使用Wireshark捕获网络流量

目录

简介

本文档介绍如何使用Wireshark捕获网络流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella DNS层安全。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

有时，Cisco Umbrella支持人员会要求捕获计算机与网络之间流动的互联网流量的数据包。捕获功能允许Umbrella支持从低级别分析流量并识别潜在问题。

在大多数情况下，比较两组数据包捕获来演示工作场景和非工作场景非常有用。

- 确保您可以在问题发生时复制问题并完成以下步骤。 生成显示非工作场景的数据包捕获。请记下时区的日期和时间，以便此信息可与其他数据关联。

- 如果可能，在禁用Umbrella软件（和/或Umbrella DNS转发）的情况下重复这些说明。 生成显示工作场景的数据包捕获。 请记下时区的日期和时间，以便此信息可与其他数据关联。

Wireshark说明

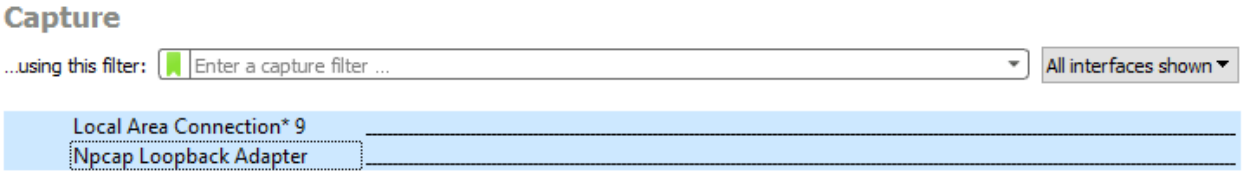
准备

1. 下载Wireshark。
2. 断开所有不必要的网络连接。
    1. 断开VPN连接，除非需要它们来复制问题。
    2. 仅使用有线或无线连接，不能同时使用两者。
3. 关闭不需要复制问题的任何其他软件。
4. 从浏览器中清除Cookie和缓存。
5. 刷新DNS缓存。在Windows上使用命令：

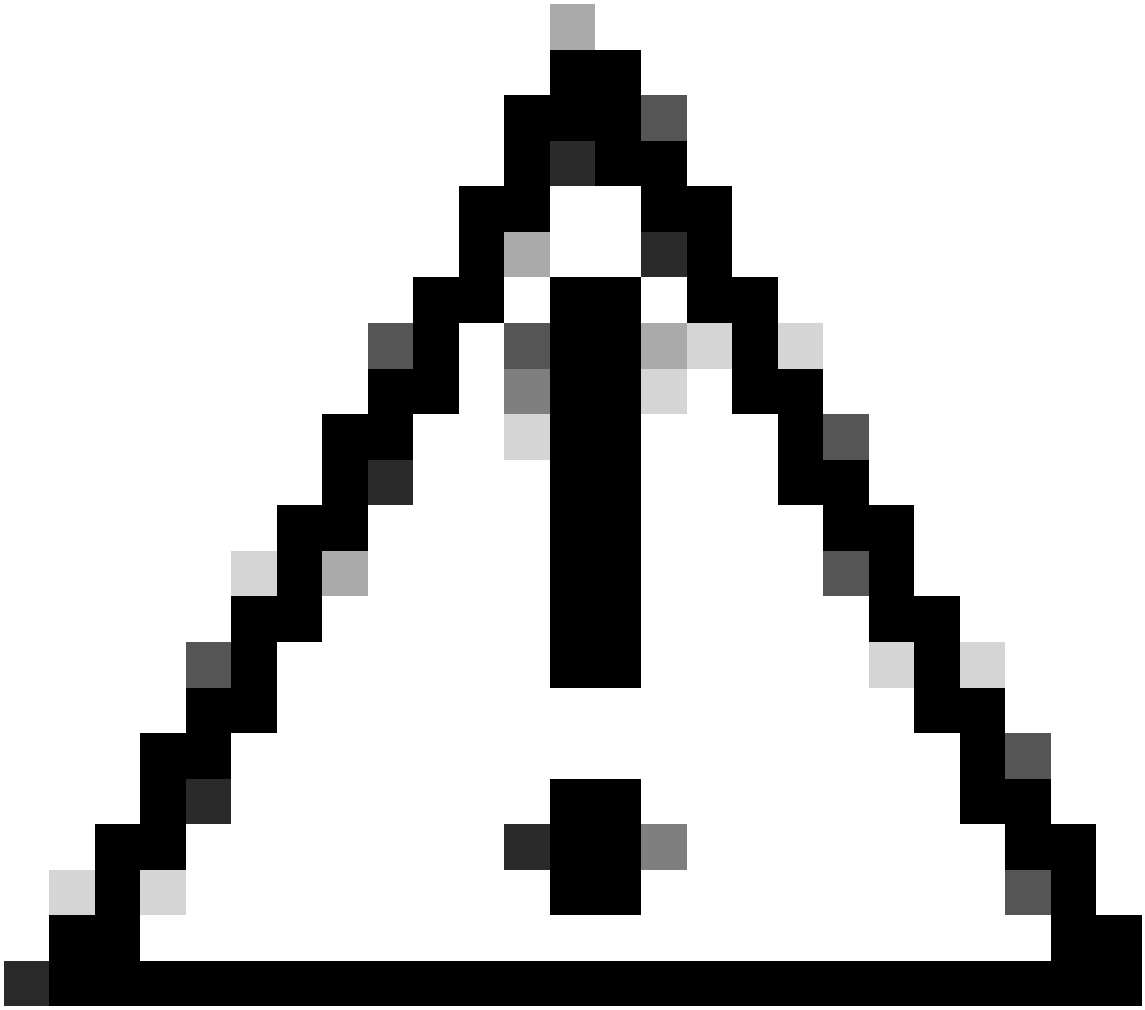
```
ipconfig /flushdns
```

基本Wireshark捕获

1. 启动 Wireshark。
2. Capture面板显示网络接口。选择相关接口。 在选择时，可以使用CTRL键(Windows)或CMD键(Mac)选择多个接口。

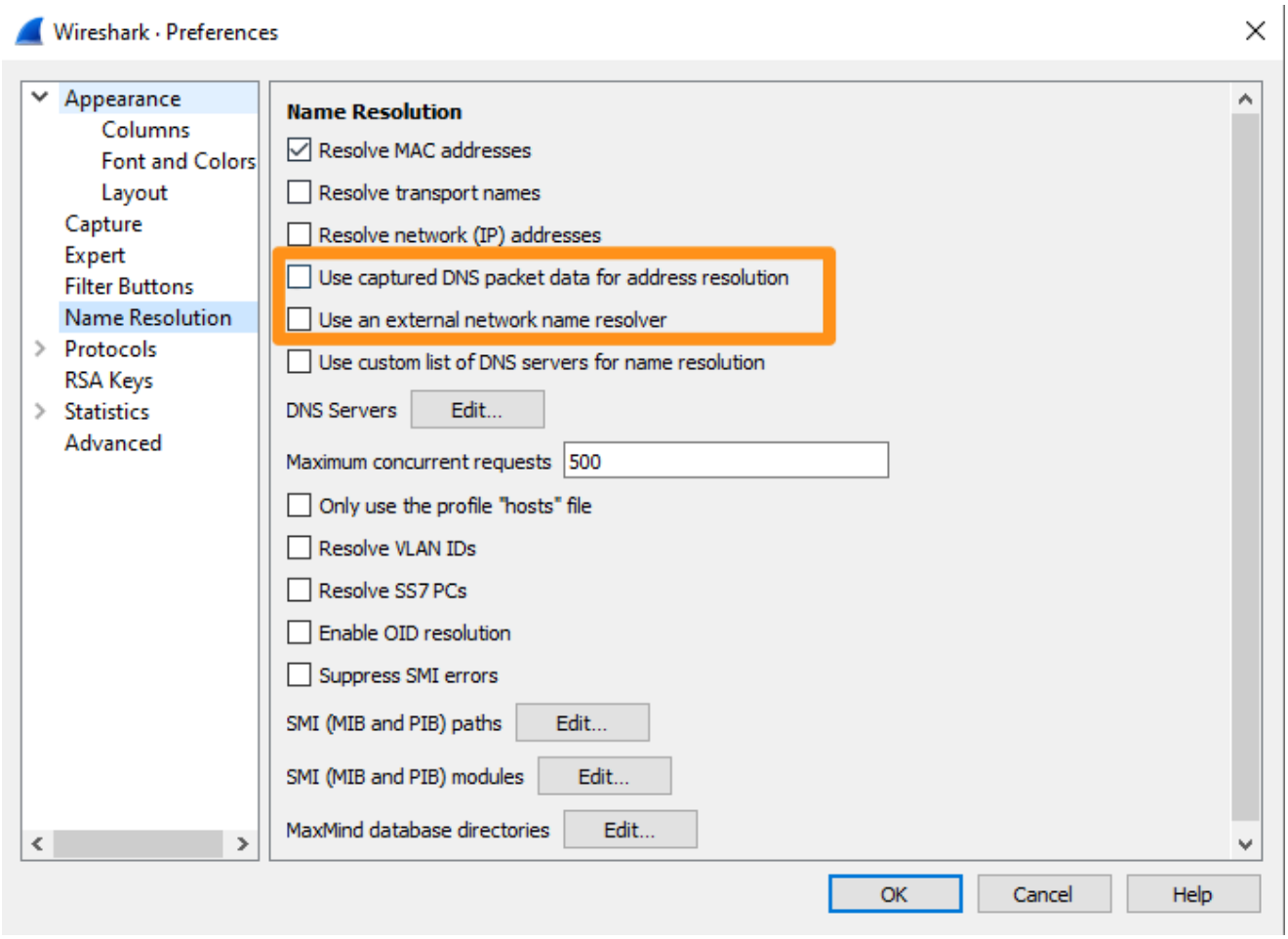


wireshark_1.png



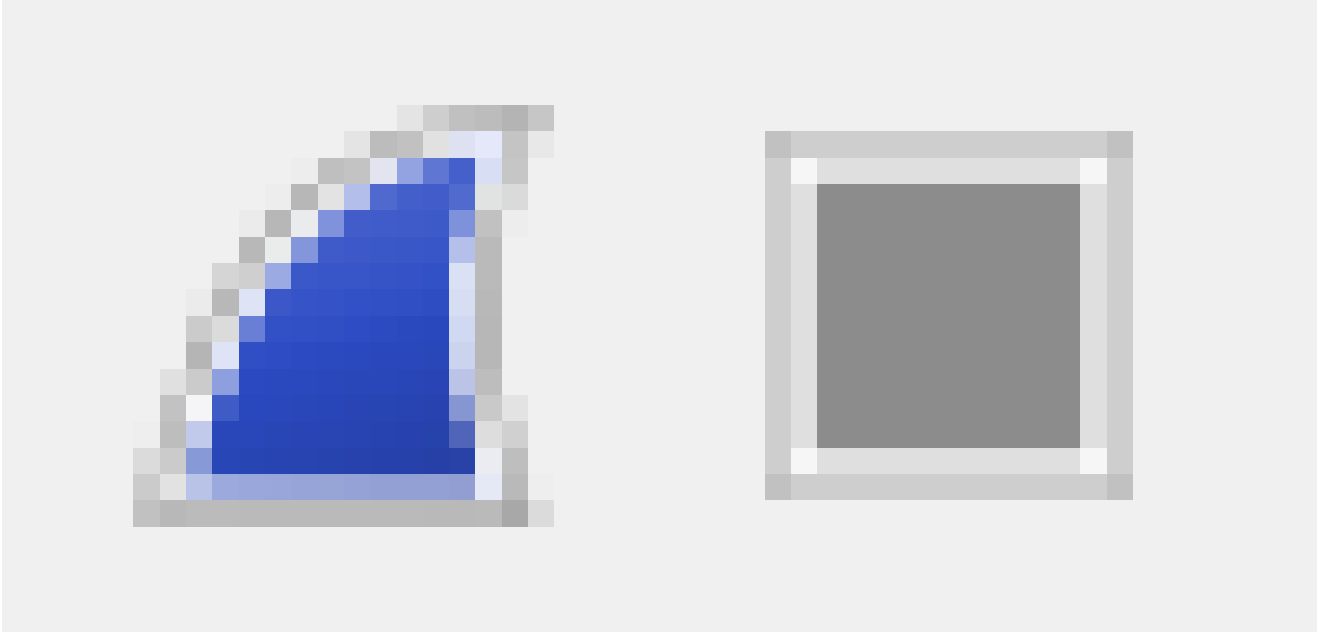
警告：选择包含网络流量的正确接口非常重要。 使用“ipconfig”命令(Windows)或“ifconfig”命令(Mac)查看有关网络接口的详细信息。漫游客户端用户必须额外选择NPCAP环回适配器或环回：lo0接口。如有疑问，请选择所有接口。

3. 确保未选择Use captured DNS packet data for address resolution和Use an external network name resolver以确保Wireshark不会进行DNS查询，因为这会使捕获变得复杂并影响AnyConnect。设置自Wireshark 3.4.9起有效：



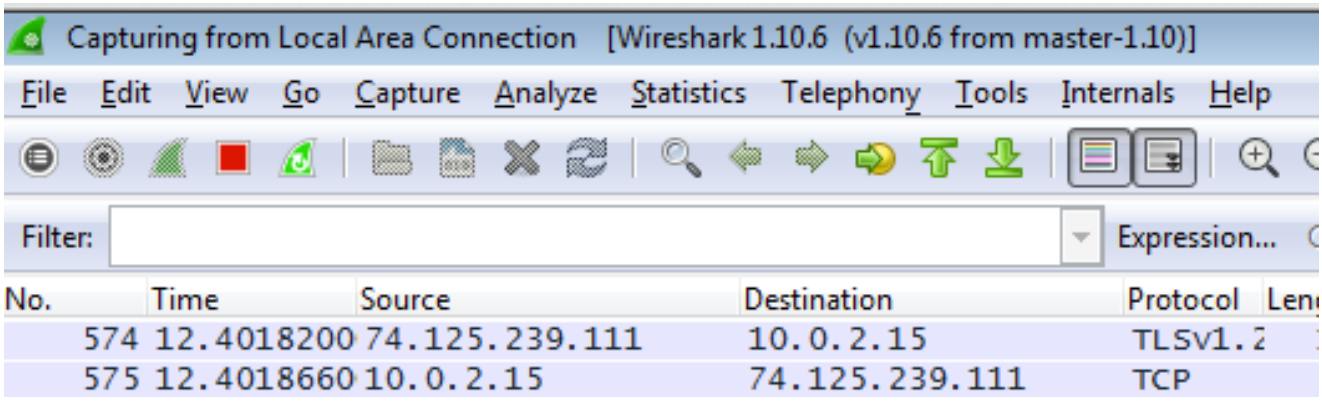
Capture_PNG.png

4. 选择Capture > Start或选择Blue start图标。



wireshark_2.png

5. 当Wireshark在后台运行时，重现问题。



wireshark_3.png

6. 问题完全复制后，选择Capture > Stop或使用红色的Stop图标。
7. 导航到文件>另存为，然后选择要保存文件的位置。确保文件保存为PCAPNG类型。 保存的文件可以提交给Cisco Umbrella支持部门进行审核。

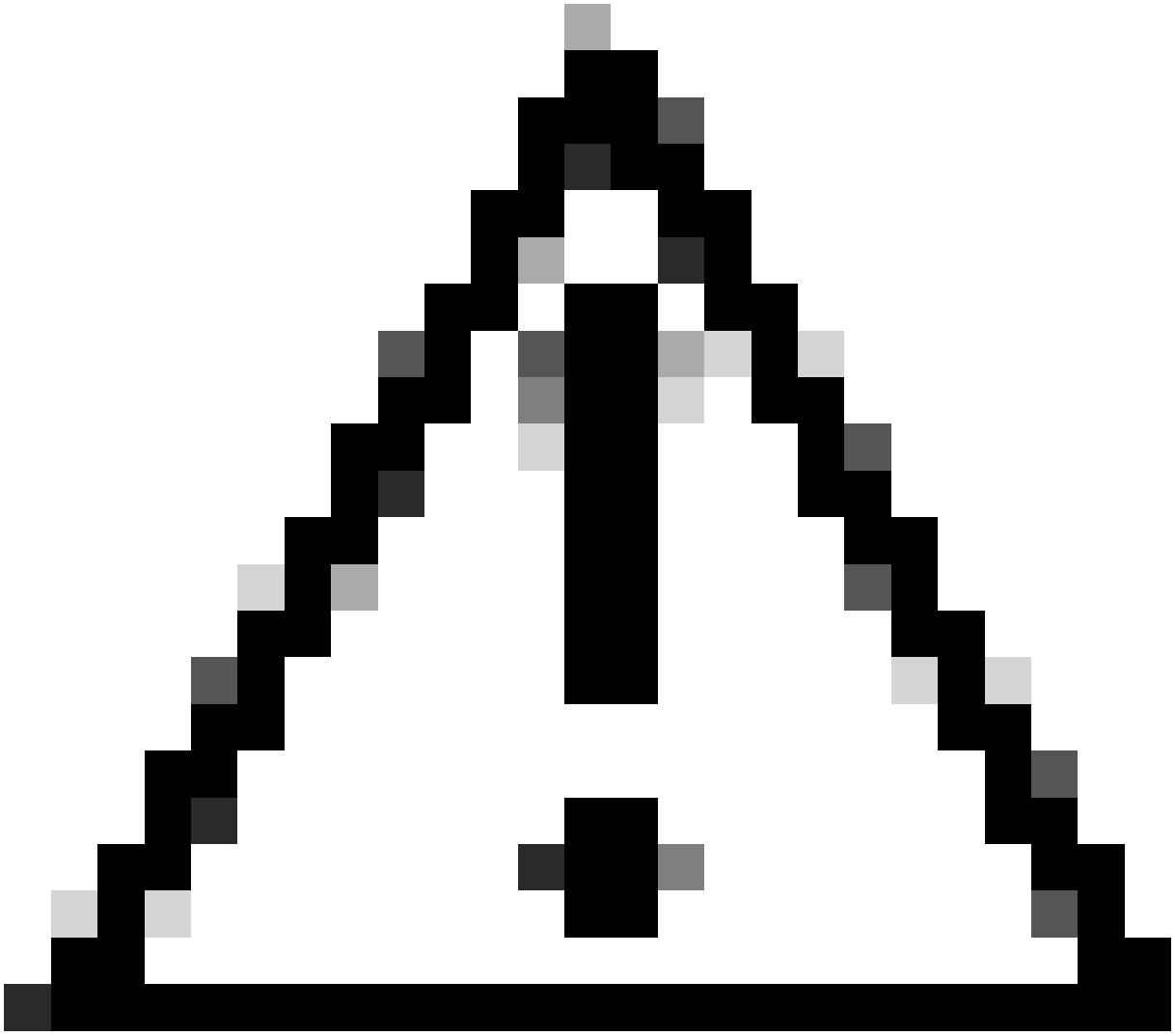
漫游客户端 — 附加步骤

对于独立漫游客户端和AnyConnect漫游模块用户，还必须完成以下附加步骤：

环回流量

选择接口时，除了捕获其他网络接口外，还必须捕获环回接口(127.0.0.1)上的流量。漫游客户端的DNS代理在此接口上侦听，因此查看操作系统和漫游客户端之间的流量至关重要。

- Windows 窗口版本:选择NPCAP环回适配器
- MAC :选择Loopback:lo0



警告：Wireshark的较新Windows版本附带支持环回驱动程序的NPCAP捕获驱动程序。如果缺少环回适配器，请更新到最新版本的Wireshark或使用rawcap.exe说明。

加密DNS流量

在正常情况下，漫游客户端和Umbrella之间的流量是加密的，不可人工读取。在某些情况下，Umbrella支持可以请求您禁用DNS加密，以查看漫游客户端和Umbrella云之间的DNS流量。 有两种方法可以执行此操作：

- 为UDP 443到208.67.220.220和208.67.222.222创建本地防火墙块。
- 或者，根据您的操作系统和漫游客户端版本创建文件：
  - Windows 窗口版本:

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

  - Windows AnyConnect:

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

- Windows安全客户端：

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

- macOS:

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

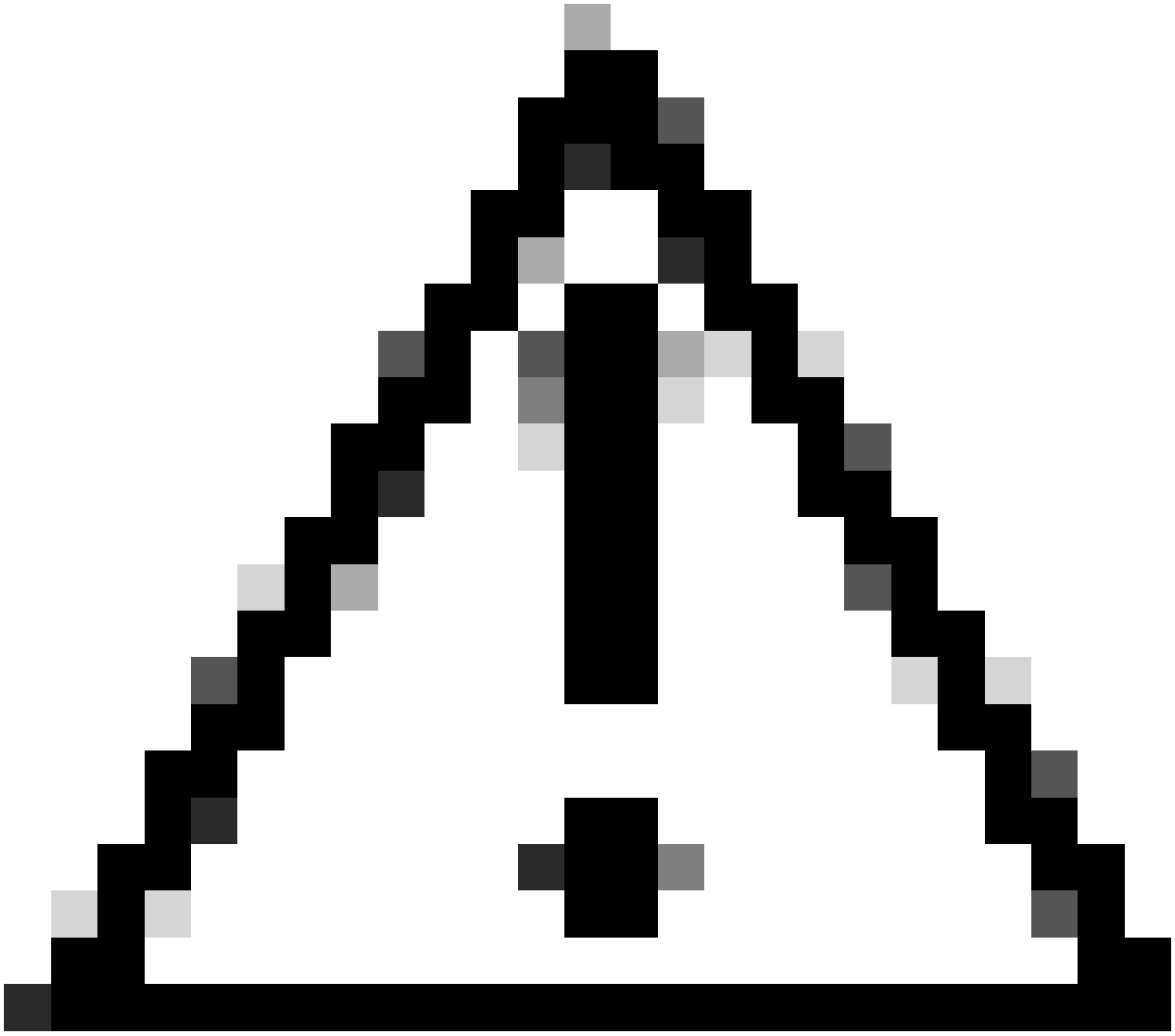
- mac OS AnyConnect:

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

- mac OS安全客户端：

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

执行此操作后，请重新启动服务或您的计算机。



警告：Windows上的Wireshark的更新版本包括NPCAP捕获驱动程序，它不支持Umbrella VPN接口。 在Windows上，您可能需要使用rawcap.exe工具作为替代工具。

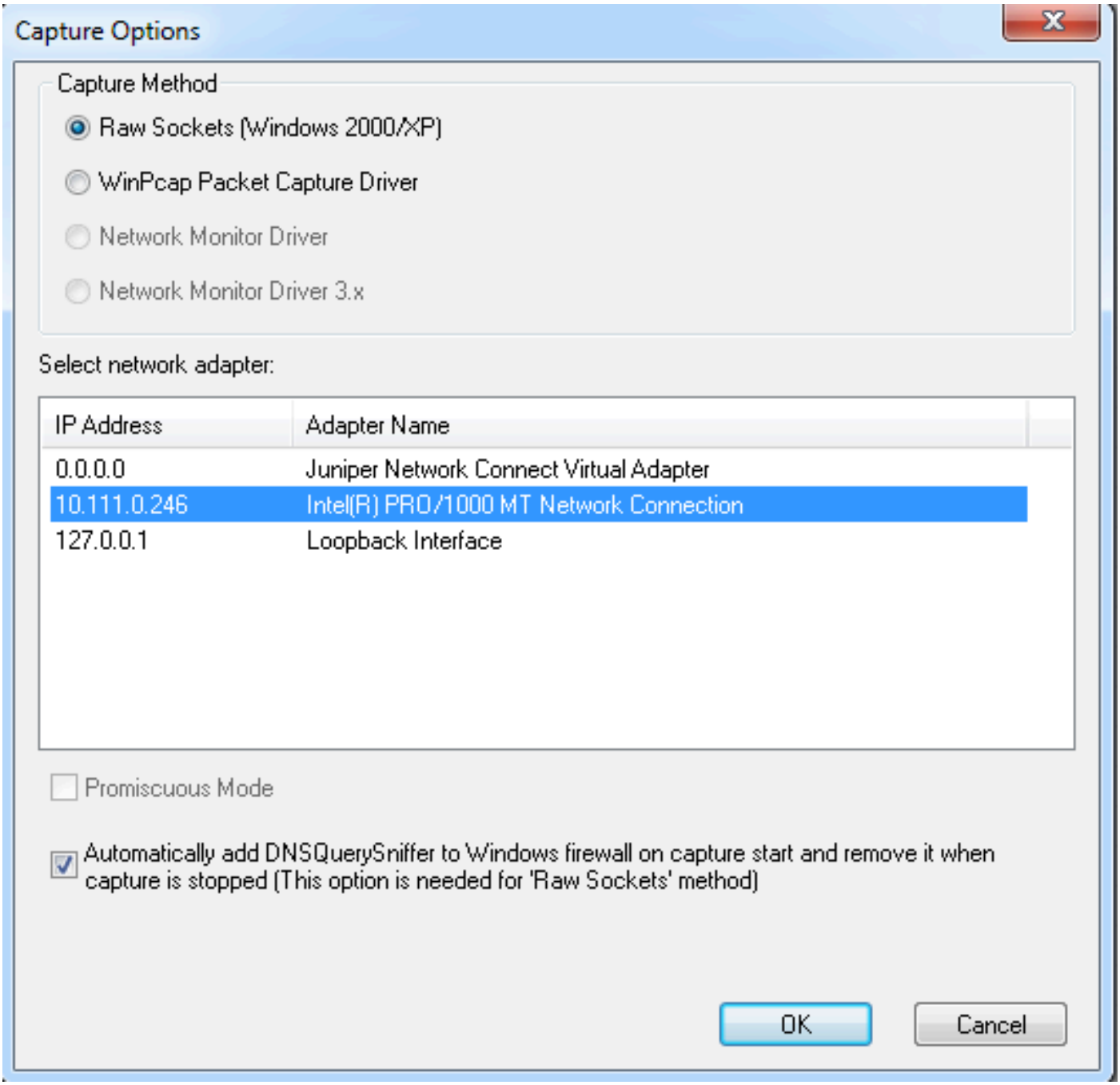
DNSQuerySniffer - Windows替代方法

DNSQuery嗅探器是用于Windows的仅DNS网络嗅探器，用于监控和显示大量有用数据。与Wireshark或Rawcap不同，它仅用于DNS，并且更容易检查和提取相关信息。但是，它没有Wireshark的强大过滤工具。

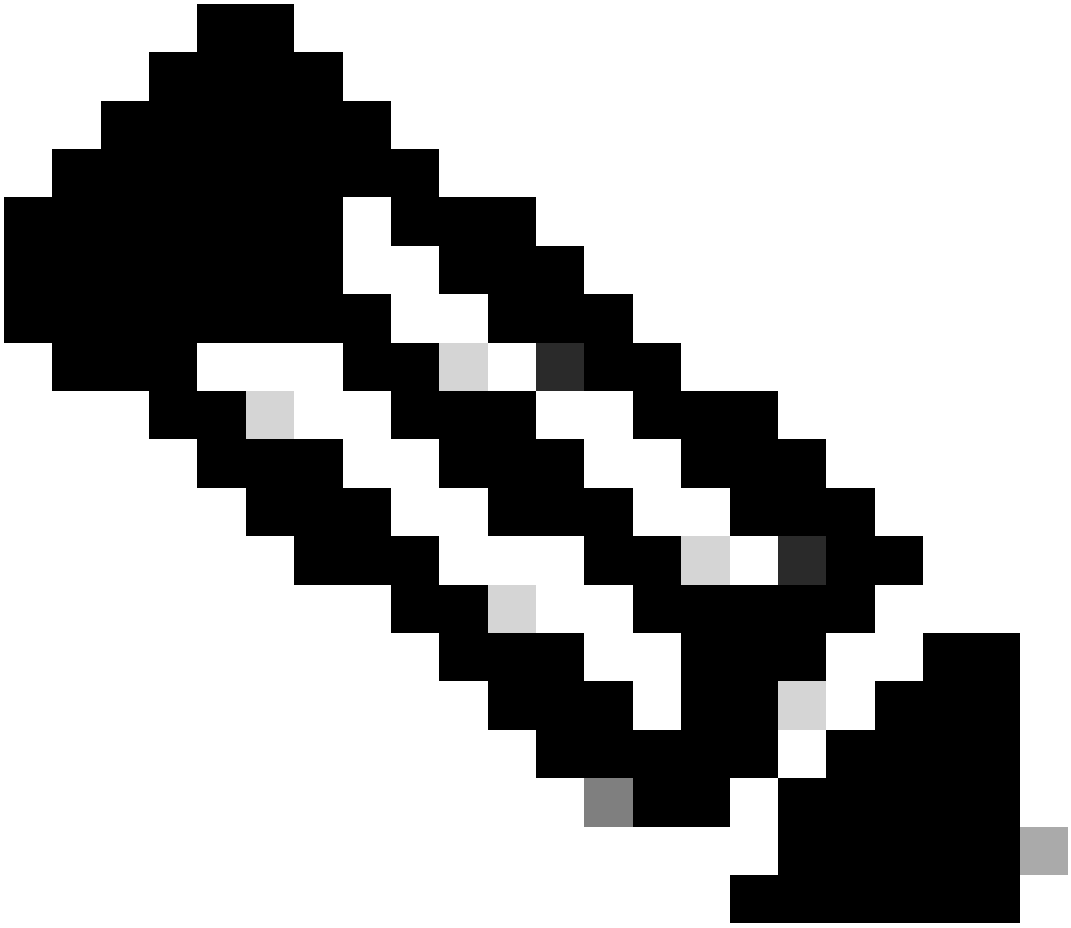
这是一个轻巧且易于使用的工具。使用这种方法的优点是，您可以在禁用漫游客户端服务时嗅探数据包，开始捕获，并且您可以在漫游客户端启动时查看漫游客户端发送的每个DNS查询，而不是在漫游客户端已启动后开始捕获。

有两种捕获方法：

1. 如果选择常规网络接口，则只能看到位于Internal Domains列表上的查询，或者未特别通过dnscryptproxy的查询。


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
10.111.0.246
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_1.png

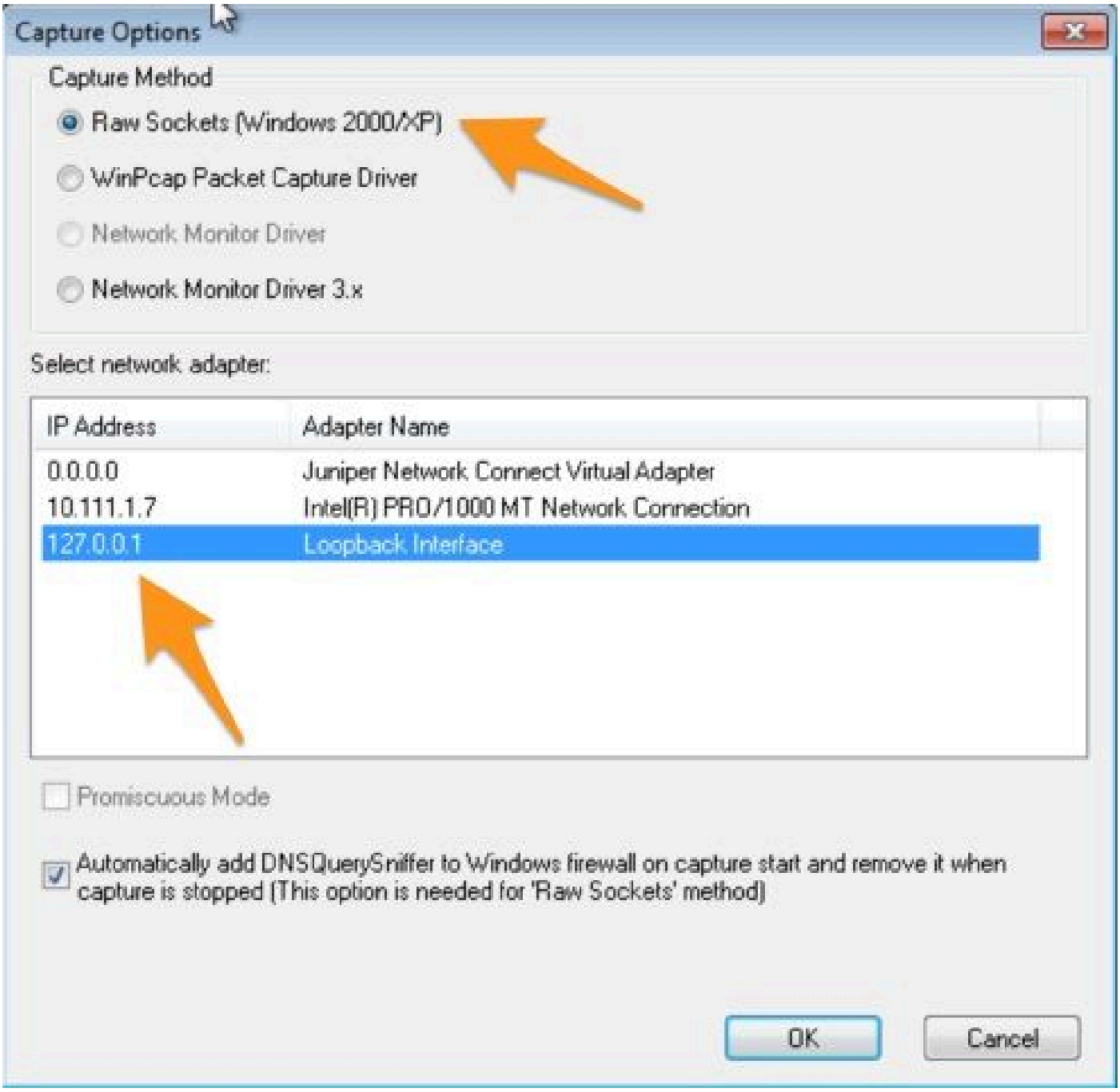


注意：这些列显示在捕获中的右侧，您必须滚动相当多才能看到它们。

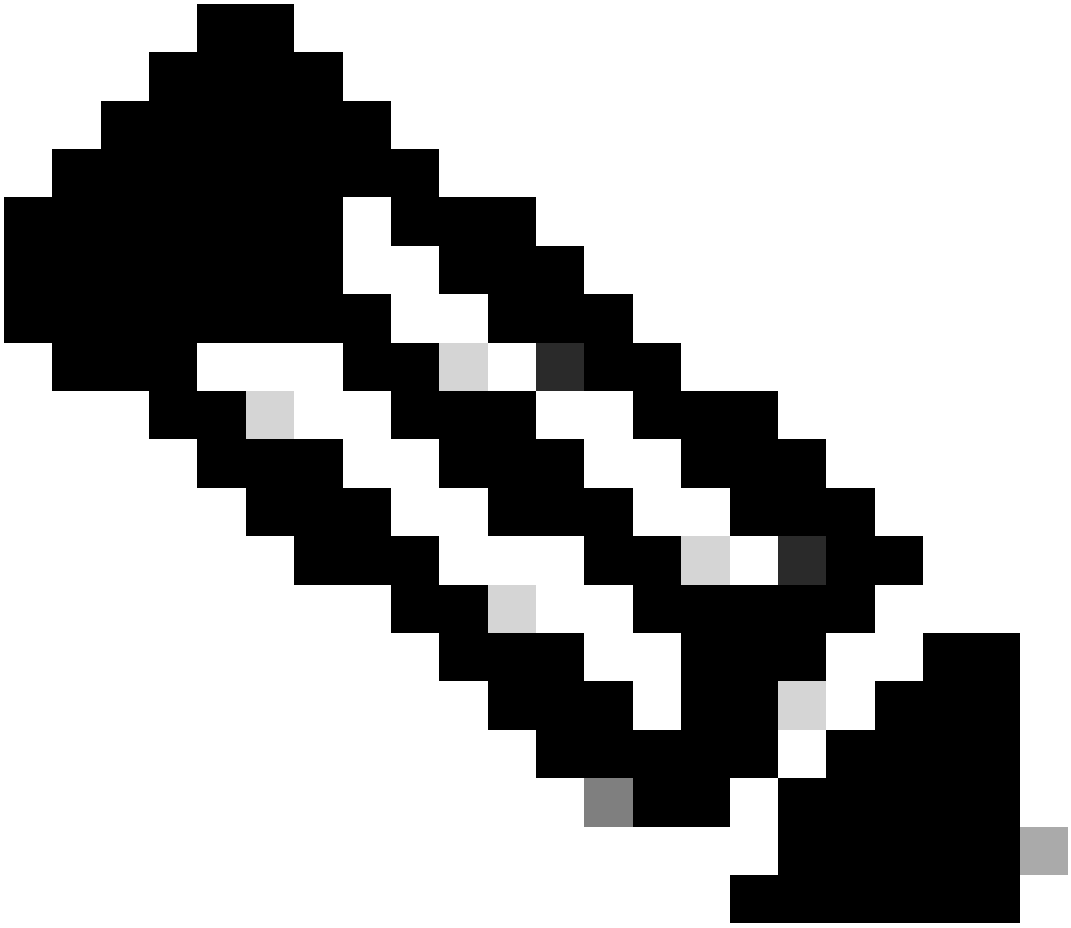
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

DNSSniffer列

2. 如果选择Loopback接口，则会看到通过dnscryptproxy发送的所有DNS查询，但看不到内部域列表中域的实际目标IP地址。但是，它仍会显示查询和答案。


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

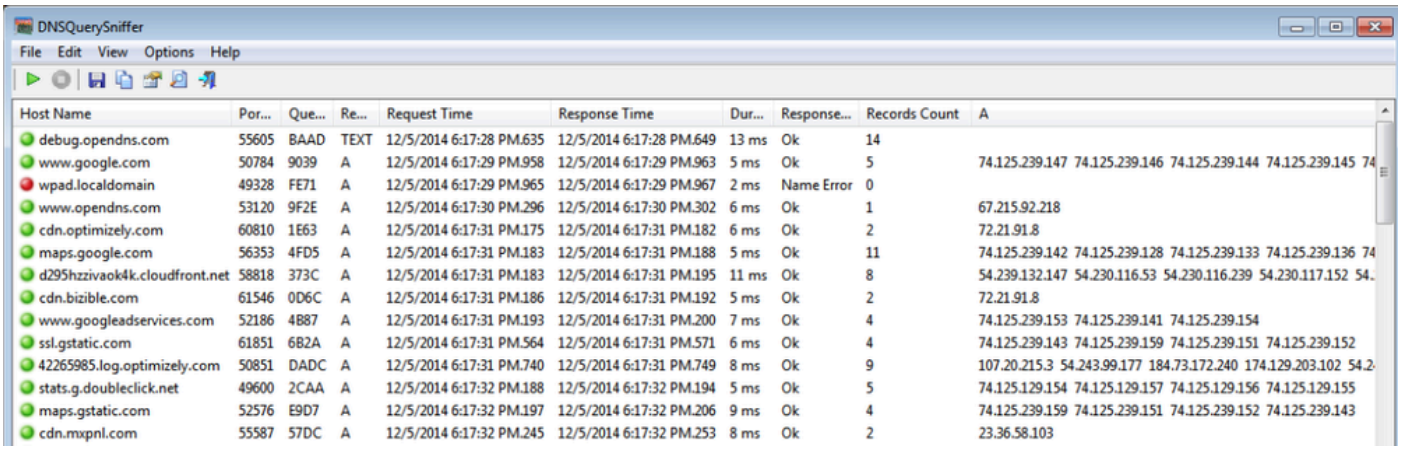


注意：这些列显示在捕获中的右侧，您必须滚动相当多才能看到它们。

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

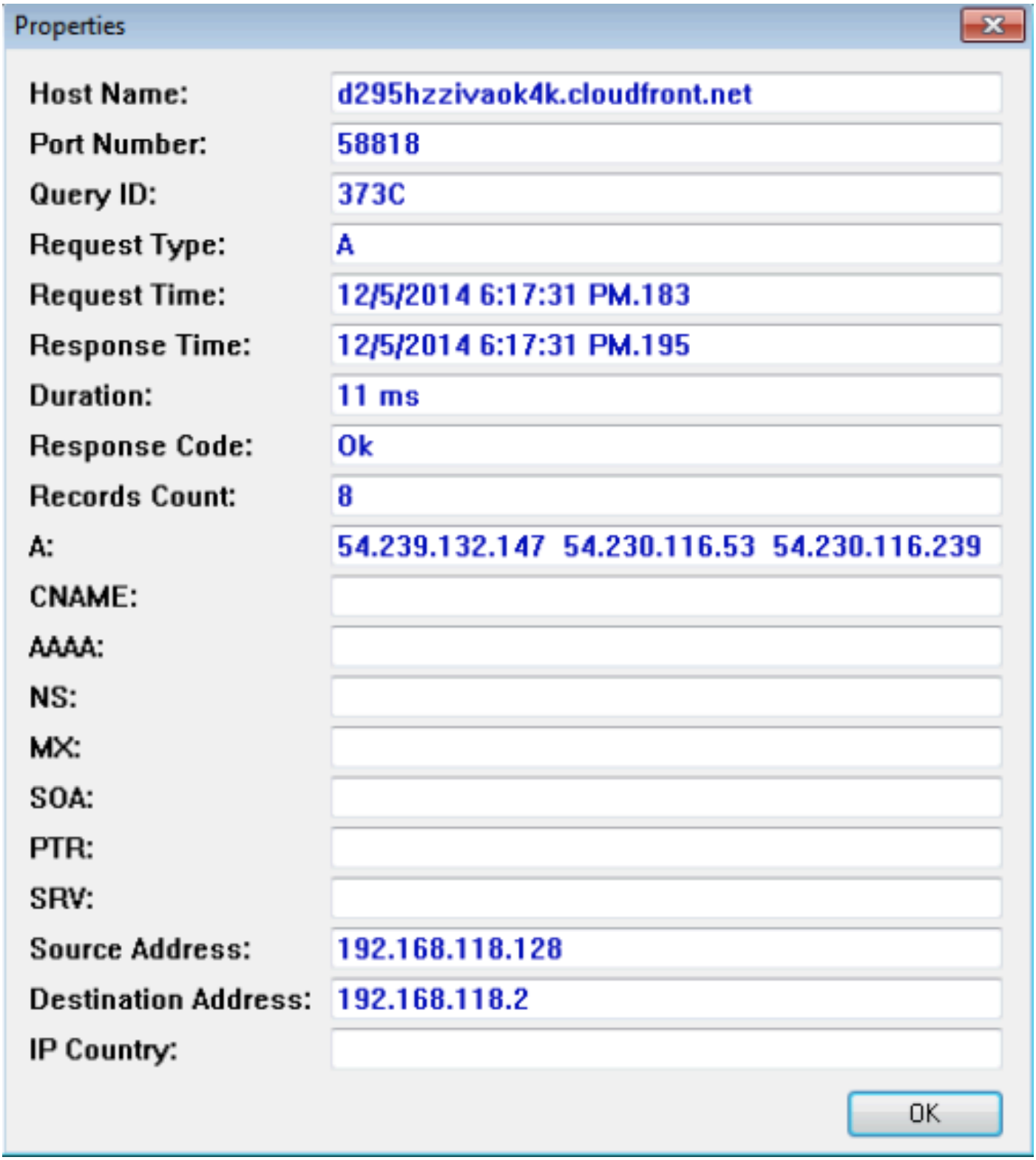
DNSSniffer列

结果如下：



dns_3.png

单个查找的视图：



dns_4.png

RawCap.exe - Windows替代程序

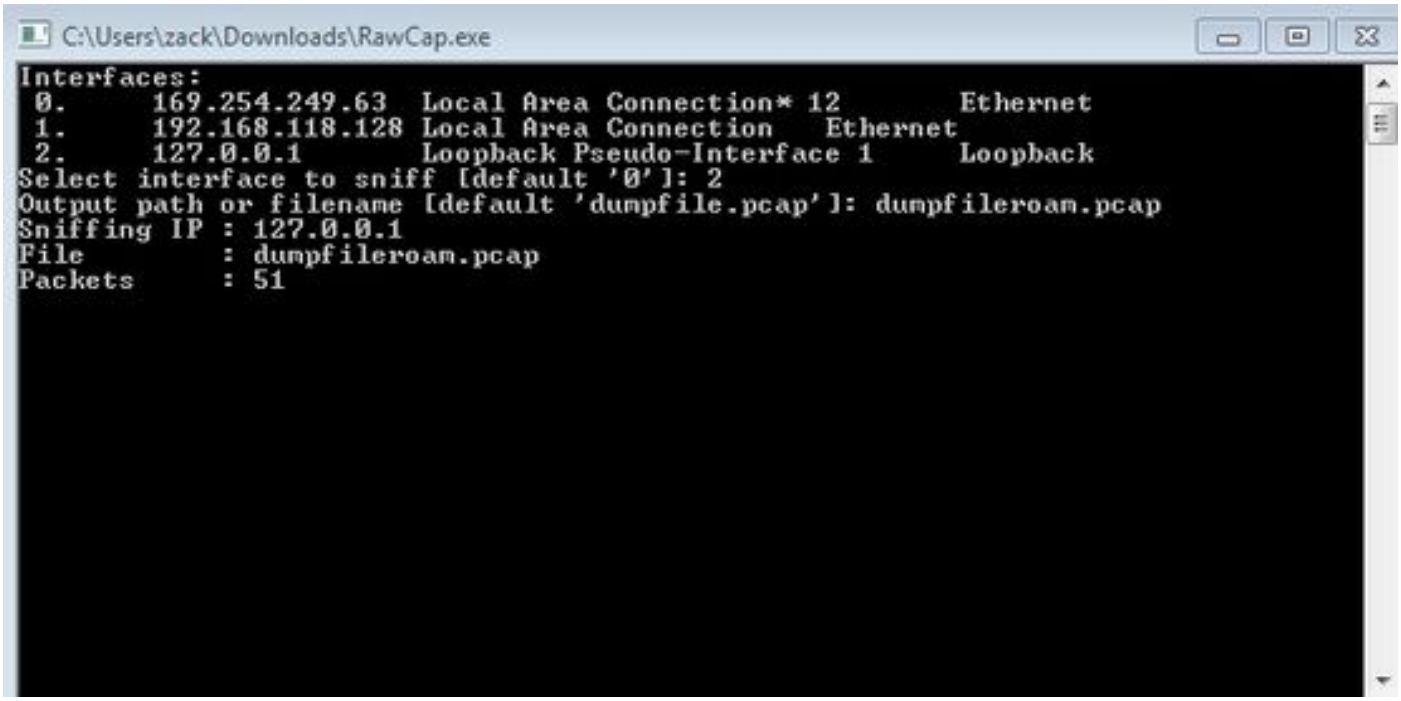
在某些情况下，Wireshark随附的数据包捕获驱动程序不支持您需要使用的接口。这可能对环回接口造成问题。

在这些情况下，我们可以使用RawCap.exe:

1. 完成本文前面所述的步骤，使用Wireshark捕获正常流量。

2. 同时，运行RawCap.exe。
3. 通过指定相应的列表编号选择接口。
4. 指定输出文件名，然后将其关闭。
5. SelectControl-C何时要停止捕获。

保存的文件将放置在运行RawCap.exe的文件夹中：



rawcap_1.jpg

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。