Erfassen von Netzwerkverkehr mit Wireshark

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Überblick

Anweisungen zu Wireshark

- Vorbereitungen
- Grundlegende Wireshark-Erfassung

Roaming-Client - Weitere Schritte

- Loopback-Datenverkehr
- Verschlüsselter DNS-Datenverkehr

DNSQuerySniffer - Windows-Alternative

RawCap.exe - Windows-Alternative

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Netzwerkverkehr mit Wireshark erfassen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Umbrella DNS Layer Security.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

In manchen Fällen bitten Cisco Umbrella Support-Mitarbeiter um eine Paketerfassung des Internetdatenverkehrs, der zwischen Ihrem Computer und dem Netzwerk übertragen wird. Die Erfassung ermöglicht Umbrella Support, den Datenverkehr auf niedriger Ebene zu analysieren und potenzielle Probleme zu identifizieren.

In den meisten Fällen ist es hilfreich, zwei Paketerfassungssätze zu vergleichen, um ein funktionierendes und ein nicht funktionierendes Szenario zu veranschaulichen.

- Stellen Sie sicher, dass Sie das Problem replizieren und diese Schritte ausführen können, während das Problem auftritt. Generieren Sie eine Paketerfassung, die ein nicht funktionierendes Szenario anzeigt. Bitte beachten Sie Datum und Uhrzeit mit Zeitzone, damit diese Informationen mit anderen Daten korreliert werden können.
- Wiederholen Sie nach Möglichkeit diese Anweisungen, und deaktivieren Sie Umbrella-Software (und/oder Umbrella DNS Forwarding). Generieren Sie eine Paketerfassung, die das Arbeitsszenario zeigt. Bitte beachten Sie Datum und Uhrzeit mit Zeitzone, damit diese Informationen mit anderen Daten korreliert werden können.

Anweisungen zu Wireshark

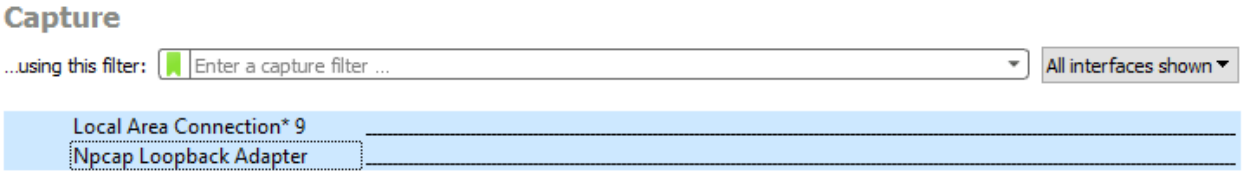
Vorbereitungen

1. Wireshark herunterladen
2. Trennen Sie alle nicht benötigten Netzwerkverbindungen.
    1. Trennen Sie die VPN-Verbindungen, es sei denn, sie werden zur Replikation des Problems benötigt.
    2. Verwenden Sie nur kabelgebundene oder drahtlose Verbindungen und nicht beides zusammen.
3. Schließen Sie alle anderen Softwareprogramme, die für die Replikation des Problems nicht erforderlich sind.
4. Löschen Sie die Cookies und den Cache aus Ihrem Browser.
5. Leeren Sie den DNS-Cache. Unter Windows mit dem Befehl:

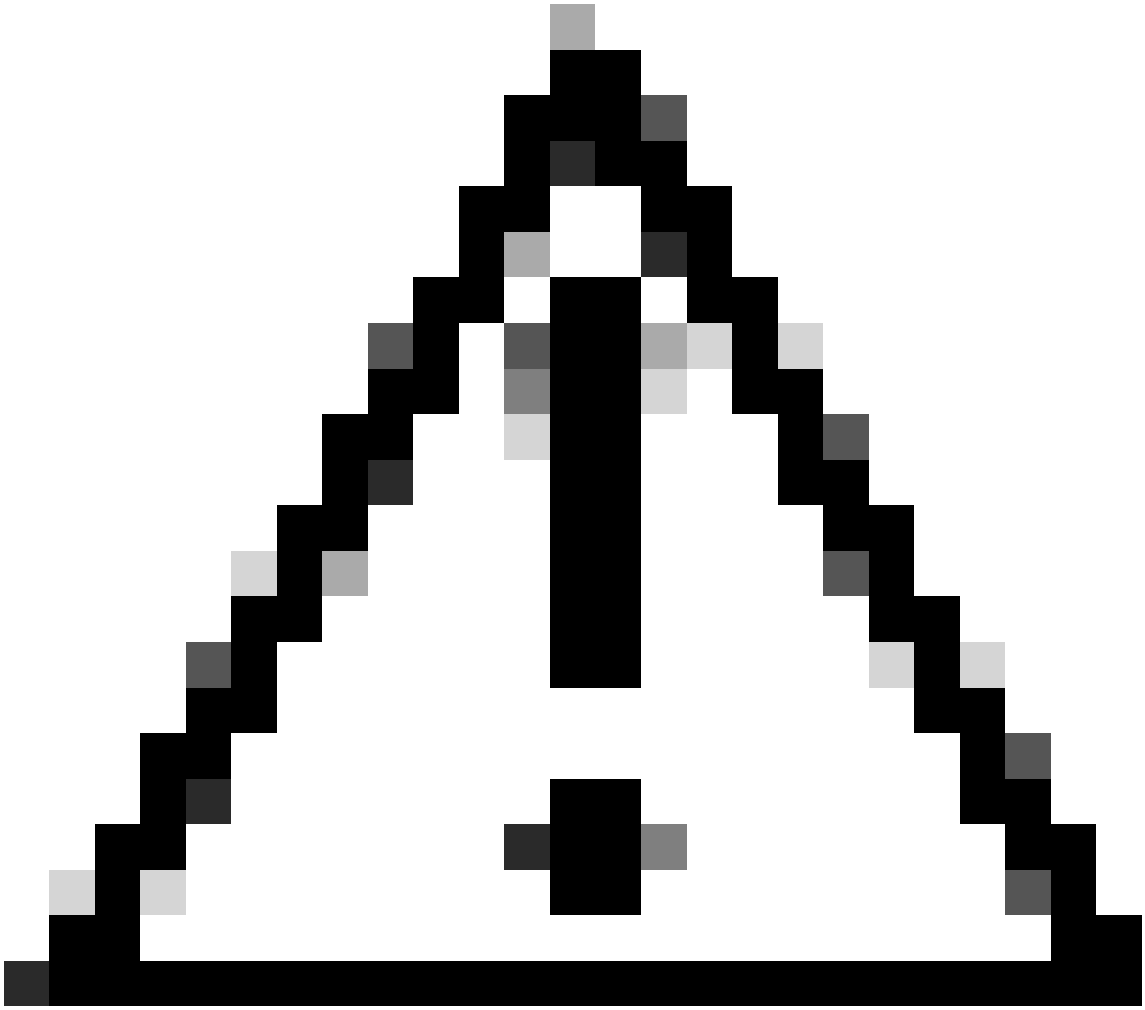
```
ipconfig /flushdns
```

Grundlegende Wireshark-Erfassung

1. Starten Sie Wireshark.
2. Im Bereich Capture (Erfassung) werden Ihre Netzwerkschnittstellen angezeigt. Wählen Sie die entsprechenden Schnittstellen aus. Bei der Auswahl können mehrere Schnittstellen über die STRG-Taste (Windows) oder die CMD-Taste (Mac) ausgewählt werden.

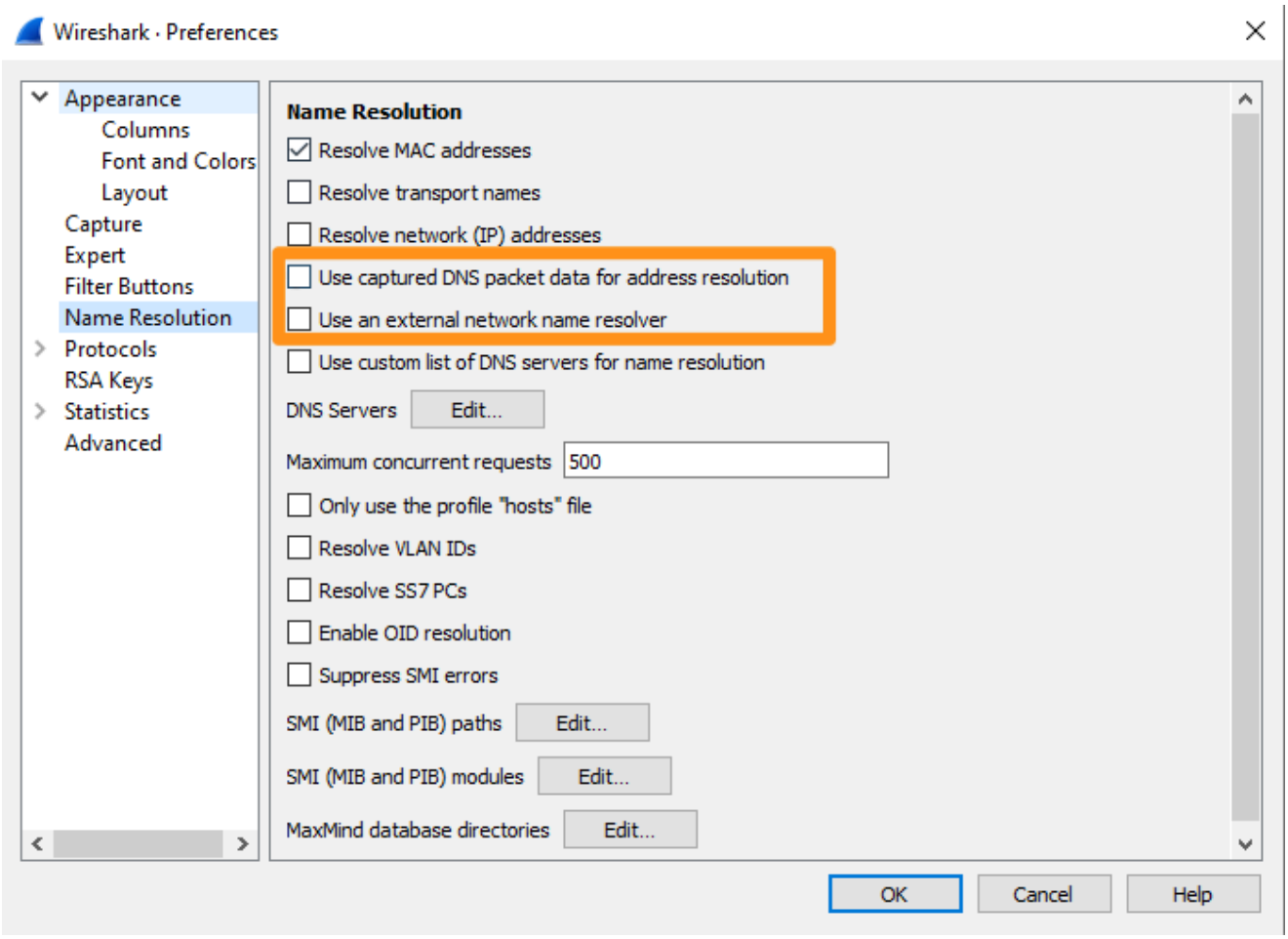


wireshark_1.png



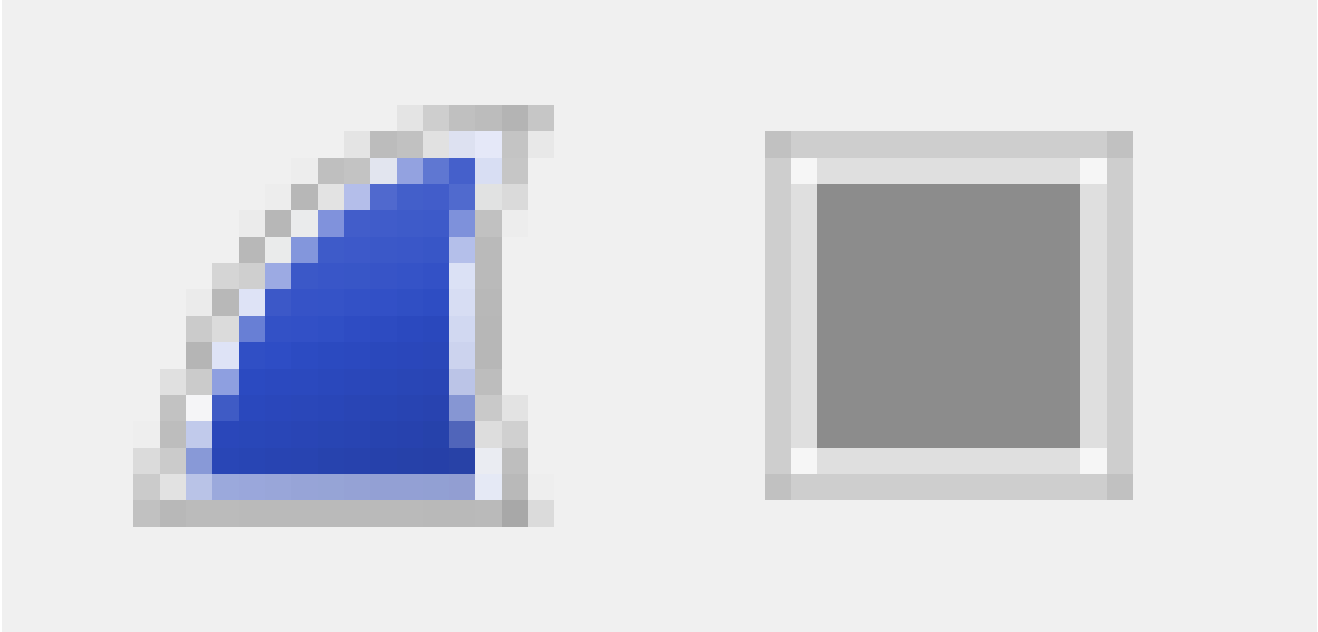
Vorsicht: Es ist wichtig, die richtigen Schnittstellen auszuwählen, die den Netzwerkverkehr enthalten. Verwenden Sie den Befehl "ipconfig" (Windows) oder den Befehl "ifconfig" (Mac), um weitere Details zu Ihren Netzwerkschnittstellen anzuzeigen. Roaming-Client-Benutzer müssen zusätzlich den NPCAP-Loopback-Adapter ODER Loopback auswählen: lo0-Schnittstellen. Im Zweifelsfall alle Schnittstellen auswählen.

3. Stellen Sie sicher, dass Erfasste DNS-Paketdaten für die Adressauflösung verwenden und Externen Netzwerknamensauflöser verwenden NICHT ausgewählt sind, um sicherzustellen, dass Wireshark keine DNS-Abfragen durchführt, da dies die Erfassung komplizieren und AnyConnect beeinträchtigen kann. Die Einstellungen gelten ab Wireshark 3.4.9:



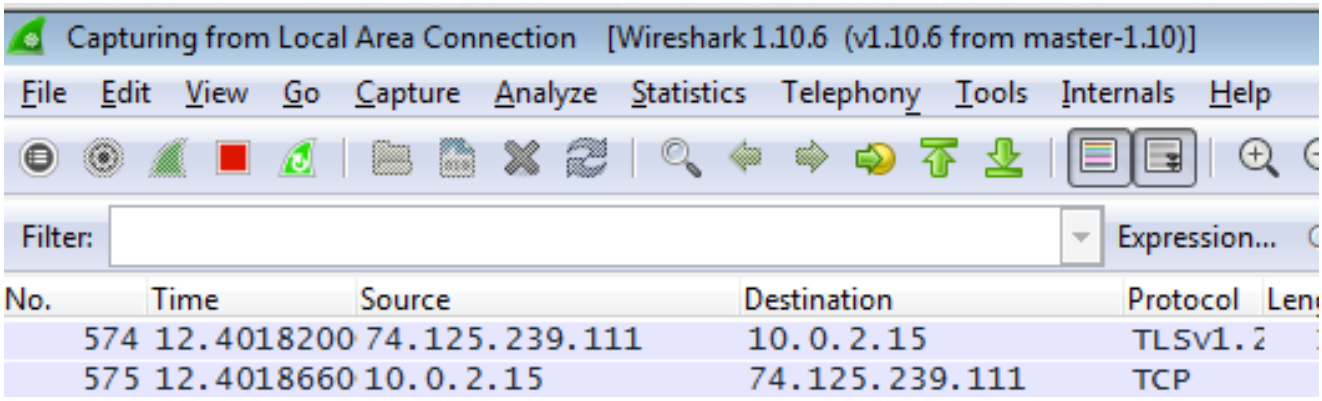
Capture_PNG.png

4. Wählen Sie Capture > Start oder das blaue Startsymbol aus.



wireshark_2.png

5. Während Wireshark im Hintergrund läuft, replizieren Sie das Problem.



wireshark_3.png

6. Wenn das Problem vollständig repliziert wurde, wählen Sie Capture > Stopp aus, oder verwenden Sie das rote Symbol Stopp.
7. Navigieren Sie zu Datei > Speichern unter, und wählen Sie einen Speicherort für die Datei aus. Stellen Sie sicher, dass die Datei als PCAPNG-Typ gespeichert wird. Die gespeicherte Datei kann zur Überprüfung an den Cisco Umbrella Support gesendet werden.

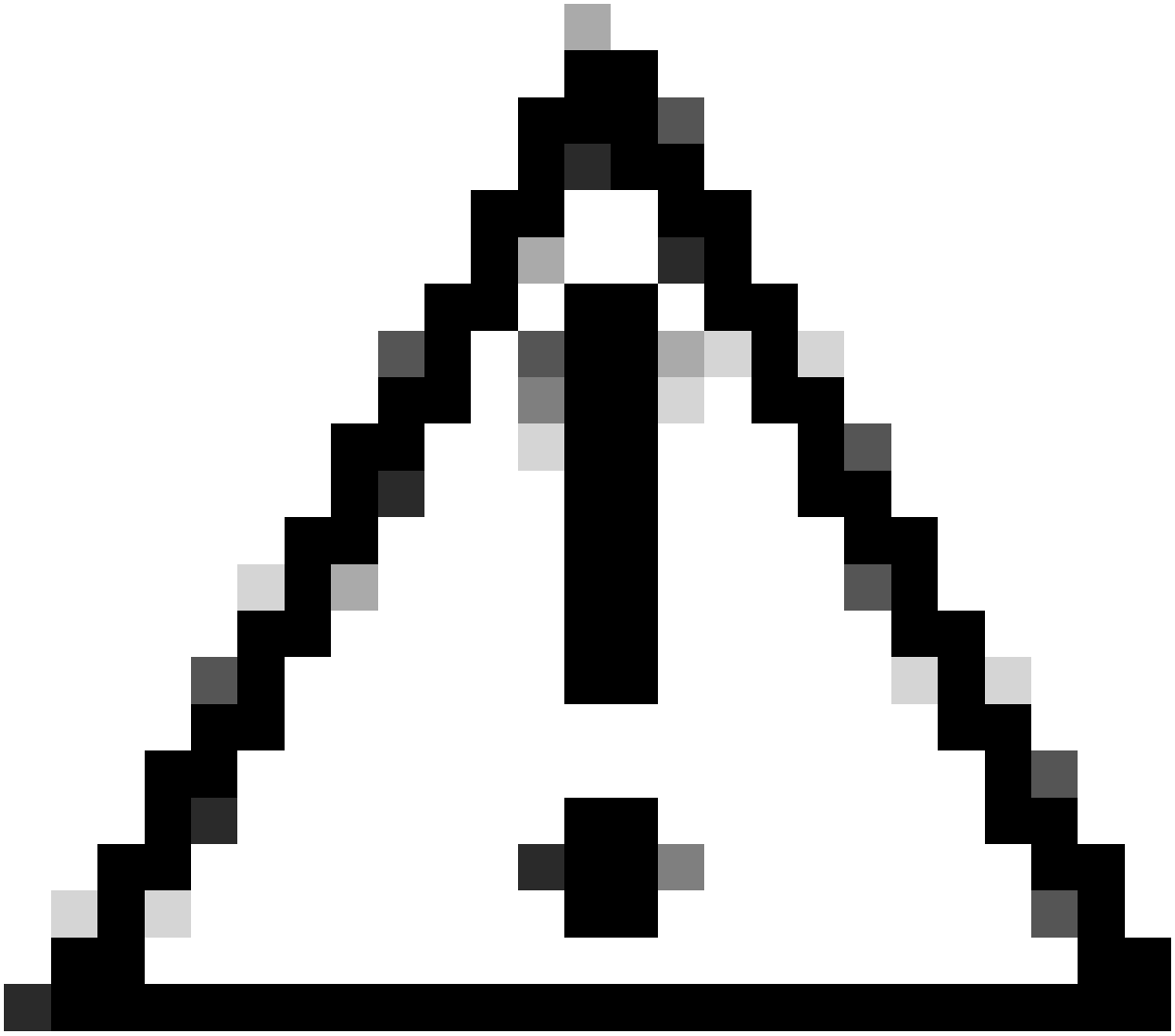
Roaming-Client - Weitere Schritte

Sowohl für Benutzer des Standalone Roaming-Clients als auch für Benutzer des AnyConnect Roaming-Moduls müssen zusätzliche Schritte ausgeführt werden:

Loopback-Datenverkehr

Wenn Sie eine Schnittstelle auswählen, müssen Sie neben anderen Netzwerkschnittstellen auch den Datenverkehr an der Loopback-Schnittstelle (127.0.0.1) erfassen. Der DNS-Proxy des Roaming-Clients hört diese Schnittstelle ab. Daher ist es wichtig, den Datenverkehr zwischen dem Betriebssystem und dem Roaming-Client zu beobachten.

- Windows: NPCAP-Loopback-Adapter auswählen
- Mac: Loopback auswählen: lo0



Vorsicht: Neuere Windows-Versionen von Wireshark werden mit dem NPCAP-Erfassungstreiber ausgeliefert, der den Loopback-Treiber unterstützt. Wenn der Loopback-Adapter fehlt, aktualisieren Sie auf die neueste Version von Wireshark, oder verwenden Sie die Anweisungen in rawcap.exe.

Verschlüsselter DNS-Datenverkehr

Unter normalen Umständen ist der Datenverkehr zwischen dem Roaming-Client und Umbrella verschlüsselt und nicht für Menschen lesbar. In einigen Fällen kann die Umbrella-Unterstützung anfordern, dass Sie die DNS-Verschlüsselung deaktivieren, um den DNS-Verkehr zwischen dem Roaming-Client und der Umbrella-Cloud anzuzeigen. Es gibt zwei Möglichkeiten, dies zu tun:

- Erstellen Sie einen lokalen Firewall-Block für UDP 443 bis 208.67.220.220 und 208.67.222.222.
- Oder erstellen Sie die Datei abhängig von Ihrem Betriebssystem und der Version des Roaming-Clients:
    - Windows:

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

- Windows AnyConnect:

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

- Sicherer Windows-Client:

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

- MacOS:

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

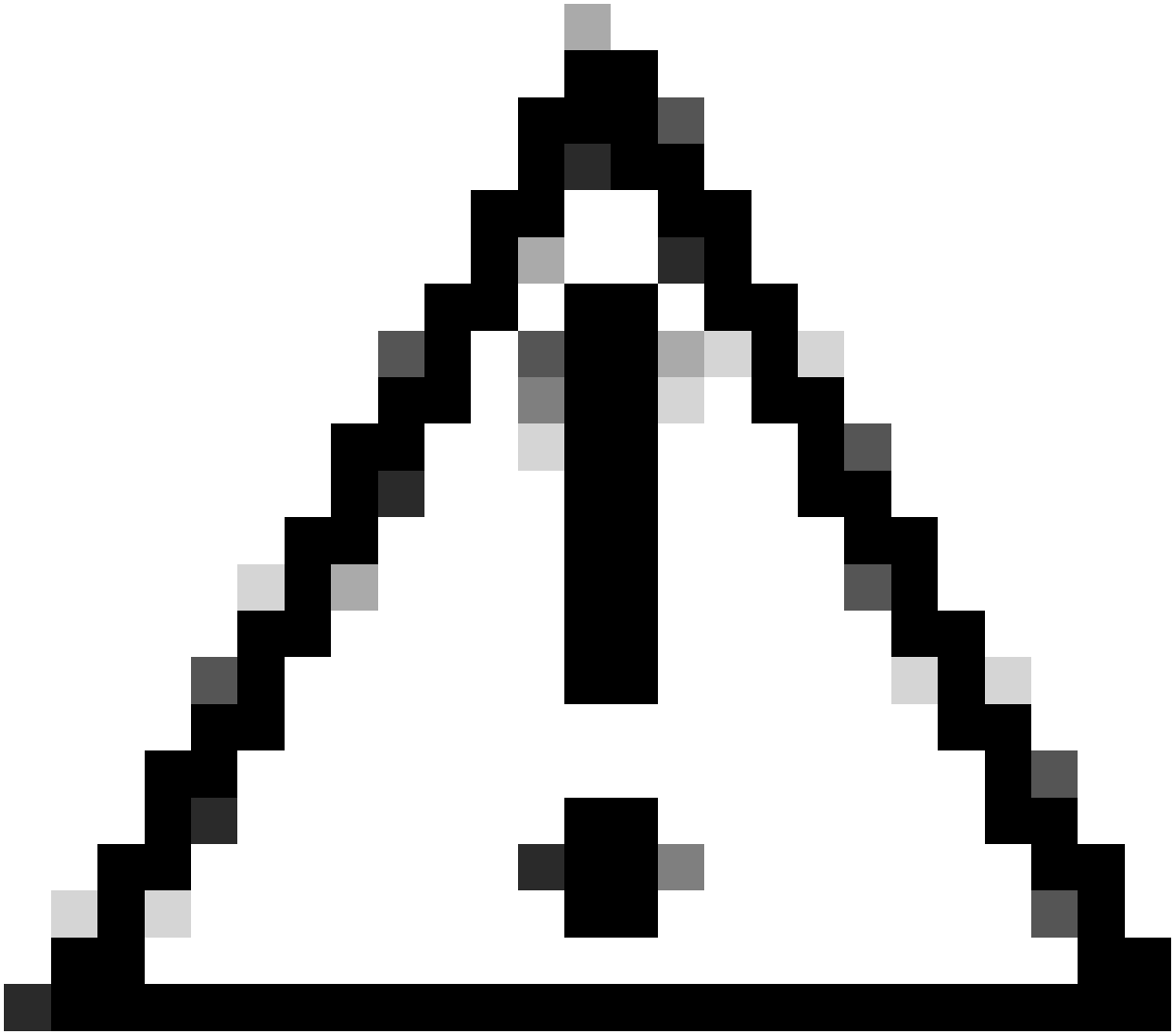
- Mac OS AnyConnect:

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

- Mac OS Secure Client:

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

Starten Sie anschließend den Dienst oder den Computer neu.



Vorsicht: Neuere Versionen von Wireshark unter Windows enthalten den NPCAP-Erfassungstreiber, der die Umbrella VPN-Schnittstelle nicht unterstützt. Unter Windows müssen Sie möglicherweise das Tool rawcap.exe als Alternative verwenden.

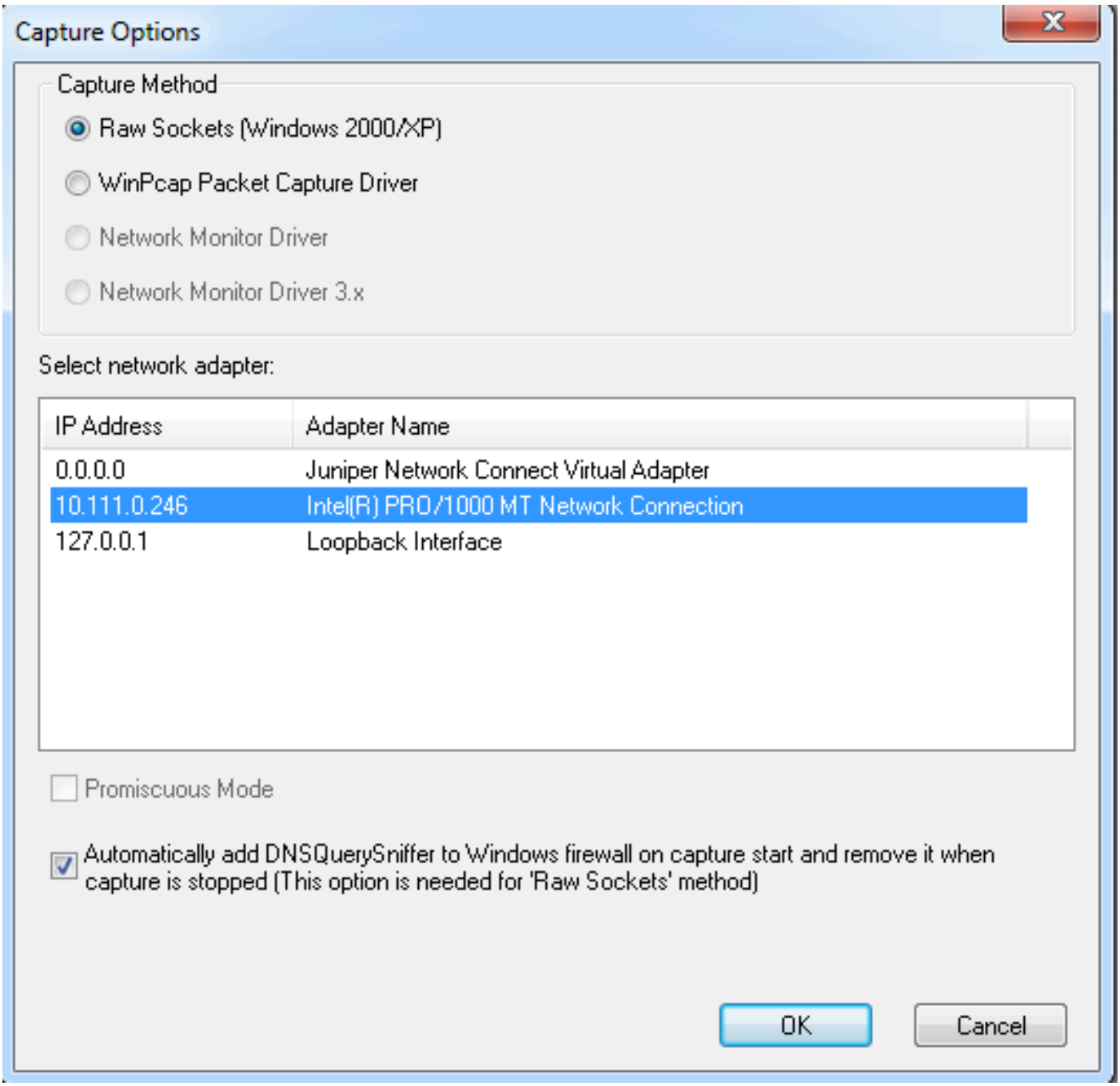
DNSQuerySniffer - Windows-Alternative

DNSQuery Sniffer ist ein reiner DNS-Netzwerk-Sniffer für Windows, der Unmengen nützlicher Daten überwacht und anzeigt. Im Gegensatz zu Wireshark oder Rawcap wird es nur für DNS verwendet und ist viel einfacher, relevante Informationen zu untersuchen und zu extrahieren. Es verfügt jedoch nicht über die leistungsstarken Filtertools von Wireshark.

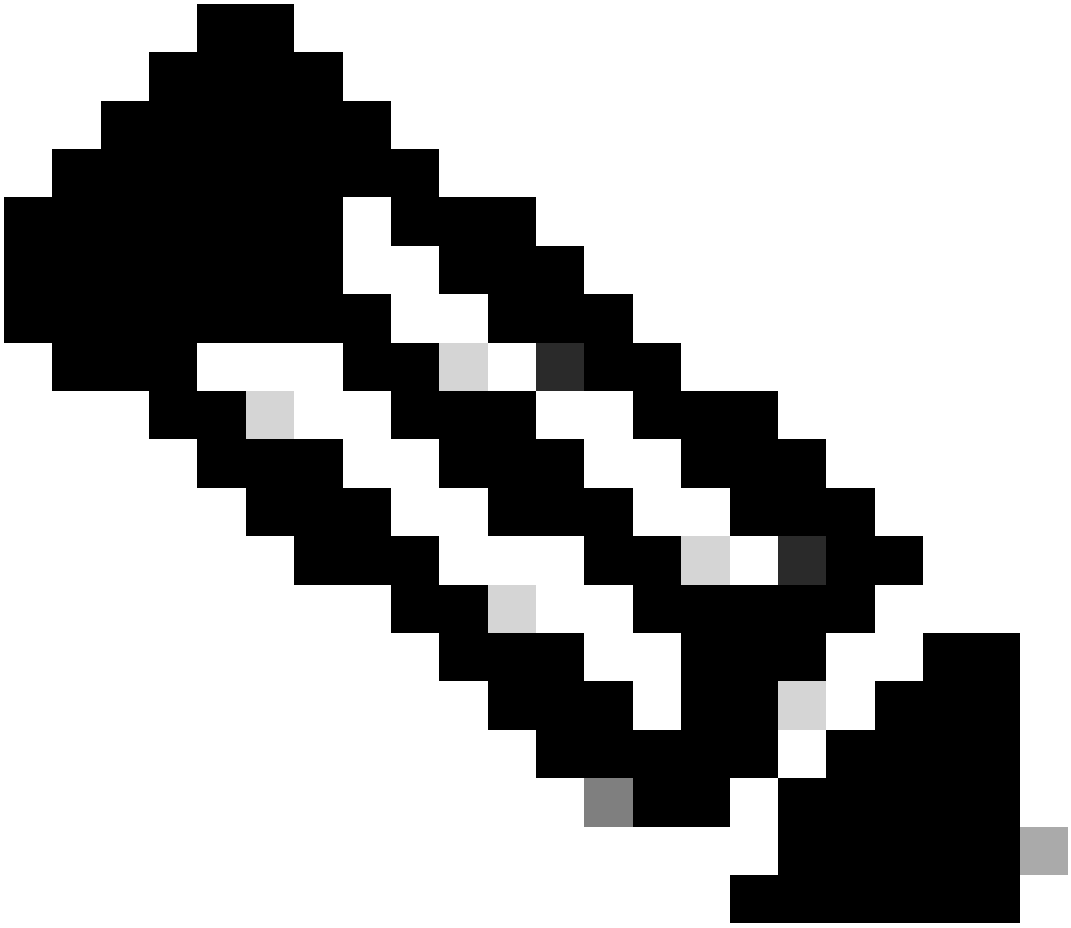
Dies ist ein leichtes und benutzerfreundliches Tool. Ein Vorteil dieser Funktion besteht darin, dass Sie Pakete abhören können, während der Roaming-Client-Dienst deaktiviert ist, die Erfassung starten und jede DNS-Abfrage anzeigen können, die der Roaming-Client von dem Moment an sendet, an dem er startet, anstatt eine Erfassung zu starten, nachdem der Roaming-Client bereits gestartet wurde.

Es gibt zwei Erfassungsmethoden:

1. Wenn Sie die reguläre Netzwerkschnittstelle auswählen, werden nur Abfragen angezeigt, die sich in der Liste Interne Domänen befinden oder nicht explizit den dnscryptproxy durchlaufen haben.



DNS 1.png

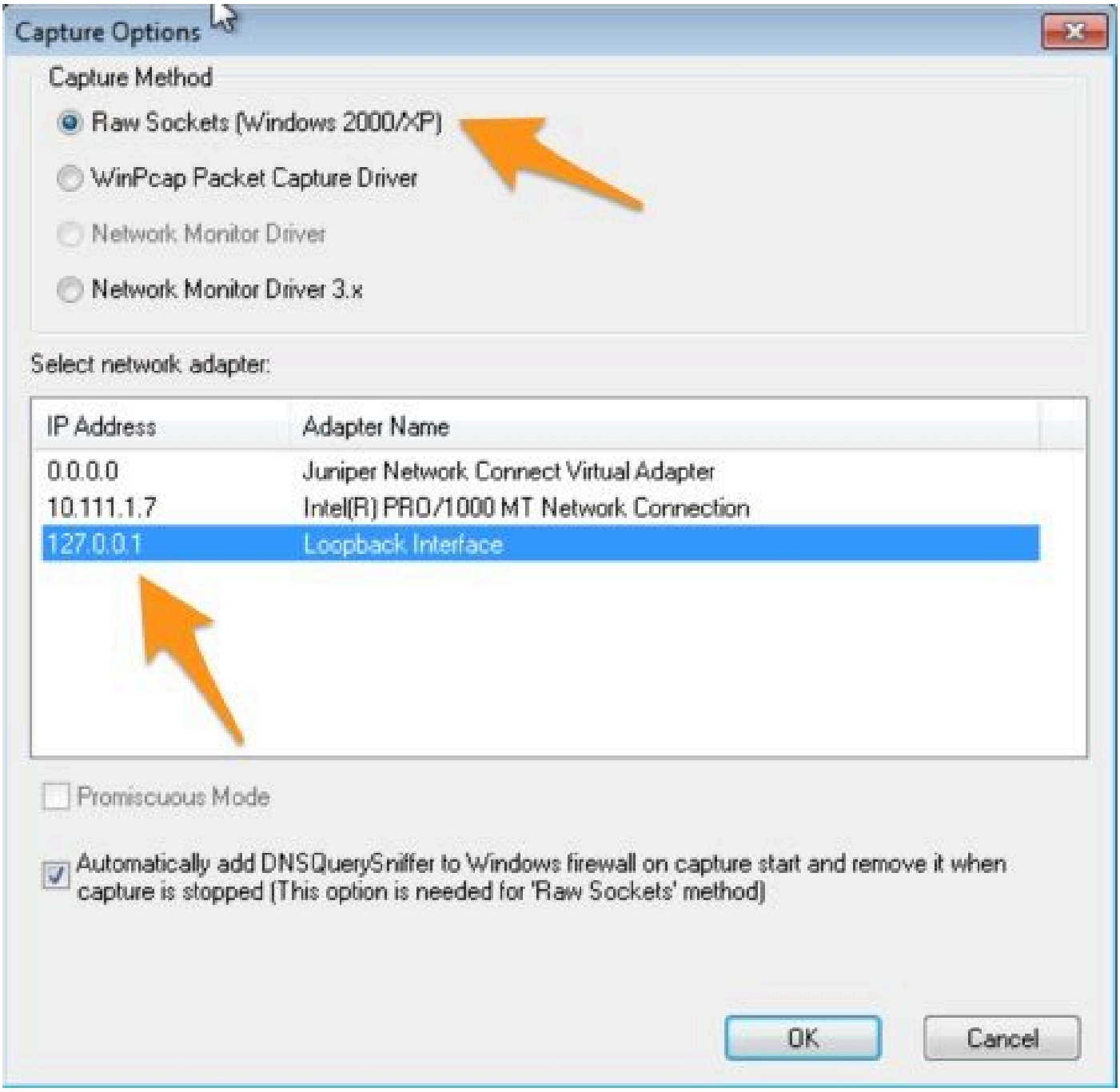


Anmerkung: Diese Spalten erscheinen ganz rechts in der Aufnahme, und Sie müssen einen Bildlauf durchführen, um sie zu sehen.

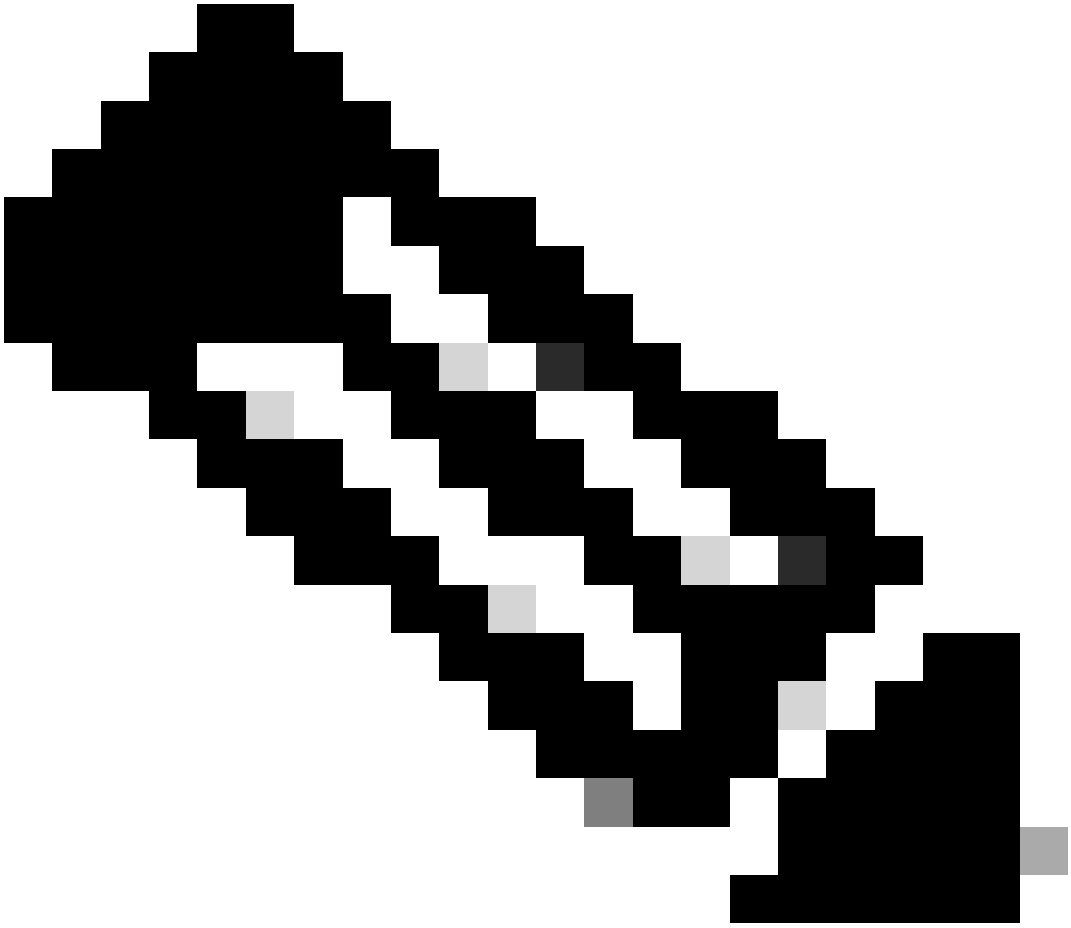
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

DNSSniffer-Spalten

2. Wenn Sie die Loopback-Schnittstelle auswählen, werden alle DNS-Abfragen angezeigt, die über den dnscryptproxy gesendet werden. Die tatsächliche Ziel-IP-Adresse für Domänen wird jedoch in der Liste Interne Domänen nicht angezeigt. Die Abfrage und die Antwort werden jedoch weiterhin angezeigt.


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

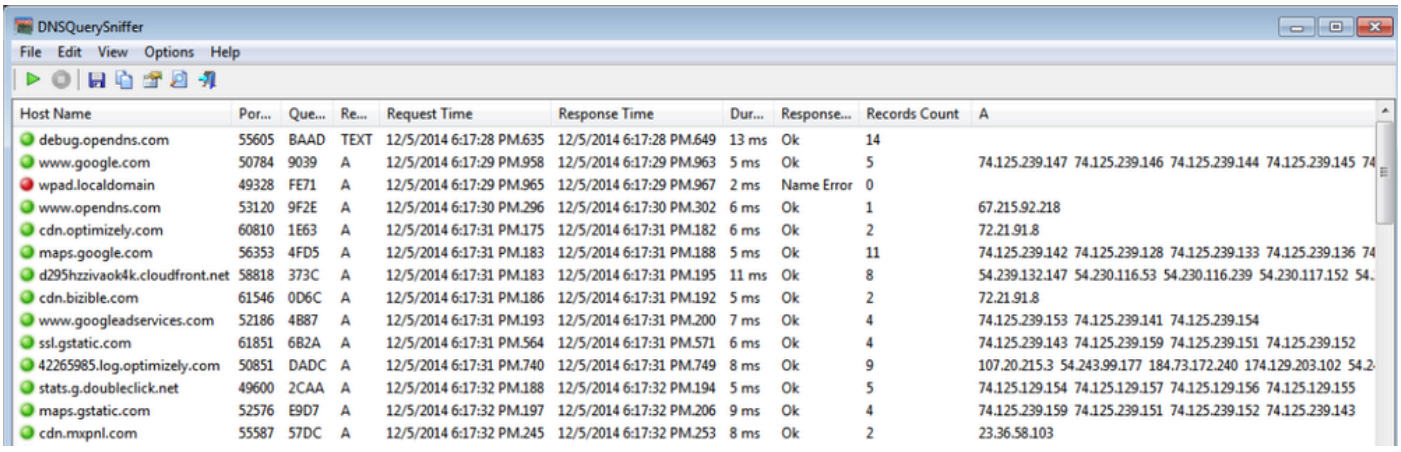


Anmerkung: Diese Spalten erscheinen ganz rechts in der Aufnahme, und Sie müssen einen Bildlauf durchführen, um sie zu sehen.

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

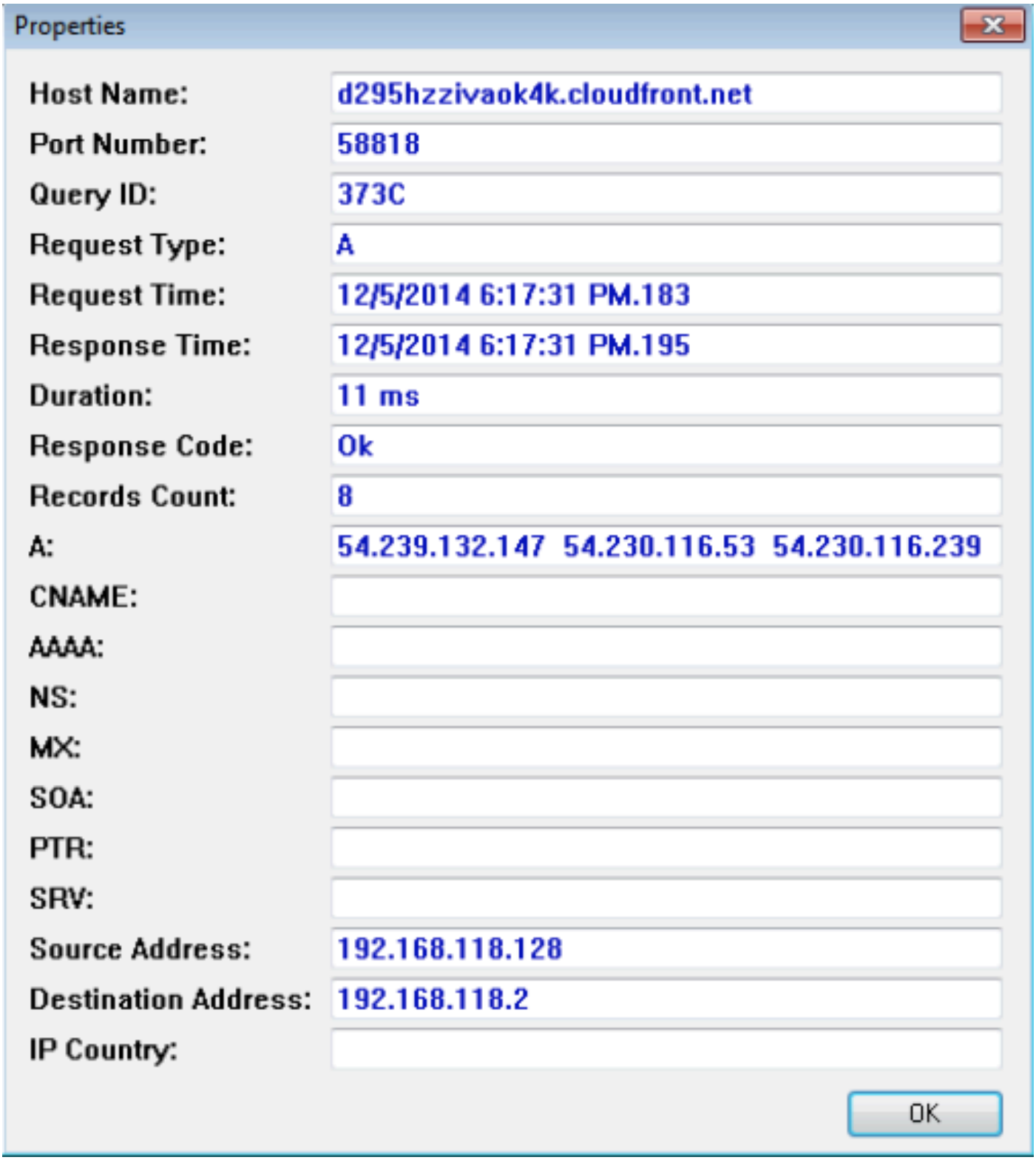
DNSSniffer-Spalten

Die Ergebnisse sehen wie folgt aus:



DNS 3.png

Ansicht einer individuellen Suche:



DNS 4.png

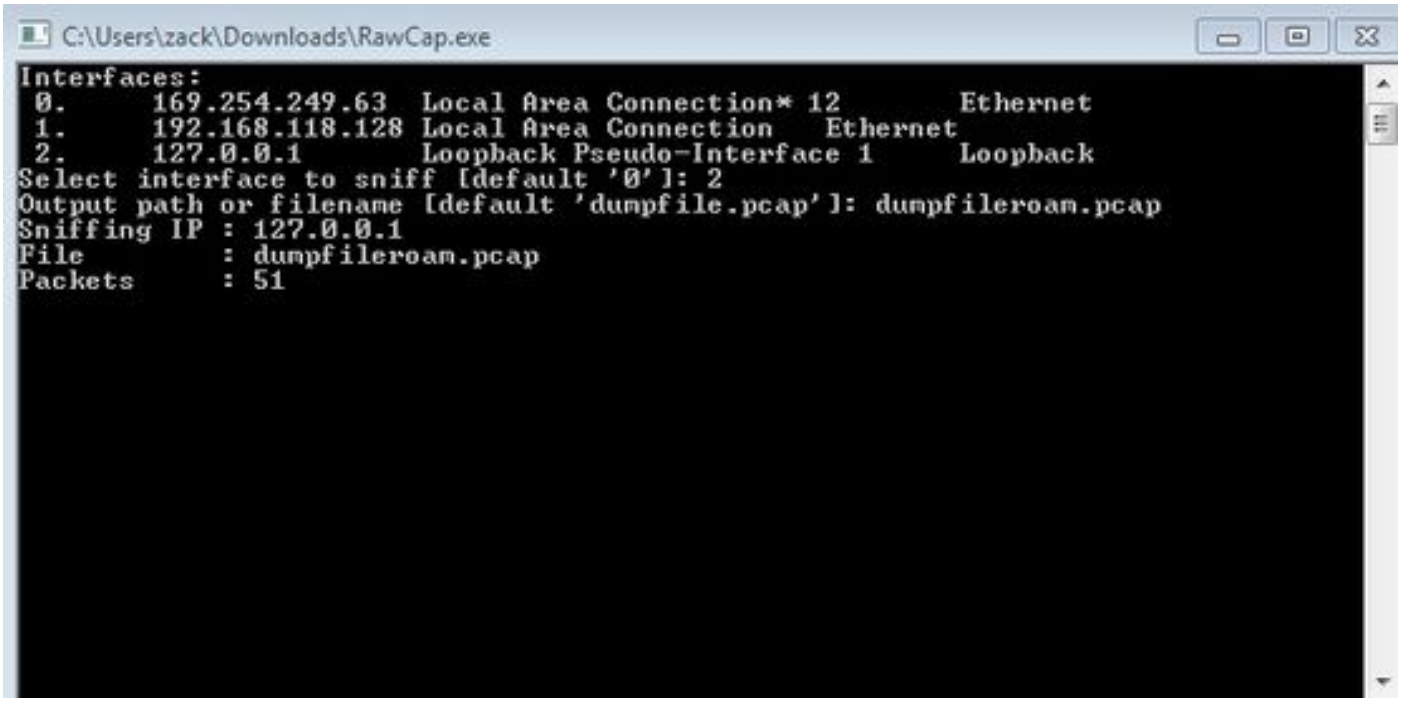
RawCap.exe - Windows-Alternative

Unter bestimmten Umständen wird die Schnittstelle, mit der Sie arbeiten müssen, nicht von dem in Wireshark enthaltenen Paketerfassungstreiber unterstützt. Dies kann ein Problem für die Loopback-Schnittstelle darstellen.

In diesen Fällen können Sie RawCap.exe verwenden:

1. Führen Sie die Schritte aus dem vorherigen Artikel aus, um Wireshark zur Erfassung des normalen Datenverkehrs zu verwenden.
2. Führen Sie gleichzeitig RawCap.exe aus.
3. Wählen Sie die Schnittstelle aus, indem Sie die entsprechende Listennummer angeben.
4. Geben Sie einen Namen für die Ausgabedatei an und ab geht es.
5. Wählen SieControl-Cwenn Sie die Erfassung beenden möchten.

Die gespeicherte Datei wird in dem Ordner abgelegt, in dem Sie RawCap.exe ausgeführt haben:



rawcap_1.jpg

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.