

طبارل لوصول ةطقن مزح بللقم ليوحت Wireshark

تايوتحمل

[ةمدقملا](#)

[ةيساس الابلطتملا](#)

[ءارءالا](#)

[ةمزلءا ءيرفت ذيفنت](#)

[ءارءالا فلم فيظنت](#)

[فيظنتلا ةمزلءا صءلم تامولعم](#)

[ءانزالا تامالعو ةيادلل اءافاسم ءانا](#)

[ةمزلءا ءانا ءيحصت](#)

[مزلءا تيب اءءو لصف](#)

[PCAP لىلا يصنلا فلملا ليوحت](#)

[Wireshark ربع \(GUI\) ةيموسرلا مءءتسملا ءءاو](#)

[ءماوالا رطس ربع](#)

[ءءال صاو ءاطء ال فاشك تسا](#)

[مزلءا ءءارق ءءكم ال 2pcap صنلا نكل ءيحص صنلا فلم](#)

[ءقسا نءم ريء ءانا](#)

ةمدقملا

لىل CoS لوصول ةطقنل ءءاشنل مءل ءل ءمزلءا ءيرفت ليوحت ءي ءي ءنءتسملا اءء ءضوي
مءءال ءوء لىل لىءب لءءك Wireshark ل PCAP قيسنءت

ةيساس الابلطتملا

- Windows لء طقف رفوتم - Notepad++
- Wireshark ل ءيءالءا ءاىءبءءال لء نءمضم - Text2pcap ءبءم

ءارءالا

ةمزلءا ءيرفت ذيفنت

لىل <multi options> verbose ءي ءءل لء ال debug traffic رءال لىءءشءب AP ءمزلءا ءيرفت طءءال
ءاءءاولو ءءءءم ءي ءصء لءمءو نىب رايءءال لءنءمى AP رءاولو رطس

ةي ءرطال ءءءول لىل ءسءلءال لءءس

رءءال ءورءالو ءلءب مءي قلاء ءءءلءا ءاطءض نء رءقم لءل لاسر لىل اصيرء نء
يءل رءءال ءيظنءال ءسفن طاءءال لىل لىمءنء ال ءلءل فلملا لىل ءءابءلل ءي لءبءاق

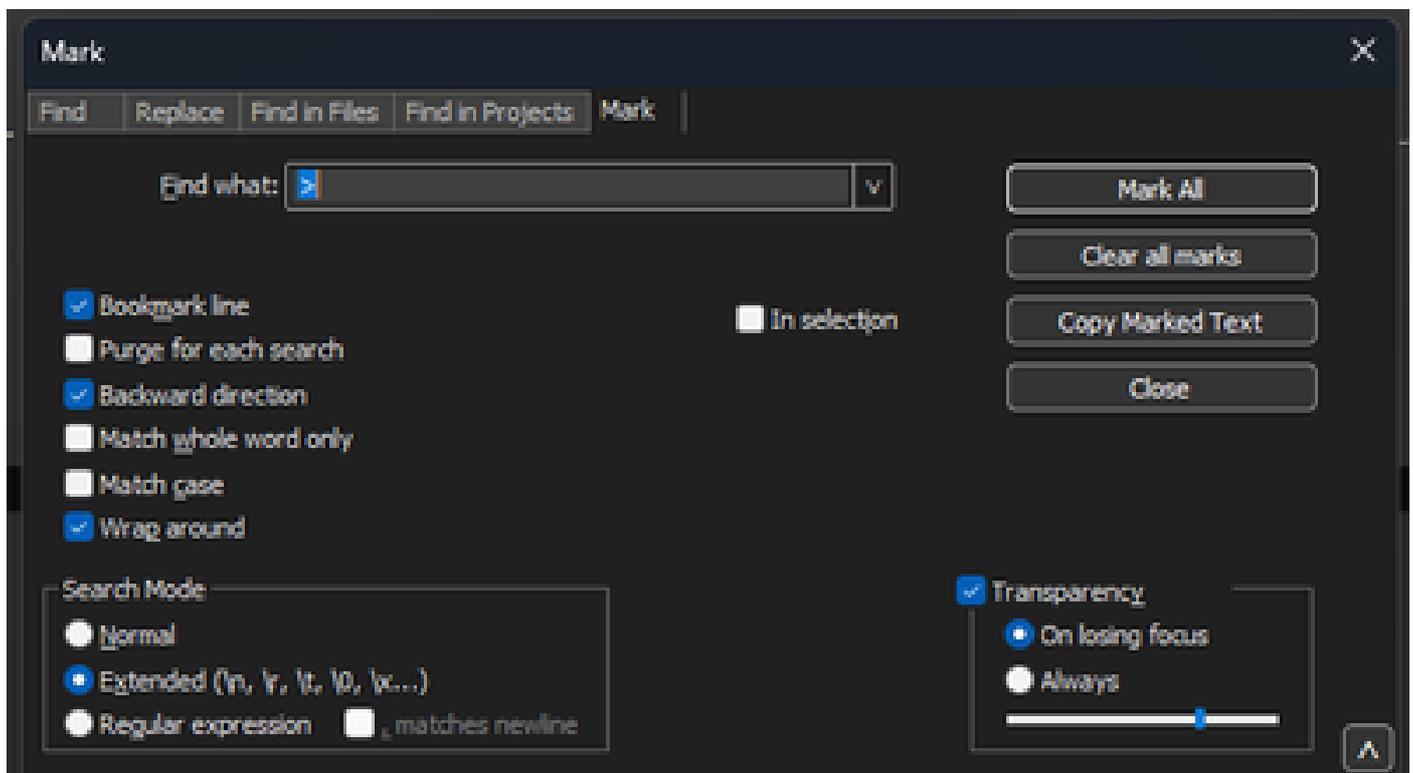

```
22:35:17.1669188 IP CSCO-W-PF320YP6.1an.60354 > 239.255.255.250.3702: UDP, length 656
0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030: 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040: 636f 6469 6e67 3d22 7574 662d 3822 3f3e
<truncated>
0x0070: 444c 4e41 444f 432f 312e 3530 2050 6c61
0x0080: 7469 6e75 6d2f 312e 302e 342e 320d 0a4d
0x0090: 414e 3a20 2273 7364 703a 6469 7363 6f76
0x00a0: 6572 220d 0a53 543a 2073 7364 703a 616c
0x00b0: 6c0d 0a4d 583a 2033 0d0a 0d0a
```

فيظنتلا ةمزح صخلم تامولعم

00000 ةديج ةحازا روهظ دنع ةديج ةمزح ةيادب فاشتكام تي اهتلازا لضألا نم نوكي لكاشملا بنجتلا، ةمزح لك لبق ةعوبطملا صخلملا تامولعم

عضو نا نم دكات، اهديحتو ةمالع بيوبتلا ةمالع نع شح > شحبالا لىل لقتنا Notepad++ في عسوم شحبالا

لك لىل ريشة ةيلمعلا هذه. لكلا زييمت رقن او > زمرلا لقلحلا لخدي: اذام نع شحبالا في زمرلا > لىل عيوتحت يتلا طوطخللا



لخادللا Chevron فرح لىل عيوتحتي يذلا لقلحلا نع شحبالا عم Notepad++ Mark راوخللا عبرم

لثم دنتسمل روطس عيچ لىل عوضال Notepad++ طلسي، س وورلا زييمت دعب

```
debug wired sample - Copy.log [2]
1 22:35:17.1669188 IP CSCO-W-PF320YP6.lan.60354 > 239.255.255.250.3702: UDP, length 656
2 0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
3 0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
4 0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
```

نورفيشال لىل يوتحي يذلا زربملا طخلال عم مزلال غيرفت عصاصق

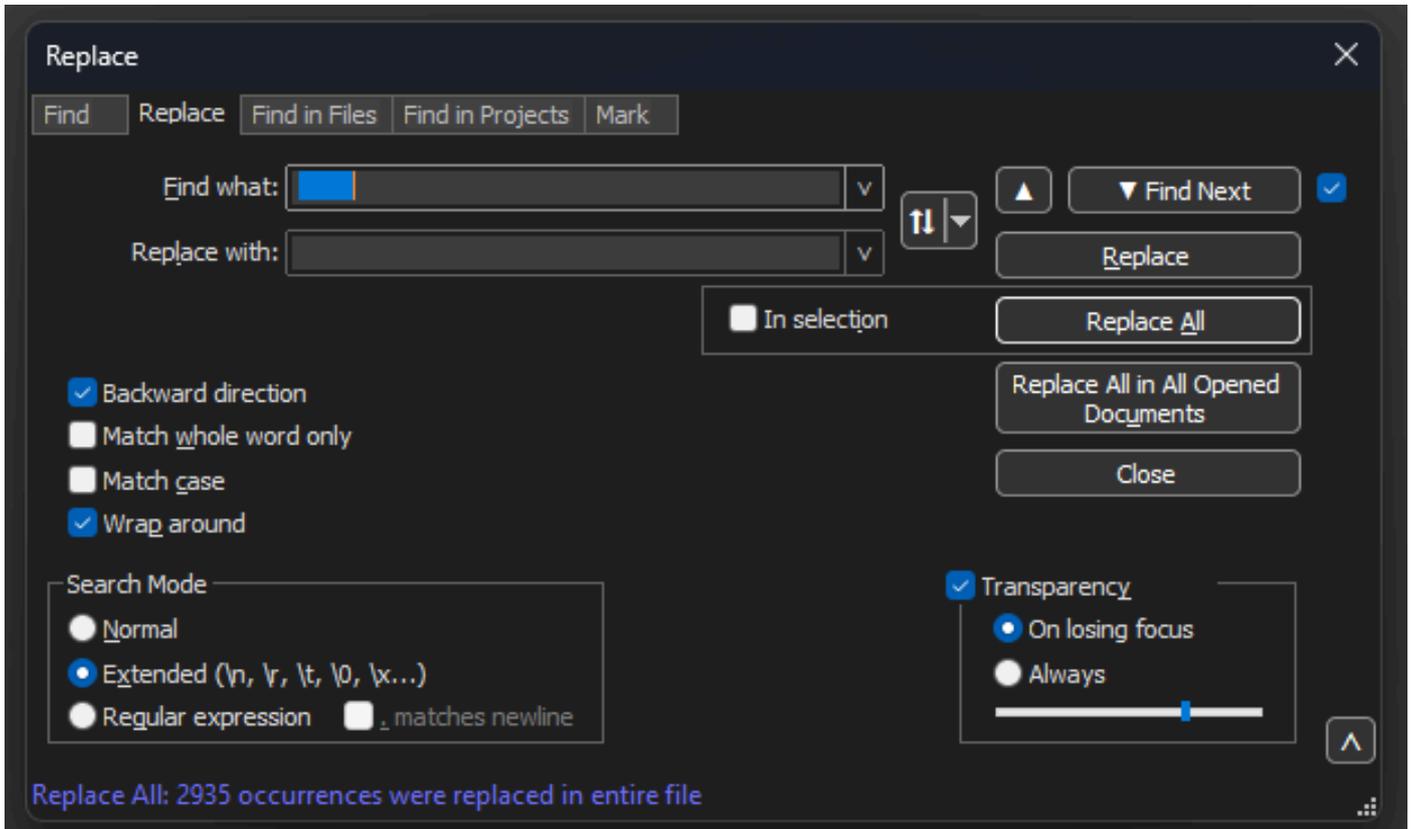
مايقلال دعب. عيچرم عراشإب عملم طوطخ علازا لىل رقناو عيچرم عراشإ>ثحب لىل لقتنا
عصاصقلال هذه لثم فلمال ودبي، كلذب

```
0x0000: 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010: 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020: fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030: 7665 7273 696f 6e3d 2231 2e30 2220 656e
```

عازالال تامالعو عيادبلال تافاسم علازا

ثحبالال عضونا نم دكأتف، اهددح مث لادبتسإ بيوبتلال عمالع نع ثحب>ثحب لىل لقتنا
عسوم.

قوق رقناو غراف لقلال: ب لادبتسإ كرتأ. عاضيب تافاسم 8 لقلال لخدي: اذام نع ثحب لىل
لك عيادب يف عيالاتتملا عينامثلال عاضيبلال تاغارفال لك لدبتسي اذه. لكل لادبتسإ
عروصلال هذه لثم ودبت لادبتسالال عاشاش. لاعف لكش ب مهف ذحيو، عيش الب رطس



Notepad++ Replace ب Find the What field with 8 spaces.

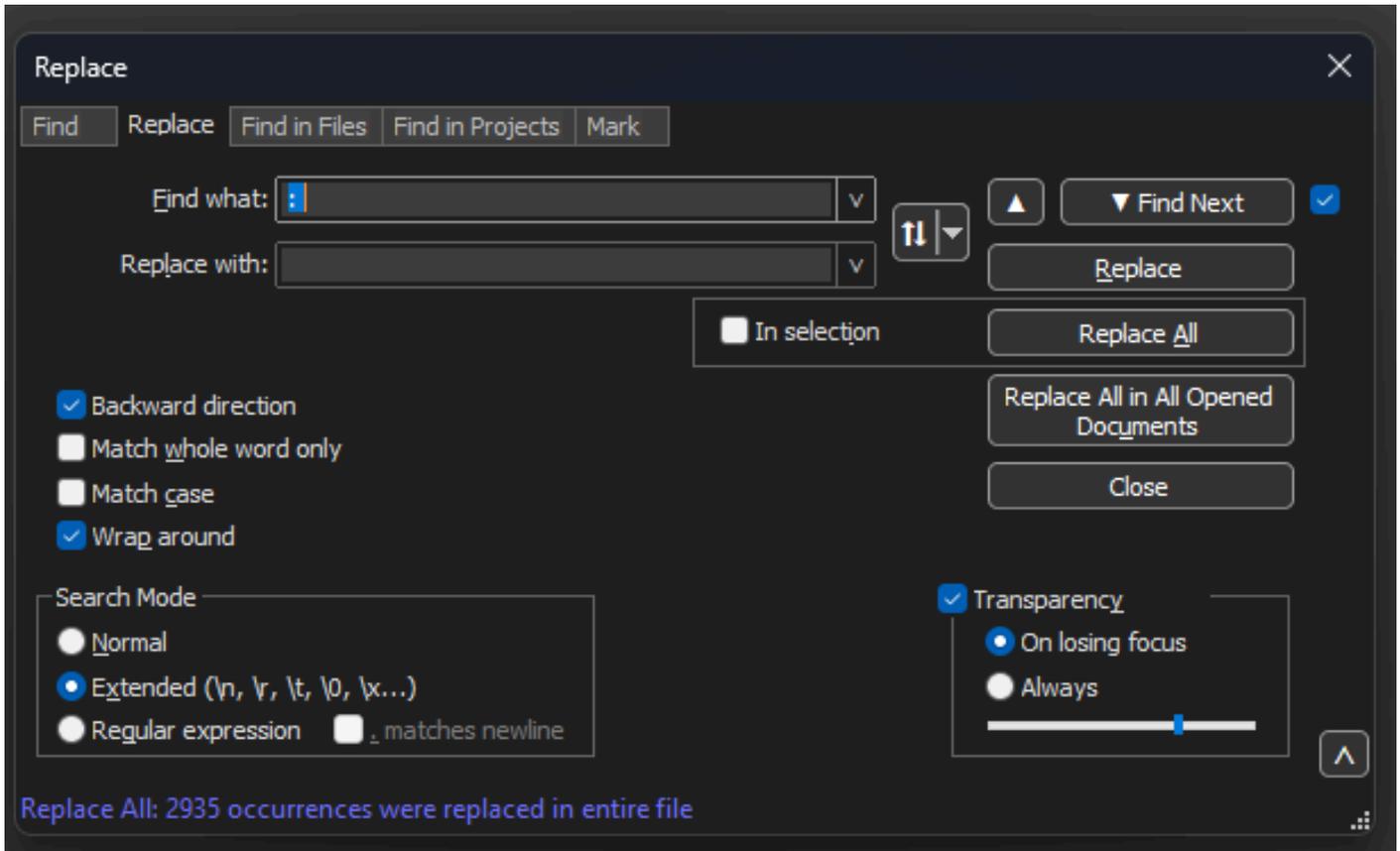
ةصاصقلا لثم ةي لمعلا هذه دعب جتانلا فلملا ودبي

```

0x0000:  0100 5e7f fffa 806d 971d a040 0800 4500
0x0010:  02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020:  fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030:  7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040:  636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050:  3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060:  6d6c 6e73 3a73 6f61 703d 2268 7474 703a
0x0070:  2f2f 7777 772e 7733 2e6f 7267 2f32 3030

```

عضونا نم دكأت، ةحفصلا هذه ددحو لادبتسا بيوبتلا ةمالع نع شحب > شحب ىلا لقتنا كرتأ. اذام نع شحب لققحلا ىلع (نيتطقنلا دعب ةغرافلا ةحاسملا ظحال) : لخدأ. عسوم شحبلا لكلا لادبتسا قوف رقناو غراف لققحلا : ب لادبتسا ةحازالا دعب ىلوالا تاغرافلا واولالا لك لادبتسي اذه.



ةحاسمو ةريغص ةطقنب هؤلم مت يذلا لققنل نع ثحبلا ةزيمب راولح اعبرم لادبتس | Notepad++

ةصاقللا هذه لثم ودبي جتانللا تاجرخلما فلم نإف، ةقباسللا ةيلمعلا دعب

```

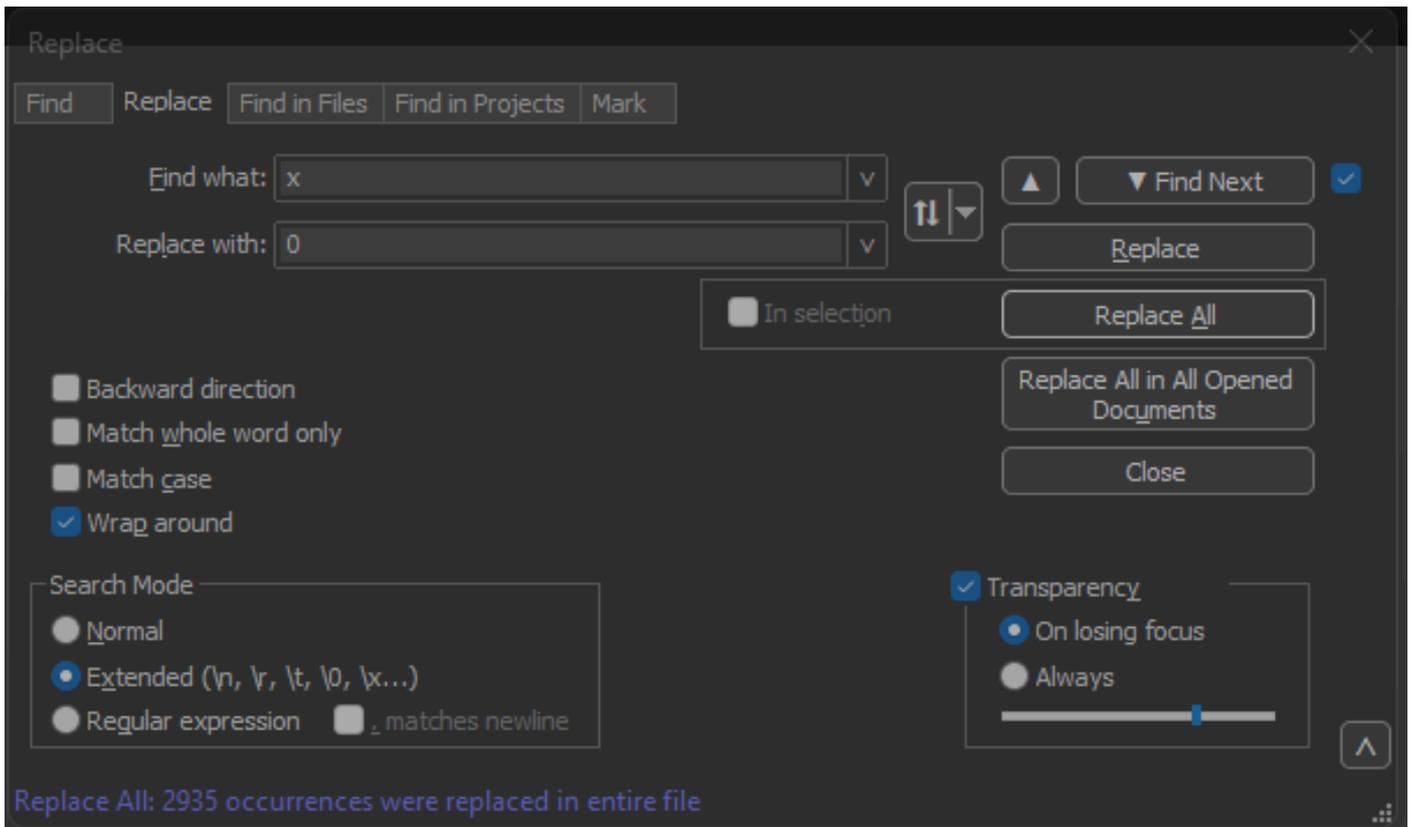
0x0000 0100 5e7f fffa 806d 971d a040 0800 4500
0x0010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
0x0020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
0x0030 7665 7273 696f 6e3d 2231 2e30 2220 656e
0x0040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
0x0050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
0x0060 6d6c 6e73 3a73 6f61 703d 2268 7474 703a
0x0070 2f2f 7777 772e 7733 2e6f 7267 2f32 3030

```

ةمزحللا ةحازا حيحصت

فأ 6 نم ةنوكم ةيرشع ةيسادس ةلسلسك ةمزح لك لخد ةمزحللا ةحازا Text2pcap عقوتي اذه حيحصتل. لكذ نم الادب ةحازالا زيمرتل AP 0x مزح طاقسلا تايلمع مادختسا متي نكلو عسوم ثحبلا عوضونا نم دكأت، لادبتسلا بيوبتلا ةمالع ديدحتو ثحب > ثحبلا لقتنا، رمالا

موقى. لكلا لادبتسلا لعل رقناو 0 ب: ب لادبتسلا لققن ةئبعت. اذام نع ثحب لققنلا يف x لخدأ Text2pcap ل عقوتملا ةحازالا قيسنت قباطيل 0 ب ةحازالا لخد دوجوملا x لك لادبتسلا اذه



0 فرحلاب أبعمل لادبتساو x فرحلاب لرحل لرحل نع شحب ب راوخل ع برم لادبتسا | Notepad++

ةصاقللا هذه لثم ودبي جتانللا تاجرحملا فلم نإف، ةقباسلا ةيلعمل دعب

```
000000 0100 5e7f fffa 806d 971d a040 0800 4500
000010 02ac d4bb 0000 0111 cd11 c0a8 64d1 efff
000020 fffa ebc2 0e76 0298 757b 3c3f 786d 6c20
000030 7665 7273 696f 6e3d 2231 2e30 2220 656e
000040 636f 6469 6e67 3d22 7574 662d 3822 3f3e
000050 3c73 6f61 703a 456e 7665 6c6f 7065 2078
```

مزحلل تياب تادحو لصف

نع ةيرشع ةيسادس ميقي نم جوز لك لصف متي نأ Text2pcap تانايب قيسنت بلطتي تانايب ةعارقب Text2PCAP موقوي نأ يف حيحص ريغ قيسنت ببستتي ف، ةفاسم قيرط لشف ي مث ةحازا ةئيه ىلع ةمزحلل.

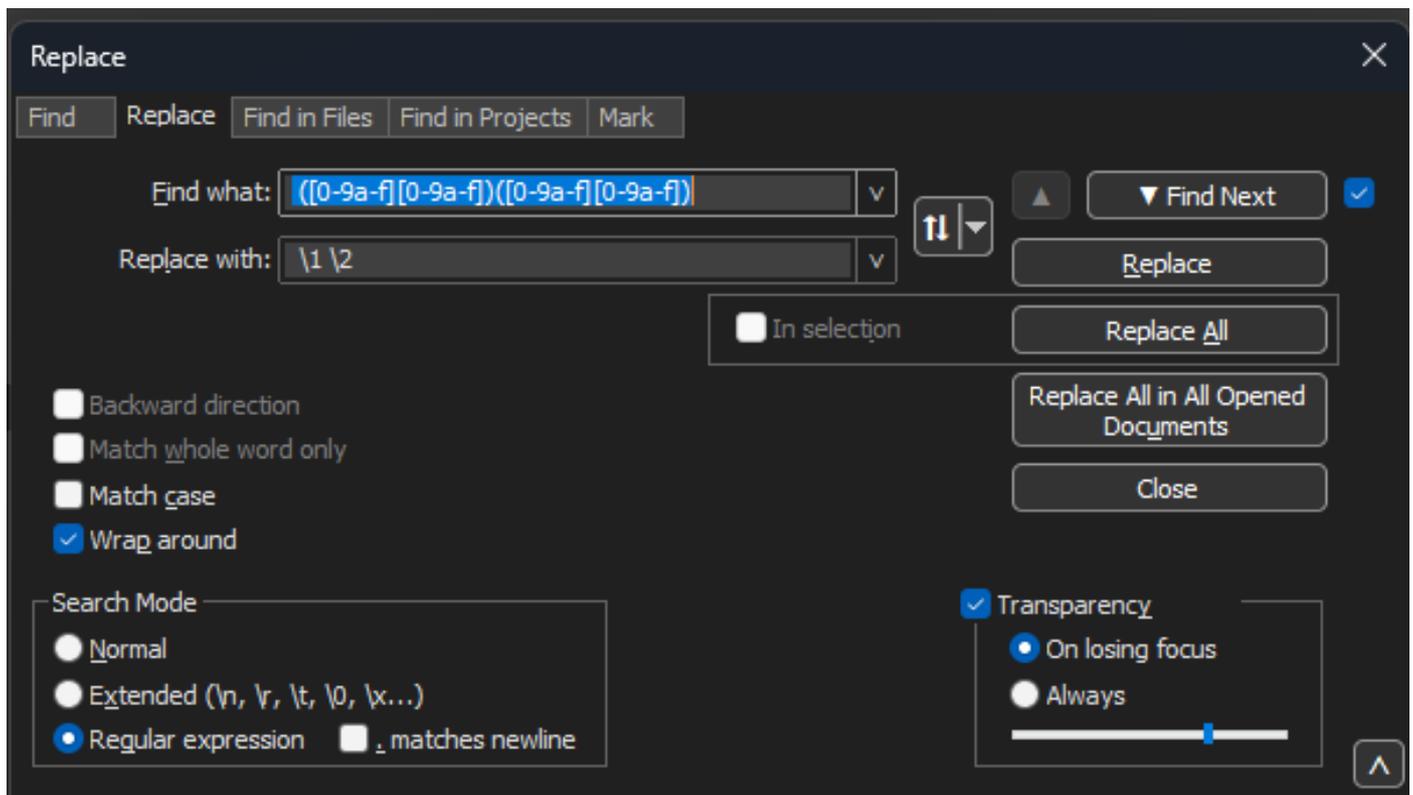
وه شحلل عضو نأ نم دكأت، اهددح مث لادبتسا بيوبتللا ةمالع نع شحب>شحب ىللا لقتنا يداع ريبعت.

إذا ما ن ع شح ل ل ق ح ل ل ي ل ع (ة ئ د ا ب ل ا ع ح ا س م ل ا ط ح ا ل) ([0-9a-f][0-9a-f])([0-9a-f][0-9a-f]) ل خ د أ

ل ك ل ل ا د ب ت س ا ي ل ع ر ق ن ا و (ة ئ د ا ب ل ا ع ف ا س م ل ا ط ح ا ل) \1 \2 ب : ب ل ا د ب ت س ا ي ل ق ح أ ل م ا

ن ي ب ة ف ا س م ل خ د ت و ة م ز ل ل ة ي ر ش ع ل ا ة ي س ا د س ل ا ت ي ا ب ل ا ت ا د ح و ن ع ل ا د ب ت س ا ل ا ة ي ل م ع ش ح ب ت
ة و م ج م ي ف م ه ظ ف ح ي ، ي ر ش ع ي س ا د س م ا ق ر ا ج و ز ا ه ع ب ت ي ة ح ا س م regex ق ب ا ط ي . ج و ز ل ك
ة و م ج م ي ف م ه ظ ف ح ي و ، ة ي ر ش ع ل ا ة ي س ا د س ل ا م ا ق ر ا ل ا ن م ر و ا ج م ل ا ج و ز ل ا ذ خ ا ي م ث ، 1 ط ا ق ت ل ل ا ل ا
ة و م ج م ل ك ي و ت ح م ل ك ل ذ ك و ة ب و ل ط م ل ا ت ا ح ا س م ل ا ن م ا ل ك ل ا د ب ت س ا ل ا ع ب ط ي . 2 ط ا ق ت ل ل ا ل ا
ط ا ق ت ل ل ا

ل و ص و ل ا ة ر ك ا ذ ن م ر ي ث ك ل ل م د خ ت س ي ه ن ا . ف ل م ل ا ل و ط ب س ح ق ي ا ق د و ا ن ا و ث ة د ع ر م أ ل ا ق ر غ ت س ي
ا ر و ب ص ن ك ، ا ر ي ب ك ف ل م ل ا ن ا ك ا ذ ا ل ي غ ش ت ل ا ء ا ن ث ا (RAM) ي ء ا و ش ل ا



ر خ ا ي د ا ع ر ي ب ع ت ب ه ؤ ل م م ت ي ذ ل ا ل ا د ب ت س ا ل ا ل ق ح و ي ن و ن ا ق ر ي ب ع ت ب ه ؤ ل م م ت ا م ي ل ع ر و ث ع ب ر ا و ح ل ا ع ب ر م ل a د ب ت س a | Notepad++

م ت ي ل ز ه ا ج و ه و ة ص ا ص ق ل ل ا ذ ه ل ث م و د ب ي ج ت ا ن ل ل ا ت ا ج ر خ م ل ا ف ل م ن ا ف ، ة ق ب ا س ل a ة ي ل م ع ل a د ع ب
ر خ a Text2pcap. ة ط س ا و ب ه ل ي و ح ت

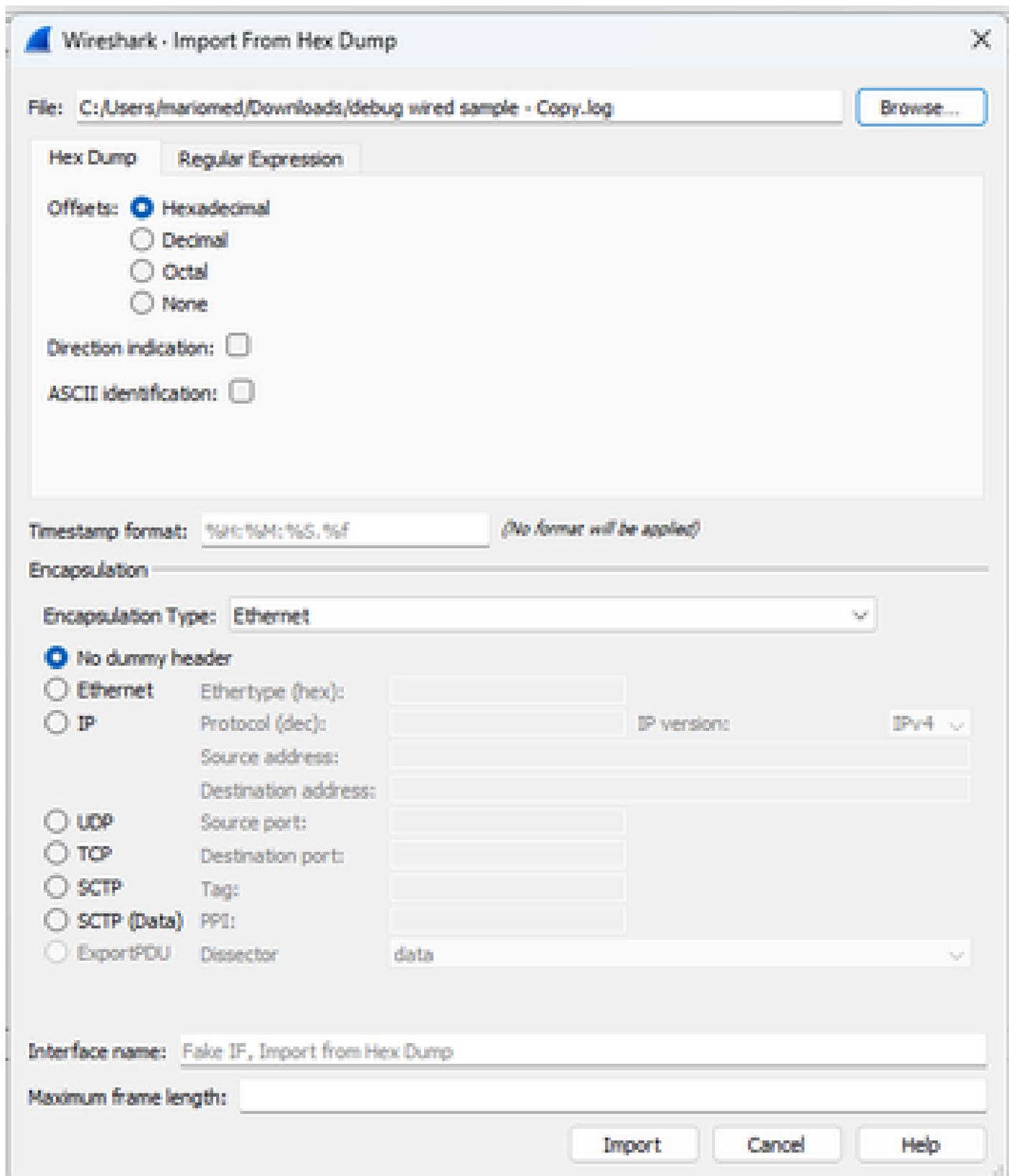
```
000000 01 00 5e 7f ff fa 80 6d 97 1d a0 40 08 00 45 00
000010 02 ac d4 bb 00 00 01 11 cd 11 c0 a8 64 d1 ef ff
000020 ff fa eb c2 0e 76 02 98 75 7b 3c 3f 78 6d 6c 20
000030 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e
000040 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e
000050 3c 73 6f 61 70 3a 45 6e 76 65 6c 6f 70 65 20 78
```

000060 6d 6c 6e 73 3a 73 6f 61 70 3d 22 68 74 74 70 3a
000070 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30
000080 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f
000090 70 65 22 20 78 6d 6c 6e 73 3a 77 73 61 3d 22 68

PCAP ىل اىصننلا فلملا لىوت

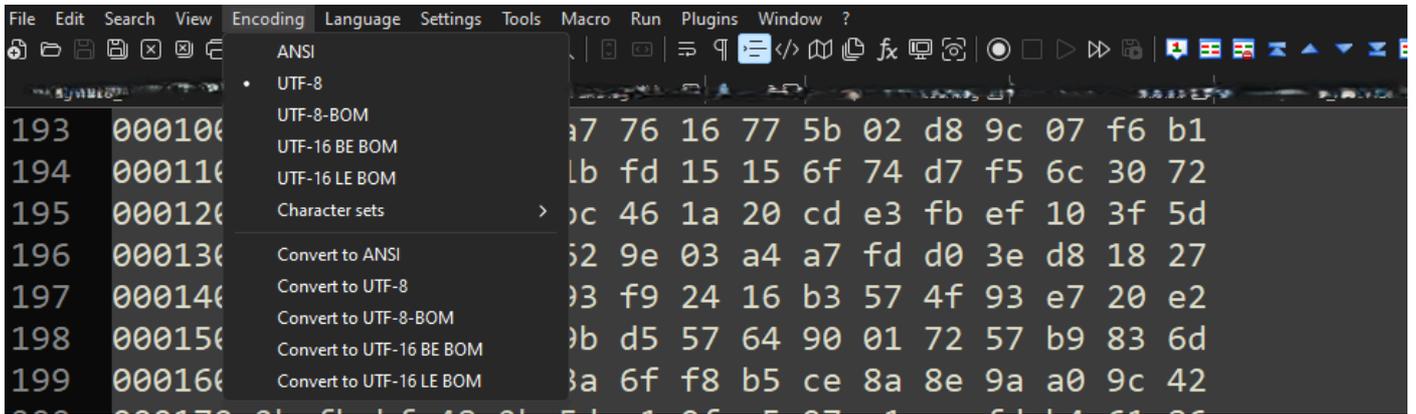
Wireshark ربع (GUI) ةيموسرلا مدختسملا ةهجاو

غرفت نم داريتس اىفلم اىل اىصننلا فلملا لىوت، PCAP ىل اىصننلا فلملا لىوت،
راوح بزم رهظي، ايسادس



Wireshark داریت س | ةشاش

یس ادس وه ددحم لآ ءازالآ عون نأ نم دكأت .ی صن لآ فلم لآ ءیرفت ددحو .. ء ءصت رز یل ء رونا یم وه سآر ددحت متی ملو تنرثیا وه نی مضت لآ عون ، رشع



Notepad++ زيمرتل اعمئاق تاراخي

عمقسانتم ريغ عمازا

لكشب عمزحلل اىل ع تانايبلا عجب عصاخلا تيايلا تادحو لصف م تي ال ام دنع اطلال اذه رهظي في لشفيو وديج عمز عميادب ضررت في Text2PCAP لعج اىل ايدوي اذهو، جاوزا في حيحص عميروفلا عمجرتلا.

undebg all لثم عمزحلل اوتحم طسو في لسالس وا لصف نودب عمزحلل تيايلا تادحو اىل عم شحبا رمالا.

```
C:\Users\mariomed>text2pcap "C:\Users\mariomed\Downloads\debug wired sample - Copy.log" output.pcap
Input from: C:\Users\mariomed\Downloads\debug wired sample - Copy.log
Output to: output.pcap
Output format: pcapng
** (text2pcap:81244) 10:30:46.781149 [(none) MESSAGE] -- Inconsistent offset. Expecting 75, got 80. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.781712 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782136 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782446 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782599 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782748 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.782891 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783033 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783169 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783319 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
** (text2pcap:81244) 10:30:46.783456 [(none) MESSAGE] -- Inconsistent offset. Expecting 10, got 10. Ignoring rest of packet
```

تارم عميروفلا عمزحلل اىل عمقسانتملا ريغ عمازالا عبطت. حل اص ريغ فلم ليوت عم لوجم دع Windows رم او رطس جارخا.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا