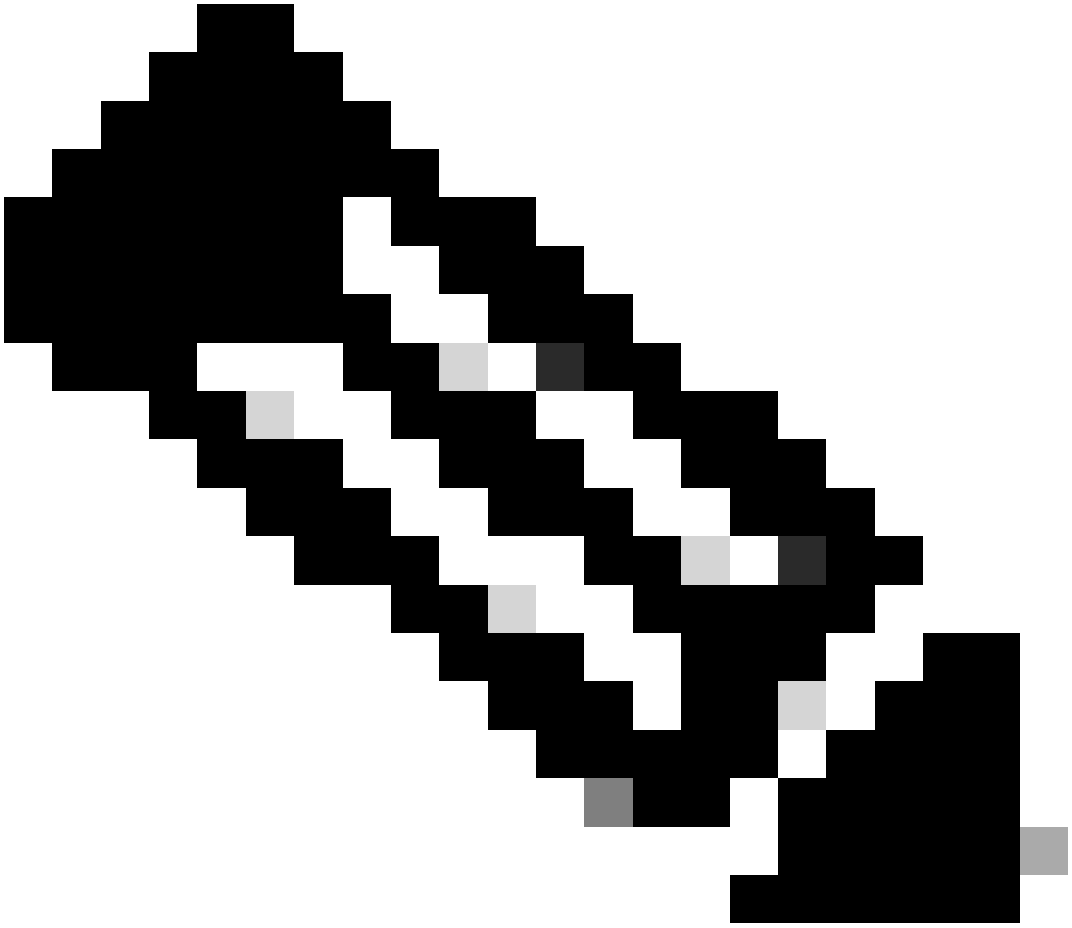
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

Columnas DNSSniffer

2. Si selecciona la interfaz Loopback, verá todas las consultas DNS que se envían a través del dnscryptproxy, pero no podrá ver la dirección IP de destino verdadera para los dominios en la lista Dominios internos. Sin embargo, sigue mostrando la consulta y la respuesta.


Capture Options
Capture Method
Raw Sockets (Windows 2000/XP)
WinPcap Packet Capture Driver
Network Monitor Driver
Network Monitor Driver 3.x
Select network adapter:
IP Address
Adapter Name
0.0.0.0
Juniper Network Connect Virtual Adapter
10.111.1.7
Intel(R) PRO/1000 MT Network Connection
127.0.0.1
Loopback Interface
Promiscuous Mode
Automatically add DNSQuerySniffer to Windows firewall on capture start and remove it when capture is stopped (This option is needed for 'Raw Sockets' method)
OK
Cancel

dns_2.jpg

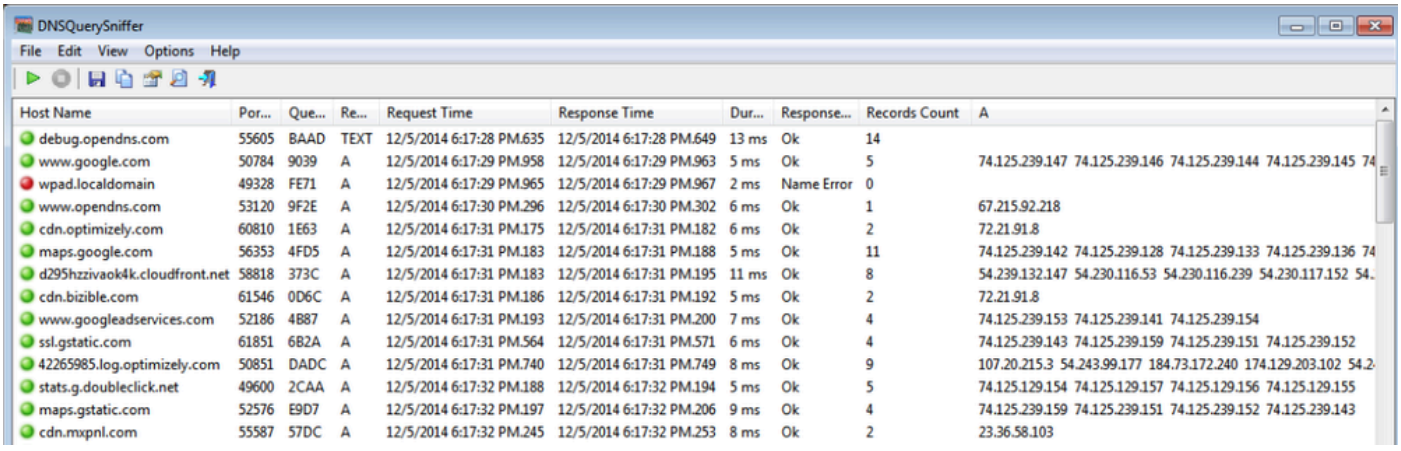


Nota: Estas columnas aparecen a la derecha de la captura y hay que desplazarse un poco para verlas.

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

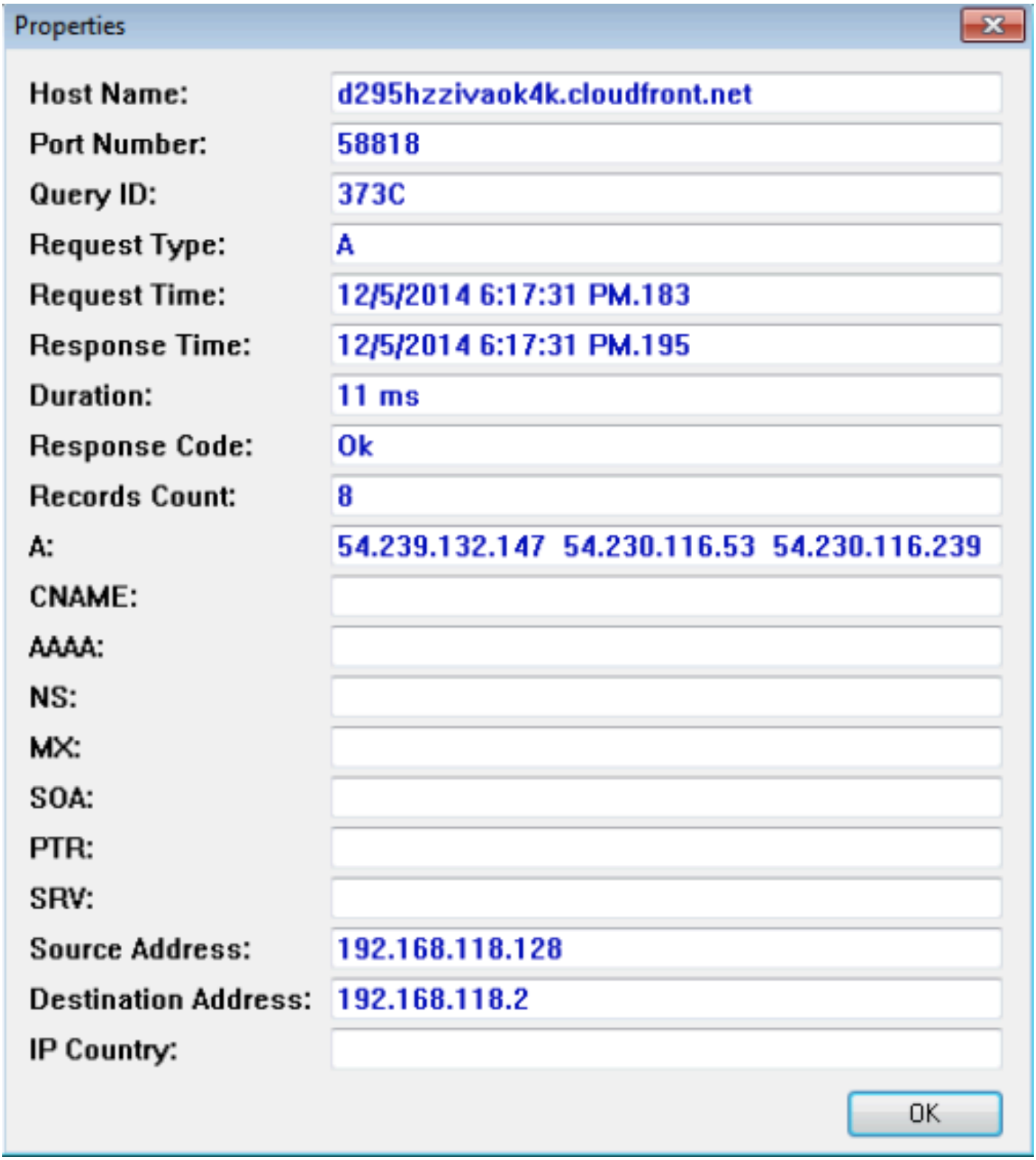
Columnas DNSSniffer

Los resultados son los siguientes:



dns_3.png

Vista de una búsqueda individual:



dns_4.png

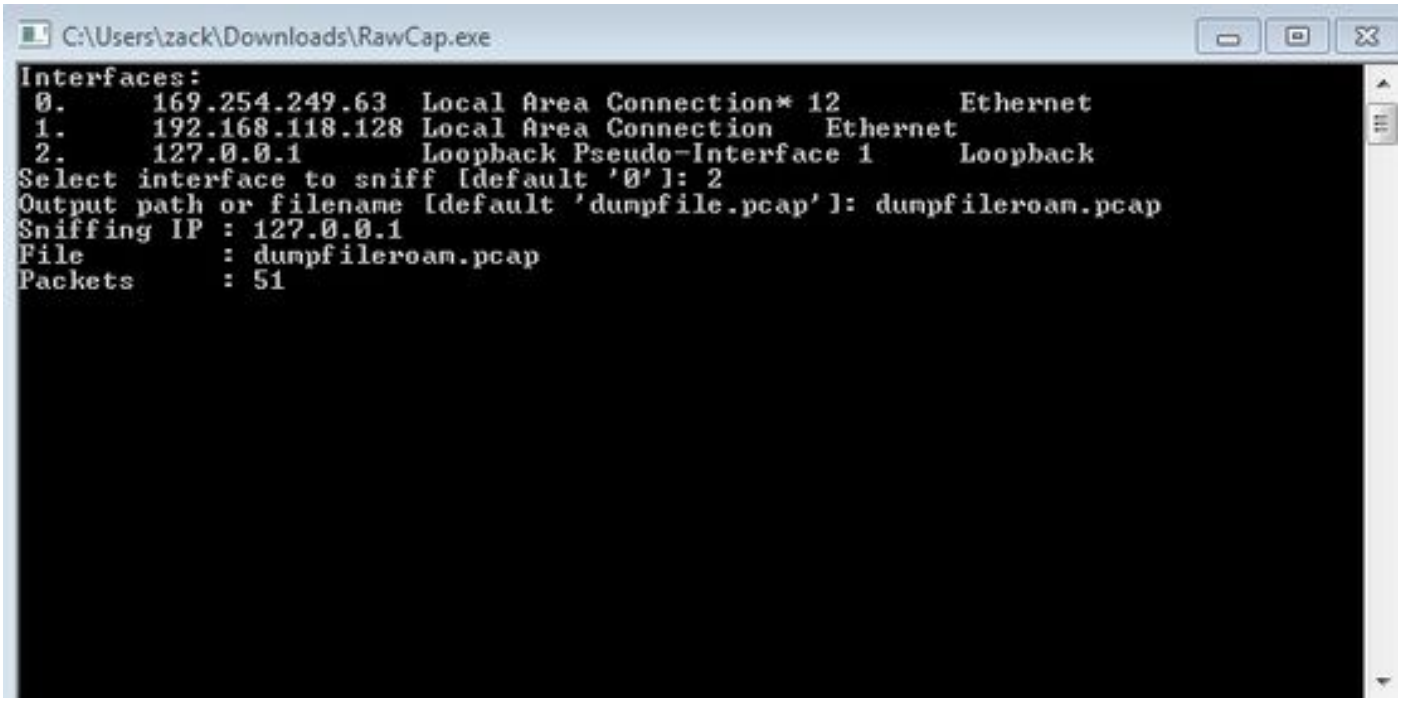
RawCap.exe: alternativa de Windows

En algunas circunstancias, el controlador de captura de paquetes incluido con Wireshark no admite la interfaz con la que debe trabajar. Esto puede ser un problema para la interfaz de loopback.

En estos casos, podemos utilizar RawCap.exe:

1. Complete los pasos descritos anteriormente en el artículo para utilizar Wireshark para capturar el tráfico normal.
2. Al mismo tiempo, ejecute RawCap.exe.
3. Seleccione la interfaz especificando el número de lista correspondiente.
4. Especifique un nombre de archivo de salida y desaparecerá.
5. Seleccione Control-Ccuando desee detener la captura.

El archivo guardado se coloca en la carpeta desde la que se ejecutó RawCap.exe:



rawcap_1.jpg

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).