Wireshark로 네트워크 트래픽 캡처

목차

소개

이 문서에서는 Wireshark를 사용하여 네트워크 트래픽을 캡처하는 방법을 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella DNS Layer Security를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Cisco Umbrella Support 직원이 컴퓨터와 네트워크 간에 흐르는 인터넷 트래픽의 패킷 캡처를 요청하는 경우가 있습니다. 이 캡처를 통해 Umbrella는 낮은 레벨에서 트래픽을 분석하고 잠재적인 문제를 식별할 수 있습니다.

대부분의 경우 작동 시나리오와 비작동 시나리오를 모두 보여 주는 두 패킷 캡처 집합을 비교하는 것이 유용합니다.

- 문제가 발생하는 동안 문제를 복제하고 다음 단계를 완료할 수 있는지 확인합니다. 비작동 시나리오를 보여주는 패킷 캡처를 생성합니다. 이 정보가 다른 데이터와 상관 관계를 분석할 수 있도록 표준 시간대의 날짜 및 시간을 기록해 두십시오.
- 가능한 경우 Umbrella 소프트웨어(및/또는 Umbrella DNS 포워딩)를 비활성화한 상태에서 이 지침을 반복합니다. 작업 시나리오를 보여주는 패킷 캡처를 생성합니다. 이 정보가 다른 데이터와 상관 관계를 분석할 수 있도록 표준 시간대의 날짜 및 시간을 기록해 두십시오.

Wireshark 지침

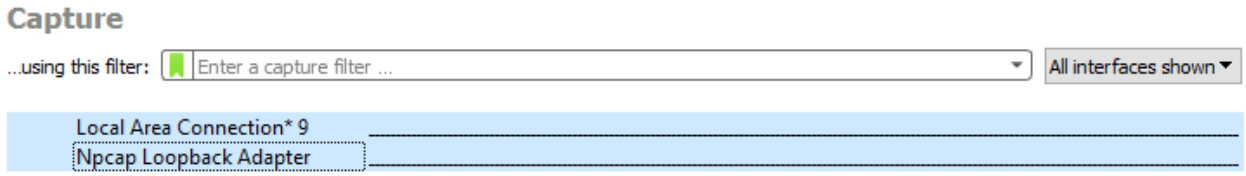
준비

1. Wireshark 다운로드
2. 불필요한 네트워크 연결을 모두 끊습니다.
    1. 문제를 복제하는 데 필요한 경우가 아니면 VPN 연결을 끊습니다.
    2. 유선 또는 무선 연결만 사용하고 둘 다 사용하지 마십시오.
3. 문제를 복제하는 데 필요하지 않은 다른 모든 소프트웨어를 닫습니다.
4. 브라우저에서 쿠키 및 캐시를 지웁니다.
5. DNS 캐시를 플러시합니다. Windows에서 다음 명령을 사용합니다.

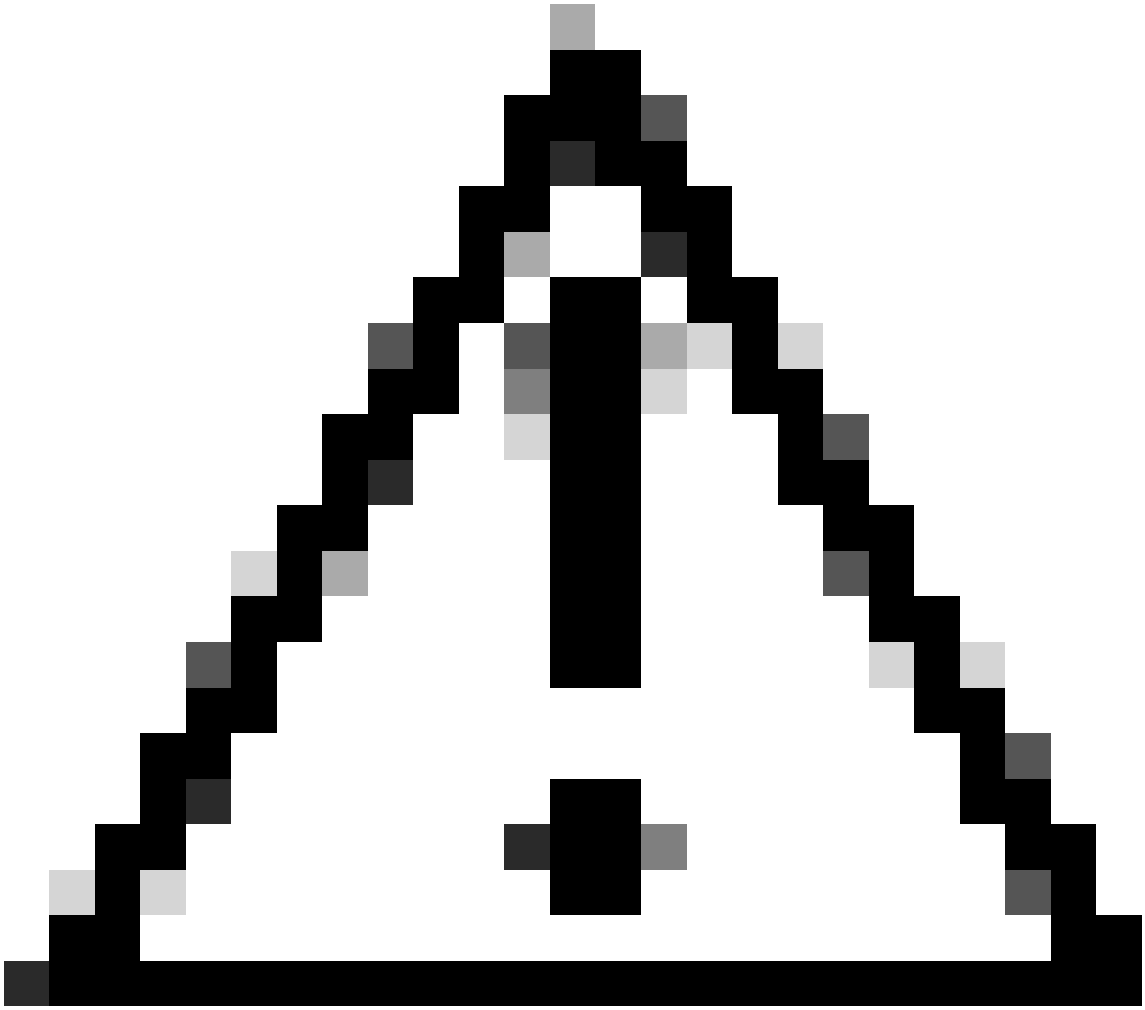
```
ipconfig /flushdns
```

기본 Wireshark 캡처

1. Wireshark 시작
2. Capture(캡처) 패널에는 네트워크 인터페이스가 표시됩니다. 관련 인터페이스를 선택합니다. 여러 인터페이스는 선택하는 동안 CTRL 키(WIndows) 또는 CMD 키(Mac)를 사용하여 선택할 수 있습니다.

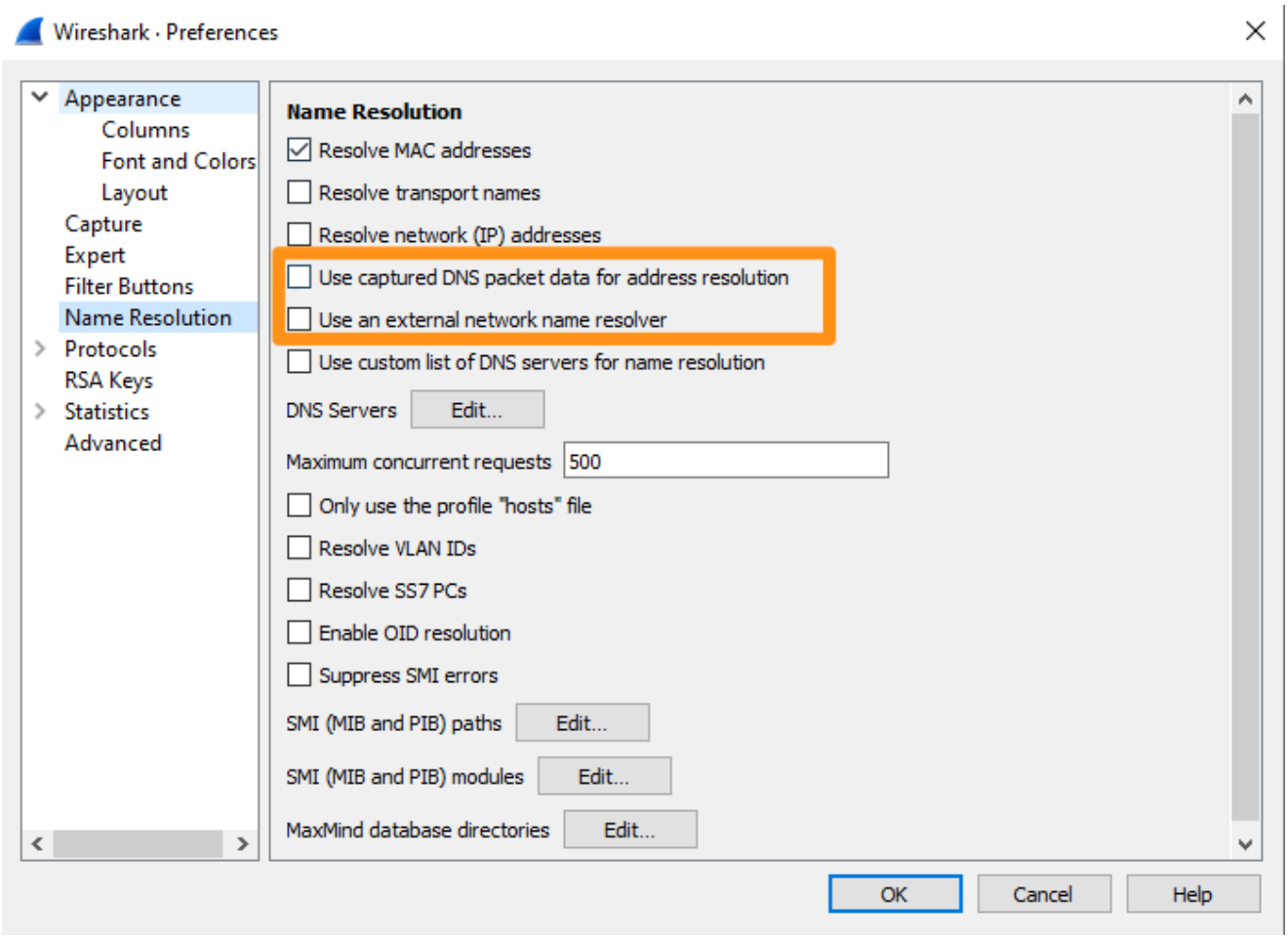


wireshark_1.png



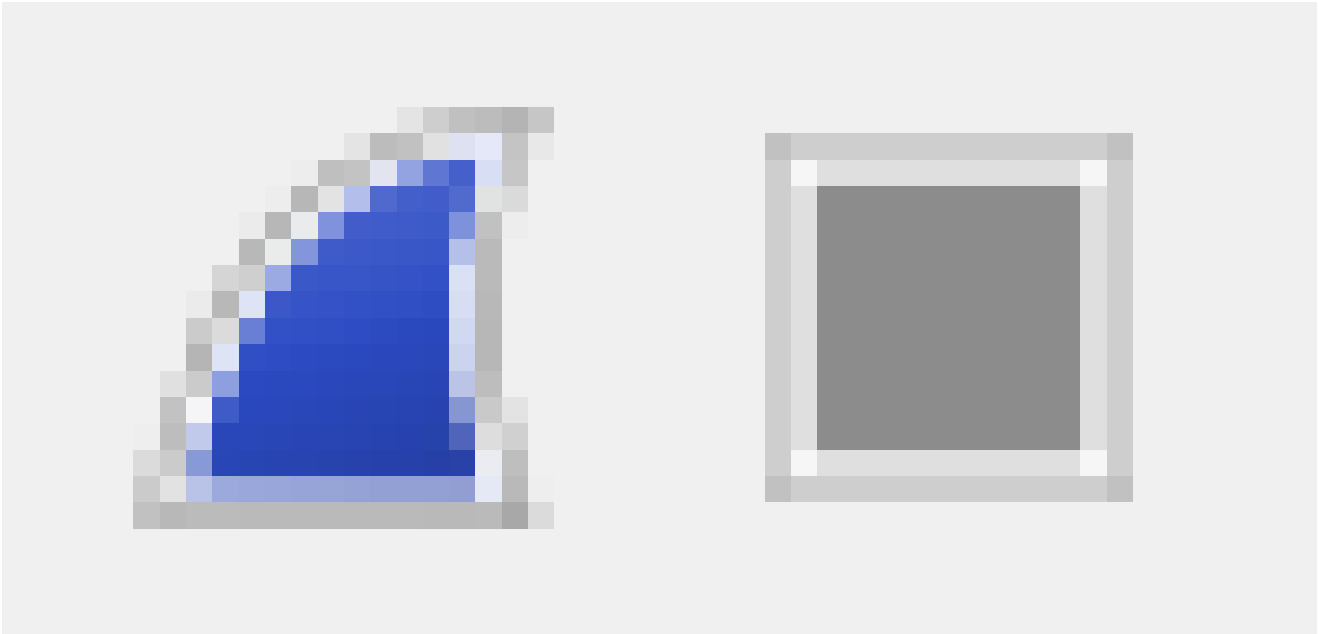
주의: 네트워크 트래픽을 포함하는 올바른 인터페이스를 선택하는 것이 중요합니다. 네트워크 인터페이스에 대한 자세한 내용을 보려면 "ipconfig" 명령(Windows) 또는 "ifconfig" 명령(Mac)을 사용합니다. 로밍 클라이언트 사용자는 NPCAP 루프백 어댑터 또는 루프백을 추가로 선택해야 합니다. lo0 인터페이스. 확실하지 않은 경우 모든 인터페이스를 선택합니다.

3. 캡처한 DNS 패킷 데이터를 주소 확인에 사용하고 외부 네트워크 이름 확인자 사용을 선택하지 않도록 하여 Wireshark가 DNS 쿼리를 만들지 않도록 하십시오. 이 경우 캡처가 복잡해지고 AnyConnect에 영향을 줄 수 있습니다. 설정은 Wireshark 3.4.9부터 유효합니다.



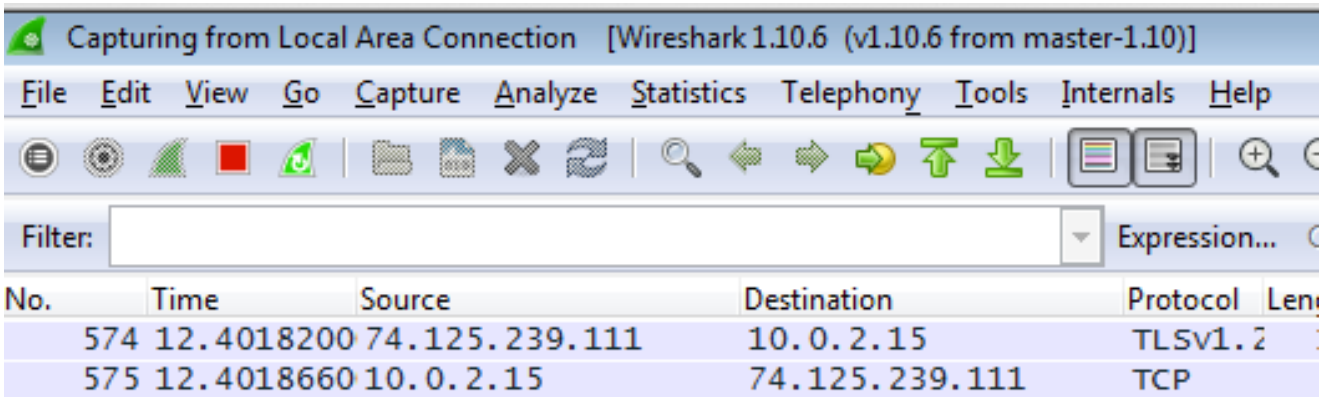
Capture_PNG.png

4. Capture(캡처) > Start(시작)를 선택하거나 파란색 시작 아이콘을 선택합니다.



wireshark_2.png

5. Wireshark가 백그라운드에서 실행되는 동안 문제를 복제합니다.



wireshark_3.png

6. 문제가 완전히 복제되면 Capture(캡처) > Stop(중지)을 선택하거나 빨간색 Stop(중지) 아이콘을 사용합니다.
7. 파일 > 다른 이름으로 저장으로 이동하여 파일을 저장할 위치를 선택합니다. 파일이 PCAPNG 유형으로 저장되었는지 확인합니다. 저장된 파일은 검토를 위해 Cisco Umbrella 지원에 제출할 수 있습니다.

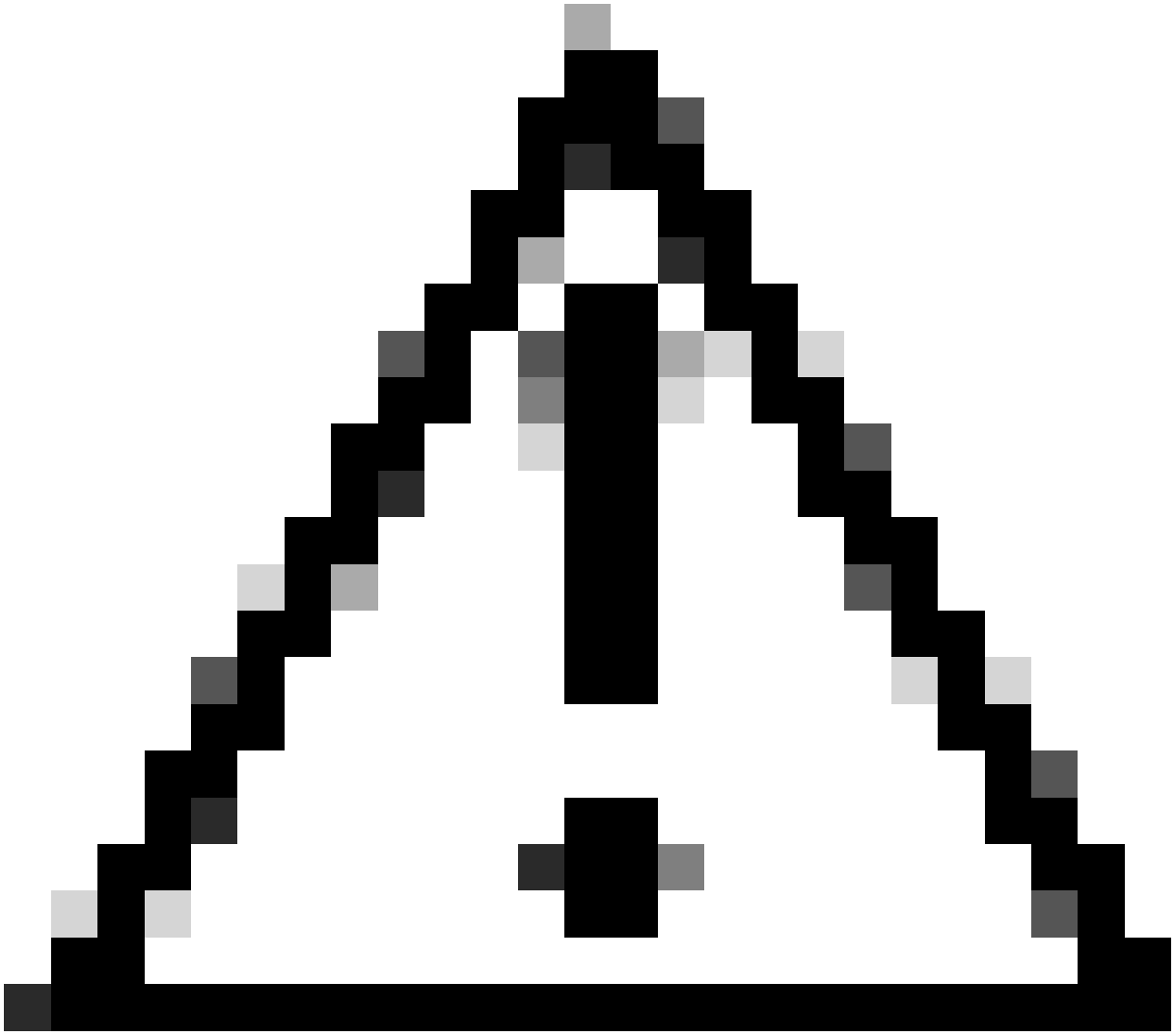
로밍 클라이언트 - 추가 단계

독립형 로밍 클라이언트 및 AnyConnect 로밍 모듈 사용자 모두에 대해 완료해야 하는 추가 단계가 있습니다.

루프백 트래픽

인터페이스를 선택할 경우 다른 네트워크 인터페이스 외에 루프백 인터페이스(127.0.0.1)에서도 트래픽을 캡처해야 합니다. 로밍 클라이언트의 DNS 프록시는 이 인터페이스에서 수신하므로 운영 체제와 로밍 클라이언트 간에 트래픽이 이동하는 것을 확인하는 것이 중요합니다.

- 창: NPCAP 루프백 어댑터 선택
- Mac: 루프백 선택: lo0



주의: 루프백 드라이버를 지원하는 NPCAP 캡처 드라이버가 포함된 최신 Windows 버전의 Wireshark가 제공됩니다. 루프백 어댑터가 없는 경우 최신 버전의 Wireshark로 업데이트하거나 rawcap.exe 명령을 사용합니다.

암호화된 DNS 트래픽

정상적인 상황에서는 로밍 클라이언트와 Umbrella 간의 트래픽이 암호화되며 사람이 읽을 수 없습니다. 경우에 따라 Umbrella 지원에서 로밍 클라이언트와 Umbrella 클라우드 간의 DNS 트래픽을 확인하기 위해 DNS 암호화를 비활성화하도록 요청할 수 있습니다. 두 가지 방법으로 이를 수행할 수 있습니다.

- UDP 443~208.67.220.220 및 208.67.222.222에 대한 로컬 방화벽 블록을 생성합니다.
- 또는 로밍 클라이언트의 OS 및 버전에 따라 파일을 만듭니다.
    - 창:

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

- Windows AnyConnect

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

- Windows 보안 클라이언트:

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

- macOS:

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

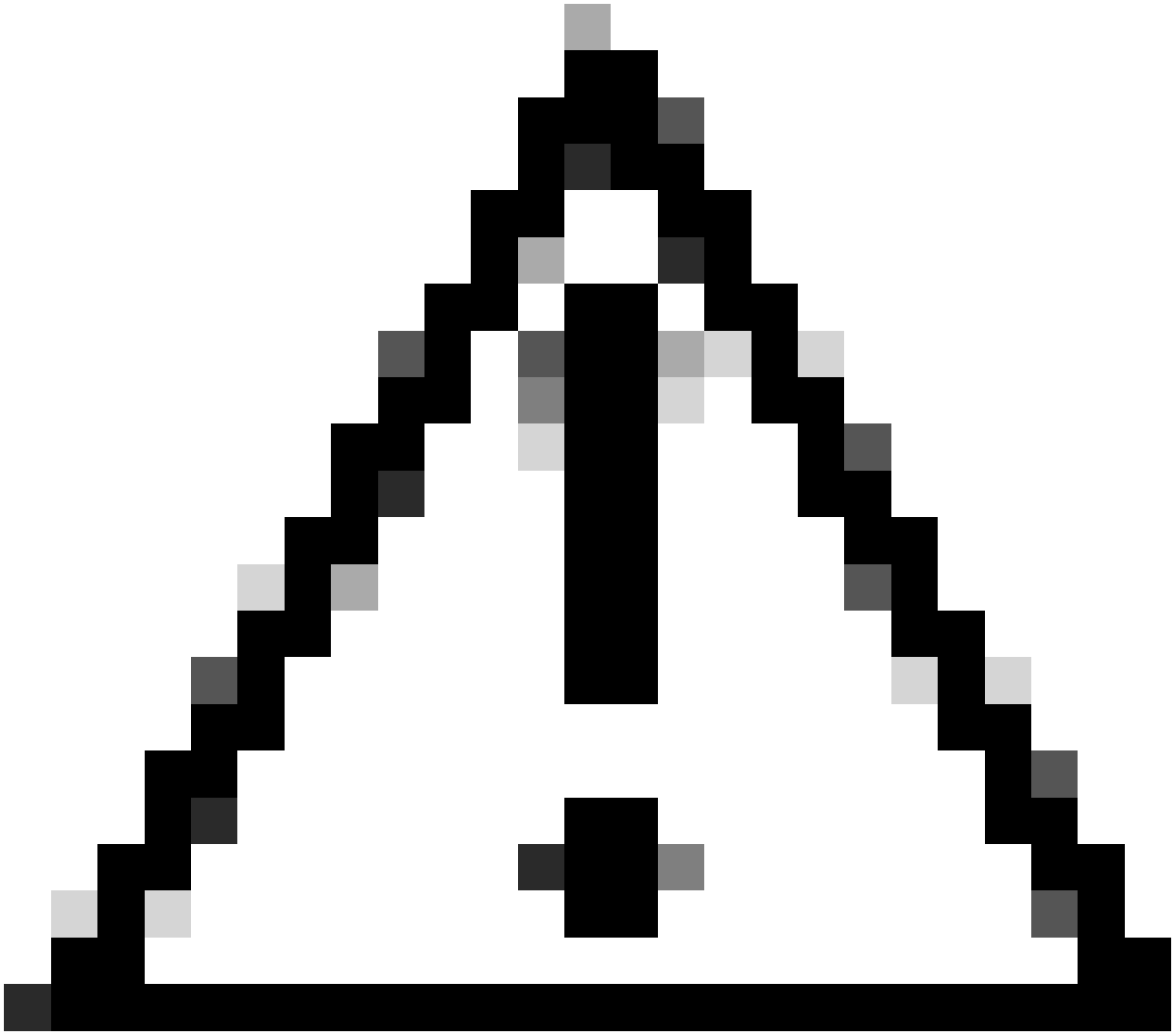
- mac OS AnyConnect:

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

- mac OS 보안 클라이언트:

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

이 작업을 수행한 후 서비스 또는 컴퓨터를 다시 시작합니다.



주의: Windows의 최신 Wireshark 버전에는 Umbrella VPN 인터페이스를 지원하지 않는 NPCAP 캡처 드라이버가 포함되어 있습니다. Windows에서는 rawcap.exe 도구를 대체 도구로 사용해야 할 수도 있습니다.

DNSQuerySniffer - Windows 대체

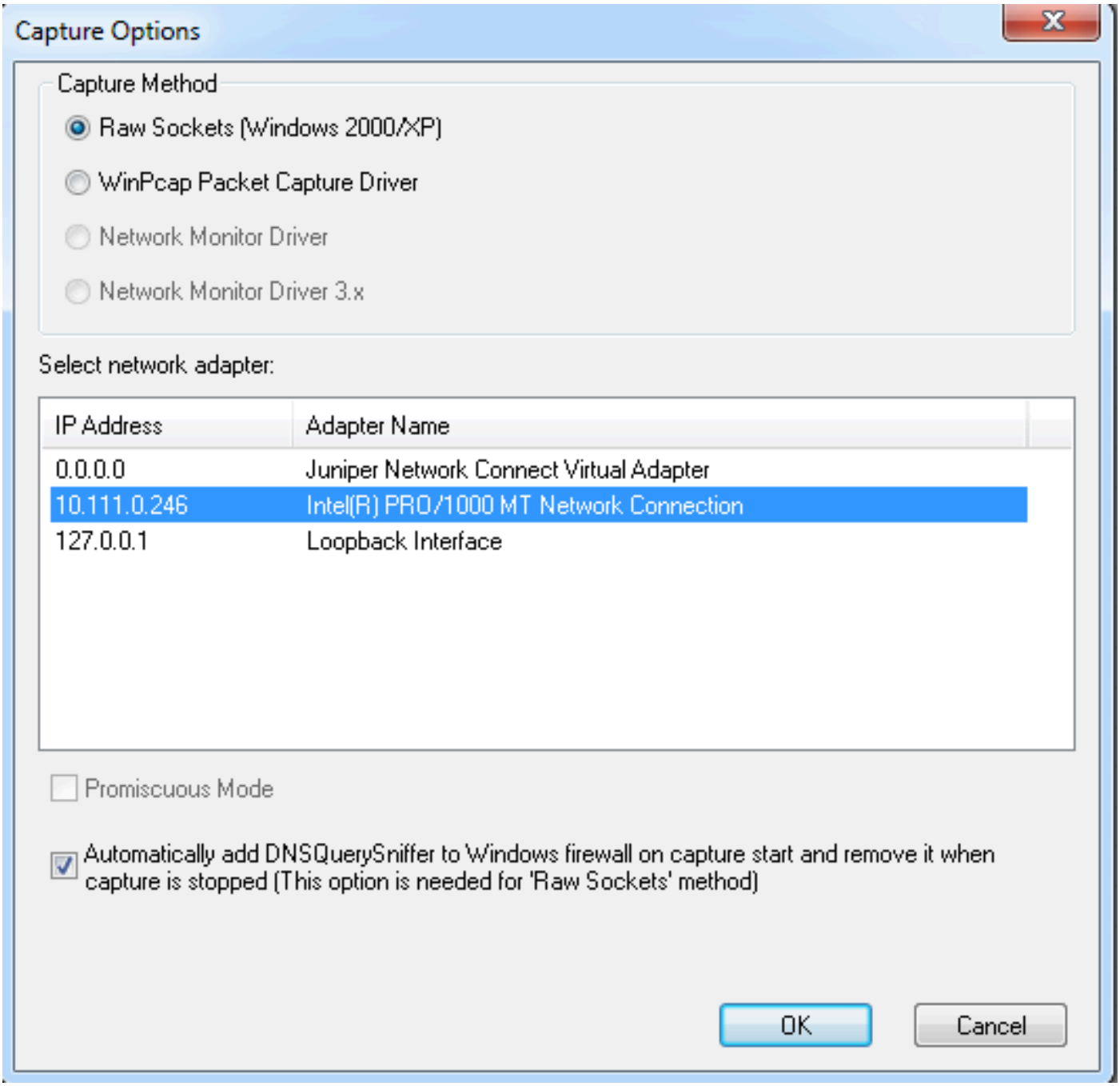
DNSQuery Sniffer는 다량의 유용한 데이터를 모니터링하고 표시하는 Windows용 DNS 전용 네트워크 스니퍼입니다. Wireshark나 Rawcap과 달리 DNS에만 사용되며, 관련 정보를 검토하고 추출하는 것이 훨씬 쉽습니다. 그러나 Wireshark의 강력한 필터링 툴은 없습니다.

이것은 가볍고 사용하기 쉬운 도구입니다. 이 기능을 사용하면 로밍 클라이언트 서비스가 비활성화된 상태에서 패킷을 스니핑하고 캡처를 시작할 수 있으며, 로밍 클라이언트가 이미 시작된 후 캡처를 시작하는 대신 로밍 클라이언트가 시작하는 순간부터 전송하는 모든 DNS 쿼리를 볼 수 있다는 이점이 있습니다.

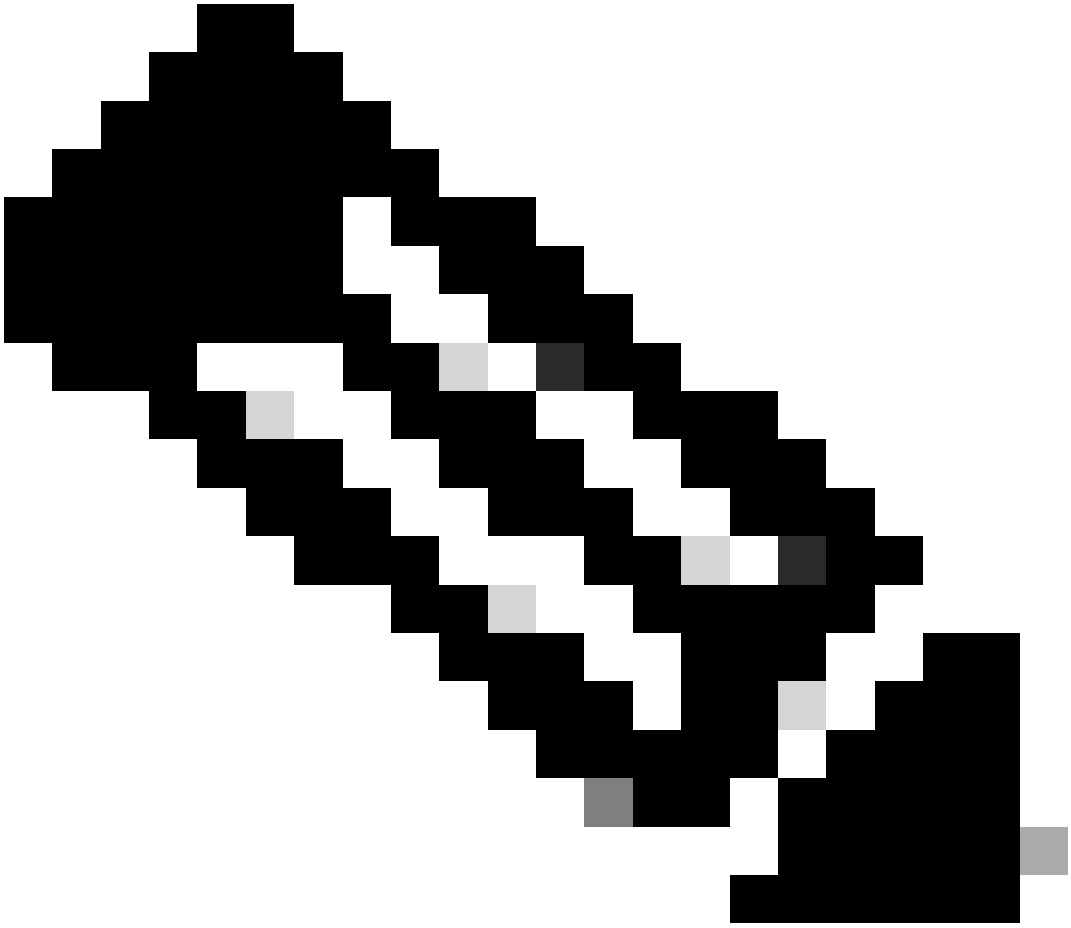
두 가지 캡처 방법이 있습니다.

1. 일반 네트워크 인터페이스를 선택하면 Internal Domains(내부 도메인) 목록에 있거나

dnscryptproxy를 특별히 거치지 않은 쿼리만 볼 수 있습니다.



dns_1.png

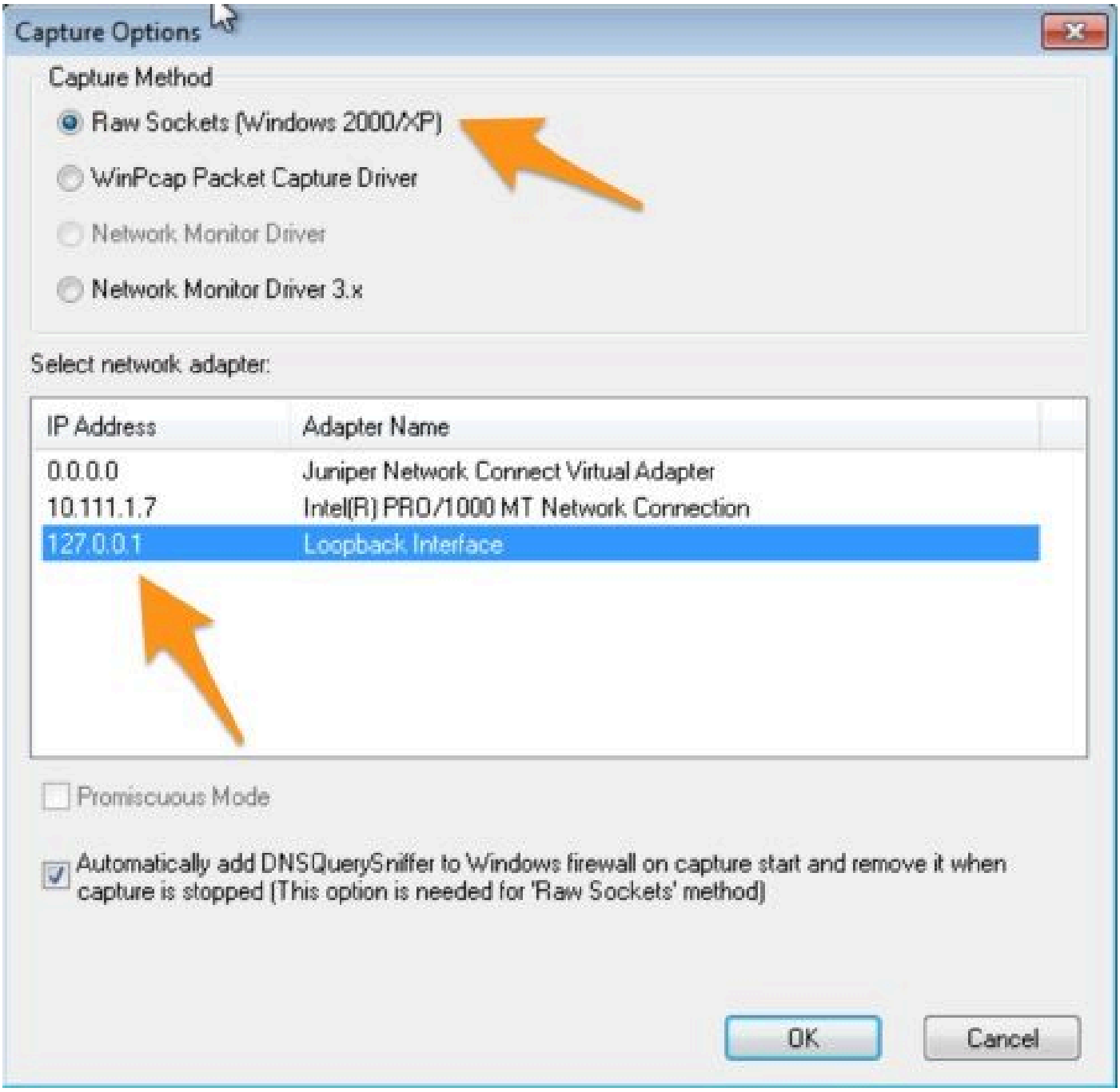


참고: 이 열은 캡처에서 오른쪽에 나타나며 이 열을 보려면 꽤 스크롤해야 합니다.

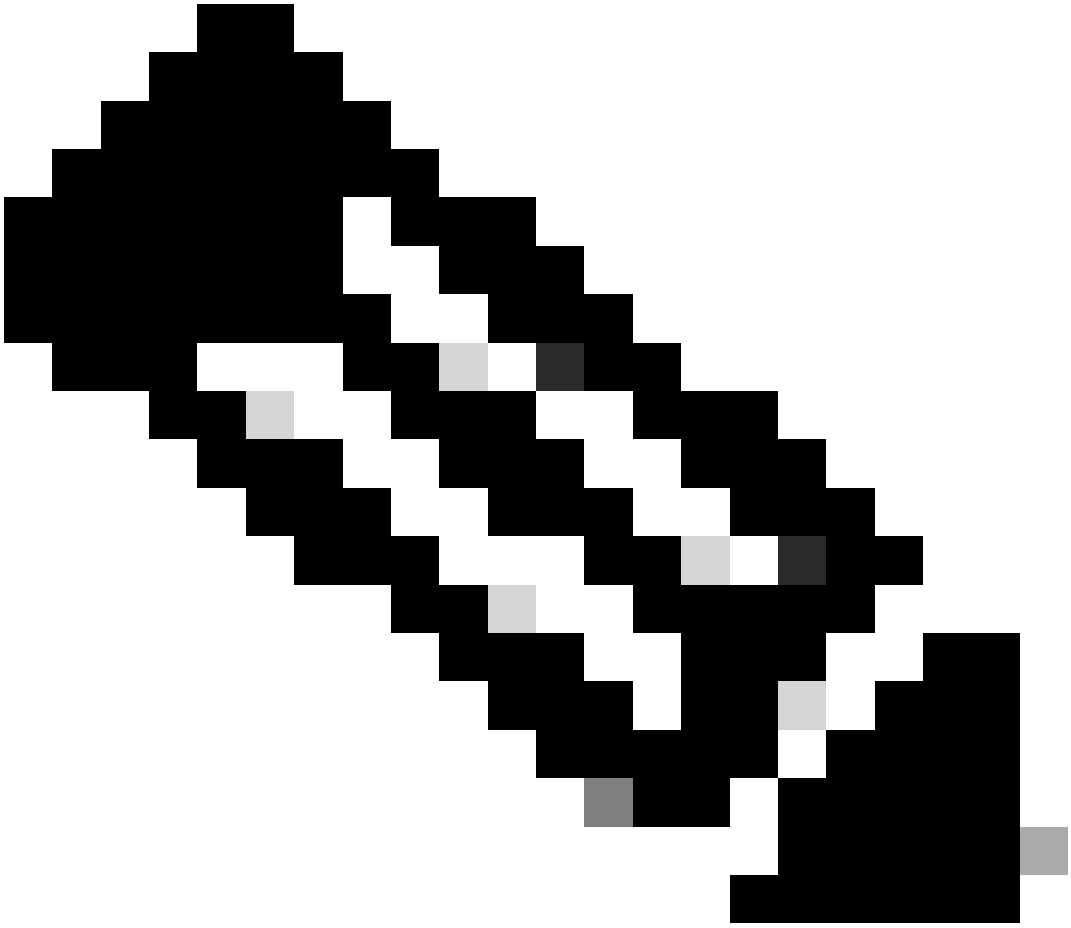
Source Address	Destination Address
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8
10.111.0.246	8.8.8.8

DNSSniffer 열

2. 루프백 인터페이스를 선택하면 dnscryptproxy를 통해 전송되는 모든 DNS 쿼리가 표시되지만, Internal Domains(내부 도메인) 목록에서 도메인의 실제 목적지 IP 주소는 표시되지 않습니다. 그러나 여전히 질의와 응답이 표시됩니다.


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

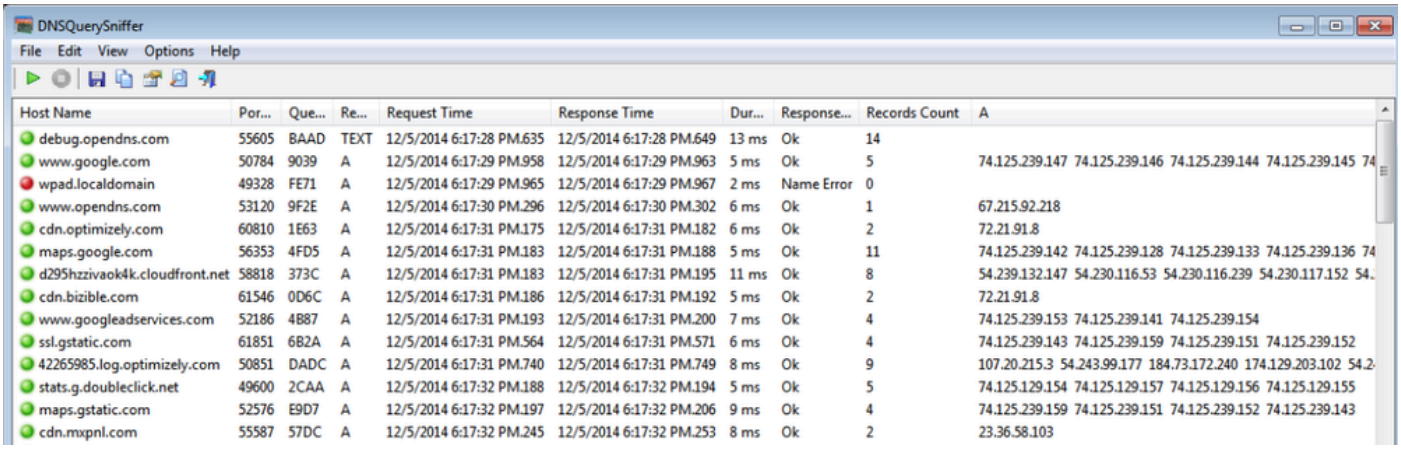


참고: 이 열은 캡처에서 오른쪽에 나타나며, 이 열을 보려면 꽤 많이 스크롤해야 합니다.

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

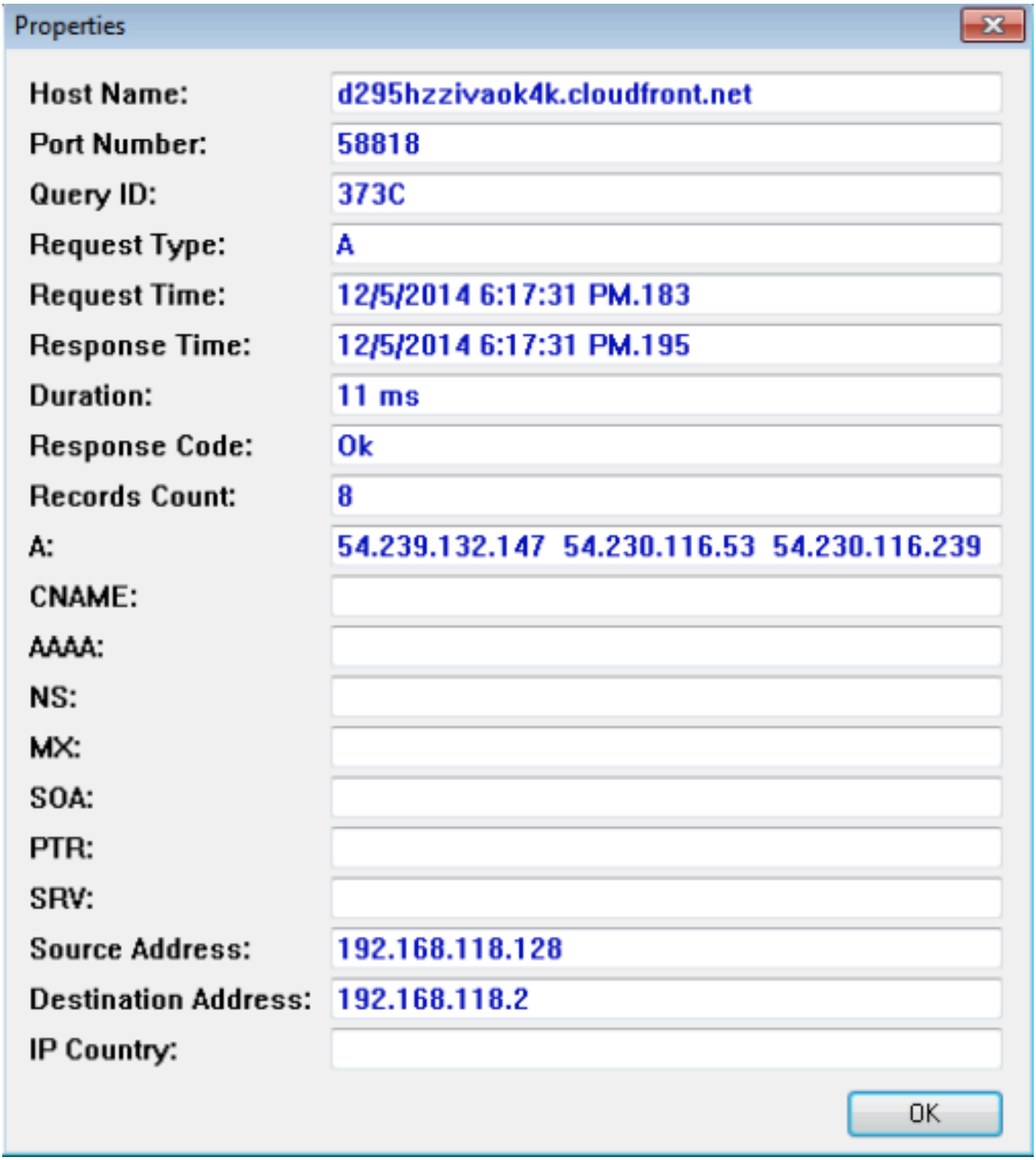
DNSSniffer 열

결과는 다음과 같습니다.



dns_3.png

개별 조회 보기:



dns_4.png

RawCap.exe - Windows 대체

경우에 따라 작업해야 하는 인터페이스는 Wireshark에 포함된 패킷 캡처 드라이버에서 지원되지 않습니다. 이는 루프백 인터페이스에 문제가 될 수 있습니다.

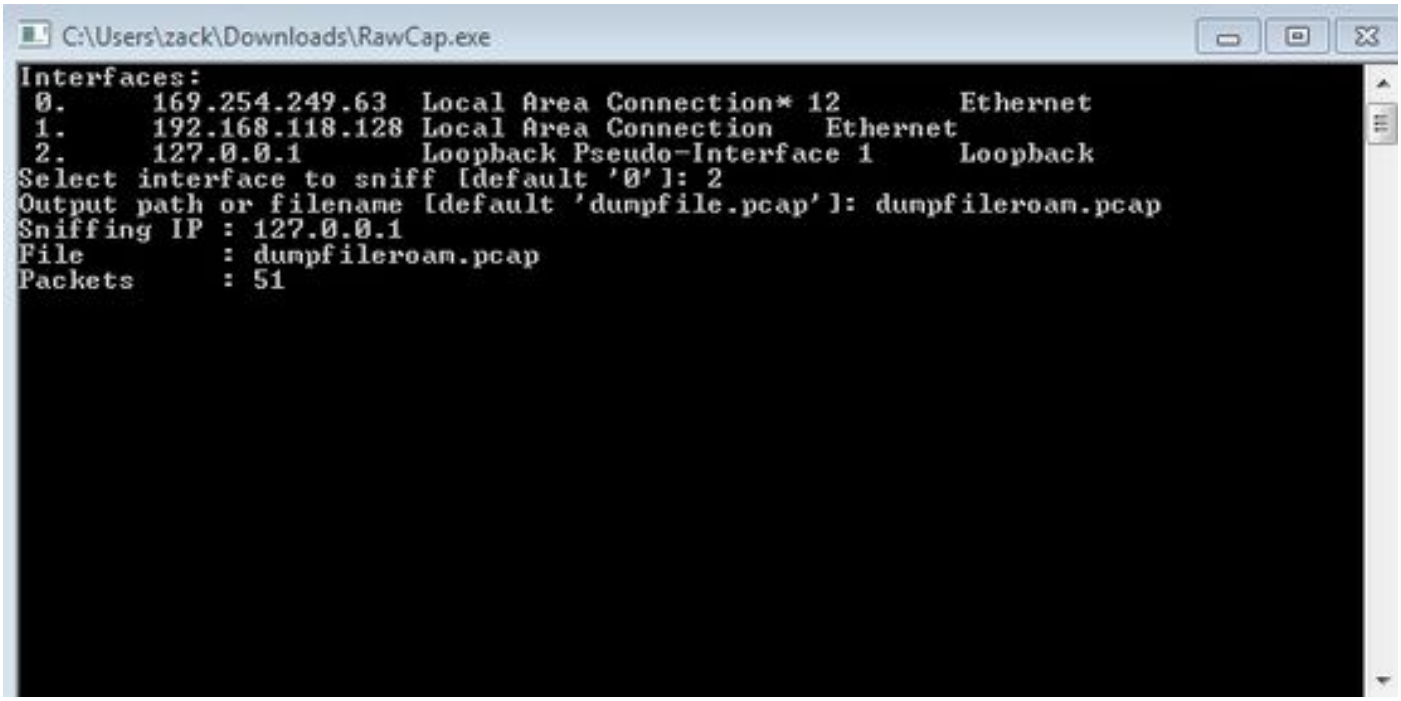
이러한 경우 RawCap.exe를 사용할 수 있습니다.

1. Wireshark를 사용하여 정상 트래픽을 캡처하려면 이 문서의 앞부분에서 설명한 단계를 완료

합니다.

2. 동시에 RawCap.exe를 실행합니다.
3. 해당 목록 번호를 지정하여 인터페이스를 선택합니다.
4. 출력 파일 이름을 지정하고 이 파일을 해제합니다.
5. 캡처를 중지하려면 SelectControl-C를 선택합니다.

저장된 파일은 RawCap.exe를 실행한 폴더에 저장됩니다.



rawcap_1.jpg

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.