التقاط حركة مرور الشبكة باستخدام Wireshark

المحتويات

المقدمة

يوضح هذا المستند كيفية التقاط حركة مرور الشبكة باستخدام Wireshark.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى أمان طبقة DNS Umbrella.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

هناك أوقات يطلب فيها موظفو دعم Cisco Umbrella التقاط حزمة من حركة مرور الإنترنت المتدفقة بين الكمبيوتر والشبكة. يتيح التقاط دعم Umbrella لتحليل حركة المرور في مستوى منخفض وتحديد المشاكل المحتملة.

في معظم الحالات، من المفيد مقارنة مجموعتين من لقطات الحزم توضح سيناريو العمل وغير العمل على حد سواء.

- ضمنت أنت يستطيع كررت المشكلة وأتممت هذا steps بينما الإصدار يقع. قم بإنشاء التقاط حزمة يوضح سيناريو غير صالح. الرجاء ملاحظة التاريخ والوقت مع المنطقة الزمنية بحيث يمكن ربط هذه المعلومات ببيانات أخرى.
- إن أمكن، كرر هذه التعليمات مع برنامج Umbrella (و/أو إعادة توجيه DNS ل Umbrella) معطل. قم بإنشاء التقاط حزمة يوضح سيناريو العمل. الرجاء ملاحظة التاريخ والوقت مع المنطقة الزمنية بحيث يمكن ربط هذه المعلومات ببيانات أخرى.

تعليمات Wireshark

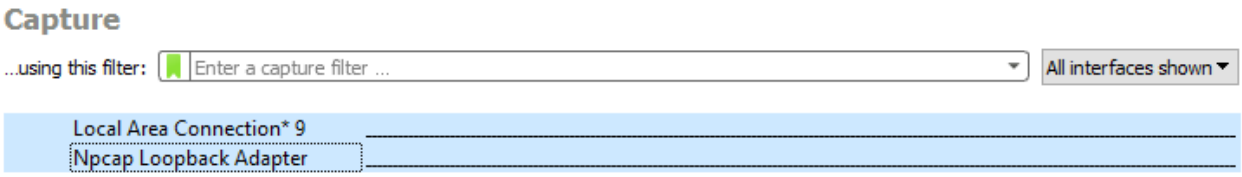
تحضيرات

1. تنزيل Wireshark.
2. قطع اتصال أية إتصالات شبكة غير ضرورية.
    1. افصل إتصالات VPN ما لم تكن مطلوبة لتكرار المشكلة.
    2. لا تستخدم إلا التوصيل السلكي وأ اللاسلكي وليس كليهما معا.
3. قم بإغلاق أي برنامج آخر غير مطلوب لتكرار المشكلة.
4. قم بمسح ملفات تعريف الارتباط وذاكرة التخزين المؤقت من المستعرض.
5. مسح ذاكرة التخزين المؤقت ل DNS. على Windows باستخدام الأمر:

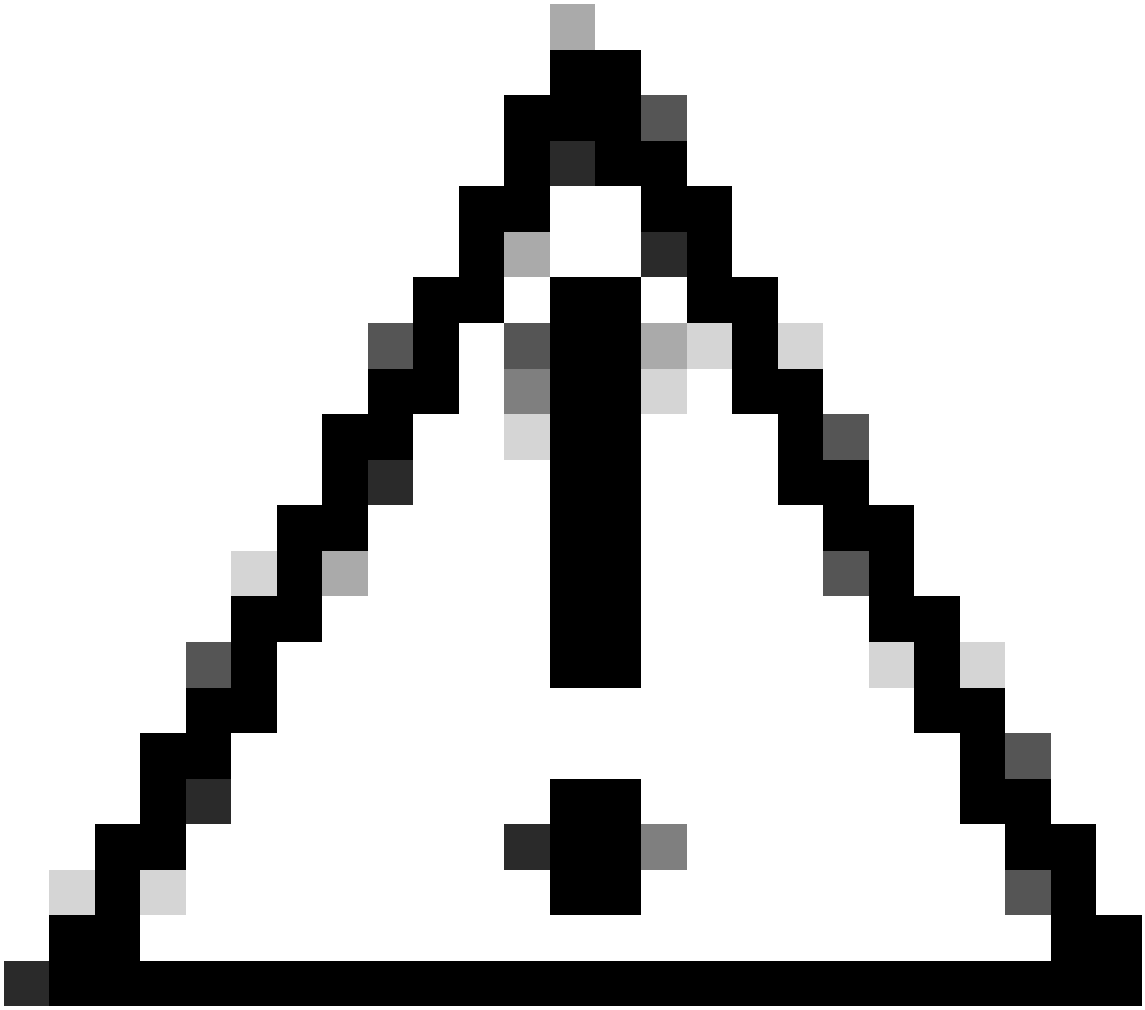
```
ipconfig /flushdns
```

أسر أساسي لأوراق الفلاش

1. إطلاق Wireshark.
2. تعرض لوحة الالتقاط واجهات الشبكة. حدد الواجهات ذات الصلة. يمكن تحديد واجهات متعددة باستخدام مفتاح CTRL (في Windows) أو مفتاح CMD (في Mac) أثناء التحديد.

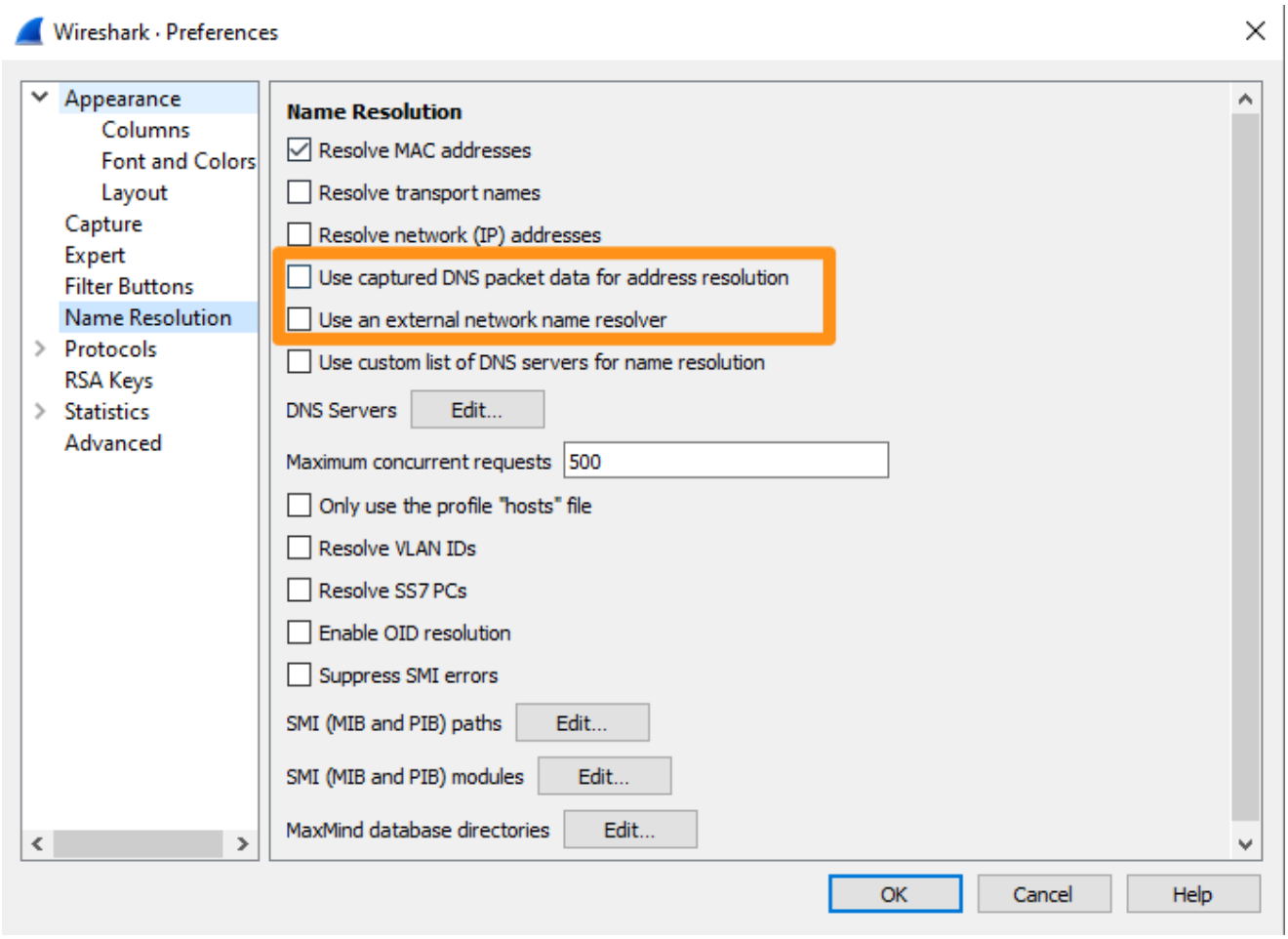


wireshark_1.png



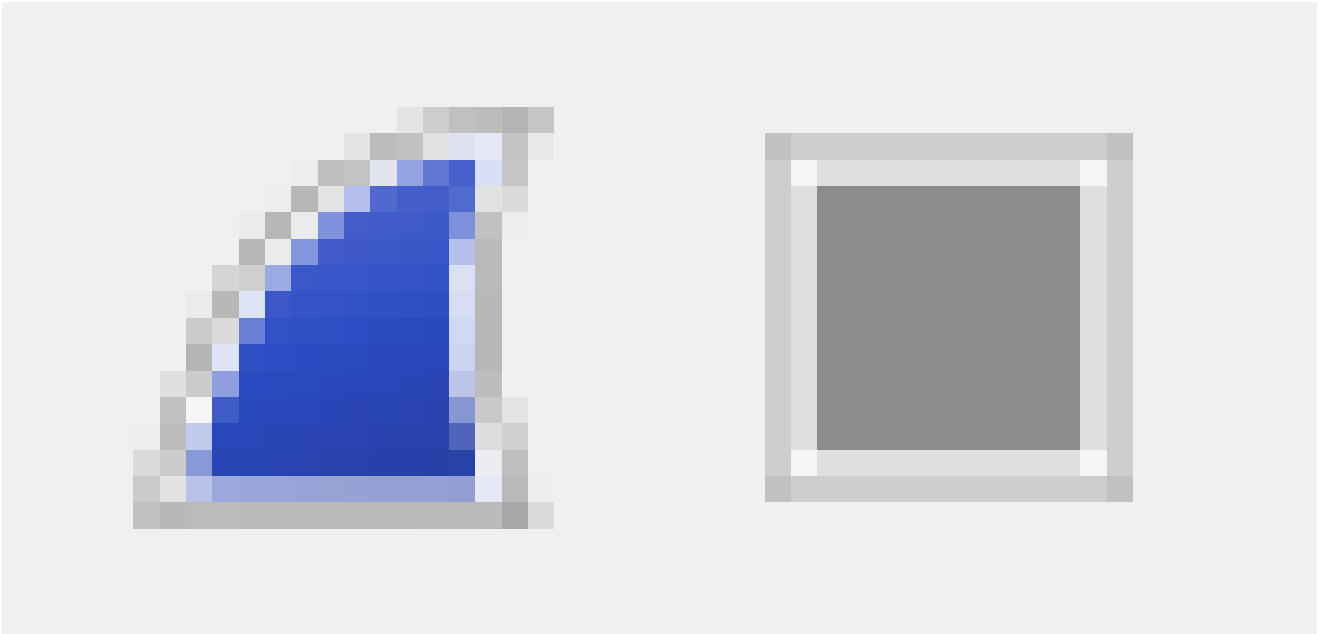
تحذير: من المهم تحديد الواجهة (الواجهات) الصحيحة التي تحتوي على حركة مرور الشبكة. أستخدم الأمر ipconfig" (في Windows) أو الأمر ifconfig (في Mac) لعرض مزيد من التفاصيل حول واجهات الشبكة. يجب على مستخدمي العميل المتجول تحديد مهايئ إسترجاع NPCAP أو الاسترجاع بشكل إضافي: واجهات Lo0. إذا كنت في شك، فحدد جميع الواجهات.

3. تأكد من أن إستخدام بيانات حزمة DNS الملتقطة لدقة العنوان وإستخدام محلل اسم DNS لأن ذلك يمكن أن يعقد الالتقاط ويؤثر على AnyConnect. الإعدادات صالحة اعتبارا من Wireshark 3.4.9:



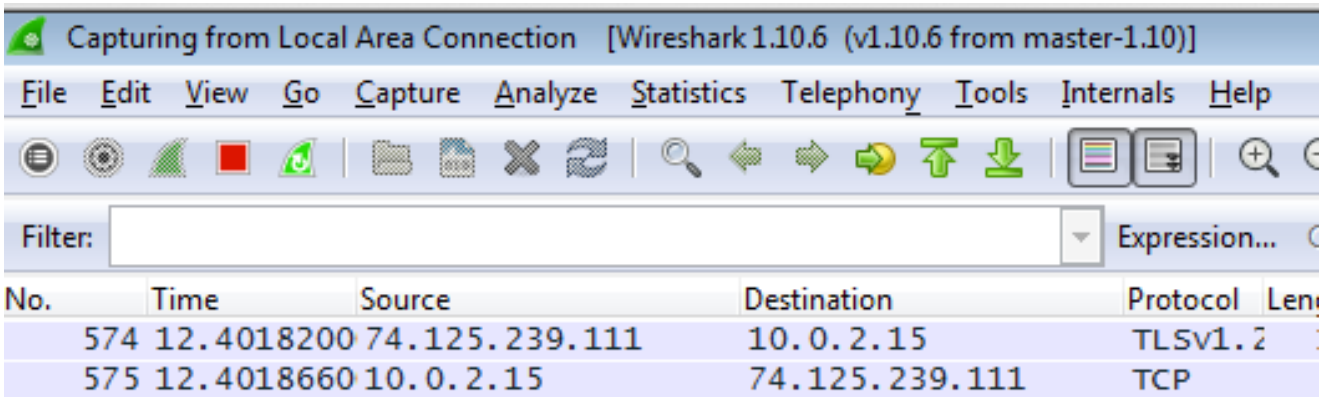
capture_png.png

4. حدد التقاط > بدء أو حدد أيقونة بداية زرقاء.



wireshark_2.png

5. بينما يعمل Wireshark في الخلفية، كرر المشكلة.



wireshark_3.png

6. بمجرد أن يتم نسخ المسألة نسخا متماثلا بالكامل، حدد التقاط > إيقاف أو أستخدم أيقونة التوقف الأحمر.
7. انتقل إلى ملف > حفظ باسم وحدد مكانا لحفظ الملف. تأكد من حفظ الملف كنوع PCAPNG. يمكن إرسال الملف المحفوظ إلى دعم Cisco Umbrella للمراجعة.

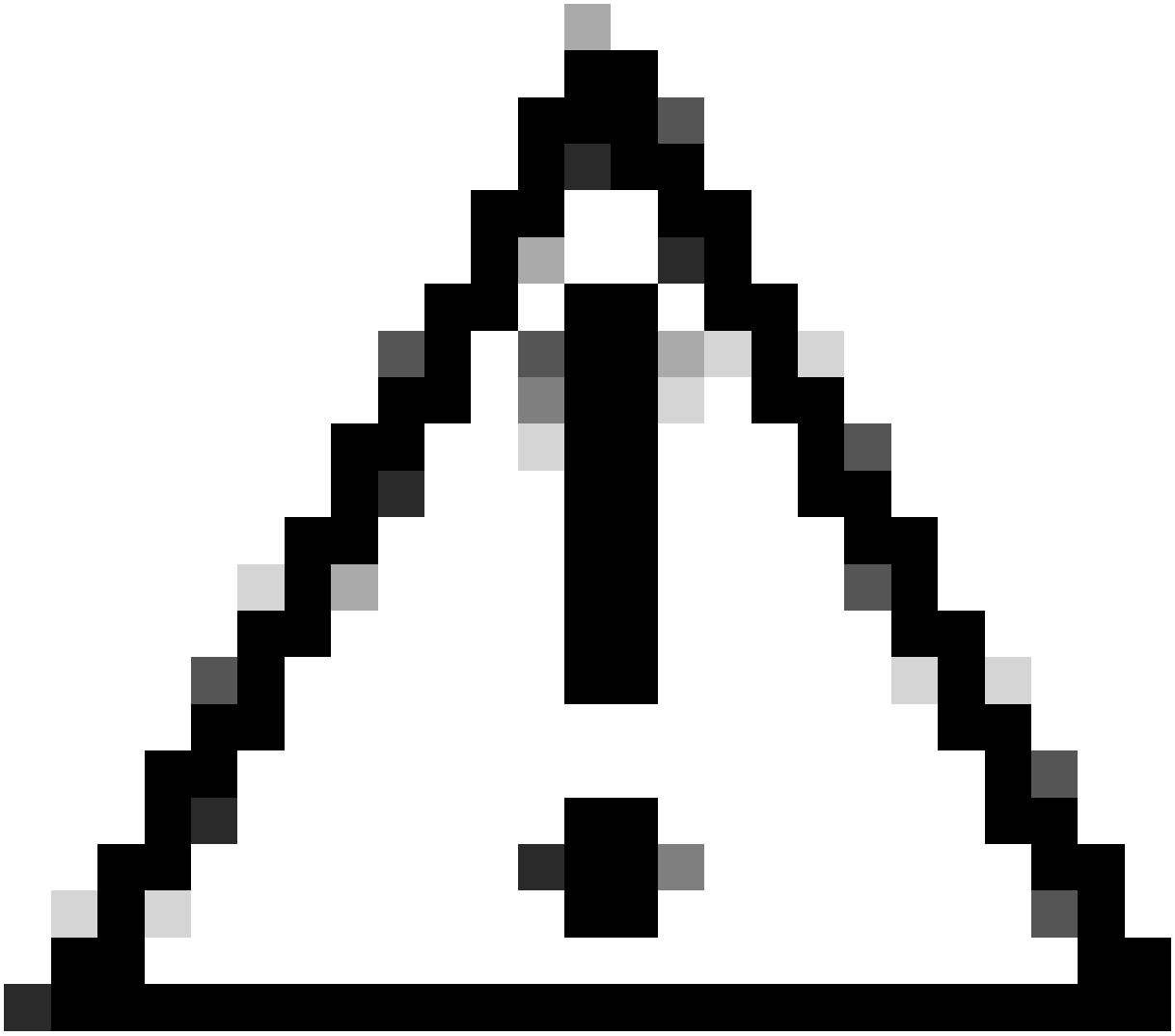
العميل المتجول - خطوات إضافية

هناك خطوات إضافية يجب إكمالها لكل من عملاء التوجال المستقلين ومستخدمي AnyConnect الوحدات النمطية المتجولة:

حركة مرور الاسترجاع

عند تحديد واجهة، يجب أيضا التقاط حركة مرور البيانات على واجهة الاسترجاع (127.0.0.1) بالإضافة إلى واجهات الشبكة الأخرى. يقوم وكيل DNS الخاص بالعميل المتجول بالإصغاء على هذه الواجهة، لذلك فمن المهم أن ترى حركة مرور البيانات بين نظام التشغيل والعميل المتجول.

- Windows: حدد موائئ إسترجاع NPCAP
- ماك: تحديد الاسترجاع: lo0



تحذير: إصدارات أحدث من Windows للشحن السلكي مع برنامج تشغيل التقاط NPCAP، والذي يدعم برنامج تشغيل الاسترجاع. إذا كان مهايئ الاسترجاع غير موجود، فقم بتحديث أحدث إصدار من Wireshark أو أستخدم تعليمات rawcap.exe.

حركة مرور DNS المشفرة

في الظروف العادية، يتم تشفير حركة مرور البيانات بين العميل المتجول والمظلة والتي يتم قراءتها بواسطة البشر. في بعض الحالات، يمكن أن يطلب دعم Umbrella أن تقوم بتعطيل تشفير DNS لرؤية حركة مرور DNS بين العميل المتجول وسحابة Umbrella. هناك طريقتان للقيام بذلك:

- إنشاء كتلة جدار حماية محلي لـ UDP 443 إلى 208.67.220.220 و 208.67.222.222.
- أو قم بإنشاء الملف بناء على نظام التشغيل وإصدار العميل المتجول:
  - 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
  ```

- ماك وأ إس:

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

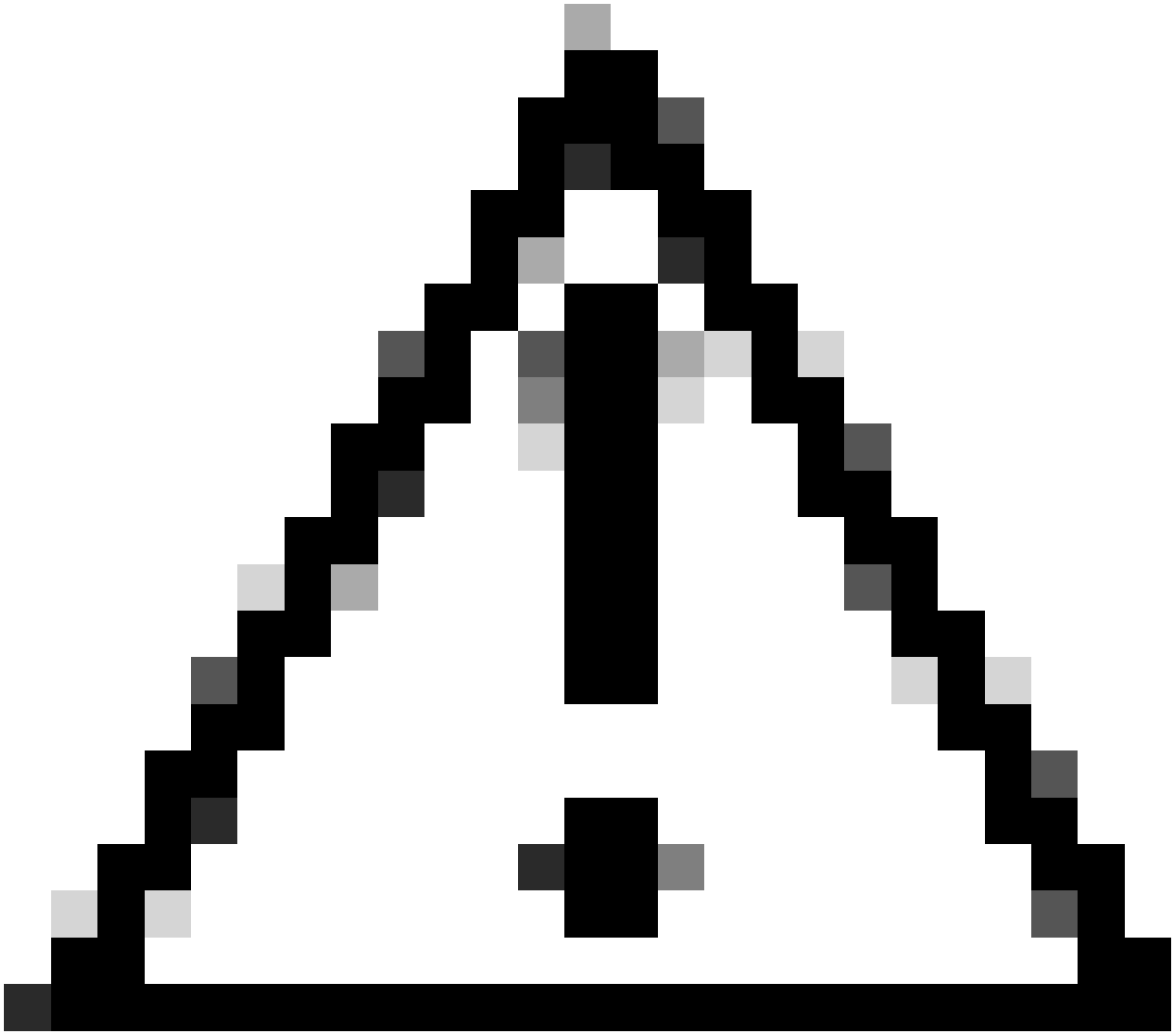
- نظام التشغيل Mac OS AnyConnect:

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

- نظام التشغيل Mac OS العميل الآمن:

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

بعد القيام بذلك، قم بإعادة تشغيل الخدمة أو الكمبيوتر.



تحذير: تتضمن الإصدارات الأحدث من Wireshark على Windows برنامج تشغيل التقاط NPCAP، والذي لا يدعم واجهة Umbrella VPN. على Windows، قد تحتاج لاستخدام أداة rawcap.exe كبديل.

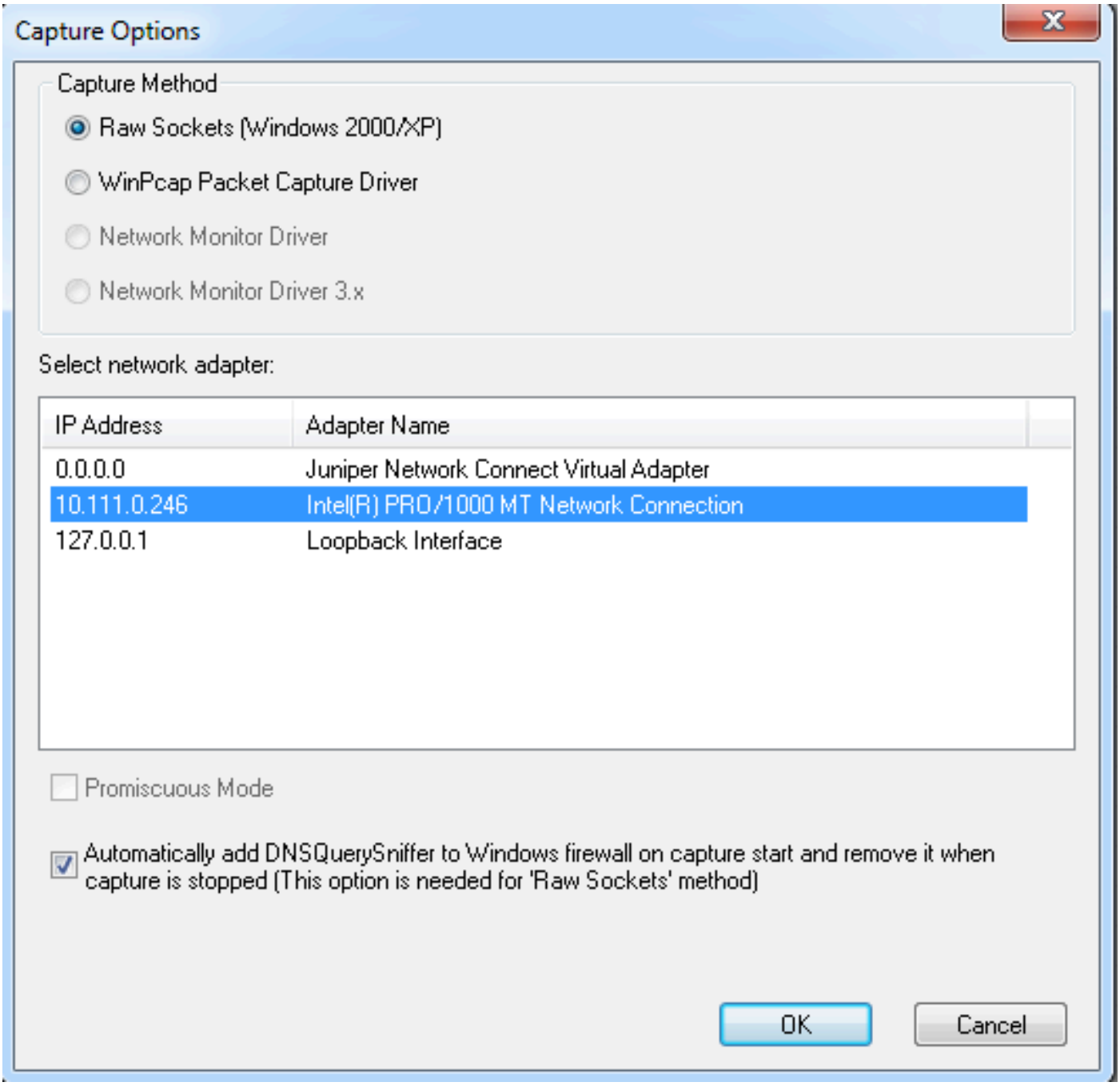
DNSQuerySniffer - Windows Alternative

DNSQuery sniffer هو sniffer شبكة DNS فقط لـ Windows والذي يراقب ويعرض أطنان من البيانات المفيدة. وعلى النقيض من ويرشارك وأ وارك، فإن إستخدام هذا النهج يقتصر على نظام أسماء النطاقات (DNS)، وهو أسهل كثيرا في فحص واستخلاص المعلومات ذات الصلة. إلا أنها لا تمتلك أدوات التصفية القوية التي يتمتع بها موقع Wireshark.

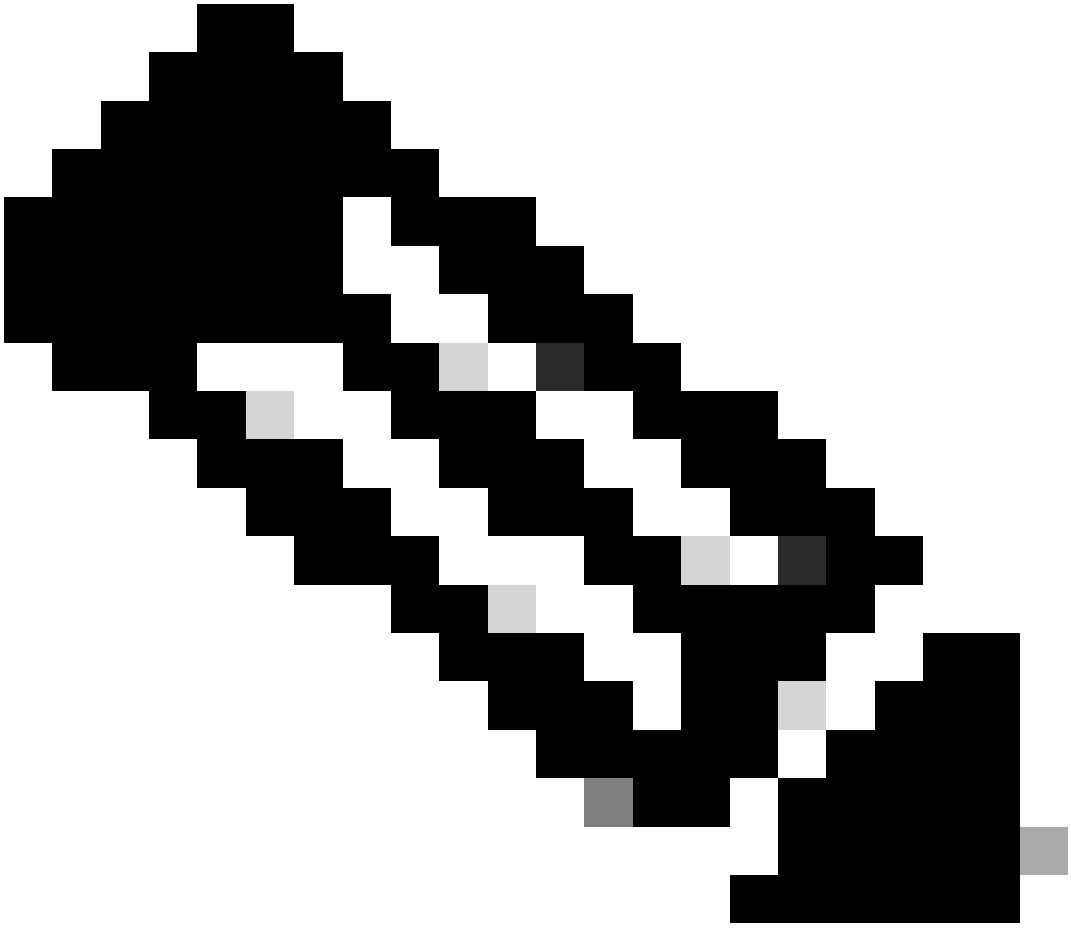
هذه أداة خفيفة الوزن وسهلة الاستخدام. من مميزات إستخدام هذا الخيار أنه يمكنك التقاط الحزم أثناء تعطيل خدمة "العميل المتجول"، وبعد التقاط، ويمكنك مشاهدة كل استعلام DNS يرسله العميل المتجول من اللحظة التي يبدأ فيها تشغيل الالتقاط بدلا من بدء الالتقاط بعد بدء تشغيل "العميل المتجول" بالفعل.

هناك طريقتان للالتقاط:

1. إذا حددت واجهة الشبكة العادية، فيمكنك رؤية الاستعلامات الموجودة في قائمة المجالات الداخلية فقط، أو التي لم تمر تحديدا عبر dnscryptproxy.



dns_1.png

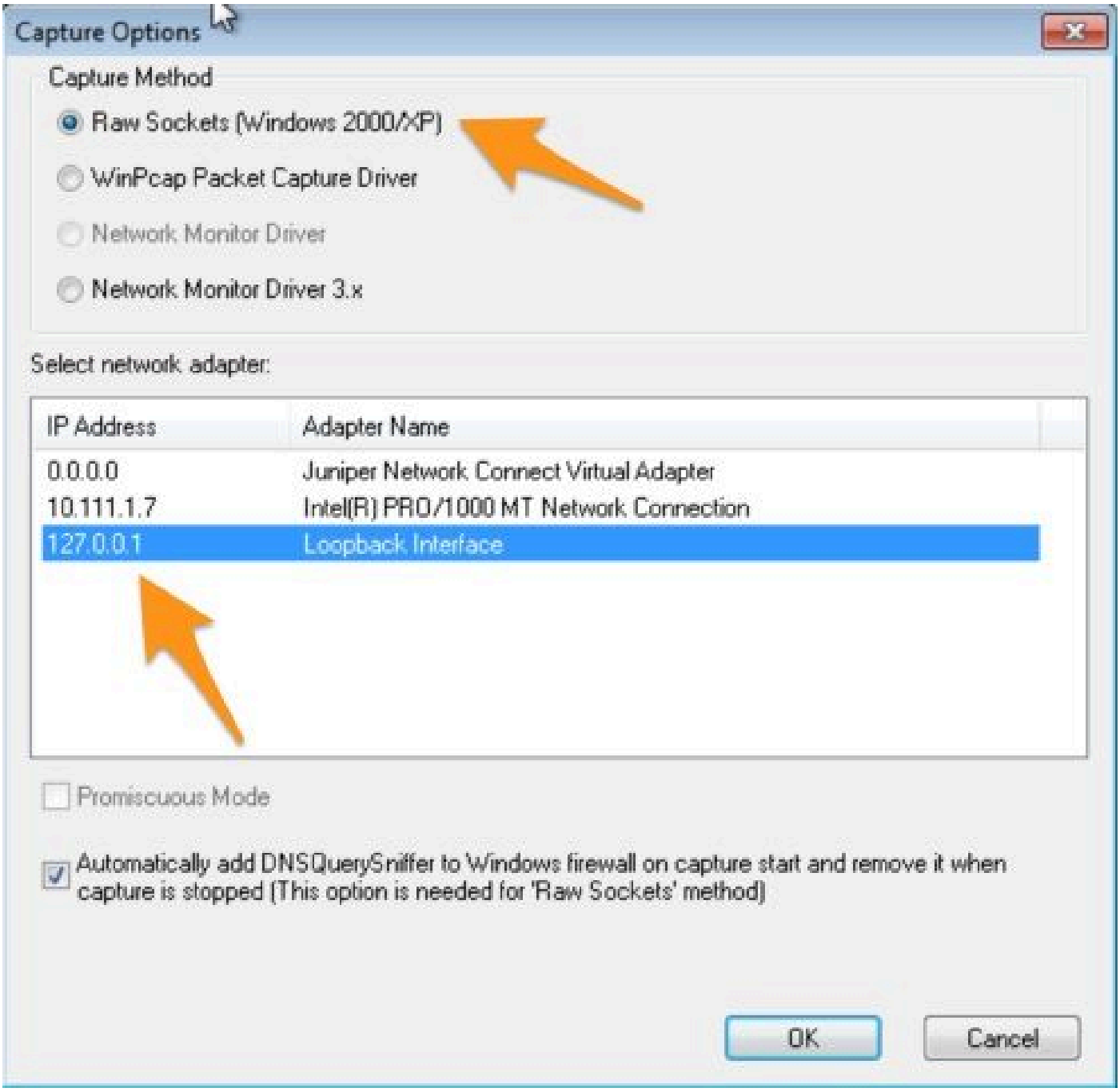


ملاحظة: تظهر هذه الأعمدة في إتجاه اليمين في الالتقاط وعليك أن تنزلق فوقهم قليلا جدا لرؤيتهم.

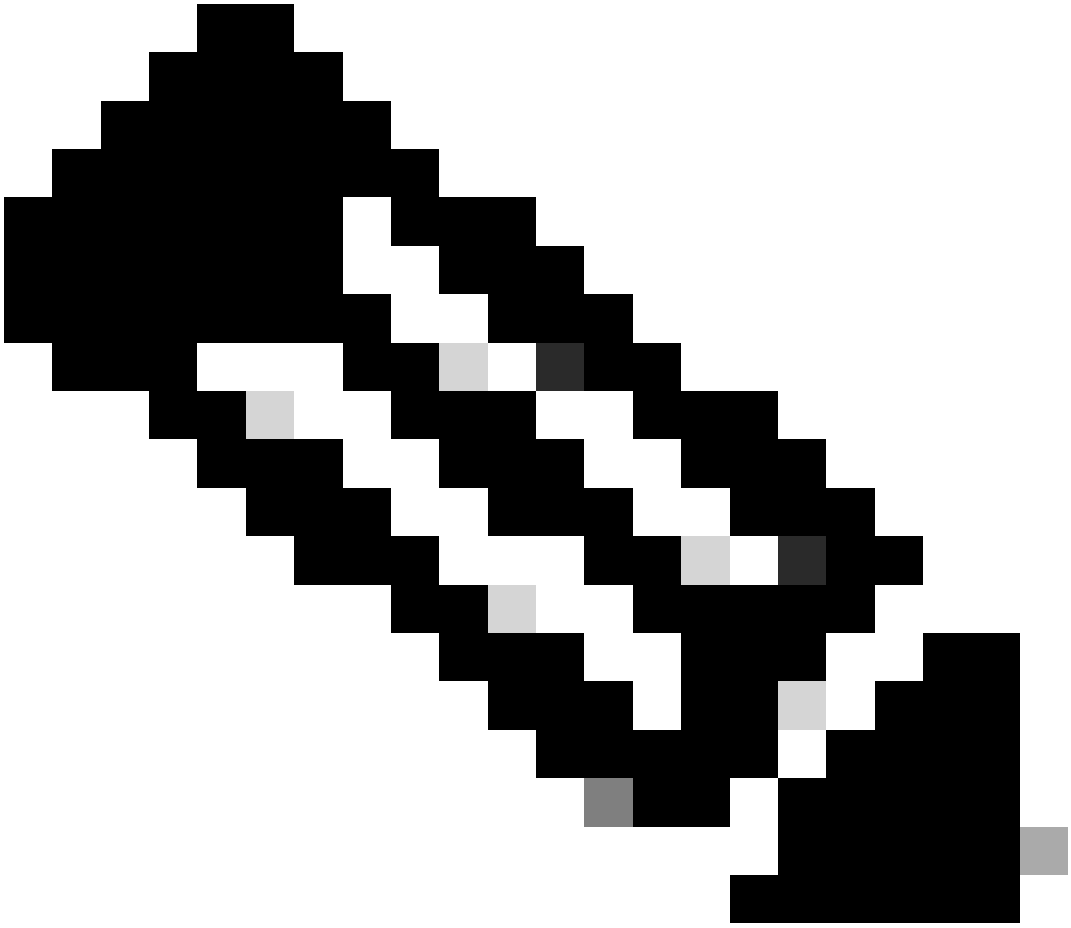
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

أعمدة DnssNiffer

2. إذا حددت واجهة الاسترجاع، فسترى جميع استعلامات DNS التي يتم إرسالها من خلال DNSCRYPTPROXY، ولكن لا يمكنك رؤية عنوان IP الوجهة الحقيقي للمجالات الموجودة في قائمة المجالات الداخلية. ومع ذلك، فإنه لا يزال يعرض الاستعلام والإجابة.


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

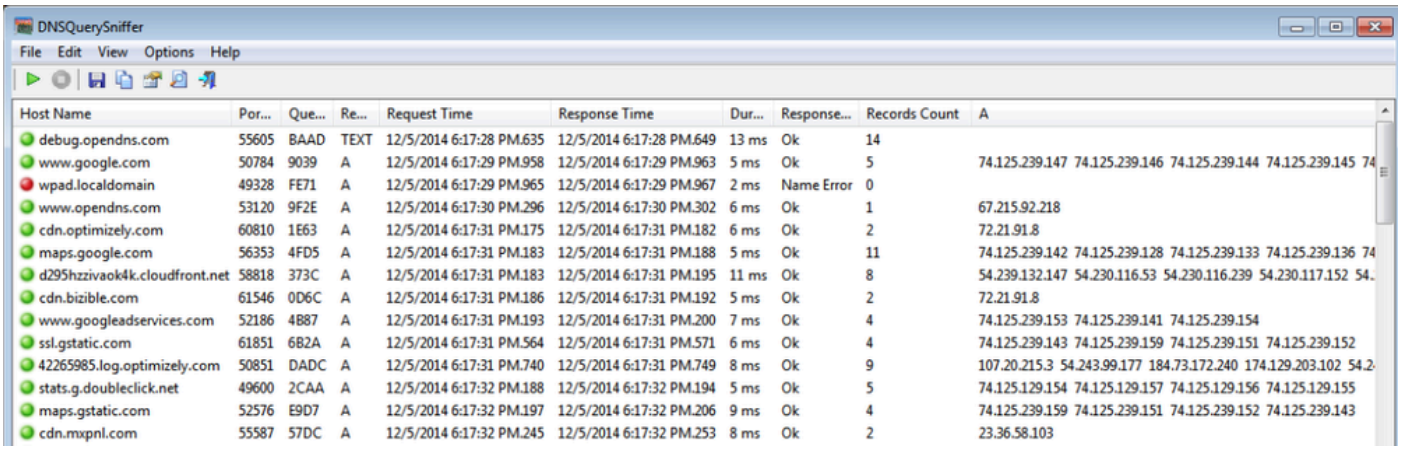


ملاحظة: تظهر هذه الأعمدة في إتجاه اليمين في الالتقاط، وعليك أن تنزلق فوقهم قليلا جدا لرؤيتهم.

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

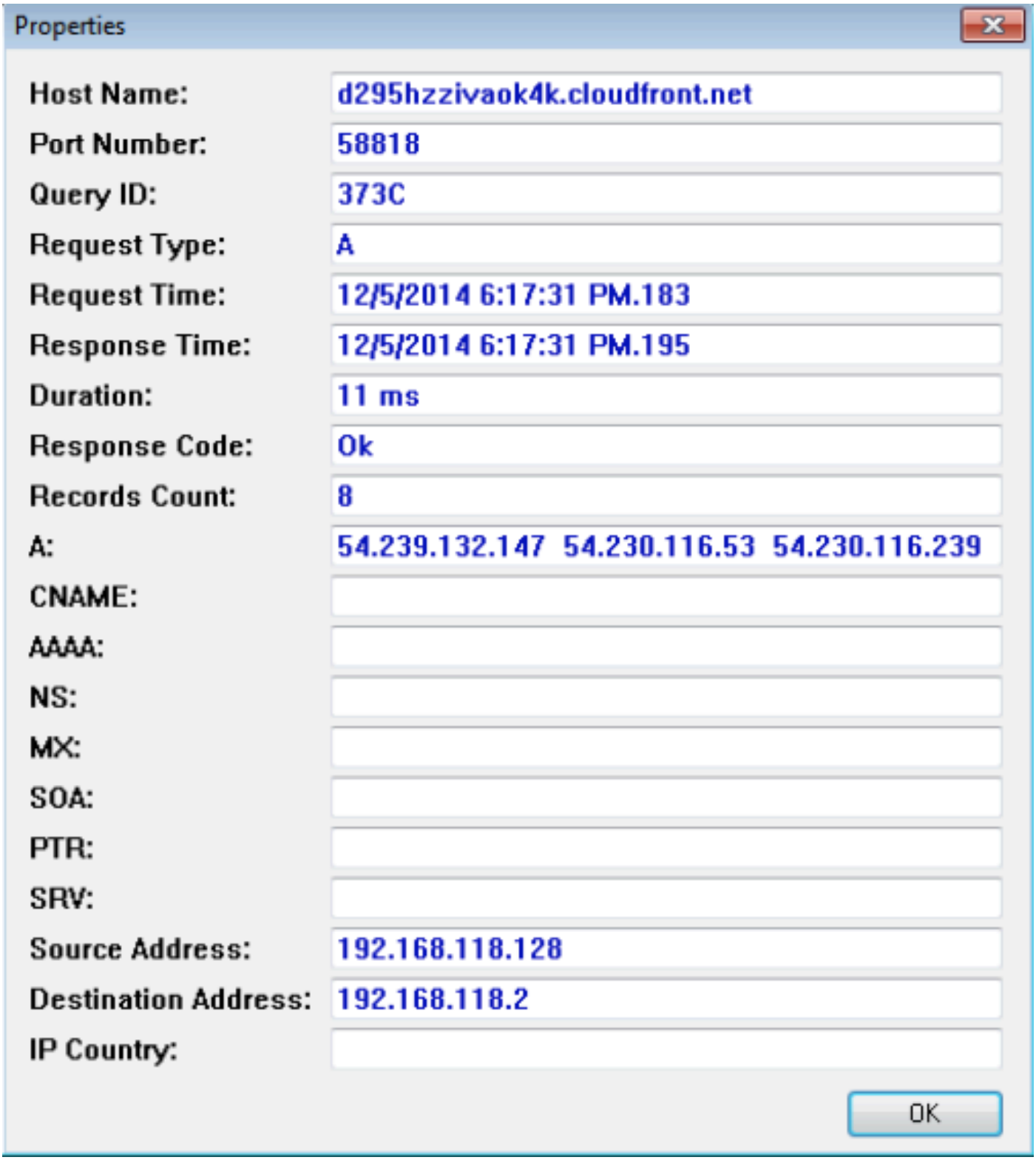
أعدة DnssNiffer

النتائج تبدو كما يلي:



dns_3.png

عرض البحث الفردي:



dns_4.png

RawCap.exe - Windows Alternative

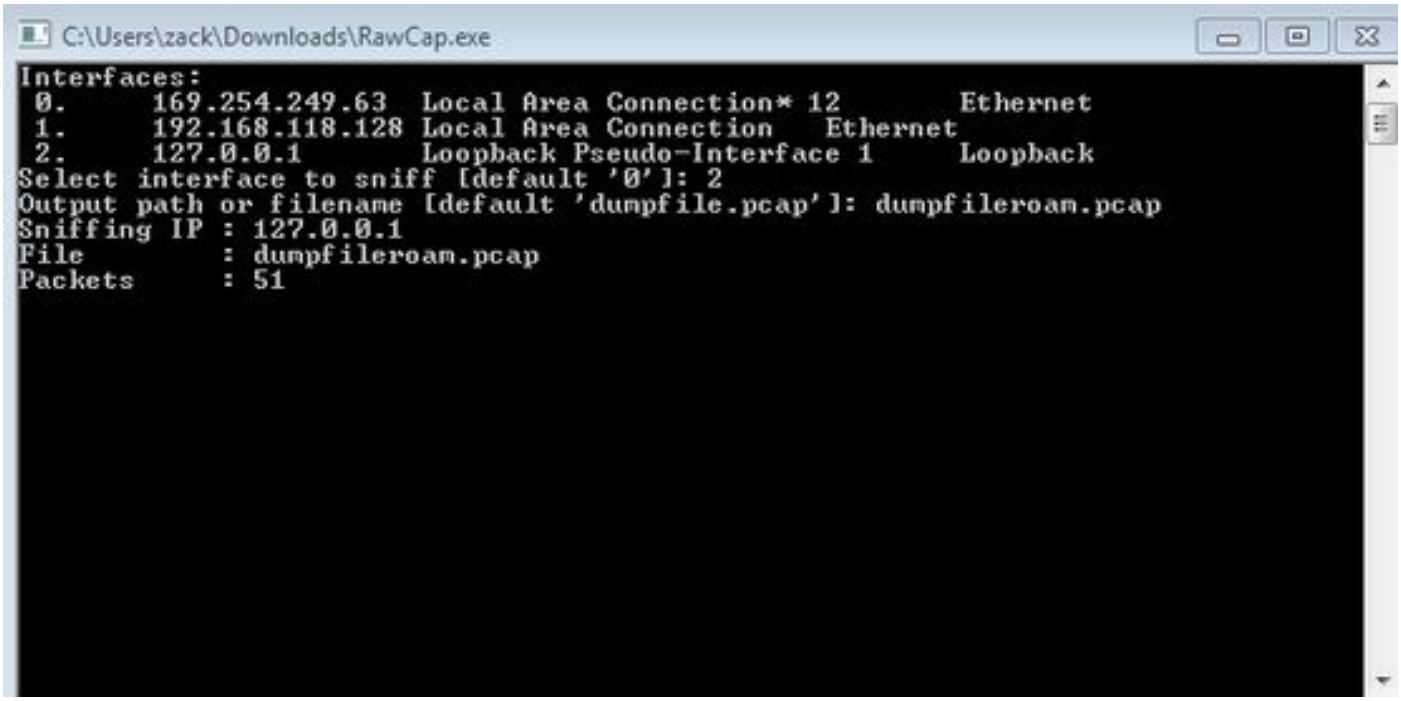
في بعض الحالات، ال يدعم برنامج تشغيل التقاط الحزمة المضمن مع Wireshark الواجهة التي تحتاج إلى العمل معها. يمكن أن يكون هذه مشكلة لواجهة الاسترجاع.

في هذه الأمثلة، يمكننا إستخدام RawCap.exe:

1. أتمت ال steps من قبل في المقالة أن يستعمل Wireshark أن على قبض حركة مرور عادي.

2. في نفس الوقت، قم بتشغيل RawCap.exe.
3. قم بتحديد الواجهة عن طريق تحديد رقم القائمة المطابق.
4. قم بتعيين اسم ملف مخرجات ثم يتم تشغيله.
5. SelectControl-Cwhen الذي تريد إيقاف الالتقاط.

يتم وضع الملف المحفوظ في المجلد الذي قمت بتشغيل RawCap.exe منه:



rawcap_1.jpg

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).