

Umbrella Roaming Client에서 패킷 및 DNS 캡처 문제 해결

목차

[소개](#)

[WireShark - Windows와 MacOS는 모두 루프백 캡처를 지원합니다.](#)

[DNSQuerySniffer\(Windows\)](#)

소개

이 문서에서는 아웃바운드 DNS 쿼리를 캡처하는 방법에 대해 설명합니다. Umbrella 로밍 클라이언트에는 현재 생성되는 모든 아웃바운드 DNS 쿼리를 캡처할 수 있는 방법이 없습니다. DNS를 캡처해야 하는 경우 다음 툴 중 하나를 사용할 수 있습니다.

WireShark - Windows와 MacOS는 모두 루프백 캡처를 지원합니다.

Wireshark를 사용하면 로컬 루프백 인터페이스(127.0.0.1)로 전송된 패킷을 캡처할 수 있으므로 암호화 여부에 관계없이 Umbrella 로밍 클라이언트로 전송된 DNS 요청을 확인할 수 있습니다.

특히 로컬 DNS 확인이 중요한 경우 모든 활성 네트워크 인터페이스에서 캡처



DNS만

DNS 요청만 확인하려는 경우

Filter: dns

DNS + HTTP

DNS 및 HTTP 요청만 확인하려는 경우

Filter: dns or http

디버그 조회 필터링(프로브)

debug.opendns.com에서 Probe 관련 문제 또는 문제를 명시적으로 테스트하지 않는 경우 필터 표시줄에 debug.opendns.com을 입력하여 필터링할 수 있습니다.

Filter: dns && not dns contains debug.opendns.com

Wireshark의 기능을 활용하는 방법에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- <http://wiki.wireshark.org/DisplayFilters>

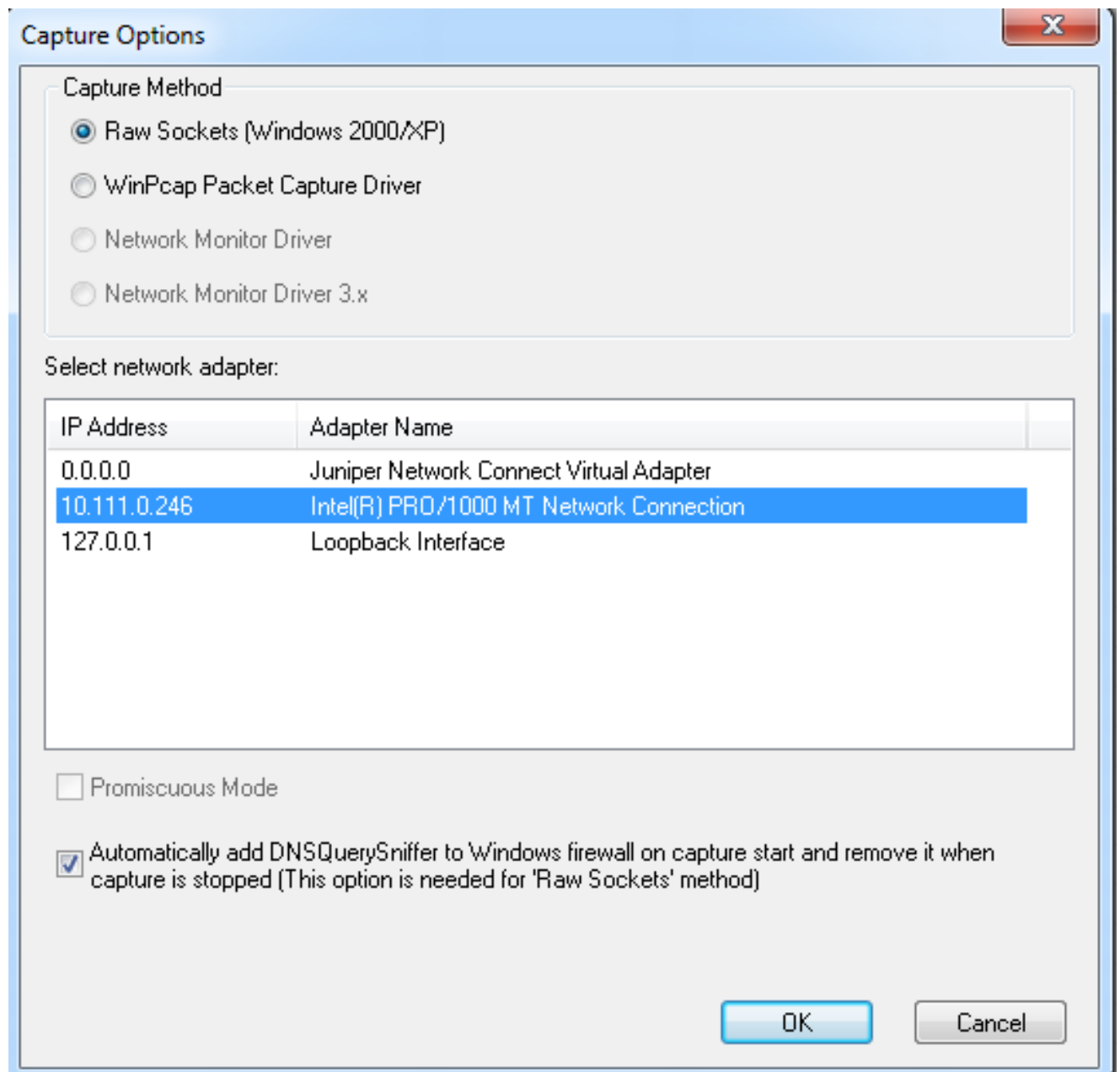
DNSQuerySniffer(Windows)

[DNSQuery Sniffer](#)는 다량의 유용한 데이터를 모니터링하고 표시하는 Windows용 DNS 전용 네트워크 스니퍼입니다. Wireshark나 Rawcap과 달리 DNS에만 사용되며, 관련 정보를 훨씬 쉽게 조사하고 추출할 수 있습니다. 그러나 Wireshark의 강력한 필터링 툴은 없습니다.

이것은 가볍고 사용하기 쉬운 도구입니다. Umbrella 로밍 클라이언트 서비스가 비활성화된 상태에서 패킷을 스니핑하고 캡처를 시작하면 Umbrella 로밍 클라이언트가 이미 시작한 후 캡처를 시작하는 대신 Umbrella 로밍 클라이언트가 전송하는 모든 DNS 쿼리가 갑자기 표시됩니다.

두 가지 캡처 방법이 있습니다.

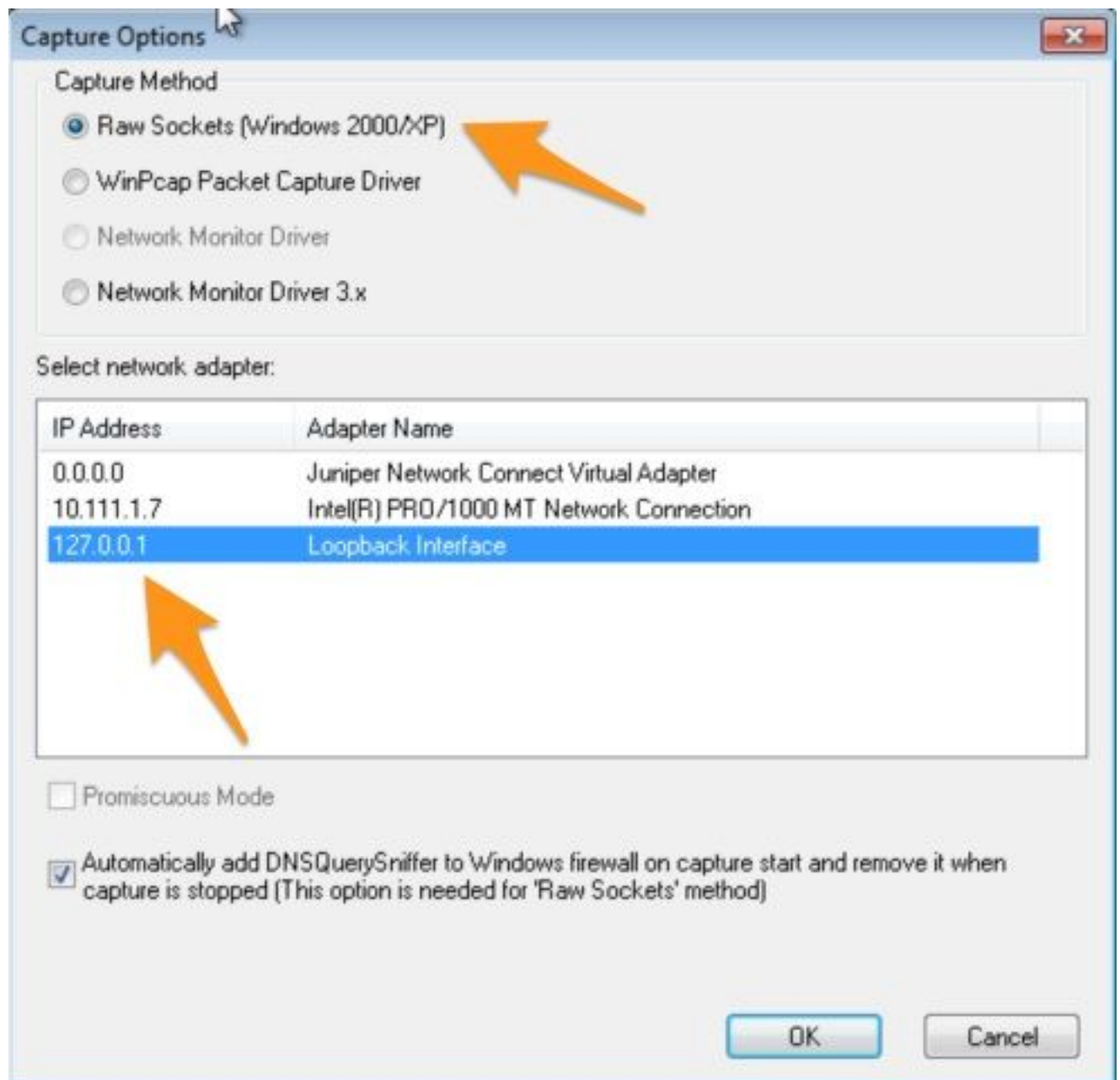
- 메서드 1 - 일반 네트워크 인터페이스를 선택하면 Internal Domains(내부 도메인) 목록에 있거나 dnscryptproxy를 특별히 거치지 않은 쿼리만 표시됩니다.



이 열은 캡처의 맨 오른쪽에 나타나며 상당히 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
10.111.0.246	8.8.8.8

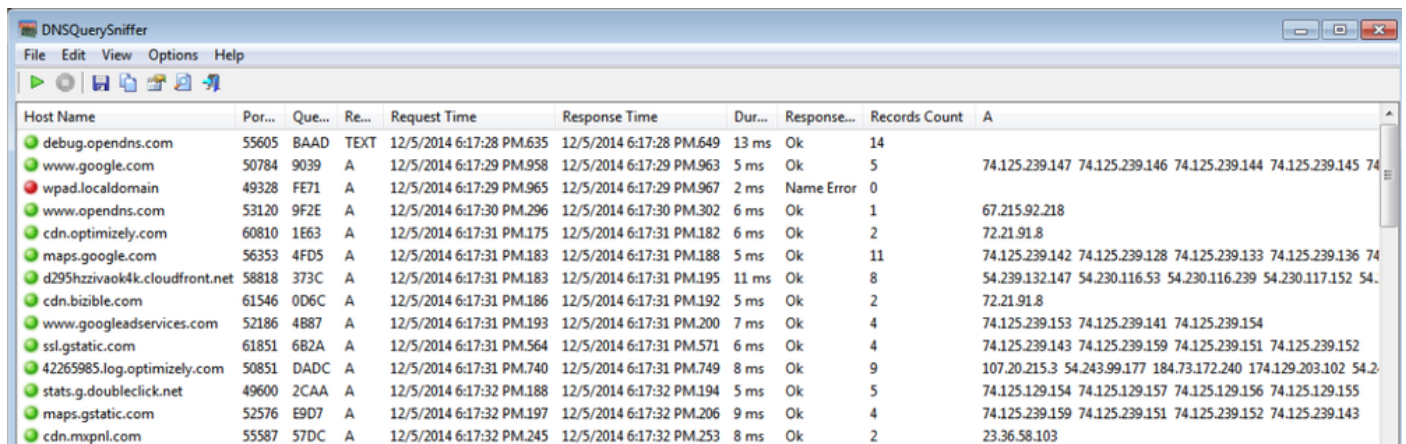
- 메서드 2 - 루프백 인터페이스를 선택하면 dnscryptproxy를 통해 전송되는 모든 DNS 쿼리가 표시되지만 내부 도메인 목록에 있는 도메인의 실제 대상 IP 주소는 표시되지 않습니다. 그러나 질의와 답변이 표시됩니다.



이 열은 캡처의 맨 오른쪽에 나타나며 상당히 스크롤해야 합니다.

Source Address	Destination Address
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1
127.0.0.1	127.0.0.1

결과는 다음과 같습니다.



Host Name	Port	Queue	Request	Response	Duration	Response	Records Count	A
debug.opendns.com	55605	BAAD	TEXT	12/5/2014 6:17:28 PM.635	12/5/2014 6:17:28 PM.649	13 ms	Ok	14
www.google.com	50784	9039	A	12/5/2014 6:17:29 PM.958	12/5/2014 6:17:29 PM.963	5 ms	Ok	5
wpad.localdomain	49328	FE71	A	12/5/2014 6:17:29 PM.965	12/5/2014 6:17:29 PM.967	2 ms	Name Error	0
www.opendns.com	53120	9F2E	A	12/5/2014 6:17:30 PM.296	12/5/2014 6:17:30 PM.302	6 ms	Ok	1
cdn.optimizely.com	60810	1E63	A	12/5/2014 6:17:31 PM.175	12/5/2014 6:17:31 PM.182	6 ms	Ok	2
maps.google.com	56353	4FD5	A	12/5/2014 6:17:31 PM.183	12/5/2014 6:17:31 PM.188	5 ms	Ok	11
d295hzzivaok4k.cloudfront.net	58818	373C	A	12/5/2014 6:17:31 PM.183	12/5/2014 6:17:31 PM.195	11 ms	Ok	8
cdn.bizible.com	61546	0D6C	A	12/5/2014 6:17:31 PM.186	12/5/2014 6:17:31 PM.192	5 ms	Ok	2
www.googleadservices.com	52186	4887	A	12/5/2014 6:17:31 PM.193	12/5/2014 6:17:31 PM.200	7 ms	Ok	4
ssl.gstatic.com	61851	6B2A	A	12/5/2014 6:17:31 PM.564	12/5/2014 6:17:31 PM.571	6 ms	Ok	4
42265985.log.optimizely.com	50851	DADC	A	12/5/2014 6:17:31 PM.740	12/5/2014 6:17:31 PM.749	8 ms	Ok	9
stats.g.doubleclick.net	49600	2CAA	A	12/5/2014 6:17:32 PM.188	12/5/2014 6:17:32 PM.194	5 ms	Ok	5
maps.gstatic.com	52576	E9D7	A	12/5/2014 6:17:32 PM.197	12/5/2014 6:17:32 PM.206	9 ms	Ok	4
cdn.mxpnl.com	55587	57DC	A	12/5/2014 6:17:32 PM.245	12/5/2014 6:17:32 PM.253	8 ms	Ok	2

개별 조회 보기:

Properties



Host Name:	d295hzzivaok4k.cloudfront.net
Port Number:	58818
Query ID:	373C
Request Type:	A
Request Time:	12/5/2014 6:17:31 PM.183
Response Time:	12/5/2014 6:17:31 PM.195
Duration:	11 ms
Response Code:	Ok
Records Count:	8
A:	54.239.132.147 54.230.116.53 54.230.116.239
CNAME:	
AAAA:	
NS:	
MX:	
SOA:	
PTR:	
SRV:	
Source Address:	192.168.118.128
Destination Address:	192.168.118.2
IP Country:	

OK

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.