Netwerkverkeer vastleggen met Wireshark

Inhoud

Inleiding

In dit document wordt beschreven hoe u netwerkverkeer kunt vastleggen met Wireshark.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Umbrella DNS Layer Security.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Er zijn momenten waarop Cisco Umbrella Support-medewerkers vragen om een pakketopname van het internetverkeer dat tussen uw computer en het netwerk stroomt. Met de opname kan Umbrella Support het verkeer op een laag niveau analyseren en potentiële problemen identificeren.

In de meeste gevallen is het handig om twee sets pakketopnames te vergelijken die zowel een werkend als een niet-werkend scenario aantonen.

- Zorg ervoor dat u het probleem kunt repliceren en deze stappen kunt voltooien terwijl het probleem zich voordoet. Genereer een pakketopname met een niet-werkend scenario. Houd rekening met de datum en tijd met de tijdzone, zodat deze informatie kan worden gecorreleerd met andere gegevens.
- Herhaal deze instructies indien mogelijk met Umbrella software (en/of Umbrella DNS forwarding) uitgeschakeld. Genereer een pakketopname die het werkscenario laat zien. Houd rekening met de datum en tijd met de tijdzone, zodat deze informatie kan worden gecorreleerd met andere gegevens.

Wireshark-instructies

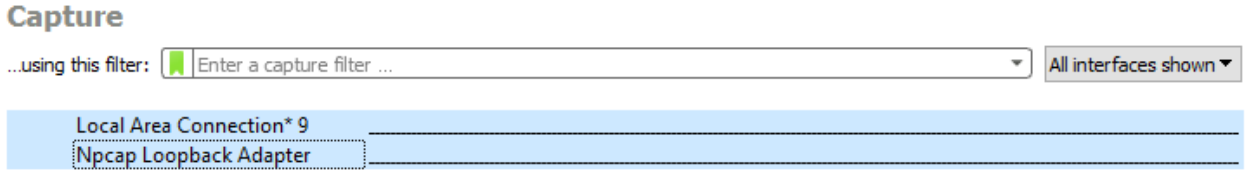
Voorbereidingen

1. Download Wireshark.
2. Verbreek de verbinding met onnodige netwerkverbindingen.
    1. Verbreek de VPN-verbindingen, tenzij ze nodig zijn om het probleem te repliceren.
    2. Gebruik alleen een bekabelde of draadloze verbinding en niet beide samen.
3. Sluit alle andere software die niet nodig is om het probleem te repliceren.
4. Verwijder de cookies en cache uit uw browser.
5. Spoel je DNS Cache door. In Windows met de opdracht:

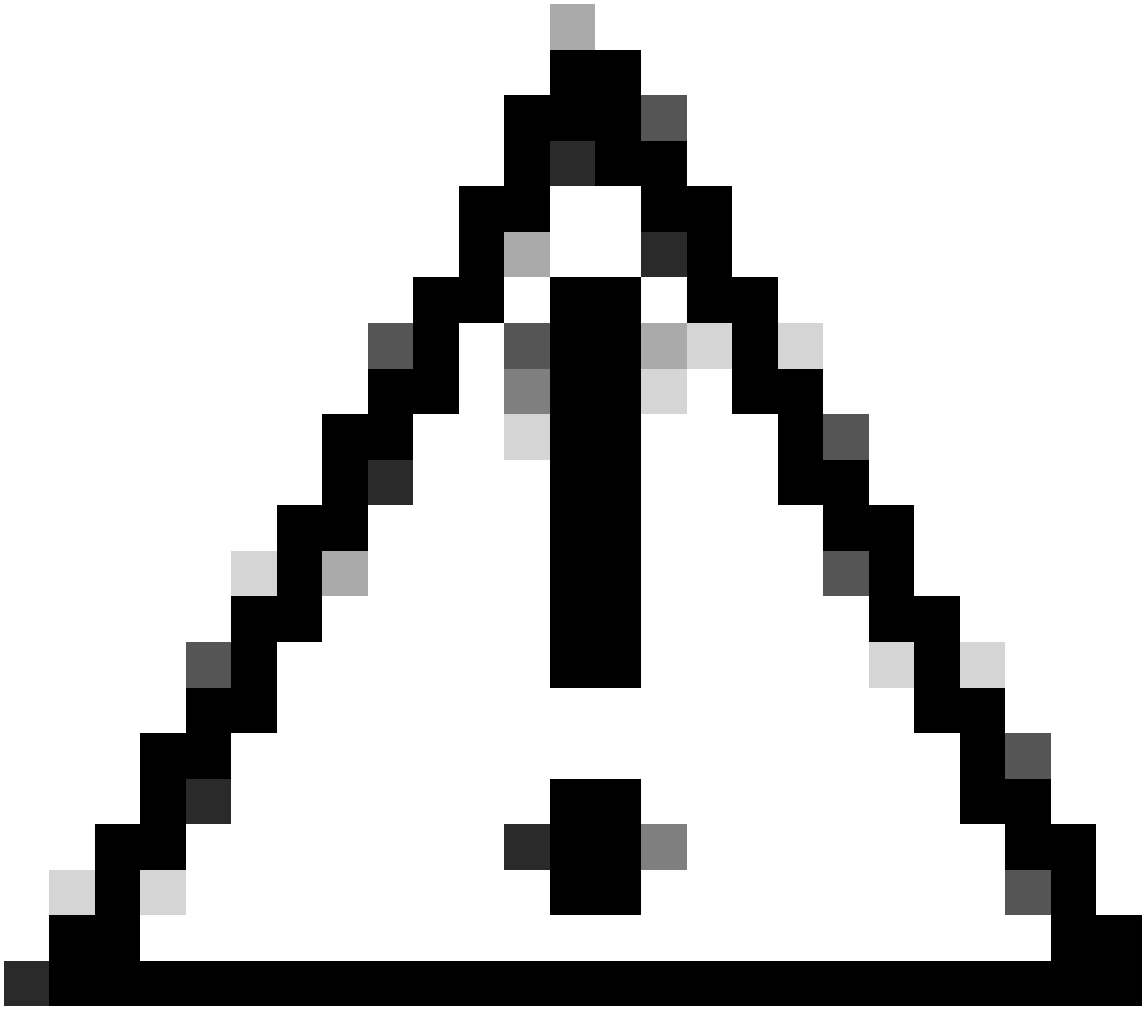
```
ipconfig /flushdns
```

Basic Wireshark Capture

1. Start Wireshark.
2. Het deelvenster Vastleggen toont uw netwerkinterfaces. Selecteer de relevante interfaces. U kunt meerdere interfaces selecteren met de CTRL-toets (Windows) of de CMD-toets (Mac) terwijl u selecteert.



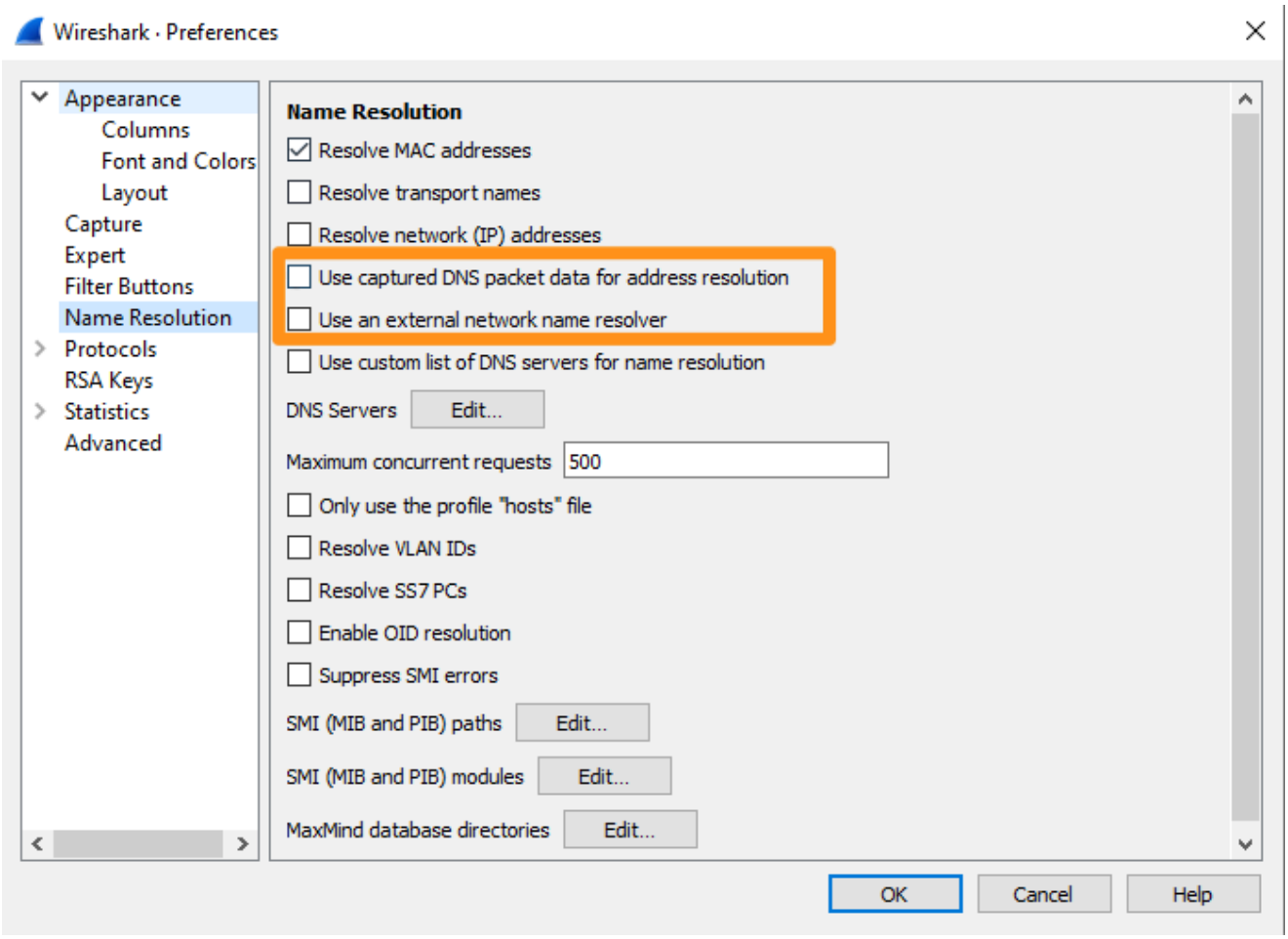
Wireshark_1.png



Let op: Het is belangrijk om de juiste interface(s) te selecteren die netwerkverkeer bevatten. Gebruik de opdracht "ipconfig" (Windows) of "ifconfig" (Mac) om meer details over uw netwerkinterfaces te bekijken. Zwervende clientgebruikers moeten daarnaast de NPCAP Loopback Adapter OF Loopback: lo0-interfaces selecteren. Als u twijfelt, selecteert u alle interfaces.

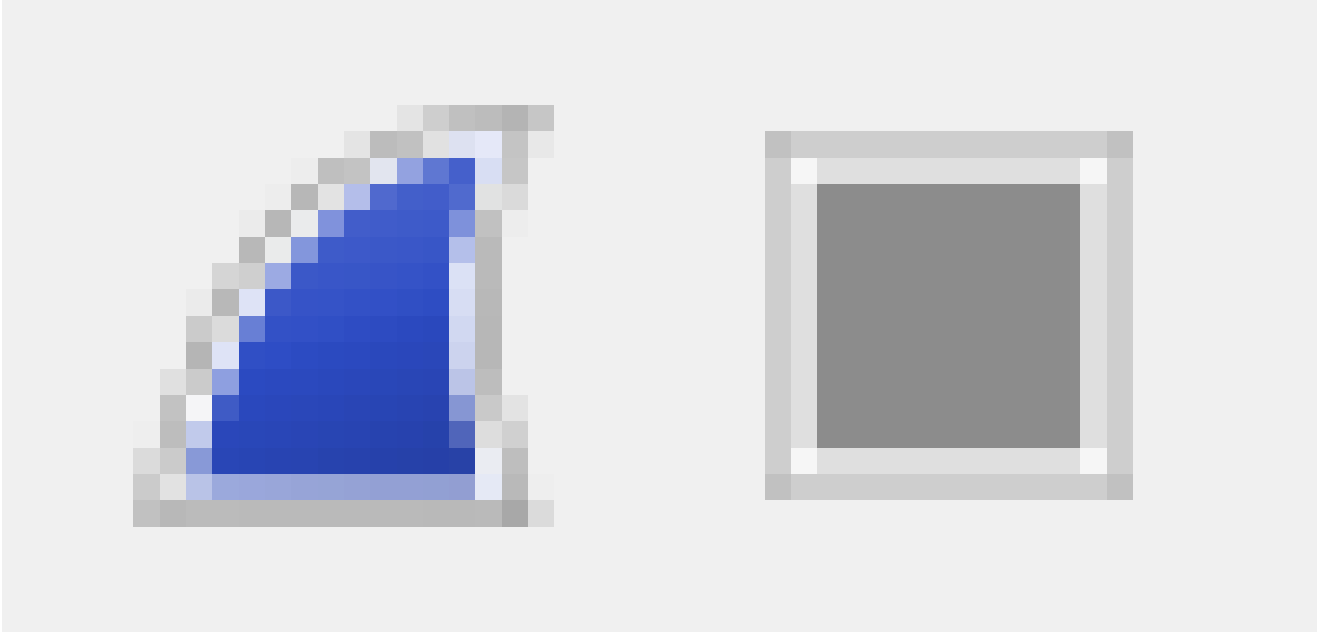
---

3. Zorg ervoor dat vastgelegde DNS-pakketgegevens gebruiken voor adresresolutie en gebruik een externe netwerknaamoplosser NIET zijn geselecteerd om ervoor te zorgen dat Wireshark geen DNS-query's maakt, omdat dit het vastleggen kan bemoeilijken en AnyConnect kan beïnvloeden. Instellingen zijn geldig vanaf Wireshark 3.4.9:



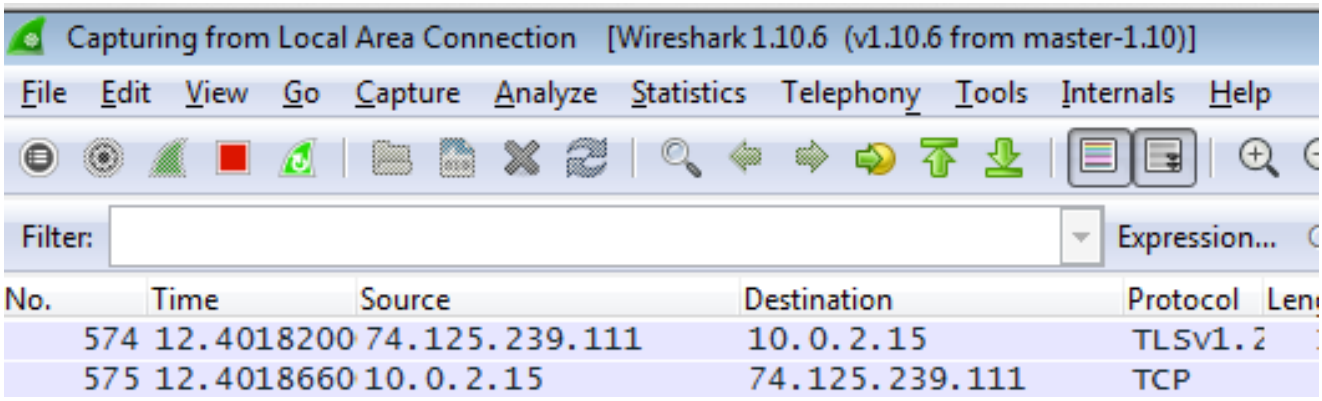
Capture_PNG.png

4. Selecteer Vastleggen > Starten of selecteer het pictogram Blauw starten.



Wireshark_2.png

5. Terwijl Wireshark op de achtergrond wordt uitgevoerd, repliceert u het probleem.



Wireshark_3.png

6. Zodra het probleem volledig is gerepliceerd, selecteert u Vastleggen > Stoppen of gebruikt u het rode pictogram Stoppen.
7. Navigeer naar Bestand > Opslaan als en selecteer een plaats om het bestand op te slaan. Controleer of het bestand is opgeslagen als een PCAPNG-type. Het opgeslagen bestand kan ter beoordeling worden ingediend bij Cisco Umbrella Support.

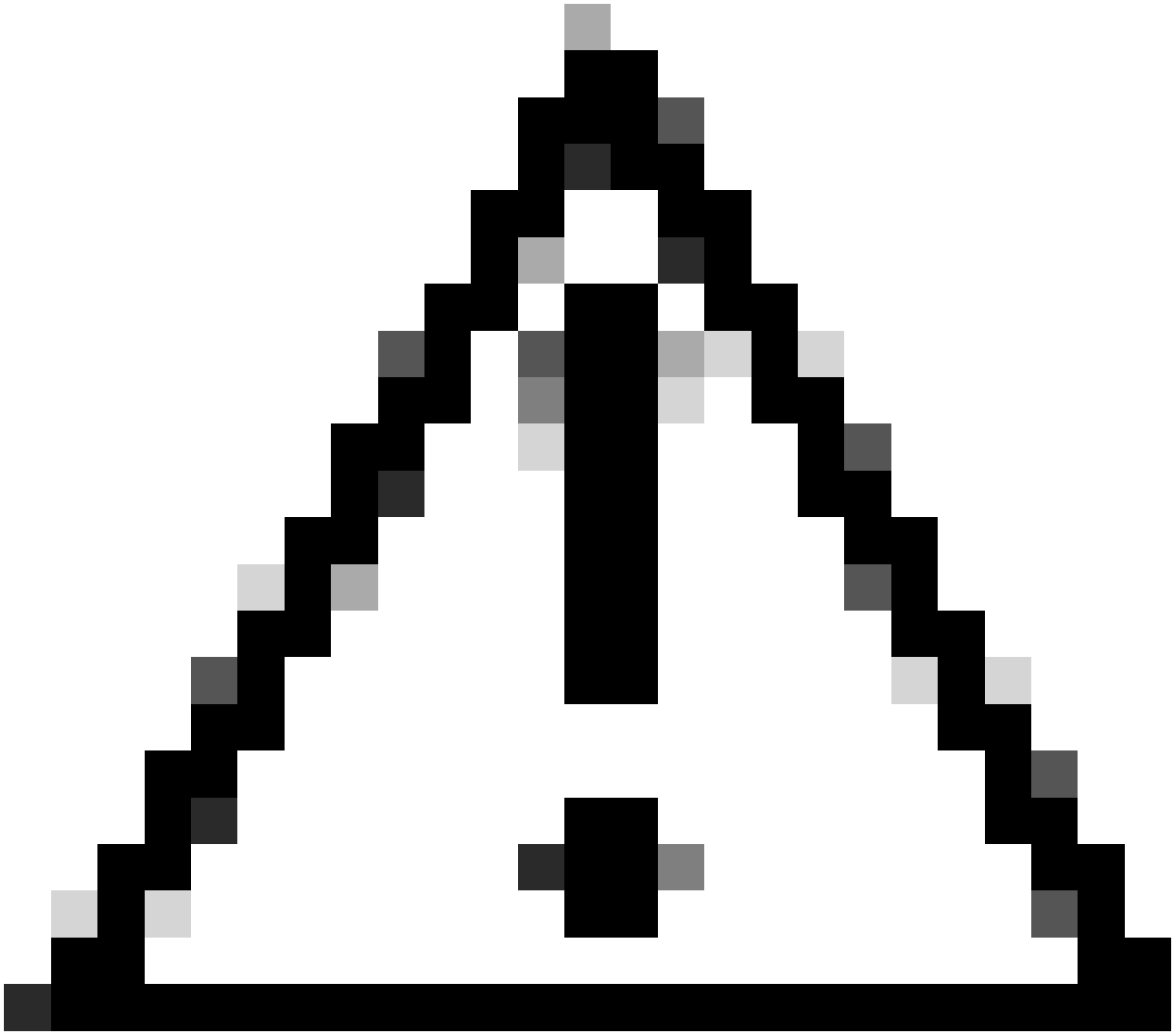
Zwervende client - aanvullende stappen

Er zijn aanvullende stappen die moeten worden uitgevoerd voor gebruikers van zowel de zelfstandige roamingclient als de AnyConnect-roamingmodule:

Loopback-verkeer

Wanneer u een interface selecteert, moet u naast andere netwerkinterfaces ook verkeer vastleggen op de loopback-interface (127.0.0.1). De DNS-proxy van de roamingclient luistert naar deze interface, dus het is van vitaal belang om het verkeer tussen het besturingssysteem en de roamingclient te zien.

- Windows: NPCAP-loopbackadapter selecteren
- Mac: Selecteer Loopback: lo0



Let op: Nieuwere Windows-versies van Wireshark worden geleverd met het NPCAP-opnamestuurprogramma, dat het loopback-stuurprogramma ondersteunt. Als de loopback-adapter ontbreekt, werkt u deze bij naar de nieuwste versie van Wireshark of gebruikt u de instructies voor rawcap.exe.

Gecodeerd DNS-verkeer

In normale omstandigheden is het verkeer tussen de roamingclient en de paraplu versleuteld en niet leesbaar voor mensen. In sommige gevallen kan Umbrella Support u vragen om DNS-codering uit te schakelen om het DNS-verkeer tussen de Zwervende client en de Umbrella-cloud te zien. Er zijn twee methoden om dit te doen:

- Maak een lokaal firewallblok voor UDP 443 tot 208.67.220.220 en 208.67.222.222.
- Of maak het bestand afhankelijk van uw besturingssysteem en de versie van de zwervende client:
    - Windows:

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

- Windows AnyConnect:

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

- Windows Secure Client:

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

- macOS:

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

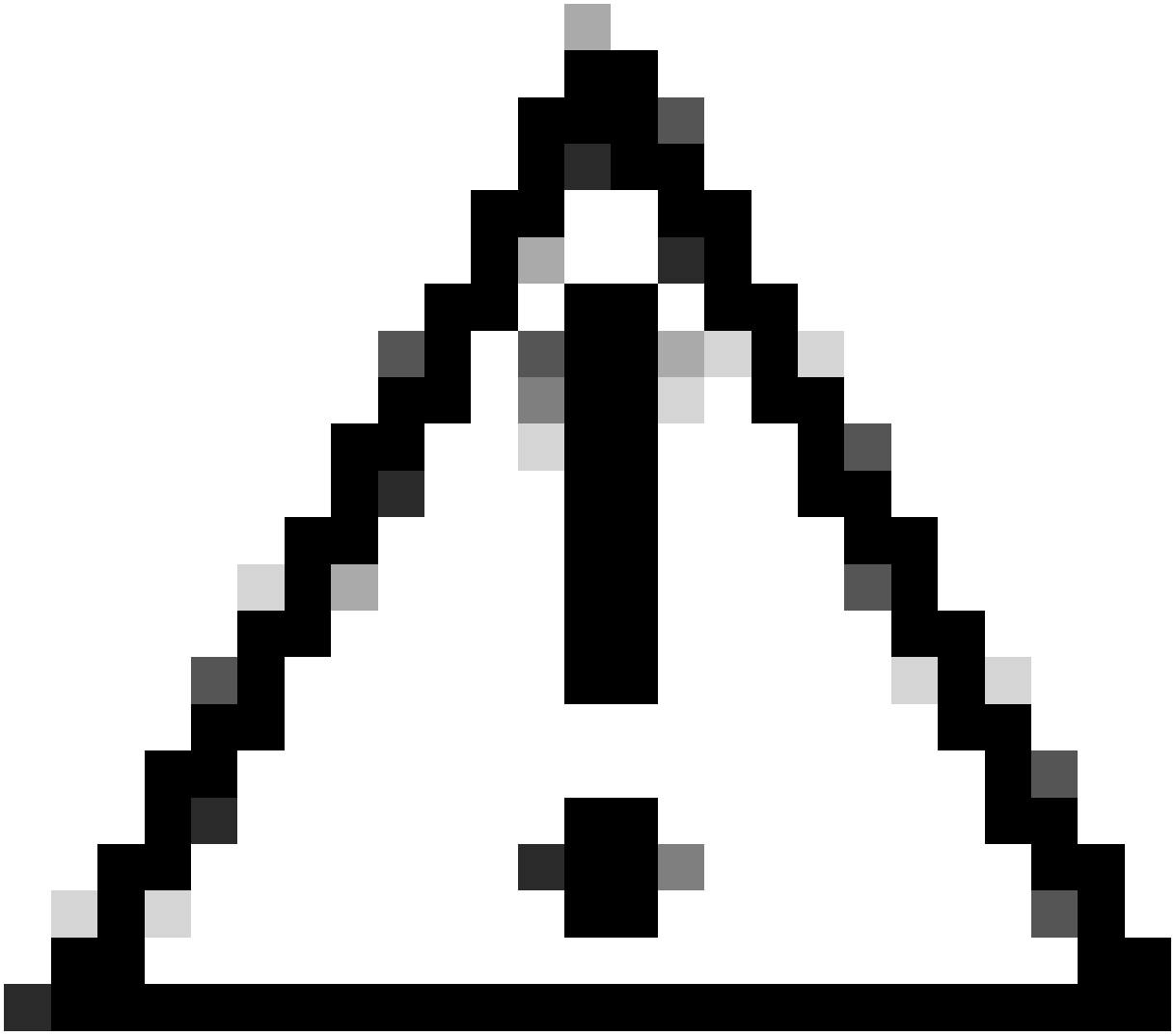
- mac OS AnyConnect:

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

- mac OS Secure Client:

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

Start de service of uw computer opnieuw op nadat u dit hebt gedaan.



Waarschuwing: Nieuwere versies van Wireshark op Windows bevatten NPCAP capture driver, die de Umbrella VPN-interface niet ondersteunt. In Windows moet u mogelijk het hulpprogramma rawcap.exe als alternatief gebruiken.

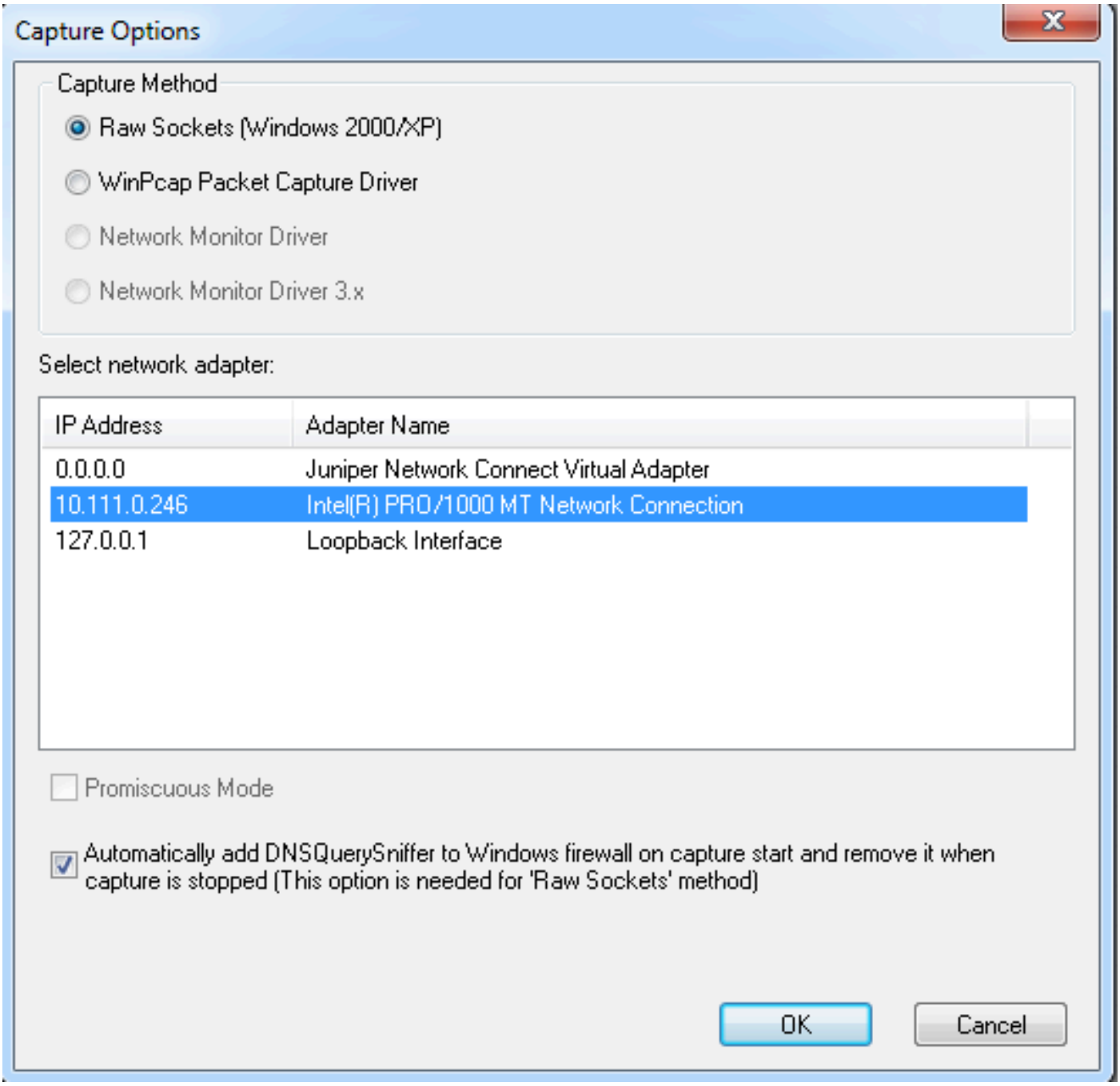
DNSQuerySniffer - Windows Alternative

DNSQuery Sniffer is een DNS-only netwerksnuiver voor Windows die tonnen nuttige gegevens bewaakt en weergeeft. In tegenstelling tot Wireshark of Rawcap, wordt het alleen gebruikt voor DNS en is het veel gemakkelijker om relevante informatie te onderzoeken en te extraheren. Het heeft echter niet de krachtige filtertools van Wireshark.

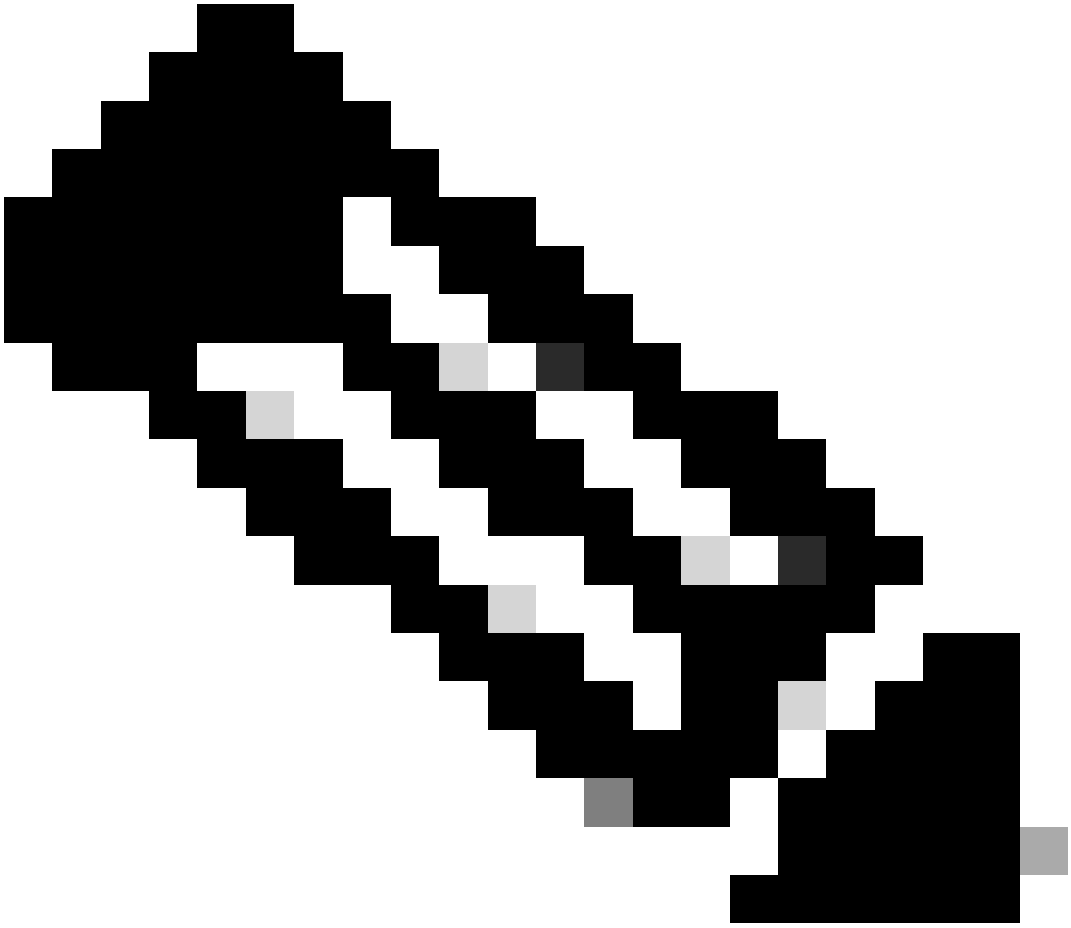
Dit is een lichtgewicht en eenvoudig te gebruiken tool. Een voordeel van het gebruik hiervan is dat u pakketten kunt snuiven terwijl de Roaming Client-service is uitgeschakeld, de opname kunt starten en u elke DNS-query kunt zien die de Roaming Client verzendt vanaf het moment dat deze wordt gestart in plaats van een opname te starten nadat de Roaming Client al is gestart.

Er zijn twee vangmethoden:

1. Als u de reguliere netwerkinterface selecteert, kunt u alleen query's zien die in de lijst Interne domeinen staan of die niet specifiek door de dencryptproxy zijn gegaan.



DNS_1.png

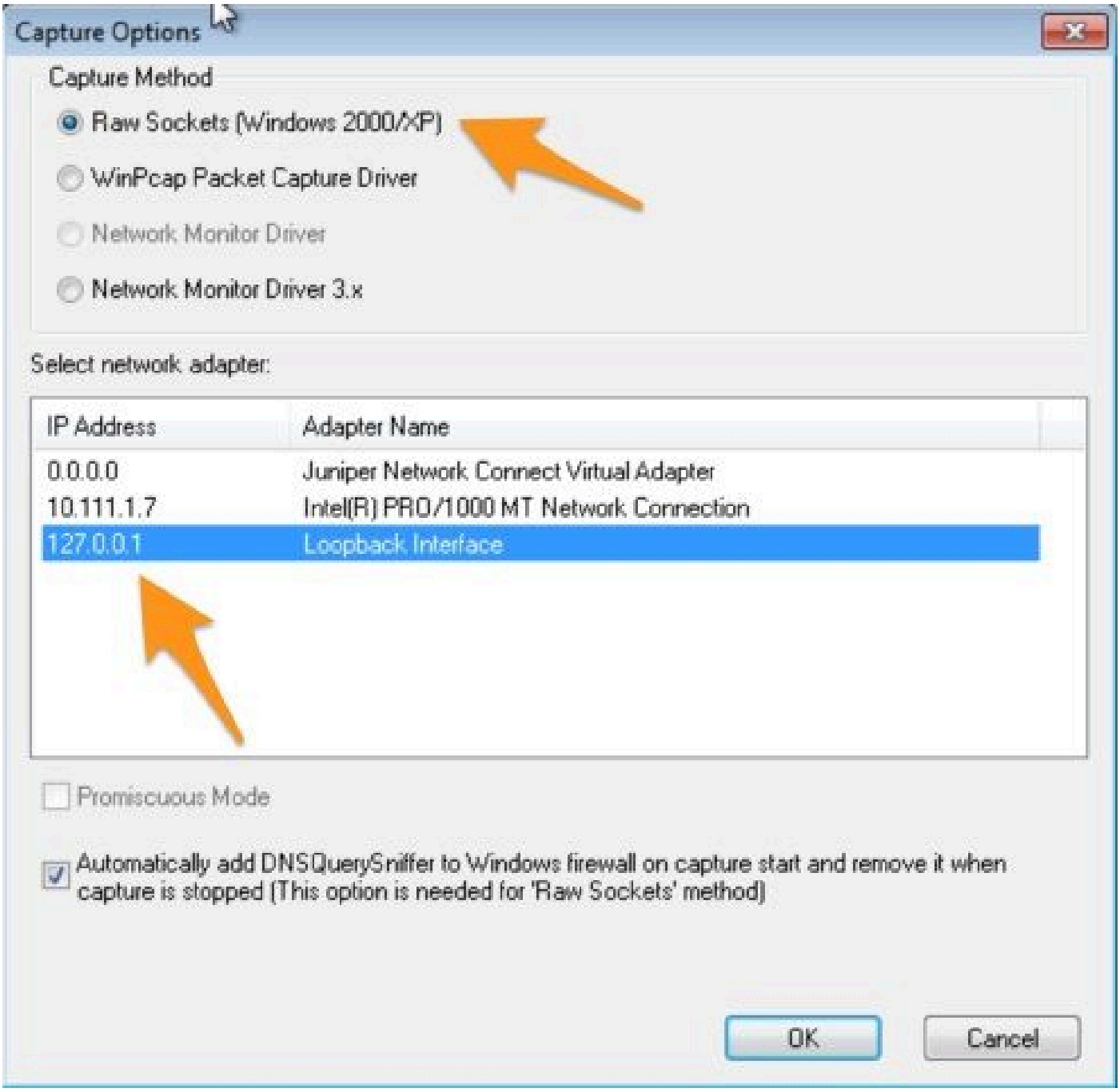


Opmerking: deze kolommen verschijnen helemaal rechts in de opname en je moet behoorlijk scrollen om ze te zien.

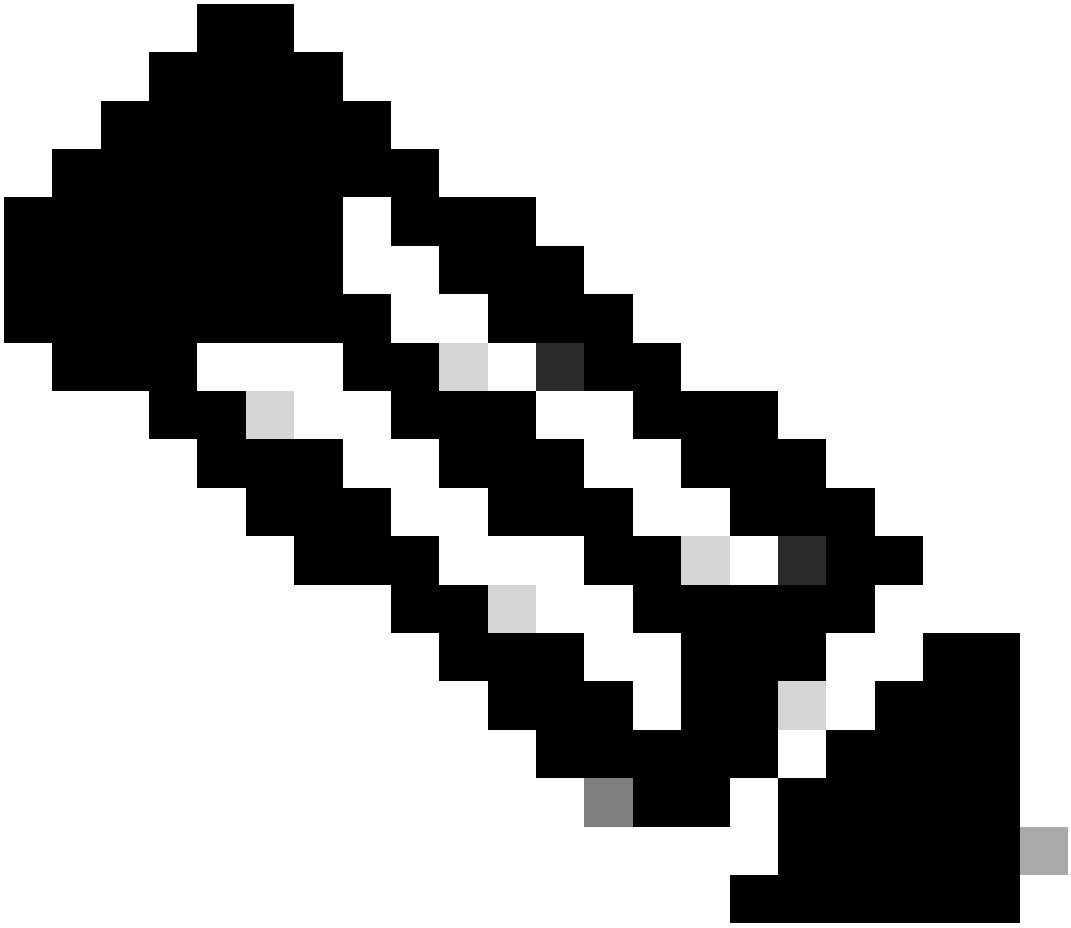
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

DNSSniffer-kolommen

2. Als u de Loopback-interface selecteert, ziet u alle DNS-query's die via de encryptieproxy worden verzonden, maar ziet u niet het echte IP-adres van de bestemming voor domeinen in de lijst Interne domeinen. Het geeft echter nog steeds de vraag en het antwoord weer.


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

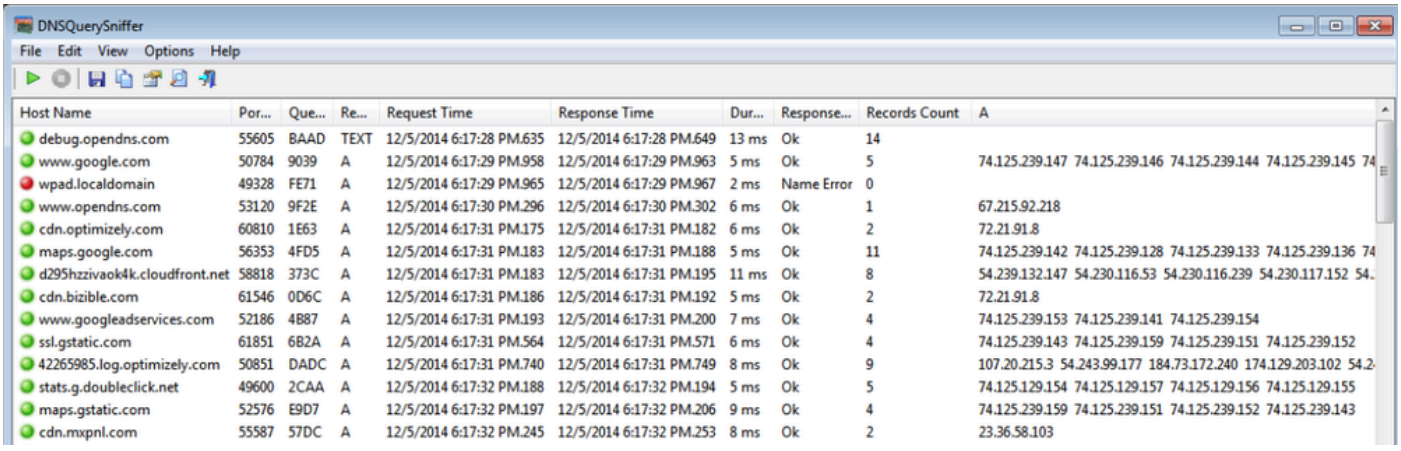


Opmerking: deze kolommen verschijnen helemaal rechts in de opname en je moet nogal wat scrollen om ze te zien.

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

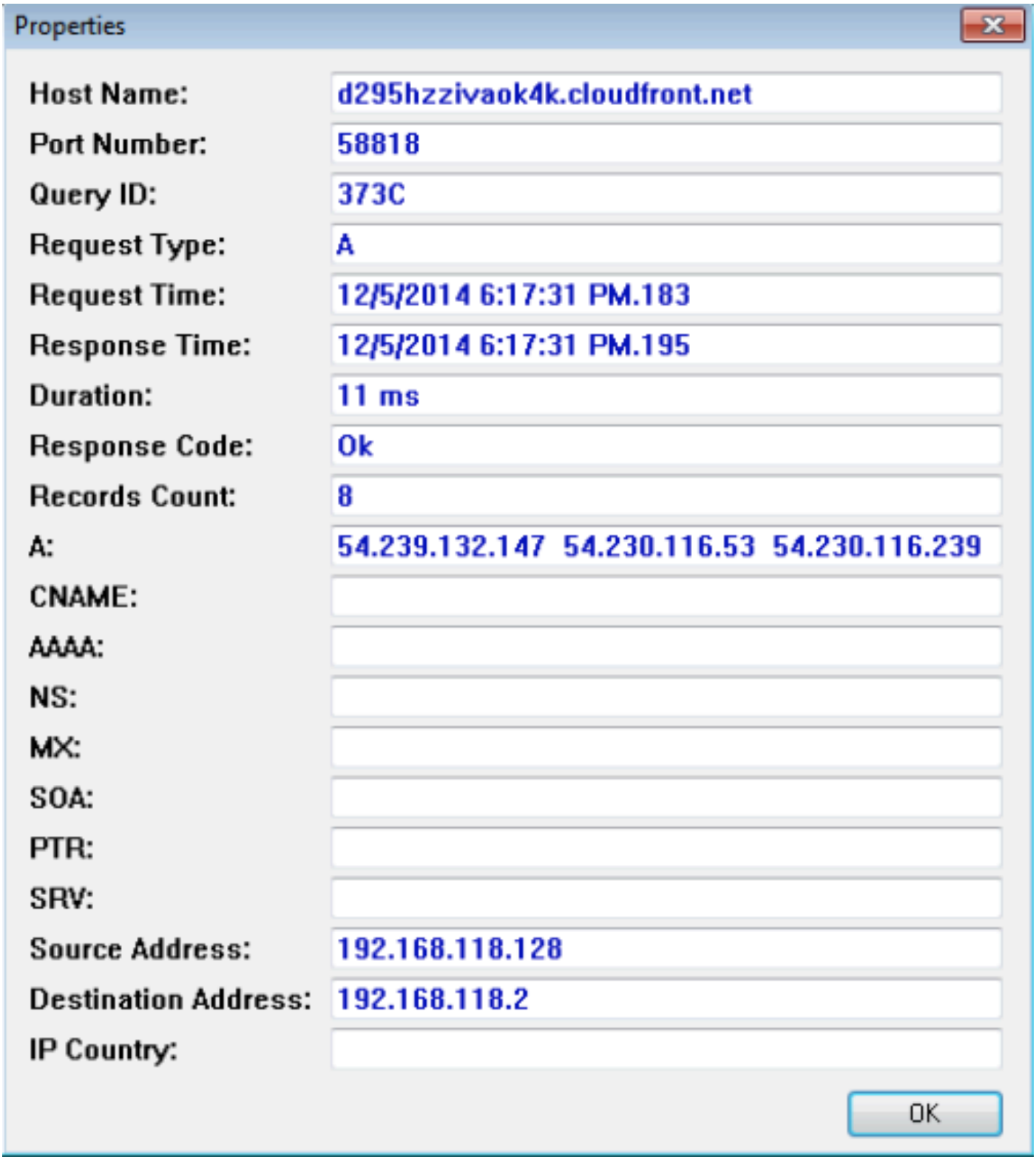
DNSSniffer-kolommen

De resultaten zien er als volgt uit:



DNS_3.PNG

Overzicht van een individuele lookup:



DNS_4.PNG

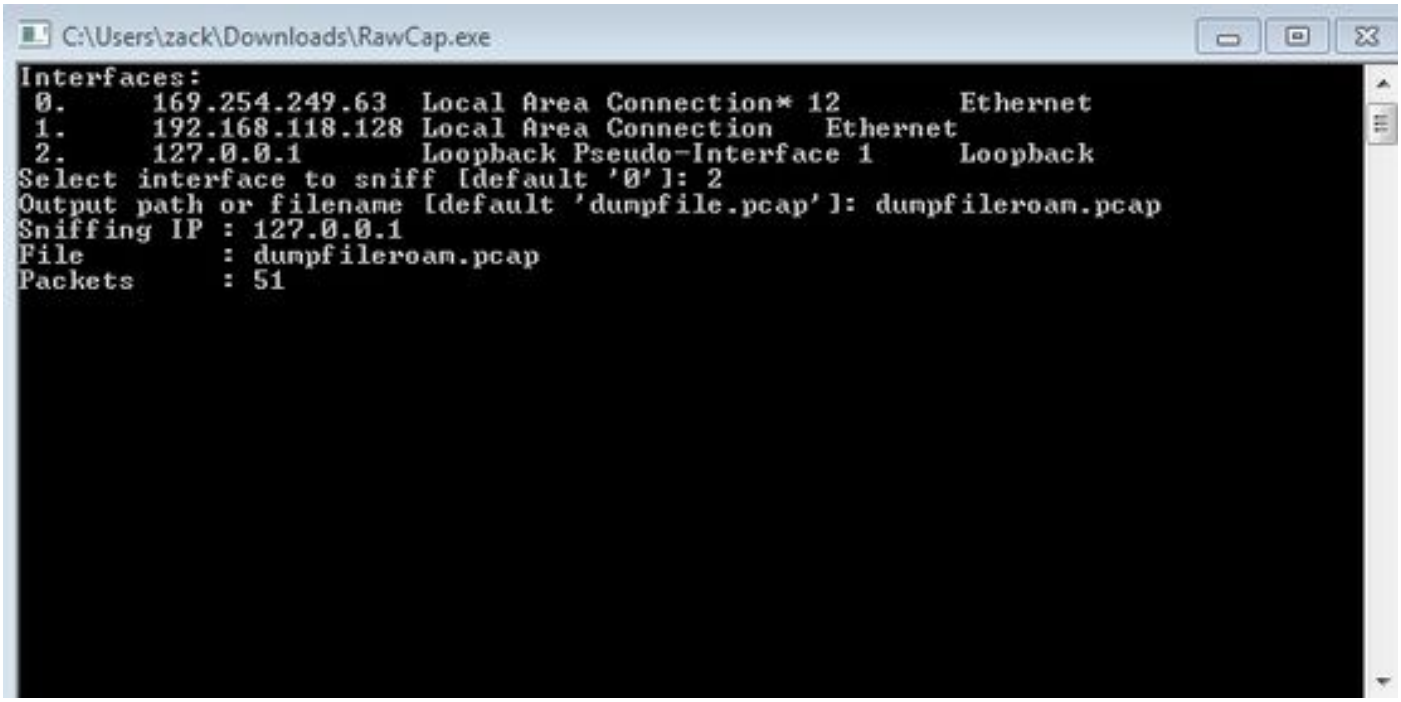
RawCap.exe - Windows Alternatief

In sommige omstandigheden wordt de interface waarmee u moet werken niet ondersteund door het stuurprogramma voor pakketregistratie dat bij Wireshark is geleverd. Dit kan een probleem zijn voor de loopback-interface.

In deze gevallen kunnen we RawCap.exe gebruiken:

1. Voltooi de stappen van eerder in het artikel om Wireshark te gebruiken om normaal verkeer vast te leggen.
2. Voer tegelijkertijd RawCap.exe uit.
3. Selecteer de interface door het bijbehorende lijstnummer op te geven.
4. Geef een uitvoerbestandsnaam op en deze wordt uitgeschakeld.
5. Selecteer Control-C wanneer u de opname wilt stoppen.

Het opgeslagen bestand wordt geplaatst in de map van waaruit u RawCap.exe hebt uitgevoerd:



rawcap_1.jpg

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.