

مادختساب ةكبشال رورم ةكرح طاقنال Wireshark

تاوتحمل

[ةمدقملا](#)

[ةيساسالابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةماع قرطن](#)

[Wireshark تاميلعت](#)

[تاريضحت](#)

[شالفلل قارواليساسأرسأ](#)

[ةيفاضا تاوطخ - لوحتملا لي عمل](#)

[عاجرتسال رورم ةكرح](#)

[ةرفشملا DNS رورم ةكرح](#)

[DNSQuerySniffer - Windows Alternative](#)

[RawCap.exe - Windows Alternative](#)

ةمدقملا

Wireshark. مادختساب ةكبشال رورم ةكرح طاقنال ةيفيك دنتسملا اذه حضوي

ةيساسالابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال

ةمدختسملا تانوكملا

DNS Umbrella. ةقبط نامأ ىلإ دنتسملا اذه يف ةدراول تامولعمل دنتست

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عيمج تأدب رما يال لم تحملا ريثأتلل كمهف نم دكأتف ،ليغشتال ديق كتكبش

ةماع قرطن

تنرتنإل رورم ةكرح نم ةمزح طاقنال Cisco Umbrella معد وفظوم اهيف بلطي تاقوا كانه رورملا ةكرح لي لحتل Umbrella معد طاقنالال حيتي .ةكبشالاورتوي بمكلال ني ب ةقف دتملا .ةلم تحملا لكاشملا دي دحتو صفخنم يوتسم يف

لمعال ويرانيس حضوت مزحل تاطقل نم نيت عومجم ةنراقم ديفملا نم ،تالاحل مظعم يف ءاوس دح ىلع لمعال ريغو

- عاشناب مق .عقي رادصلال امنيب steps اذه تمت أو ةلكشملا تترك عيطتسي تنأ تنمض ةقطنملا عم تقولواوخي راتلا ةطحالم عاجرلا .حل اص ريغ ويرانيس حضوي ةمزح طاقتللا ىرخأ تانايبب تامولعملل هذه طبر نكمي ثيحب ةينمزللا
- (Umbrella ل DNS هيجوت ةداعإ أو/و) Umbrella جم انرب عم تاميلعتلا هذه ررك ،نكمأ نإ تقولواوخي راتلا ةطحالم عاجرلا .لمعال ويرانيس حضوي ةمزح طاقتللا عاشناب مق .لطم ىرخأ تانايبب تامولعملل هذه طبر نكمي ثيحب ةينمزللا ةقطنملا عم

Wireshark تاميلعت

تاريضحت

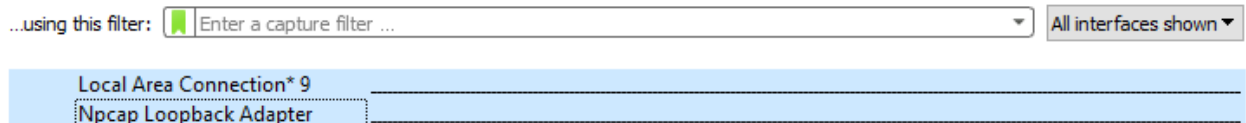
1. Wireshark لي زنت .
2. ةرورض ريغ ةكبش تالاصتإ ةيأ لاصتا عطق .
 1. ةلكشملا راركتل ةبولطم نكت مل ام VPN تالاصتإ لصفأ .
 2. اعم امهيك سيلولو كلساللا وأ كلساللا ليصوتلا ال مدختست ال .
3. ةلكشملا راركتل بولطم ريغ رخآ جم انرب يأ قالغب مق .
4. ضرعتسملا نم تقوؤملا نيزختلا ةركاذو طابترالا فيرعت تافلحسمب مق .
5. رملال مادختساب Windows ىلع DNS ل تقوؤملا نيزختلا ةركاذو حسم :

```
ipconfig /flushdns
```

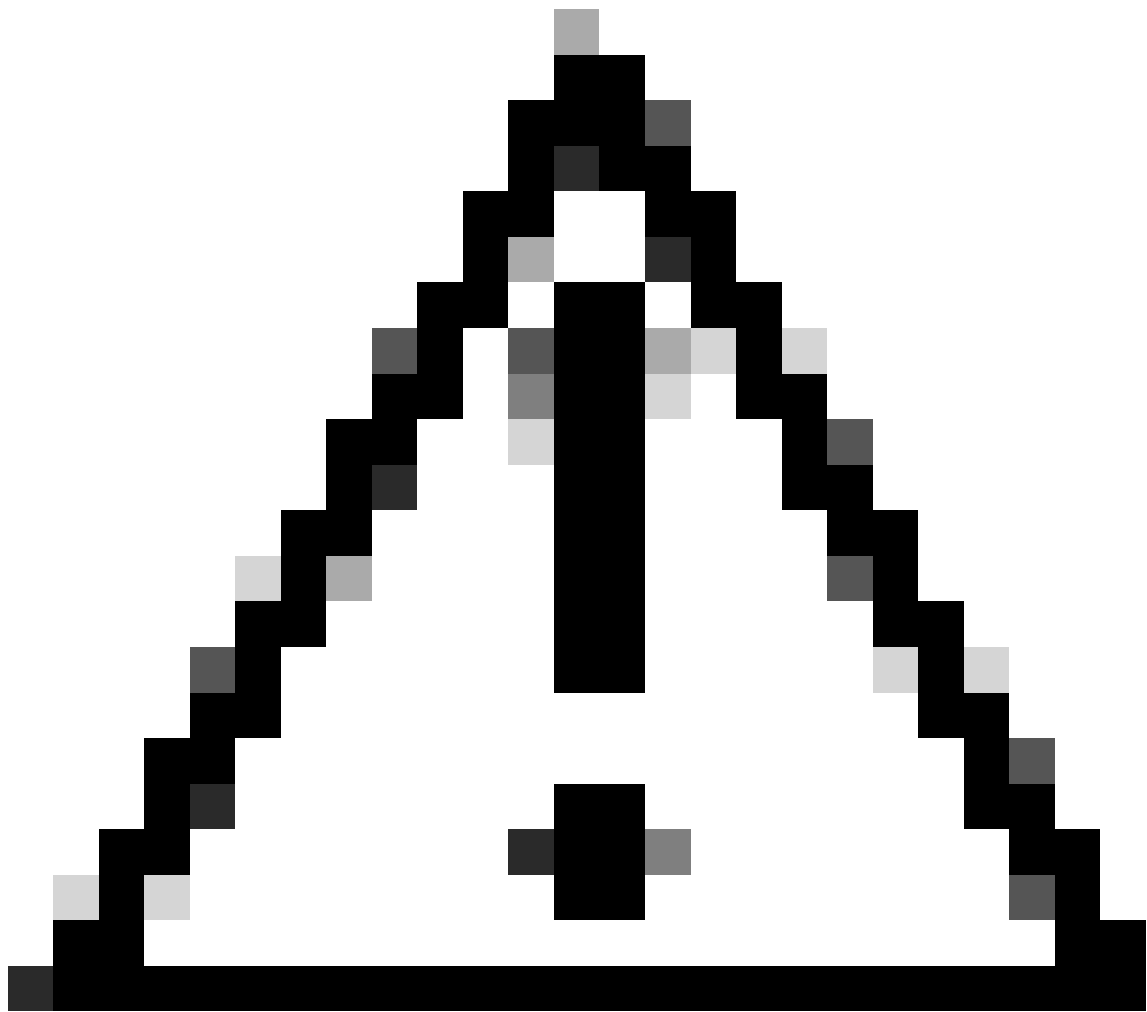
شالفلل قاروال يساسأ رسأ

1. Wireshark قالطإ .
2. تاهجاو ديدحت نكمي .ةلصللا تاذ تاهجاوالا ددح .ةكبشلل تاهجاو طاقتللا ةحول ضرعت .ديدحتلا ءانثأ (Mac في) CMD حاتفم وأ (Windows في) CTRL حاتفم مادختساب ةددعت

Capture

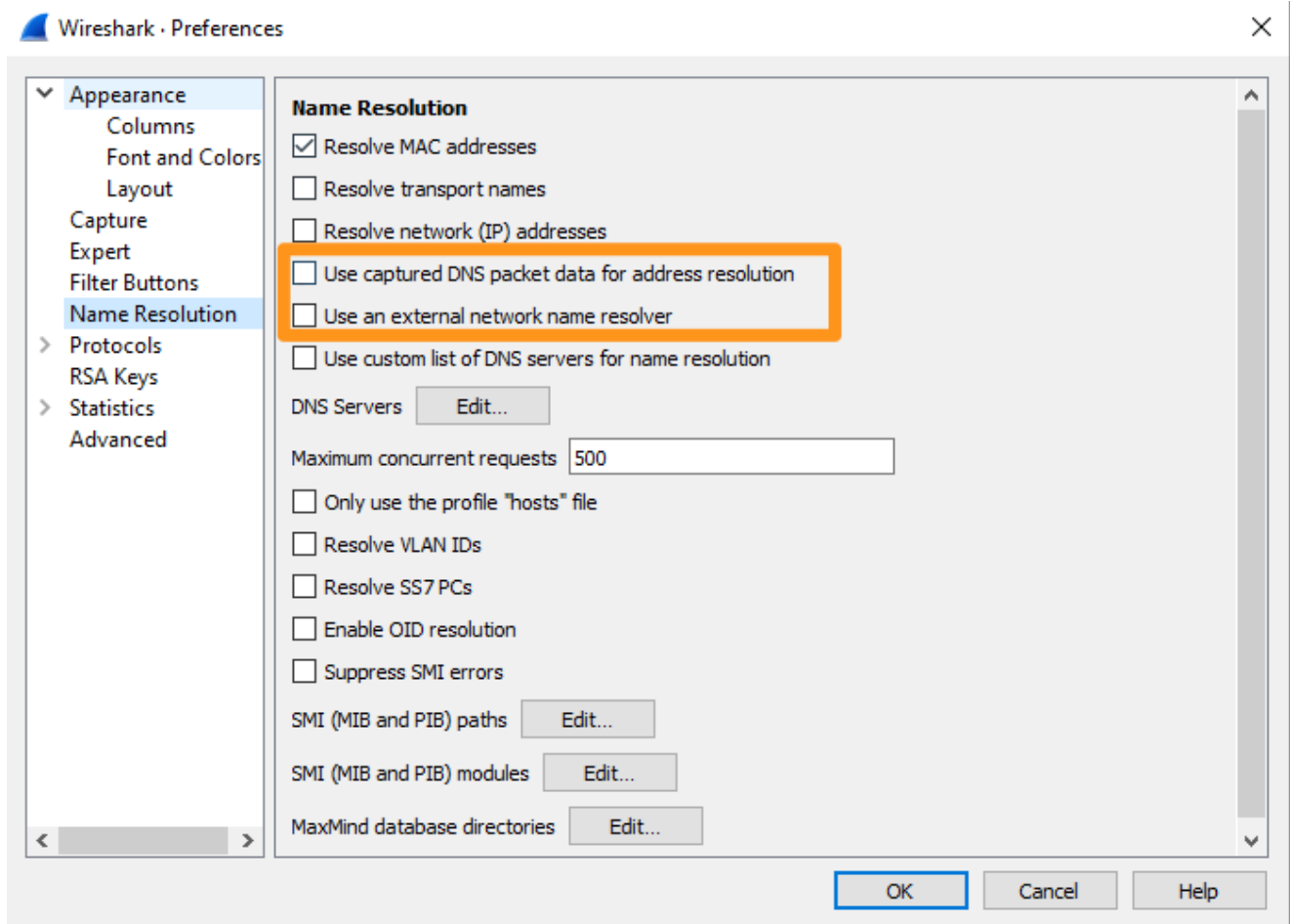


wireshark_1.png



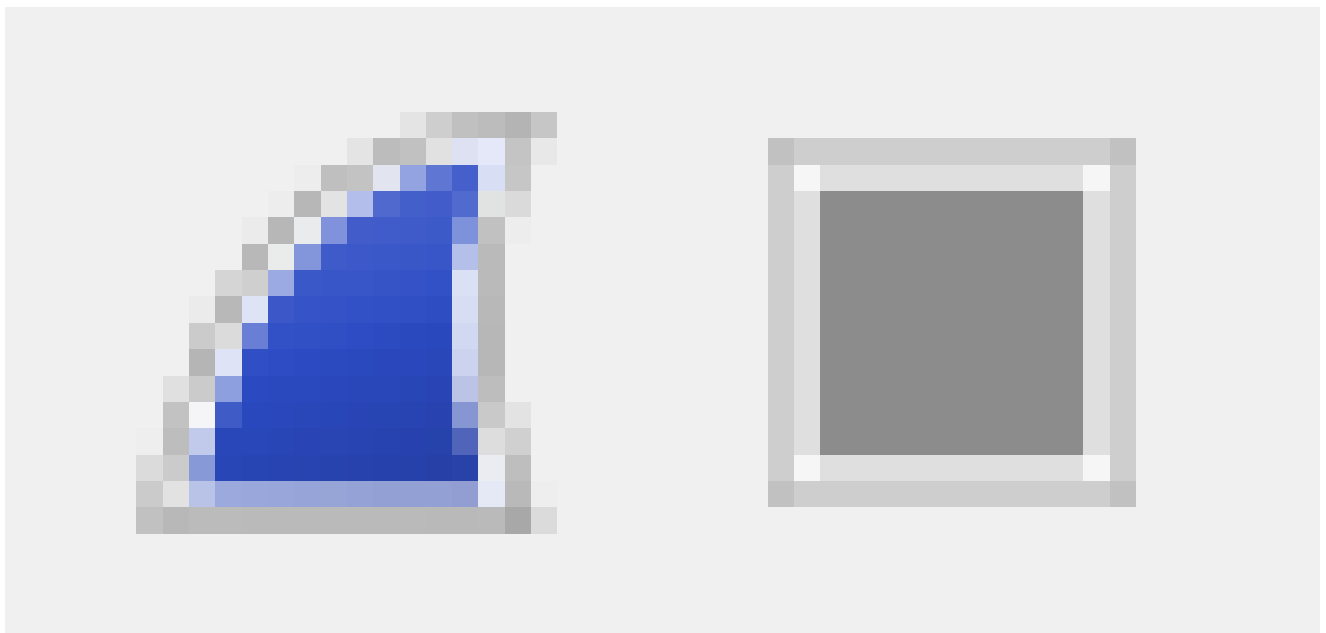
رورم ةكرح ىل ع يوتحت يتل ةححصلا (تاهاولا) ةهاولا ديدحت مهمل نم :ريذحت
ضرعل (Mac في) ifconfig رمالا وأ (Windows في) "ipconfig" رمالا مدختسا . ةكبشلا
لوچتملا ليمعلا مديختسم ىل ع بجي . ةكبشلا تاهاولا لوح ليصافتلا نم ديزم
تنك اذا . Lo0 تاهاولا :يفاضا لكشب عاجرتسالا وأ NPCAP عاجرتسا ئيها مديذحت
تاهاولا عيجم ددحف ، كش في

-
3. مسال لحم مادختسا وناونعلا ةقذل ةطقتلملا DNS ةمزح تانايب مادختسا نأ نم دكأت .
لكلذل نأل DNS تامالعتسا عارجاب موقيا ال Wireshark نأ نامضل ددحم ريغ يجرأ ةكبش
Wireshark نم اربا عا ةحلاص تادادعلا . AnyConnect ىل ع رثؤو طاقتلالا دقعيا نأ نكمي
3.4.9:



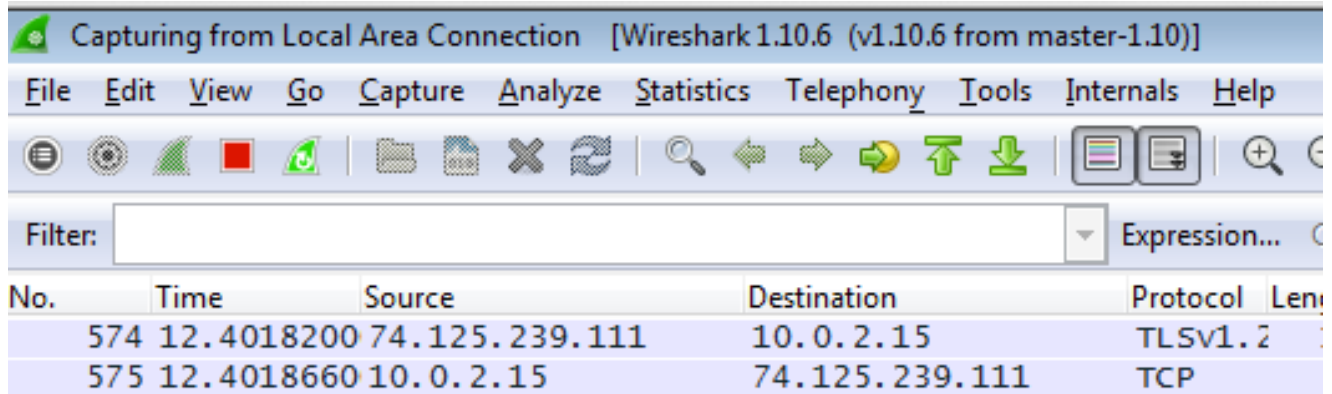
capture_png.png

4. عاقرز ةيادب ةنوقيأ ددح وأ ادب > طاقا لا ددح .



wireshark_2.png

5. ةلاشم لا ررك ،ةيفللخال في Wireshark لمعي امنيب .



No.	Time	Source	Destination	Protocol	Length
574	12.4018200	74.125.239.111	10.0.2.15	TLSv1.2	
575	12.4018660	10.0.2.15	74.125.239.111	TCP	

wireshark_3.png

6. مدخستسأ وأ فاقبي > طاقثلا ددح، لمكالب الثامتم اخسن ةلأسملا خسن متي نأ درجمب 6. رملأا فقوقثلا ةنوقيأ.
7. عونك فلملا ظفح نم دكأت. فلملا ظفحل اناكم ددحو مساب ظفح > فلم ىلإ لقتنا 7. ةعجارملل Cisco Umbrella معد ىلإ ظوفحمل فلملا لاسرا نكمي PCAPNG.

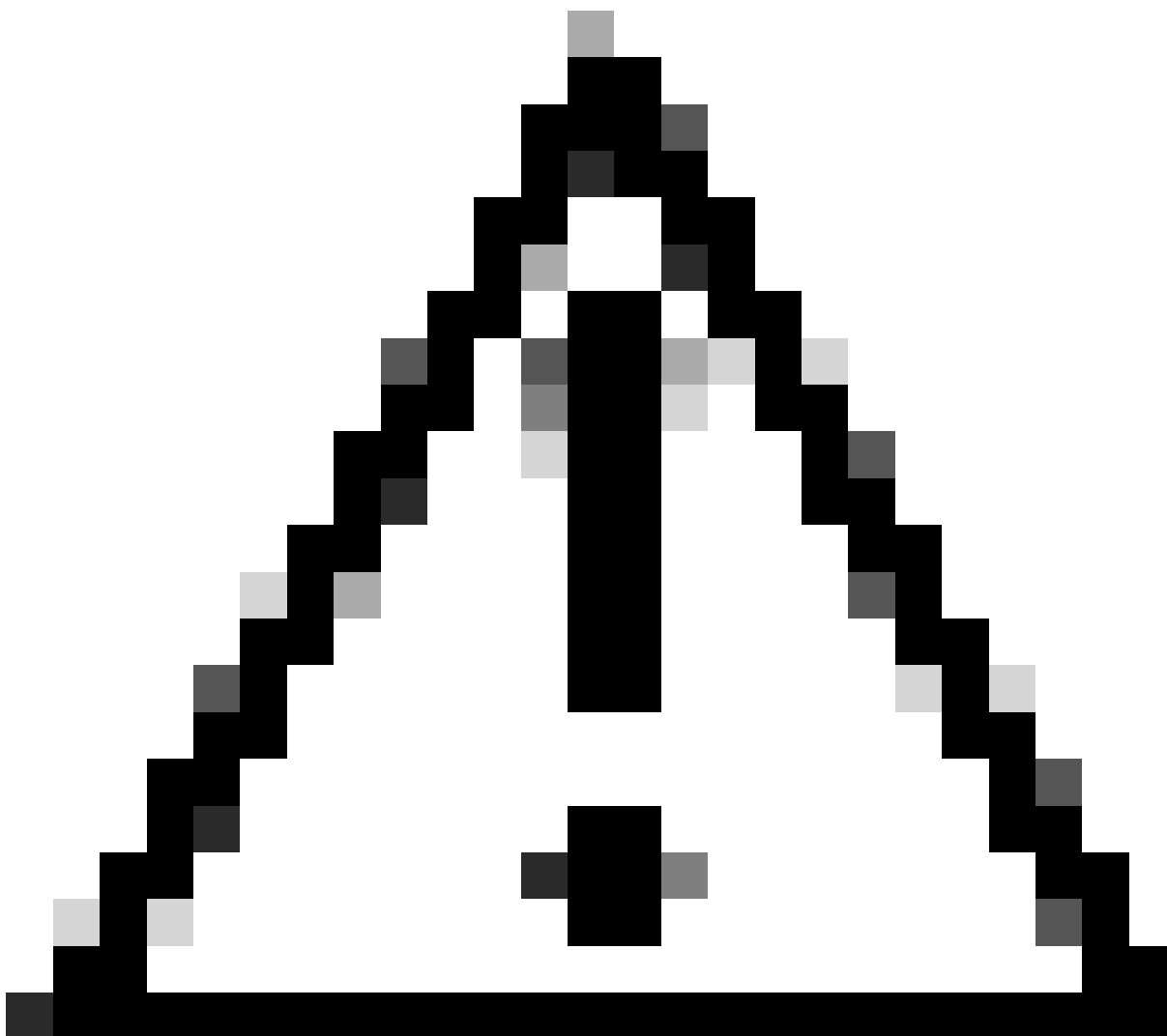
ةيفاضا تاوطخ - لوجتملا ليمعلا

ي مدخستسمو نيلقتسملا لوجتملا ءالمع نم لكل اهلماك بجي ةيفاضا تاوطخ كانه
 ةلوجتملا ةيطمننلا تادحول AnyConnect:

عاجرتسال رورم ةكرح

(127.0.0.1) عاجرتسال ةهجاو ىلع تانايبلا رورم ةكرح طاقثلا اضيأ بجي، ةهجاو ديدحت دنع
 ءاغصالب لوجتملا ليمعالب صاخلا DNS ليكو موقي. ىرخألا ةكبشلا تاهجاو ىلإ ةفاضالب
 ليمعلاو ليغشتلا ماظن نيب تانايبلا رورم ةكرح ىرت نأ مهمل نم فك لذل، ةهجاو هذه ىلع
 لوجتملا.

- Windows: عاجرتسال ئيها م ددح NPCAP
- Io0: عاجرتسال ديدحت: كام



طاقات ال ليغشت جمانرب عم يكلسالال نحلل Windows نم ثدحأ تارادصا: ريذحت دوجوم ريغ عاجرتسالال ئيهاهم ناك اذا. عاجرتسالال ليغشت جمانرب معددي يذلاو، NPCAP، rawcap.exe تاميلعت مدختسا وأ Wireshark نم رادصا ثدحأ ثيذحتب مقف

ةرفشمال DNS رورم ةكرح

الو ةلظملاو لوجتمال ليمعال نيپ تانايبال رورم ةكرح ريفشت متي، ةيداعال فورظال في موقت نا Umbrella معد بلطي نا نكمي، تالاحال ضعب في. رشبال ةطساوب اهتءارق متي كانه. Umbrella ةباحسول لوجتمال ليمعال نيپ DNS رورم ةكرح ةيؤرل DNS ريفشت لي طعتب كلذب مايقلل ناتقيرط:

- 208.67.222.222 و 208.67.220.220 لىل UDP 443 ل لىلحم ةيماح رادج ةلتك عاشنا
- لوجتمال ليمعال رادصاو ليغشتال ماظن لىل عانب فلمال عاشناپ مق وأ
 - 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

- سلا وأ كام:

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

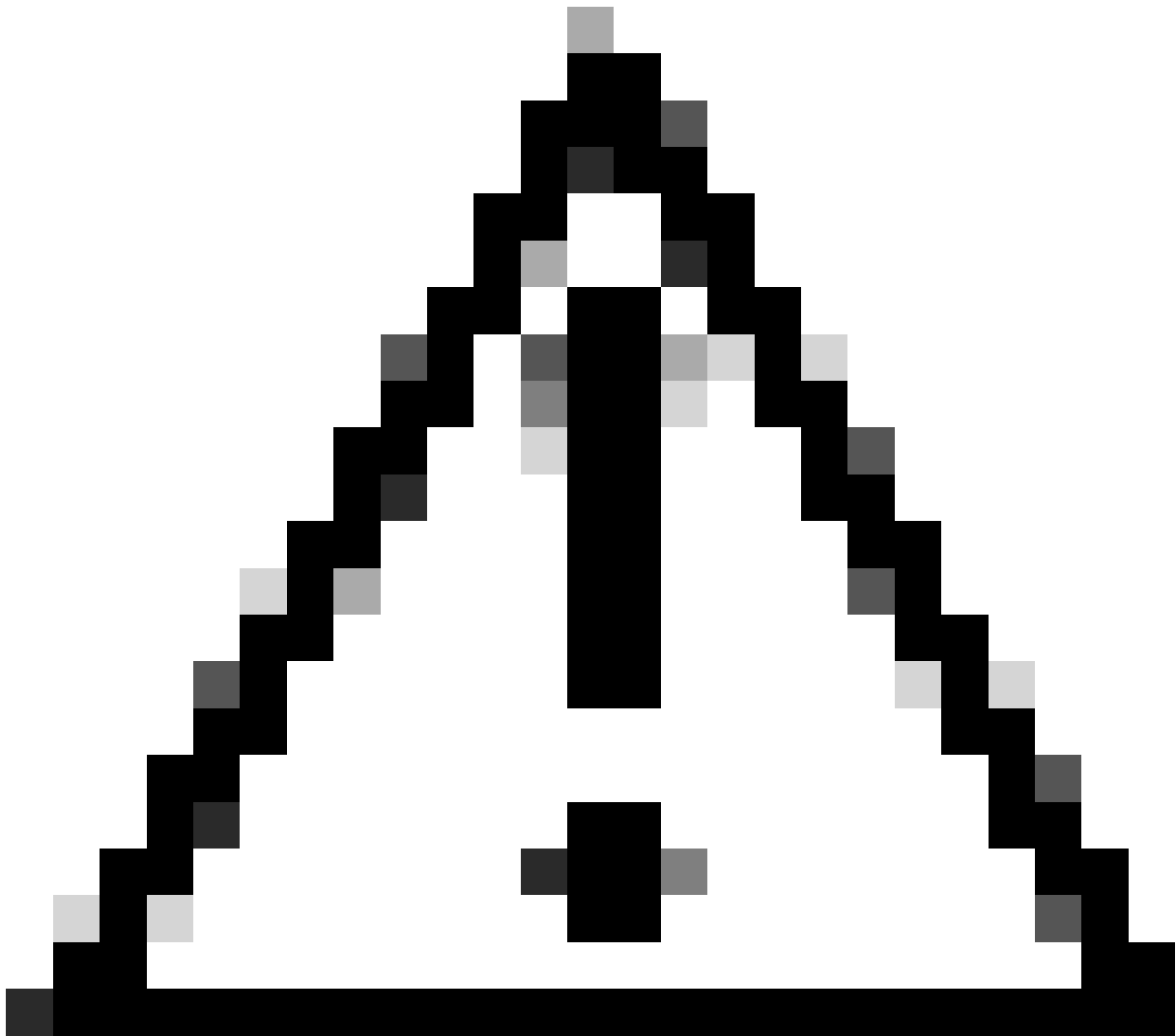
- Mac OS AnyConnect لي غشتلا ماطن:

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

- نملال لي مغل Mac OS لي غشتلا ماطن:

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

رتوي بمكلا وأ مغللا لي غشتلا ماطن، كلذب مايقللا دعب



لېځشت چم ان رڼ Windows ځي لځ Wireshark نم ش دحلأا تارا دصلإا نمضتت :ريذحت
جاتحت دق Windows، ځي لځ Umbrella VPN هه ځاو معدي ال ځي ذلوا، NPCAP طاقا ل
لځي دېك rawcap.exe ادا م اذخت سال.

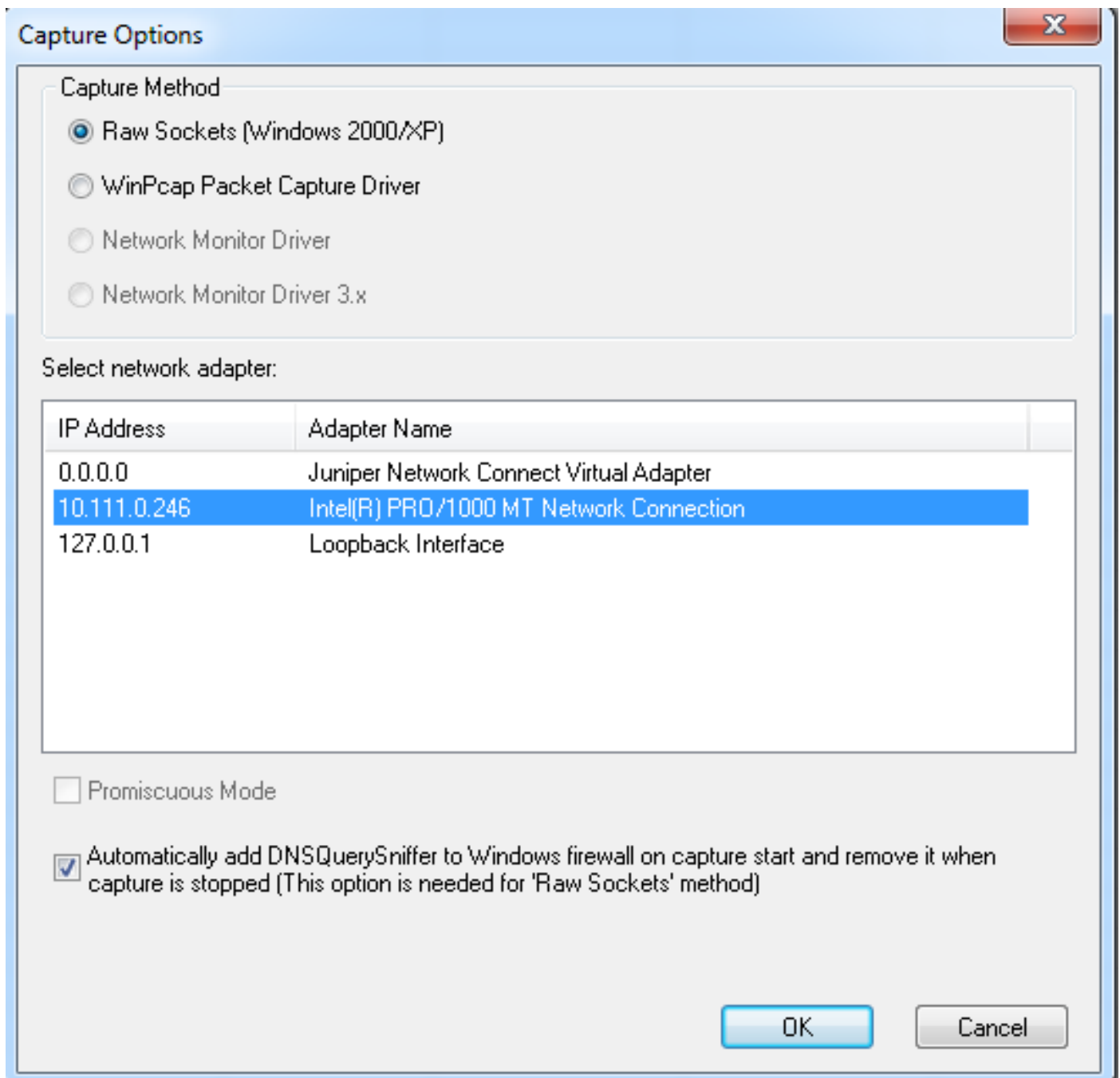
DNSQuerySniffer - Windows Alternative

نم نان طأ ضرعيو بځاري ځي ذلوا Windows ل طقف DNS ةكېش sniffer وه DNSQuery sniffer
رصتقي جهنلا اذه م اذختسإ نإف ،باكوار وا كراشيريو نم ضيقي نل ځي لځو . ةديفم ل تانايب ل
تاذا م ول عمل صالختساو صحف ي ف اريثك لهسا وهو ، (DNS) تاقاطنل عامسا ماظن ځي لځ
Wireshark ع قوم اهب عتمتي يتي ل ةيوقل ةيفصتلا تاودا كلتمت ال اهنأ ال . ةلصل

طاقا ل كنكمي هنأ راځل اذه م اذختسإ تازيم نم . م اذختسالا ةلهسو نزول ةفي ف ځا اذه
مالعتسا لك ةدهاشم كنكمي و ، طاقا لال اءبو ، "لوچتمل ليمعلا" ةمدخ لي طعت اناثأ مزحل
ءب نم ال دې طاقا لال لېځشت اهي ف اءبي يتي ل ةطحلل نم لوچتمل ليمعلا هل سري DNS
لځل فاب "لوچتمل ليمعلا" لېځشت ءب دعب طاقا لال

طاقا لال ل ناتقي رط كانه

1. عمىاق يف ءءوءوملأا ءامالعل ءالال ءىؤرك نكمىف ، ءىءاعلال ءكبشلال ءهءاوءءءء اءل .
dnscryptproxy ربع اءىءء رمل مل ىءلال وأ ، طقف ءىلءاءلال ءالاءملا



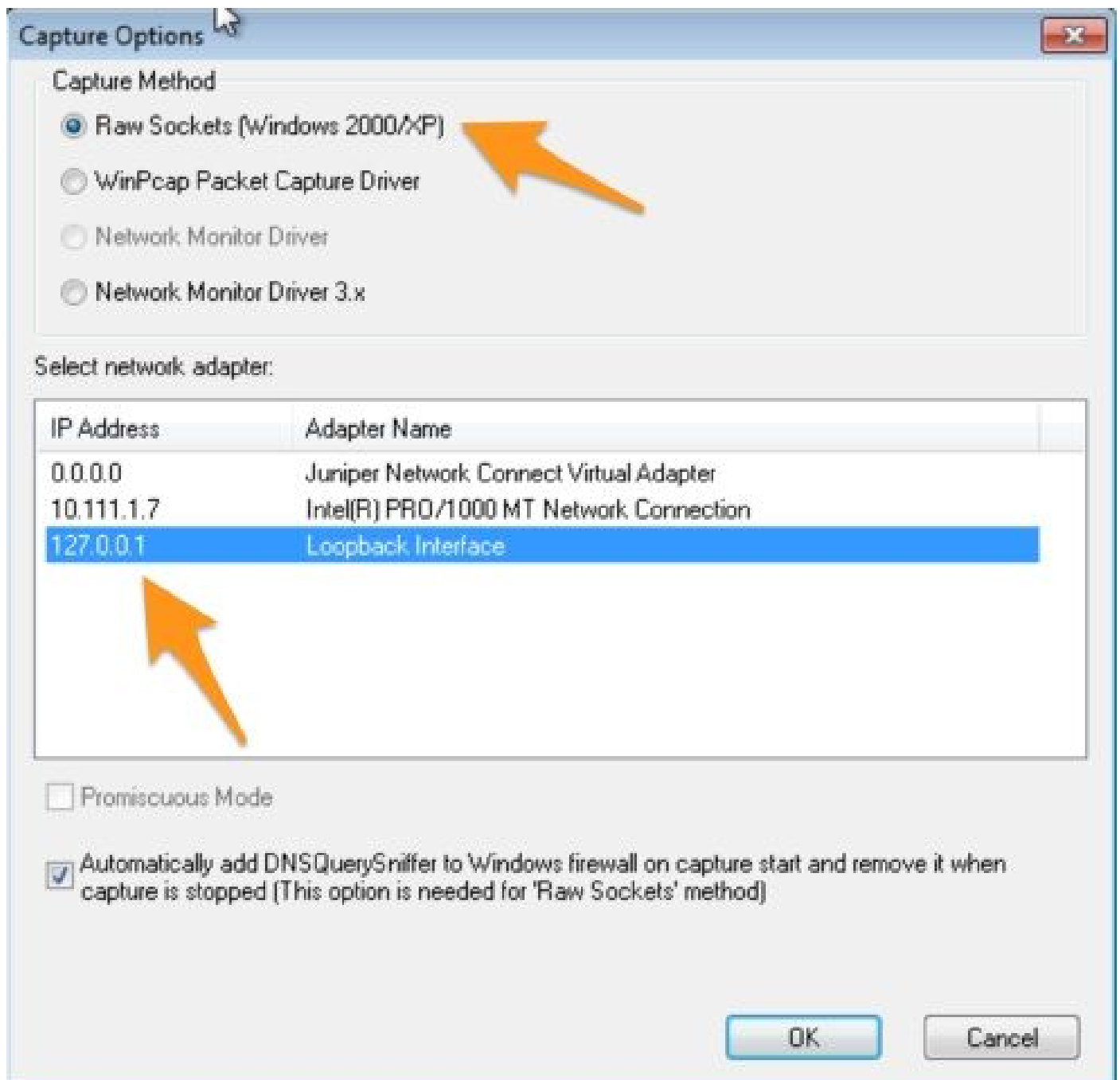


مەقۇوف قىلزنن نأ كىل عو طاقت لالال فى نىمىللا ھاجتلا فى ەدمعأالا ھذە رەظت : ەظحال م
مەتپۇرل ادجالىلق

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

أدعم DnssNiffer

2. لالځ نم اهل اس را م تي تي ال DNS تامال عتسا عي مج ى رتس ف ، عاجرتسالا هجاو تدح اذا .
 دوجومل تالاجملل يقي قحلا هجول IP ناو نع ةيؤر كنكمي ال نكلو ، DNSCRYPTPROXY ،
 ةباجال او مالعتسال اضري لازي ال هناف ، كلذ عمو . ةيلخادل تالاجمل ةمئاق يف .





مەقۇف قىلزنن ئا كىلەو، طاقتىللا يى نىمىلا ھاجىتى يى ەدمەللا ەزە رەظت: ەظھالم
مەتپۇرل ادج الپلق

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

أدومع DnssNiffer

ي:لي امك ودبت جئاتنل

DNSQuerySniffer										
Host Name	Port	Queue	Request	Request Time	Response Time	Dur...	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	74.125.239.147 74.125.239.146 74.125.239.144 74.125.239.145 74.125.239.146	
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	67.215.92.218	
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	72.21.91.8	
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	74.125.239.142 74.125.239.128 74.125.239.133 74.125.239.136 74.125.239.147	
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	54.239.132.147 54.239.116.53 54.239.116.239 54.239.117.152 54.239.117.153	
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	72.21.91.8	
www.googleadservices.com	52186	4B87	A	12/5/2014 6:17:31 PM.193	12/5/2014 6:17:31 PM.200	7 ms	Ok	4	74.125.239.153 74.125.239.141 74.125.239.154	
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	74.125.239.143 74.125.239.159 74.125.239.151 74.125.239.152	
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	107.20.215.3 54.243.99.177 184.73.172.240 174.129.203.102 54.239.117.153	
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	74.125.129.154 74.125.129.157 74.125.129.156 74.125.129.155	
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	74.125.239.159 74.125.239.151 74.125.239.152 74.125.239.143	
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	23.36.58.103	

dns_3.png

ي:درفل ثحب ال ضرع

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

dns_4.png

RawCap.exe - Windows Alternative

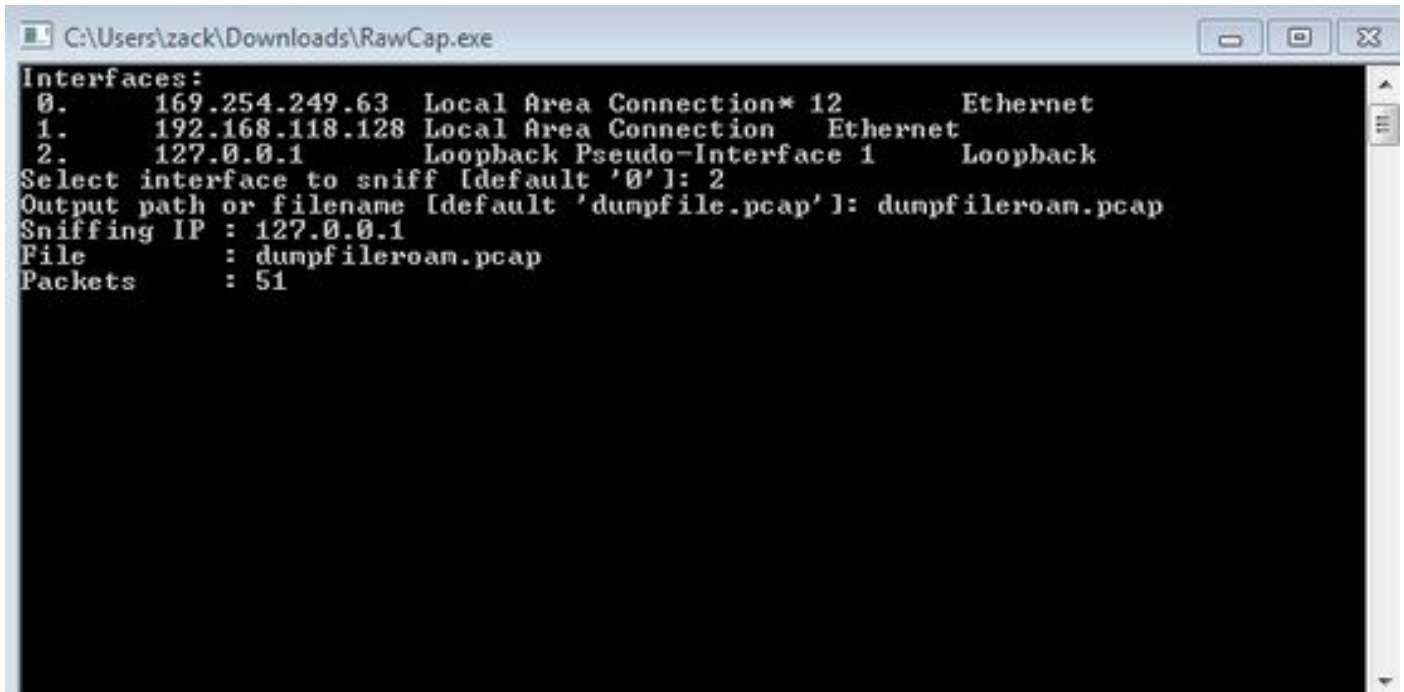
هه الاول Wireshark عم نمضم الة مزحل طاق ال ل يغشت جم ان رب معد ي ال ، ال اح ال ضع ب ي ف ع ا ج ر ت س ال ال هه اول قل كش م اذه نو ك ي ن ا ن ك م ي . ا ه ع م ل م ع ال ال ا ج ا ت ح ت ي ت ال

RawCap.exe م ا د خ ت س ا ا ن ن ك م ي ، ال م ا ل ه ذه ي ف

ي د ا ع ر و ر م ال ك ر ح ض ب ق ال ع ن ا Wireshark ل م ع ت س ي ن ا ال ا ق م ال ي ف ل ب ق ن م steps ال ت م ت ا . 1.

2. RawCap.exe لي غشت ب مق ،تقول اسفن ي ف.
3. قباطم لة مئاق ل مقرر دي دحت قيرط نع ةهجاو ل دي دحت ب مق .
4. هلي غشت متي مئ تاجرم فلم مسا نبي عت ب مق .
5. طاق تلال افاقي دي رت يذل SelectControl-Cwhen .

هنا RawCap.exe لي غشت ب تمق يذل دلجم ل ي ف ظو ف ح م ل فلم ل عضو متي :



```
C:\Users\zack\Downloads\RawCap.exe
Interfaces:
0. 169.254.249.63 Local Area Connection* 12 Ethernet
1. 192.168.118.128 Local Area Connection Ethernet
2. 127.0.0.1 Loopback Pseudo-Interface 1 Loopback
Select interface to sniff [default '0']: 2
Output path or filename [default 'dumpfile.pcap']: dumpfileroam.pcap
Sniffing IP : 127.0.0.1
File : dumpfileroam.pcap
Packets : 51
```

rawcap_1.jpg

ةمچرتل هذه لوح

ةيلآل اتي نقتل نم ةومجم مادختساب دنتسمل اذه Cisco تمچرت
ملاعلا اناء عي مجي في ني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوكت نل ةيلآ ةمچرت لصف اناء ظحال ميجري. ةصاغل مهتغلب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه
ىلإ امئاد عوچرلاب يصوت و تامچرتل هذه ةقदन ع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصأل ايزيلجنلإا دنتسمل