Capturar o tráfego de rede com o Wireshark

Contents

Introdução

Este documento descreve como capturar o tráfego de rede com o Wireshark.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas na segurança de camada DNS do Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Às vezes, a equipe do Cisco Umbrella Support solicita uma captura de pacote do tráfego da Internet que flui entre o computador e a rede. A captura permite que o suporte do Umbrella analise o tráfego em um nível baixo e identifique possíveis problemas.

Na maioria dos casos, é útil comparar dois conjuntos de capturas de pacotes que demonstram um

cenário funcional e um não funcional.

- Verifique se você pode replicar o problema e concluir essas etapas enquanto o problema ocorre. Gere uma captura de pacote mostrando um cenário de não funcionamento. Anote a data e a hora com o fuso horário para que essas informações possam ser correlacionadas com outros dados.
- Se possível, repita essas instruções com o software Umbrella (e/ou o encaminhamento DNS Umbrella) desabilitado. Gere uma captura de pacote mostrando o cenário de trabalho. Anote a data e a hora com o fuso horário para que essas informações possam ser correlacionadas com outros dados.

Instruções do Wireshark

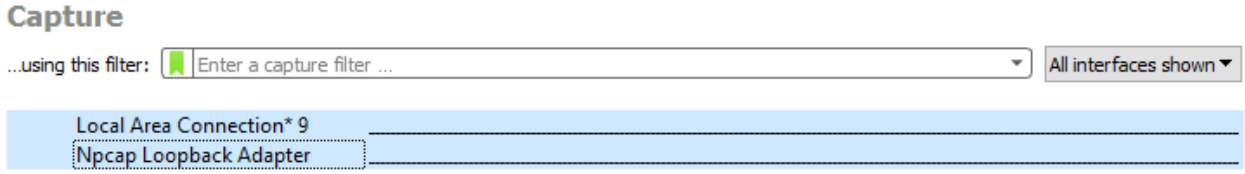
Preparações

1. Faça o download do Wireshark.
2. Desconecte todas as conexões de rede desnecessárias.
    1. Desconecte as conexões VPN, a menos que elas sejam necessárias para replicar o problema.
    2. Use apenas conexões com ou sem fio e não ambas juntas.
3. Feche qualquer outro software que não seja necessário para replicar o problema.
4. Limpe os Cookies e o Cache do seu navegador.
5. Limpe o cache DNS. No Windows, com o comando:

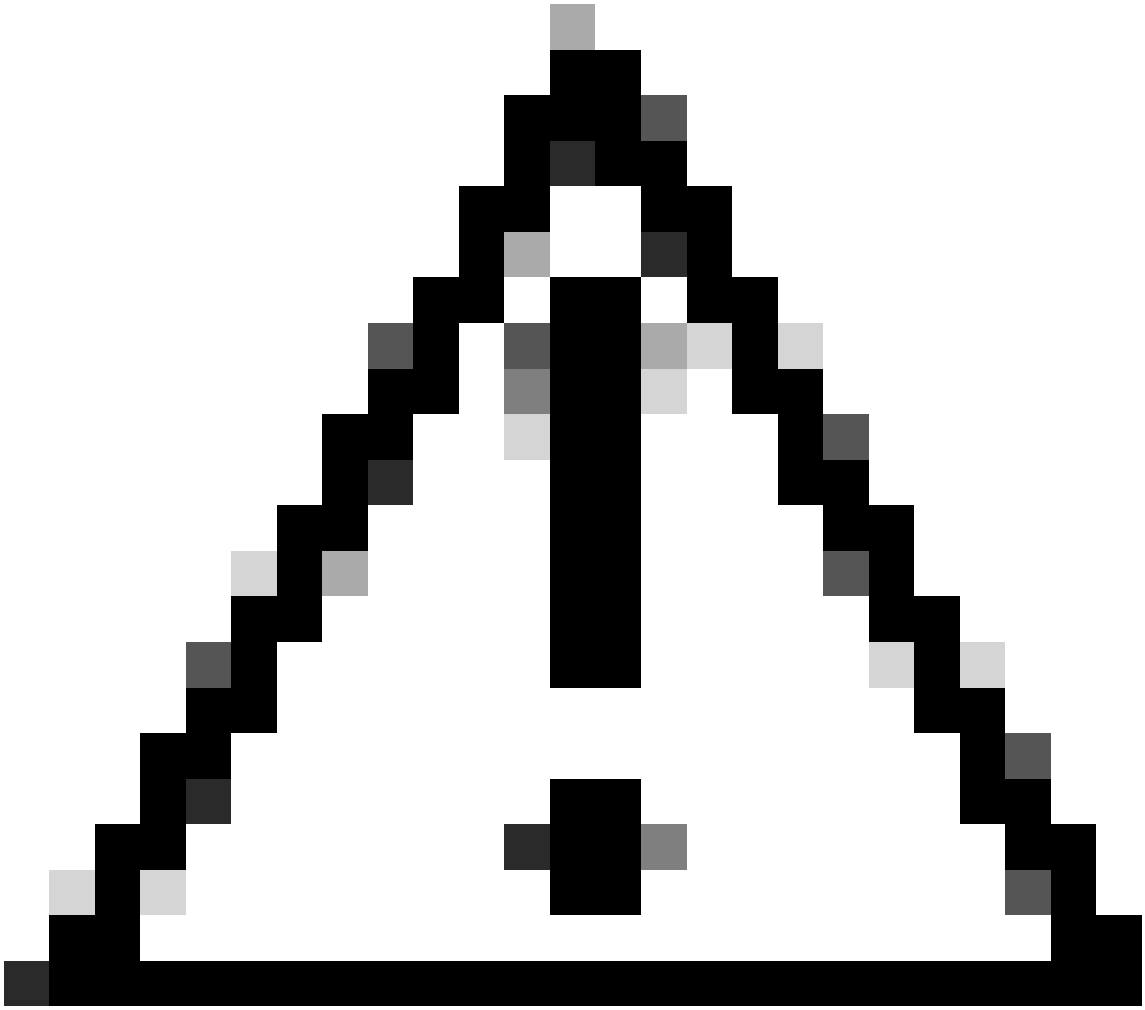
```
ipconfig /flushdns
```

Captura básica do Wireshark

1. Inicie o Wireshark.
2. O painel Capture mostra suas interfaces de rede. Selecione as interfaces relevantes. Várias interfaces podem ser selecionadas usando a tecla CTRL (Windows) ou a tecla CMD (Mac) ao selecionar.

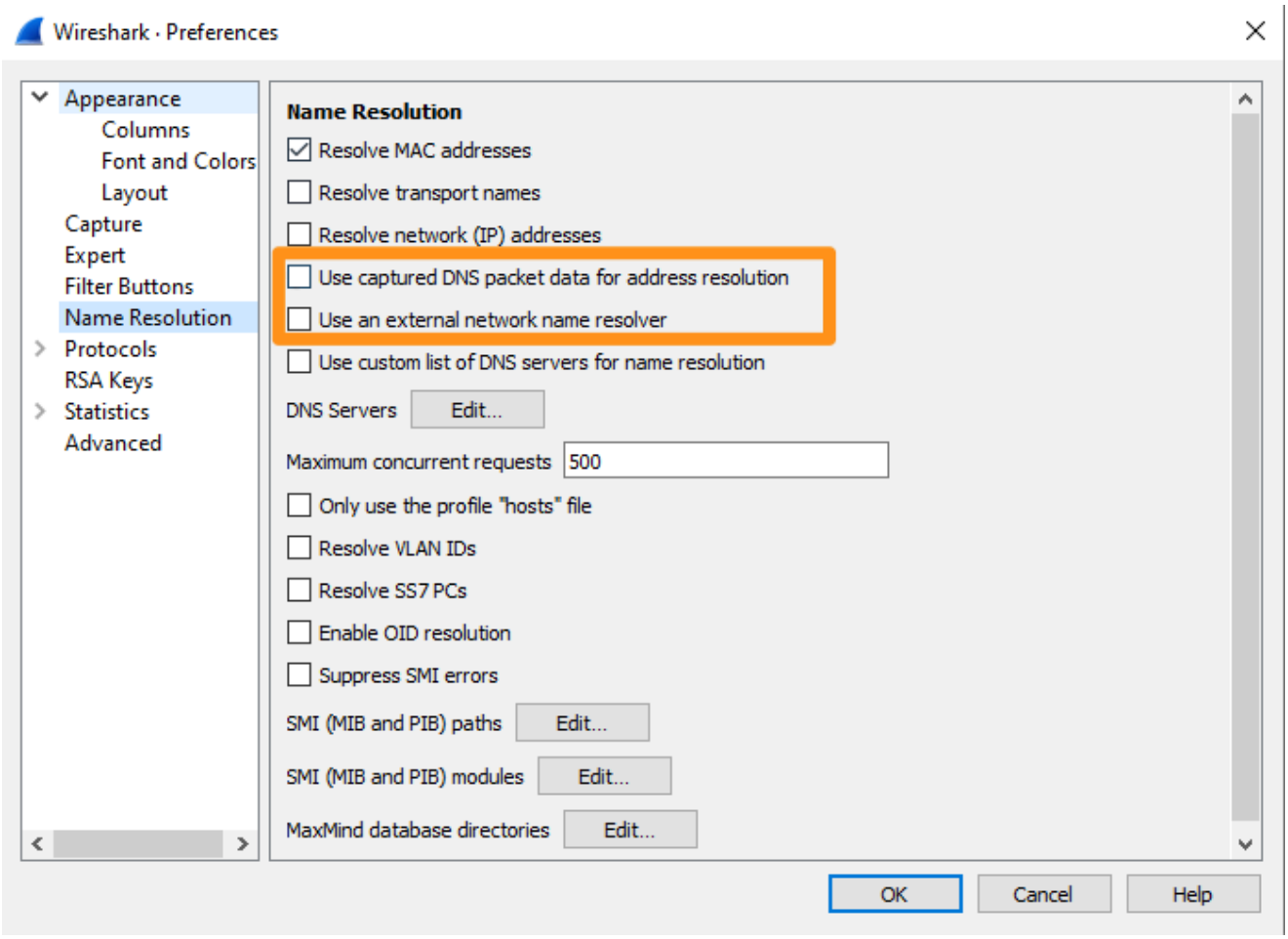


wireshark_1.png



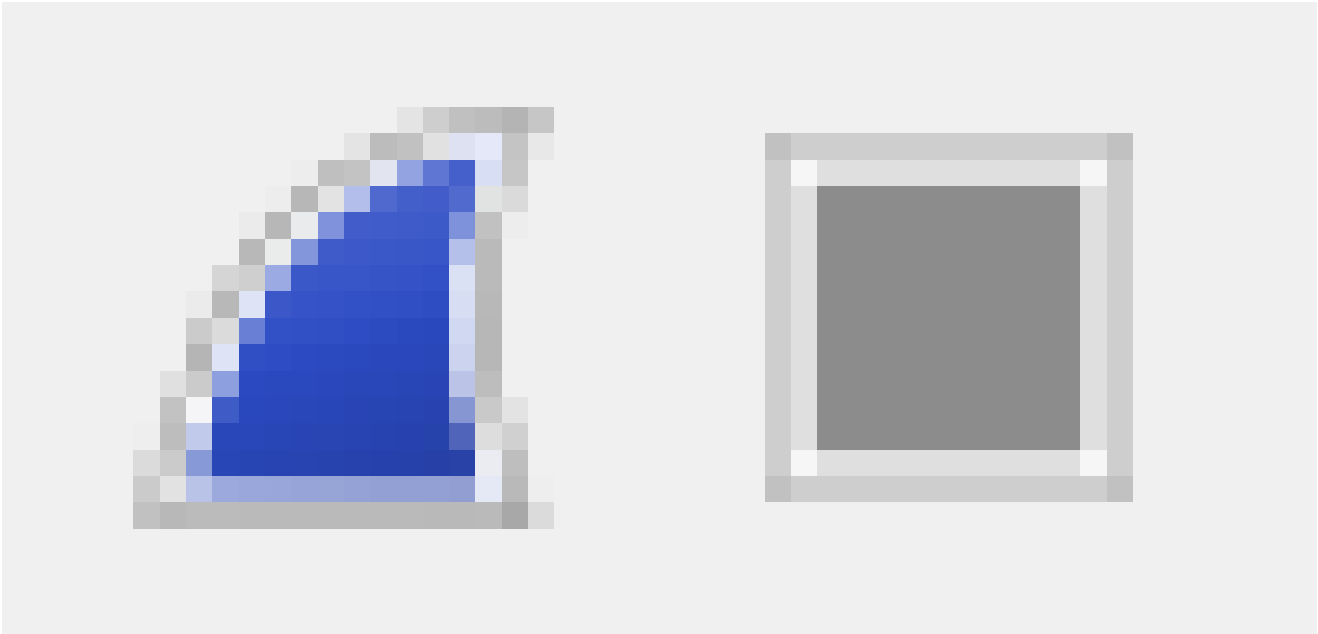
Caution: É importante selecionar as interfaces corretas que contêm o tráfego de rede. Use o comando "ipconfig" (Windows) ou o comando "ifconfig" (Mac) para exibir mais detalhes sobre suas interfaces de rede. Os usuários do cliente de roaming também devem selecionar o adaptador de loopback NPCAP OU o loopback: interfaces lo0. Se estiver em dúvida, selecione todas as interfaces.

3. Certifique-se de que Usar dados do pacote DNS capturado para resolução de endereço e Usar um resolvedor de nome de rede externo estejam NOT selecionados para garantir que o Wireshark não esteja fazendo consultas DNS, pois isso pode complicar a captura e afetar o AnyConnect. As configurações são válidas a partir do Wireshark 3.4.9:



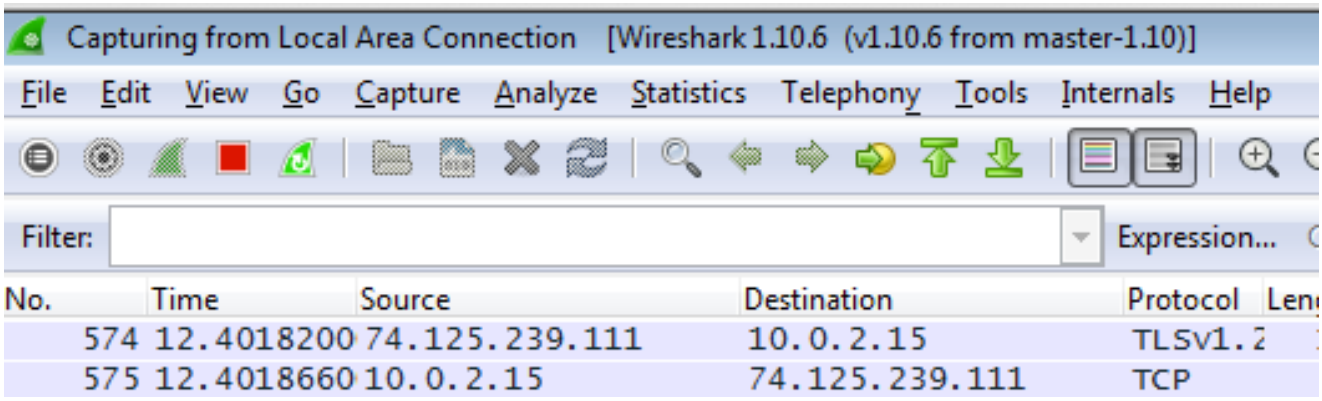
Capture_PNG.png

4. Selecione Capture > Start ou selecione o ícone de início azul.



wireshark_2.png

5. Enquanto o Wireshark estiver em execução em segundo plano, replique o problema.



wireshark_3.png

6. Depois que o problema tiver sido totalmente replicado, selecione Capture > Stop ou use o ícone vermelho Stop.
7. Navegue até File > Save As e selecione um local para salvar o arquivo. Certifique-se de que o arquivo seja salvo como um tipo PCAPNG. O arquivo salvo pode ser enviado ao suporte do Cisco Umbrella para revisão.

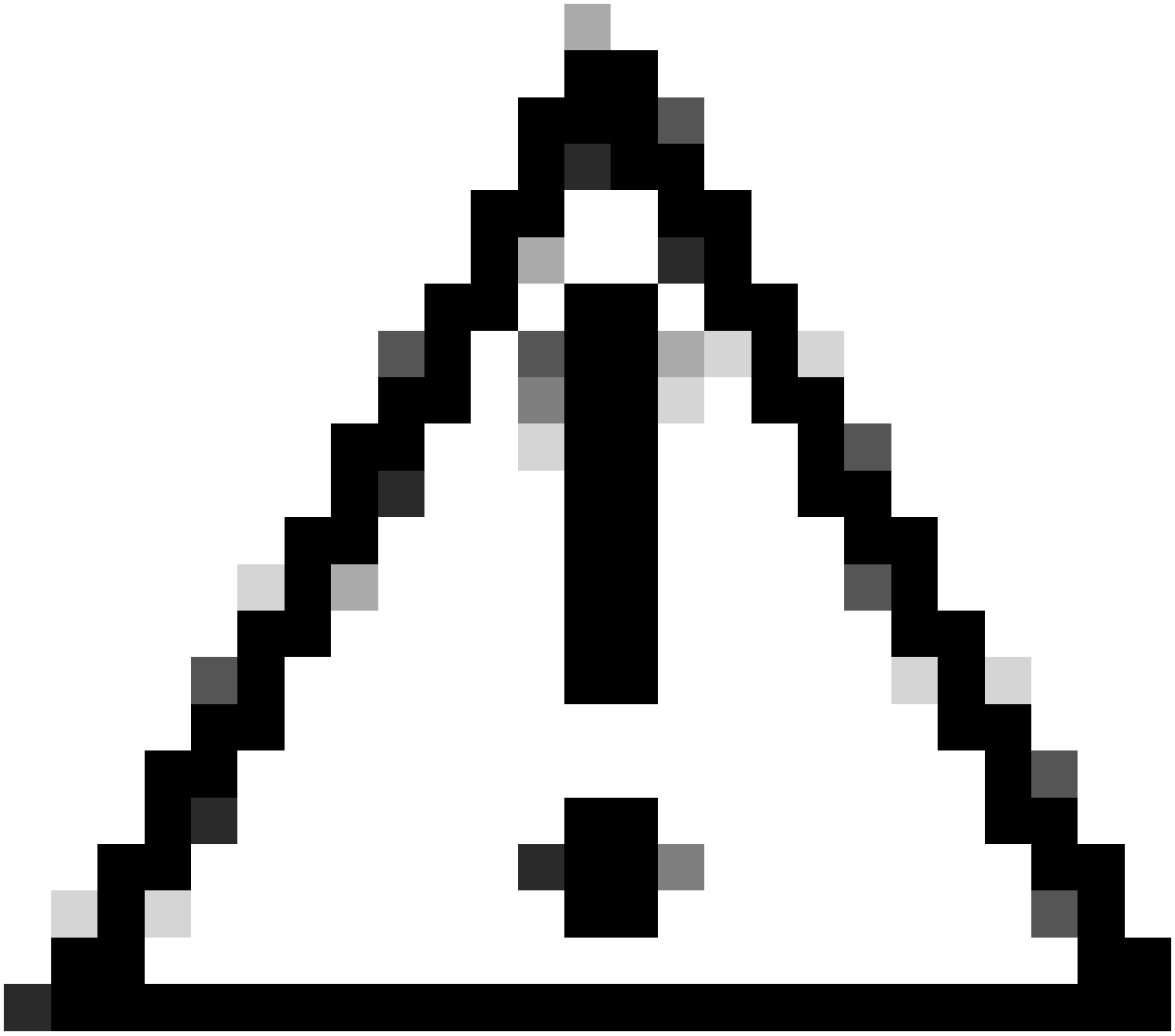
Cliente de roaming - etapas adicionais

Há etapas adicionais que devem ser concluídas para usuários do cliente de roaming independente e do módulo de roaming do AnyConnect:

Tráfego de loopback

Ao selecionar uma interface, você também deve capturar o tráfego na interface de loopback (127.0.0.1), além de outras interfaces de rede. O proxy DNS do cliente de roaming escuta nessa interface, portanto, é vital ver o tráfego entre o sistema operacional e o cliente de roaming.

- Windows: Selecionar adaptador de loopback NPCAP
- Mac: Selecionar loopback: lo0



Caution: As versões mais recentes do Windows do Wireshark são fornecidas com o driver de captura NPCAP, que suporta o driver de loopback. Se o adaptador de loopback estiver ausente, atualize para a versão mais recente do Wireshark ou use as instruções rawcap.exe.

Tráfego DNS criptografado

Em circunstâncias normais, o tráfego entre o cliente de roaming e o Umbrella é criptografado e não legível por humanos. Em alguns casos, o suporte do Umbrella pode solicitar que você desabilite a criptografia DNS para ver o tráfego DNS entre o cliente de roaming e a nuvem do Umbrella. Há dois métodos para fazer isso:

- Crie um bloco de firewall local para UDP 443 a 208.67.220.220 e 208.67.222.222.
- Ou crie o arquivo dependendo do seu SO e da versão do 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 do Windows:

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

- MacOS:

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

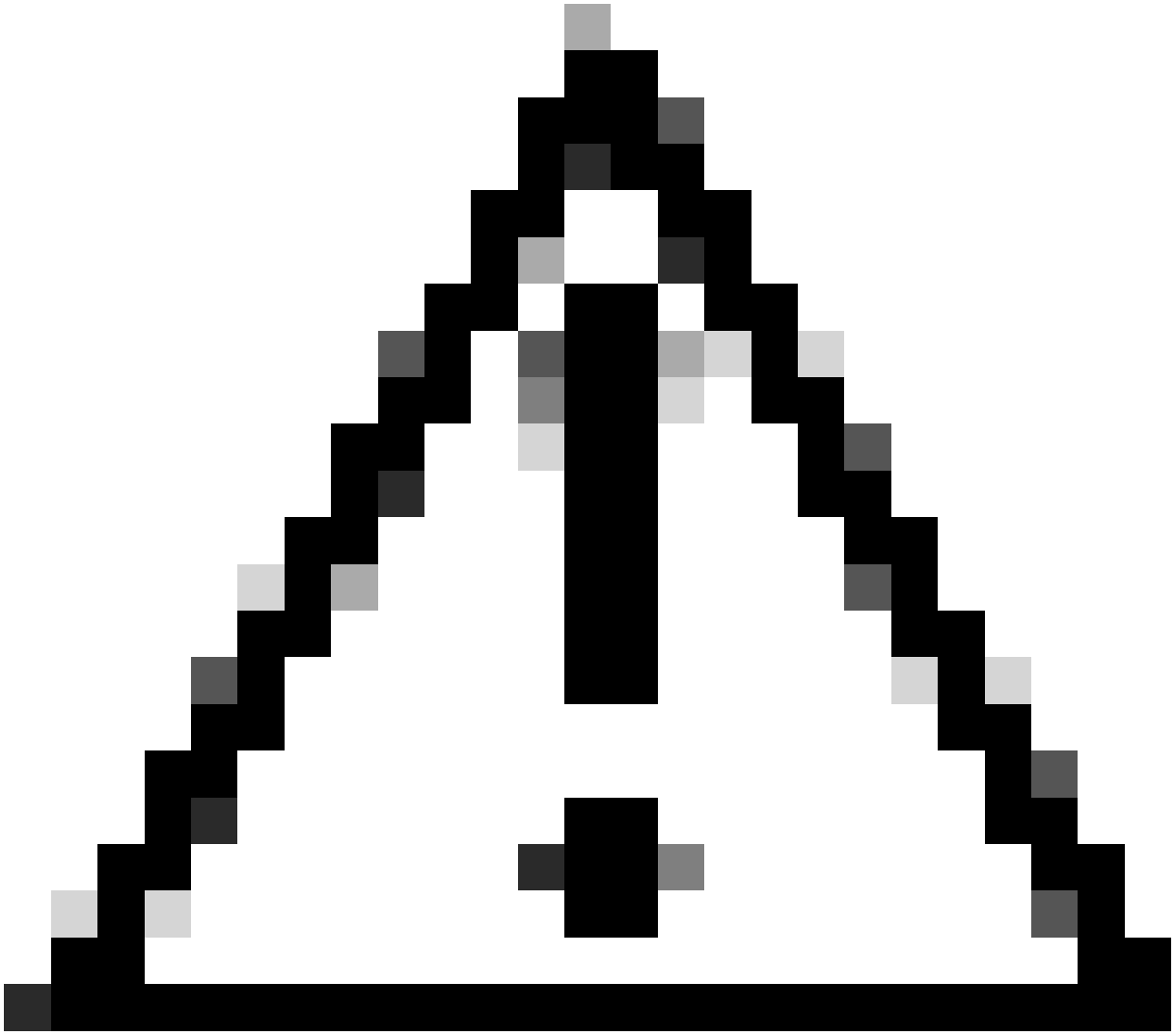
- AnyConnect do Mac OS:

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

- Cliente seguro do Mac OS:

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

Após fazer isso, reinicie o serviço ou o computador.



Caution: As versões mais recentes do Wireshark no Windows incluem o driver de captura NPCAP, que não suporta a interface Umbrella VPN. No Windows, talvez seja necessário usar a ferramenta rawcap.exe como alternativa.

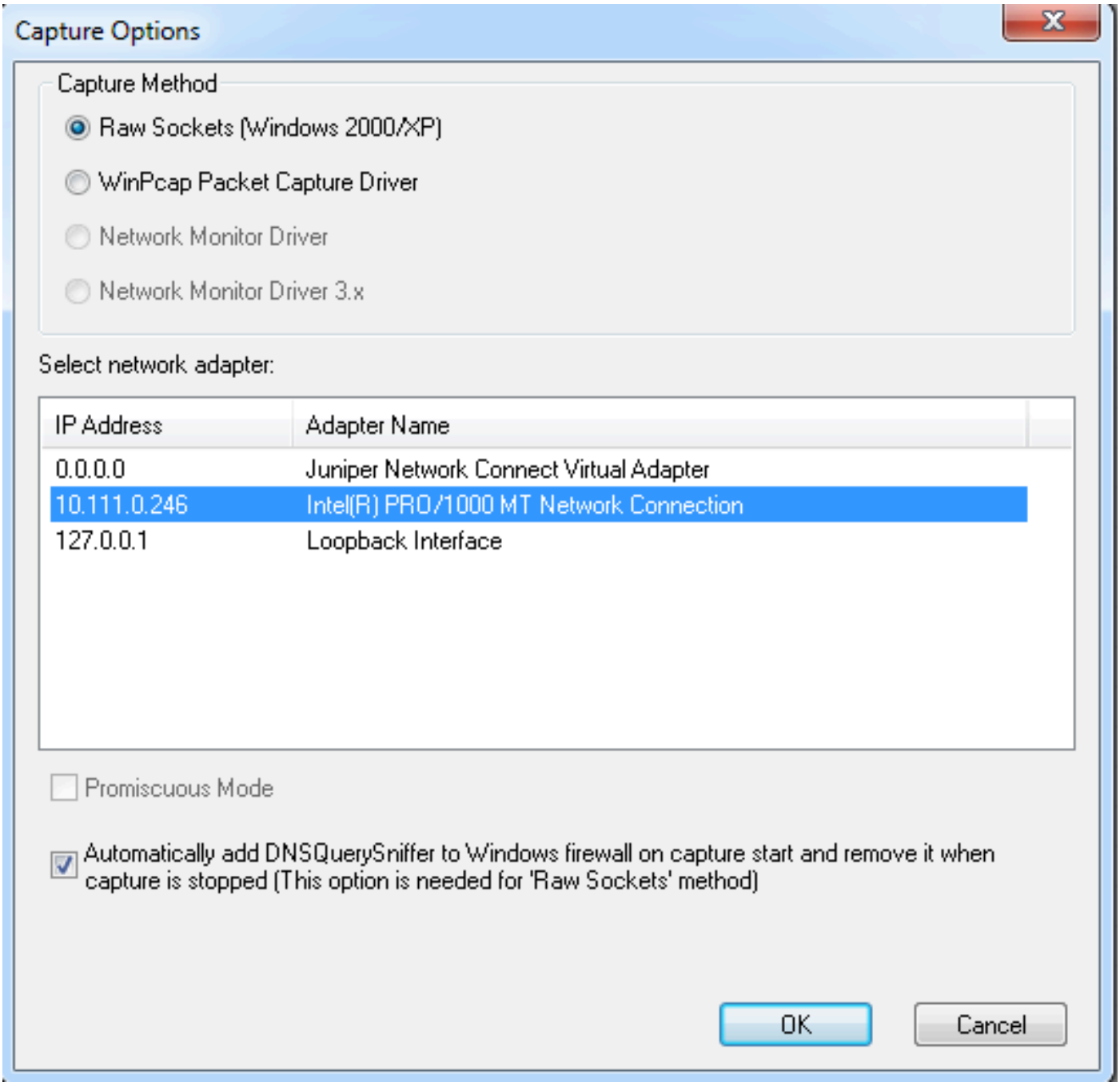
DNSQuerySniffer - Alternativa para Windows

O DNSQuery Sniffer é um sniffer de rede apenas para DNS para Windows que monitora e exibe toneladas de dados úteis. Ao contrário do Wireshark ou Rawcap, ele é usado apenas para DNS e é muito mais fácil de examinar e extrair informações relevantes. No entanto, ele não tem as ferramentas de filtragem poderosas do Wireshark.

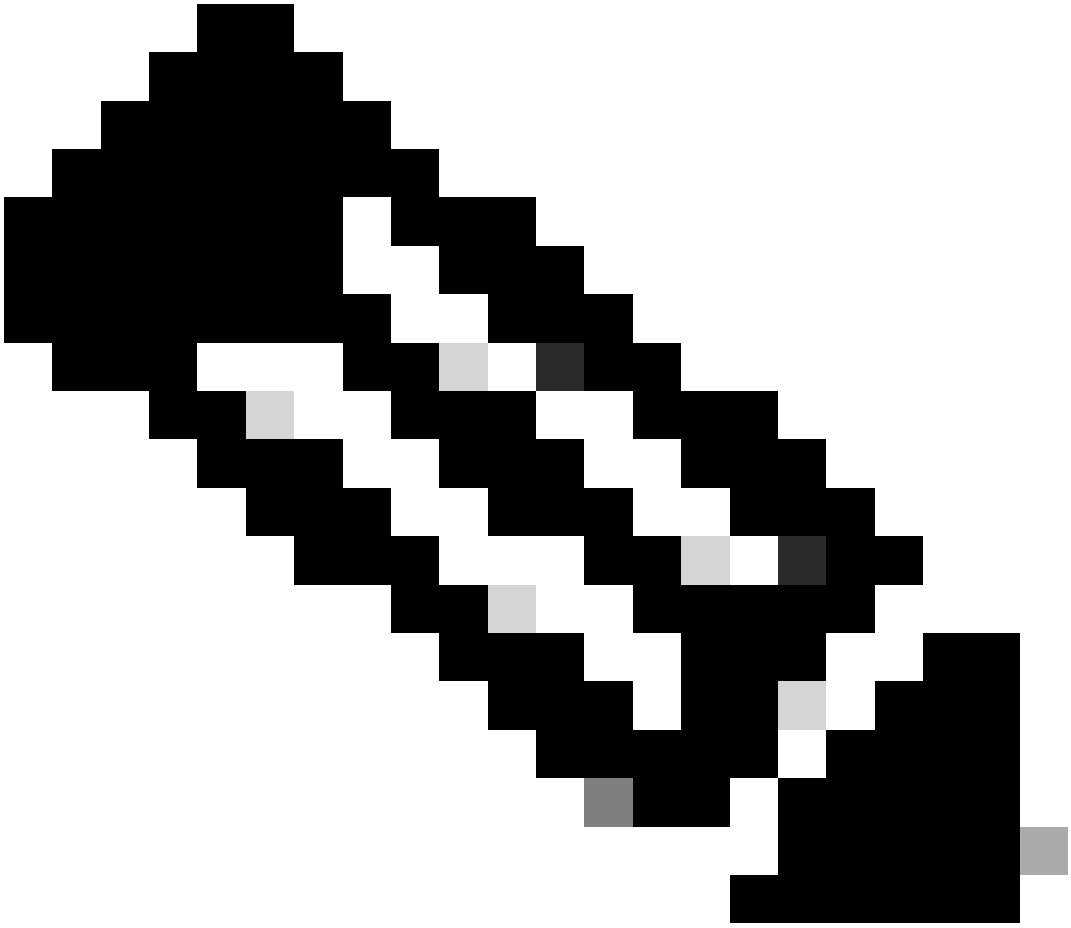
Esta é uma ferramenta leve e fácil de usar. Uma vantagem de usar isso é que você pode farejar pacotes enquanto o serviço do cliente de roaming está desativado, iniciar a captura e ver todas as consultas DNS que o cliente de roaming envia a partir do momento em que inicia, em vez de iniciar uma captura depois que o cliente de roaming já tiver iniciado.

Há dois métodos de captura:

1. Se você selecionar a interface de rede regular, poderá ver apenas as consultas que estão na lista Domínios internos ou que não passaram especificamente pelo dnscryptproxy.



dns_1.png

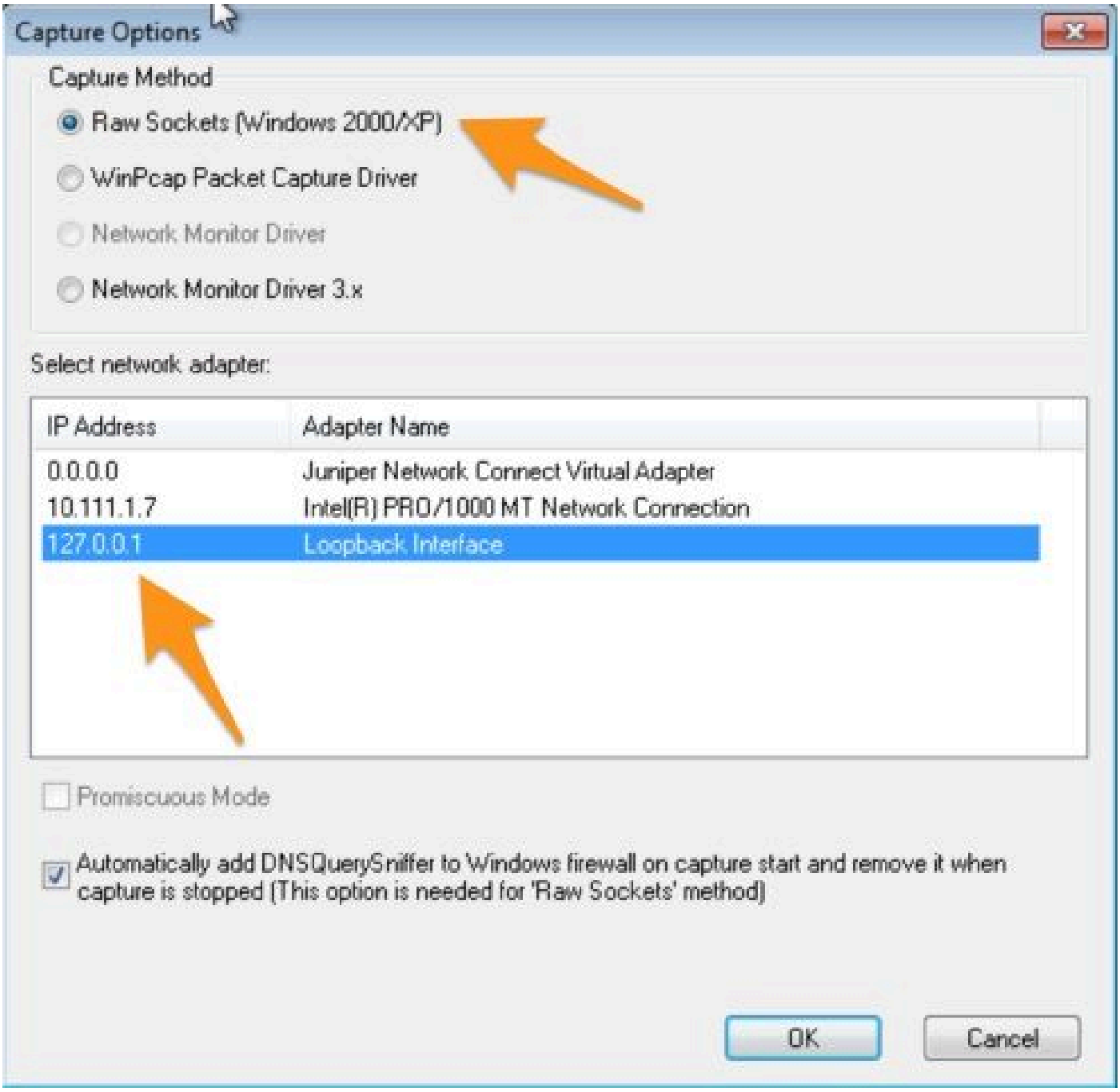


Note: Essas colunas aparecem à direita na captura e você tem que rolar um pouco para vê-las.

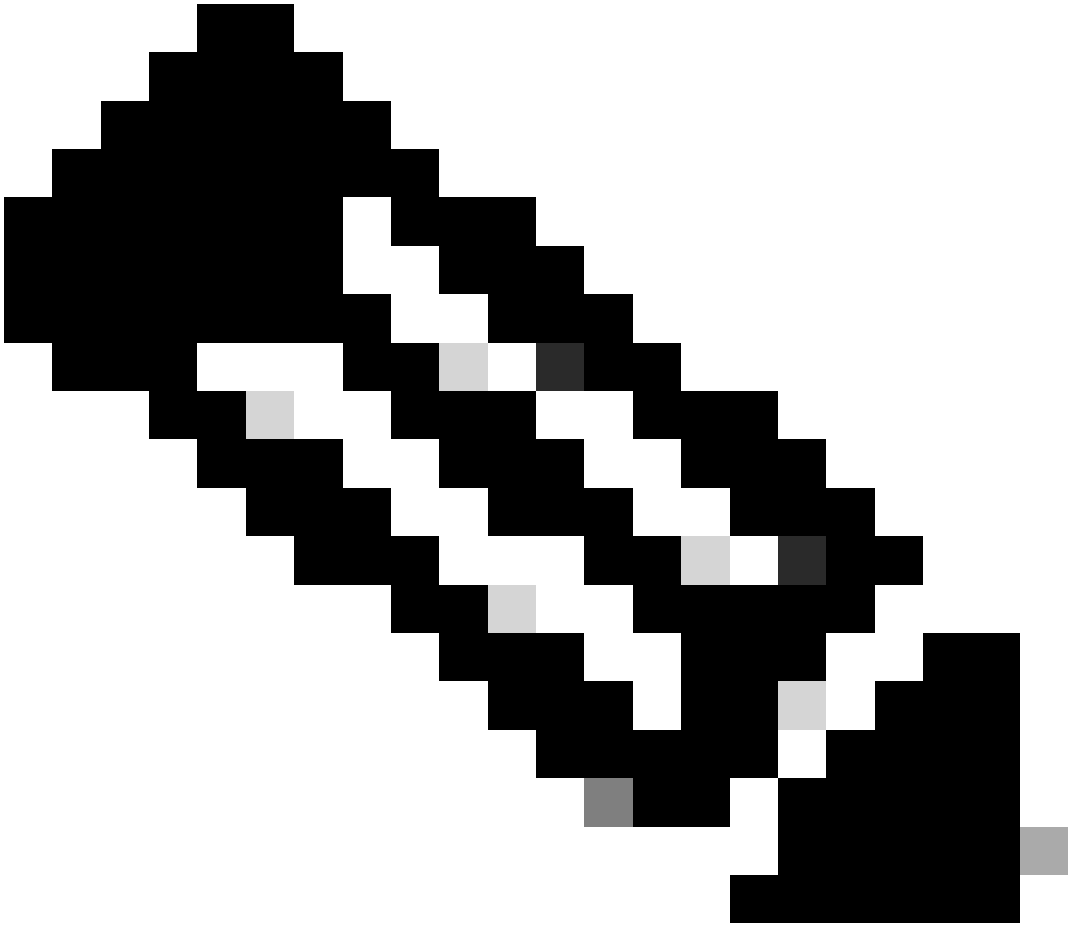
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

Colunas do DNSSniffer

2. Se você selecionar a interface de loopback, verá todas as consultas DNS que são enviadas por meio do dnscryptproxy, mas não poderá ver o endereço IP de destino verdadeiro para domínios na lista Domínios internos. No entanto, ele ainda exibe a consulta e a resposta.


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

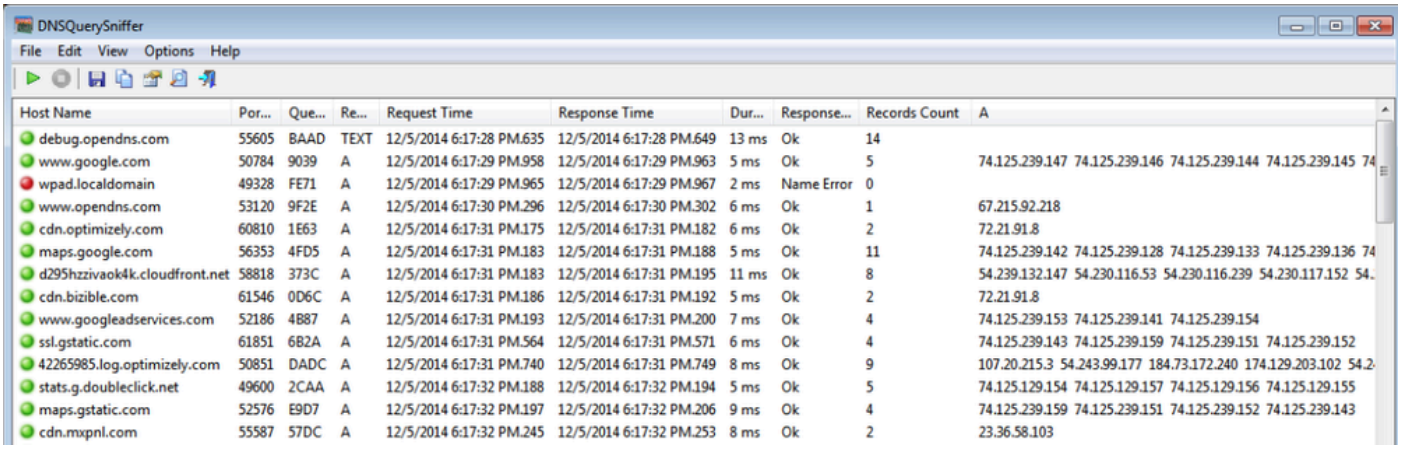


Note: Essas colunas aparecem à direita na captura, e você tem que rolar um pouco para vê-las.

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

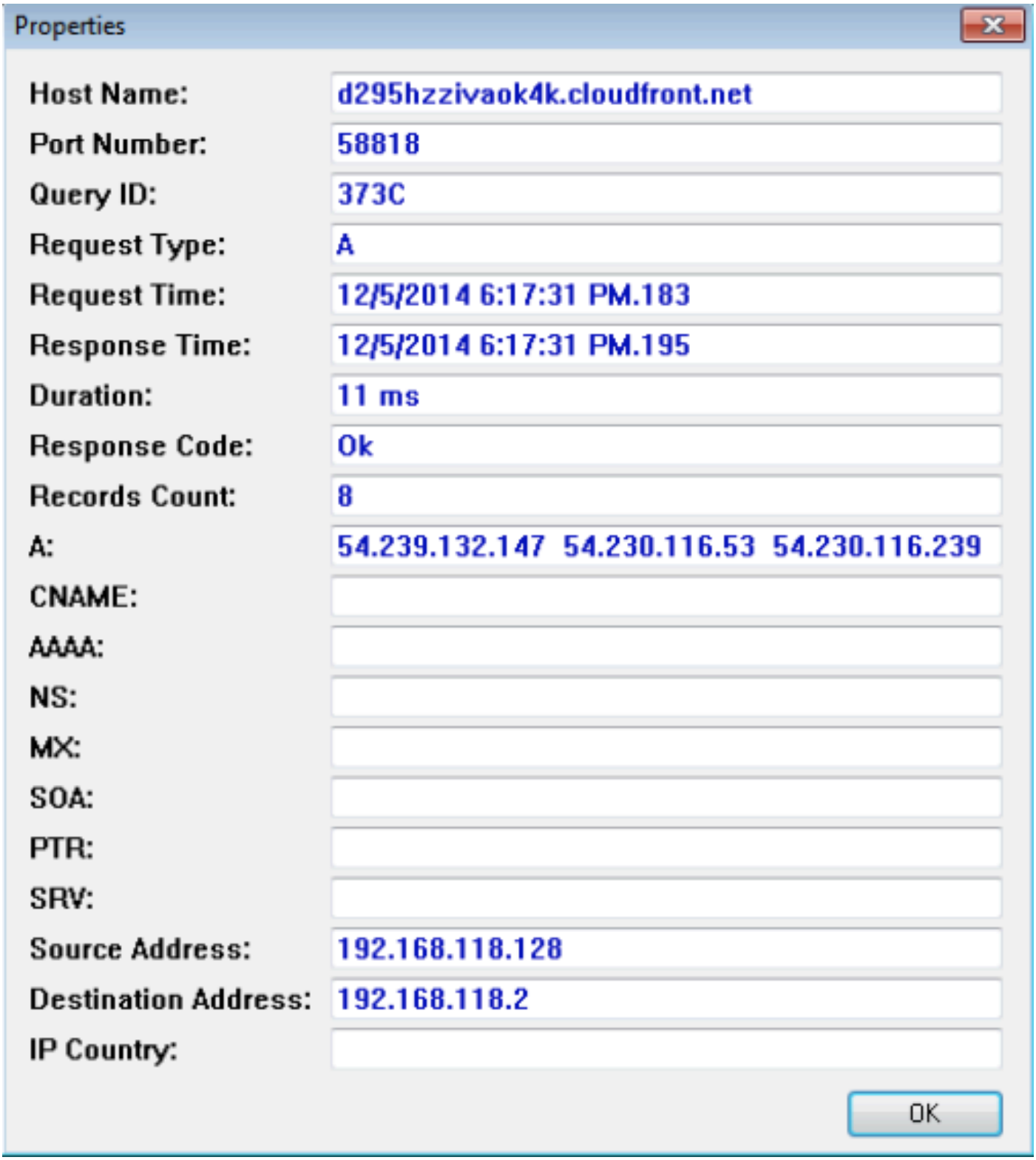
Colunas do DNSSniffer

Os resultados se parecem com:



dns_3.png

Exibição de uma pesquisa individual:



dns_4.png

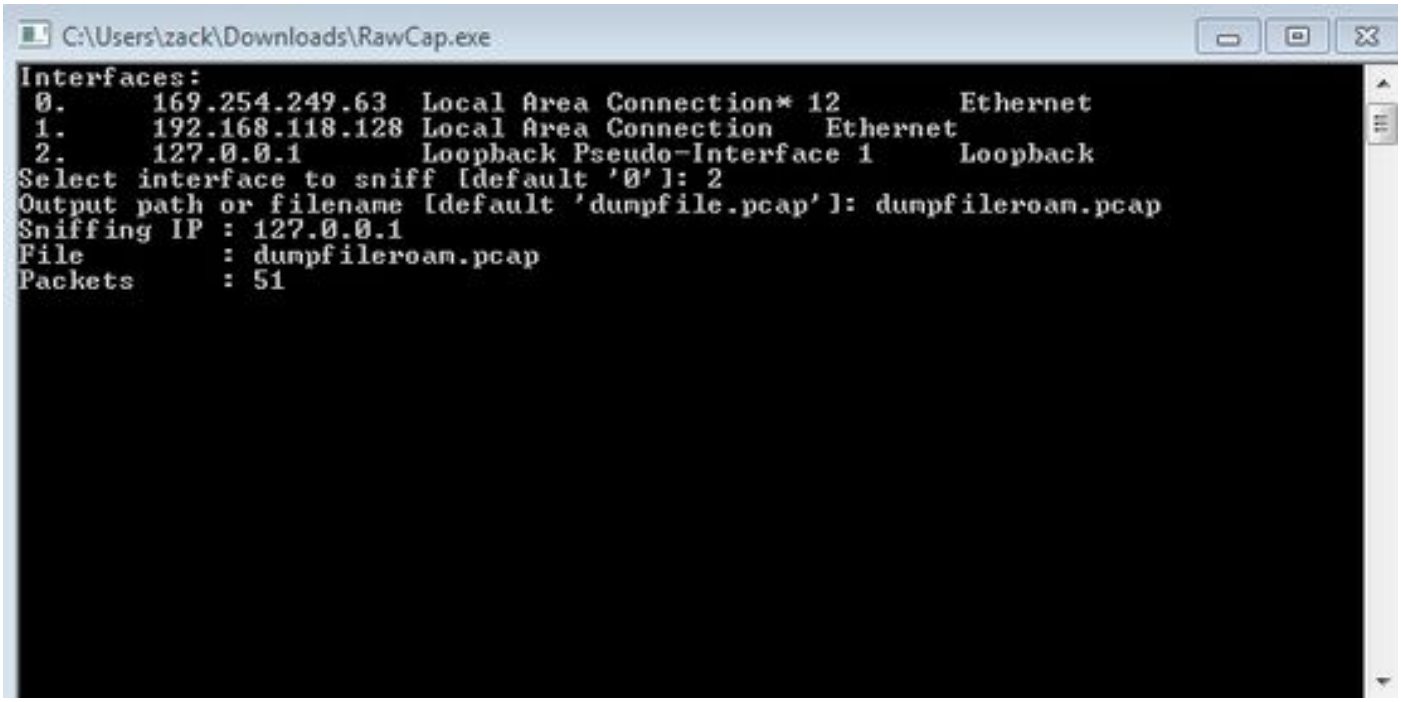
RawCap.exe - Alternativa para Windows

Em algumas circunstâncias, a interface com a qual você precisa trabalhar não é suportada pelo driver de captura de pacotes incluído no Wireshark. Isso pode ser um problema para a interface de loopback.

Nesses casos, podemos usar RawCap.exe:

1. Conclua os passos desde o início do artigo para usar o Wireshark para capturar o tráfego normal.
2. Ao mesmo tempo, execute RawCap.exe.
3. Selecione a interface especificando o número da lista correspondente.
4. Especifique um nome de arquivo de saída e desative-o.
5. SelectControl-Cquando quiser interromper a captura.

O arquivo salvo é colocado na pasta da qual você executou RawCap.exe:



rawcap_1.jpg

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.