Acquisire il traffico di rete con Wireshark

Sommario

Introduzione

Questo documento illustra come acquisire il traffico di rete con Wireshark.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulla sicurezza del livello DNS Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

In alcuni casi, il personale del supporto Cisco Umbrella chiede di acquisire un pacchetto del traffico Internet che passa tra il computer e la rete. L'acquisizione consente al supporto Umbrella di analizzare il traffico a un basso livello e identificare potenziali problemi.

Nella maggior parte dei casi è utile confrontare due set di acquisizioni di pacchetti per dimostrare

uno scenario funzionante e uno non funzionante.

- Assicurarsi di poter replicare il problema e completare questi passaggi mentre il problema si verifica. Generare un'acquisizione pacchetto che mostri uno scenario non funzionante. Annota la data e l'ora con il fuso orario in modo che queste informazioni possano essere correlate ad altri dati.
- Se possibile, ripetere queste istruzioni con il software Umbrella (e/o l'inoltro DNS Umbrella) disattivato. Generare un'acquisizione pacchetto che mostri lo scenario di lavoro. Annota la data e l'ora con il fuso orario in modo che queste informazioni possano essere correlate ad altri dati.

Istruzioni per Wireshark

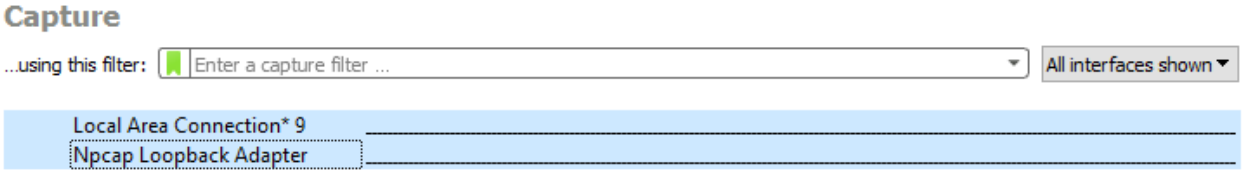
Preparazioni

1. Scarica Wireshark.
2. Disconnettere tutte le connessioni di rete non necessarie.
    1. Disconnettere le connessioni VPN, a meno che non siano necessarie per replicare il problema.
    2. Utilizzare solo connessioni cablate o wireless e non entrambe insieme.
3. Chiudere tutte le applicazioni non necessarie per la replica del problema.
4. Cancella i cookie e la cache dal browser.
5. Scaricare la cache DNS. In Windows con il comando:

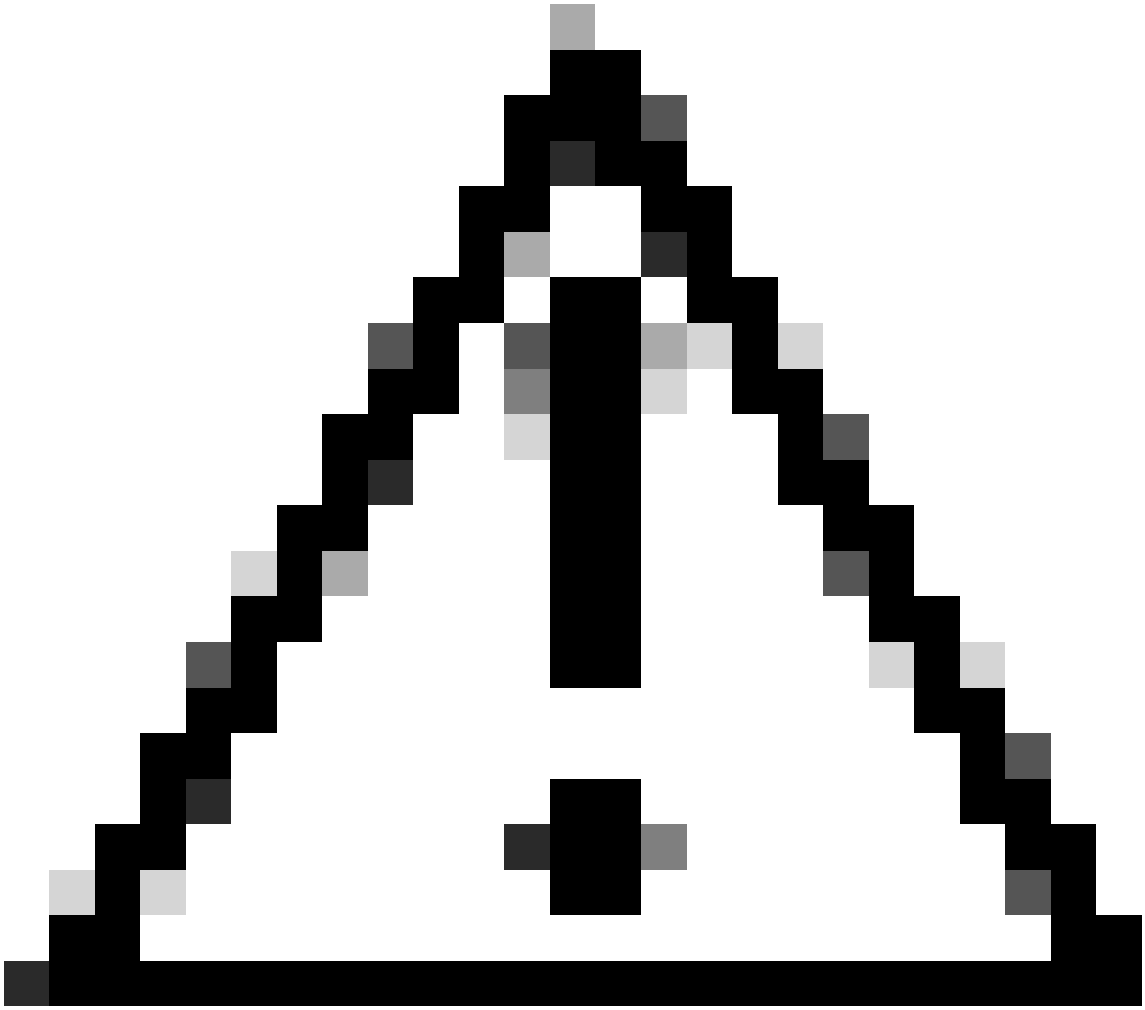
```
ipconfig /flushdns
```

Acquisizione di base di Wireshark

1. Lanciare Wireshark.
2. Il pannello Acquisizione mostra le interfacce di rete. Selezionare le interfacce rilevanti. È possibile selezionare più interfacce utilizzando il tasto CTRL (Windows) o CMD (Mac) durante la selezione.

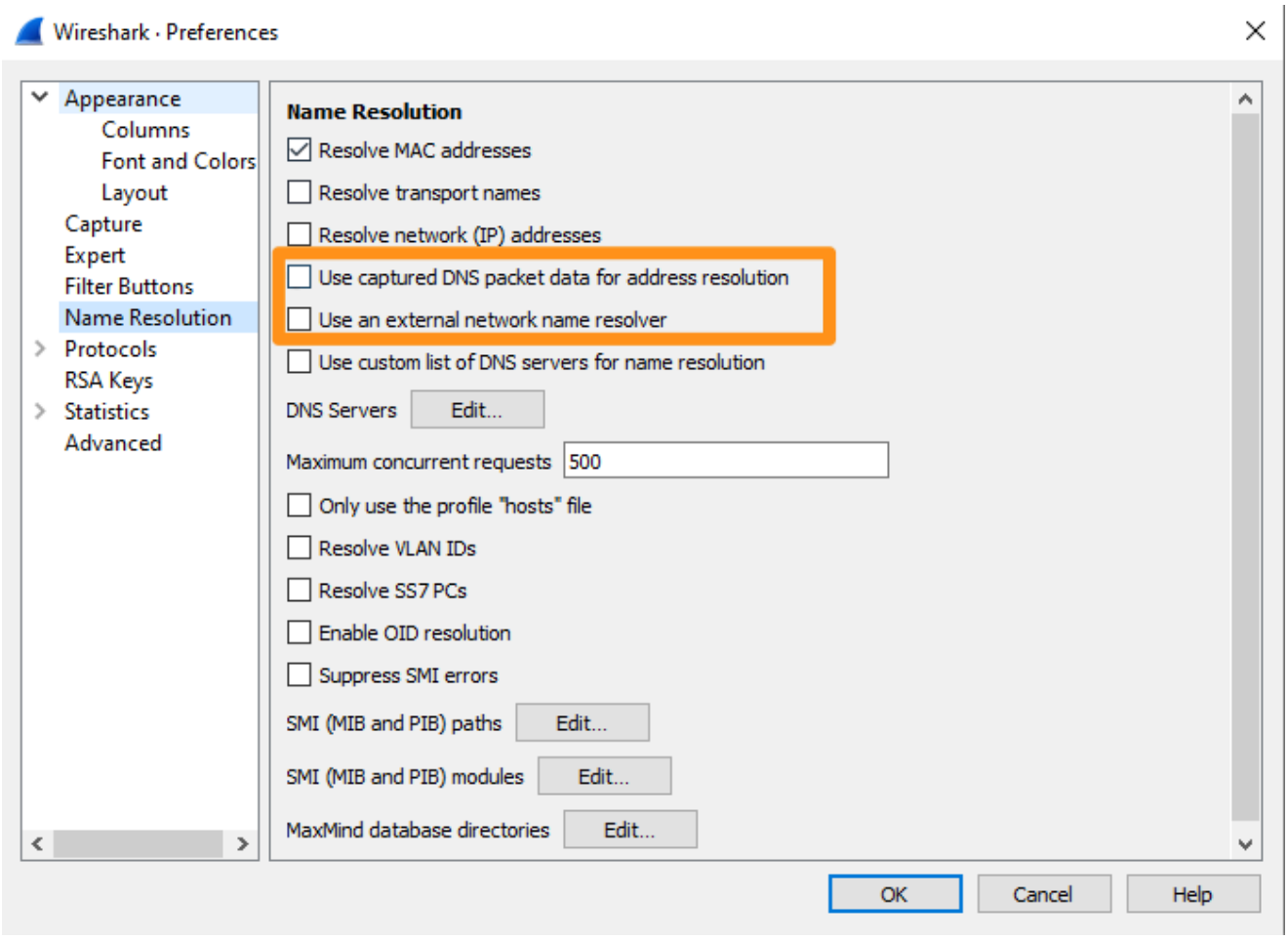


wireshark_1.png



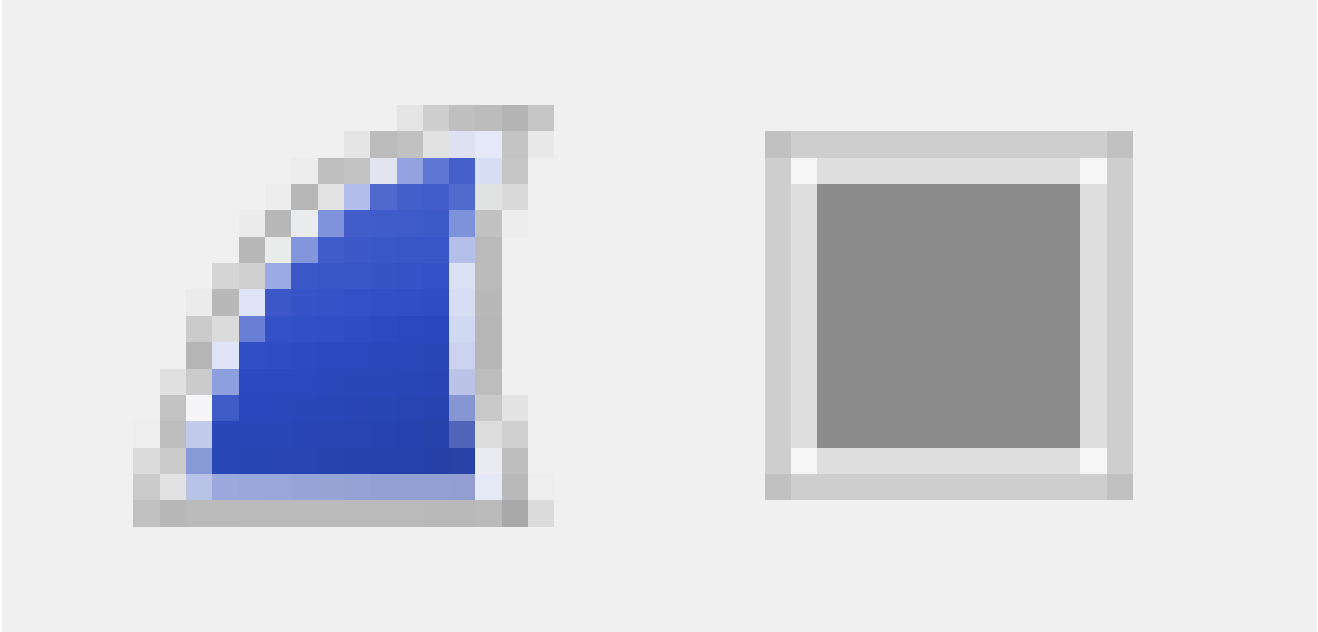
Attenzione: È importante selezionare le interfacce corrette che contengono il traffico di rete. Usare il comando "ipconfig" (Windows) o il comando "ifconfig" (Mac) per visualizzare ulteriori dettagli sulle interfacce di rete. Gli utenti client mobili devono inoltre selezionare la scheda di loopback NPCAP O il loopback: interfacce lo0 In caso di dubbio, selezionare tutte le interfacce.

3. Accertarsi che le opzioni Usa dati pacchetto DNS acquisiti per la risoluzione degli indirizzi e Usa resolver dei nomi di rete esterni siano selezionate NON per assicurarsi che Wireshark non esegua query DNS in quanto ciò può complicare l'acquisizione e influire su AnyConnect. Le impostazioni sono valide a partire dalla versione Wireshark 3.4.9:



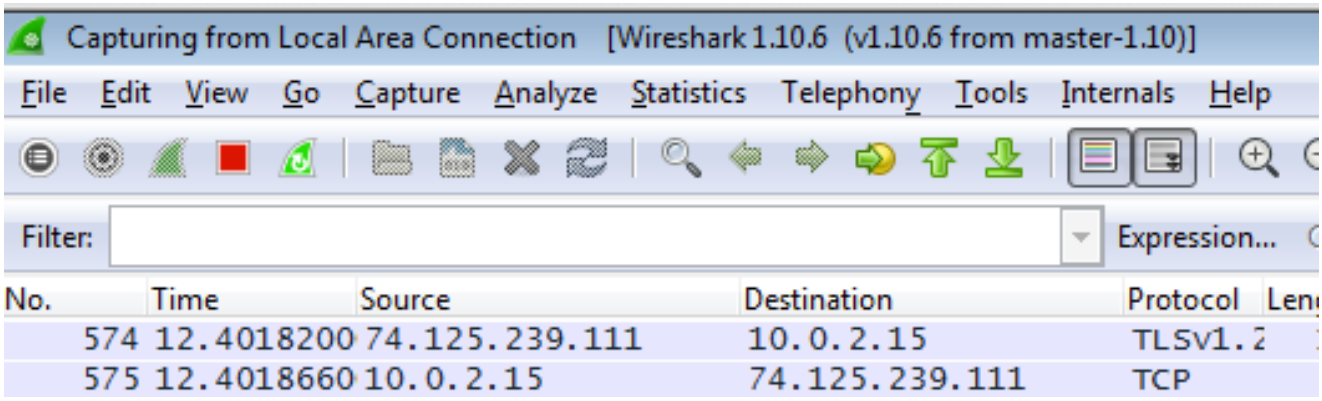
Capture_PNG.png

4. Selezionare Cattura > Avvia o l'icona di avvio blu.



wireshark_2.png

5. Quando Wireshark è in esecuzione in background, replicare il problema.



wireshark_3.png

6. Una volta replicato completamente il problema, selezionare Cattura > Arresta o utilizzare l'icona rossa Arresta.
7. Passare a File > Salva con nome e selezionare una posizione in cui salvare il file. Assicurarsi che il file sia stato salvato come tipo PCAPNG. Il file salvato può essere inviato al supporto Cisco Umbrella per la revisione.

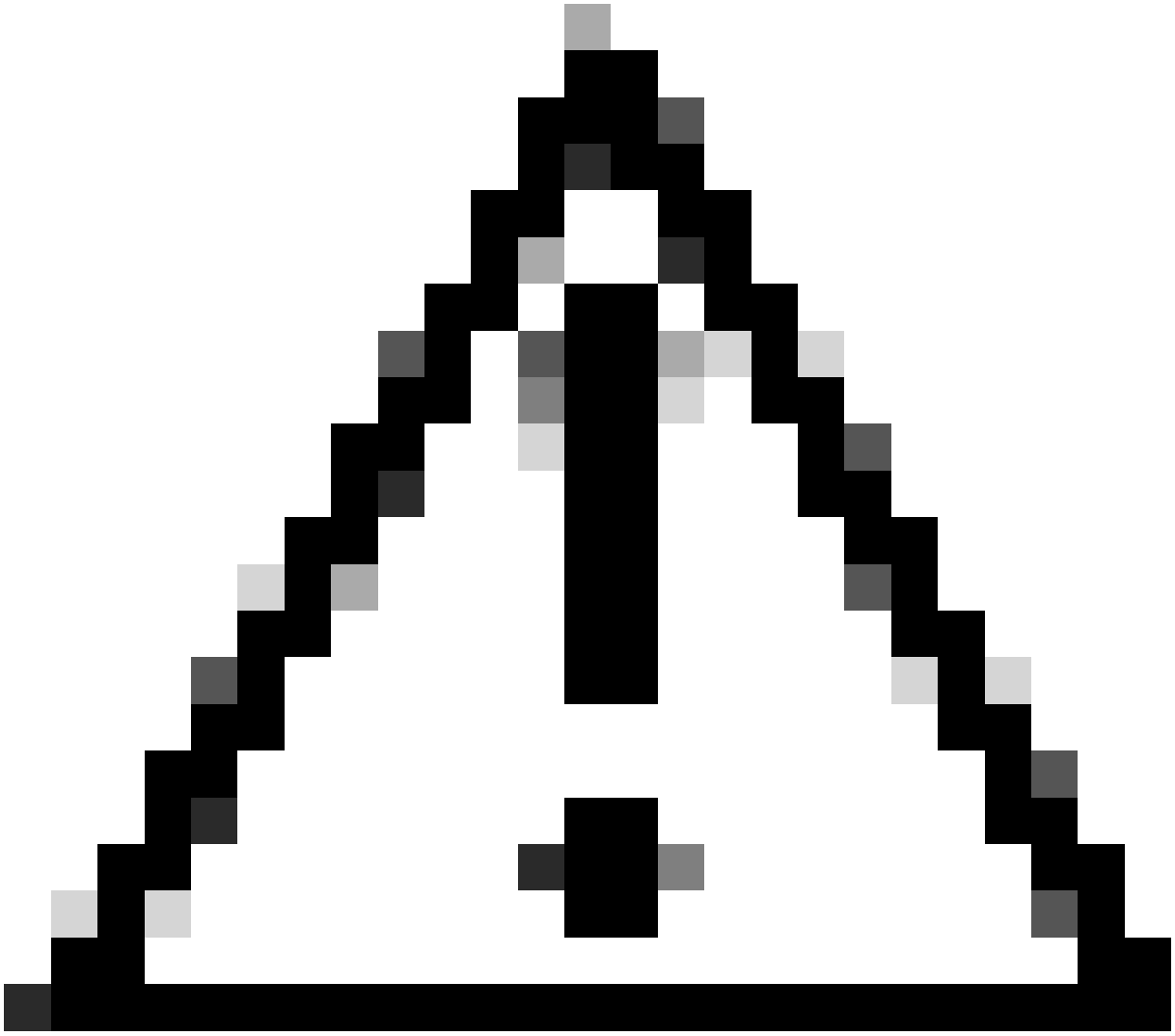
Client roaming - Ulteriori passaggi

Per gli utenti di AnyConnect Roaming Client e AnyConnect Roaming Module in modalità standalone, è necessario completare alcuni passaggi aggiuntivi:

Traffico di loopback

Quando si seleziona un'interfaccia, è necessario acquisire anche il traffico sull'interfaccia di loopback (127.0.0.1) oltre ad altre interfacce di rete. Il proxy DNS del client di roaming è in ascolto su questa interfaccia, quindi è fondamentale che il traffico tra il sistema operativo e il client di roaming sia visibile.

- Windows: Seleziona scheda di loopback NPCAP
- Mac: Selezionare loopback: lo0



Attenzione: Le versioni più recenti di Windows di Wireshark vengono fornite con il driver di acquisizione NPCAP, che supporta il driver di loopback. Se l'adattatore loopback non è presente, eseguire l'aggiornamento alla versione più recente di Wireshark o utilizzare le istruzioni di rawcap.exe.

Traffico DNS crittografato

In circostanze normali, il traffico tra il cliente in roaming e Umbrella è crittografato e non leggibile dall'uomo. In alcuni casi, il supporto Umbrella può richiedere la disabilitazione della crittografia DNS per visualizzare il traffico DNS tra il client di roaming e il cloud Umbrella. A tale scopo, è possibile procedere in due modi:

- Creare un blocco firewall locale per UDP da 443 a 208.67.220.220 e 208.67.222.222.
- In alternativa, creare il file in base al sistema operativo e alla versione del client di roaming:
    - Windows:

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

- Windows AnyConnect:

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

- Client protetto Windows:

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

- macOS:

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

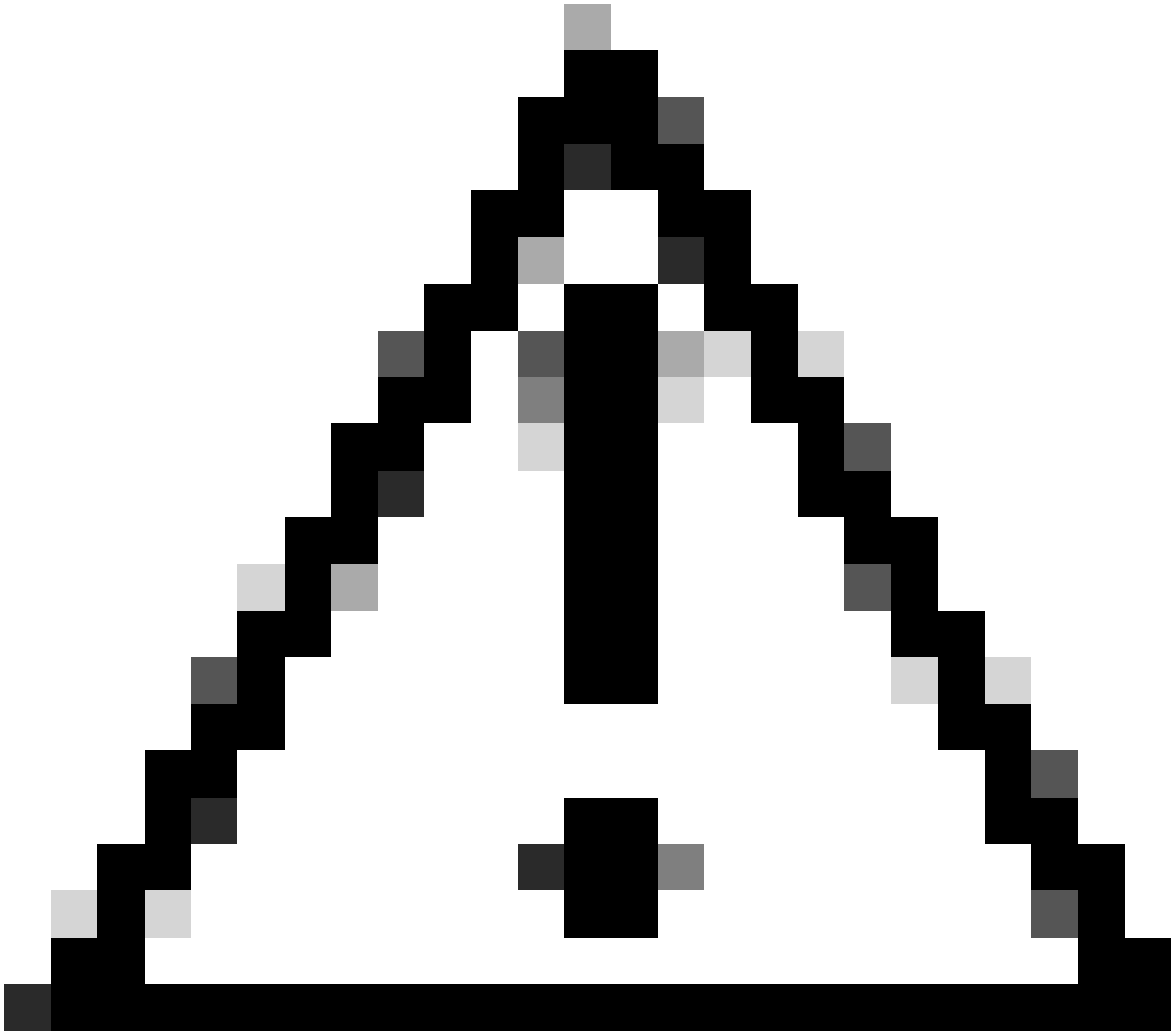
- mac OS AnyConnect:

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

- Client protetto mac OS:

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

Al termine, riavviare il servizio o il computer.



Attenzione: Le versioni più recenti di Wireshark su Windows includono il driver di acquisizione NPCAP, che non supporta l'interfaccia Umbrella VPN. In Windows, potrebbe essere necessario utilizzare lo strumento rawcap.exe come alternativa.

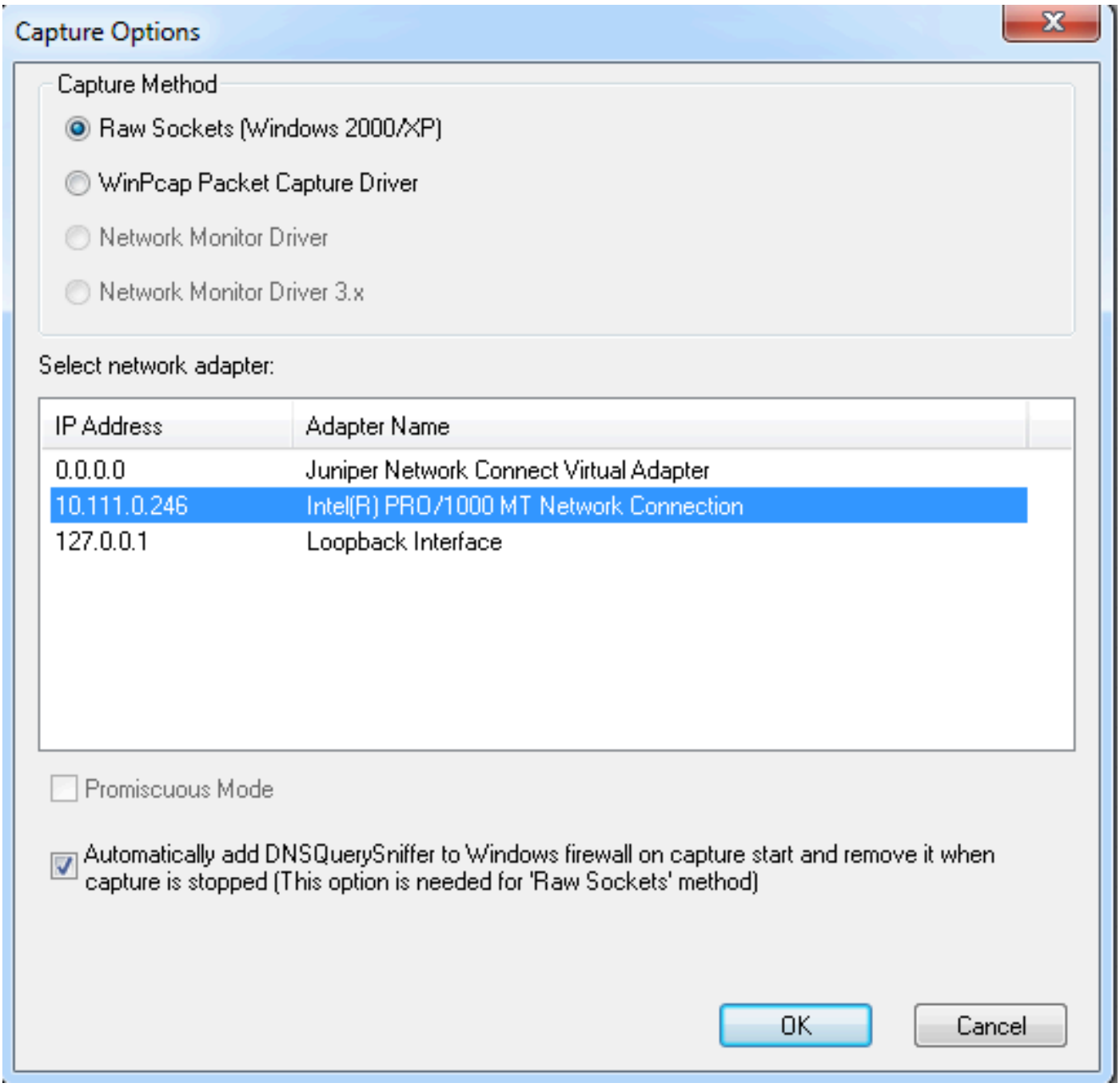
DNSQuerySniffer - Alternativa a Windows

DNSQuery Sniffer è uno sniffer di rete solo DNS per Windows che monitora e visualizza tonnellate di dati utili. A differenza di Wireshark o Rawcap, è utilizzato solo per il DNS ed è molto più facile esaminare ed estrarre informazioni rilevanti. Tuttavia, non ha i potenti strumenti di filtraggio di Wireshark.

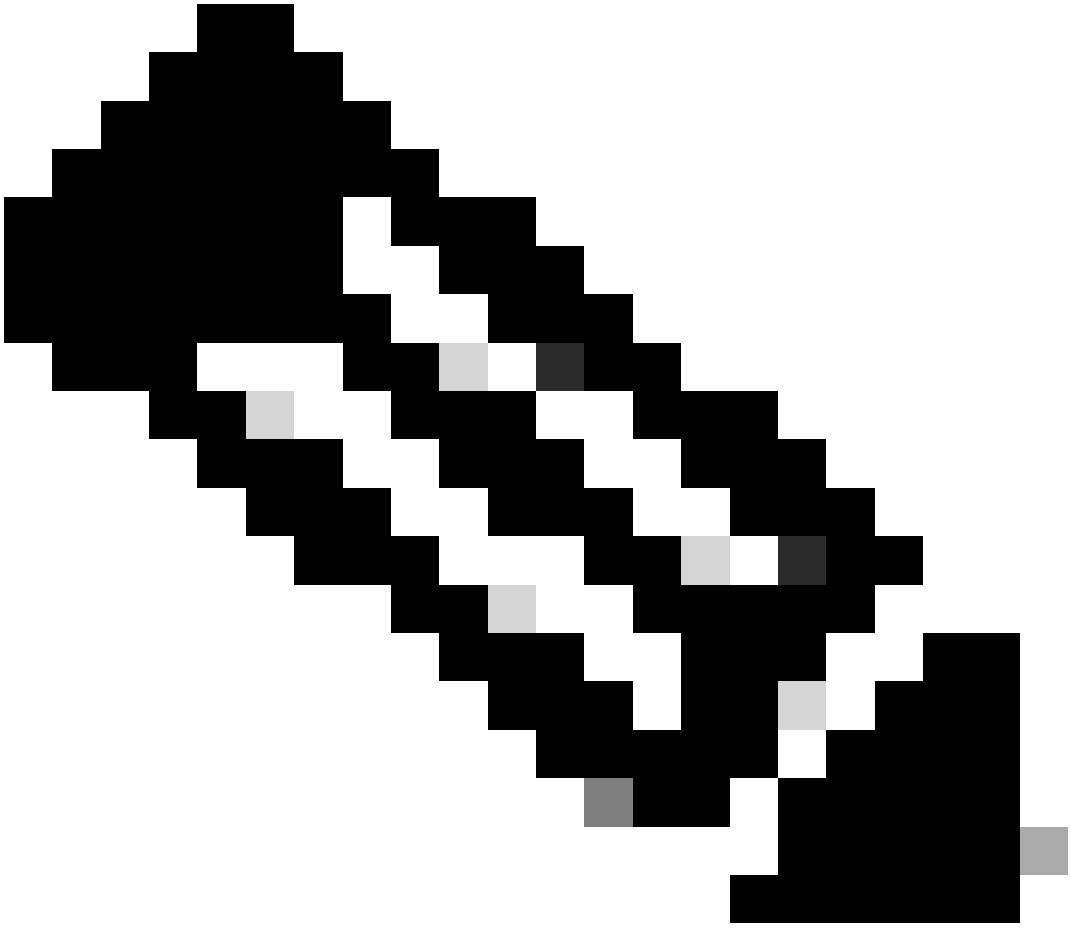
Si tratta di uno strumento leggero e facile da utilizzare. Il vantaggio di questa funzionalità consiste nella possibilità di individuare i pacchetti quando il servizio client roaming è disabilitato, avviare l'acquisizione e visualizzare tutte le query DNS inviate dal client roaming dal momento in cui viene avviato, anziché avviare un'acquisizione dopo che il client roaming è già stato avviato.

Esistono due metodi di acquisizione:

1. Se si seleziona l'interfaccia di rete normale, è possibile visualizzare solo le query presenti nell'elenco Domini interni o che non sono state specificamente passate attraverso dnscryptproxy.



dns_1.png

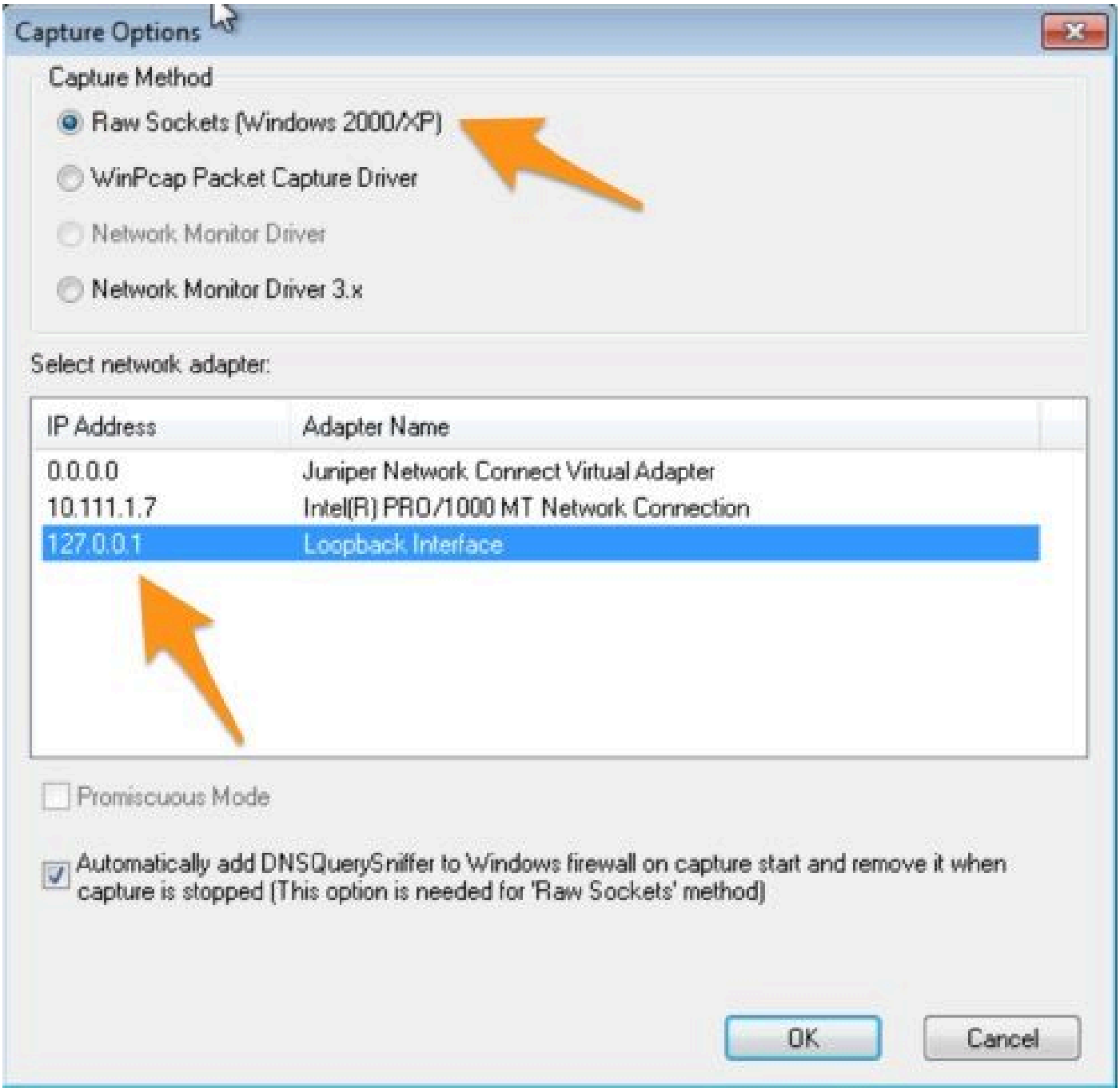


Nota: Queste colonne appaiono nella parte destra della cattura e dovete scorrere su un po 'per vederle.

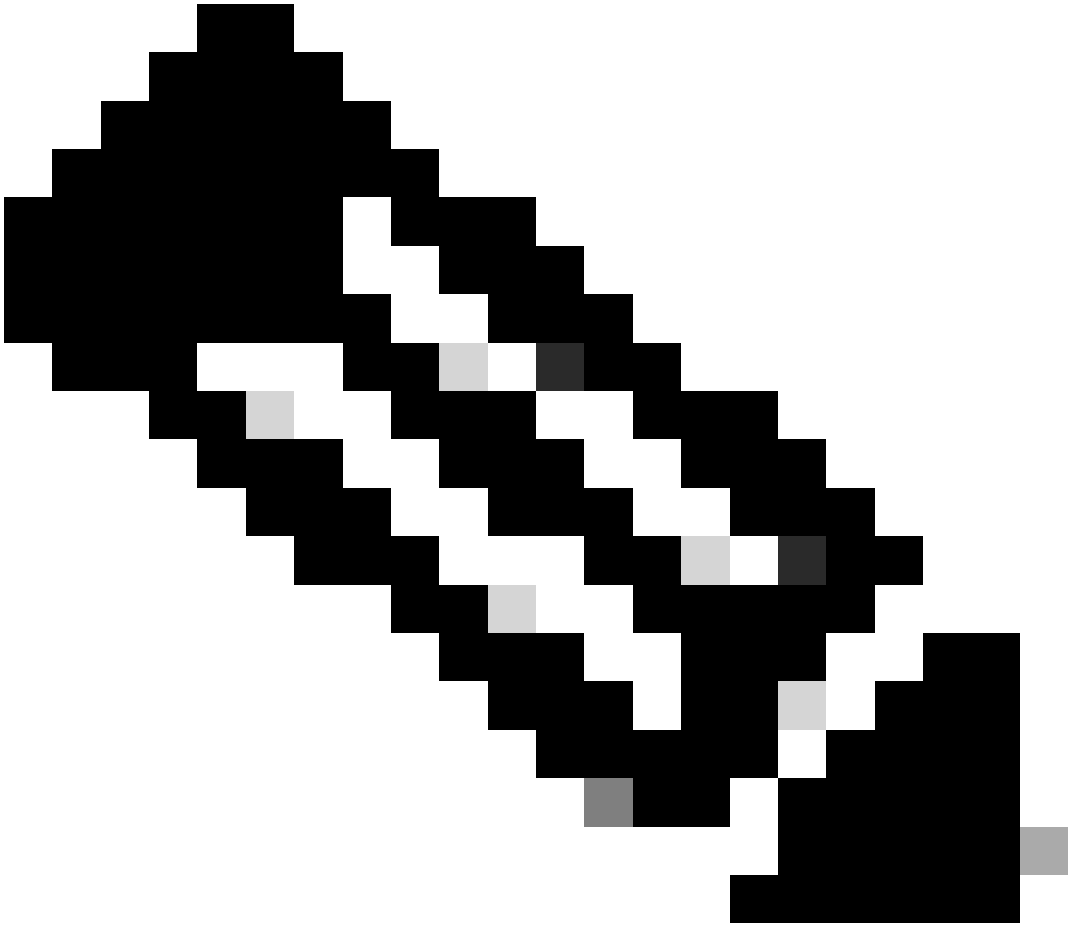
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

Colonne DNSSniffer

2. Se si seleziona l'interfaccia Loopback, verranno visualizzate tutte le query DNS inviate tramite dnscryptproxy, ma non sarà possibile visualizzare l'indirizzo IP di destinazione reale per i domini inclusi nell'elenco Domini interni. La query e la risposta vengono comunque visualizzate.


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

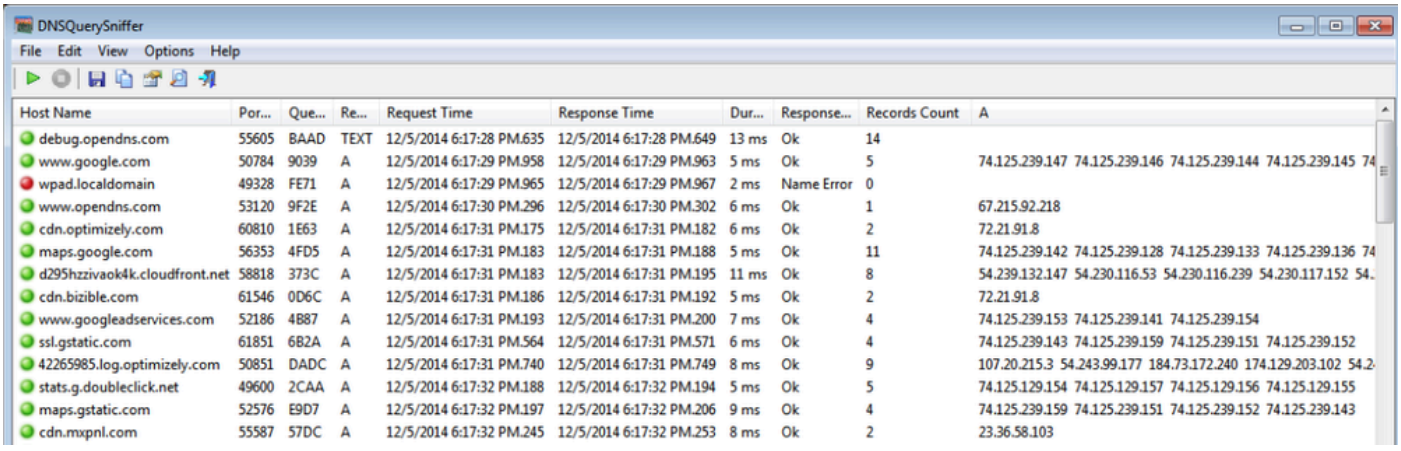


Nota: Queste colonne appaiono nella parte destra della cattura e bisogna scorrere su un po' per vederle.

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

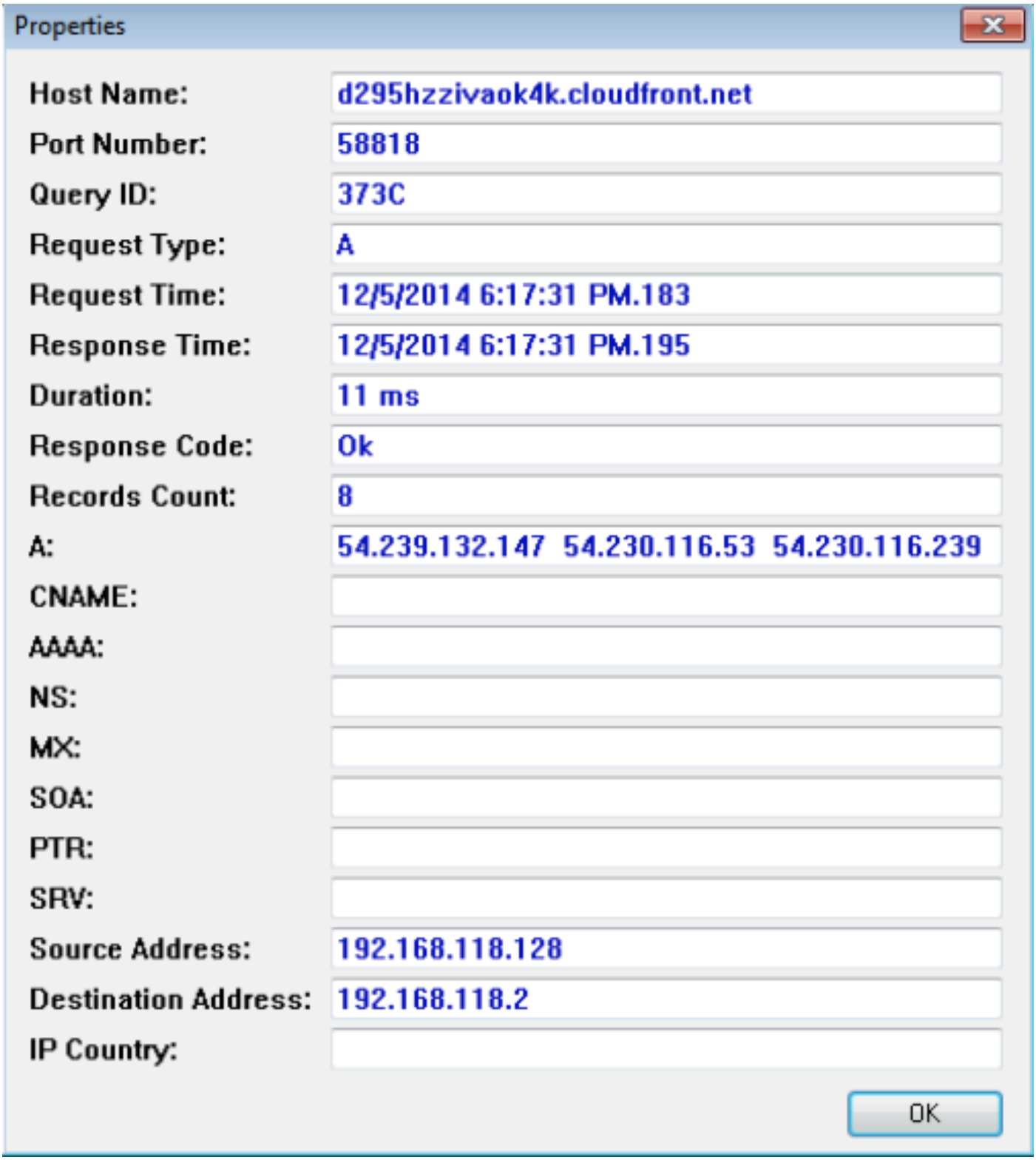
Colonne DNSSniffer

I risultati saranno simili a quelli riportati di seguito:



dns_3.png

Visualizzazione di una singola ricerca:



dns_4.png

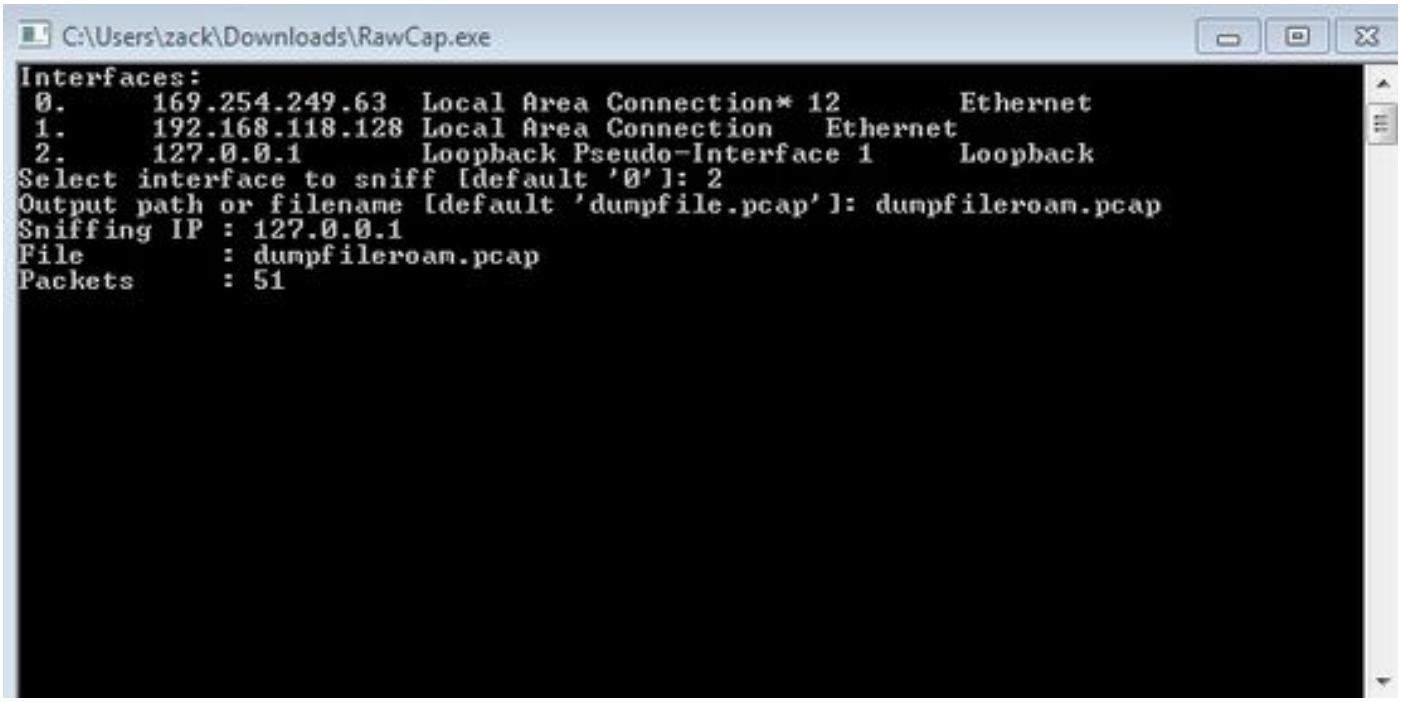
RawCap.exe - Alternativa a Windows

In alcune circostanze, l'interfaccia con cui è necessario lavorare non è supportata dal driver di acquisizione pacchetti incluso con Wireshark. Questo può rappresentare un problema per l'interfaccia di loopback.

In questi casi, è possibile utilizzare RawCap.exe:

1. Completare la procedura descritta in precedenza per utilizzare Wireshark per catturare il normale traffico.
2. Eseguire contemporaneamente RawCap.exe.
3. Selezionare l'interfaccia specificando il numero di elenco corrispondente.
4. Specificate un nome file di output e disattivatelo.
5. Selezionare Control-Cquando si desidera arrestare l'acquisizione.

Il file salvato viene inserito nella cartella da cui è stato eseguito RawCap.exe:



rawcap_1.jpg

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).