Wiresharkによるネットワークトラフィックのキャプチャ

内容

はじめに

このドキュメントでは、Wiresharkでネットワークトラフィックをキャプチャする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Umbrella DNSレイヤセキュリティに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Cisco Umbrellaのサポートスタッフから、コンピュータとネットワークの間を流れるインターネットトラフィックのパケットキャプチャを求められることがあります。このキャプチャにより、

Umbrellaサポートは低レベルでトラフィックを分析し、潜在的な問題を特定できます。

ほとんどの場合、正常なシナリオと正常でないシナリオの両方を示す2組のパケットキャプチャを比較することは有効です。

- 問題を再現できることを確認し、問題が発生している間に次の手順を実行します。 正常に動作しないシナリオを示すパケットキャプチャを生成します。 この情報を他のデータと関連付けられるように、タイムゾーンの日付と時刻に注意してください。
- 可能であれば、Umbrellaソフトウェア（またはUmbrella DNS転送）を無効にして、これらの手順を繰り返します。 作業シナリオを示すパケットキャプチャを生成します。 この情報を他のデータと関連付けられるように、タイムゾーンの日付と時刻に注意してください。

Wiresharkの手順

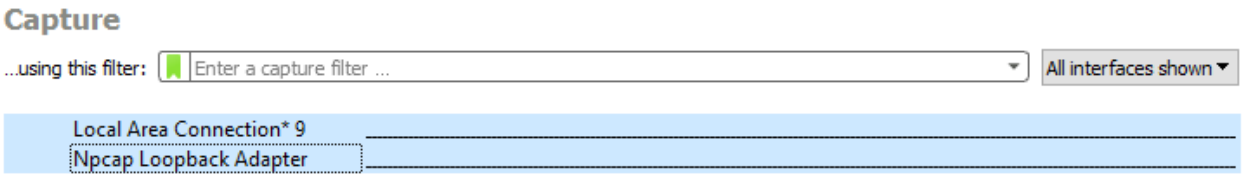
準備

1. Wiresharkをダウンロードします。
2. 不要なネットワーク接続をすべて切断します。
    1. 問題の再現に必要でない限り、VPN接続を切断します。
    2. 有線接続または無線接続のみを使用し、両方を同時に使用することはできません。
3. 問題の再現に必要でない他のソフトウェアをすべて閉じます。
4. ブラウザからCookieとキャッシュを消去します。
5. DNSキャッシュをフラッシュします。Windowsの場合は次のコマンドを使用します。

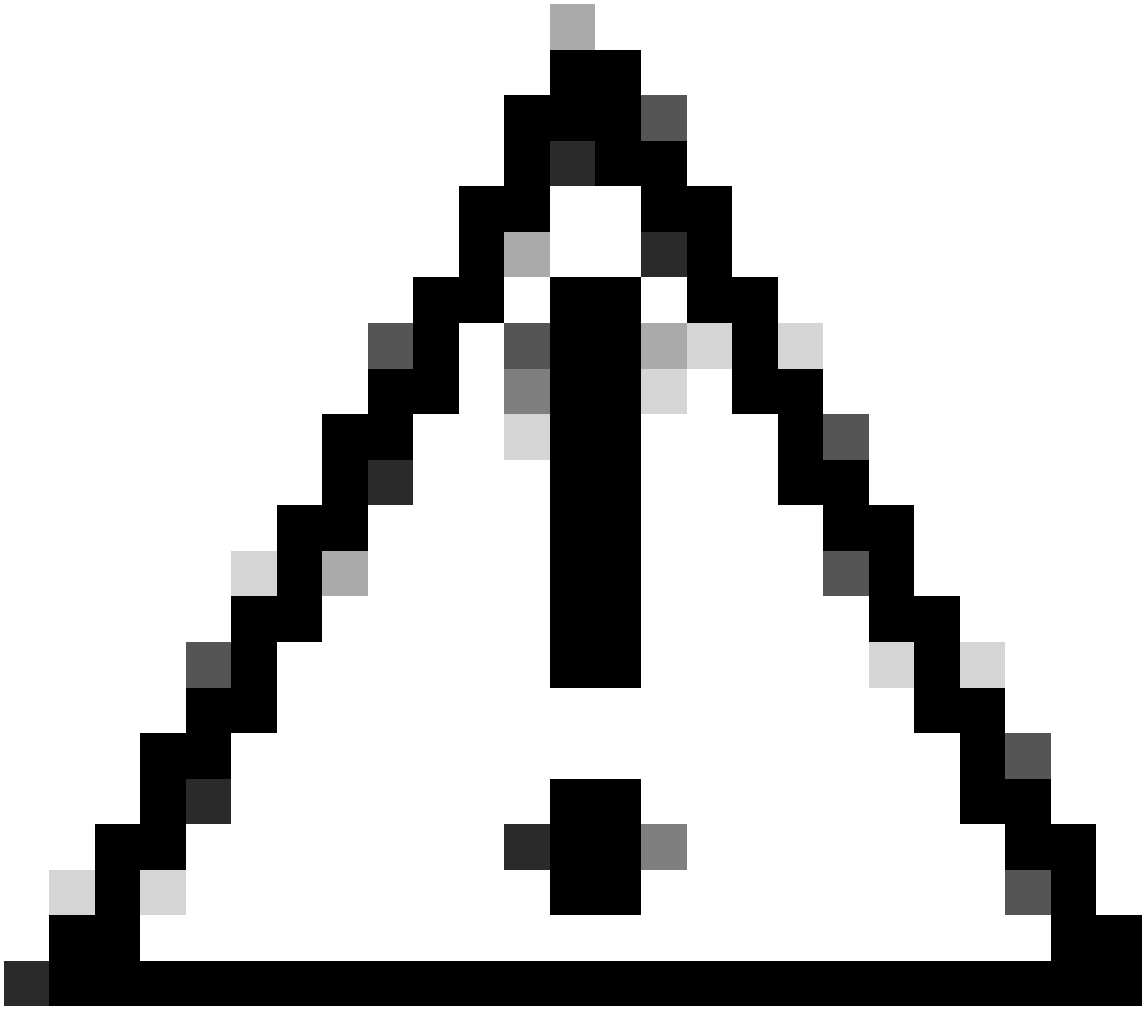
```
ipconfig /flushdns
```

基本的なWiresharkキャプチャ

1. Wiresharkを起動します。
2. Captureパネルにネットワークインターフェイスが表示されます。関連するインターフェイスを選択します。 複数のインターフェイスを選択するには、Ctrl キー(Windows)またはCmd キー(Mac)を押しながらインターフェイスを選択します。

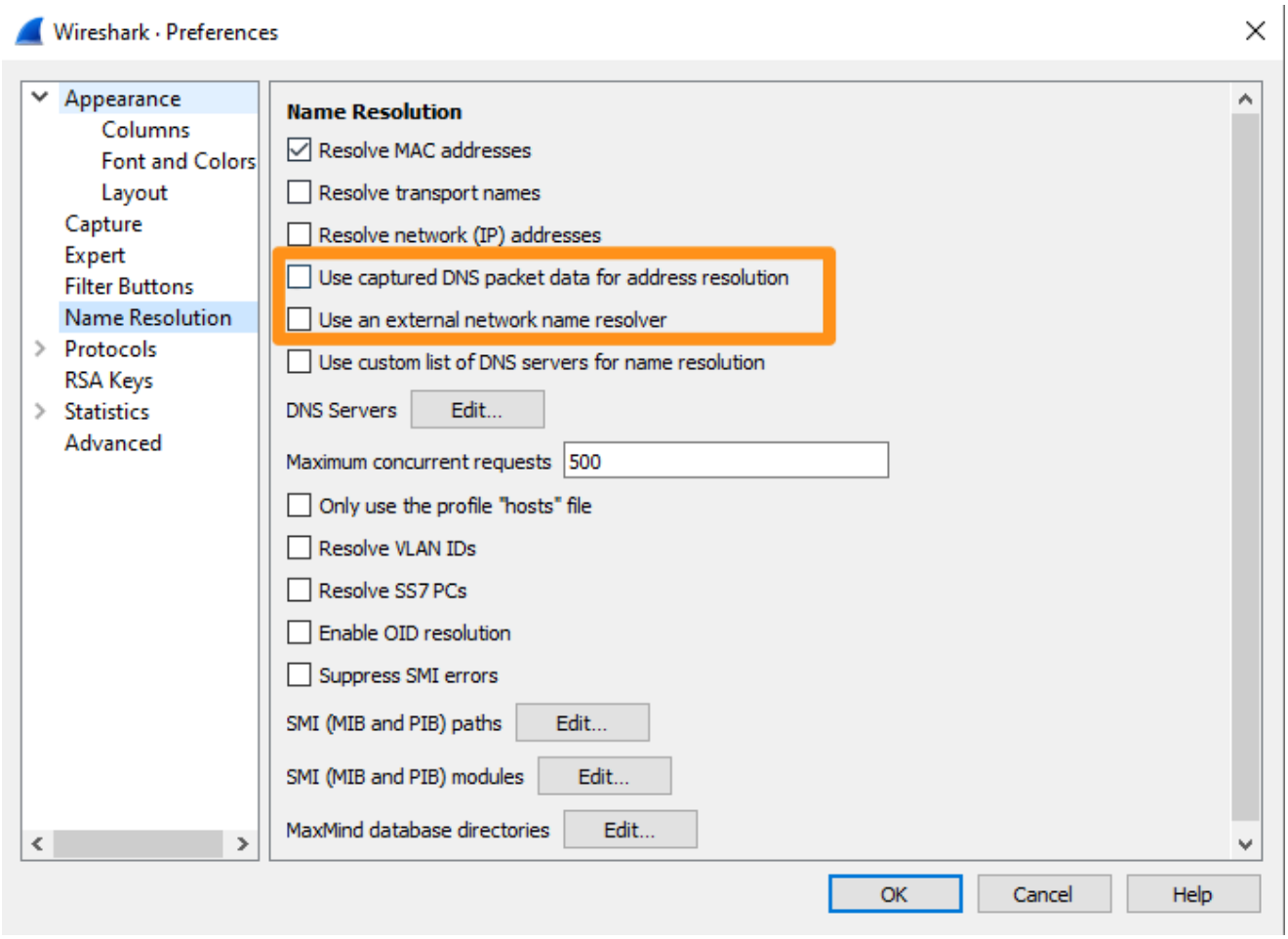


wireshark_1.pngファイル



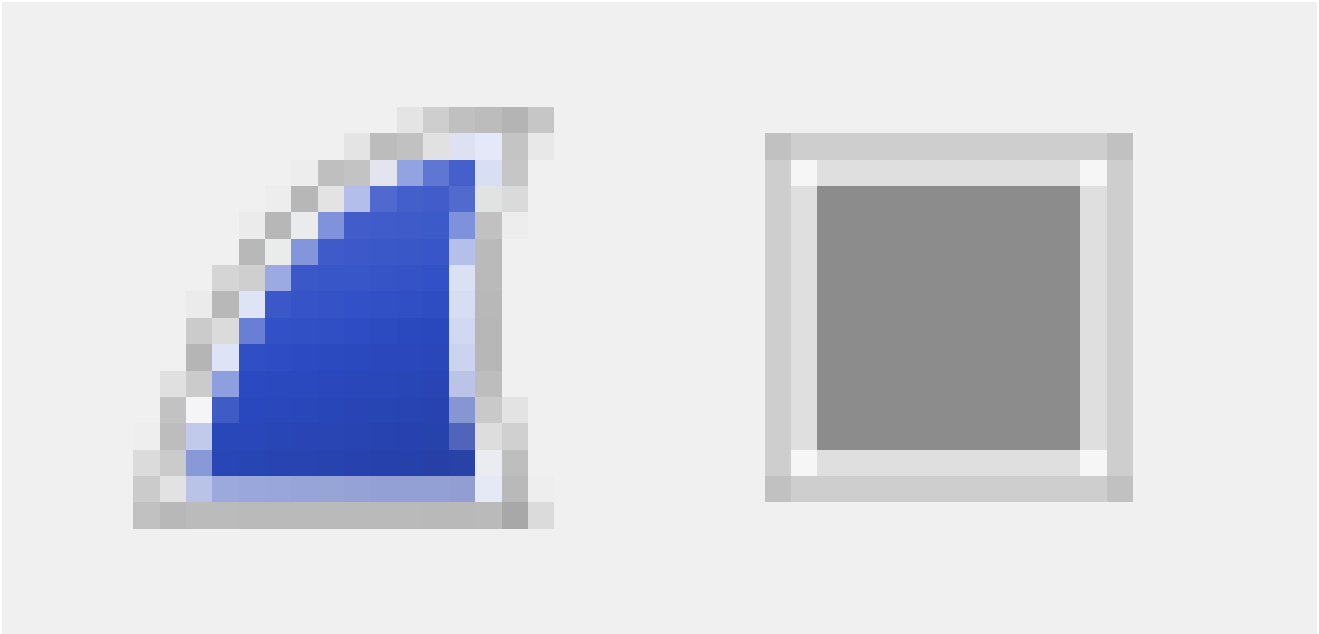
注意：ネットワークトラフィックを含む正しいインターフェイスを選択することが重要です。 ipconfigコマンド(Windows)またはifconfigコマンド(Mac)を使用して、ネットワークインターフェイスの詳細情報を表示します。ローミングクライアントのユーザは、さらにNPCAP Loopback AdapterまたはLoopback: lo0インターフェイスを選択する必要があります。不明な場合は、すべてのインターフェイスを選択してください。

3. WiresharkでDNSクエリが実行されていないことを確認するために、「キャプチャされたDNSパケットデータをアドレス解決に使用する」と「外部ネットワーク名リゾルバを使用する」が選択されていないことを確認します。選択すると、キャプチャが複雑になり、AnyConnectに影響する場合があります。設定はWireshark 3.4.9以降で有効です。



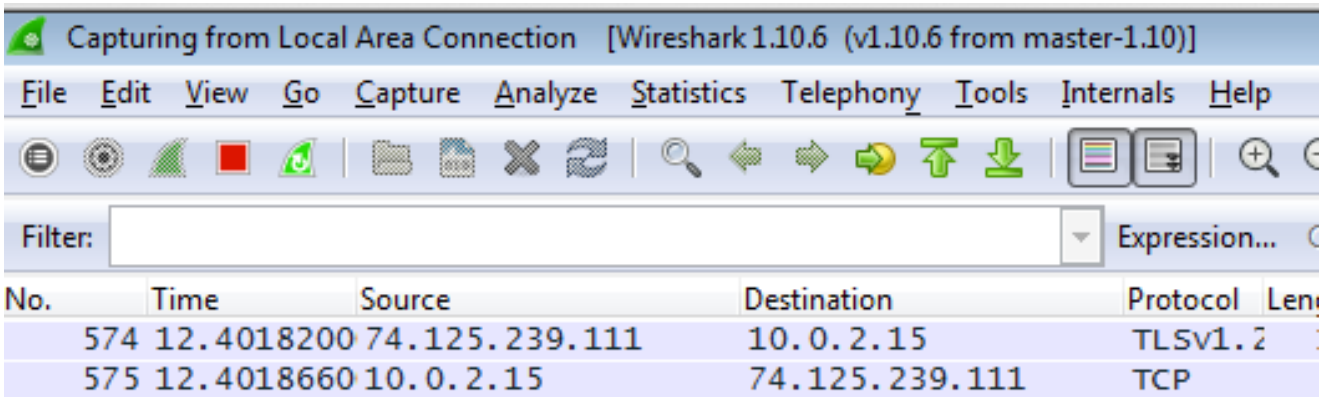
キャプチャ_PNG.png

4. Capture > Startの順に選択するか、青い開始アイコンを選択します。



wireshark_2.pngファイル

5. Wiresharkがバックグラウンドで実行されている間に、問題を再現します。



wireshark_3.pngファイル

6. 問題が完全に複製されたら、Capture > Stopの順に選択するか、赤色のStopアイコンを使用します。
7. File > Save Asの順に移動し、ファイルを保存する場所を選択します。ファイルがPCAPNGタイプとして保存されていることを確認します。 保存したファイルは、Cisco Umbrellaサポートに送信して確認できます。

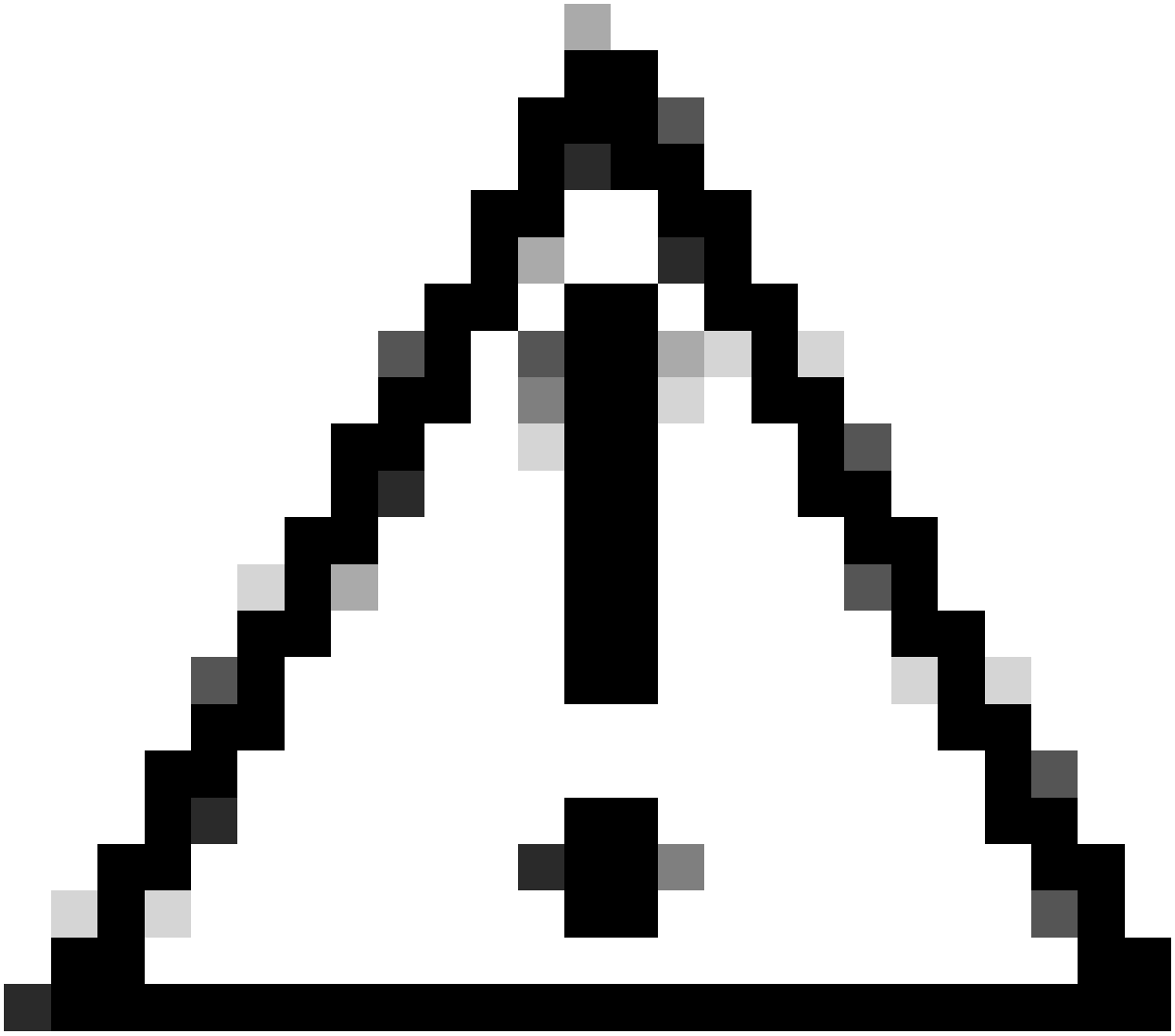
クライアントのローミング – 追加手順

スタンドアロンのRoaming ClientユーザとAnyConnect Roaming Moduleユーザの両方に対して実行する必要がある追加の手順は次のとおりです。

ループバックトラフィック

インターフェイスを選択するときは、他のネットワークインターフェイスに加えて、ループバックインターフェイス(127.0.0.1)上のトラフィックもキャプチャする必要があります。Roaming ClientのDNSプロキシはこのインターフェイスでリッスンするため、オペレーティングシステムとRoaming Client間のトラフィックを確認することが重要です。

- Windows:NPCAPループバックアダプタの選択
- Mac:Loopback:lo0を選択します。



注意:Wiresharkの新しいWindowsバージョンには、ループバックドライバをサポートするNPCAPキャプチャドライバが付属しています。ループバックアダプタが見つからない場合は、Wiresharkの最新バージョンに更新するか、rawcap.exeの手順を使用します。

暗号化されたDNSトラフィック

通常の状況では、Roaming ClientとUmbrellaの間のトラフィックは暗号化されており、人間が読み取ることはできません。場合によっては、Umbrellaサポートから、Roaming ClientとUmbrellaクラウド間のDNSトラフィックを確認するためにDNS暗号化を無効にするよう要求されることがあります。 これを行うには、次の2つの方法があります。

- UDP 443から208.67.220.220および208.67.222.222へのローカルファイアウォールブロックを作成します。
- または、OSとRoaming Clientのバージョンに応じて、ファイルを作成します。
  - Windows：

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

- Windows AnyConnect:

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

- Windows Secureクライアント：

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

- macOS:

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

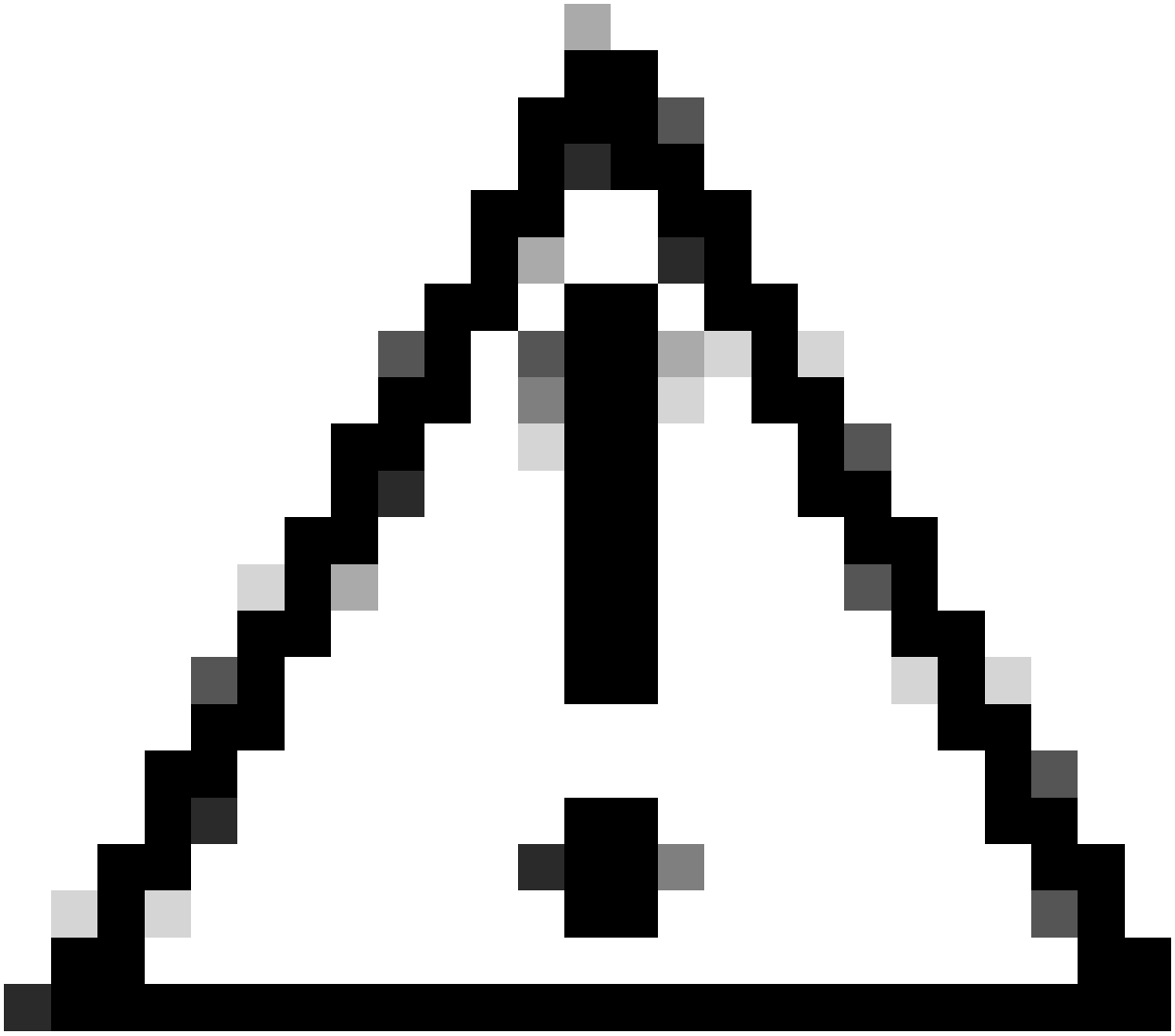
- mac OS AnyConnect:

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

- mac OSセキュアクライアント：

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

その後、サービスまたはコンピュータを再起動します。



注意:WindowsでのWiresharkの新しいバージョンには、NPCAPキャプチャドライバ（Pansla VPNインターフェイスをサポートしない）が含まれています。 Windowsでは、代わりにrawcap.exeツールを使用する必要がある場合があります。

DNSQuerySniffer:Windowsの代替

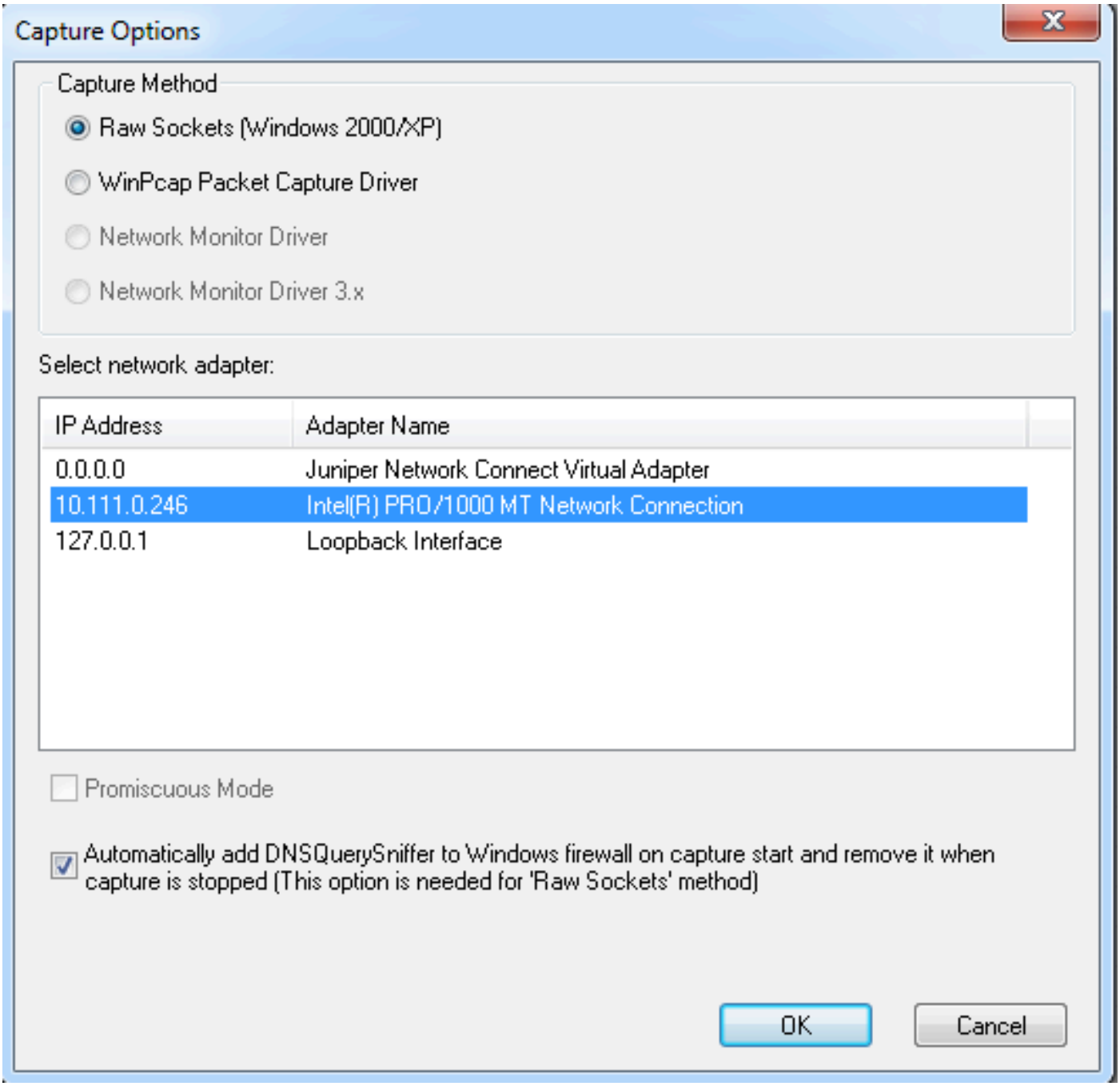
DNSQueryスニファは、大量の有用なデータをモニタおよび表示するWindows用のDNS専用ネットワークスニファです。WiresharkやRawcapとは異なり、DNSのみに使用され、関連情報の調査と抽出が非常に簡単です。ただし、Wiresharkの強力なフィルタリングツールはありません。

これは軽量で使いやすい道具です。これを使用する利点は、ローミングクライアントサービスが無効の間にパケットを傍受し、キャプチャを開始できることと、ローミングクライアントがすでに開始した後にキャプチャを開始するのではなく、ローミングクライアントが開始した時点から送信されるすべてのDNSクエリを確認できることです。

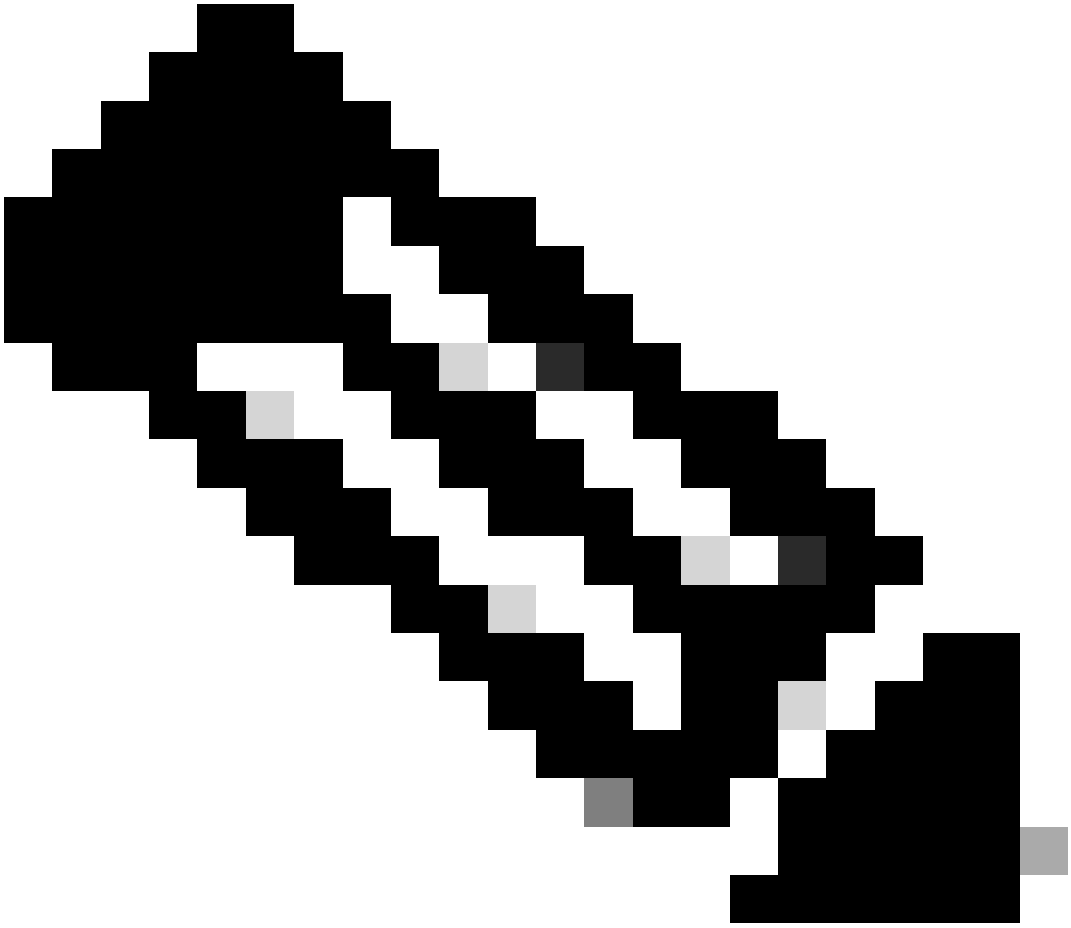
次の2つのキャプチャ方法があります。

1. 通常のネットワークインターフェイスを選択すると、「Internal Domains」リストに含まれ

るクエリ、またはdnscryptproxyを明示的に通過しなかったクエリだけが表示されます。



dns_1.png

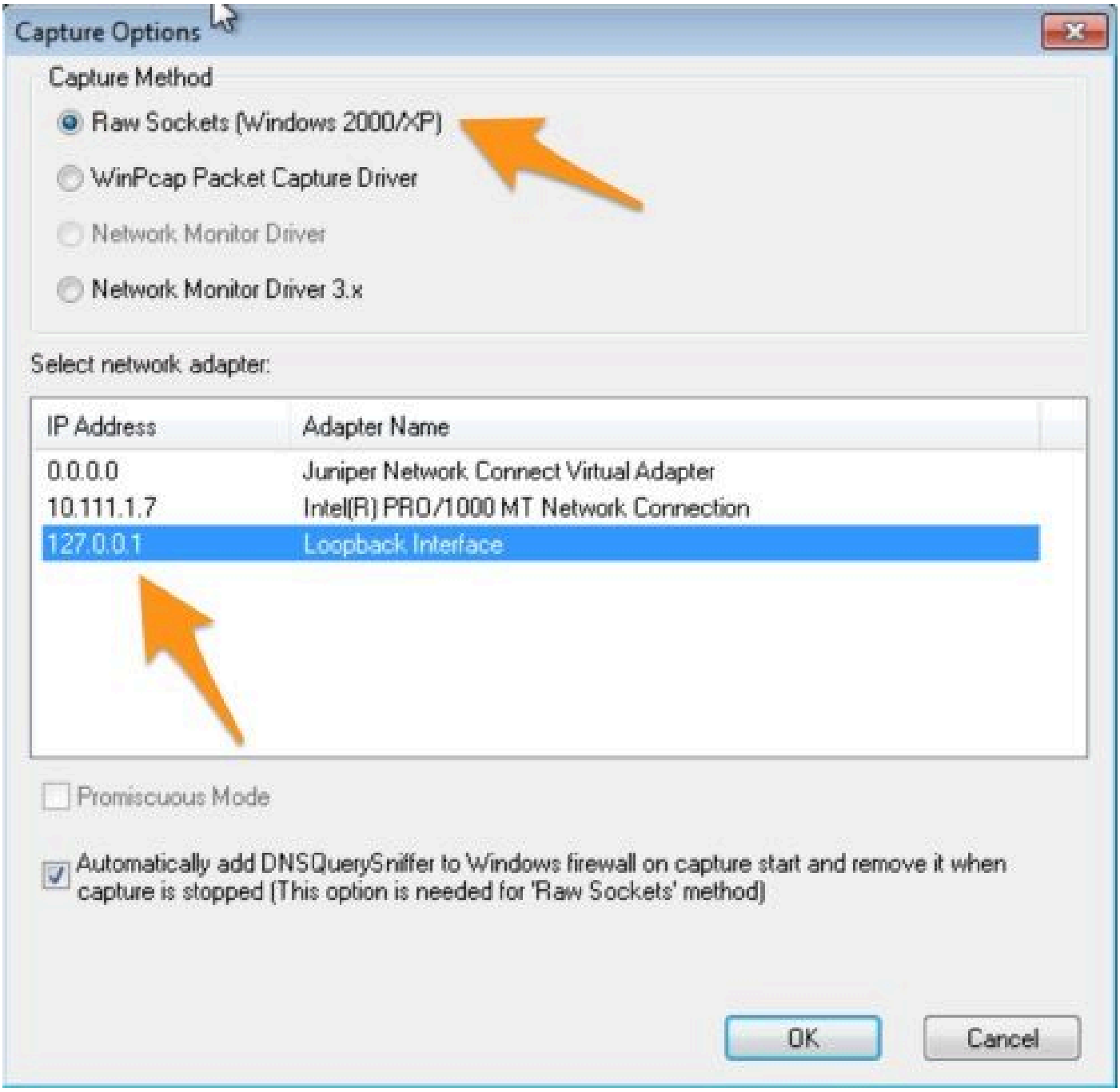


注：これらの列はキャプチャの右側に表示され、表示するにはかなりスクロールする必要があります。

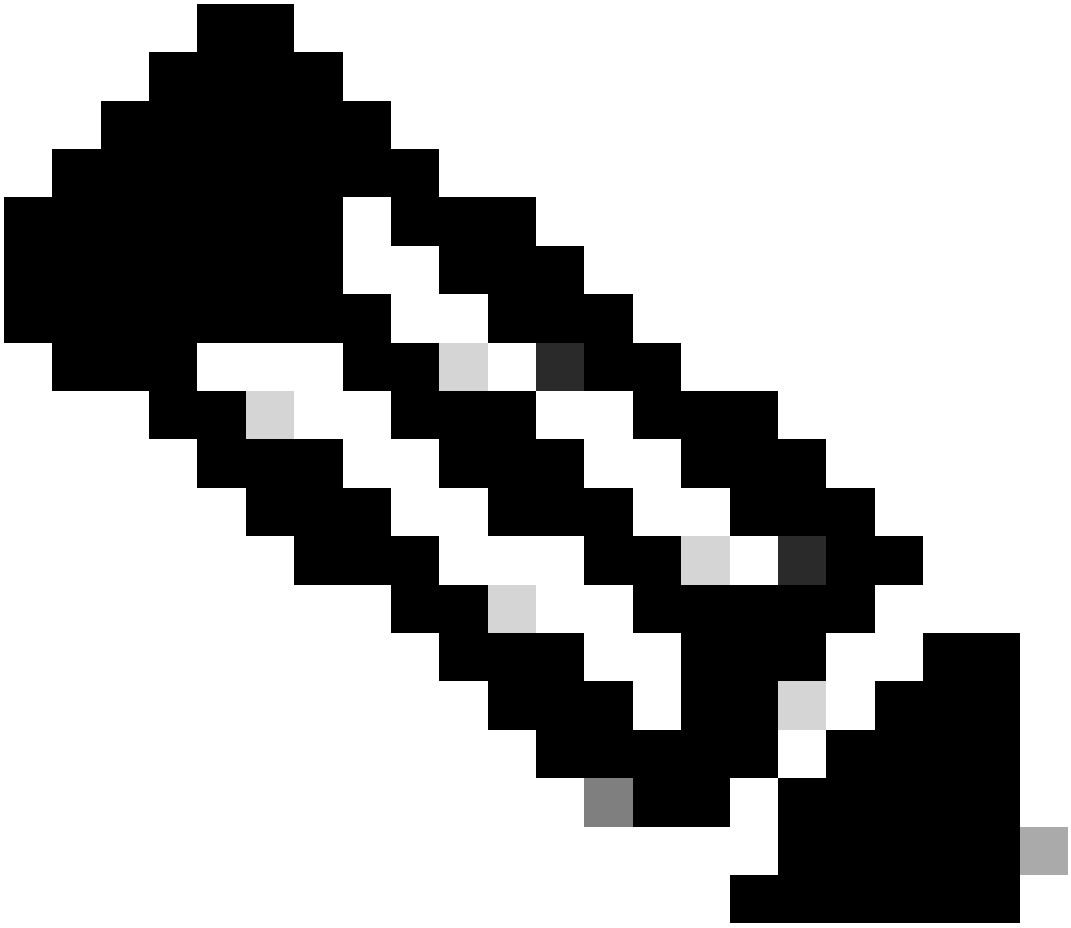
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

DNSSnifferカラム

2. Loopbackインターフェイスを選択した場合、dnscryptproxyを介して送信されたすべてのDNSクエリが表示されますが、内部ドメインリストにドメインの実際の宛先IPアドレスは表示されません。ただし、引き続きクエリーと応答が表示されます。


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

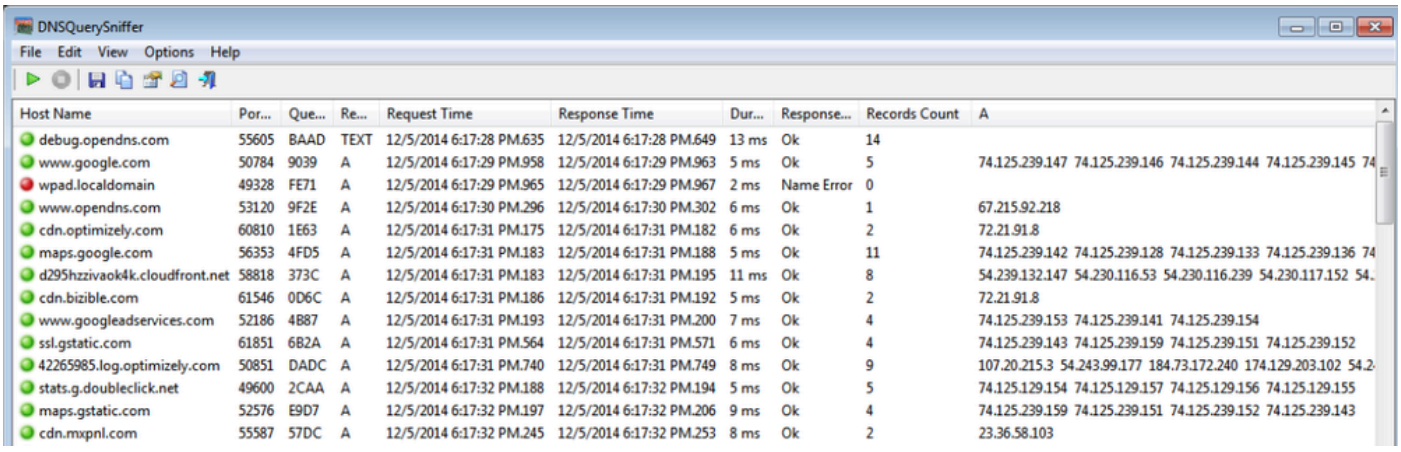


注：これらの列はキャプチャの右側に表示され、表示するにはかなりスクロールする必要があります。

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

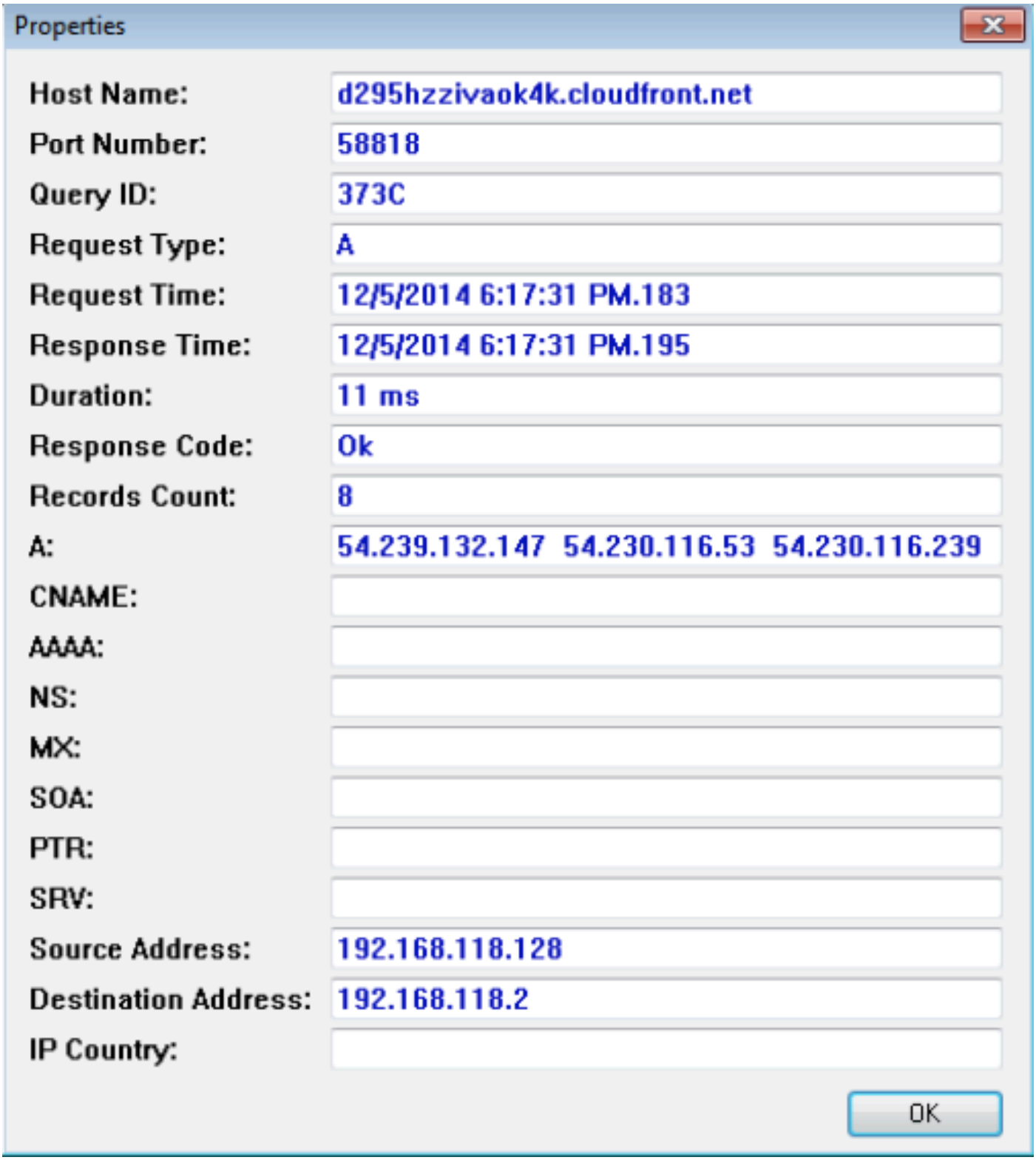
DNSSnifferカラム

結果は次のようになります。



dns_3.png

個々のルックアップのビュー：



dns_4.png

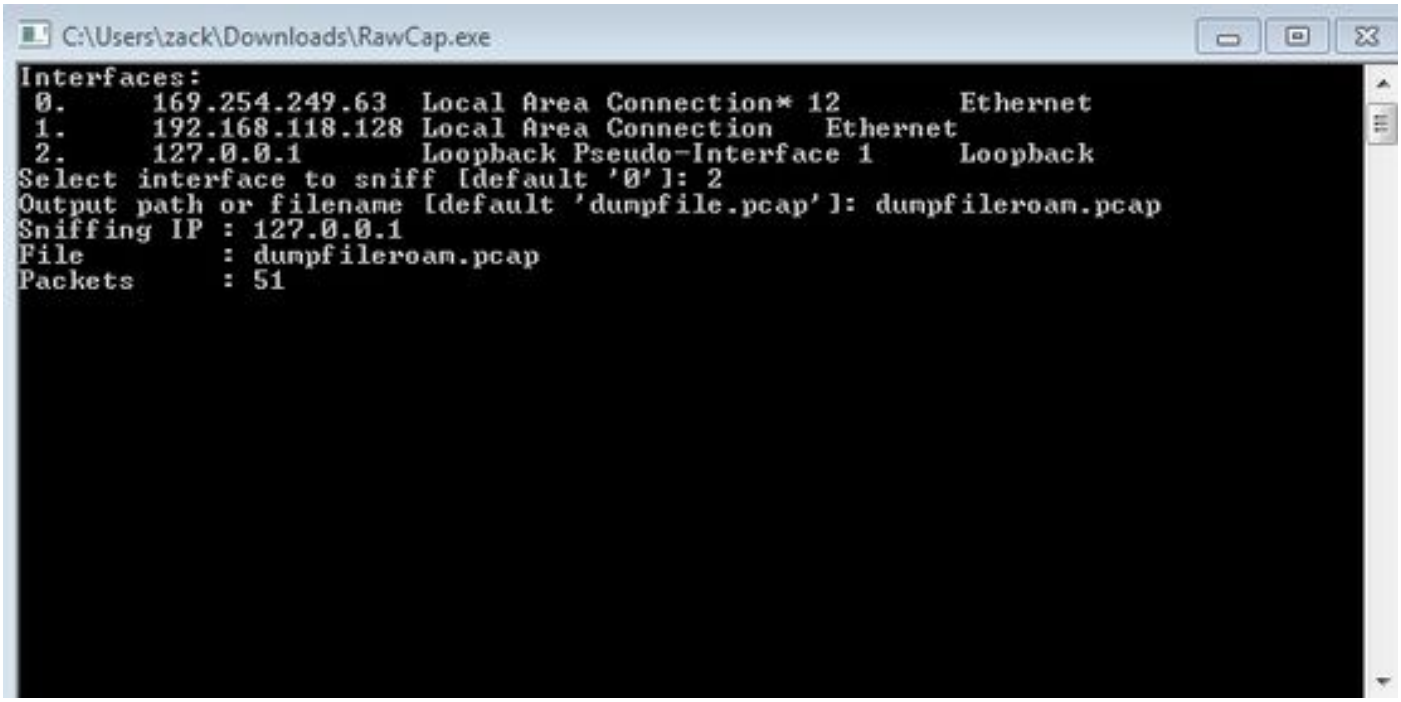
RawCap.exe - Windowsの代替

状況によっては、使用する必要があるインターフェイスが、Wiresharkに含まれているパケットキャプチャドライバでサポートされていない場合があります。これはループバックインターフェイスの問題である可能性があります。

このような場合は、RawCap.exeを使用できます。

1. Wiresharkを使用して通常のトラフィックをキャプチャするには、前述の手順を実行します。
2. 同時に、RawCap.exeを実行します。
3. 対応するリスト番号を指定して、インターフェイスを選択します。
4. 出力ファイル名を指定すると、出力ファイルはオフになります。
5. SelectControl-キャプチャを停止するタイミングを選択します。

保存したファイルは、RawCap.exeを実行したフォルダに保存されます。



rawcap_1.jpg

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。