

## الفصل الرابع



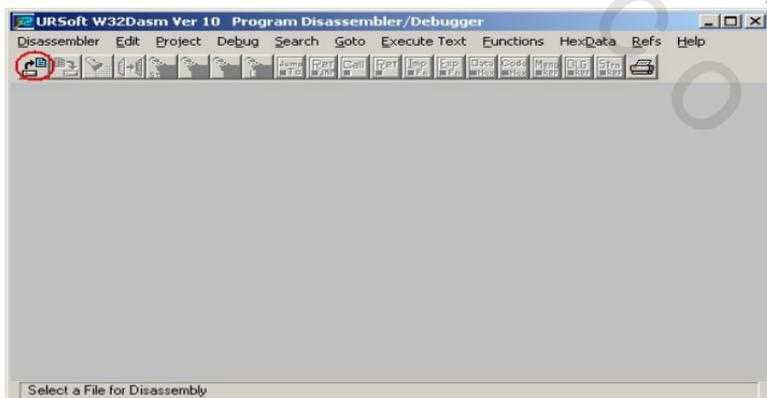
إعادة الهندسة

## Reverse engineering إعادة الهندسة

تعنى عملية إعادة الهندسة هي تحويل تعليمات الملف التنفيذي التي أصبحت بصورة ثنائيته إلى تعليمات بلغة الاسمبلي مما يمكننا من الوصول إلى أي مكان بالملف وتعديله بدون إفساد الملف ويمكننا أيضا البحث عن نص معين داخله أو حتى داله محدد وفيما يلي أشهر وأقوى برامج إعادة الهندسة W32Dasm وبرنامج IDA Pro

برنامج W32Dasm:

من البرامج العريقة ومن أول الأدوات الأساسية للكرارك ويقوم البرنامج بكل بساطه بترجمة ملف exe إلى كود بالاسمبلي حيث يمكن متابعة عنوانين كل أمر وخصوصا أوامر القفز مثل JNE, JMP, JZ وغيرها. ويستخدم هذا البرنامج دائما مع برنامج Hview حيث يمكن عن طريق الأخير تعديل ملف exe بسهولة وسنتكلم لاحقا عن هذا البرنامج الهام. والشاشة الرئيسية للبرنامج بها قوائم الأوامر ومفاتيح الاختصار لتنفيذ الأوامر بطريقة سريعة وأول مفتاح هام هو مفتاح فتح الملف التنفيذي كما يتضح بالشكل التالي:



بعد الضغط على هذا المفتاح يتم فتح ديالوج للسؤال عن الملف التنفيذي المراد تحويله وبعد التحويل تجد أن كود الاسمبلي للملف موجود بالشاشة الرئيسية للبرنامج ومعظم مفاتيح الاختصار تم تفعيلها كما يتضح من الشكل التالي:

The screenshot shows the URSoft W32Dasm Ver 10 interface. The assembly code is as follows:

```

:00455DA7 8D4C2410      lea ecx, dword ptr [esp+10]
:00455DAB E87FED0500    call 004B1B2F

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
|:00455D0D(C), :00455D68(C)

:00455DB0 5A2F          push 0000002F
:00455DB2 8D4C2414      lea ecx, dword ptr [esp+14]
:00455DB6 E8B9B90500    call 004B1774
:00455DBE 85C0          test eax, eax
:00455DD1 7E35          jle 00455DF4
:00455DBF 8B4C2410      mov ecx, dword ptr [esp+10]
:00455DC3 8D542438      lea edx, dword ptr [esp+38]
:00455DC7 8B49F8        mov ecx, dword ptr [ecx-08]
:00455DCA 2BC8          sub ecx, eax
:00455DCC 49            dec ecx
:00455DCD 51            push ecx
:00455DCE 52            push edx

```

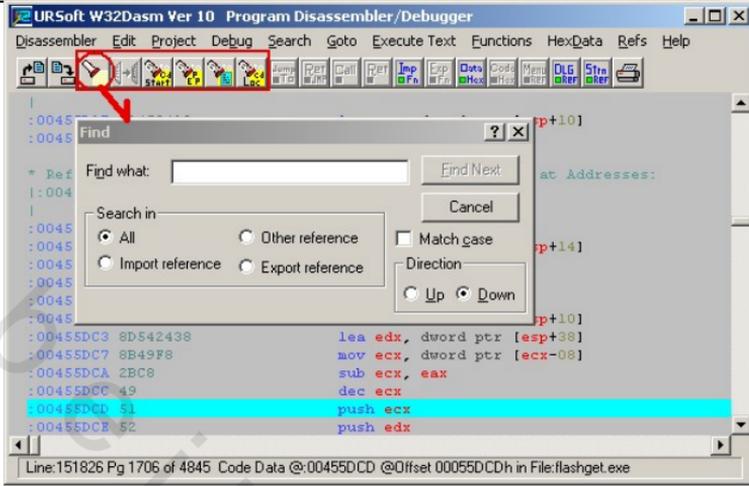
Annotations in the image:

- A**: Points to the instruction `lea ecx, dword ptr [esp+14]`.
- B**: Points to the instruction `push 0000002F`.
- C**: Points to the instruction `push ecx`.

لاحظ من الشكل التالي:

- ✦ المقطع A من الشاشة الرئيسية يحتوى على أوامر الاسمبلي
- ✦ المقطع B يحتوى على عنوان كل أمر بالملف
- ✦ المقطع C يحتوى على العنوان الحالي للأمر الذي يوجد فوقه شريط التركيز ويوجد بجانب العنوان الاوفست (عنوان محلى للملف) الرقم الفعلي للأمر بالبرنامج وعن طريقة يمكن تعديل الملف بسهولة ببرنامج Hview

كما يحتوى هذا البرنامج عدة وظائف هامه منها البحث عن نص داخل البرنامج عن طريق الضغط على مفتاح البحث في شريط مفاتيح الاختصار كما يتضح من الشكل التالي:



✦ المفتاح الذي يليه يستخدم لنسخ السطر الحالي

✦ المفتاح الثالث يستخدم للذهاب مباشرة إلى أول مقطع من لكود

✦ المفتاح الرابع الذهاب مباشرة إلى نقطة التحميل الخاصة بالملف

التنفيذي المشهورة بالاسم PE أو Program Entry Point

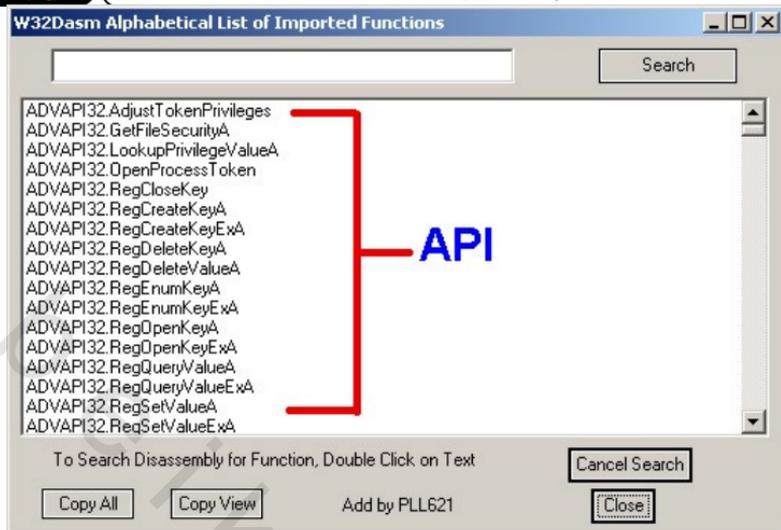
✦ المفتاح الخامس يستخدم للتنقل بسهولة بين صفحات الكود

✦ المفتاح السادس يستخدم للذهاب إلى اوفست أو عنوان محدد بالملف

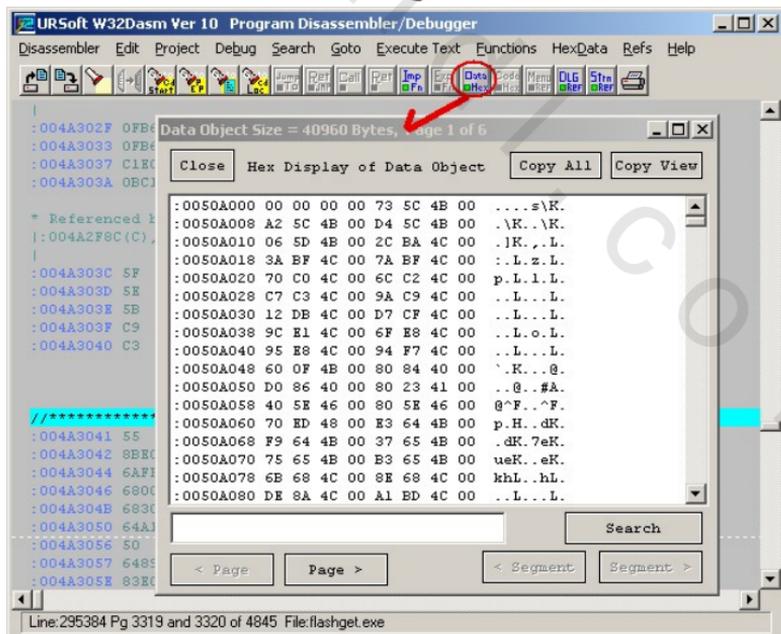
كما يحتوى البرنامج على مفتاحين الأول يسمى imports والثاني يسمى

exports ويظهران بالتحديد دوال API (دوال الويندوز الأساسية) المعرفة

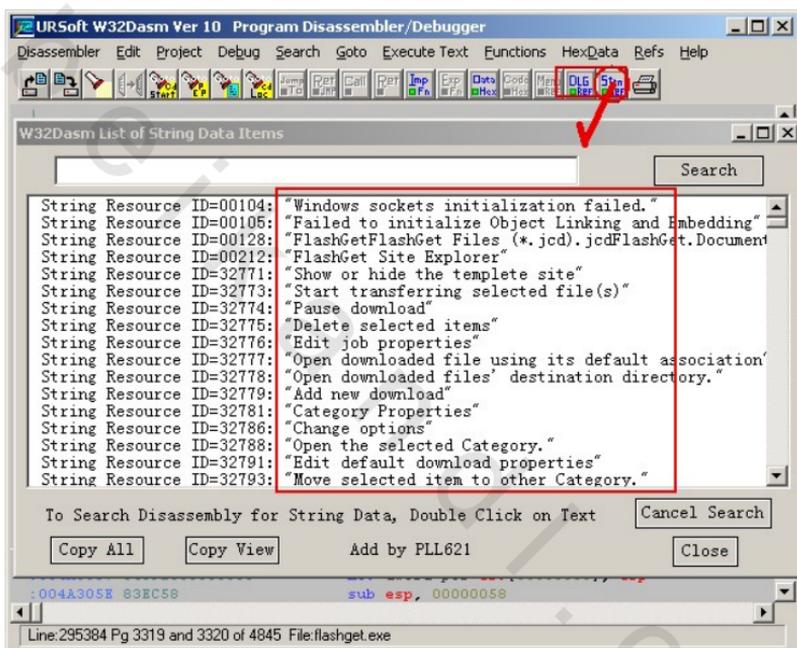
بالبرنامج أو المستخدمة من الويندوز كما يتضح من الشكل التالي:



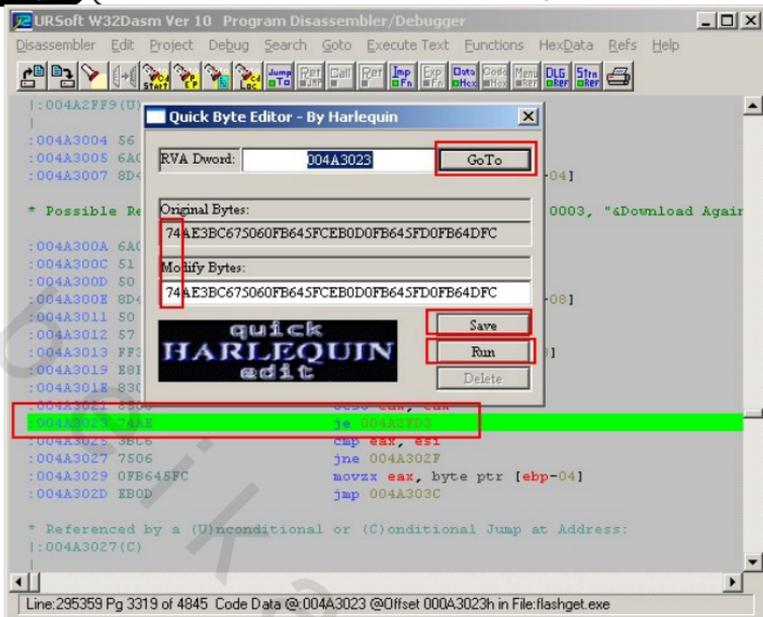
يمكنك أيضا من خلال هذا البرنامج رؤية البيانات المقابلة للاسمبلى بصورة الحدود السداسية عشر من خلال مفتاح يسمى hex display كما بالشكل:



ومن المميزات الهامة جدا لهذا البرنامج هو إمكانية الوصول إلى عنوان أو نص الرسائل التي توجد بالملف وهذه الخاصية هامة جدا للبحث عن رسائل تطلب السيريال مثلا ويمكن الوصول إلى هذه الرسائل عن طريق الضغط على مفتاح dialog references أو string data references كما يتضح بالشكل:



و من الإضافات الجديدة للبرنامج إمكانية تعديل الملف من داخله قم الآن بالوقوف على احد أوامر القفز ثم افتح القائمة edit واختر quick edit فيظهر دياالوج تستطيع من خلاله تغيير بايت القفز لكن بالنظام السداسي عشر كما يتضح من الشكل التالي:



لاحظ من الشكل انه يمكنك تعديل بيانات القفز مثلا من 74 إلى 75 ثم تقوم بحفظ الملف وتشغيله لاختبار تأثير التعديل على البرنامج و يمكننا أيضا إعادة هندسة برنامج بالذاكرة وبهذه الطريقة يتحول برنامج w32dasm إلى برنامج debugger أي يمكننا من الوقوف على مواضع معينة من الكود ويتم ذلك باختيار الأمر attach to an active process من القائمة debug وتظهر قوائم التحكم في سير البرنامج ومحتوى الذاكر من متغيرات أو مسجلات البرنامج.

Code Address : 77F767CE is in Module ntdll.dll

```

:77F767C5 mov edx, 7FFE0300
:77F767CA call edx
:77F767CC ret
DbgBreakPoint()
:77F767CD int 03
:77F767CE ret
DbgUserBreakPoint()
:77F767CF int 03
:77F767D0 ret
:77F767D1 mov eax, dword ptr [esp+04]
:77F767D5 int 03

```

Enable Documented API Details Copy  
 Enable UnDocumented API Details API  
 Enable Local Function Details Goto Address  
 Stop Auto On API Patch Code  
 Step Into "rep" Instruction Bypass Terminate

AutoStep Into F5 AutoStep Over F6 Step Into F7 Step Over F8 Pause Run

Eip:004BBA1B is in Module: flashget.exe

Regs	Copy	O	D	I	T	S	Z	A	P	C	#Processes:	#Threads:
EAX=00000001		<input type="checkbox"/>	001	002								
EBX=00000000												
ECX=000003E8												
EDX=77FE0304												
ESI=00513940												
EDI=00513970												
EBP=00513970												
ESP=0012FEEC												

Floating  Paused  SS Free  SS Into  Terminated

Source For Data Disp 1

Reg	Address	Value	Comment
eip	[esp-00000014]	- 004bbalb	..K.
eax	[esp-00000010]	- 00000001	....
ebx	[esp-0000000C]	- 00000000	....
ecx	[esp-00000008]	- 00000000	....
edx	[esp-00000004]	- 00000000	....
esi	[esp+00000000]	- 00000000	....
edi	[esp+00000004]	- 00513940	@9Q.
ebp	[esp+00000008]	- 004bb563	c.K.
esp	[esp+0000000C]	- 00513940	@9Q.
UA1	[esp+00000010]	- 00513940	@9Q.
UA2	[esp+00000014]	- 0012ffe0	

On Off Mode-> DWord Word Byte Code

Source For Data Disp 2

Disp 1 Address: 00000000 is Not in a Loaded Module.  
\*\*\*\*\* Data is NOT Accessible \*\*\*\*\*

UA1  
UA2  
Oper

Active DLLs

- ADVAPI32.dll
- COMCTL32.dll
- comctl32.dll

Proc Create Brk  
 Proc Exit Brk  
 Thrd Create Brk  
 Thrd Exit Brk  
 DLL Load Brk  
 DLL Unload Brk

Ev0043 Exiting Thread @ EIP:7ffe0304  
 Modify Data Goto Current Eip

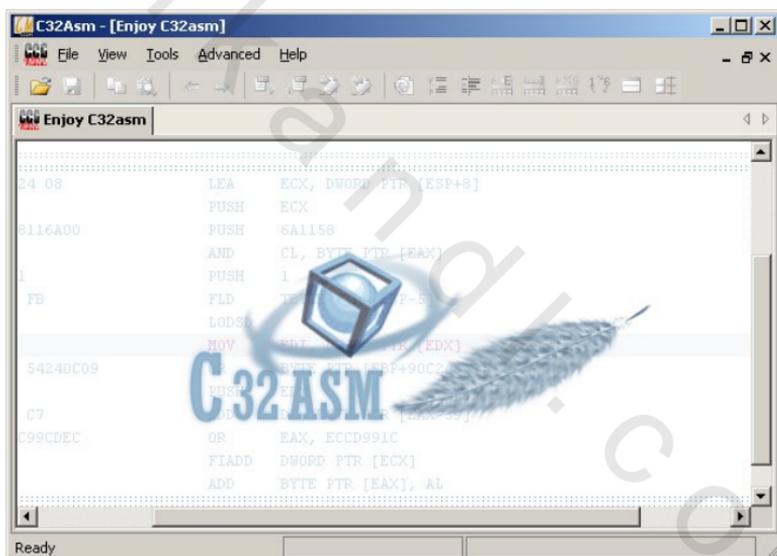
ملحوظة : للأسف هذا البرنامج لا ينفذ مع طرق الحماية الجديدة التي تقوم بتشغيل محتواها أو ضغطها كما أن بعض البرامج تقوم بفحص الذاكرة فإذا وجدت برنامج w32dasm محملا تقوم بإغلاق نفسها وأحيانا إغلاق الكمبيوتر كعقاب للكرامر .

و من نقاط الضعف فيه أيضا انه لا يستطيع متابعة البرامج المكتوبة بلغة فيجوال بيزيك حتى الإصدار السادس رغم أن هذا النوع من البرامج يعتبر أسهل لغة يمكن كسر حمايتها لذلك نستخدم دائما برنامج smartcheck مع برامج الفيجوال بيزيك

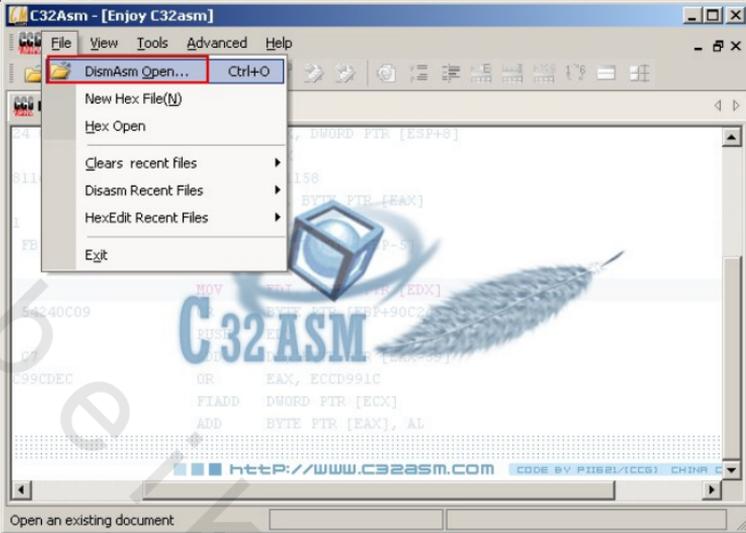
ويمكنك دائما معرفة نوع اللغة المستخدمة عن طريق برامج التحرير خصوصا التي تعتمد على تحرير الملفات بالنظام السداسي عشر ولكن الأسهل استخدام برنامج File Inspector وهو من الأدوات الأساسية للكرامر .

## برنامج C32ASM:

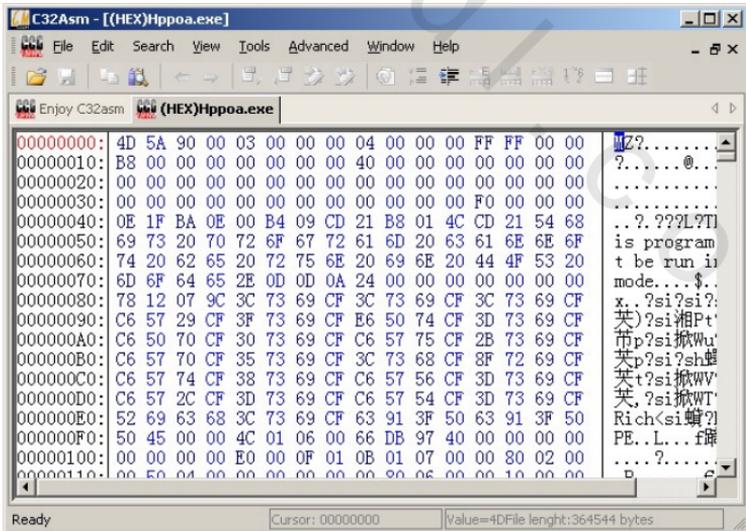
هذا البرنامج يقوم أيضا بنفس عمل برنامج W32Dasm لكن يضاف إليه واجهة استخدام سهلة وواضحة ورغم أن معظم استخدامات الكرارز يكون ببرنامج W32Dasm إلا أن هذا البرنامج لا يقل عنه وستقوم الآن بشرح البرنامج ويمكنك أن تقارن وتستخدم ما تريد يفتح البرنامج على نافذة ترحيب جميلة ويتكون مثل معظم البرامج من قوائم أوامر ومفاتيح اختصار تكون كلها غير فعالة حتى تقوم بفتح الملف التنفيذي المراد كسره.



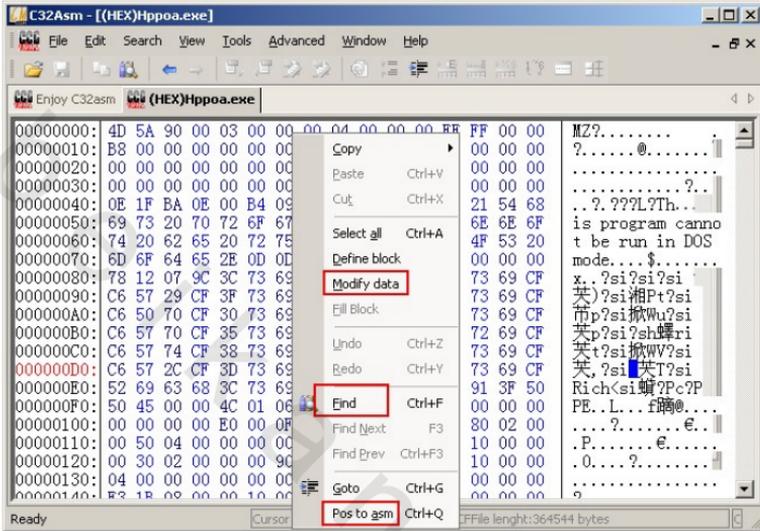
ولكي تقوم بفتح الملف اختار الأمر File DisAsm Open كما يلي:



أما إذا استخدمت الأمر File Hex Open فيتحول البرنامج محرر بالنظام السداسي عشر ويمكن أن تحтар أي ملف وتحريره في نافذة مستقلة.

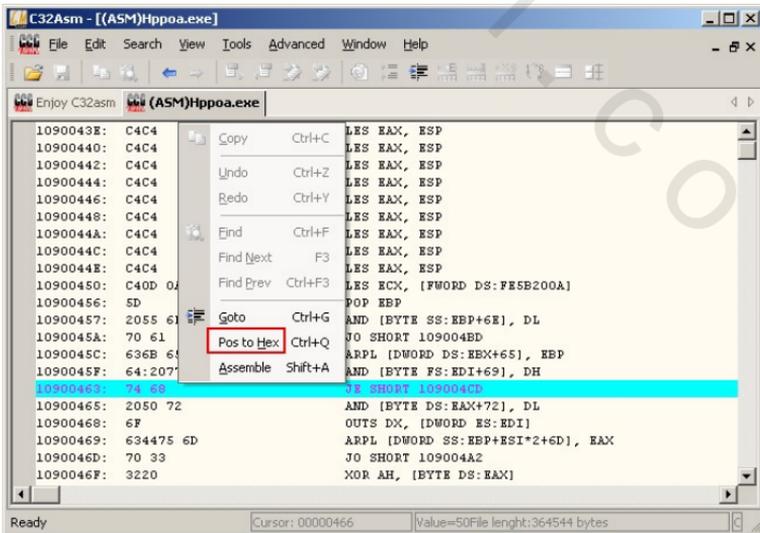


كما يمكنك عن طريق قائمة الأوامر المختصرة البحث عن أي نص أو تعديل محتويات الملف .

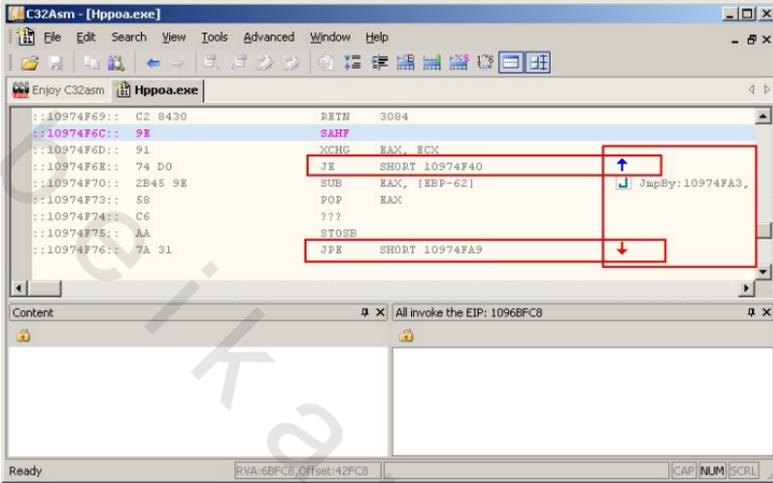


ويمكنك أيضا الذهاب إلى التعليمات الاسمبلى المكافئة للموقع الحالي عن طريق

أمر Pos to asm



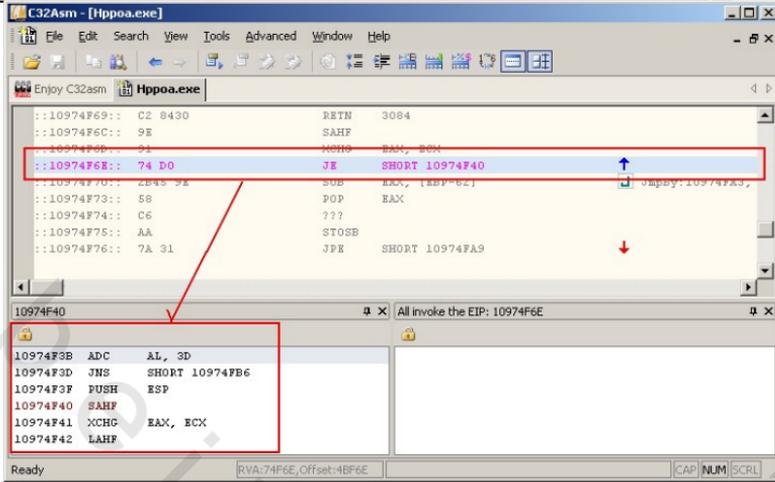
بالمثل يمكنك الرجوع إلى نافذة Pos to Hex من قائمة الأوامر المختصرة قم الآن بفتح الملف المراد كسره بالطريقة العادية ويجب أن ترى الشكل التالي:



يقوم البرنامج بأخذ بعض الوقت حتى يقوم بتحليل الملف وبعد ذلك ستجد نافذة disassembly هي النافذة الأساسية أمامك ويمكنك أن ترى أن مواقع القفز موضحة بأسهم ملونه وأيضا اتجاه القفز وإذا وجدت ايقونه J بجانب تعليمة اسمبلى فهذا معناه سطر تم القفز إليه ويعطيك البرنامج العنوان الذي تم القفز منه

و يمكنك التنقل بسهولة بين أوامر القفز كما يلي:

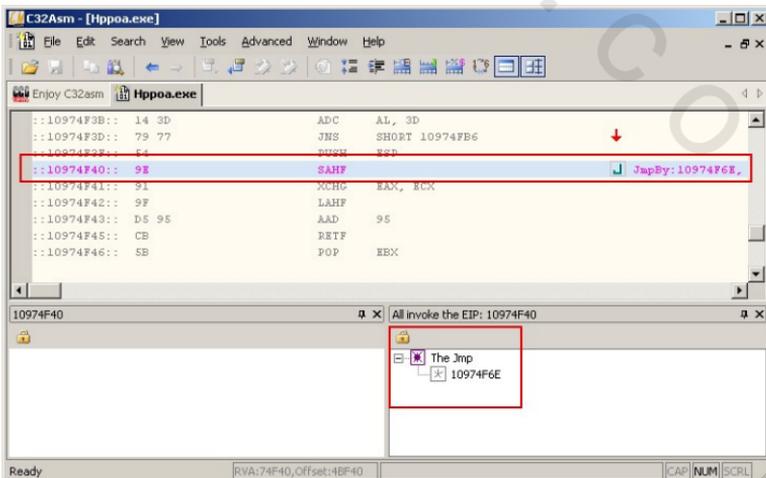
◀ قم أولا بالوقوف على أمر القفز حتى يصبح الأمر الحالي



لاحظ أن نافذة content تحتوي على تعليمات الاسمبلي التي سيتم القفز إليها ويمكنك الذهاب إلى هذا المكان بالضغط على مفتاح الاختصار Jmp أو Ctrl+J



و يجب الآن أن تجد مكانك تم تغييره إلى العنوان الجديد



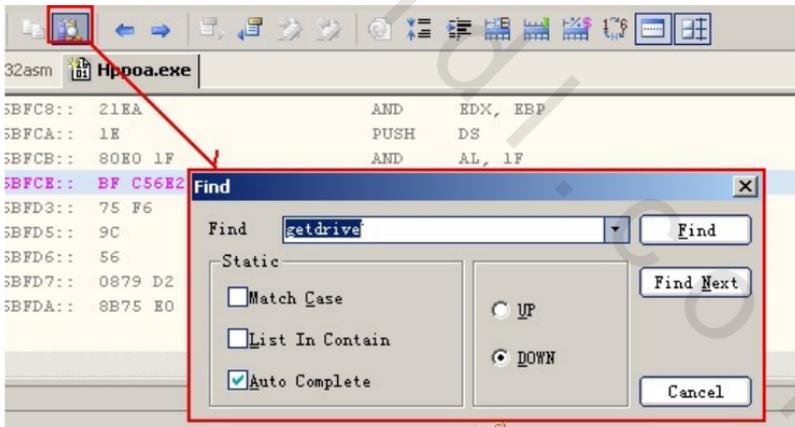
لاحظ أن البرنامج يقوم بإظهار أن هذا المكان تم القفز إليه ويكتب العنوان الذي تم القفز منه ويمكنك الرجوع إلى نفس المكان السابق بالضغط على المفتاح `ret` أو `jmp` أو `Ctrl+Shift+J`



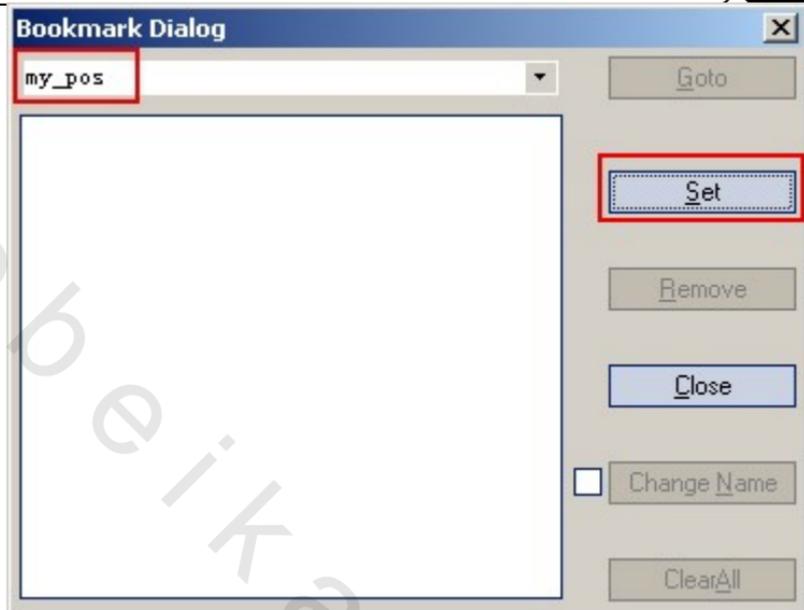
و يمكنك أيضا التنقل السريع بين الأماكن عن طريق مفتاح الذهاب إلى آخر مكان أو الذهاب إلى المكان التالي



للبحث عن أي نص أو أمر اسمبلى قم بالضغط على مفتاح البحث أو `Ctrl+F`



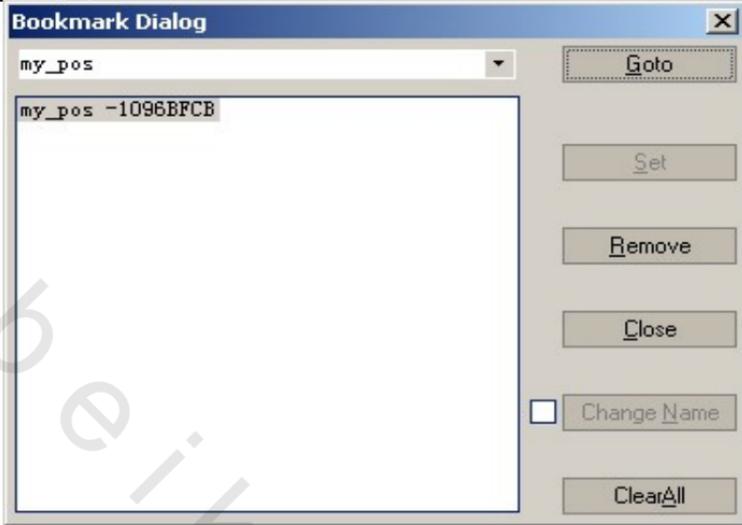
كامل يعطى البرنامج إمكانية لوضع مؤشر للتعليم ويتم ذلك عن طريق الأمر `Search | Bookmark` أو `Ctrl+M` فيتم فتح ديايوج للمؤشرات



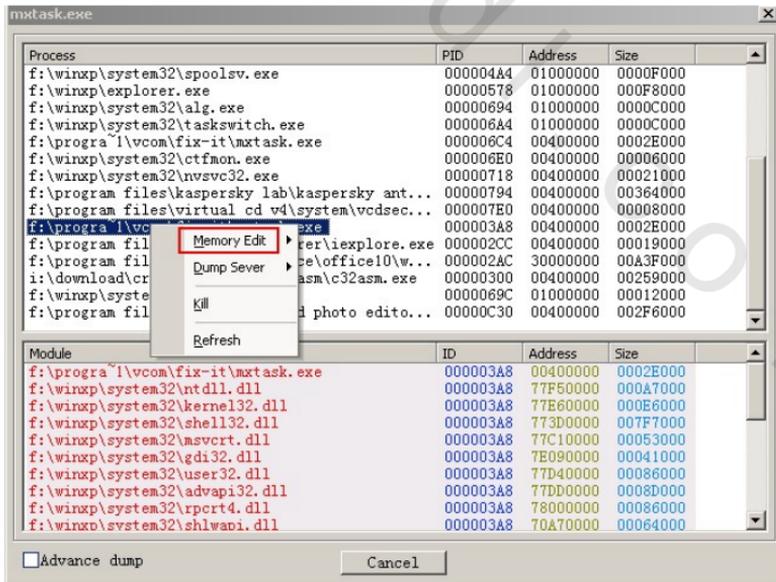
و يجب كتابة أي تعليق ثم الضغط على المفتاح set ويجب أن تشاهد المؤشر كما يلي:

::1096BFC7::	44	INC	ESP
::1096BFC8::	21EA	AND	EDX, EBP
::1096BFCA::	1E	PUSH	DS
0x77::1096BFCB::	80E0 1F	AND	AL, 1F
::1096BFCE::	BF C56E20FF	MOV	EDI, FF206EC5
::1096BFD3::	75 F6	JNZ	SHORT 1096BFCB
::1096BFD5::	9C	PUSHFD	
::1096BFD6::	56	PUSH	ESI

و يمكنك التنقل بين المؤشرات بالمفاتيح F2 للتالي أو Ctrl+F2 للسابق ويمكن أيضا تنفيذ ذلك بفتح الديالوج السابق واختيار نقطة المؤشر والضغط على المفتاح Goto أو لإزالة المؤشر اضغط على المفتاح remove

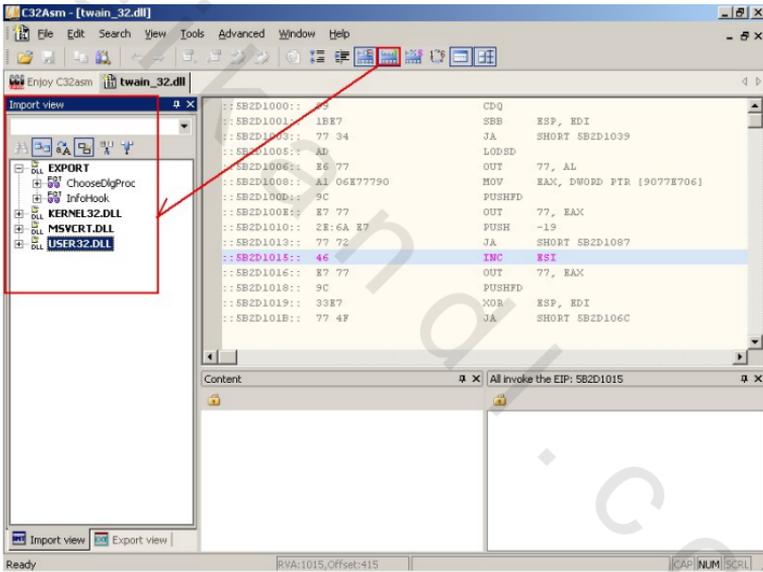


و يمكنك أيضا عن هذا البرنامج رؤية الذاكرة الخاصة بأحد البرامج المحملة وتقيفها ويتم ذلك عن طريق الأوامر **Tools | Process edit**

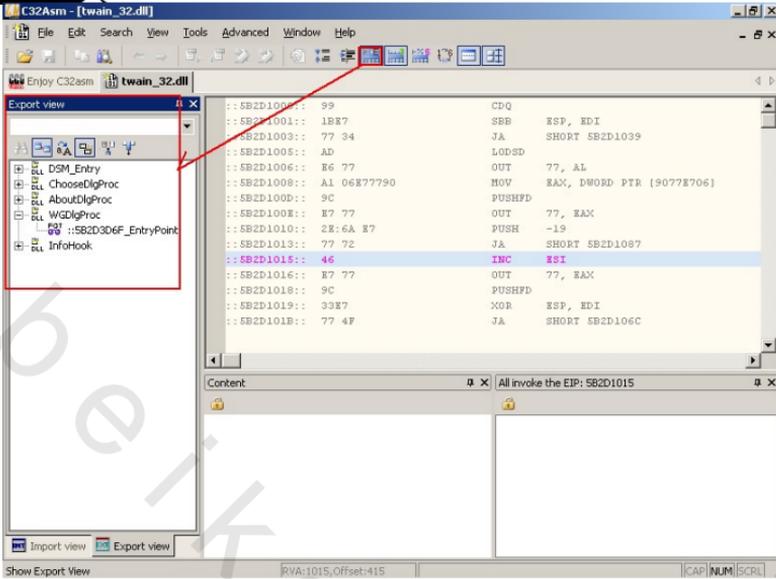


وعن طريق قائمة الأوامر المختصرة يمكنك اختيار Memory Edit ويمكنك بعد ذلك اختيار أي جزء من الذاكرة تريد تعديله وسيتم فتح محرر بالنظام السداسي عشر ، كما يمكنك أيضا تفرغ محتويات ملف عن طريق الأمر Dump Server واختيار أي جزء تريد تفرغها تعطى القائمة View العديد من الإمكانيات الهامة منها:

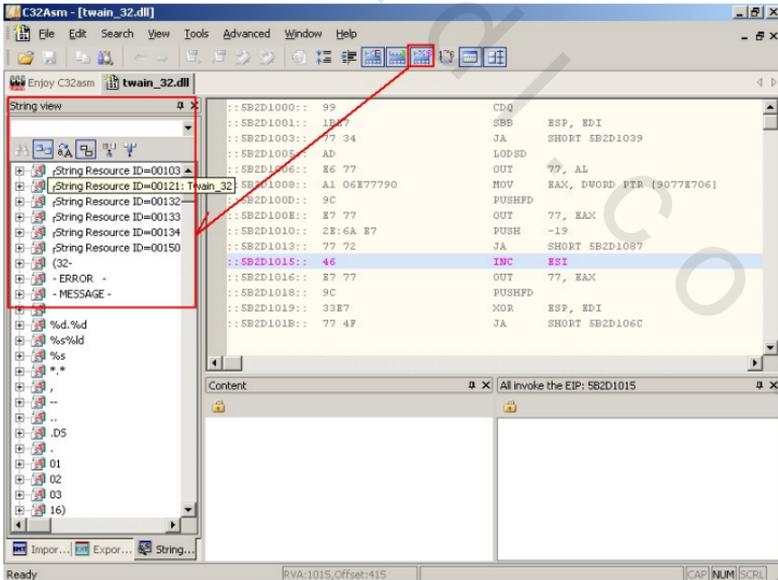
- رؤية دوال API التي يستخدمها الملف عن طريق الأمر View | Import



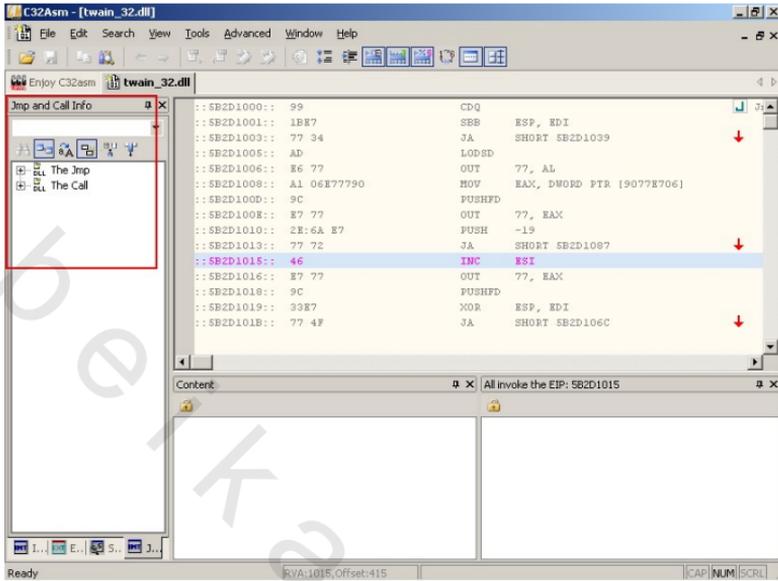
- رؤية الدوال التي يقوم الملف بتصديرها عن طريق الأمر View | Export



- رؤية النصوص التي يحتويها الملف Strings | View



- رؤية كل عناوين القفز والنداء Jmps and calls | View



ومن المزايا الهامة في هذا البرنامج والتي لا توجد ببرنامج W32Dasm هي إمكانية فتح أكثر من ملف في نفس الوقت.



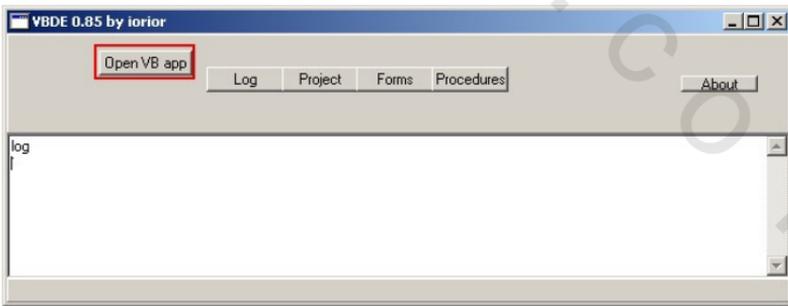
## برامج إعادة التجميع Decompile

كما ذكرنا فإن كل لغة يتم فيها ترجمة الأوامر المكتوبة بها إلى لغة الاسمبلي عن طريق مترجم يسمى المعالج compiler وتختلف كل لغة في طريقة المعالجة باختلاف المعالج التي تستخدمه فمثلا معالج فيجوال بيزيك يقوم بترجمة الكود سطر سطر بينما معالج السي يقوم بترجمة كل الكود ويقوم بإظهار ناتج عملية الترجمة في النهاية.

وهناك أيضا نوع آخر من المعالجات وهي المسئولة عن إنتاج برامج التنصيب وهناك أيضا نوع آخر من المعالجات وهي المسئولة عن إنتاج برامج التنصيب مثل setup install shield وغيره من برامج التنصيب وأحيانا يقوم برنامج التنصيب بالسؤال عن كلمة سر اثنا التنصيب لذلك علينا أن نقوم بإعادة تجميع الملف لمعرفة كلمة السر وفيما يلي أهم البرامج التي تمكننا من أداء ذلك.

### برنامج VBDE:

وهو من البرامج البسيطة جدا وكما ترى فإنه يستخدم لإعادة ترجمة برامج فيجوال بيزيك ويتكون البرنامج من عدة مفاتيح كل منها لعرض نوع معين من وحدات الفيجوال بيزيك

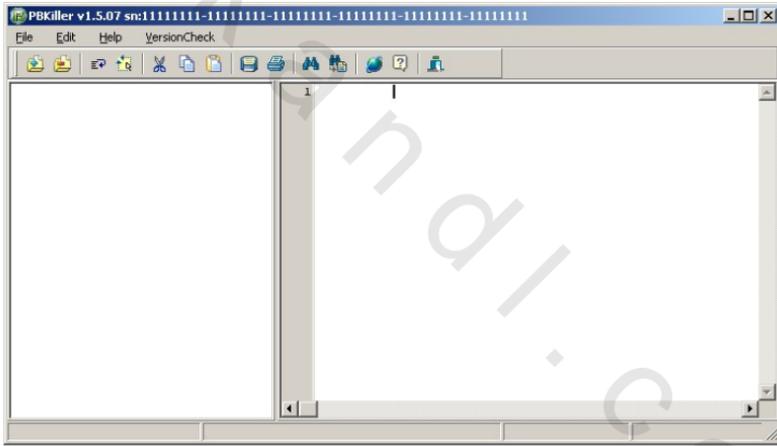


أولا يجب أن تقوم بفتح برنامج VB من المفتاح Open VB app ثم قم باختيار Project لترى الكود الأساسي الخاص بالمشروع.

والمفتاح forms يمكنك من رؤية جميع النماذج أو النوافذ الموجودة بالبرنامج.  
والمفتاح Procedures لرؤية الإجراءات والإحداث التي تحتوى على كود vb.

برنامج Pbkiler:

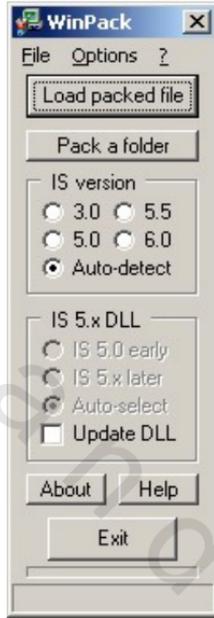
هذا البرنامج متخصص لبرامج power builder الإصدارات 6 - 7  
- 8 - 9 وإذا كنت لا تعرف هذا البرنامج فهو عبارة عن لغة برمجة تعتمد على  
SQL وتستخدم قاعدة بيانات Sybase  
و يتكون البرنامج من قوائم ومفاتيح اختصار كما نرى من النافذة الافتتاحية  
التالية:



وعندما تقوم بفتح ملف مكتوب بلغة power builder يتم عرض جميع  
المعلومات الخاصة بالكود والنوافذ المستخدمة وهكذا.

هذا البرنامج متخصص لفك تجميع ملفات برنامج install shield

الشهير ويتكون من مفاتيح أساسيه هي :



قم بفتح ملف \*.cab أو \*.hdr لبرنامج التنصيب من المفتاح Load

package file وسيقوم البرنامج بالتعرف على الإصدار المناسب للفك وكما

ترى فهذا البرنامج يمكنه فك تنصيب الإصدارات 3 - 5 - 5.5 - 6

## أدوات التحرير Editors

أدوت التحرير من الأدوات الهامة للتعديل في ملفات البرامج وفيما يلي نستعرض أهم هذه البرامج وإمكاناتها.

## برنامج Hackers View:

من الأدوات العريقة في مجال كسر حماية البرامج وعادة يستخدم مع برامج disassembly وهذا البرنامج رغم انه يعتمد على الدوس الا انه في غاية القوة ويستطيع التعامل مع جميع أنواع الملفات.

```

I:\download\crack tutorials\hiew7.2\hiew32.exe
I:\download\crack tutorials\hiew7.2
..
>UP--DIR|Attr--|Date--|Time--
dexen32.exe 23552 a.. 12-04-2001 19:03:11
edump32.exe 53248 a.. 21-03-2005 10:09:11
files.lst 814 a.. 23-12-2004 00:40:23
file_id.diz 1104 a.. 31-05-2005 17:06:23
hiew.vnn 28156 a.. 01-04-1998 18:46:06
hiew.xlt 1584 a.. 29-01-1997 13:01:03
hiew32.exe 160768 a.. 27-07-2005 06:40:28
hiew32demo.txt 514 a.. 31-05-2005 17:10:02
hiew4657.key 395 a.. 13-04-2005 08:33:05
hiew7.hlp 34928 a.. 07-06-2005 10:53:06
hiew7.ini 7936 a.. 23-12-2004 01:24:13
hiew7.ord 305684 a.. 31-07-2003 17:07:28
hiew_en.txt 23160 a.. 06-07-2005 11:07:02
hiew_ru.txt 26872 a.. 06-07-2005 11:10:03
ldump32.exe 38912 a.. 05-11-2004 18:38:00
license.txt 2760 a.. 26-01-2005 10:25:25
  
```

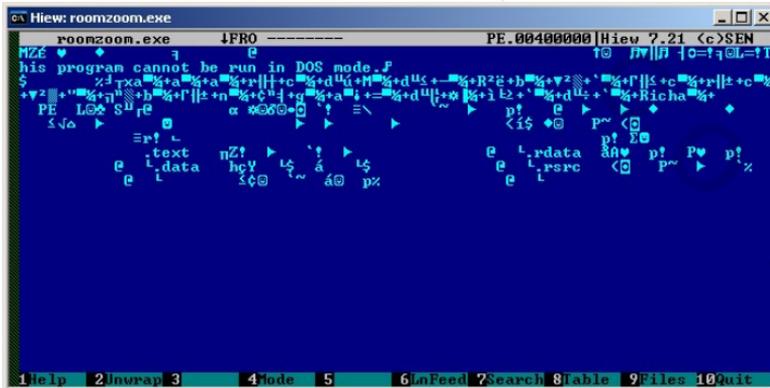
ويتكون البرنامج كما نرى من الصورة من عدة أعمده يقوم فيها البرنامج بعرض الملفات فيعرض في أول عمود اسم الملف والثاني الحجم والثالث خصائص الملف والأخير تاريخ ووقت إنشاء الملف.

كما يتكون من عدة مفاتيح في أسفل البرنامج يمكن تنفيذ هذه الأوامر باستخدام مفاتيح الوظائف .

لكي تستطيع الانتقال إلى الدليل الذي يوجد به الملف المراد تعديله قم بالضغط على المفاتيح Alt+F1 فتظهر نافذة يمكن اختيار منها حرف المشغل المراد استعراضه.



بعد ذلك انتقل إلى الملف المراد تعديله بمفاتيح الأسهم ومفتاح الإدخال وعندما تصل للملف قم بالضغط على مفتاح الإدخال.



فيتم فتح الملف وتراه بالشكل النصي ASCII قم بالضغط على مفتاح الإدخال مره أخرى لترى الملف بالشكل السداسي عشر.



```

roomzoom.exe 4FRO ----- a16 PE.00400089 |Hiew 7.21 <c>SEN
0040005D: 6E outsb
0040005E:
0040005F:
00400060:
00400062:
00400063:
00400064:
00400065:
00400066:
00400067:
00400068:
00400069:
0040006A:
0040006B:
0040006C:
0040006E:
0040006F:
00400070:
00400071:
00400072:
00400073:
00400074:
00400075:
00400076:
00400077:
00400078:
00400079:
0040007A:
0040007B:
0040007C:
0040007E:
0040007F:
00400080:
00400081:
00400082:
00400083:
00400084:
00400085:
00400086:
00400087:
00400088:
00400089: DFAC2B61 fild q,[edi+1612B]
1|help 2|hidden 3|byName 4|byExt 5|byLine 6|size 7|insert 8|Revers 9|Filter

```

للبحث في الملف يمكنك الضغط على المفتاح F7 وكتابة النص المراد البحث عنه بصيغة ASCII أو بالصيغة السداسية.

```

roomzoom.exe 4FRO ----- a32 PE.0040013F |Hiew 7.21 <c>SEN
0040013F: 0000 add [eax],al
00400141: 60 pushad
00400142: 7E00 jle .000400144 <1>
00400144: 0010 add [eax],dl
00400146: 0000 add [eax],al
00400148: 007021 add [eax][21],dh
0040014B: 0000 add [eax],al
0040014D: 004000 add [eax][00],al
[Forward *File *Case 1]
ASCII:
Hex:
0040015E: 0000 add [eax],al
00400160: 0400 add al,0
00400162: 0000 add [eax],al
00400164: 0000 add [eax],al
00400166: 0000 add [eax],al
00400168: F3 repe
00400169: FB sti
0040016A: 7F00 jg .00040016C <2>
1|help 2|Direct 3|Area 4|GoLast 5|6|7|In 8|9|10

```

وللذهاب إلى أوفست أو عنوان محدد قم بالضغط على المفتاح F5 واكتب العنوان ثم اضغط مفتاح الإدخال ويتم الذهاب إليه على الفور.



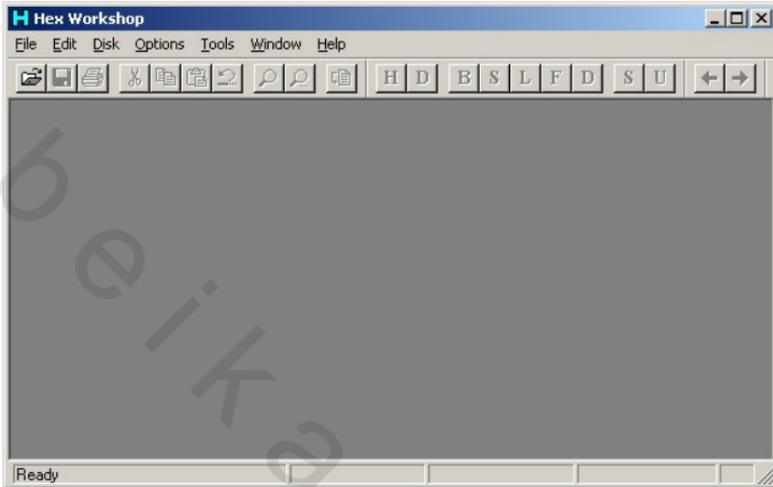


```

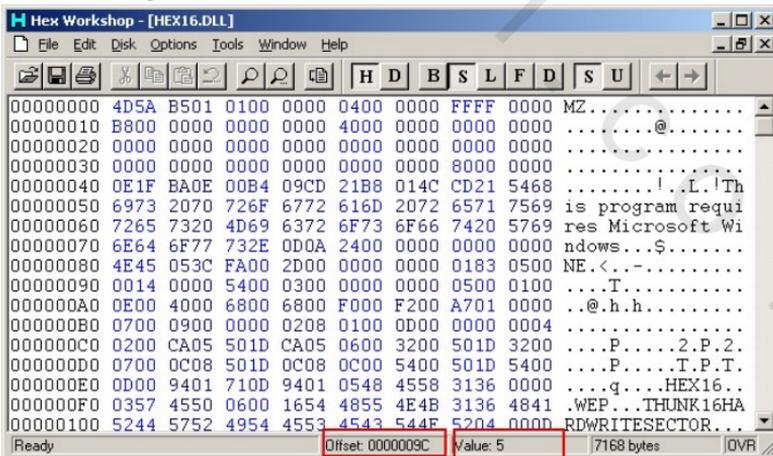
c:\> Hiew: AIRXONIX.EXE
AIRXONIX.EXE 1FWO ----- a16 PE.00400060 |Hiew 7.21 (c)SEN
.0040005D: 6E outsb
.0040005E: 6E outsb
.0040005F: 6F
0
0
Count of sections: 10
Symbol table: 0
Size of option: 0
Linker version: 10
Export Name RVA Size
Export 00000000 00000000
Import 0000173C 00000030
Resource 00006000 00002300
Exception 00000000 00000000
Security 00000000 00000000
Inte1386
0:22:22 2000
er 010B
4.00
0000158: RVA 00000000/0
000015C: $ize 00000000/0
Sound Import 00000000 00000000
Import Table 00004000 00000008
Delay Import 00000000 00000000
COM Runtime 00000000 00000000
(reserved) 00000000 00000000
000/00001000
Stacksum 16
0
0
00400083: F0
00400084: F8
00400085: B524
mov ch,024 ; '$'
1 Help 2 3 Edit 4 Index 5 G/L Loc 6 ? 8 9 Update:0

```

من البرامج الخفيفة والسريعة ويمكنه تعديل الملفات ذات الحجم الكبير



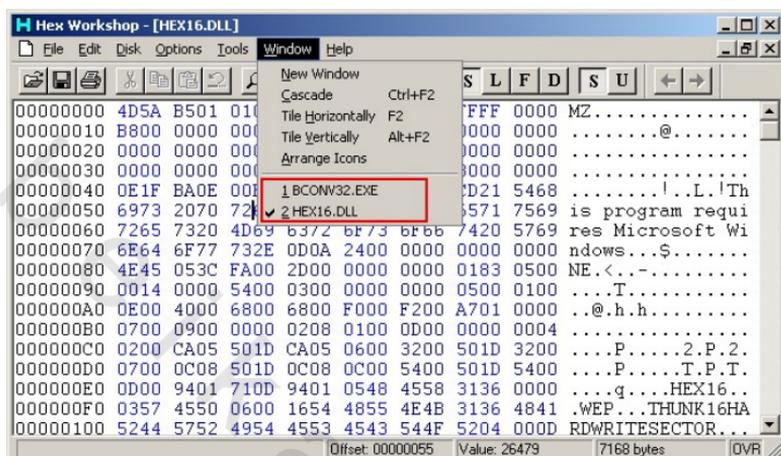
قم بفتح الملف المراد التعديل فيه بالا ومر **File | Open** ويقوم البرنامج بفتح نافذة مستقلة للملف يمكنك التعديل فيها مباشرة بالنظام السداسي.



كما يمكنك معرفة الاوفست والقيمة الحالية له من شرط الحالة بأسفل البرنامج

ومن مزايا هذا البرنامج إمكانية فتح أكثر من ملف والتنقل بينهم عن طريق نافذة

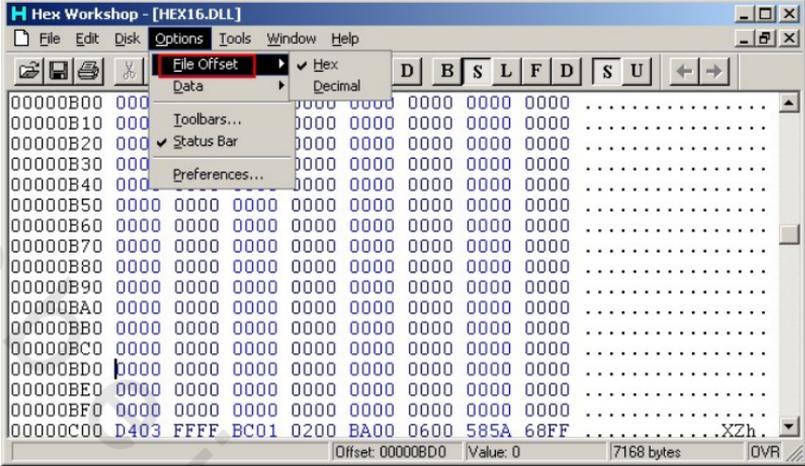
Window



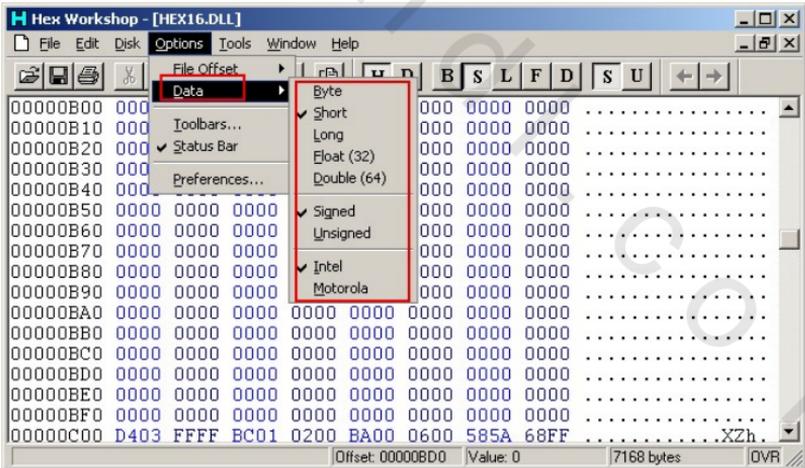
للبحث في البرنامج قم بالضغط على  $Alt + F3$  ويمكنك من خلال ديايوج البحث كتابة نص ASCII أو أرقام بالنظام السداسي.



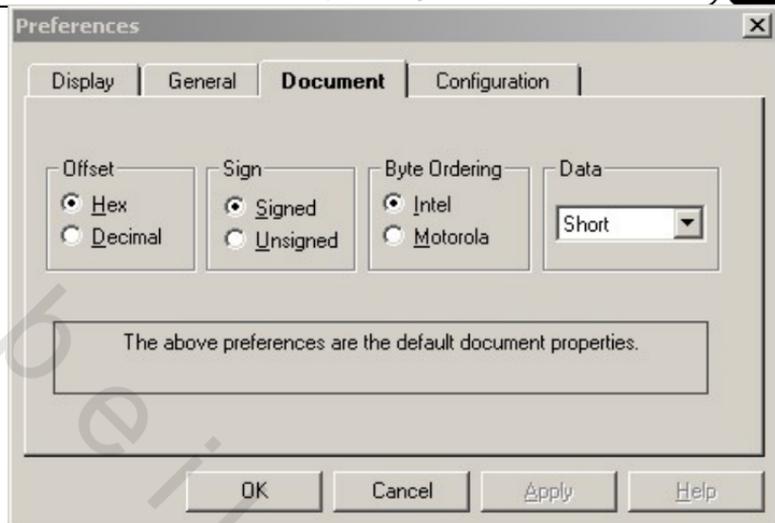
ومن قائمة Option يمكنك تغيير طريقة عرض البيانات في البرنامج فيمكنك عرض العناوين بالنظام العشري أو السداسي.



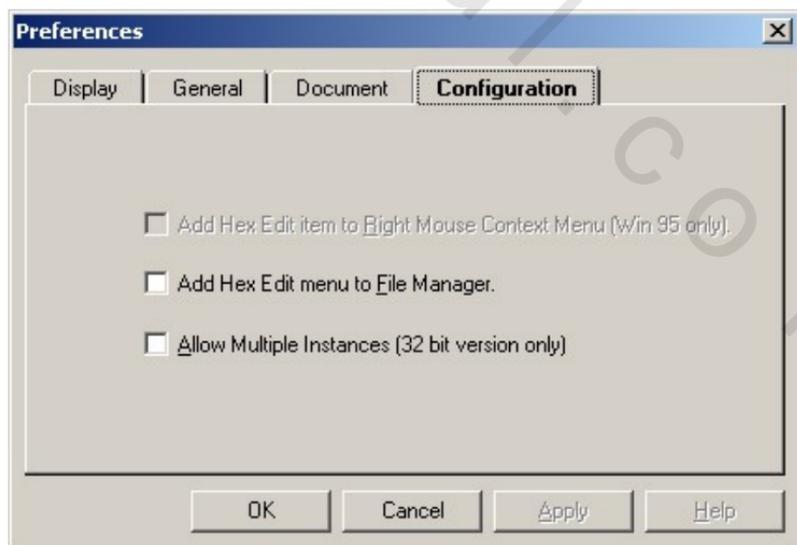
كما يمكنك التحكم في عرض بيانات الملف نفسه من الأمر Data واختيار نوع البيانات المراد.



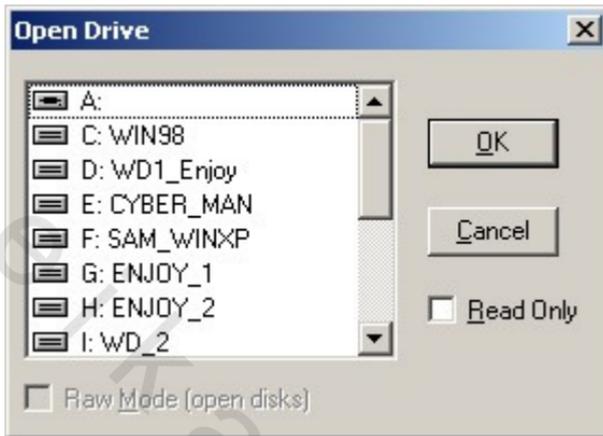
ويمكنك اختيار الشكل الافتراضي للملف من خلال الأمر Preferences واختيار الصفحة Document.



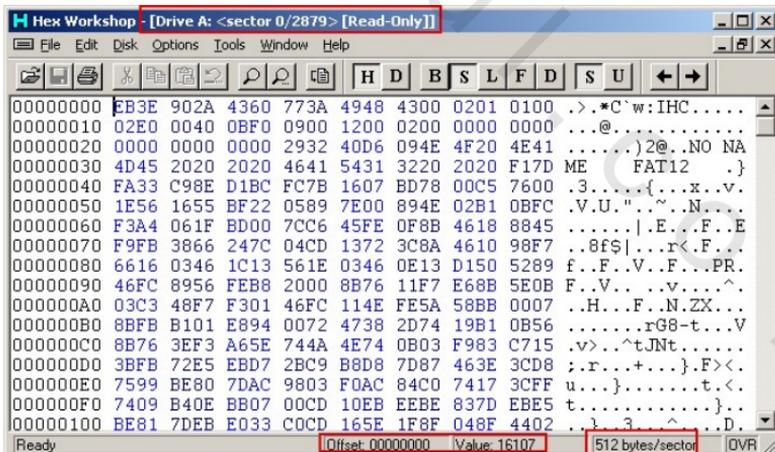
ويمكنك وضع أمر للتحريير بواسطة هذا البرنامج في قائمة الأوامر المختصرة الخاصة بالويندوز عندما تقوم باختيار أي ملف ويتم ذلك من الصفحة configuration



و يمكنك أيضا عن طريق هذا البرنامج فتح وتعديل احد مشغلي الكمبيوتر ويتم ذلك من الأوامر Disk | Open Drive واختيار احد المشغلات.

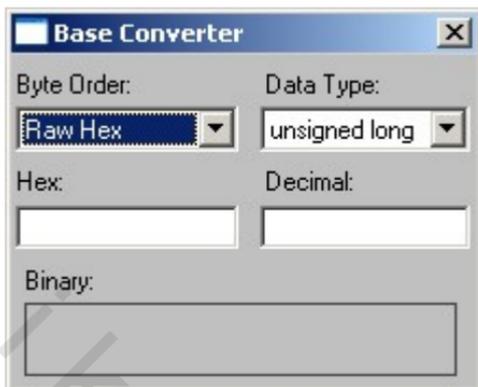


و يمكنك التعديل في sector المشغل نفسه



يحتوى البرنامج أيضا على عدة أدوات هامة وهى:

- التحويل بين النظام العشري والسادسي ويتم ذلك من قائمة Tools | Base Converter

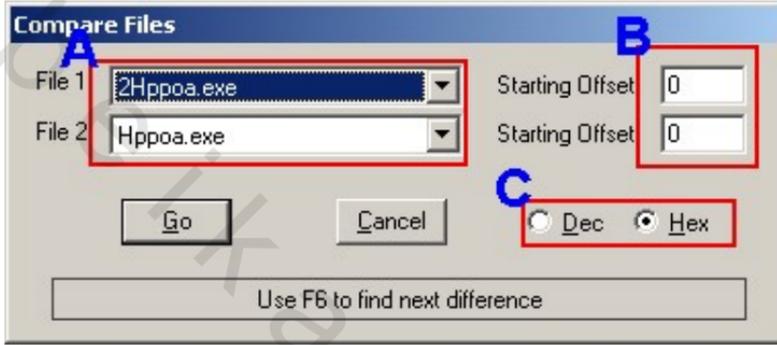


- آله حاسبه بالنظام السادسي Tools | Hex calculator

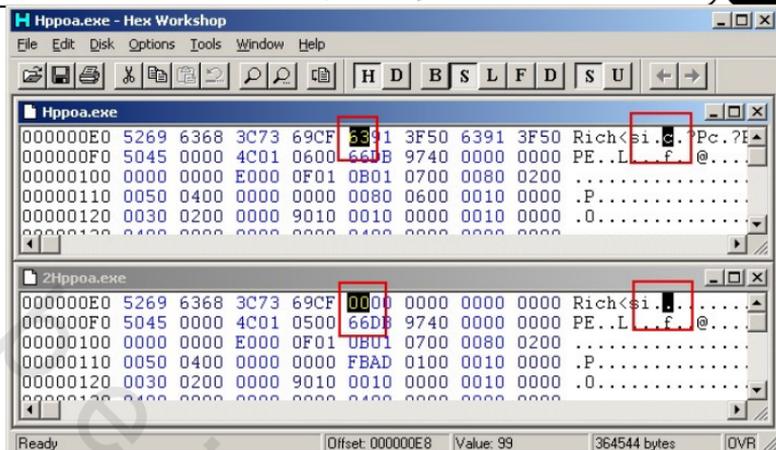


يمكنك عن طريق هذه الأداة إجراء عمليات حسابيه على حدود سداسيه ويظهر الناتج بالنظام السادسي عشر.

من المزايا الهامة لهذا البرنامج إجراء مقرنه سريعة على ملفين ولكي يمكنك القيام بذلك قم أولاً بفتح الملفين المراد مقارنتهم ثم افتح دياالوج المقارنة من الأوامر Tools | Compare



1. قم باختيار الملفين المراد مقارنتهم من بين الملفات المفتوحة.
  2. قم باختيار مكان بدء المقارنة
  3. نوع إظهار البيانات سداسي أو عشري
- اضغط على مفتاح ok ويقوم البرنامج بالوقوف على أول مكان يوجد به الاختلاف ولكي ترى المقارنة بوضوح بين الملفين قم باختيار الأمر Window | Tile Horizontally أو F2



ولكي ترى مزيد من الاختلاف قم بالضغط على المفتاح F6  
قائمة Help:

تتميز قائمة Help في هذا البرنامج بتقديم معلومات مفيدة عن أنواع البيانات وجدول ASCII فمثلا لكي ترى كود الحروف بالنظام العشري والسداسي افتح

القائمة Help | ASCII Table

Dec	Hex	Char	Code
0	00	€	NUL
1	01	€	SOH
2	02	€	STX
3	03	€	ETX
4	04	€	EOT
5	05	€	ENQ
6	06	€	ACK
7	07	€	BEL
8	08	€	BS
9	09	€	HT
10	0A	€	LF
11	0B	€	VT
12	0C	€	FF
13	0D	€	CR
14	0E	€	SO
15	0F	€	SI
16	10	€	SLF

ولكي ترى أنواع البيانات المختلفة ومدى كل نوع قم باختيار الأوامر | help

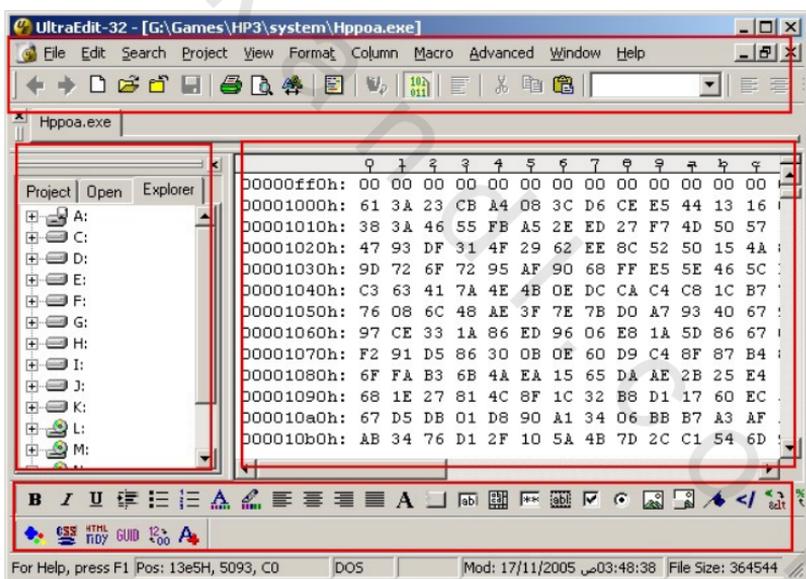
## Data Types

Type Name	Bytes	Range of Values
(signed) byte	1	-128 to 127
unsigned byte	1	0 to 255
(signed) short	2	-32,768 to 32,767
unsigned short	2	0 to 65,535
(signed) long	4	-2,147,483,648 to 2,147,483,647
unsigned long	4	0 to 4,294,967,295
float	4	3.4E +/- 38
double	8	1.7E +/- 308
long double	10	1.2E +/- 4932

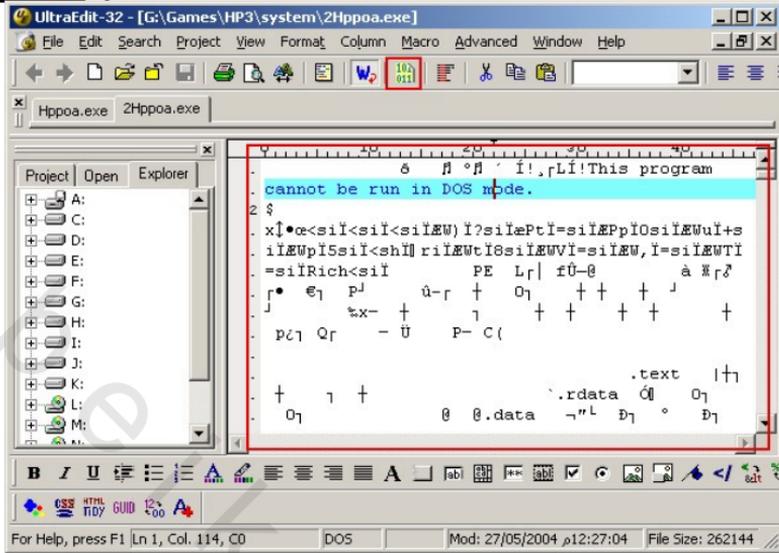
## برنامج Ultra-Edit:

هذا البرنامج اكبر حجما من برنامج Hex Workshop ويحتاج لتصيبه ولكن يوجد به العديد من المزايا الاحترافية تجعله أكثر برامج التحرير قوه ويستخدم بشكل أساسي للتعديل في الأجزاء الالكترونية وتحميلها على رقاقات IC ولكننا هنا سنركز على استخدامه للكراك.

النافذة الافتراضية للبرنامج تحتوى على قوائم الأوامر ومفاتيح اختصار علوية وسفلية وإذا قمت من قبل بفتح ملف فيقوم البرنامج تلقائيا باعداه فتحه مره أخرى في المرة القادمة التي تقوم فيها بتشغيل البرنامج كما يحتوى في الجزء الأيسر على لوحه تحتوى على ثلاث صفحات.



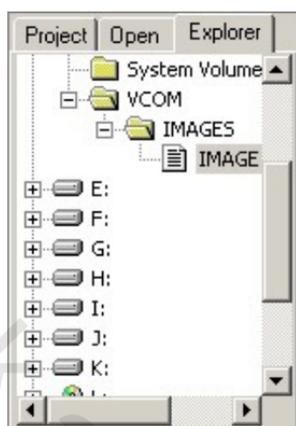
قم أولاً كما تعرف باختيار ملف وفتحه من القائمة File | Open ويتم فتح الملف في نافذة والتعديل فيه مباشرة ويمكنك عرض الملف بشكل نصي عن طريق الأوامر Edit | Hex function | Hex Edit وبالعكس.



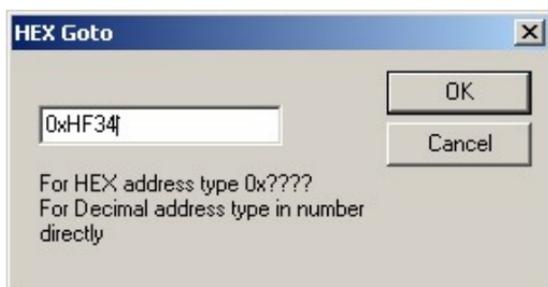
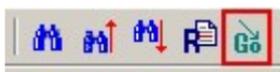
- وتحتوى لوحة الأدوات صفحة تسمى Open يمكنك من خلالها اختيار آخر ملفات قمت بفتحهم بسرعة.



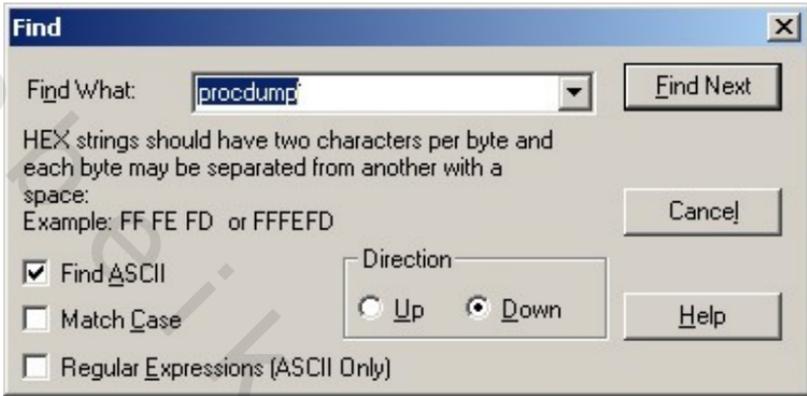
كما يمكنك فتح الملف الذي تريده مباشرة من الصفحة Explorer باختيار رمز المشغل واختيار الملف.



- بالنسبة لإمكانيات البحث فهذا البرنامج يمكنه البحث والتنقل في الملف بطرق كثيرة فيمكنك الذهاب مباشرة إلى سطر معين عن طريق كتابة العنوان offset بالنظام السداسي مثلا ويمكنك فتحه من القائمة Search | goto line



أما إذا أردت البحث عن نص محدد أو كود سداسي فقم باختيار الأوامر  
Alt+F3 أو Search | Find

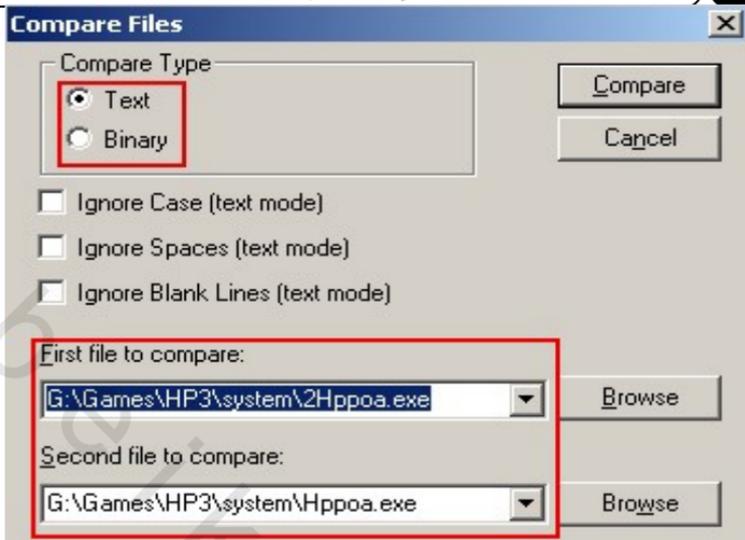


كما يمكنك التنقل بين نتائج البحث عن طريق مفاتيح الاختصار التالية:

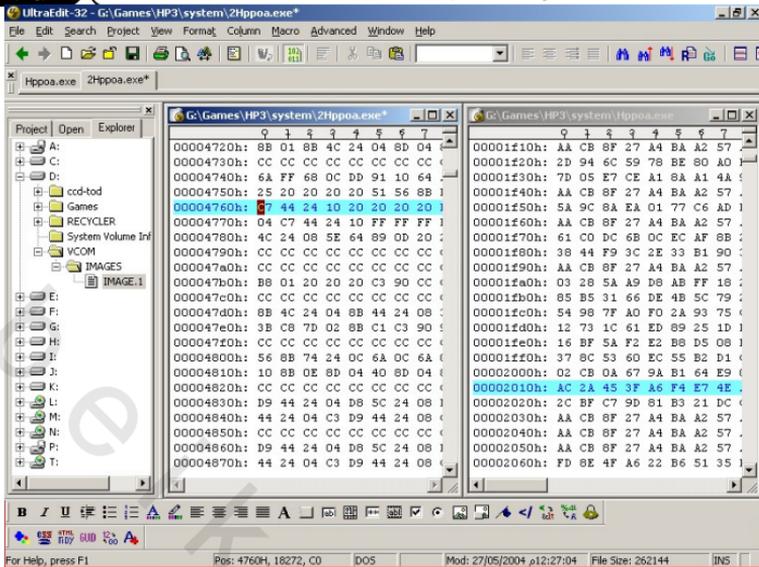


كما يحتوي البرنامج على إمكانية لتسجيل مجموعه من الإحداثيات للبرنامج وتكرارها ويتم ذلك من قائمة Macro كما يمكنك تغيير شكل النصوص مثل الخط والألوان من القائمة Format

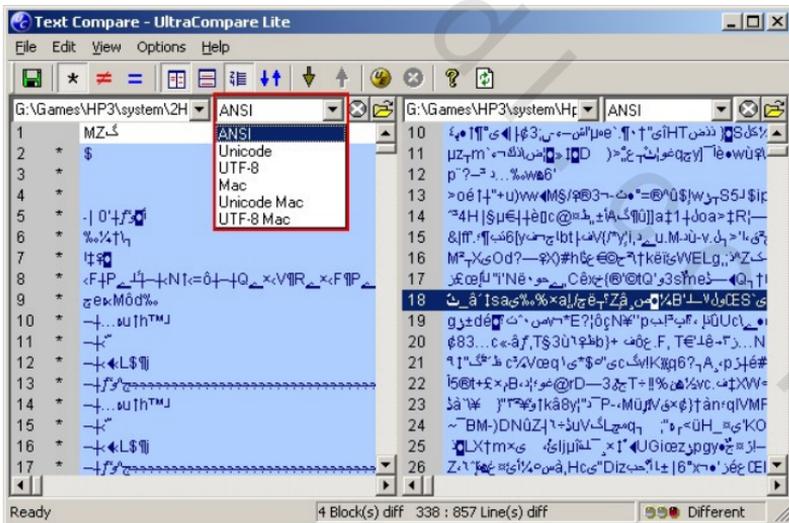
ولكي تقوم بمقارنة ملفين قم باختيار الأوامر File | Compare Files



قم باختيار نوع المقارنة نصي أو ثنائي وتأكد من اختيار الملفين واضغط على المفتاح Compare ويقوم البرنامج تلقائياً بفتح النافذتين وإظهار أوجه الاختلاف.



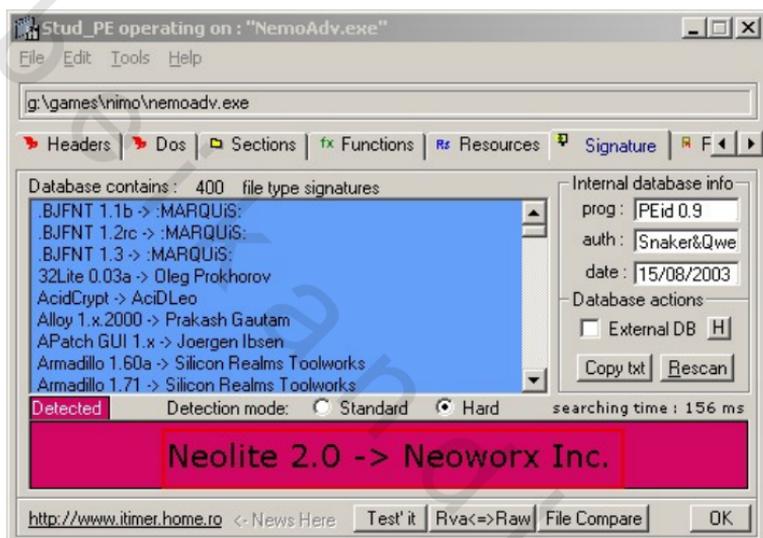
كما يقوم البرنامج بفتح الملفين بشكل نصي ويعطى أكثر من اختيار لتشكيل النص المعروف.



ويحتوى البرنامج أيضا على الكثير من الإمكانيات التي تناسب مختلف الملفات النصية مثل ملفات HTML ولغات البرمجة وغيرها وتتعدى هذا الإمكانيات حدود هذا الكتاب .

## برامج UnPacker

هذه المجموعة تعطي الإمكانية لفك تشفير وضغط الملفات بالطرق الشهيرة مثل ASPack و PE Shrink و Armadillo و Neolite وغيرها ويجب عليك أولاً معرفة نوع التشفير ويتم ذلك ببرنامج Peid أو STUD\_PE

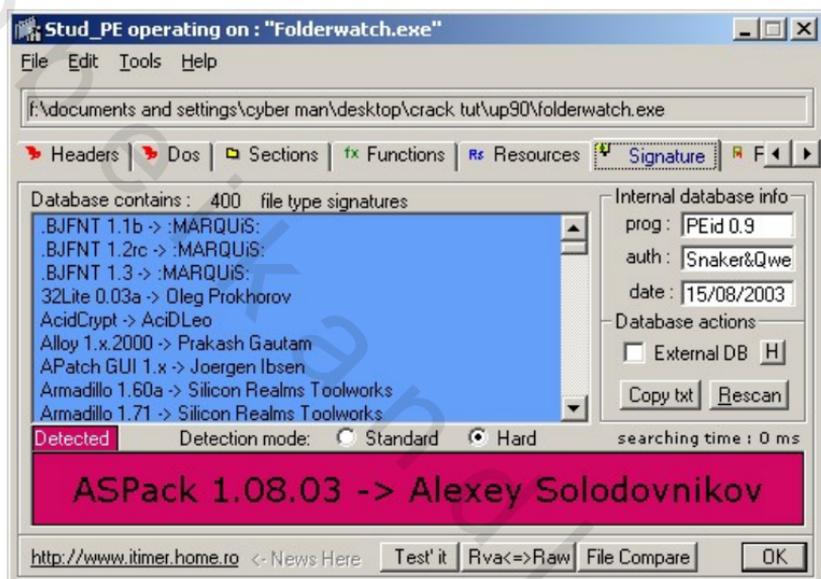


و فيما يلي أمثله عمليه:  
ملحوظة: ستجد في الاسطوانة المرفقة البرامج اللازمة للأمثلة.

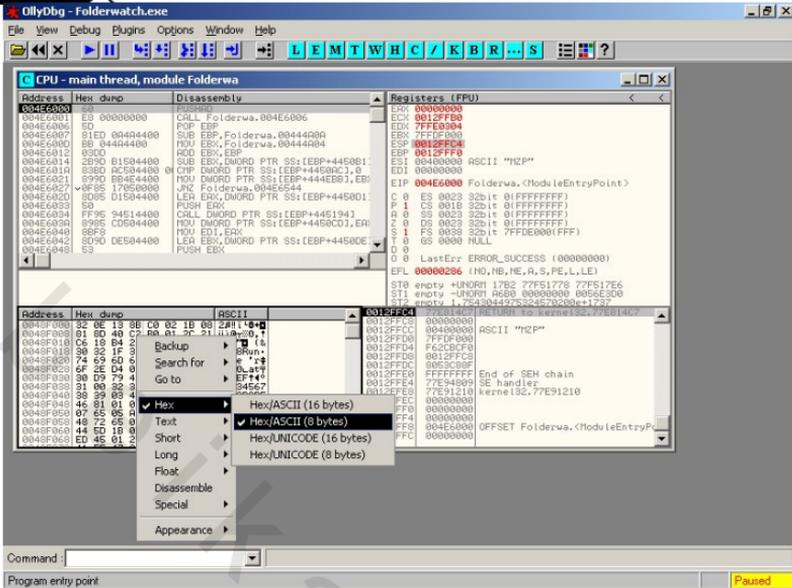
شفرة ASPack :

الأدوات: Ollydbg, Import Rec, STUD\_PE,

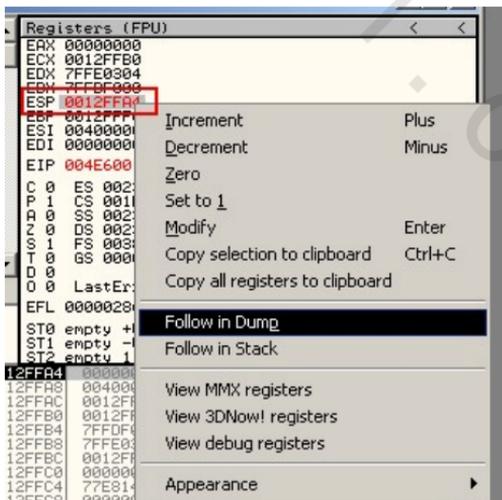
الخطوة الأولى هي التعرف على نوع الحماية المستخدمة في البرنامج قم بتشغيل برنامج stud\_pe وافحص البرنامج ستجد وجود الحماية aspack.



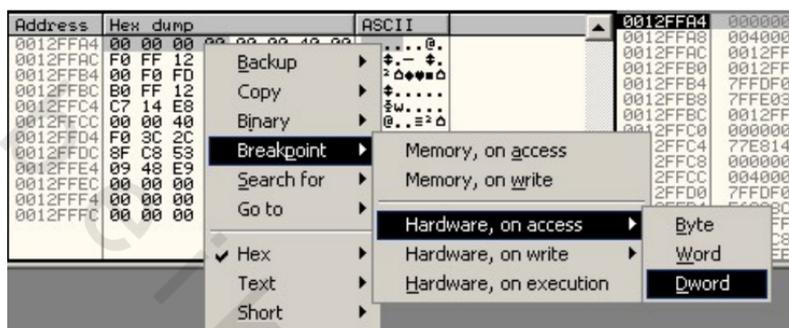
سنذهب الآن إلى برنامج ollydbg لمعرفة نقطة الدخول الحقيقية للبرنامج أو EIP افتح ollydbg وحمل البرنامج بداخله. وقم بتحويل منظر الرؤية في نافذة ال dump إلى النظام السداسي.



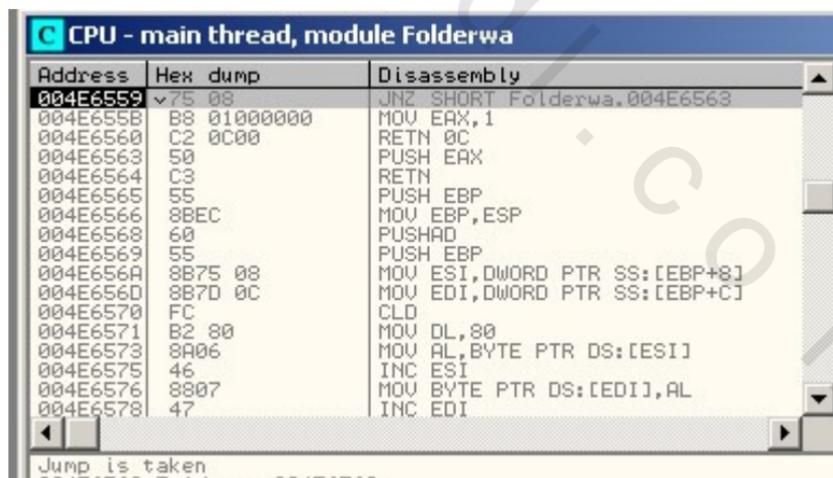
قم الآن بالضغط على مفتاح التتبع F8 ثم اذهب إلى نافذة المسجلات ووقف على المسجل ESP واختر الاختيار follow in dump



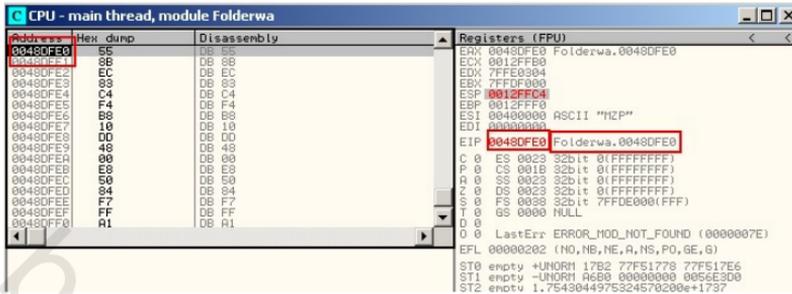
ستجد نافذة ال dump تقف الآن عند محتويات المسجل قم باختيار أول اربع بايتات واختار من قائمة الأوامر المختصرة أمر التوقف hardware on access | Dword



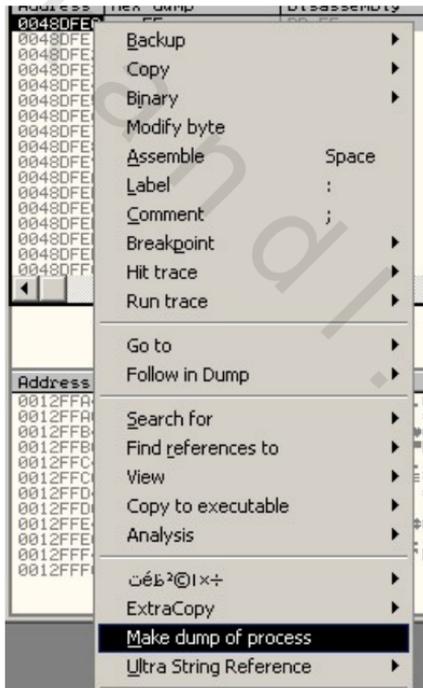
قم بالضغط على مفتاح التشغيل F9 ستجد أن البرنامج يقف عند العنوان الذي به الأمر JNZ



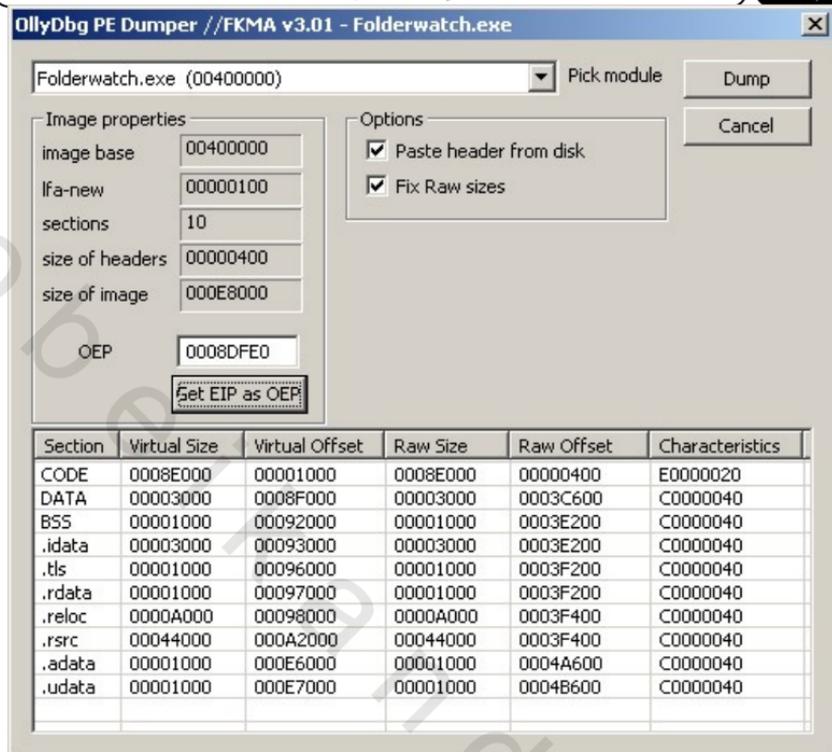
اضغط المفتاح F8 حوالي ثلاث مرات حتى تصل للعنوان 0048DFE0 وهو العنوان الحقيقي لنقطة الدخول EIP كما يتضح من نافذة المسجلات



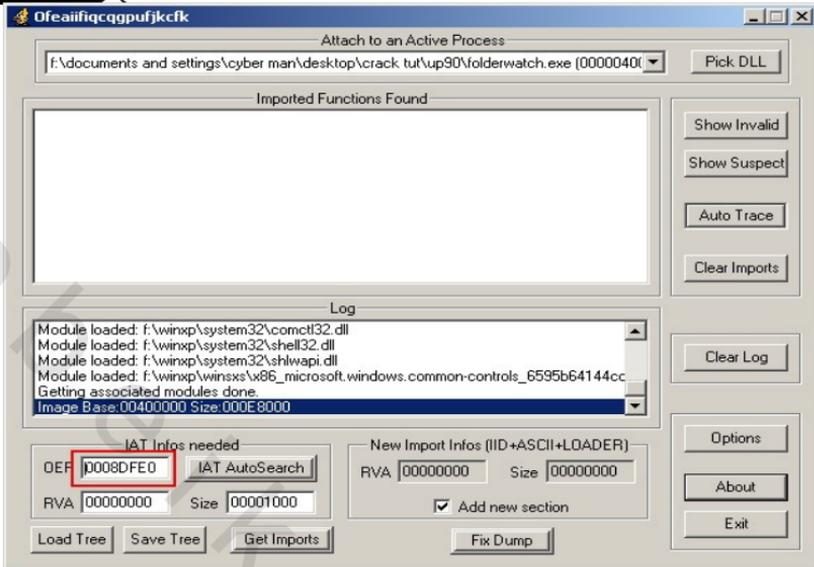
قم بالماوس على العنوان السابق واختار الأمر dump debugged process



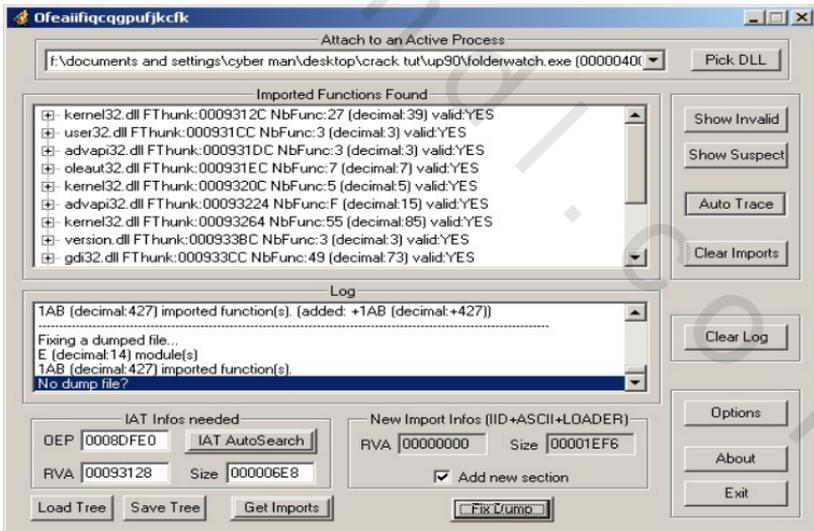
و يتم ظهور الديالوج التالي:



تأكد من الضغط على المفتاح Get EIP as OEP ثم اضغط على مفتاح  
 dump وأحفظ البرنامج باسم مختلف قم الآن بفتح برنامج Import Rec  
 واختار الملف folder watch



قم بإدخال العنوان 8DFE0 في خانة OEP ثم اضغط المفتاح IAT Auto search والمفتاح Get Imports



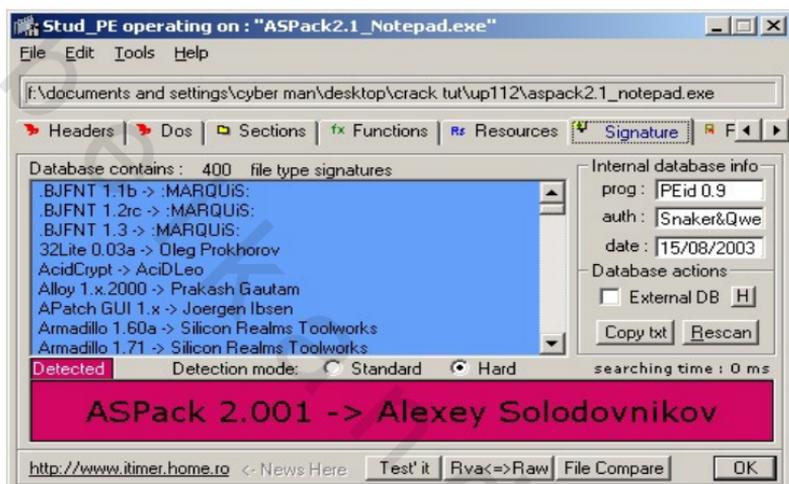
و لا يحتاج البرنامج في هذه الحالة إلى إصلاح اضغط على fix dump واحفظ الملف الجديد وهكذا تم استخراج الملف للتنفيذ الحقيقي.

برنامج Notepad:

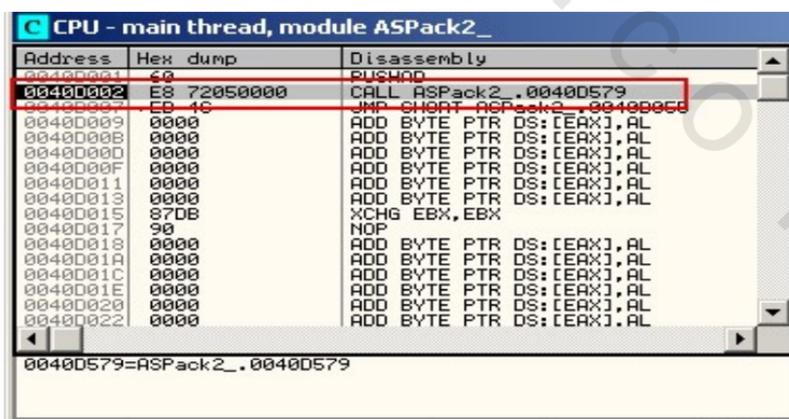
الحماية: aspack

الأدوات: stud\_pe, import rec, ollydbg

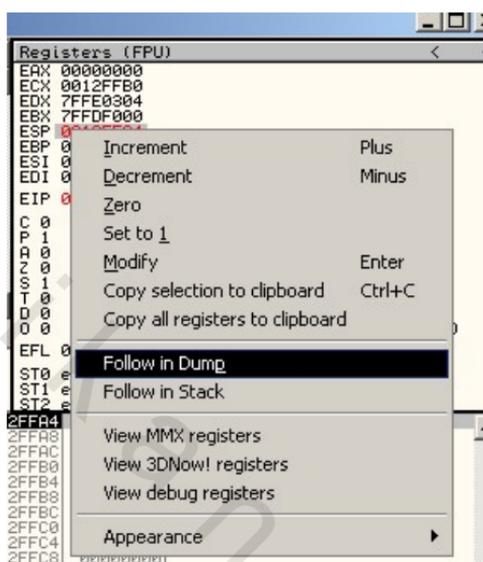
- للتأكد من نوع الحماية قم بفتح الملف في برنامج Stud\_pe



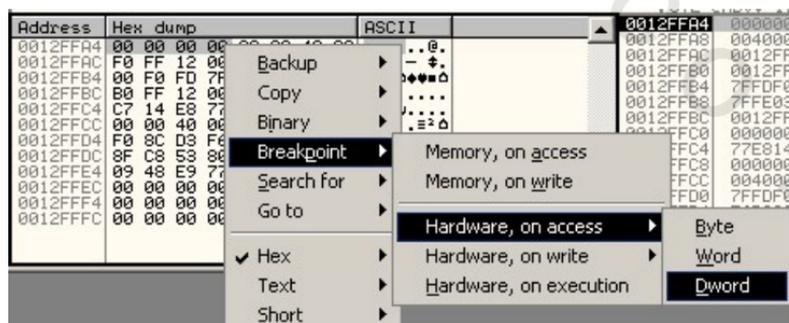
- والآن قم بفتح الملف في برنامج ollydbg واضغط F8 مرة واحدة.



- والآن انتقل إلى قسم المسجلات واختار الأمر `follow in dump` من القائمة المختصرة بالماوس وأنت تقف على المسجل ESP



- من نافذة `dump` اختر بالماوس أول أربع بايت واضغط على المفتاح الأيمن ومن القائمة المختصرة اختر الأوامر `breakpoint | hardware on access | dword`



إعادة الهندسة

- والآن اضغط F9 حتى يقف البرنامج ودائما في هذا النوع من الحماية يجب أن تجد مكان الوقوف هو أمر القفز JNZ والذي يقوم بالقفز إلى مكان الملف الحقيقي.

CPU - main thread, module ASPack2\_

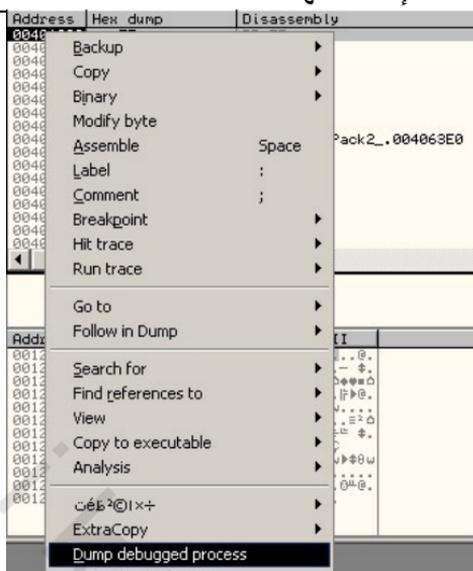
Address	Hex dump	Disassembly
004004F4	75 08	JNZ SHORT ASPack2_.004004FE
004004F5	B8 01000000	MOV EAX,1
004004FB	C2 0C00	RETN 0C
004004FE	68 CC104000	PUSH ASPack2_.004010CC
00400503	C3	RETN
00400504	8B85 08374400	MOV EAX,DWORD PTR SS:[EBP+4437D8]
0040050A	8D8D 11384400	LEA ECX,DWORD PTR SS:[EBP+443811]
00400510	51	PUSH ECX
00400511	50	PUSH EAX
00400512	FF95 E4384400	CALL DWORD PTR SS:[EBP+4438E4]
00400518	8985 B9294400	MOV DWORD PTR SS:[EBP+4429B9],EAX
0040051E	8D85 21384400	LEA EAX,DWORD PTR SS:[EBP+443821]
00400524	50	PUSH EAX
00400525	FF95 EC384400	CALL DWORD PTR SS:[EBP+4438EC]
0040052B	8985 1D384400	MOV DWORD PTR SS:[EBP+44381D],EAX
00400531	8D8D 2C384400	LEA ECX,DWORD PTR SS:[EBP+44382C]
00400537	51	PUSH ECX

Jump is taken  
004004FE=ASPack2\_.004004FE

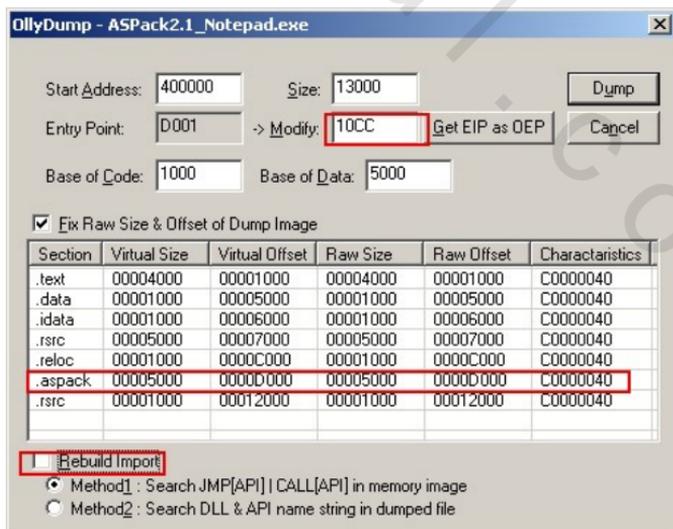
- اضغط F8 ثلاث مرات حتى تصل للشكل التالي:

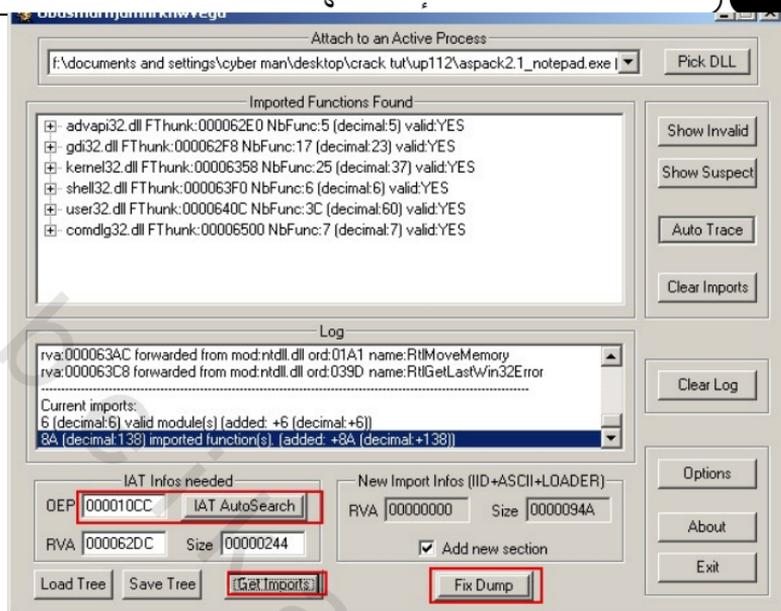
Address	Hex dump	Disassembly	Registers (FPU)
00401000	55	DB 55	EAX 00000000
00401001	5B	DB 5B	ECX 0012FFB0
00401002	EC	DB EC	EDX 7FFE0304
00401003	88	DB 88	EBX 7FFDF000
00401004	EC	DB EC	ESP 0012FFC4
00401005	44	DB 44	EBP 0012FF00
00401006	56	DB 56	ESI 00400000 ASPack2_.00400000
00401007	FF	DB FF	EDI 00000000
00401008	15 E0634000	ADC EAX,ASPack2_.004063E0	EIP 0040100C ASPack2_.004010CC
00401009	8B	DB 8B	EAX 00000000
0040100A	F0	DB F0	ECX 0012FFB0
0040100B	9A	DB 9A	EDX 7FFE0304
0040100C	00	DB 00	EBX 7FFDF000
0040100D	3C	DB 3C	ESP 0012FFC4
0040100E	22	DB 22	EBP 0012FF00
0040100F	75	DB 75	ESI 00400000 ASPack2_.00400000
00401010	13	DB 13	EDI 00000000

- و هكذا نكون وصلنا للمكان الحقيقي للملف قف الآن على هذا العنوان ثم اختار من القائمة المختصرة الأمر dump debugged process

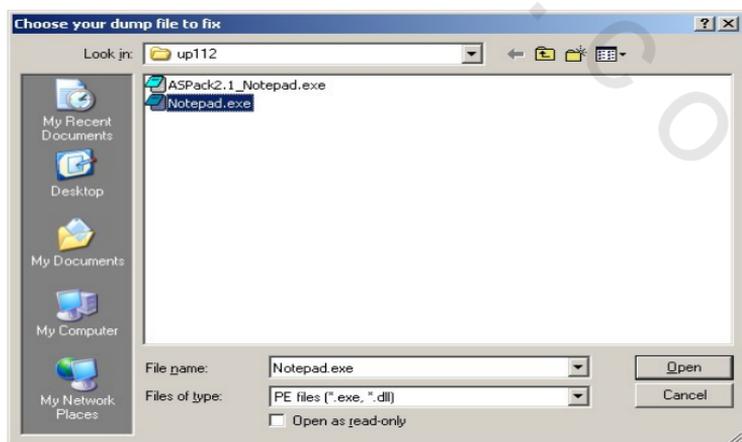


- يتم ظهور ديايوج التفرغ وتأكد من وجود العنوان الحقيقي 10CC وإزالة الاختيار rebuild import

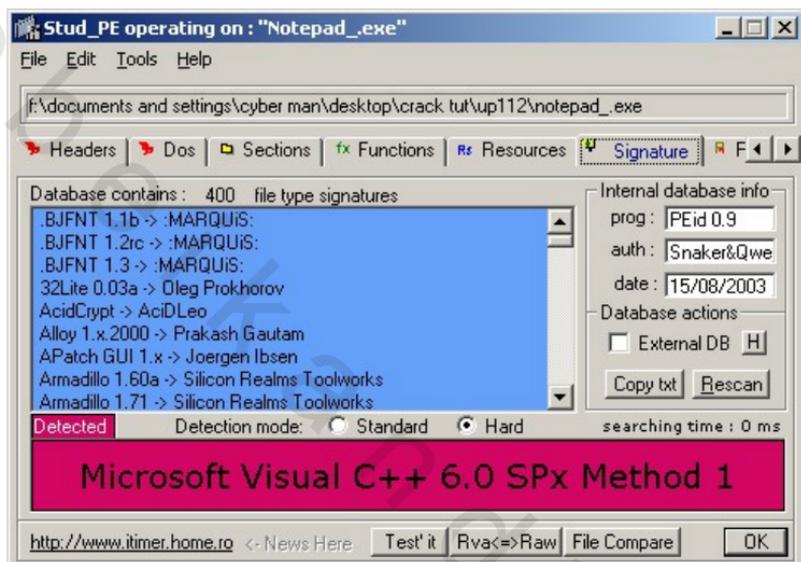




تأكد من إدخال العنوان الحقيقي OEP ثم اضغط على المفتاح IAT Auto search ثم get imports وأخيرا fix dump كما فعلنا سابقا واختار الملف الذي قمت بتفريغه



و سيقوم البرنامج بإنشاء ملف جديد بالاسم notepad\_.exe وإذا أردت التأكد من إزالة الحماية قم بوضع الملف الناتج في برنامج stud\_pe ويجب أن تجد اسم اللغة المستخدمة في البرنامج وليس حزمة التشفير

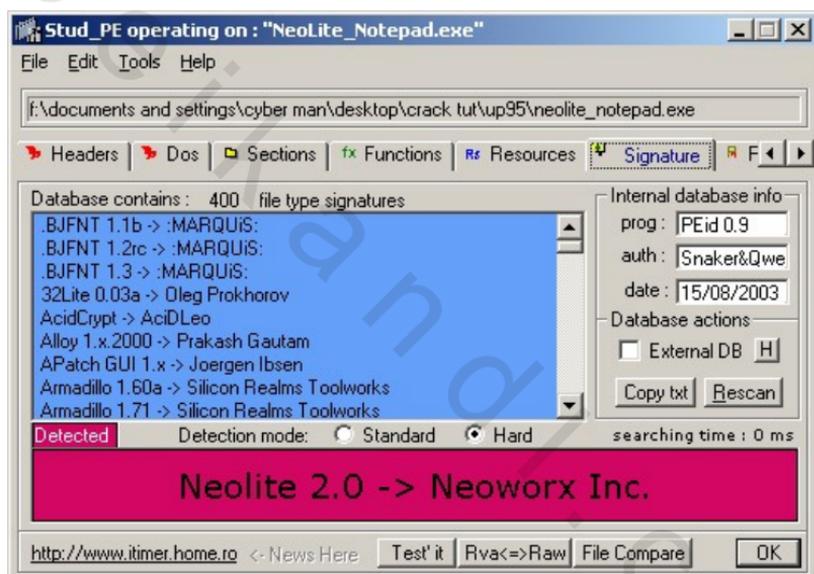


شفرة Neolite:

المثال: NotePad

الأدوات: ollydbg, stud\_pe, import rec

هذه الشفرة من أسهل الشفرات التي يمكن فكها قم الآن بفتح برنامج المثال في برنامج stud\_pe للتعرف على نوع الحماية ويجب أن تحصل على النتيجة الآتية:



و الآن بعد أن تأكدنا من وجود الشفرة قم بتحميل برنامج المثال في ollydbg - قم الآن بفتح البرنامج import rec .

CPU - main thread, module NeoLite\_

Address	Hex dump	Disassembly
0040017E	5E9 A6000000	JMP NeoLite_.00400229
00400183	DEEB4000	DD NeoLite_.0040EBDE
00400187	. 94004000	DD <&KERNEL32.LoadLibraryA>
0040018B	. 98004000	DD <&KERNEL32.GetProcAddress>
0040018F	. 00000000	DD 00000000
00400193	. DE480000	DD 00004BDE
00400197	40D24000	DD NeoLite_.0040D240
0040019B	. 4E 65 6F 4C 61	ASCII "NeoLite Executab"
004001A8	. 6C 65 20 46 61	ASCII "le File Compress"
004001BB	. 6F 72 0D 0A 41	ASCII "or/©Copyright (c)"
004001CB	. 29 20 31 39 31	ASCII ") 1998,1999 NeoLite"
004001DB	. 6F 72 78 20 41	ASCII "ork Inc/©Portion"
004001EB	. 73 20 43 6F 71	ASCII "'s Copyright (c)"
004001FB	. 31 39 39 37 21	ASCII "1997-1999 Lee Ha"
0040020B	. 73 69 75 68 01	ASCII "siuk/©All Rights"
0040021B	. 20 52 65 73 61	ASCII " Reserved. ©", 0"
00400228	. 00	DB 00

00400229=NeoLite\_.00400229

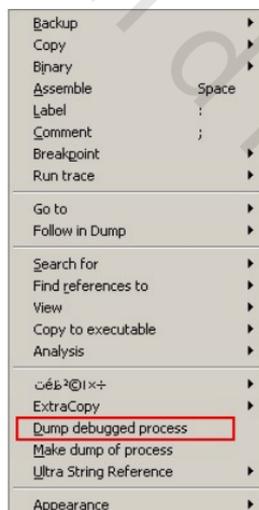
و الآن قم بالضغط على المفتاح F8 حتى تصل للسطر الذي يتم فيه القفز إلى EAX حيث تحتوى EAX على نقطة الدخول الحقيقية للملف .

Address	Hex dump	Disassembly
00400229	> 8B4424 04	MOV EAX,DWORD PTR SS:[ESP+4]
0040022D	. 2305 8FD14000	AND EAX,DWORD PTR DS:[40D18F]
00400233	. E8 ED040000	CALL NeoLite_.00400725
00400238	. FF05 28D24000	INC BYTE PTR DS:[40D228]
0040023E	. -FFE0	JMP EAX
00400240	. 805D 28D24000	CMF BYTE PTR DS:[40D228],0
00400247	. 75 13	JNZ SHORT NeoLite_.0040025C
00400249	. 90	NOP
0040024A	. 90	NOP
0040024B	. 90	NOP
0040024C	. 90	NOP
0040024D	. 50	PUSH EAX
0040024E	. 2BC0	SUB EAX,EAX
00400250	. E8 D0040000	CALL NeoLite_.00400725
00400255	. 58	POP EAX
00400256	. FF05 28D24000	INC BYTE PTR DS:[40D228]
0040025C	> C3	RETN

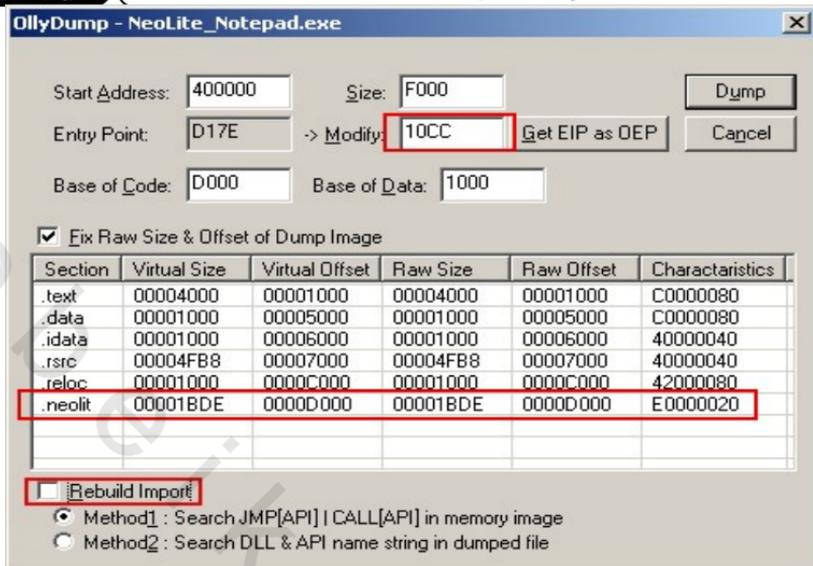
ملحوظة: عندما تظهر رسالة للذهاب إلى موقع الشفرة اجب بـ No

Address	Hex dump	Disassembly
004010CC	55	PUSH EBP
004010CD	8BEC	MOV EBP,ESP
004010CF	83EC 44	SUB ESP,44
004010D2	56	PUSH ESI
004010D3	FF15 E0634000	CALL DWORD PTR DS:[4063E0]
004010D9	8BF0	MOV ESI,EAX
004010DB	8A00	MOV AL,BYTE PTR DS:[EAX]
004010DD	3C 22	CMP AL,22
004010DF	75 13	JNZ SHORT NeoLite_.004010F4
004010E1	46	INC ESI
004010E2	8A06	MOV AL,BYTE PTR DS:[ESI]
004010E4	84C0	TEST AL,AL
004010E6	74 04	JE SHORT NeoLite_.004010EC
004010E8	3C 22	CMP AL,22
004010EA	75 F5	JNZ SHORT NeoLite_.004010E1
004010EC	803E 22	CMP BYTE PTR DS:[ESI],22
004010EF	75 00	JNZ SHORT NeoLite_.004010FE

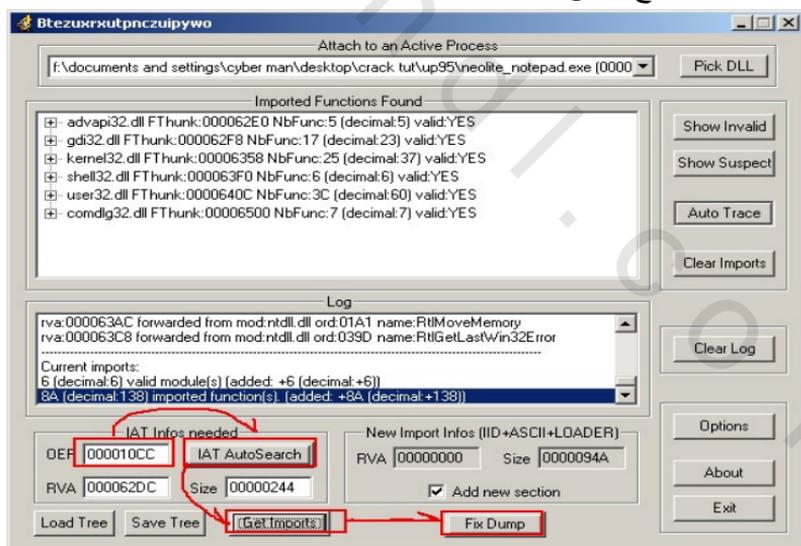
لاحظ هنا تساوى قيمة المسجل EIP مع العنوان الحالي وهذا يدل على بداية الملف الحقيقية ويمكننا أن نحصل على العنوان الحقيقي بطريق أخرى ولكن هذه أسهل طريقة ، قم الآن بفتح قائمة الأوامر المختصرة واختر الأمر Dump debugged Process



ويظهر الديالوج الخاص بالتفريغ تأكد من إزالة الاختيار rebuild import لأنه لا يقوم بالتصليح بطريقة جيدة وسنقوم باستخدام import rec



اضغط مفتاح Dump واحفظ الملف بأي اسم ثم قم بفتح البرنامج import rec  
وقم باختيار برنامج notepad

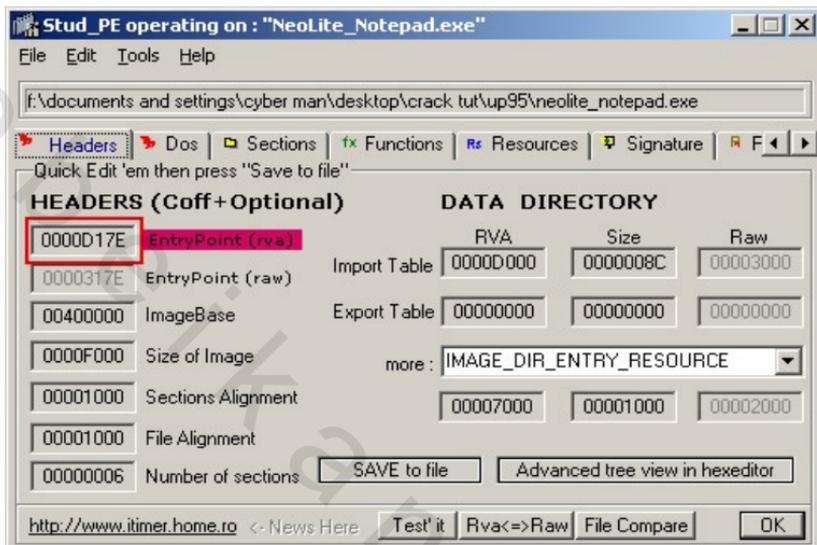


قم بتعديل OEP للقيمة 10CC ثم اضغط المفتاح IAT Auto Search  
المفتاح Get Imports ثم Fix Dump وبذلك تم فك شفرة Neolite

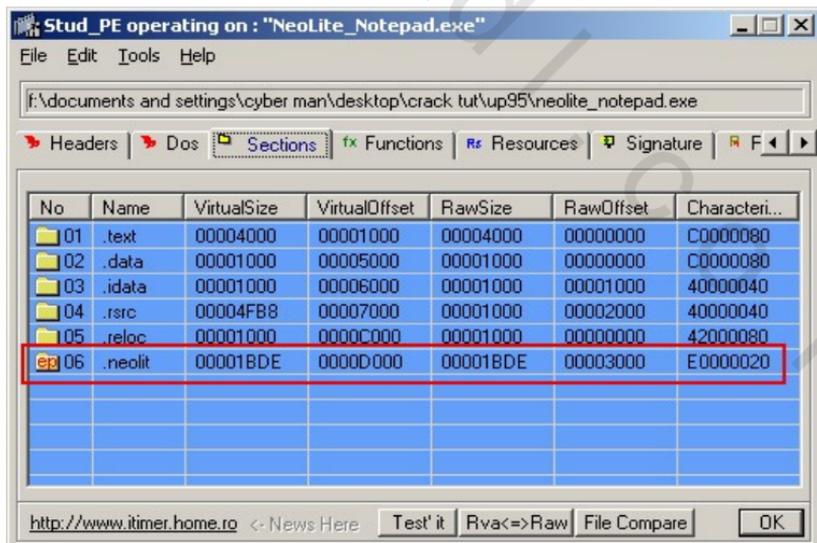
طريقة للحصول على OEP الخاص بالتشفير:

قم بفتح الملف في برنامج stud\_pe ثم اذهب headers ولاحظ نقطة

الدخول التخيلية D17E



اذهب للصفحة sections ولاحظ القسم neolite



لاحظ بيانات هذا القسم

Name:	.neolit
Virtual Size:	00001BDE
Virtual Offset	0000D000
Raw Size	00001BDE
Raw Offset	00003000
Characteristics	E0000020

وبذلك من البيانات السابقة يمكننا إيجاد EIP الحقيقية من طرح العنوان التخيلي من العنوان الحقيقي الحالي:

$$OEP = 0000D17E - (0000D000 - 00003000)$$

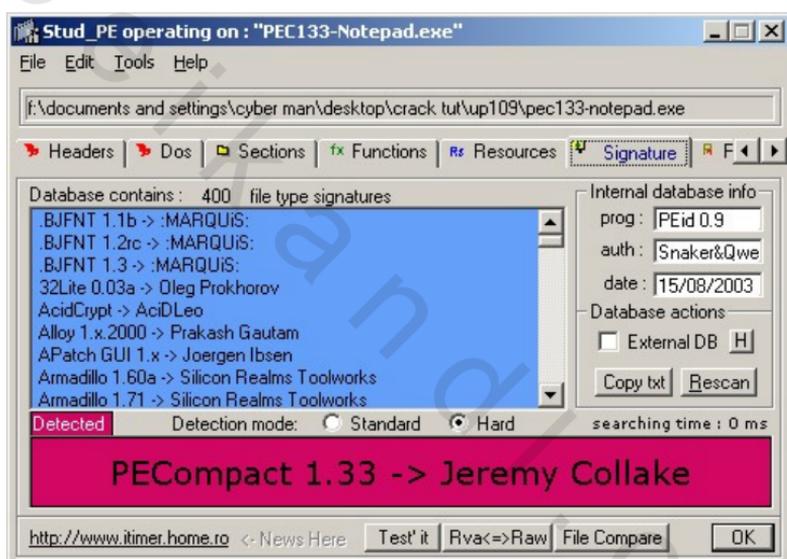
$$OEP = 0000317E$$

شفرة PE Compact :

البرنامج : notepad

الأدوات: ollydbg, import rec, stud\_pe

سنقوم أولاً بتحميل notepad في برنامج stud\_pe لمعرفة نوع الحماية وسنجدها pe compact وسنقوم في هذه الحماية باستخدام نقاط توقف في الذاكرة كما سيتضح فيما بعد.



- أغلق برنامج stud\_pe ثم قم بتحميل الملف في برنامج ollydbg  
ويجب أن ترى الأمر JMP كما بالشكل التالي:

CPU - main thread, module PEC133-N

Address	Hex dump	Disassembly
0040AC4C	EB 06	JMP SHORT PEC133-N.0040AC54
0040AC4E	68 CC100000	PUSH 10CC
0040AC53	C3	RETN
0040AC54	9C	PUSHFD
0040AC55	60	PUSHAD
0040AC56	E8 02000000	CALL PEC133-N.0040AC5D
0040AC5B	33C0	XOR EAX,EAX
0040AC5D	8BC4	MOV EAX,ESP
0040AC5F	83C0 04	ADD EAX,4
0040AC62	93	XCHG EAX,EBX
0040AC63	8BE3	MOV ESP,EBX
0040AC65	8B5B FC	MOV EBX,DWORD PTR DS:[EBX-4]
0040AC68	81EB 0F804000	SUB EBX,PEC133-N.0040800F
0040AC6E	87DD	XCHG EBP,EBX
0040AC70	8B85 A6804000	MOV EAX,DWORD PTR SS:[EBP+4080A6]
0040AC76	0185 03804000	ADD DWORD PTR SS:[EBP+408003],EAX
0040AC7C	66:C785 00804000	MOV WORD PTR SS:[EBP+408000].9090

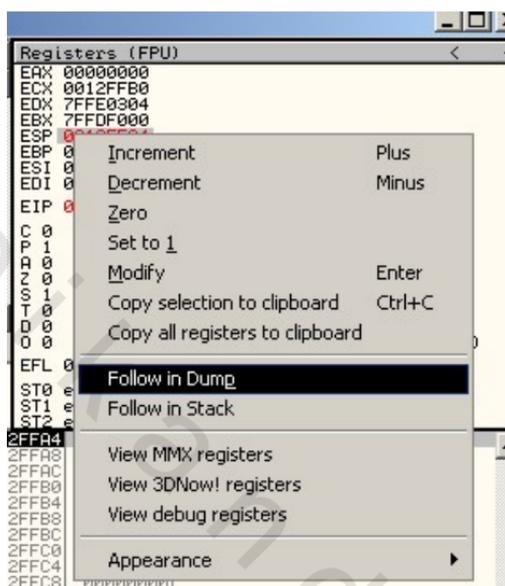
0040AC54=PEC133-N.0040AC54

الأمر التالي هو الذي يحتوي عنوان الملف الحقيقي OEP قم بالضغط مرتين على المفتاح F8 حتى تقف على الأمر pushed

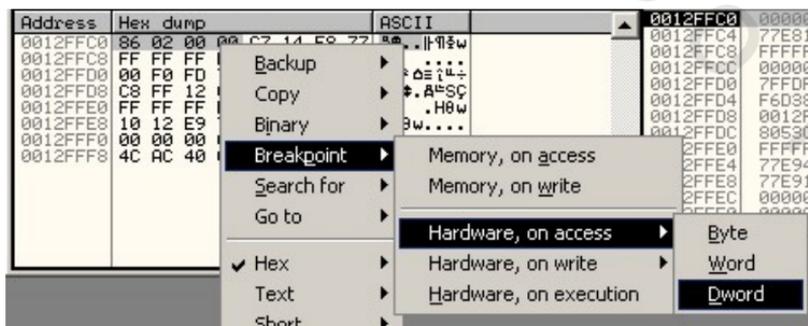
CPU - main thread, module PEC133-N

Address	Hex dump	Disassembly
0040AC4C	EB 06	JMP SHORT PEC133-N.0040AC54
0040AC4E	68 CC100000	PUSH 10CC
0040AC53	C3	RETN
0040AC54	9C	PUSHFD
0040AC55	60	PUSHAD
0040AC56	E8 02000000	CALL PEC133-N.0040AC5D
0040AC5B	33C0	XOR EAX,EAX
0040AC5D	8BC4	MOV EAX,ESP
0040AC5F	83C0 04	ADD EAX,4
0040AC62	93	XCHG EAX,EBX
0040AC63	8BE3	MOV ESP,EBX
0040AC65	8B5B FC	MOV EBX,DWORD PTR DS:[EBX-4]
0040AC68	81EB 0F804000	SUB EBX,PEC133-N.0040800F
0040AC6E	87DD	XCHG EBP,EBX
0040AC70	8B85 A6804000	MOV EAX,DWORD PTR SS:[EBP+4080A6]
0040AC76	0185 03804000	ADD DWORD PTR SS:[EBP+408003],EAX
0040AC7C	66:C785 00804000	MOV WORD PTR SS:[EBP+408000].9090

- قم الآن باختيار الأمر follow in dump من قائمة الأوامر المختصرة وأنت تقف على المسجل ESP



- واذهب إلى نافذة dump وقف على أول أربع بايت واختار الأوامر التالية breakpoint | hardware, on access | dword



- بعد ذلك اضغط shift+F9 لتصل للأمر push eax

CPU - main thread, module PEC133-N

Address	Hex dump	Disassembly
00400134	50	PUSH EAX
00400135	68 CC104000	PUSH PEC133-N.004010CC
00400136	C2 0400	RETN 4
0040013D	8BB5 5C854000	MOV ESI,DWORD PTR SS:[EBP+40855C]
00400143	0BF6	OR ESI,ESI
00400145	74 18	JE SHORT PEC133-N.0040D15F
00400147	8B95 A6804000	MOV EDX,DWORD PTR SS:[EBP+4080A6]
0040014D	03F2	ADD ESI,EDX
0040014F	E8 0F000000	CALL PEC133-N.0040D163
00400154	72 0B	JB SHORT PEC133-N.0040D161
00400156	83C6 14	ADD ESI,14
00400159	837E 0C 00	CMP DWORD PTR DS:[ESI+C],0
0040015D	75 F0	JNZ SHORT PEC133-N.0040D14F
0040015F	F8	CLC
00400160	C3	RETN
00400161	F9	STC
00400162	C3	RETN

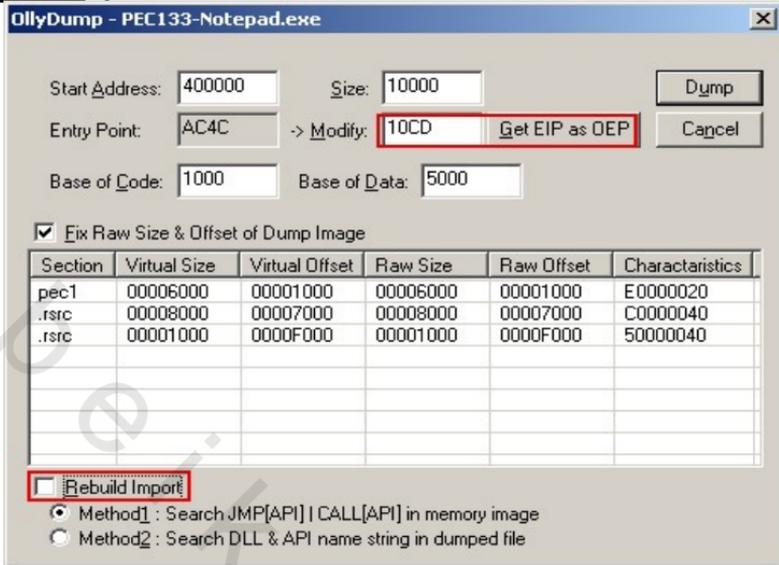
004010CC=PEC133-N.004010CC

- اضغط المفاتيح F8 مرة واحدة ويجب أن تكون الآن على نقطة الدخول الحقيقية للملف وسنقوم الآن بوضع نقطة الإيقاف في الذاكرة لذلك قم بالضغط على ALT+M لفتح نافذة الذاكرة وتأكد من الوقوف على المقطع code ثم قم باختيار الأمر التالي set memory breakpoint on access

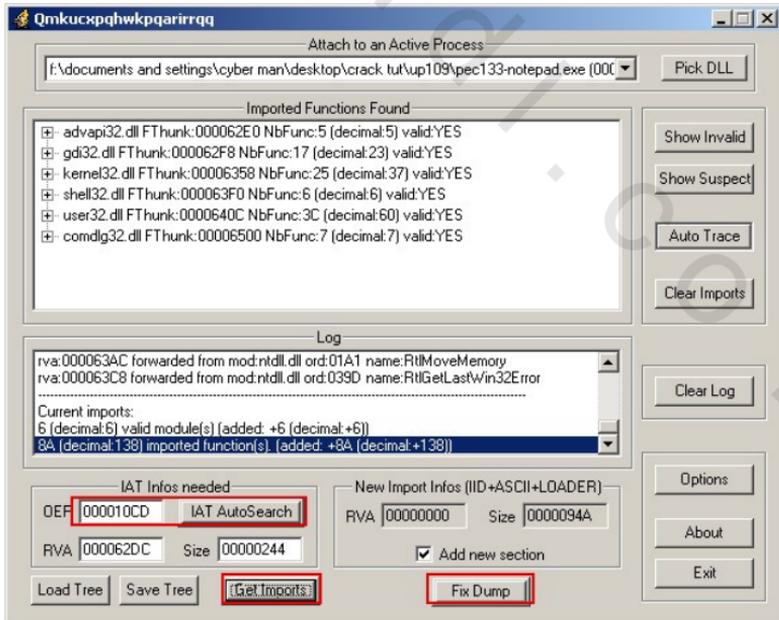
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00001000				Priv	RW	RW	
00020000	00001000				Priv	RW	RW	
0012C000	00001000				Priv	RW	Gu: RW	
0012D000	00003000			stack of ma	Priv	RW	Gu: RW	
00130000	00001000				Map	R	R	
00140000	00005000				Priv	RW	RW	
00240000	00006000				Priv	RW	RW	
00250000	00001000				Map	RW	RW	
00260000	00016000				Map	R	R	\\Device\Harddi
00280000	00034000				Map	R	R	\\Device\Harddi
002C0000	00041000				Map	R	R	\\Device\Harddi
00310000	00006000				Map	R	R	\\Device\Harddi
00320000	00004000				Priv	RW	RW	
00330000	00003000				Map	R	R	\\Device\Harddi
00340000	00008000				Priv	RW	RW	
00350000	00001000				Priv	RW	RW	
00360000	00001000				Priv	RW	RW	
00370000	00002000				Map	R	R	
00390000	00002000				Map	R	R	
00400000	00001000	PEC133-N		PE header	Imag	R	RWE	
00401000	00006000	PEC133-N	pecl	code				
00407000	00008000	PEC133-N	.rsrc	SFX, dat.				
0040F000	00001000	PEC133-N	.rsrc	imports				
00410000	00009000							
004D0000	00002000							
004E0000	00103000							
005F0000	00113000							
629C0000	00001000	LPK		PE head				
629C1000	00004000	LPK	.text	code, im				
629C5000	00001000	LPK	.data	data				
629C6000	00001000	LPK	.rsrc	resource				
629C7000	00001000	LPK	.dy	resource				

بعد ذلك قم بالضغط مره واحده على المفاتيح SHIFT+F9 لان البرنامج في هذه الحالة يقوم بالتوقف عند خطأ والضغط على المفاتيح السابقين يعطى إمكانية تخطى هذا الخطأ . و هكذا نكون وصلنا للعنوان الحقيقي وكما قمنا من قبل استخدم الأمر dump debugged process

Address	hex	dump	Disassembly	Registers (FPU)
00401000	8B		DB 8B	EAX: 00000000
00401001	83		DB 83	ECX: 0012FFB0
00401002	83		DB 83	EDX: 77FE9304
00401003	44		DB 44	EBX: 77FD0F00
00401004	56		DB 56	ESP: 0012FFC0
00401005	FF		DB FF	EBP: 0012FFF0
00401006	15		DB 15	ESI: 00000000
00401007	E0		DB E0	EDI: 00000000
00401008	63		DB 63	EIP: 004010CD PEC133-N,004010CD
00401009	4B		INC EBX	EAX: 00000000
0040100A	00		DB 00	ECX: 0012FFB0
0040100B	8B		DB 8B	EDX: 77FE9304
0040100C	F9		DB F9	EBX: 77FD0F00
0040100D	3C		DB 3C	ESP: 0012FFC0
0040100E	22		DB 22	EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
				EIP: 004010CD PEC133-N,004010CD
				EAX: 00000000
				ECX: 0012FFB0
				EDX: 77FE9304
				EBX: 77FD0F00
				ESP: 0012FFC0
				EBP: 0012FFF0
				ESI: 00000000
				EDI: 00000000
	</			



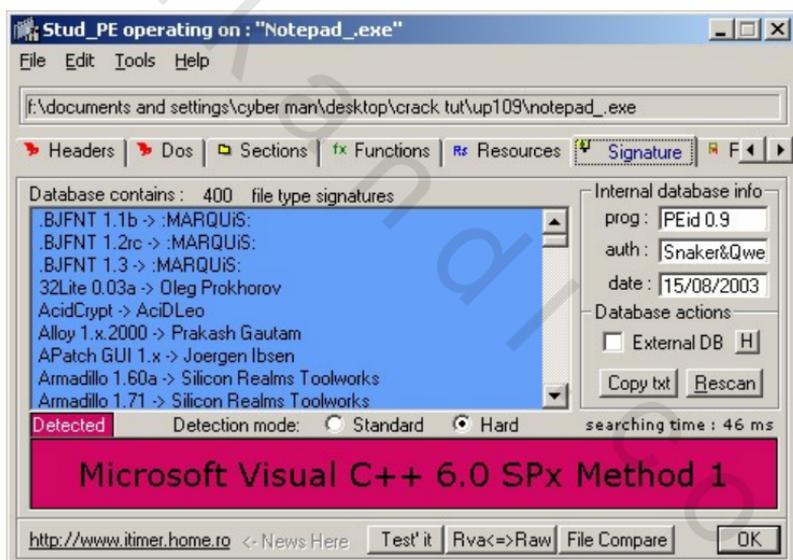
افتح الآن برنامج import rec وقم بتحميل الملف من الذاكرة وادخل عنوان OEP وهو 10CD ثم اضغط IAT AutoSearch ثم Get Imports ثم fix dumps



تأكد من اختيار الملف الذي قمنا بتفريغته من ollydbg وبعد انتهاء العملية يتم حفظ ملف بالاسم notepad\_.exe



إذا أردت التأكد أن الملف زالت الحماية منه قم بتشغيل برنامج stud\_pe وحمل الملف به ويجب أن يعطى البرنامج الآن اسم اللغة المستخدمة Visual C++

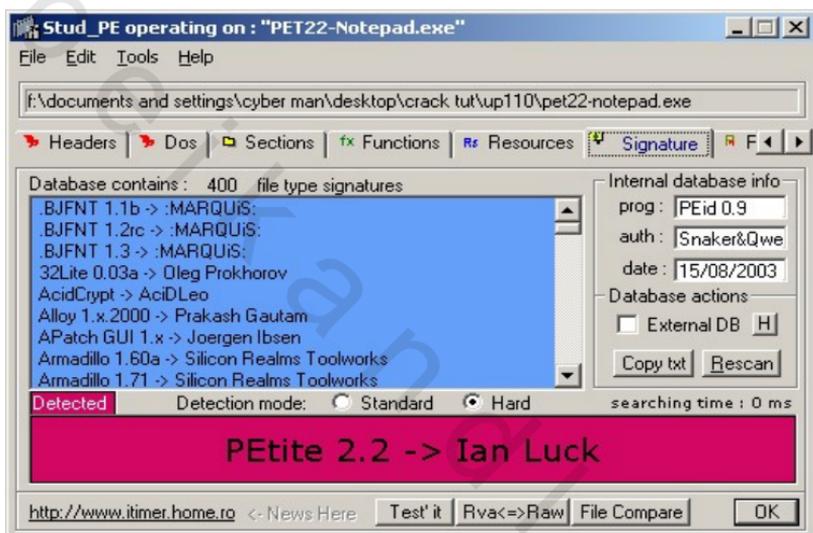


شفرة PETite

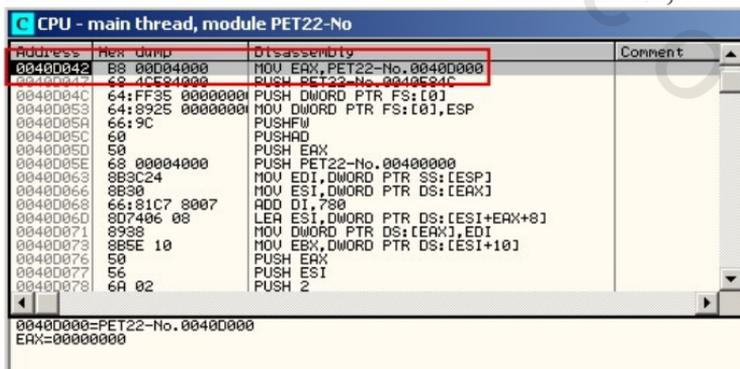
البرنامج : notepad

الأدوات: ollydbg, stud\_pe, import rec

قم بتحميل الملف في برنامج stud\_pe للتعرف على نوع الشفرة ومن الصفحة signature يمكننا أن نرى وجود شفرة Petite.



قم الآن بتحميل الملف في برنامج ollydbg ووقف البرنامج الآن على الأمر MOV EAX, Notepad

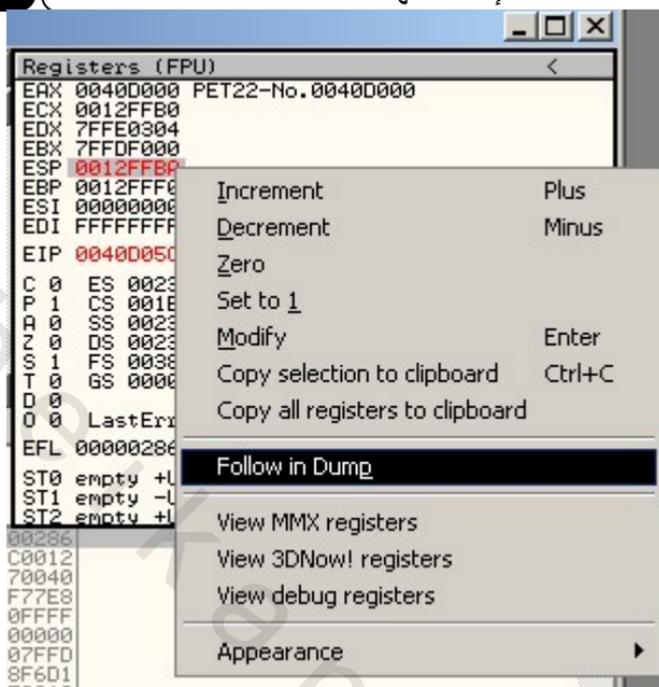


قم الآن بالضغط خمس مرات على المفتاح F8 حتى تصل للمكان  
PUSHAD

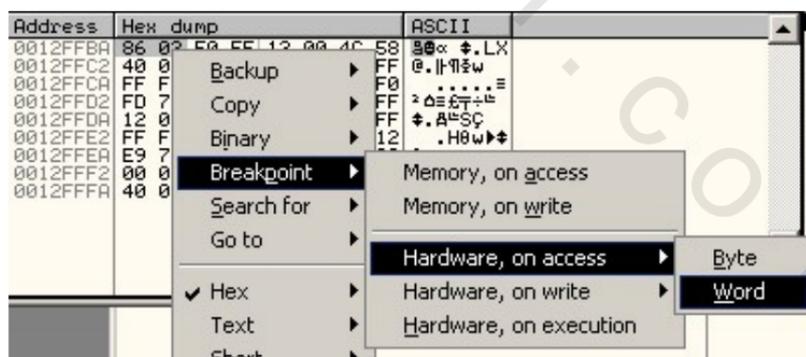
Address	Hex dump	Disassembly	Comment
00400042	B8 00004000	MOV EAX,PET22-No.00400000	
00400047	68 4C584000	PUSH PET22-No.0040584C	
0040004C	64:FF35 00000000	PUSH DWORD PTR FS:[0]	
00400053	64:3225 00000000	MOV DWORD PTR FS:[0],ESP	
00400059	66:9C	PUSHEDI	
0040005C	60	PUSHAD	
0040005D	50	PUSH EAX	
0040005E	68 00004000	PUSH PET22-No.00400000	
00400063	8B3C24	MOV EDI, DWORD PTR SS:[ESP]	
00400066	8B30	MOV ESI, DWORD PTR DS:[EAX]	
00400068	66:81C7 8007	ADD DI, 780	
0040006D	8D7406 08	LEA ESI, DWORD PTR DS:[ESI+EAX+8]	
00400071	8938	MOV DWORD PTR DS:[EAX], EDI	
00400073	8B5E 10	MOV EBX, DWORD PTR DS:[ESI+10]	
00400076	50	PUSH EAX	
00400077	56	PUSH ESI	
00400078	6A 02	PUSH 2	

00400000=PET22-No.00400000  
EAX=00000000

و الآن قف على المسجل ESP واختار الأمر follow in dump من قائمة الأوامر المختصرة.



بعد الذهاب إلى نافذة dump اختار أول اثنين بايت واختار الأمر  
breakpoint | hardware on access | word



تأكد الآن من تفعيل الاختيار memory access violation من القائمة  
Options | debugging options | exceptions

المفاتيح Shift+F9

Address	Hex dump	Disassembly	Comment
0040003F	83C4 08	ADD ESP,8	
00400042	E9 8540FFFF	JMP PET22-No.004010CC	
00400047	E9 8030E777	JMP SHELL32.ShellExecuteA	
0040004C	E9 56960977	JMP SHELL32.DragFinish	JMP to kern
00400051	E9 A09AA577	JMP kernel32._lcreat	
00400056	E9 E12FA677	JMP kernel32._lclose	
0040005B	E9 19EAA577	JMP kernel32.GetDateFormatA	
00400060	E9 FC8EA677	JMP kernel32.lstrcpmA	
00400065	E9 BA81A677	JMP kernel32.LocalReAlloc	
0040006A	E9 7290A677	JMP kernel32.lstrlenA	
0040006F	E9 2D69A677	JMP kernel32.MulDiv	
00400074	D82DA677	JMP kernel32._lread	
00400079	E9 24179477	JMP USER32.wspintfA	
0040007E	E9 69C89377	JMP USER32.GetSystemMenu	
00400083	E9 E5139477	JMP USER32.LoadCursorA	
00400088	E9 A5899577	JMP USER32.RegisterClassExA	
0040008D	E9 96A89777	JMP USER32.SetDlgItemTextA	

لاحظ السطرين التاليين

Add ESP, 8  
JMP Notepad

يتم تكرارهم في البرامج المحمية بشفرة Petite  
قم الآن بالضغط مرتين على المفتاح F8 حتى تصل للشكل التالي

Address	Hex dump	Disassembly	Comment
00401000	55	05 55	This is the This is the
00401002	EC	08 EC	
00401007	83	08 83	
00401009	EC	08 EC	
00401001	44	08 44	CHR 'D'
00401002	56	08 56	CHR '0'
00401003	FF	08 FF	
00401004	15	08 15	
00401005	E0	08 E0	
00401005	53	08 53	
00401007	40	08 40	
00401009	00	08 00	
00401009	00	08 00	
0040100A	F0	08 F0	
0040100E	8A	08 8A	
0040100C	00	08 00	

و نجد أن نقطة الدخول الحقيقية هي 10CC  
قم بتنفيذ أمر التبريع من الأمر dump debugged process

OllyDump - PET22-Notepad.exe

Start Address: 400000      Size: E000      Dump

Entry Point: D042      -> Modify: 10CC      Get EIP as DEF      Cancel

Base of Code: 1000      Base of Data: 5000

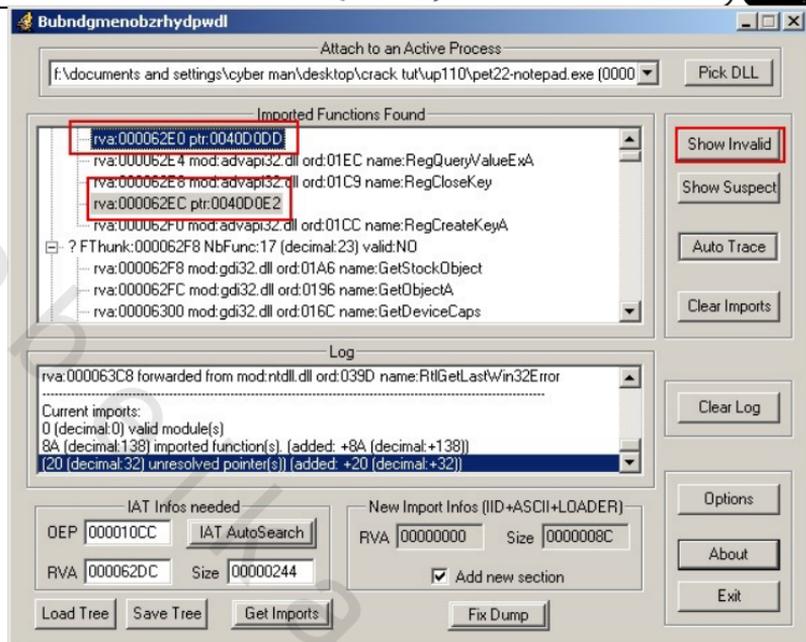
Fix Raw Size & Offset of Dump Image

Section	Virtual Size	Virtual Offset	Raw Size	Raw Offset	Characteristics
.PE----	00006000	00001000	00006000	00001000	E0000060
	00005000	00007000	00005000	00007000	C0000040
	00001000	0000C000	00001000	0000C000	C2000040
	000003CA	0000D000	000003CA	0000D000	E2000060

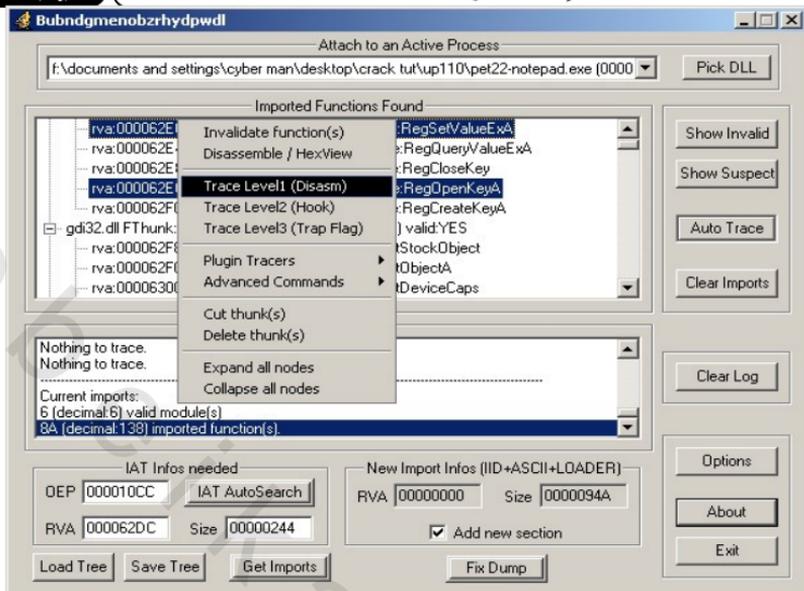
Rebuild Imports

- Method1 : Search JMP[API] | CALL[API] in memory image
- Method2 : Search DLL & API name string in dumped file

احفظ نقطة الدخول وافتح برنامج import rec واكتب بها نقطة الدخول واضغط على المفتاح IAT AutoSearch ثم Get Imports ثم show invalid لأننا سنجد هنا بعض الدوال التي تحتاج لتصليح.



و لتصليح هذه الدوال قم باختيار الأمر (disasm) trace level1 من قائمة الأوامر المختصرة.



و الآن اضغط fix dump واختار الملف السابق حفظه ويقوم البرنامج بحفظ ملف جديد بالاسم notepad\_.exe ، ويمكننا أن نرى أن الحماية تم إزالتها عن طريق تحميل الملف notepad\_.exe ببرنامج stud\_pe

