الفصل الرابع

إعادة الهندسة

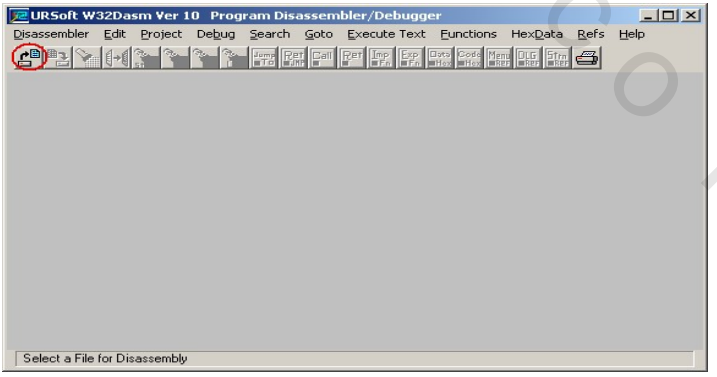
إعادة الهندسة Reverse engineering

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

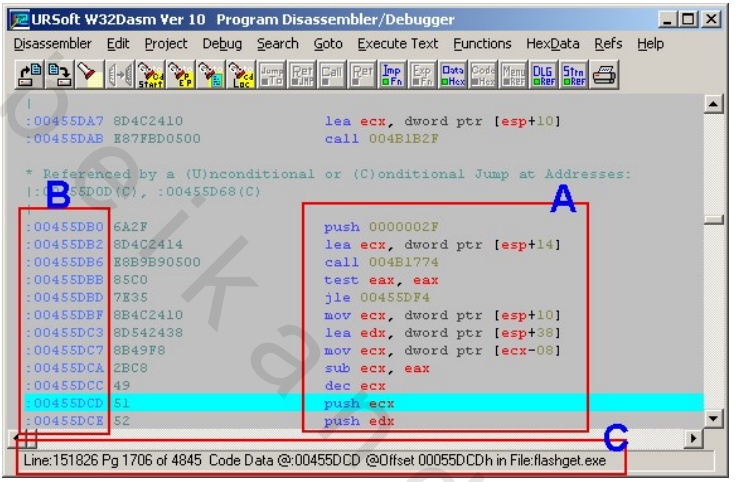
برنامج W32Dasm:

من البرامج العريقة ومن أول الأدوات الأساسية للكراك ويقوم البرنامج بكل بساطه بترجمة ملف exe إلى كود بالاسمبلى حيث يمكن متابعة عنوانين كل أمر وخصوصا أوامر القفز مثل JZ, JMP, JNE وغيرها.

ويستخدم هذا البرنامج دائما مع برنامج Hview حيث يمكن عن طريق الأخير تعديل ملف exe بسهوله 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:



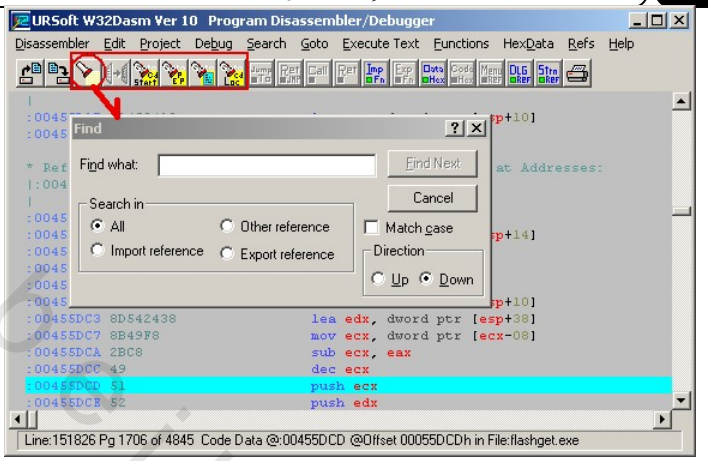
بعد الضغط على هذا المفتاح يتم فتح ديالوج للسؤال عن الملف التنفيذي المراد تحويله وبعد التحويل تجد أن كود الاسمبلى للملف موجود بالشاشة الرئيسية للبرنامج ومعظم مفاتيح الاختصار تم تفعيلها كما يتضح من الشكل التالي:



لاحظ من الشكل التالي:

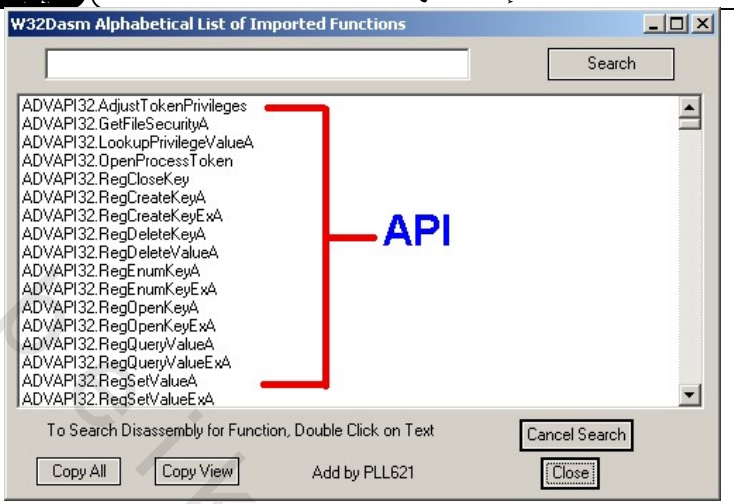
- المقطع A من الشاشة الرئيسية يحتوى على أوامر الاسمبلى
- المقطع B يحتوى على عنوان كل أمر بالملف
- المقطع C يحتوى على العنوان الحالي للأمر الذي يوجد فوقه شريط التركيز ويوجد بجانب العنوان الاوفست (عنوان محلى للملف) الرقم الفعلي للأمر بالبرنامج وعن طريقة يمكن تعديل الملف بسهوله ببرنامج Hview

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:

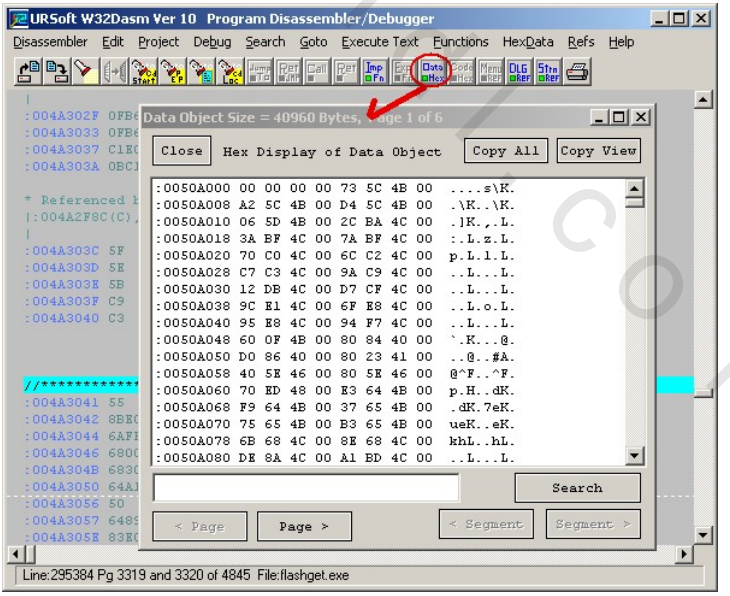


- المفتاح الذي يليه يستخدم لنسخ السطر الحالي
- المفتاح الثالث يستخدم للذهاب مباشرة إلى أول مقطع من لكود
- المفتاح الرابع الذهاب مباشرة إلى نقطة التحميل الخاصة بالملف التنفيذي المشهورة بالاسم PE أو Program Entry Point
- المفتاح الخامس يستخدم للتنقل بسهوله بين صفحات الكود
- المفتاح السادس يستخدم للذهاب إلى اوفست أو عنوان محدد بالملف

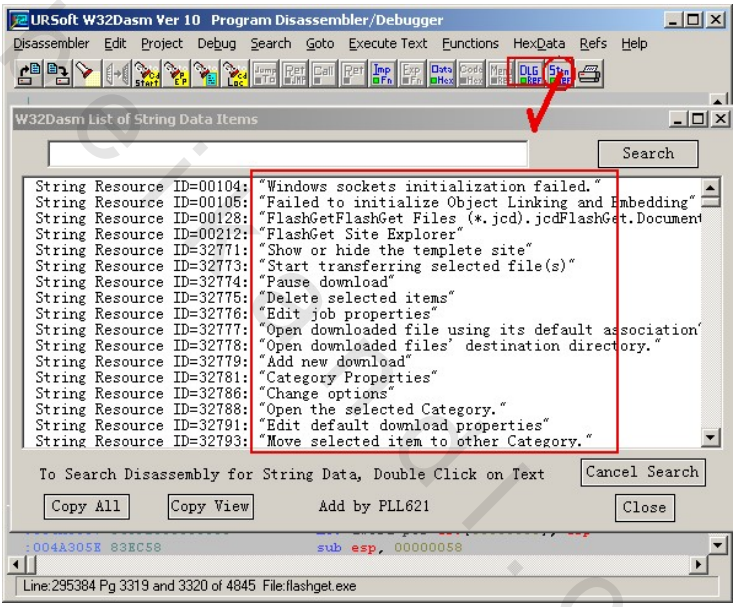
كما يحتوى البرنامج على مفتاحين الأول يسمى imports والثاني يسمى exports ويظهران بالتحديد دوال API (دوال الويندوز الأساسية) المعرفة بالبرنامج أو المستخدمة من الويندوز كما يتضح من الشكل التالي:



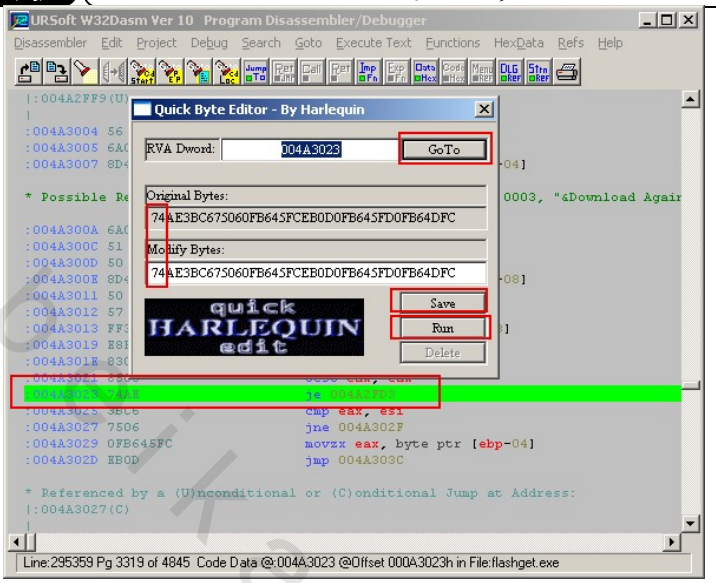
يمكنك أيضا من خلال هذا البرنامج رؤية البيانات المقابلة للاسمبلى بصورة الحدود السداسية عشر من خلال مفتاح يسمى hex display كما بالشكل:



ومن المميزات الهامة جدا لهذا البرنامج هو إمكانية الوصول إلى عنوان أو نص الرسائل التي توجد بالملف وهذه الخاصية هامه 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:

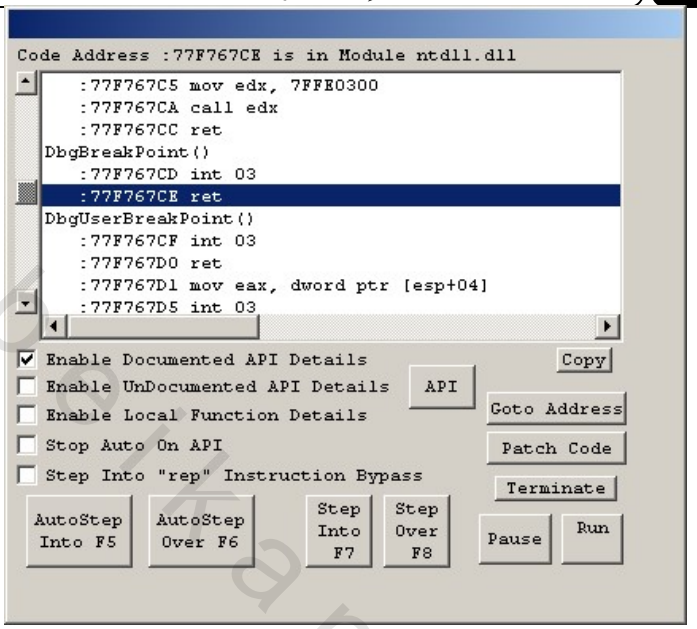


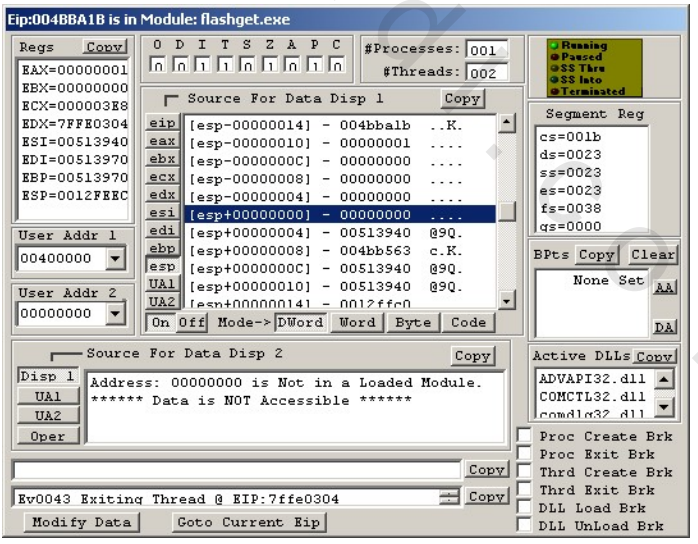
و من الإضافات الجديدة للبرنامج إمكانية تعديل الملف من داخله قم الآن بالوقوف على احد أوامر القفز ثم افتح القائمة edit واختر quick edit فيظهر ديالوج تستطيع من خلاله تغيير بايت القفز لكن بالنظام السداسي عشر كما يتضح من الشكل التالي:



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 معينه 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
Enable UnDocumented API Details
Enable Local Function Details
Stop Auto On API
Step Into "rep" Instruction Bypass
Copy
API
Goto Address
Patch Code
Terminate
AutoStep Into F5
AutoStep Over F6
Step Into F7
Step Over F8
Pause
Run


Eip:004BBA1B is in Module: flashget.exe
Regs Copy
EAX=00000001
EBX=00000000
ECX=000003E8
EDX=7FFE0304
ESI=00513940
EDI=00513970
EBP=00513970
ESP=0012FFEC
#Processes: 001
#Threads: 002
Running
Paused
SS Thre
SS Into
Terminated
Source For Data Disp 1 Copy
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] - 0012ffc0
Segment Reg
cs=001b
ds=0023
ss=0023
es=0023
fs=0038
gs=0000
User Addr 1
00400000
User Addr 2
00000000
On Off Mode-> DWord Word Byte Code
BPts Copy Clear
None Set
AA
DA
Source For Data Disp 2 Copy
Disp 1
UA1
UA2
Oper
Address: 00000000 is Not in a Loaded Module.
****** Data is NOT Accessible ******
Active DLLs Copy
ADVAPI32.dll
COMCTL32.dll
Copy
Ev0043 Exiting Thread @ EIP:7ffe0304
Copy
Proc Create Brk
Proc Exit Brk
Thrd Create Brk
Thrd Exit Brk
DLL Load Brk
DLL UnLoad Brk
Modify Data
Goto Current Eip

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

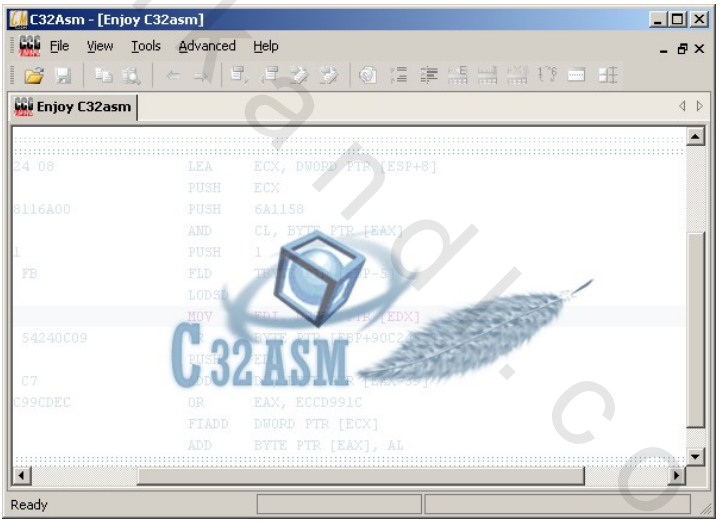
و من نقاط الضعف فيه أيضا انه لا يستطيع متابعة البرامج المكتوبة بلغة فيجوال بيزيك حتى الإصدار السادس رغم أن هذا النوع من البرامج يعتبر أسهل لغة يمكن كسر حمايتها لذلك نستخدم دائما برنامج smartcheck مع برامج الفيجوال بيزيك

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 للكراكر.

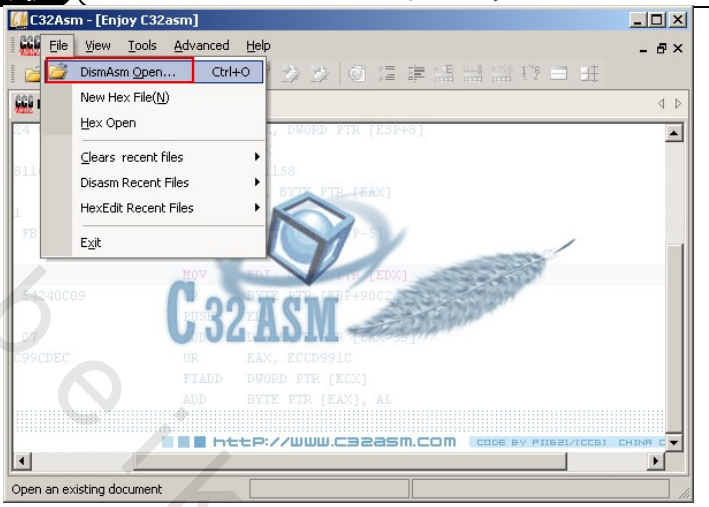
برنامج C32ASM:

هذا البرنامج يقوم أيضا بنفس عمل برنامج W32Dasm لكن يضاف إليه واجهة استخدام سهله وواضحة ورغم أن معظم استخدامات الكرارز يكون ببرنامج W32Dasm إلا أن هذا البرنامج لا يقل عنه وسنقوم الآن بشرح البرنامج ويمكنك أن تقارن وتستخدم ما تريد

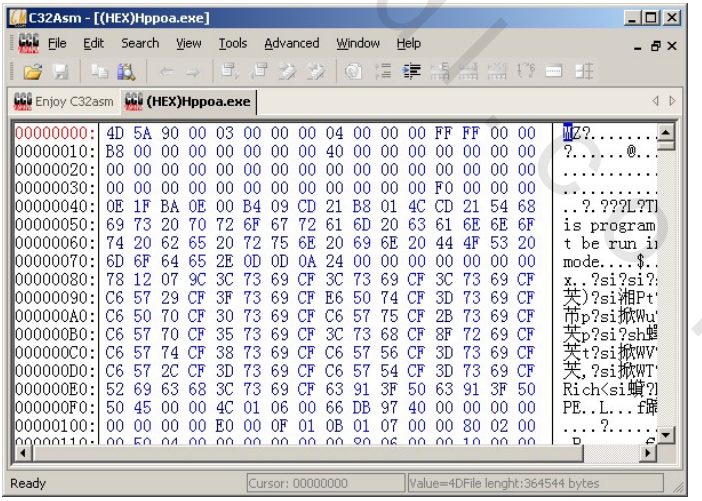
يفتح البرنامج على نافذة ترحيب جميله ويتكون مثل معظم البرامج من قوائم أوامر ومفاتيح اختصار تكون كلها غير فعاله حتى تقوم بفتح الملف التنفيذي المراد كسره.



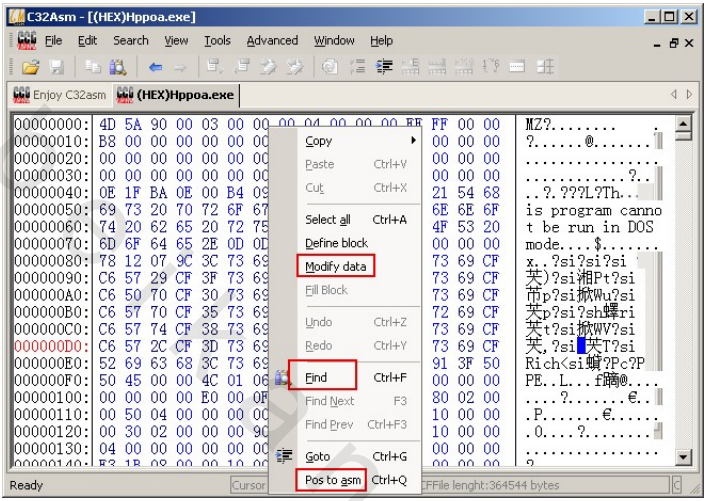
ولكي تقوم بفتح الملف اختار الأمر File DisAsm Open كما يلي:



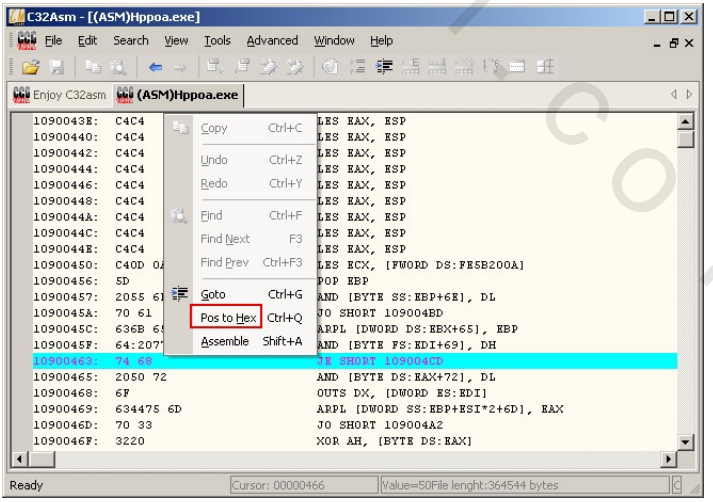
أما إذا استخدمت الأمر File Hex Open فيتحول البرنامج محرر بالنظام السداسي عشر ويمكن أن تحتار أي ملف وتحريره في نافذة مستقلة.



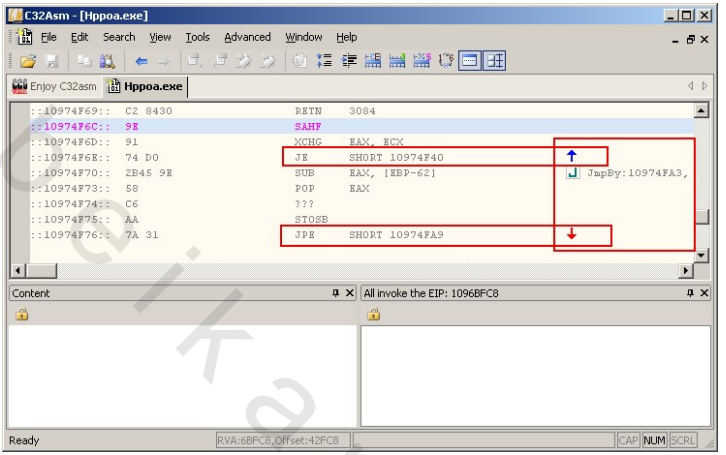
كما يمكنك عن طريق قائمة الأوامر المختصرة البحث عن أي نص أو تعديل محتويات الملف .



ويمكنك أيضا الذهاب إلى التعليمة الاسمبلى المكافئة للموقع الحالي عن طريق أمر Pos to asm



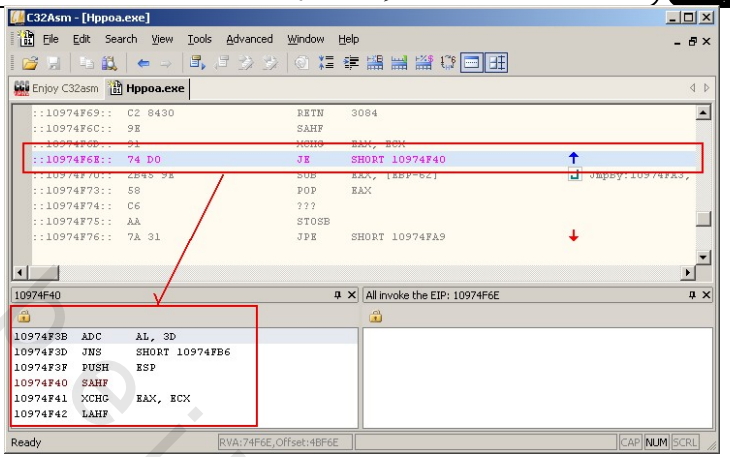
بالمثل يمكنك الرجوع إلى نافذة Pos to Hex من قائمة الأوامر المختصرة قم الآن بفتح الملف المراد كسره بالطريقة العادية ويجب أن ترى الشكل التالي:



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

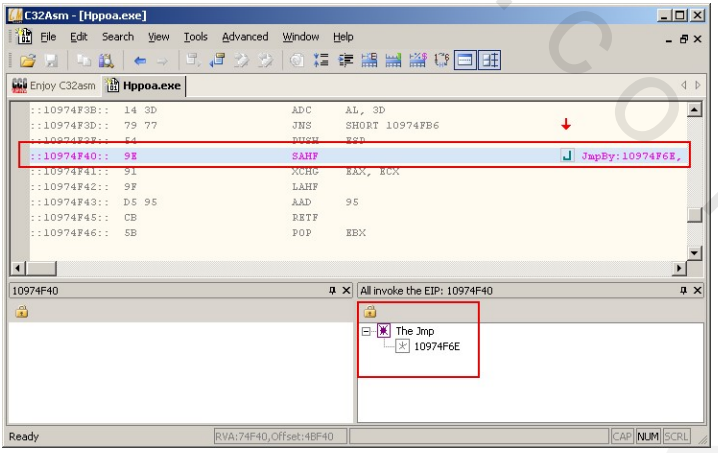
و يمكنك التنقل بسهوله بين أوامر القفز كما يلي:

- قم أولا بالوقوف على أمر القفز حتى يصبح الأمر الحالي



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

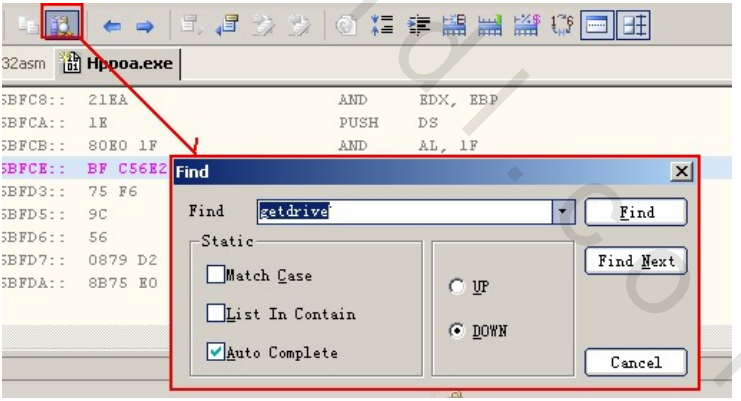
و يجب الآن أن تجد مكانك تم تغييره إلى العنوان الجديد



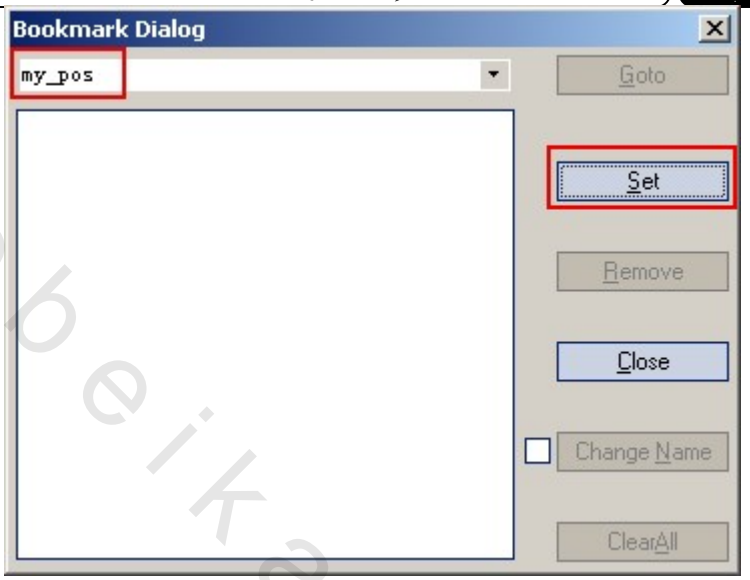
لاحظ أن البرنامج يقوم بإظهار أن هذا المكان تم القفز إليه ويكتب العنوان الذي تم القفز منه ويمكنك الرجوع إلى نفس المكان السابق بالضغط على المفتاح ret jmp أو Ctrl+Shift+J

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



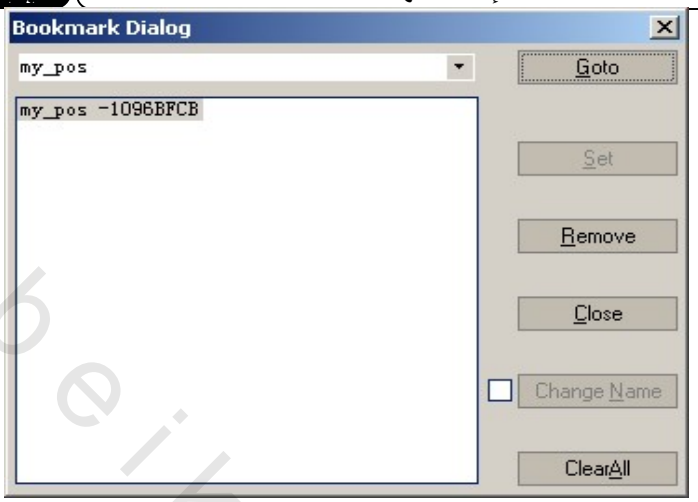
كمل يعطى البرنامج إمكانية لوضع مؤشر للتعليم ويتم ذلك عن طريق الأمر Search | Bookmark أو Ctrl+M فيتم فتح ديالوج للمؤشرات



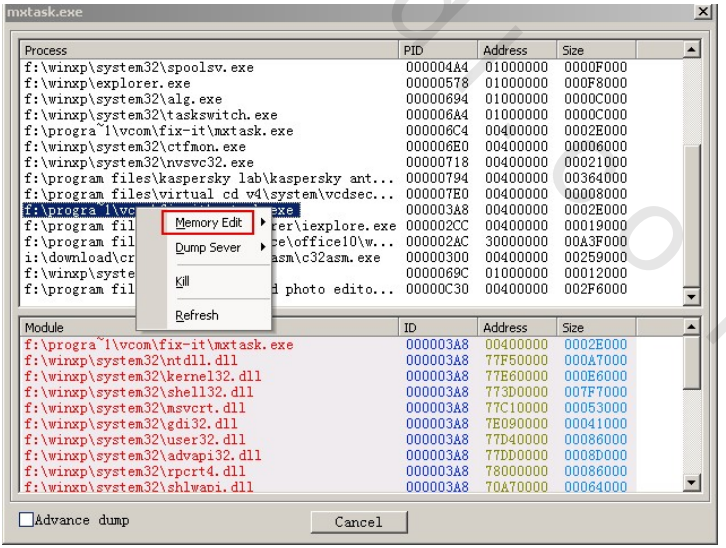
و يجب كتابة أي تعليق ثم الضغط على المفتاح set ويجب أن تشاهد المؤشر كما يلي:

```
::1096BFC7::  44              INC     ESP
::1096BFC8::  21EA            AND     EDX, EBP
::1096BFCA::  1E              PUSH    DS
::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



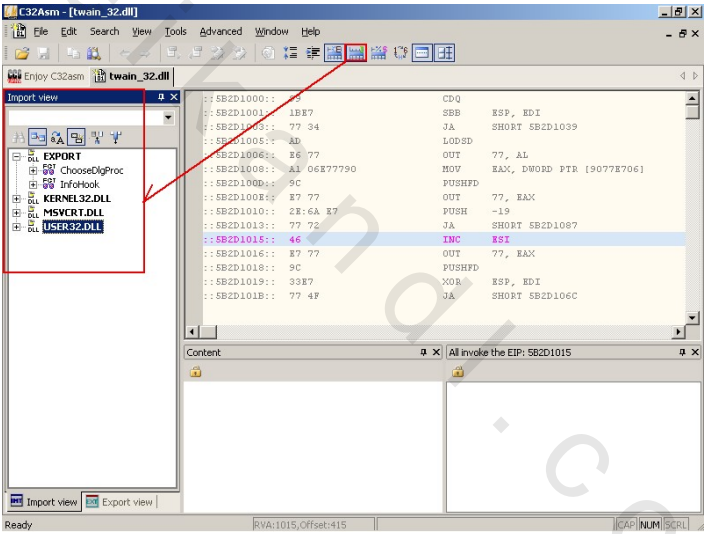
و يمكنك أيضا عن هذا البرنامج رؤية الذاكرة الخاصة بأحد البرامج المحملة وتفريغها ويتم ذلك عن طريق الأوامر Tools | Process edit



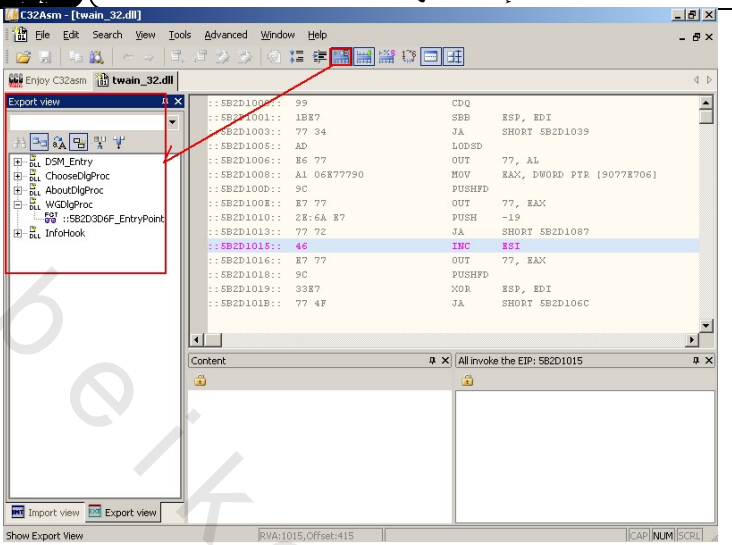
وعن طريق قائمة الأوامر المختصرة يمكنك اختيار Memory Edit ويمكنك بعد ذلك اختيار أي جزء من الذاكرة تريد تعديله وسيتم فتح محرر بالنظام السداسي عشر ، كما يمكنك أيضا تفريغ محتويات ملف عن طريق الأمر Dump Server واختيار أي جزء تريد تفريغه

تعطى القائمة View العديد من الإمكانيات الهامة منها:

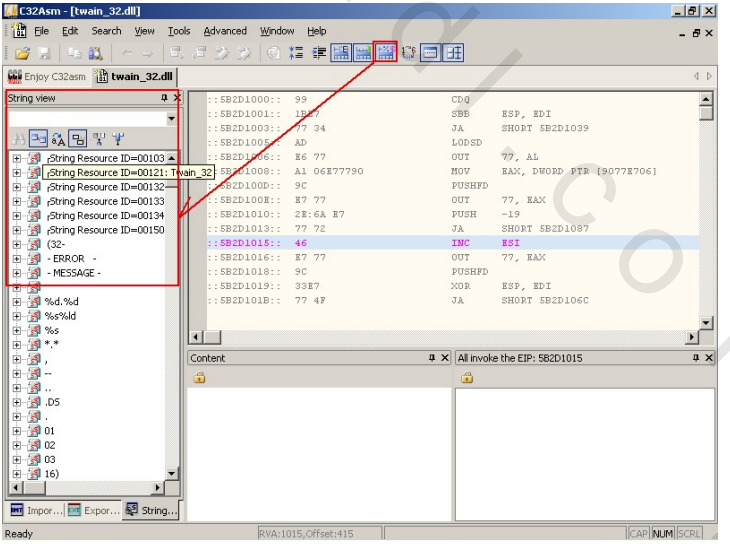
- رؤية دوال API التي يستخدمها الملف عن طريق الأمر View | Import



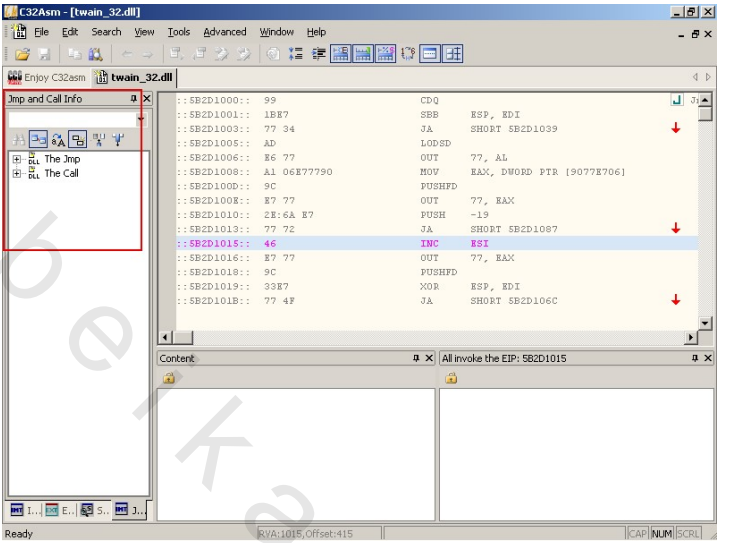
- رؤية الدوال التي يقوم الملف بتصديرها عن طريق الأمر View | Export



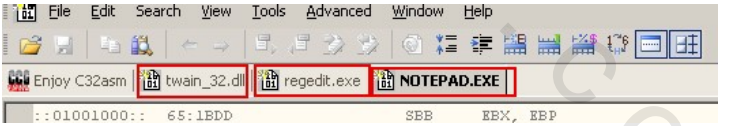
- رؤية النصوص التي يحتويها الملف View | Strings



- رؤية كل عناوين القفز والنداء View | Jmps and calls



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



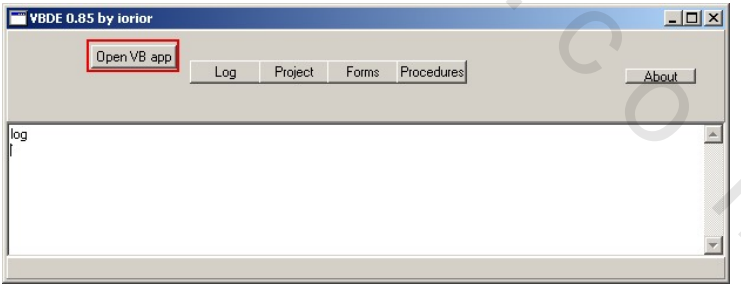
برامج إعادة التجميع Decompiles

كما ذكرنا فإن كل لغة يتم فيها ترجمة الأوامر المكتوبة بها إلى لغة الاسمبلى 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 السى يقوم بترجمة كل الكود ويقوم بإظهار ناتج عملية الترجمة في النهاية.

وهناك أيضا نوع آخر من المعالجات وهي المسئولة عن إنتاج برامج التنصيب setup مثل 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 فانه يستخدم لإعادة ترجمة برامج فيجوال بيزيك ويتكون البرنامج من عدة مفاتيح كل منها لعرض نوع معين من وحدات الفيجوال بيزيك



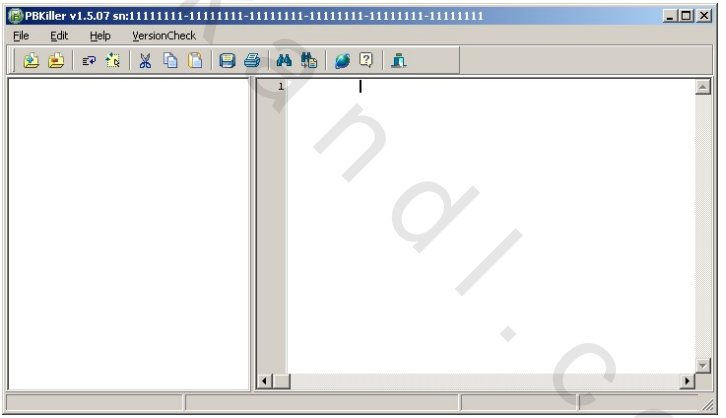
أولا يجب أن تقوم بفتح برنامج VB من المفتاح Open VB app ثم قم باختيار Project لترى الكود الأساسي الخاص بالمشروع.

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

برنامج Pbkiller:

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

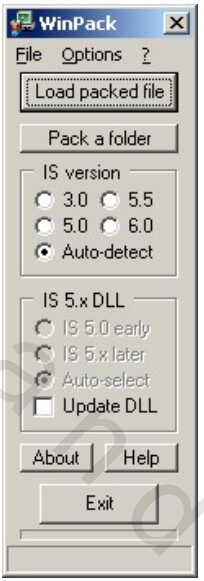
و يتكون البرنامج من قوائم ومفاتيح اختصار كما نرى من النافذة الافتتاحية التالية:



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

برنامج WinPack:

هذا البرنامج متخصص لفك تجميع ملفات برنامج install shield الشهير ويتكون من مفاتيح أساسيه هي :



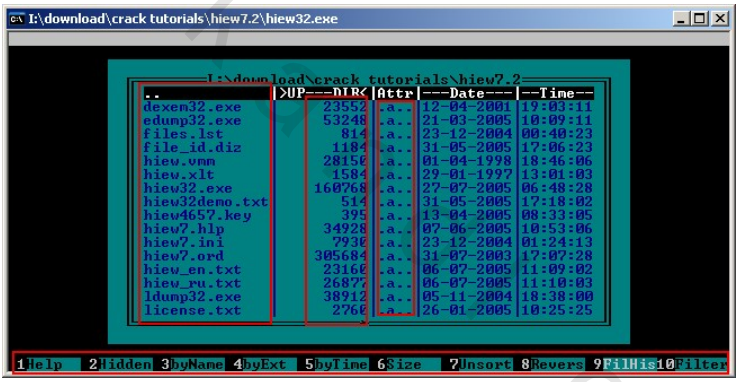
قم بفتح ملف *.cab أو *.hdr لبرنامج التنصيب من المفتاح Load package file وسيقوم البرنامج بالتعرف على الإصدار المناسب للفك وكما ترى فهذا البرنامج يمكنه فك تنصيب الإصدارات 3 – 5 – 5.5 – 6

أداوت التحرير Editors

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

برنامج Hackers View:

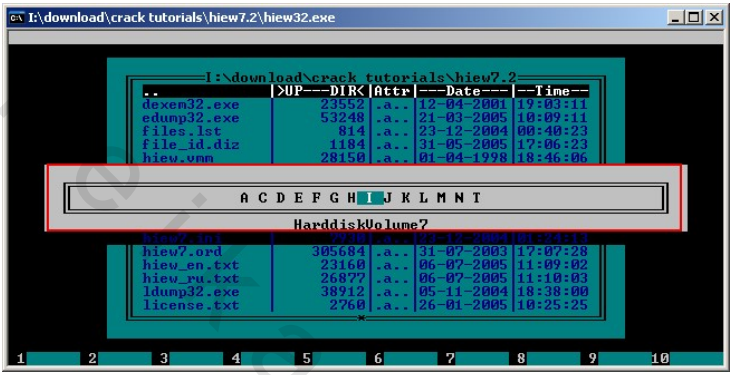
من الأدوات العريقة في مجال كسر حماية البرامج وعادة يستخدم مع برامج disassembly وهذا البرنامج رغم انه يعتمد على الدوس الا انه في غاية القوه ويستطيع التعامل مع جميع أنواع الملفات.



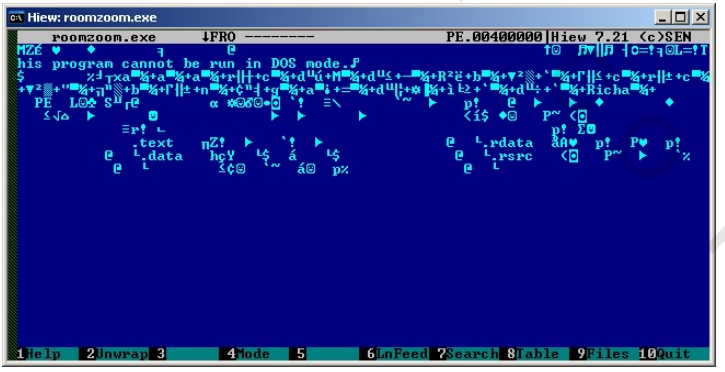
ويتكون البرنامج كما نرى من الصورة من عدة أعمده يقوم فيها البرنامج بعرض الملفات فيعرض في أول عمود اسم الملف والثاني الحجم والثالث خصائص الملف والأخير تاريخ ووقت إنشاء الملف.

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

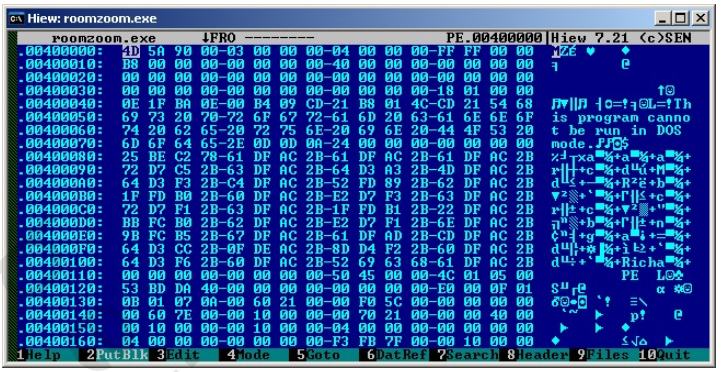
لكي تستطيع الانتقال إلى الدليل الذي يوجد به الملف المراد تعديله قم بالضغط على المفتاحين Alt+F1 فتظهر نافذة يمكن اختيار منها حرف المشغل المراد استعراضه.



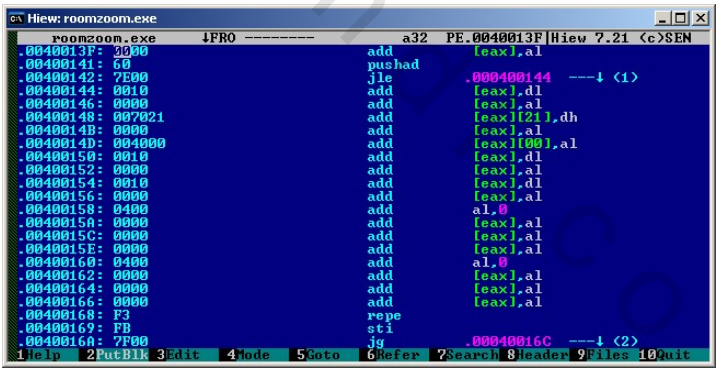
بعد ذلك انتقل إلى الملف المراد تعديله بمفاتيح الأسهم ومفتاح الإدخال وعندما تصل للملف قم بالضغط على مفتاح الإدخال.



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

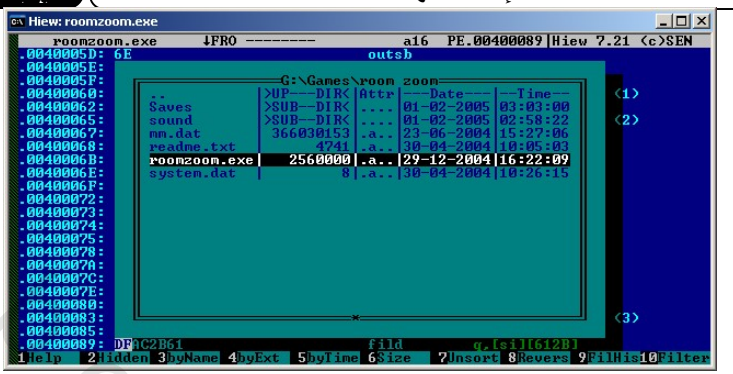


قم بالضغط مرة أخرى على مفتاح الإدخال لترى الملف بلغة التجميع وهذا هو أهم شكل نريده للتعديل في الملف .

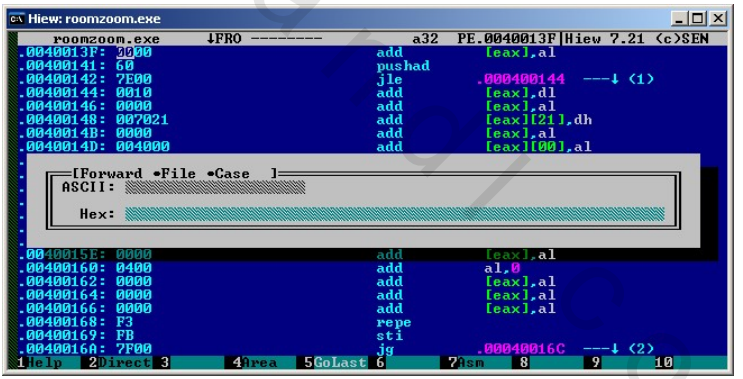


ومن الملاحظ أن المفاتيح في أسفل النافذة يتم تغييرها تبعا لشكل النافذة الحالية ويمكن بالضغط على المفتاح Ctrl أو Alt رؤية المزيد من الاختيارات.

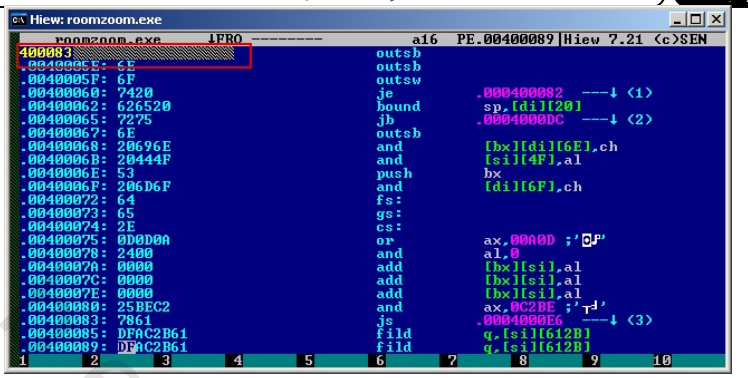
و يمكنك اختيار ملف أخر لفتحه عن طريق الضغط على المفتاح F9 .



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

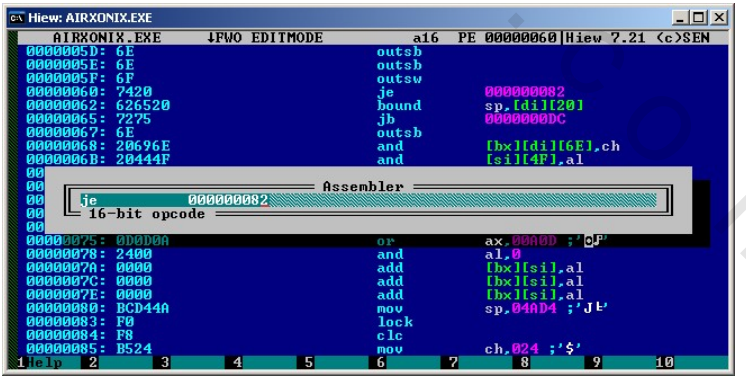


وللذهاب إلى اوفست أو عنوان محدد قم بالضغط على المفتاح F5 واكتب العنوان ثم اضغط مفتاح الإدخال ويتم الذهاب إليه على الفور.



لتعديل سطر معين قف على هذا السطر ثم اضغط على المفتاح F3 ويمكنك تعديل السطر في هذه الحالة بالنظام السداسي.

أما إذا أردت التعديل بكتابة تعليمات الاسمبلى فقم بالضغط بعد ذلك على مفتاح وبعد الانتهاء اضغط مفتاح الإدخال.

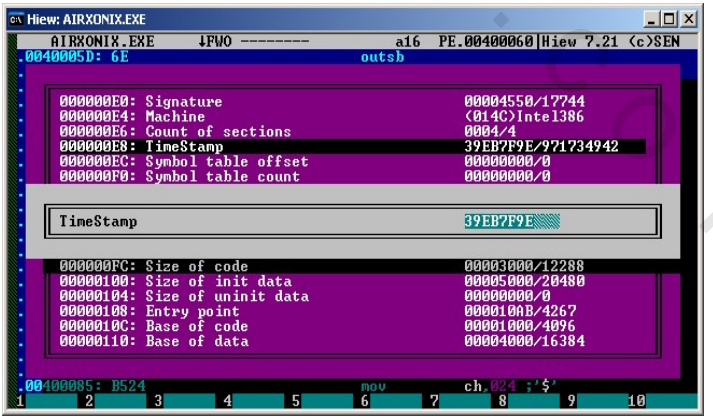


و بعد الانتهاء من كافة التعديلات اضغط F9 لحفظ التعديلات

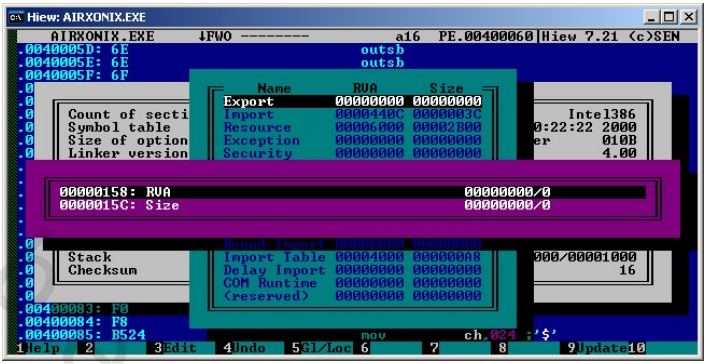
و يمكنك أيضا رؤية header الملف وتعديله بالخطوات التالية:

- قم بالضغط على المفتاح F8

- قم الآن بالضغط على F3 ثم اختار القيمة التي تريد تغييرها واضغط F3 مره أخرى

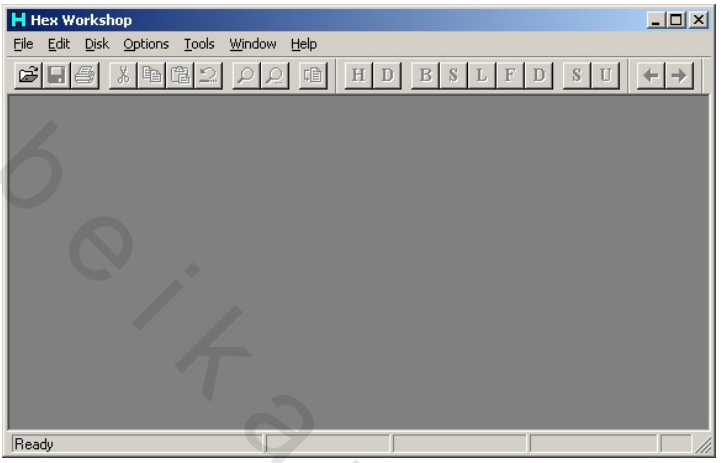


- لرؤية مقاطع الملف اضغط F10 وللتعديل فيها اضغط F3 ثم F3

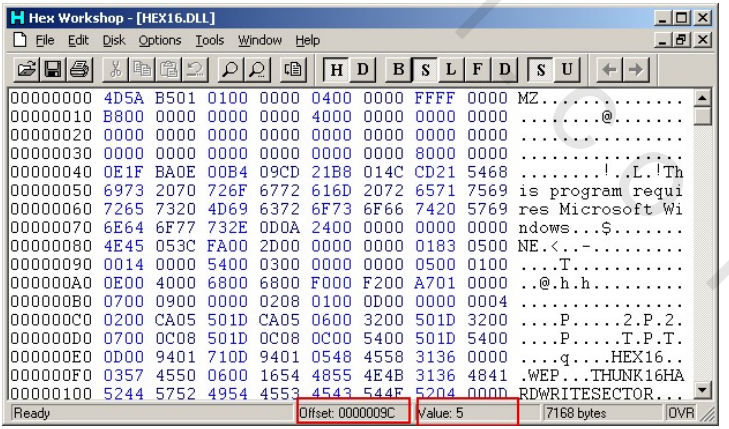


برنامج Hex workshop:

من البرامج الخفيفة والسريعة ويمكنه تعديل الملفات ذات الحجم الكبير

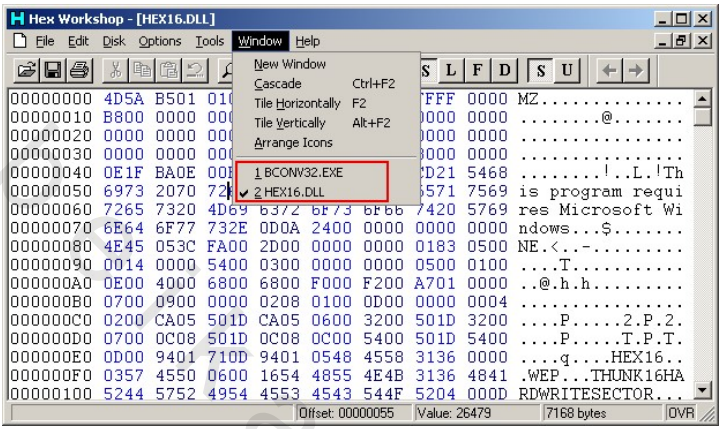


قم بفتح الملف المراد التعديل فيه بالا ومر File | Open ويقوم البرنامج بفتح نافذة مستقلة للملف يمكنك التعديل فيها مباشره بالنظام السداسي.

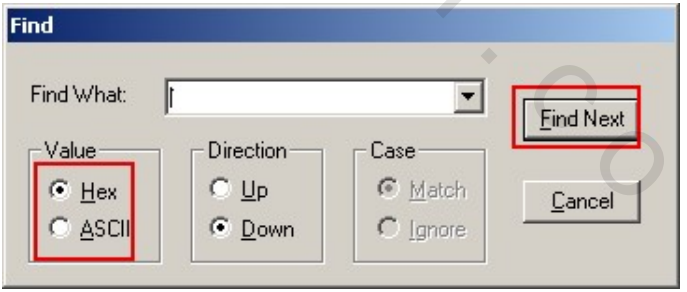


كما يمكنك معرفة الاوفست والقيمة الحالية له من شرط الحالة بأسفل البرنامج

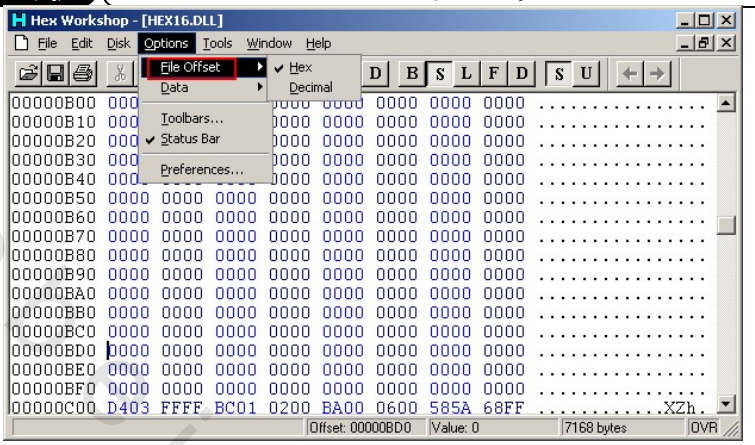
ومن مزايا هذا البرنامج إمكانية فتح أكثر من ملف والتنقل بينهم عن طريق نافذة Window



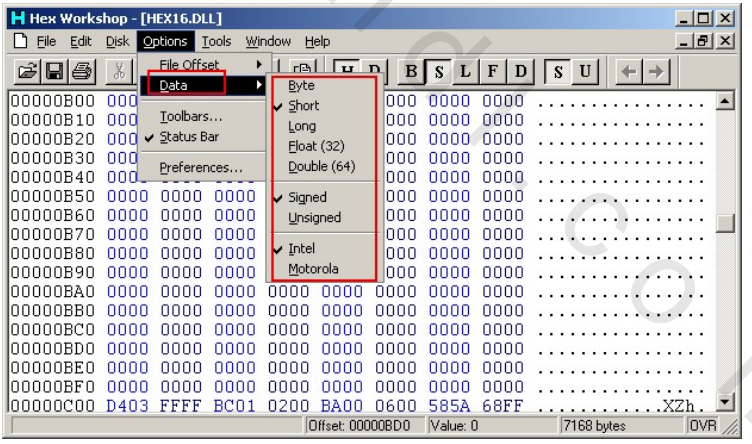
للبحث في البرنامج قم بالضغط على Alt + F3 ويمكنك من خلال ديالوج البحث كتابة نص ASCII أو أرقام بالنظام السداسي.



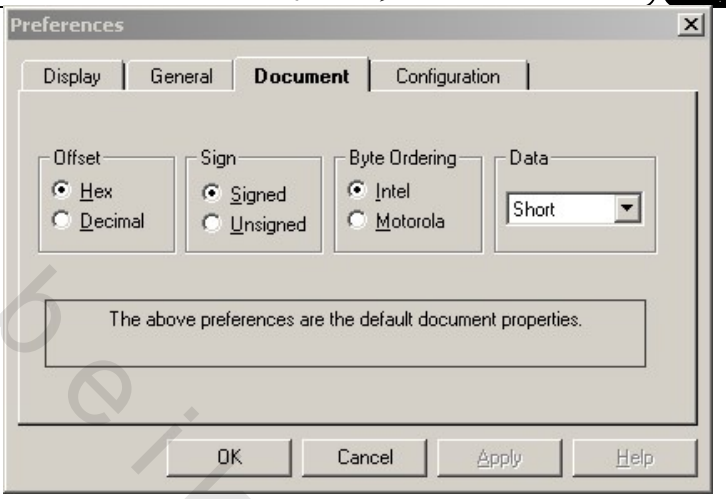
ومن قائمة Option يمكنك تغيير طريقة عرض البيانات في البرنامج فيمكنك عرض العناوين بالنظام العشري أو السداسي.



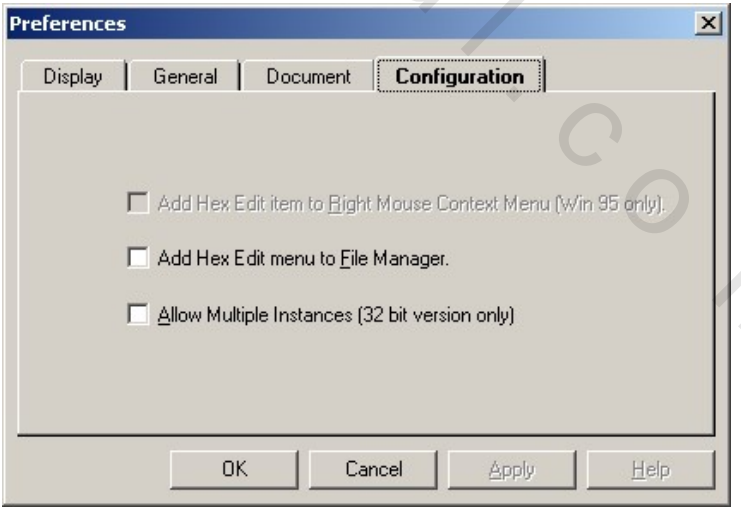
كما يمكنك التحكم في عرض بيانات الملف نفسه من الأمر Data واختيار نوع البيانات المراد.



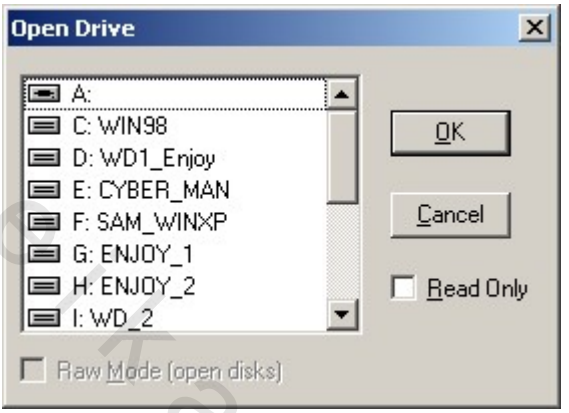
ويمكنك اختيار الشكل الافتراضي للملف من خلال الأمر Preferences واختيار الصفحة Document.



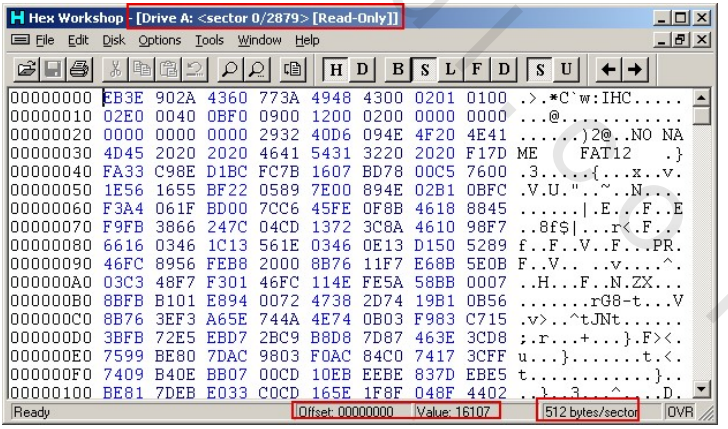
ويمكنك وضع أمر للتحرير بواسطة هذا البرنامج في قائمة الأوامر المختصرة الخاصة بالويندوز عندما تقوم باختيار أي ملف ويتم ذلك من الصفحة configuration



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

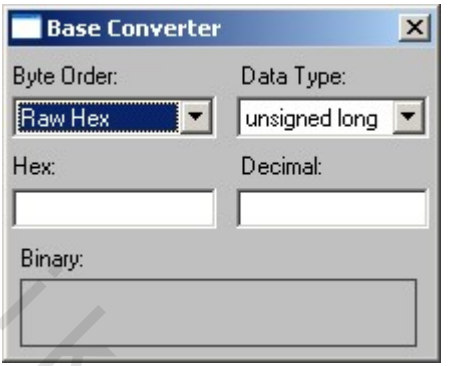


و يمكنك التعديل في sector المشغل نفسه



يحتوى البرنامج أيضا على عدة أدوات هامه وهى:

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

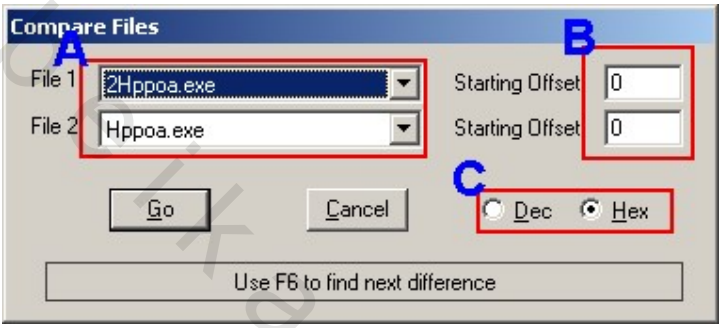


- آله حاسبه بالنظام السداسي Tools | Hex calculator

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

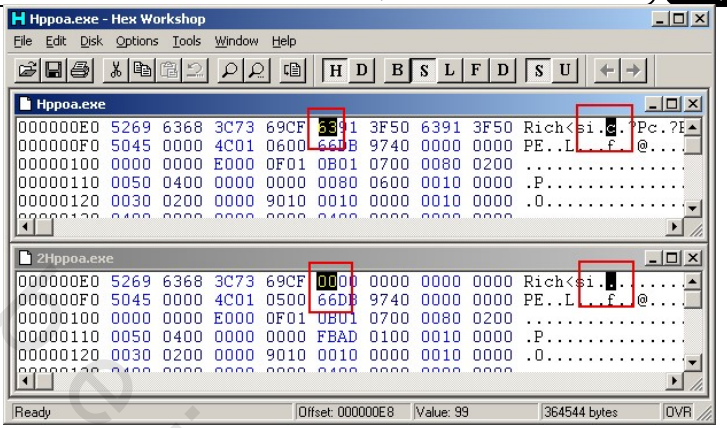
أداة المقارنة:

من المزايا الهامة لهذا البرنامج إجراء مقرنه سريعة على ملفين ولكي يمكنك القيام بذلك قم أولا بفتح الملفين المراد مقارنتهم ثم افتح ديالوج 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

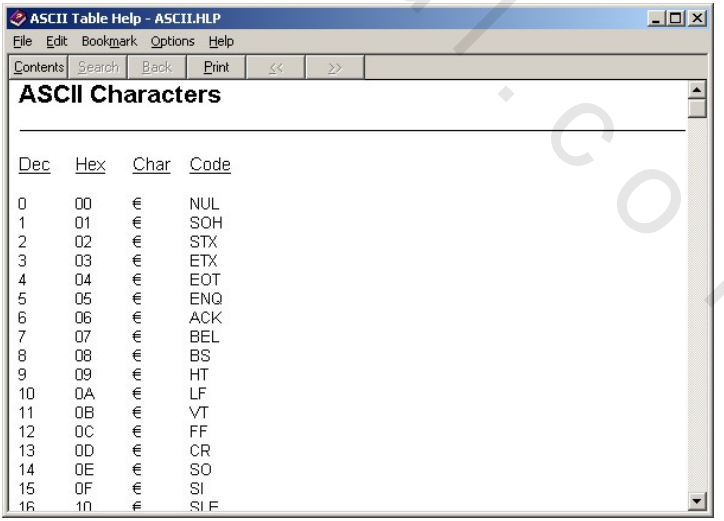
اضغط على مفتاح ok ويقوم البرنامج بالوقوف على أول مكان يوجد به الاختلاف ولكي ترى المقارنة بوضوح بين الملفين قم باختيار الأمر Window Tile Horizontally | أو F2



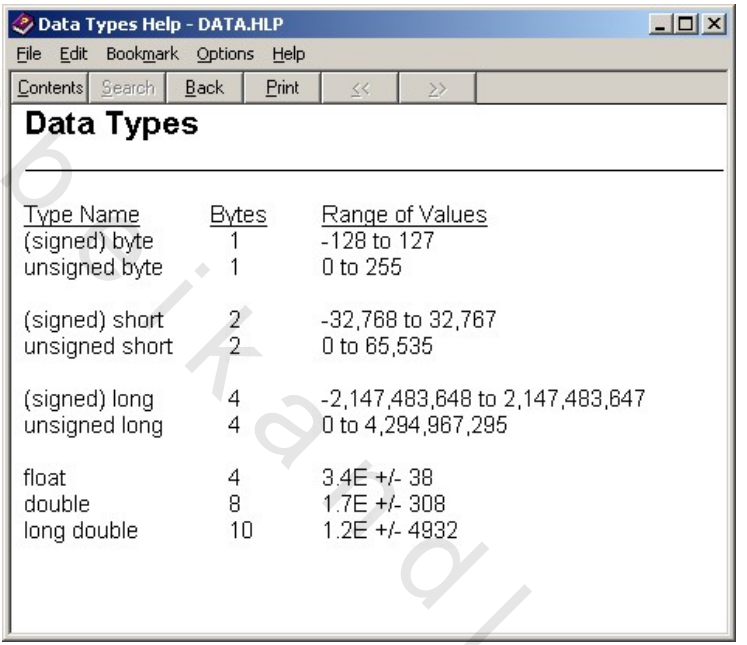
ولكي ترى مزيد من الاختلاف قم بالضغط على المفتاح F6

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



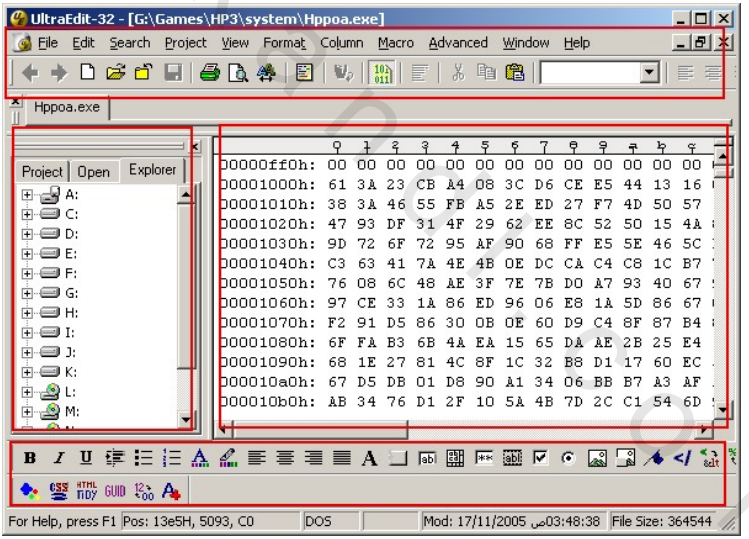
ولكي ترى أنواع البيانات المختلفة ومدى كل نوع قم باختيار الأوامر help | Data Types



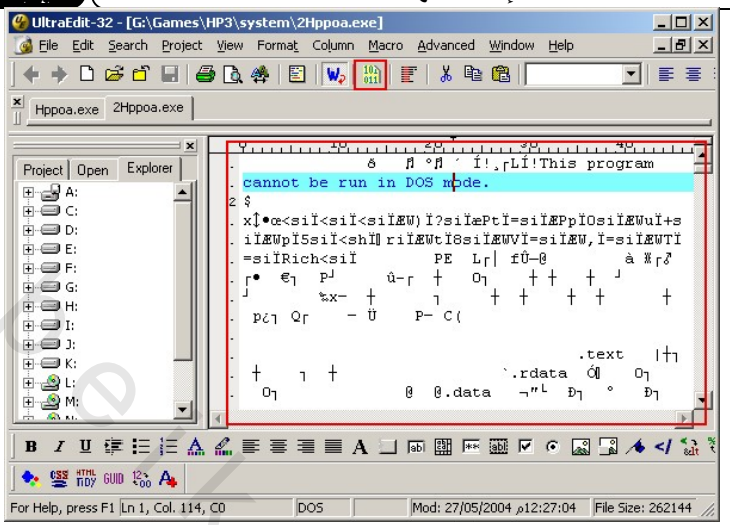
برنامج Ultra-Edit:

هذا البرنامج اكبر حجما من برنامج Hex Workshop ويحتاج لتنصيبه 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.

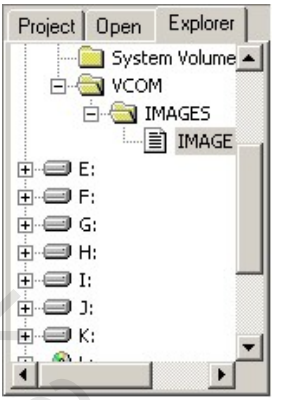


قم أولا كما تعرف باختيار ملف وفتحه من القائمة File | Open ويتم فتح الملف في نافذة والتعديل فيه مباشرة ويمكنك عرض الملف بشكل نصي عن طريق الأوامر Hex Edit | Hex function | Edit وبالعكس.

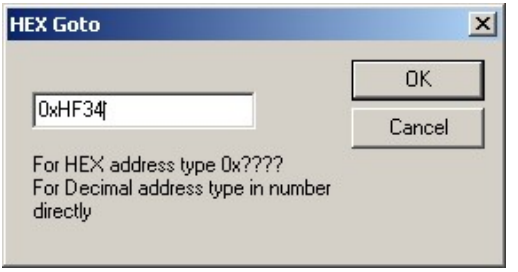


- وتحتوى لوحة الأدوات صفحة تسمى Open يمكنك من خلالها اختيار آخر ملفات قمت بفتحهم بسرعة.

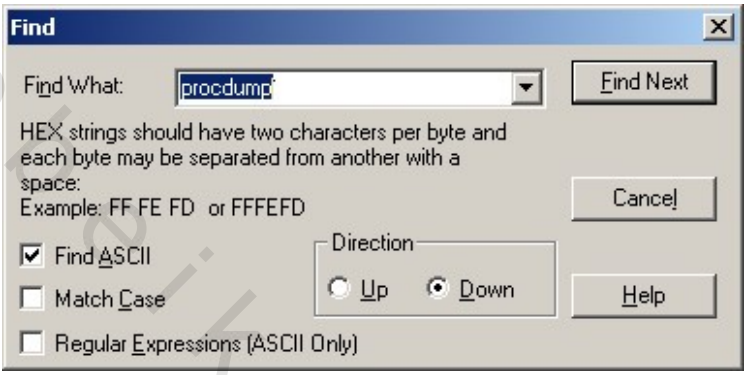
كما يمكنك فتح الملف الذي تريده مباشره من الصفحة Explorer باختيار رمز المشغل واختيار الملف.



- 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



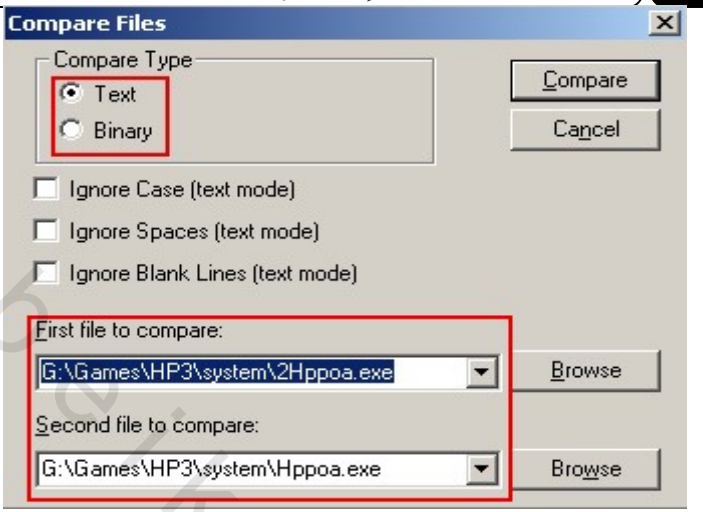
أما إذا أردت البحث عن نص محدد أو كود سداسي فقم باختيار الأوامر Search | Find أو Alt+F3



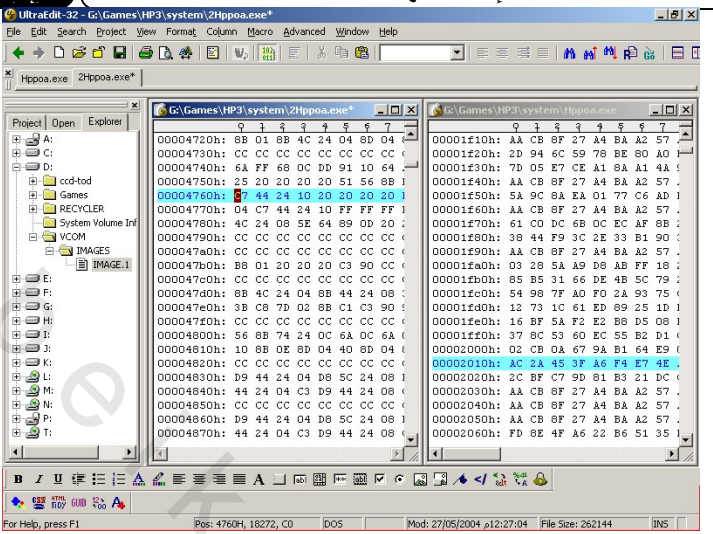
كما يمكنك التنقل بين نتائج البحث عن طريق مفاتيح الاختصار التالية:

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

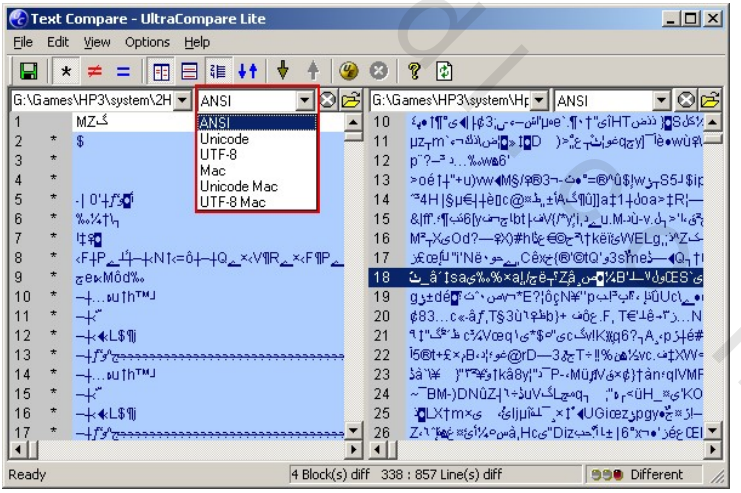
ولكي تقوم بمقارنة ملفين قم باختيار الأوامر File | Compare Files



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



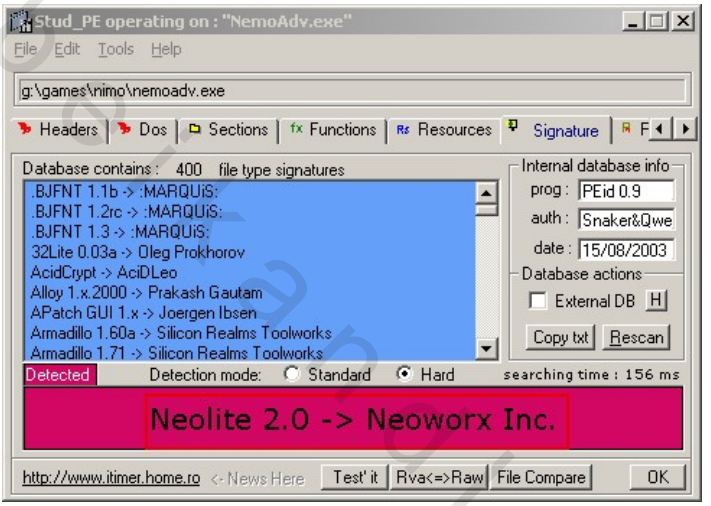
كما يقوم البرنامج بفتح الملفين بشكل نصي ويعطى أكثر من اختيار لتشكيل النص المعروض.



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 تعطى الإمكانية لفك تشفير وضغط الملفات بالطرق الشهيرة مثل ASPack وPE Shrink وArmadillo وNeolite وغيرها ويجب عليك أولا معرفة نوع التشفير ويتم ذلك ببرنامج Peid أو STUD_PE



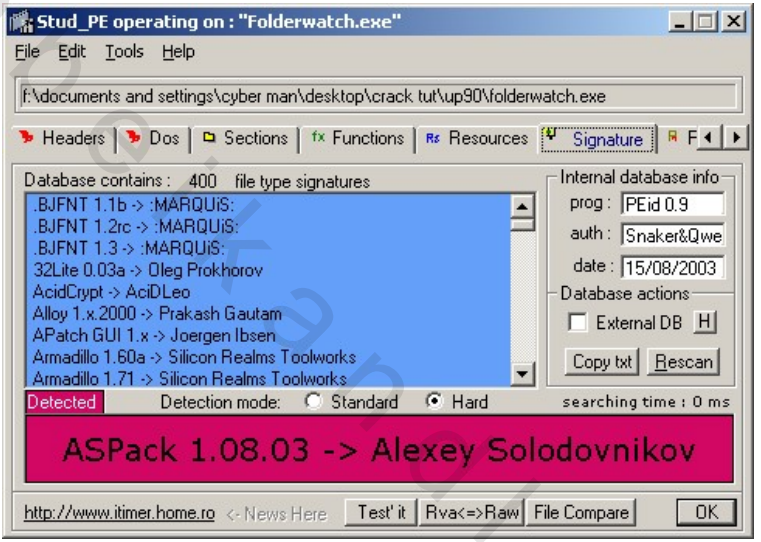
و فيما يلي أمثله عمليه:

ملحوظة: ستجد في الاسطوانة المرفقة البرامج اللازمة للأمثلة.

شفرة ASPack:

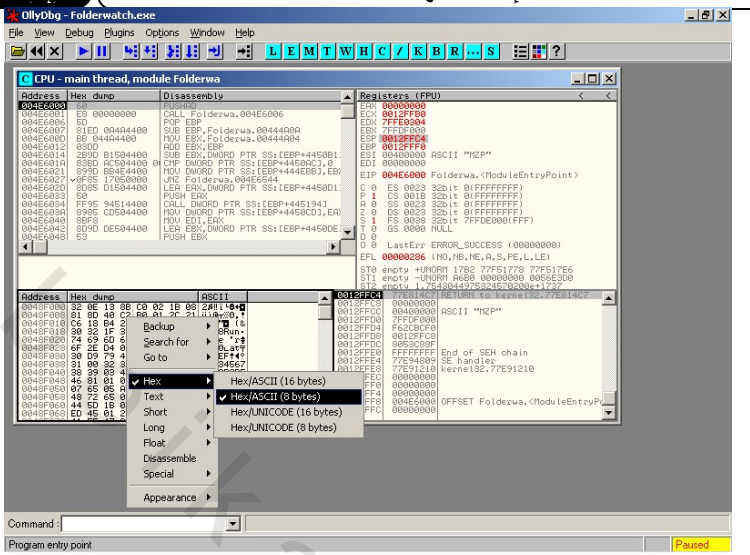
الأدوات: STUD_PE, Import Rec, Ollydbg

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

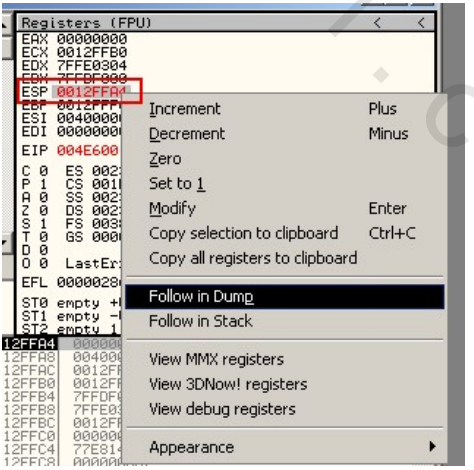


سنذهب الآن إلى برنامج ollydbg لمعرفة نقطة الدخول الحقيقية للبرنامج أو EIP افتح ollydbg وحمل البرنامج بداخله.

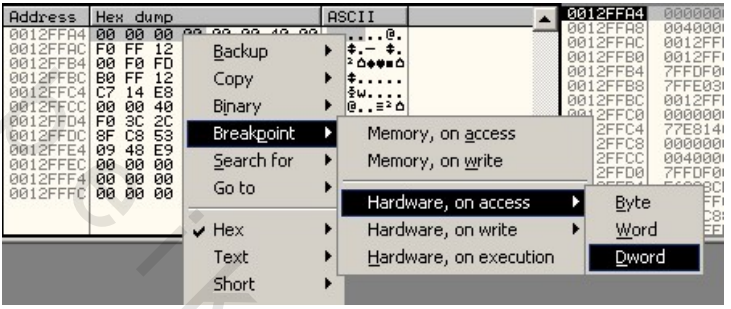
وقم بتحويل منظر الرؤية في نافذة ال dump إلى النظام السداسي.



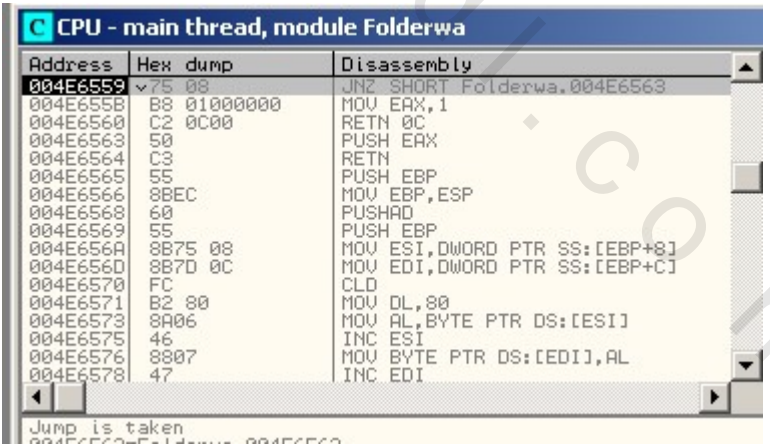
قم الآن بالضغط على مفتاح التتبع F8 ثم اذهب إلى نافذة المسجلات وقف على المسجل ESP واختر الاختيار follow in dump



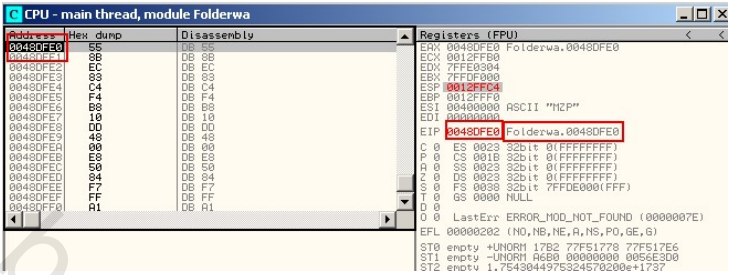
ستجد نافذة ال dump تقف الآن عند محتويات المسجل قم باختيار أول اربع بايتات واختار من قائمة الأوامر المختصرة أمر التوقف hardware on access | Dword



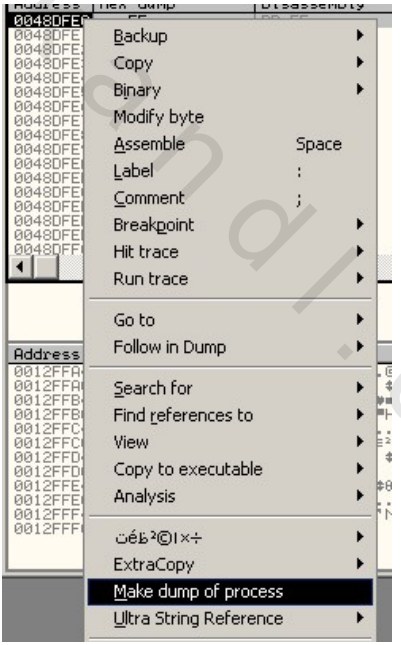
قم بالضغط على مفتاح التشغيل F9 ستجد أن البرنامج يقف عند العنوان الذي به الأمر JNZ



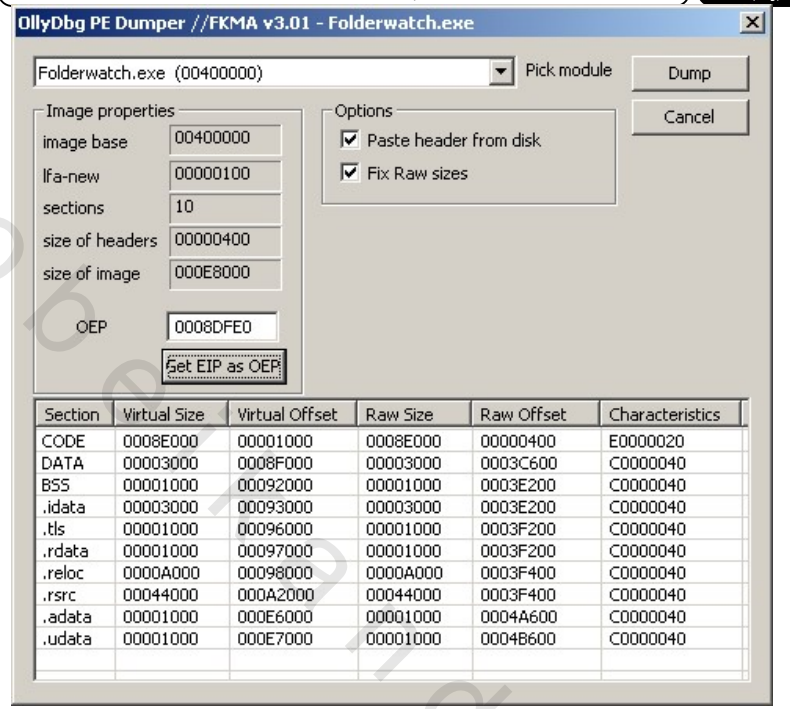
اضغط المفتاح F8 حوالي ثلاث مرات حتى تصل للعنوان 0048DFE0 وهو العنوان الحقيقي لنقطة الدخول EIP كما يتضح من نافذة المسجلات



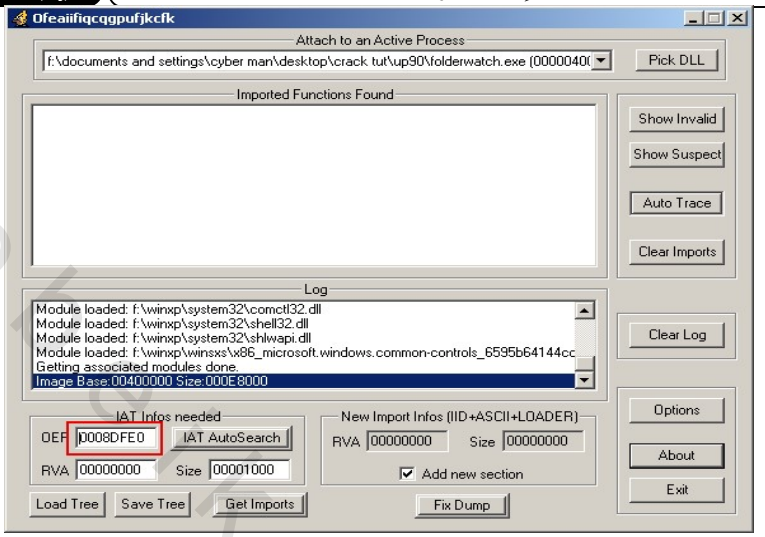
قم بالماوس على العنوان السابق واختار الأمر dump debugged process



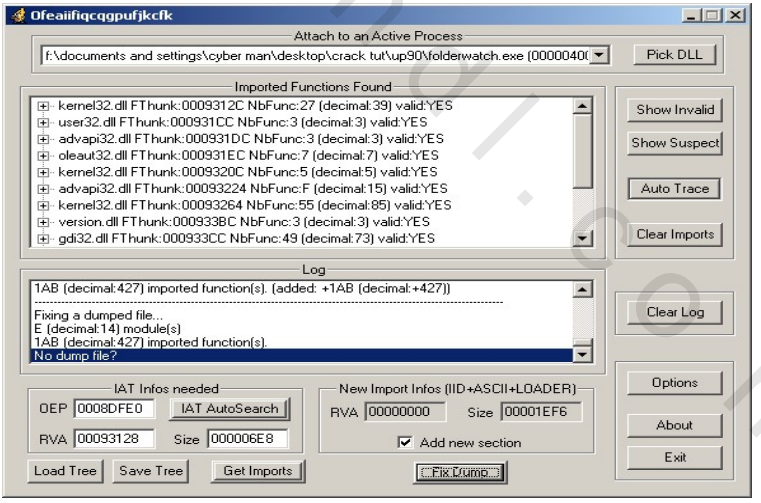
و يتم ظهور الديالوج التالي:



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



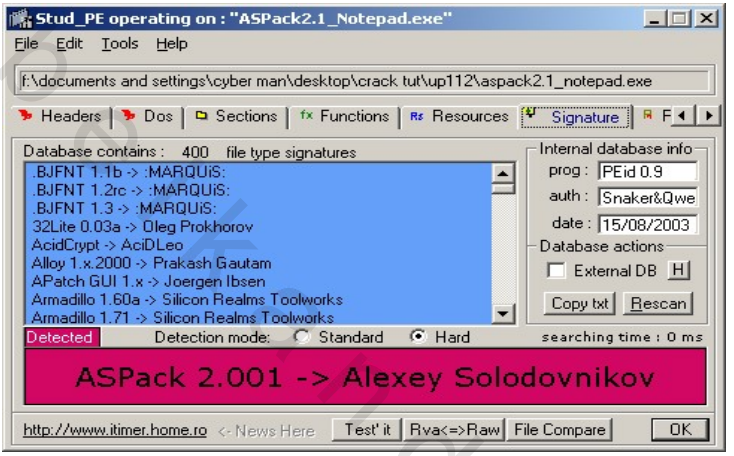
و لا يحتاج البرنامج في هذه الحالة إلى إصلاح اضغط على fix dump واحفظ الملف الجديد وهكذا تم استخراج الملف التنفيذ الحقيقي.

برنامج Notepad:

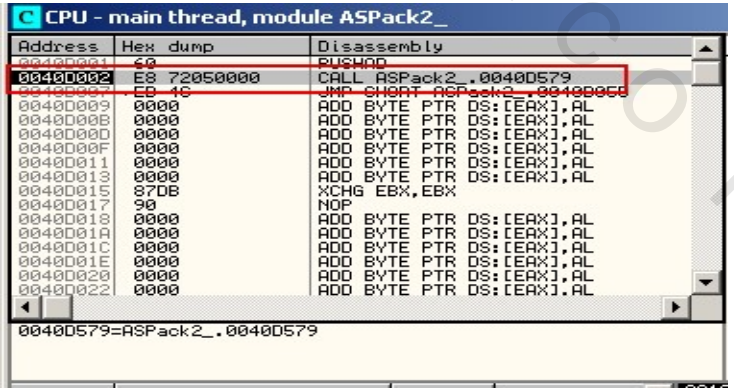
الحماية: aspack

الأدوات: ollydbg, import rec, stud_pe

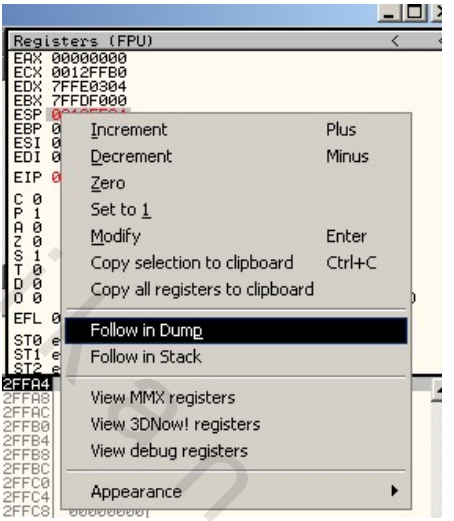
- للتأكد من نوع الحماية قم بفتح الملف في برنامج Stud_pe



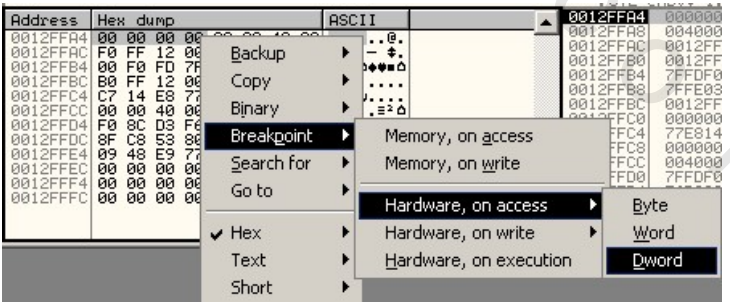
- والآن قم بفتح الملف في برنامج ollydbg واضغط F8 مرة واحدة.



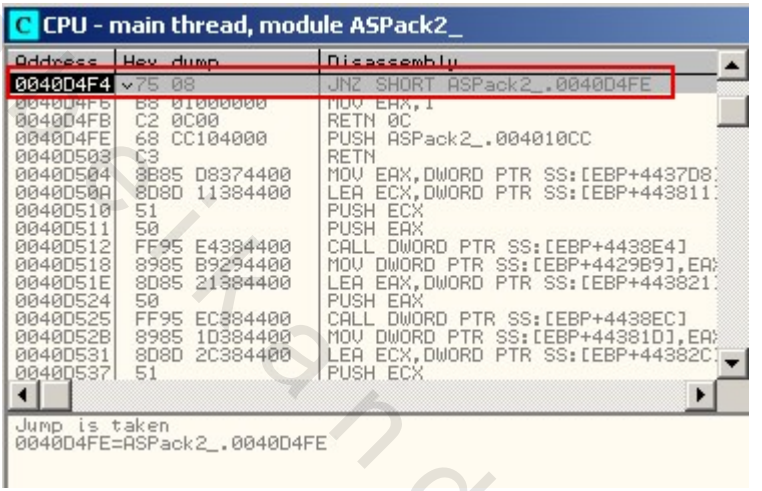
- والآن انتقل إلى قسم المسجلات واختار الأمر follow in dump من القائمة المختصرة بالماوس وأنت تقف على المسجل ESP



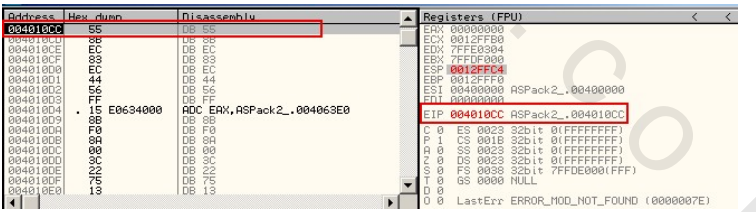
- من نافذة dump اختر بالماوس أول أربع بايت واضغط على المفتاح الأيمن ومن القائمة المختصرة اختر الأوامر breakpoint | hardware on access | dword



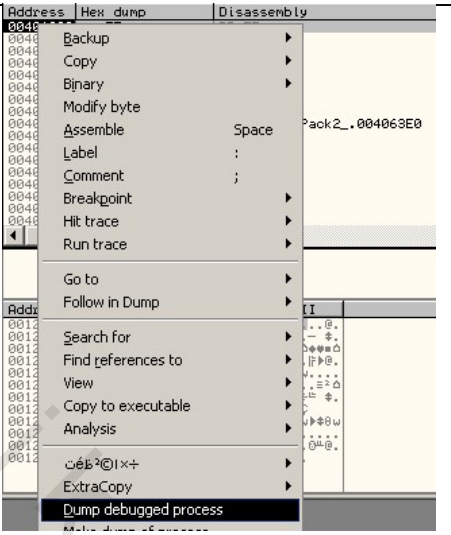
- والآن اضغط F9 حتى يقف البرنامج ودائما في هذا النوع من الحماية يجب أن تجد مكان الوقوف هو أمر القفز JNZ والذي يقوم بالقفز إلى مكان الملف الحقيقي.



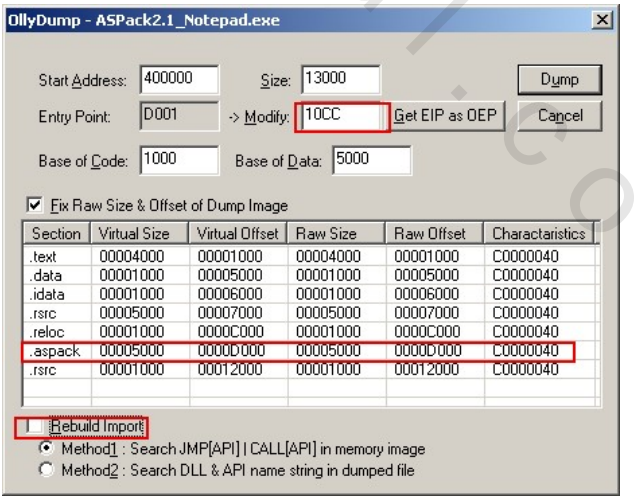
- اضغط F8 ثلاث مرات حتى تصل للشكل التالي:

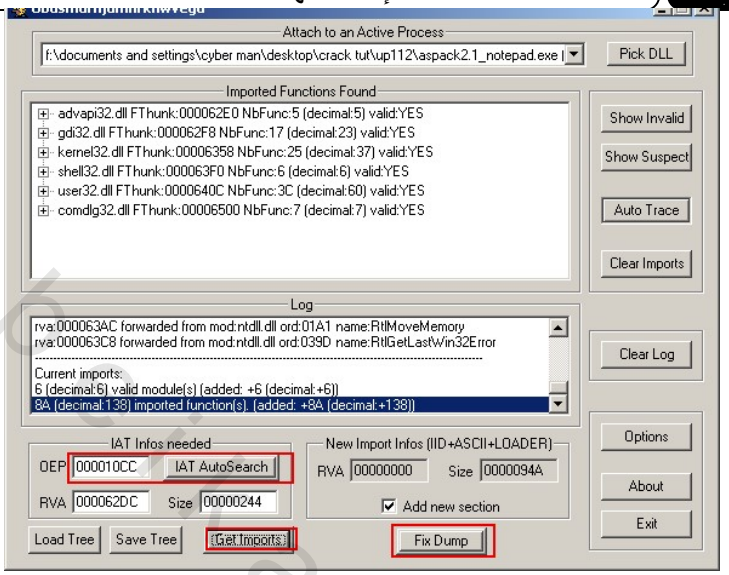


و هكذا نكون وصلنا للمكان الحقيقي للملف قف الآن على هذا العنوان ثم اختار من القائمة المختصرة الأمر dump debugged process

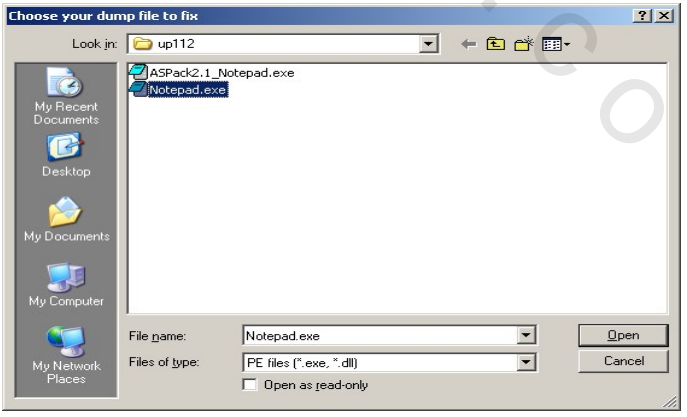


- يتم ظهور ديالوج التفريغ وتأكد من وجود العنوان الحقيقى 10CC وإزالة الاختيار rebuild import

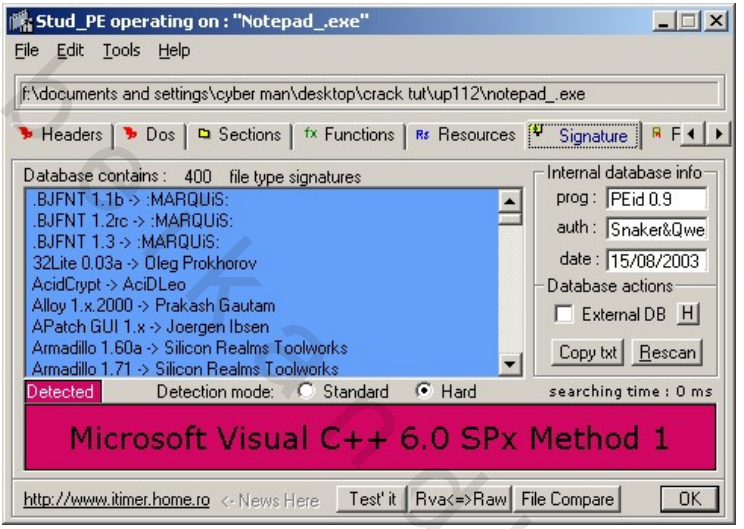




تأكد من إدخال العنوان الحقيقي OEP ثم اضغط على المفتاح IAT Auto search ثم get imports وأخيرا fix dump كما فعلنا سابقا واختار الملف الذي قمت بتفريغه



و سيقوم البرنامج بإنشاء ملف جديد بالاسم notepad_.exe وإذا أردت التأكد من إزالة الحماية قم يوضع الملف الناتج في برنامج stud_pe ويجب أن تجد اسم اللغة المستخدمة في البرنامج وليس حزمة التشفير

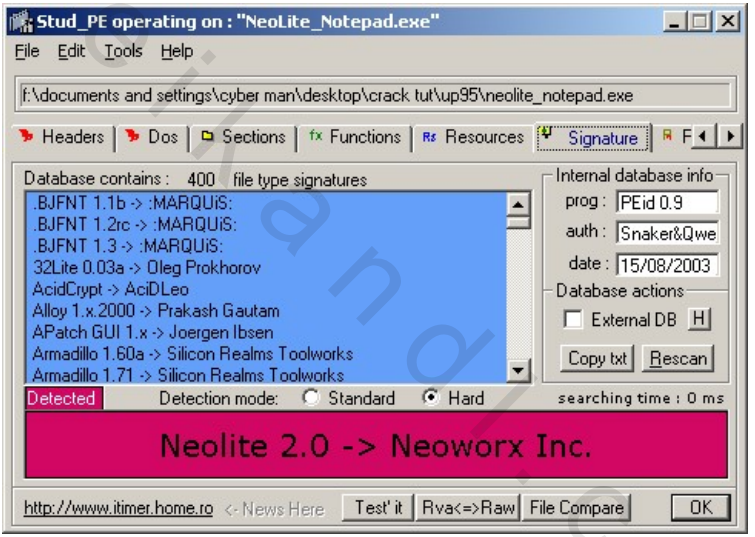


شفرة NeoLite:

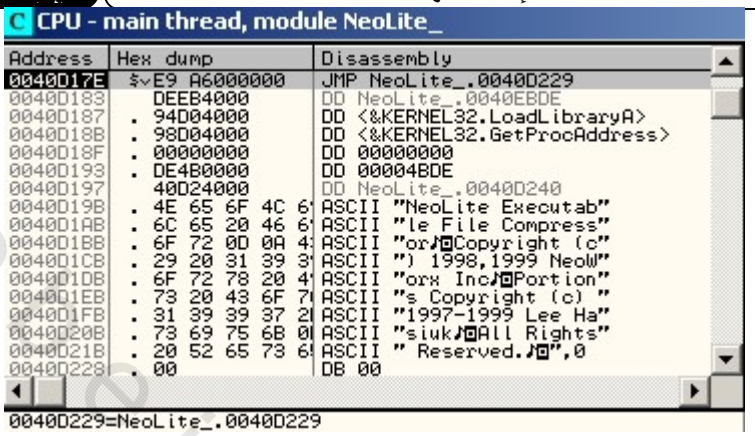
المثال: NotePad

الأدوات: ollydbg, stud_pe, import rec

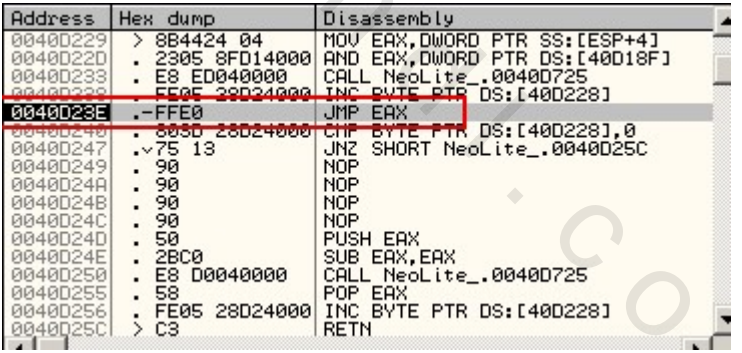
هذه الشفرة من أسهل الشفرات التي يمكن فكها قم الآن بفتح برنامج المثال في برنامج stud_pe للتعرف على نوع الحماية ويجب أن تحصل على النتيجة الآتية:



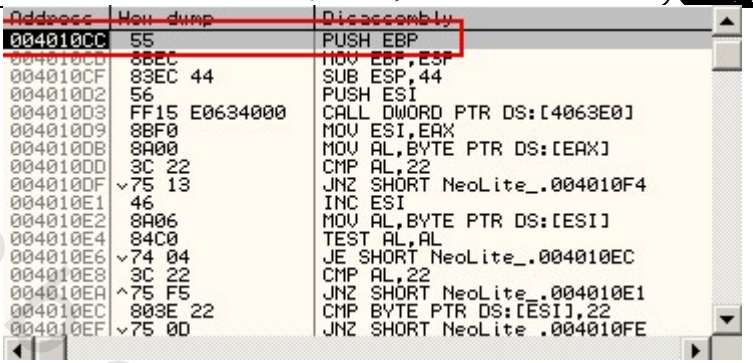
و الآن بعد أن تأكدنا من وجود الشفرة قم بتحميل برنامج المثال في ollydbg – قم الآن بفتح البرنامج import rec .



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

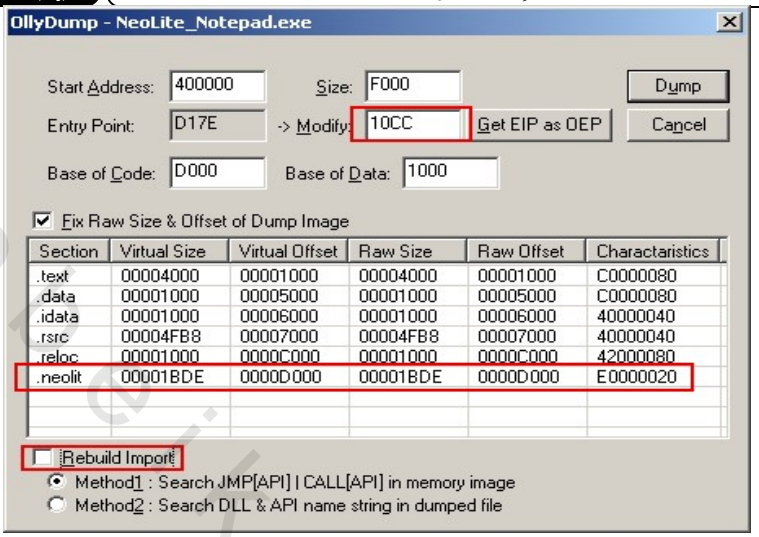


ملحوظة: عندما تظهر رسالة للذهاب إلى موقع الشفرة اجب بـ No

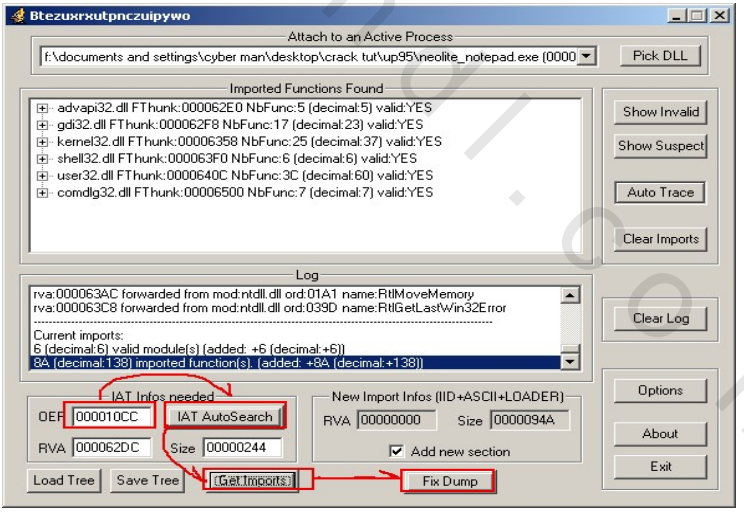


لاحظ هنا تساوى قيمة المسجل EIP مع العنوان الحالي وهذا يدل على بداية الملف الحقيقية ويمكننا أن نحصل على العنوان الحقيقي بطريق أخرى ولكن هذه أسهل طريقة ، قم الآن بفتح قائمة الأوامر المختصرة واختر الأمر Dump debugged Process

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



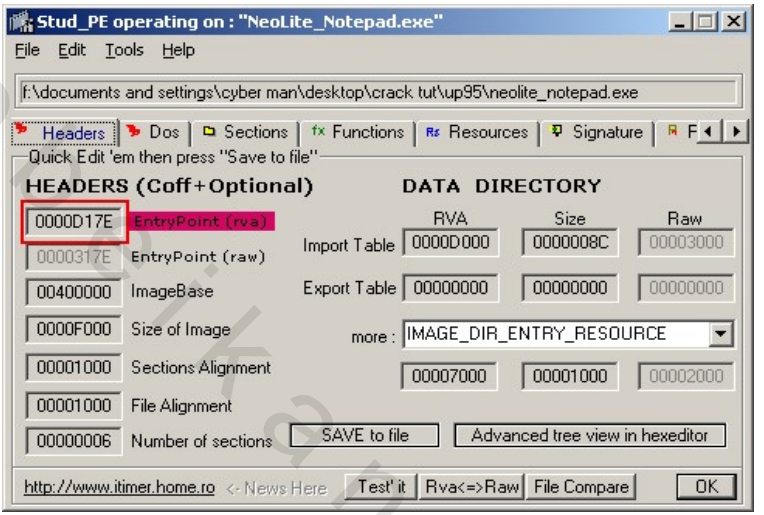
اضغط مفتاح Dump واحفظ الملف بأي اسم ثم قم بفتح البرنامج import rec وقم باختيار برنامج notepad



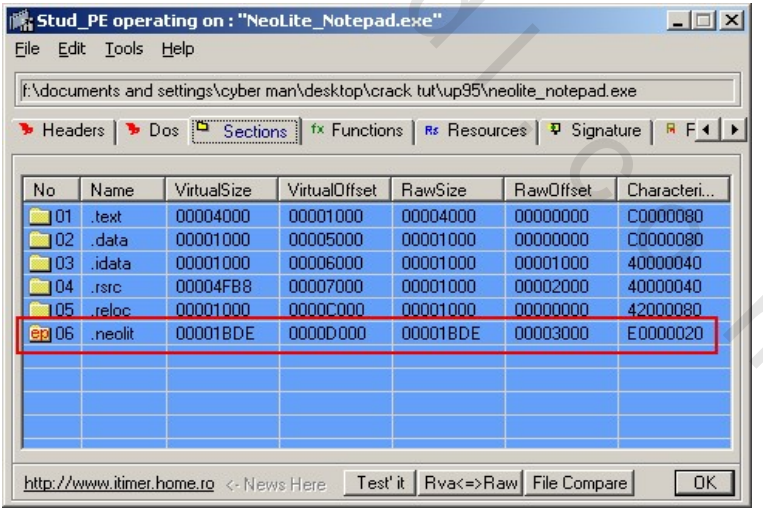
قم بتعديل OEP للقيمة 10CC ثم اضغط المفتاح IAT Auto Search ثم المفتاح Get Imports ثم Fix Dump وبذلك تم فك شفرة Neolite

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:

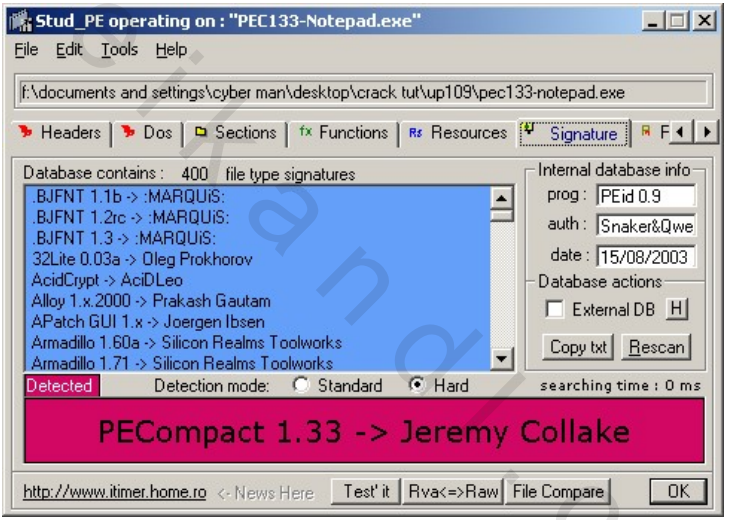
OEP = 0000D17E - (0000D000 - 00003000)
OEP = 0000317E

شفرة PE Compact:

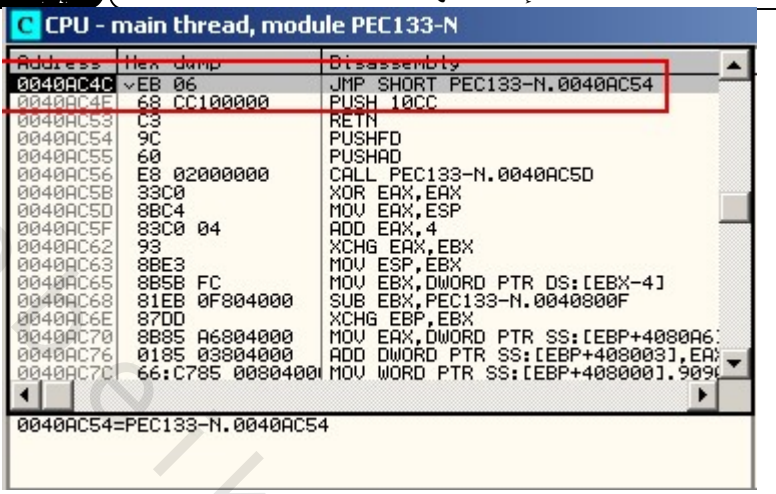
البرنامج : notepad

الأدوات: ollydbg, import rec, stud_pe

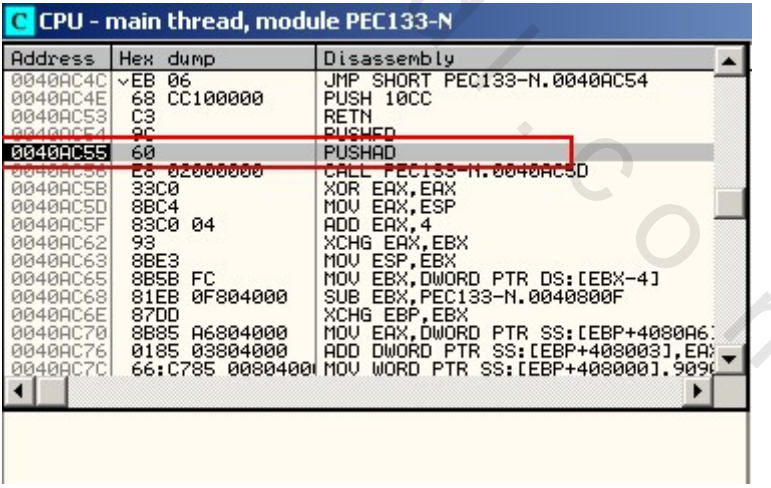
سنقوم أولا بتحميل notepad في برنامج stud_pe لمعرفة نوع الحماية وسنجدها pe compact وسنقوم في هذه الحماية باستخدام نقاط توقف في الذاكرة كما سيتضح فيما بعد.



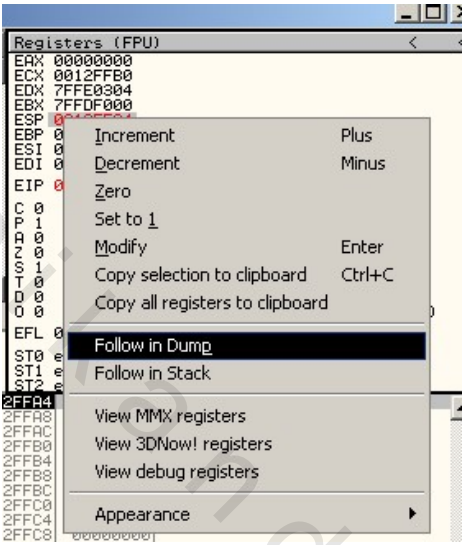
- أغلق برنامج stud_pe ثم قم بتحميل الملف في برنامج ollydbg ويجب أن ترى الأمر JMP كما بالشكل التالي:



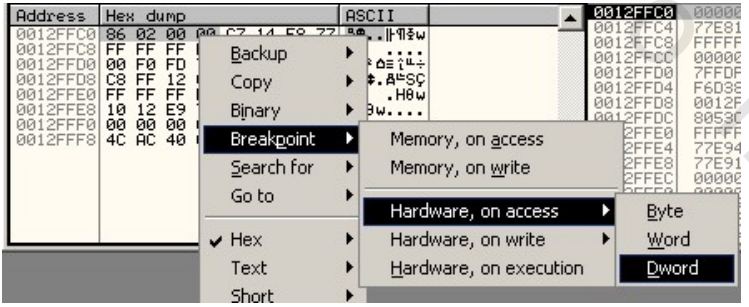
الأمر التالي هو الذي يحتوى عنوان الملف الحقيقي OEP قم بالضغط مرتين على المفتاح F8 حتى تقف على الأمر pushed



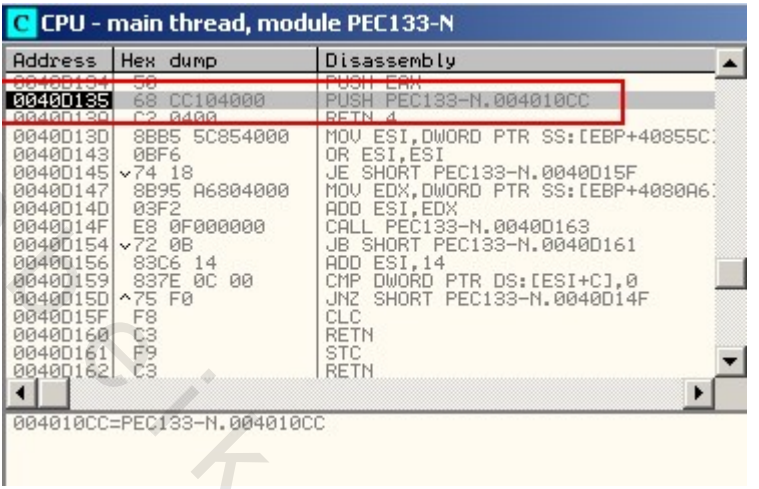
- قم الآن باختيار الأمر follow in dump من قائمة الأوامر المختصرة وأنت تقف على المسجل ESP



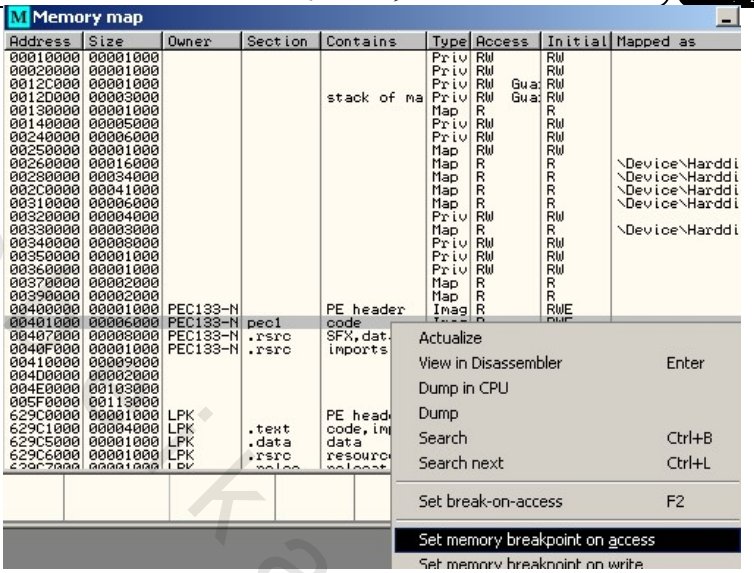
- واذهب إلى نافذة dump وقف على أول أربع بايت واختار الأوامر التالية breakpoint | hardware, on access| dword



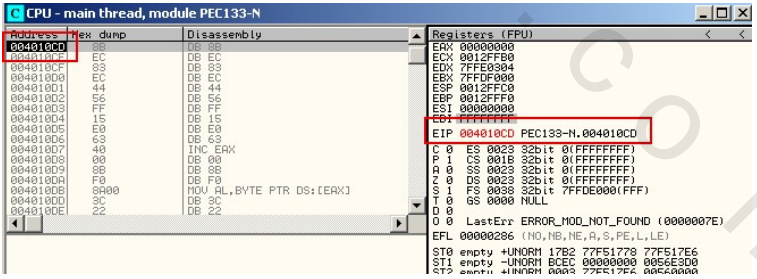
- بعد ذلك اضغط shift+F9 لتصل للأمر push eax



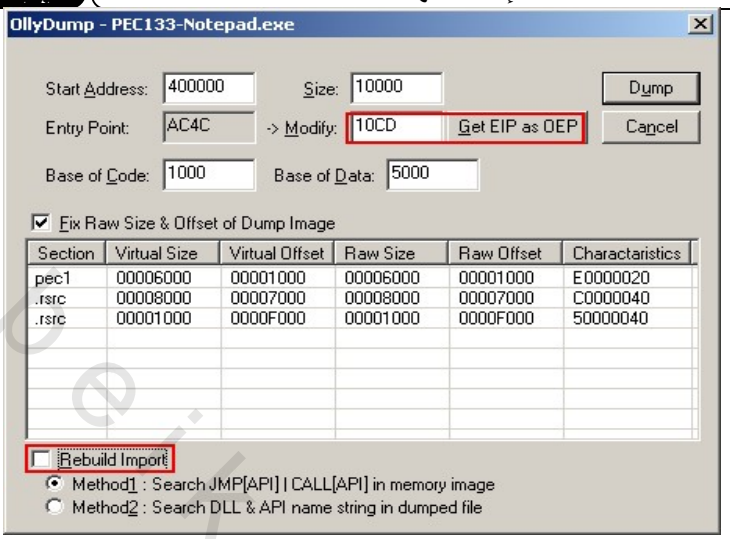
- اضغط المفتاح F8 مره واحده ويجب أن تكون الآن على نقطة الدخول الحقيقة للملف وسنقوم الآن بوضع نقطة الإيقاف في الذاكرة لذلك قم بالضغط على ALT+M لفتح نافذة الذاكرة وتأكد من الوقوف على المقطع code ثم قم باختيار الأمر التالي set memory breakpoint on access



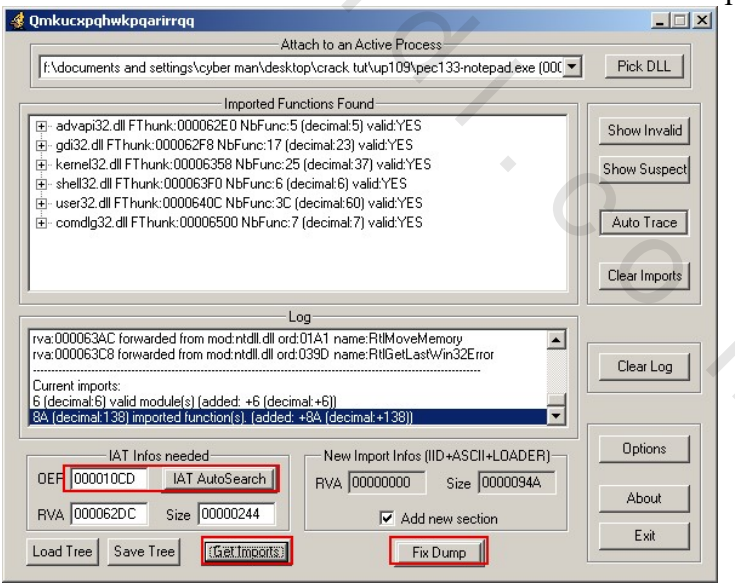
بعد ذلك قم بالضغط مره واحده على المفتاحين SHIFT+F9 لان البرنامج في هذه الحالة يقوم بالتوقف عند خطأ والضغط على المفتاحين السابقين يعطى إمكانية تخطى هذا الخطأ . و هكذا نكون وصلنا للعنوان الحقيقي وكما قمنا من قبل استخدم الأمر dump debugged process



بعد ذلك يظهر ديالوج التفريغ أزل علامة التصليح rebuild import واضغط على المفتاح dump

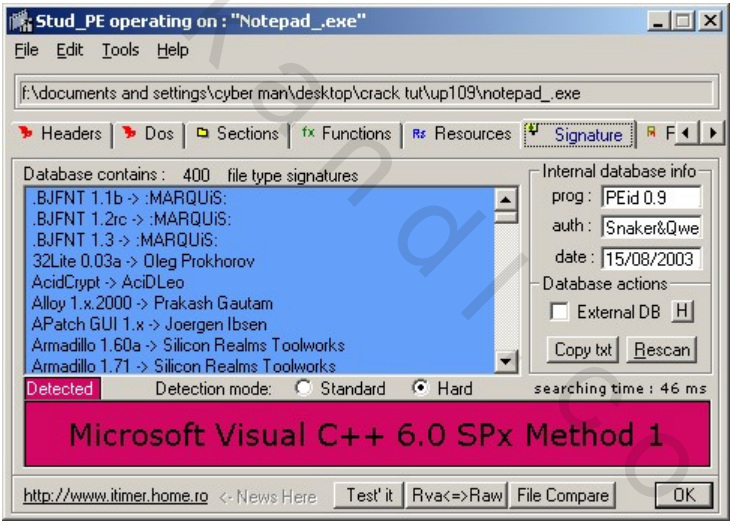


افتح الآن برنامج import rec وقم بتحميل الملف من الذاكرة وادخل عنوان OEP وهو 10CD ثم اضغط IAT AutoSearch ثم Get Imports ثم fix dumps



تأكد من اختيار الملف الذي قمنا بتفريغه 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++

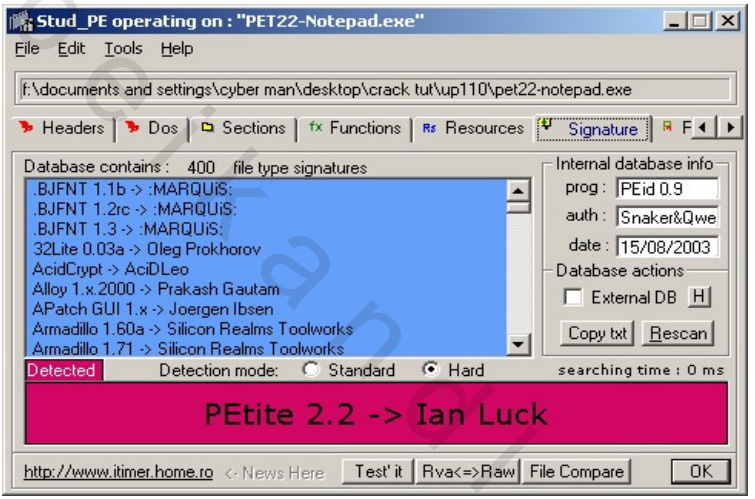


شفرة PEtite:

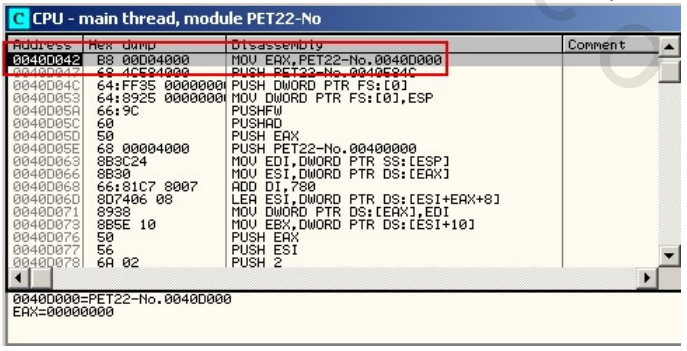
البرنامج : notepad

الأدوات: ollydbg, stud_pe, import rec

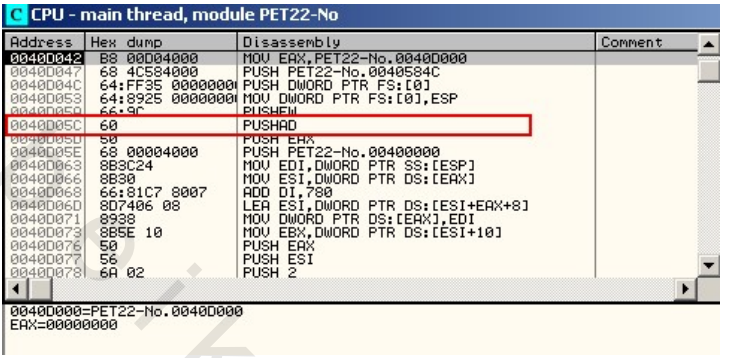
قم بتحميل الملف في برنامج stud_pe للتعرف على نوع الشفرة ومن الصفحة signature يمكننا أن نرى وجود شفرة Petite.



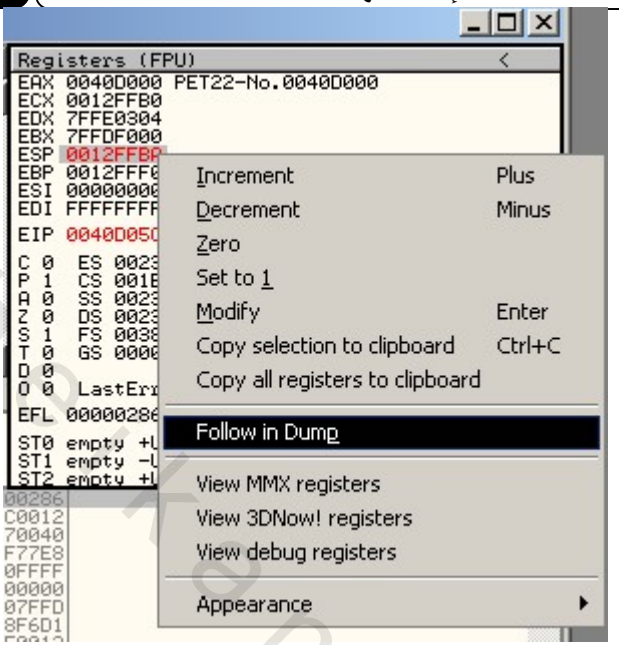
قم الآن بتحميل الملف في برنامج ollydbg ويقف البرنامج الآن على الأمر MOV EAX, Notepad



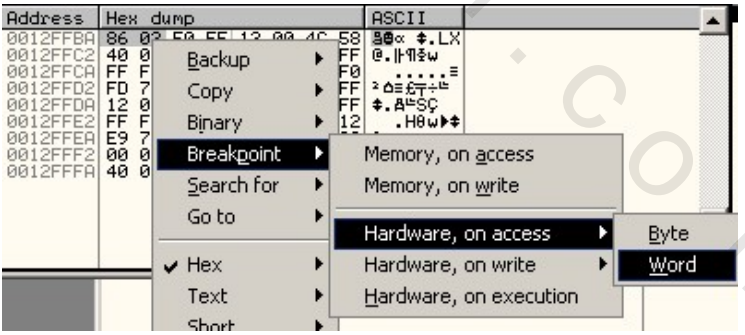
قم الآن بالضغط خمس مرات على المفتاح F8 حتى تصل للمكان PUSHAD



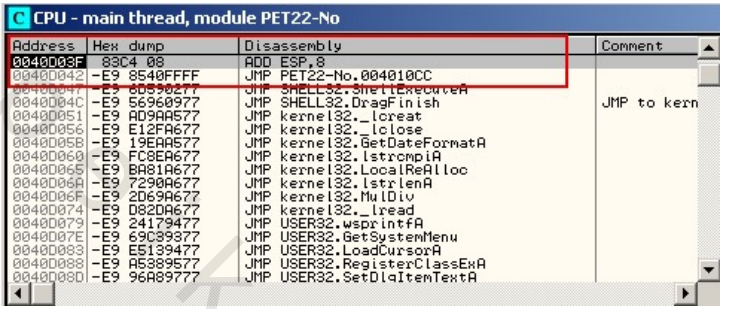
و الآن قف على المسجل ESP واختار الأمر follow in dump من قائمة الأوامر المختصرة.



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 ثم اضغط مره واحده على المفتاحين Shift+F9

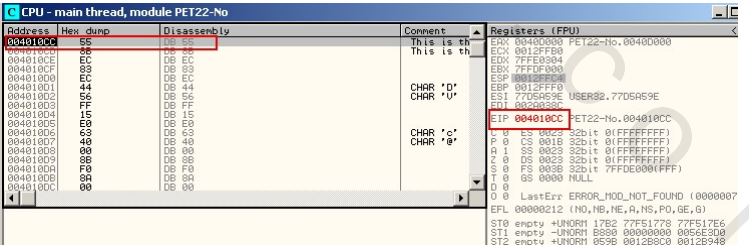


لاحظ السطرين التاليين

Add ESP, 8
JMP Notepad

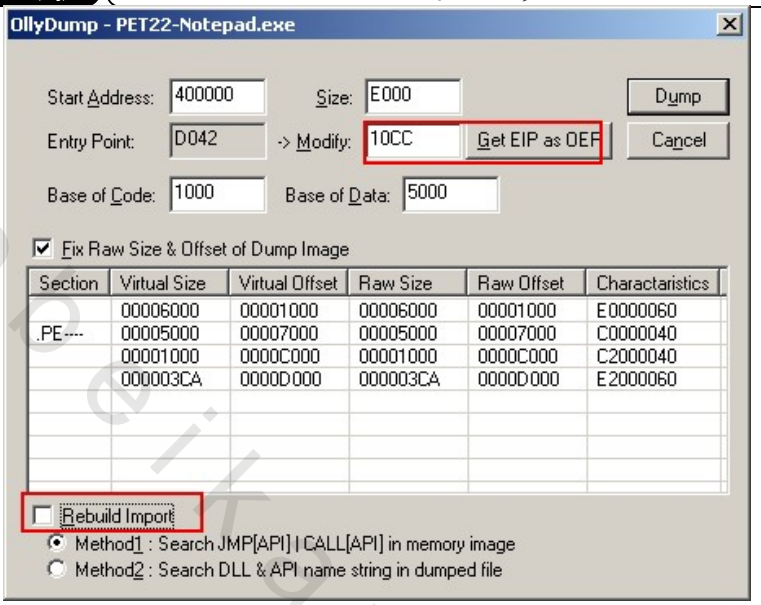
يتم تكرارهم في البرامج المحمية بشفرة PEtite

قم الآن بالضغط مرتين على المفتاح F8 حتى تصل للشكل التالي

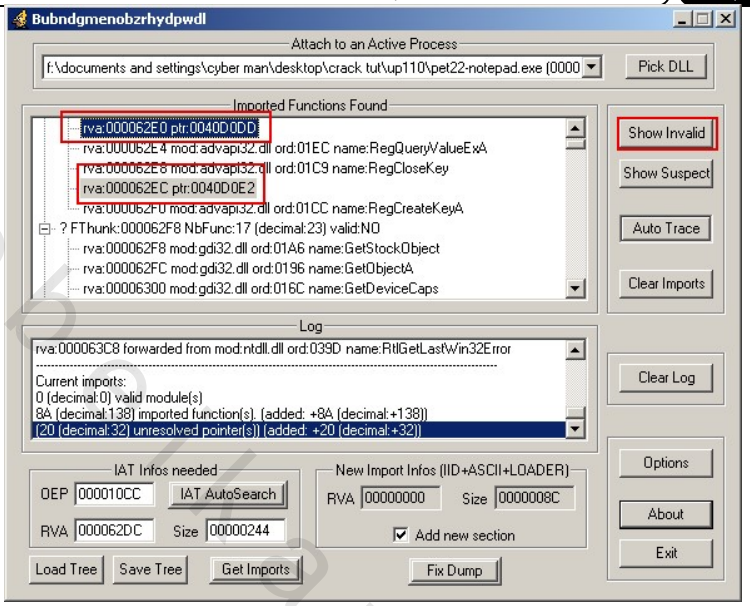


و نجد أن نقطة الدخول الحقيقية هي 10CC

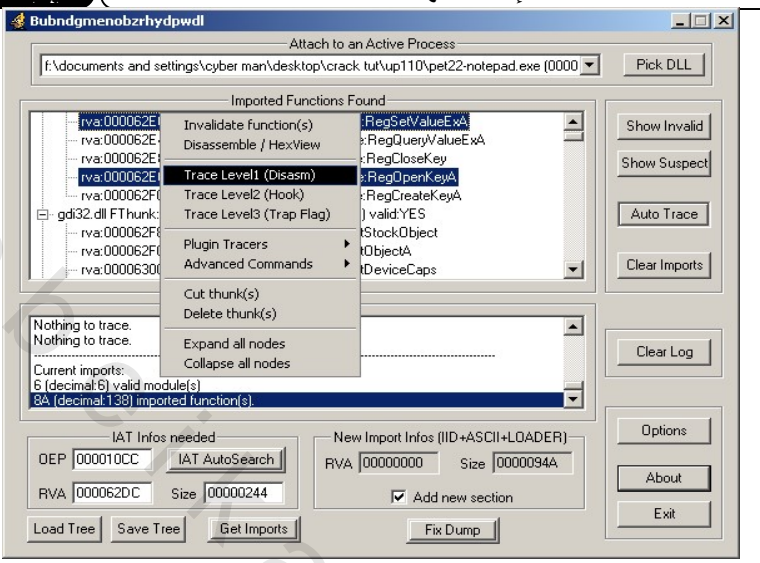
قم بتنفيذ أمر التفريغ من الأمر dump debugged process



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 trace level1 (disasm) 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