Risoluzione dei problemi relativi alle acquisizioni di pacchetti e DNS nel client di roaming Umbrella

Sommario

Introduzione

In questo documento viene descritto come acquisire le query DNS in uscita. Il client di roaming Umbrella non dispone attualmente di un metodo per l'acquisizione di tutte le query DNS in uscita eseguite. Se è necessario acquisire il DNS, è possibile utilizzare uno di questi strumenti.

WireShark - Windows e MacOS supportano entrambi l'acquisizione del loopback

Wireshark consente di acquisire pacchetti inviati all'interfaccia di loopback locale (127.0.0.1), quindi di visualizzare le richieste DNS inviate al client di roaming Umbrella sia crittografate che non crittografate.

Acquisisci su tutte le interfacce di rete attive, in particolare quando la risoluzione DNS locale è un fattore

Solo DNS

Se si desidera esaminare solo le richieste DNS.

DNS + HTTP

Se si desidera esaminare solo le richieste DNS e HTTP.

Escludi ricerche di debug (probe)

Se non si sta verificando in modo esplicito la presenza di problemi relativi ai probe con debug.opendns.com, è possibile filtrare debug.opendns.com digitando quanto segue nella barra dei filtri:

Per ulteriori informazioni su come sfruttare le potenzialità di Wireshark, vedere le risorse seguenti:

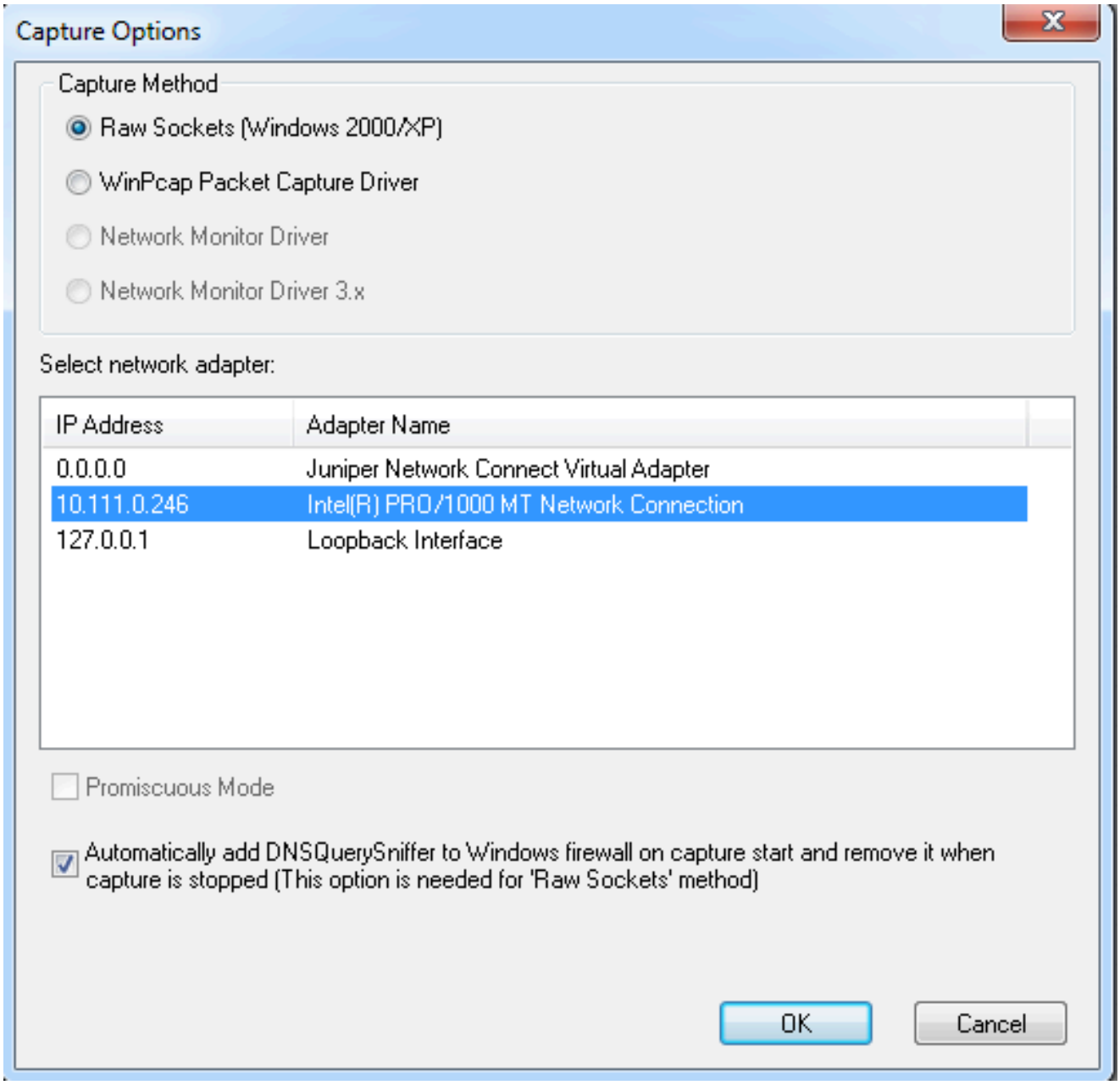
- http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- http://wiki.wireshark.org/DisplayFilters

DNSQuerySniffer (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. Un enorme vantaggio nell'utilizzo di questo è che è possibile sniffare i pacchetti mentre il servizio client di roaming Umbrella è disabilitato, avviare l'acquisizione e improvvisamente si vede ogni query DNS che il client di roaming Umbrella invia dal momento in cui si avvia, piuttosto che avviare un'acquisizione dopo che il client di roaming Umbrella è già stato avviato.

Esistono due metodi di acquisizione:

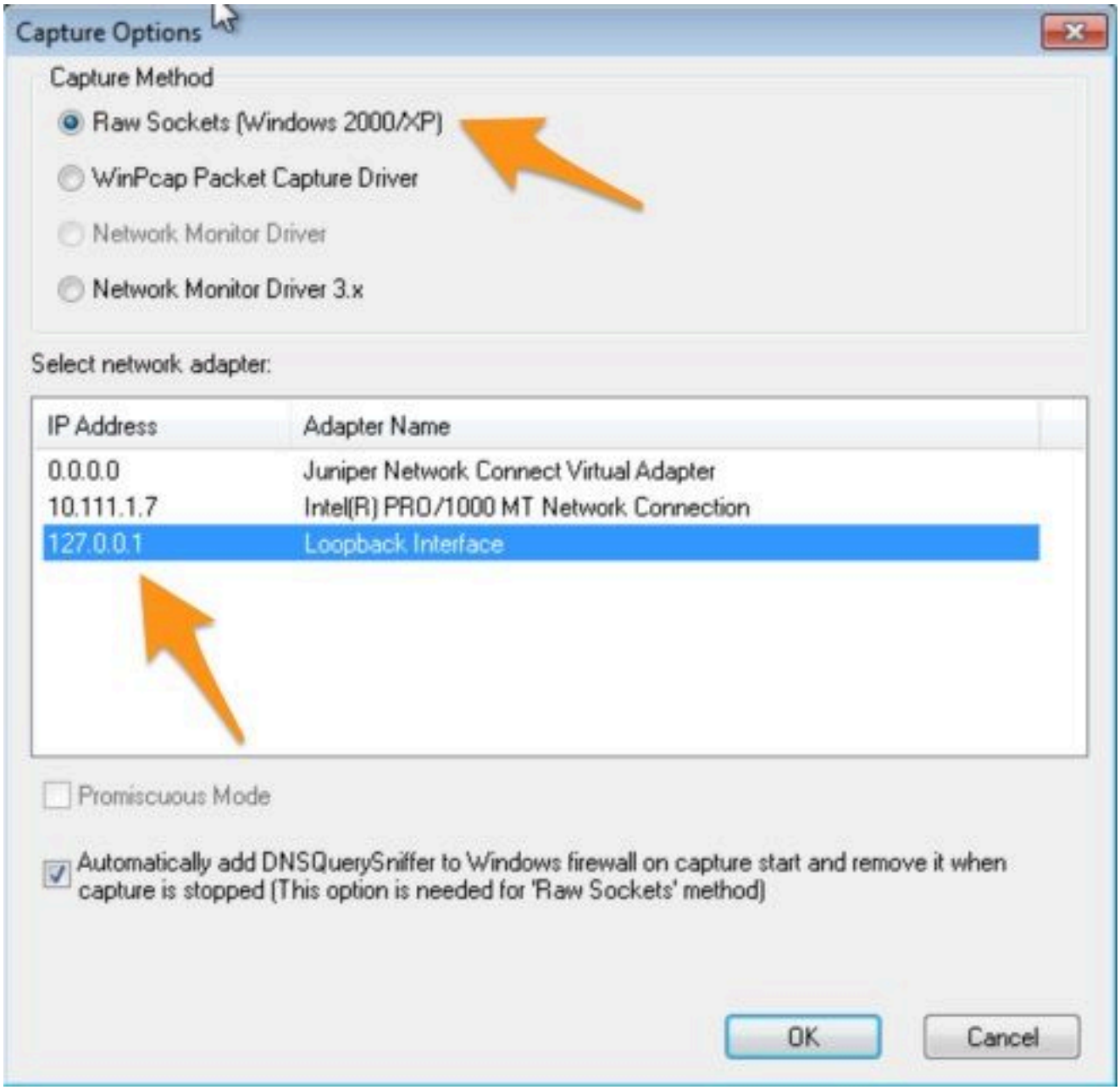
- Metodo 1 (Method One) - Se selezionate l'interfaccia di rete normale, vengono visualizzate solo le query presenti nell'elenco Domini interni (Internal Domains) o che non sono state specificamente sottoposte al comando dnscryptproxy.



Queste colonne sono visualizzate all'estrema destra nella cattura e dovete scorrere su un po'.

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

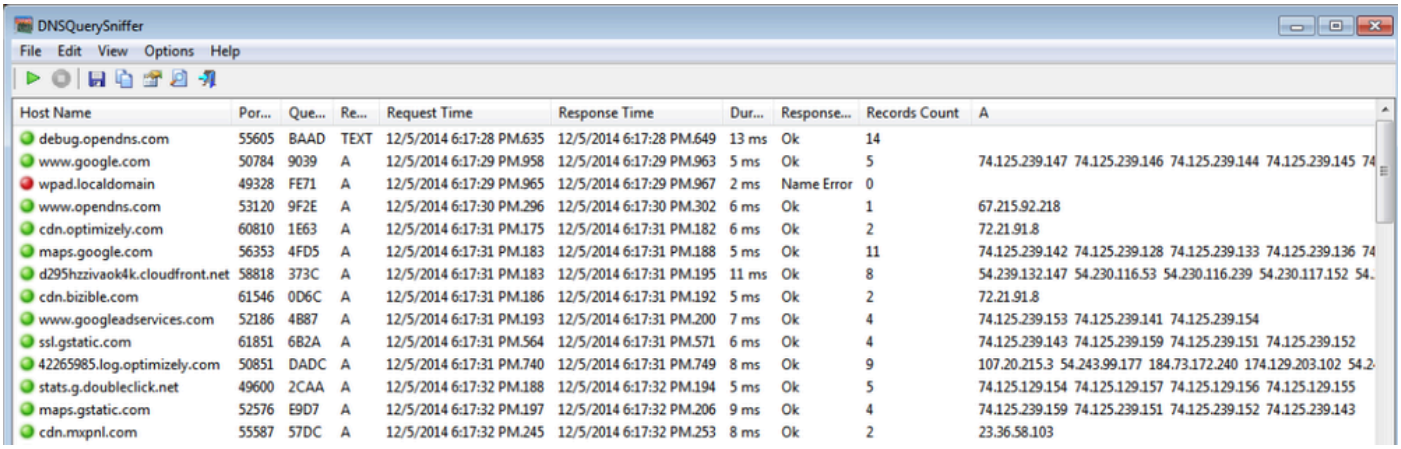
- Metodo 2: se si seleziona l'interfaccia di loopback, vengono visualizzate tutte le query DNS inviate tramite dnscryptproxy, ma non l'indirizzo IP di destinazione effettivo per i domini inclusi nell'elenco dei domini interni. verranno tuttavia visualizzate la query e la risposta.



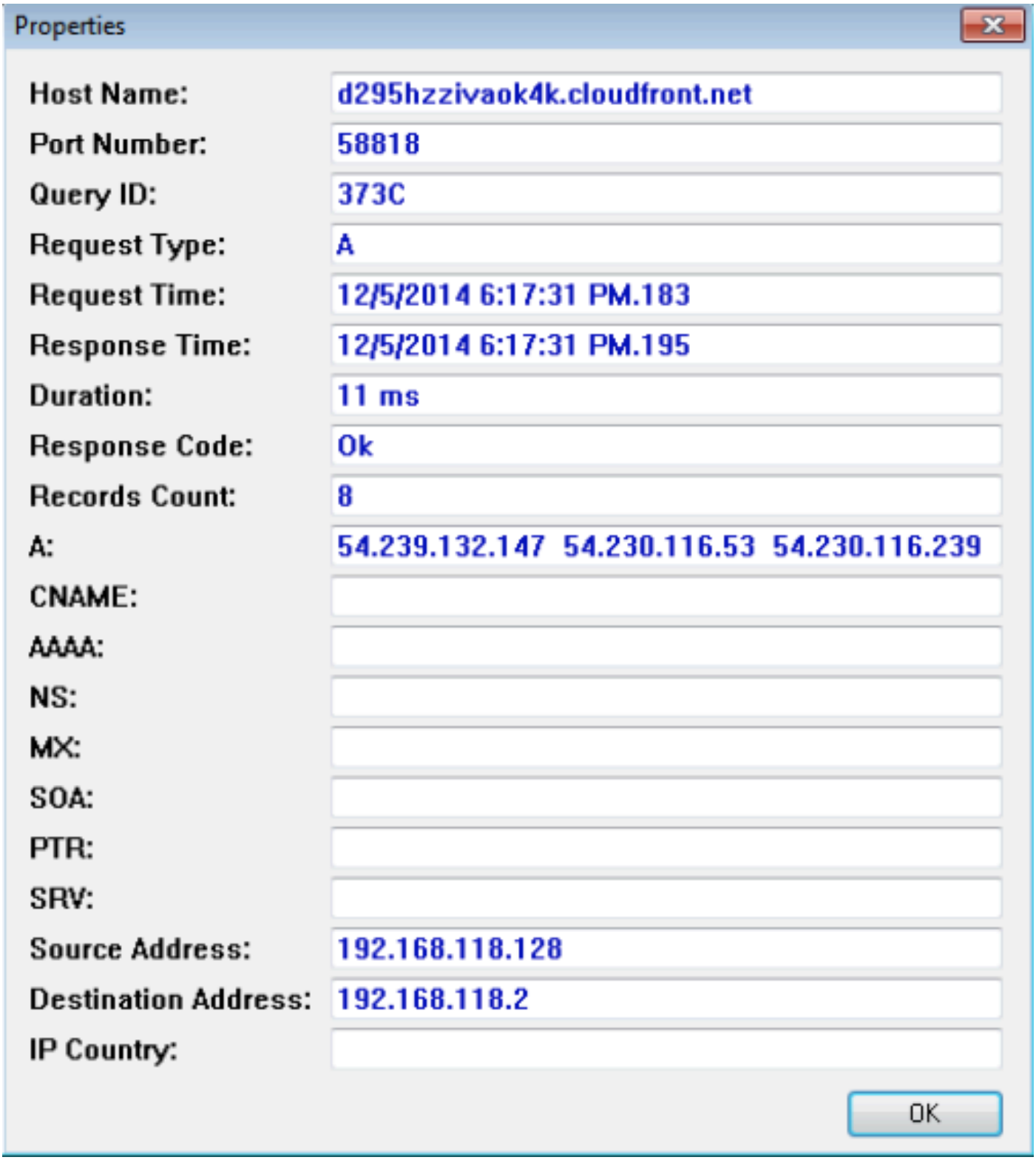
Queste colonne sono visualizzate all'estrema destra nella cattura e dovete scorrere su un po'.

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

I risultati saranno simili a quelli riportati di seguito:



Visualizzazione di una singola ricerca:


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

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).