تأليف : JAAS
الموقع : الفريق العربي للبرمجة
jaas1001@hotmail.com
http://www.arabteam2000.com

# تشفير وضغط البرامج

السلام عليكم ورحمة الله ،،،

نواصل الحديث في أساسيات البرمجة العكسية للملفات التنفيذية وقد سبق وتحدثنا عن أساسيات في هذا المجال من البرمجة - ويفترض منك أنك قمت بمحاولات لمراقبة البرامج وتتبعها لكي تفهم الفكرة . ولأن هذا الموضوع يختلف عن بقية مواضيع البرمجة لأنة يتطلب فهم أغلب لغات البرمجة وفهم كيف تعمل مترجمات هذة اللغات وأفضل طريقة للتعلم هي التجربة والتطبيق العملي على كل البرامج التي في جهازك

**وبسم الله نبدأ:**

لنفهم تشفير وفك تشفير البرامج : يجب أن نعرف

**مافائدة التشفير :**

تقوم الشركات بعد تصميم برامجها بإستخدمات برامج التشفير لضغط وتشفير بيانات البرنامج

أولا : لحماية البرنامج وثانيا : لتصغير حجم البرنامج

**معلومة** : هذة الطريقة من الحماية تعد أسهل نوع وتستخدم في البرامج الصغيرة التي توزع عن طريق شبكة الإنترنت أما في البرامج الضخمة الموزعة عن طريق الأقراص فتستخدم نوع آخر من الحماية وهي الحماية على مستوى نظام التشغيل وهنا تستخدم برامج مثل سواقات الأجهزة ومثال على هذا النوع من الحماية (الحماية بالدنجل ) وهو خارج عن موضوعنا في هذا الدرس

نرجع للموضوع :

أعتقد أنك قمت بمحاولات كثيرة لتتبع البرامج : هل وقعت في مثل هذة البرامج

مثال : برنامج يظهر مسج للمستخدم ( وعند تتبع البرنامج لم تجد دالة المسج ؟ فقط وجدت ٤ أو ٥ دوال )

مثال : تريد تعريب قوائم برنامج ( ووجدت أن البرنامج لا يحتوي على ملف مصادر أو لايحتوي على بيانات )

مثال : قمت بإدخال برنامج إلى Olly ( فجأة ظهرت رسالة "الملف مضغوظ" أو "لايوجد دالة رئيسية " )

مثال : قمت بإدخال برنامج إلى Olly ( وبدون سابق إنذار يعاد تشغيل الجهاز ؟ أو يختفي Olly )

بإختصار : مر عليك برنامج غير قياسي ولاهو طبيعي مثل بقية البرامج ( هذا هو البرنامج المشفر )

ملاحظة : حاول التغيير أو تعريب الملف المرفق مع الدرس وستعرف فائدة التشفير

توجد برامج كثيرة لمعرفة إذا كان الملف مشفر أو لا وأي نوع من التشفير مثل: Language أو PEiD

برنامج : Language موقع : http://farrokhi.net/language

شغل البرنامج ومن File إختر أي ملف تنفيذي ليتم عرض معلومات عنة ، بهذة الطريقة

ملاحظة : بدأ التشفير ينتشر بشكل كبير ونادرا ما تجد برنامج على الإنترنت غير مشفر

والنقطة الثانية توجد بعض البرامج مشفرة ولا يستطيع برنامج Language معرفتها

أما عن طريقة تشفير البرامج فهي سهلة

قم بإختيار أي برنامج تشفير من : http://www.exetools.com/compressors.htm

يوجد نوعين من البرامج ( واجهة دوس - وواجهة وندوز ) وكل الأنواع متشابهة من حيث التشفير

وطريقة إستخدام أغلب برامج التشفير متشابة .

هذة مقدمة عن التشفير والسؤال الذي يطرح نفسة كيف يتم إعادة برنامج مشفر إلى ماكان علية

أو بصيغة أخرى كيف أغير في برنامج مشفر وأحفظ هذة التغيرات

أسهل طريقة : برامج فك التشفير (عندما يظهر برنامج تشفير جديد يظهر بعدة مباشرة برنامج لفك تشفيرة)

ولاكن موضوعنا يختلف نريد أن نتعلم فك كل أنواع التشفير بطريقة يدوية مهما كان نوع التشفير

أعدك بأنك لن تعرف طريقة فك التشفير إلى إذا عرفت كيفية عمل التشفير!!

**بنية عمل التشفير :**

بكل بساطة البرنامج المشفر: هو عبارة عن تغيير في ترتيب وخواص البرنامج القياسي وكتابة كود صغير

في بداية البرنامج ووضيفة هذا الكود إعادة ترتيب خواص الملف إلى الصيغة القياسية ليفهمها نظام التشغيل

بمعنى أن البرنامج يكون مشفر فقط في القرص ولكن عند تحميلة للذاكرة يتم فك تشفيرة(ويعود للصيغة القياسية )

لنفترض أنك قمت بتصميم برنامج وبعد الإنتهاء منة قررت تشفيرة ( ماذا سيتغير في البرنامج بعد التشفير )

لاحظ الطريقة : سيقوم برنامج التشفير بقرائة كل محتوى البرنامج الخاص بك( بيانات البرنامج )

ثم سيقوم بكتابها بصيغة قانون معين ( مثلاً : FFFFCC ستتحول إلى : F4C2 )

لاحظ أن حجم البيانات صار أقل وهذة طريقة الضغط ثم يقوم بتقسيم برنامجك الذي تريد تشفيرة إلى قسمين

القسم الأول وهو البرنامج الأصلي بصيغة مشفرة - والقسم الثاني سيكتب فية برنامج خاص لفك التشفير

**لاتنسى هذة النقطة ( ينقسم البرنامج المشفر إلى برنامجين ١ - البرنامج الأصلي ٢ -برنامج فك التشفير )**

أول ما تشغل أي برنامج مشفر فإن برنامج فك التشفير يعمل ويقوم بفك تشفير البيانات للبرنامج الأصلي

ثم يقوم بإعادة ترتيب البرنامج ويكتبة بنفس الصيغة قبل التشفير ثم ينقل التنفيذ للبرنامج الأصلي وتظهر نافذتة

ويعمل بشكل طبيعي.

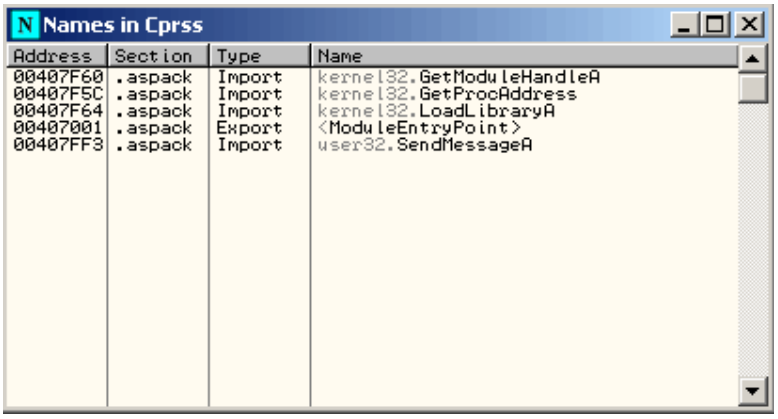
**مثال:**

تجد بالملف المرفق مع الدرس برنامج مشفر (يطلب منك إدخال رقم إذا كان خطأ يظهر لك مسج أو رسالة)

الآن نريد إيقاف البرنامج عند دالة إظهار المسج والدلة هي MessageBox

شغل برنامج Olly ثم File ثم Open إختر الملف المشفر ستظهر لك رسائل إضغط OK

ثم من نافذة CPU إضغط مفتاح Ctrl+N لتظهر لك نافذة الدوال




هل توجد دالة إظهار المسج ( بالتأكيد لا ) وبإختصار لاتوجد أصلا دوال للإستيراد (وما تراة تموية فقط)

وللمعلومة فهو ليس تموية لك وإنما للنظام (تلاحظ أنة يستخدم على الأقل دالة ١ من كل مكتبة ليقوم النظام بتحميل المكتبة)

ملاحظة : حتى لوكانت دالة المسج ظاهرة في هذة القائمة (فهي غير موجودة ) لتتأكد إضغط على أي دالة بالزر

الأيمن للماوس وإختر من القائمة التي تظهر الأمر Find references to improt لترى أنة لايوجد

إتصال لهذة الدالة في البرنامج بمعنى أنها غير مستخدمة في البرنامج

إذاً البرنامج الذي نراقبة ليس هو البرنامج الذي يظهر الرسالة وبإختصار هو القسم الثاني من البرنامج

وهو برنامج فك التشفير لأن برنامج فك التشفير لا يستخدم جدول لإستيراد الدوال ( لة طرق أخرى )

جرب تتبع البرنامج F8 ولاحظ كيف يقوم هذا البرنامج بفك شفرة البرنامج الأصلي وتشغيلة

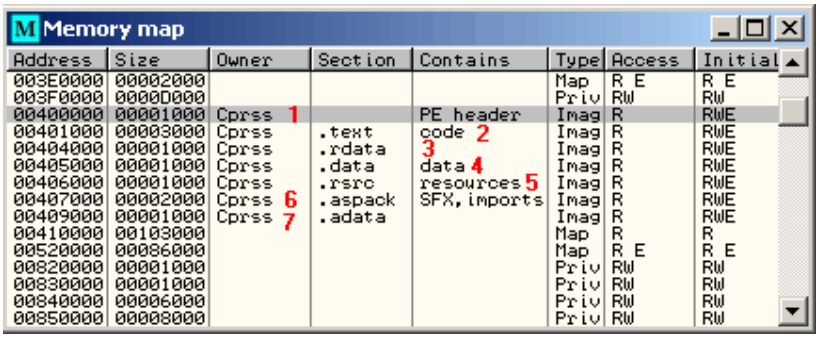
ملاحظة : في البرامج المشفرة قد لا يستجيب Olly لمتابعة التنفيذ بإستخدام F8 أو F9 لأنة يخبرك بحدوث إستثناء ولتتجاوز هذة الإستثناء إضغط مفتاح Shift قبل كل أمر بمعنى Shift+F8 أو Shift+F9 وهكذا

الآن أغلق برنامج Olly ثم قم بتشغيل البرنامج المشفر وبعد ذلك شغل Olly ومن File ثم **Attach**

ستظهر لك قائمة بالبرامج الموجودة في الذاكرة إختر البرنامج المشفر ثم إضغط **Attach**

ليقوم Olly بمراقبتة - قد تلاحظ أن الكود في نافذة CPU ليس كود البرنامج ( إضغط مفتاح Alt+M)

أو حرف M في شريط الأوامر لتظهر لك نافذة تخطيط الذاكرة



Memory map

| Address | Size | Owner | Section | Contains | Type | Access | Initial |
|---|---|---|---|---|---|---|---|
| 003E0000 | 00002000 | | | | Map | R E | R E |
| 003F0000 | 0000D000 | | | | Priv | RW | RW |
| 00400000 | 00001000 | Cprss 1 | | PE header | Imag | R | RWE |
| 00401000 | 00003000 | Cprss | .text | code 2 | Imag | R | RWE |
| 00404000 | 00001000 | Cprss | .rdata | 3 | Imag | R | RWE |
| 00405000 | 00001000 | Cprss | .data | data 4 | Imag | R | RWE |
| 00406000 | 00001000 | Cprss | .rsrc | resources 5 | Imag | R | RWE |
| 00407000 | 00002000 | Cprss 6 | .aspack | SFX, imports | Imag | R | RWE |
| 00409000 | 00001000 | Cprss 7 | .adata | | Imag | R | RWE |
| 00410000 | 00103000 | | | | Map | R | R |
| 00520000 | 00086000 | | | | Map | R E | R E |
| 00820000 | 00001000 | | | | Priv | RW | RW |
| 00830000 | 00001000 | | | | Priv | RW | RW |
| 00840000 | 00006000 | | | | Priv | RW | RW |
| 00850000 | 00008000 | | | | Priv | RW | RW |

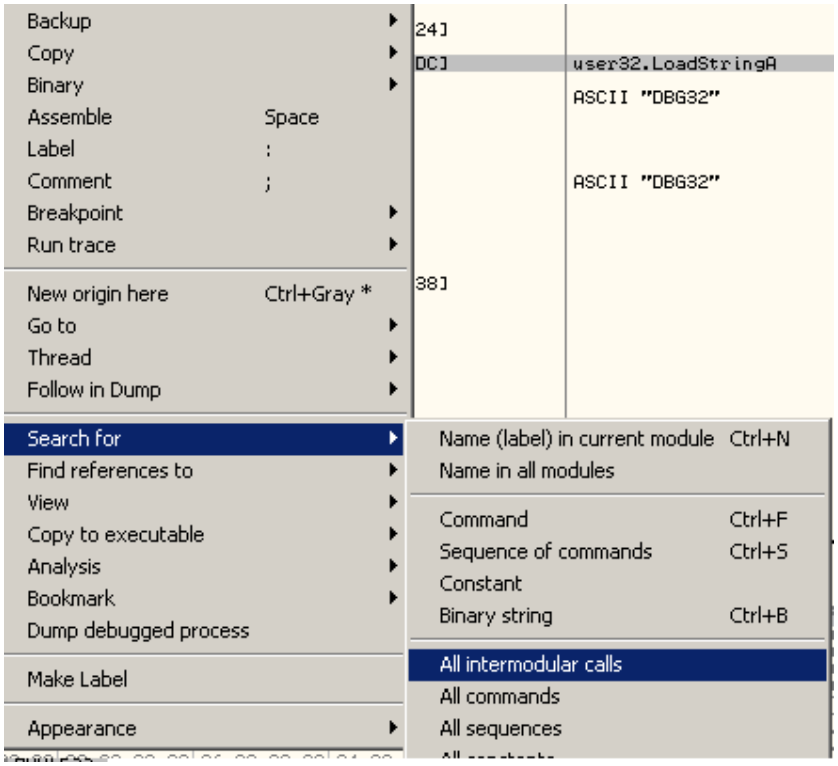
الرقم ١ هو جدول لترويسة البرنامج (ودائم في الترتيب تكون في بداية الملف )

الرقم ٢ : كود البرنامج ويجب أن يكون بعد الترويسة مباشرة ( إختر قسم الكود وإضغط زر إنتر)

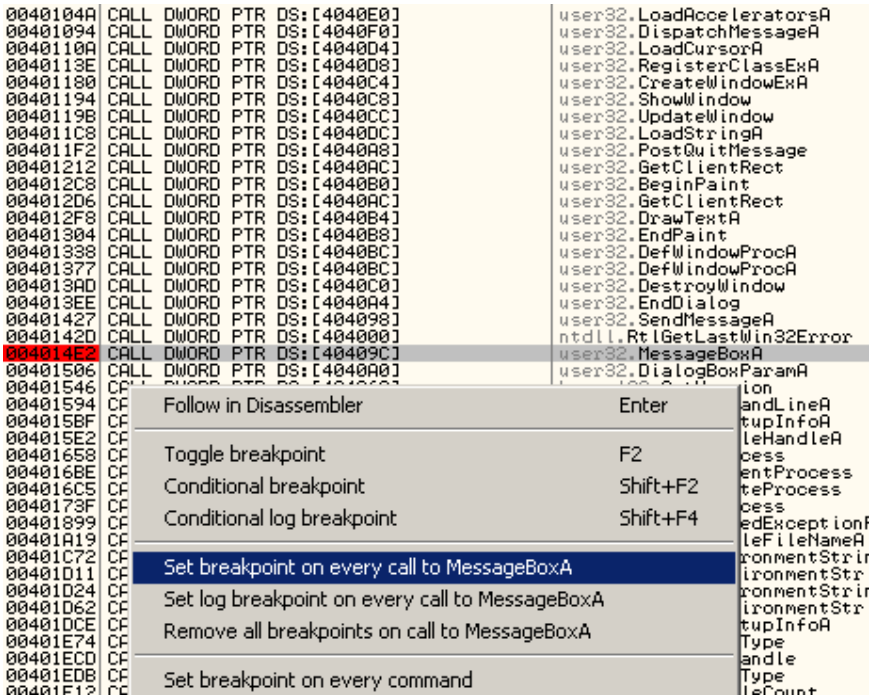
أو إضغط الزر الأيمن للماوس وإختر View in Disassembler

ملاحظة : بعض البرامج المشفرة تظهر بأن قسم الكود هو الرقم ٣ وفي هذة الحال إذهب لنافذة CPU ثم إضغط Ctrl+G وأدخل عنوان القسم رقم ٢ وهو ٤٠١٠٠٠ ثم OK

المهم : يجب أن تدخل القسم ٢ قسم الكود إلى نافذة CPU وبعد ذلك إضغط بالزر الأيمن على نافذة CPU ثم Search for ومن قائمة البحث إختر All intermodular calls




لتظهر لك نافذة الدوال




لاحظ أن كل دوال البرنامج قد ظهرت في هذة النافذة بما فيها دالة المسج

بعد أن تختار الدالة تضغط بالزر الأيمن للماوس وتختار الأمر الموضح

الآن نفذ البرنامج بإستخدام المفتاح F9 ( لتظهر لك نافذة البرنامج المشفر )

أدخل أي رقم في مربع النص وإضغط على الزر

سيتم إيقاف البرنامج عند دالة المسج

```
004014CD  83C0 10          ADD EAX,10
004014D0  3D F0000000      CMP EAX,0F0
004014D5  6A 00            PUSH 0
004014D7  v74 18           JE SHORT Cprss.004014F1
004014D9  6A 00            PUSH 0
004014DB  68 48504000      PUSH Cprss.00405048                ASCII "Error in Key"
004014E0  6A 00            PUSH 0
004014E2  FF15 9C404000    CALL DWORD PTR DS:[40409C]         user32.MessageBoxA
004014E8  33C0             XOR EAX,EAX
004014EA  81C4 04010000    ADD ESP,104
004014F0  C3               RETN
```

هل ترى تعليمة القفزة JE إقفز إذا كن يساوي إذا إستبدلتها ب JNE فإننا قد تجاوزنا المسج

في الحقيقة تستطيع أن تغير في الأمر(فقط في الذاكرة) ولكن لا تستطيع أن تحفظ هذا التغير على القرص

لأن برنامج فك التشفير يقوم بإعادة ترتيب وكتابة البرنامج الأصلي ( في كل مرة تشغل فيها البرنامج )

إذا ما هو الحل :

في مجال كسر البرامج فقد وجد حل هذة القصة بعدة طرق منها:

تغيير تعليمة Je بتعليمة JNE ثم تنفيذ البرنامج خطوة خطوة بواسطة F8

إلى أن يقوم البرنامج بكتابة معلومات التسجيل في الريجستري ( فيقوم الكراكر بحفظ هذة المعلومات )

في ملف تسجيل ويقوم بتوزيعة كملف باتش ( أكيد مر عليك كراك لملف تسجيل )

الطريقة الثانية وهي بحفظ عنوان التعليمة Je ثم تشغيل البرنامج بطريقة عادية بواسطة Olly

ثم يذهب لعنوان تعليمة القفز (قبل أن يقوم برنامج فك التشفير بالكتابة فوق التعليمة )

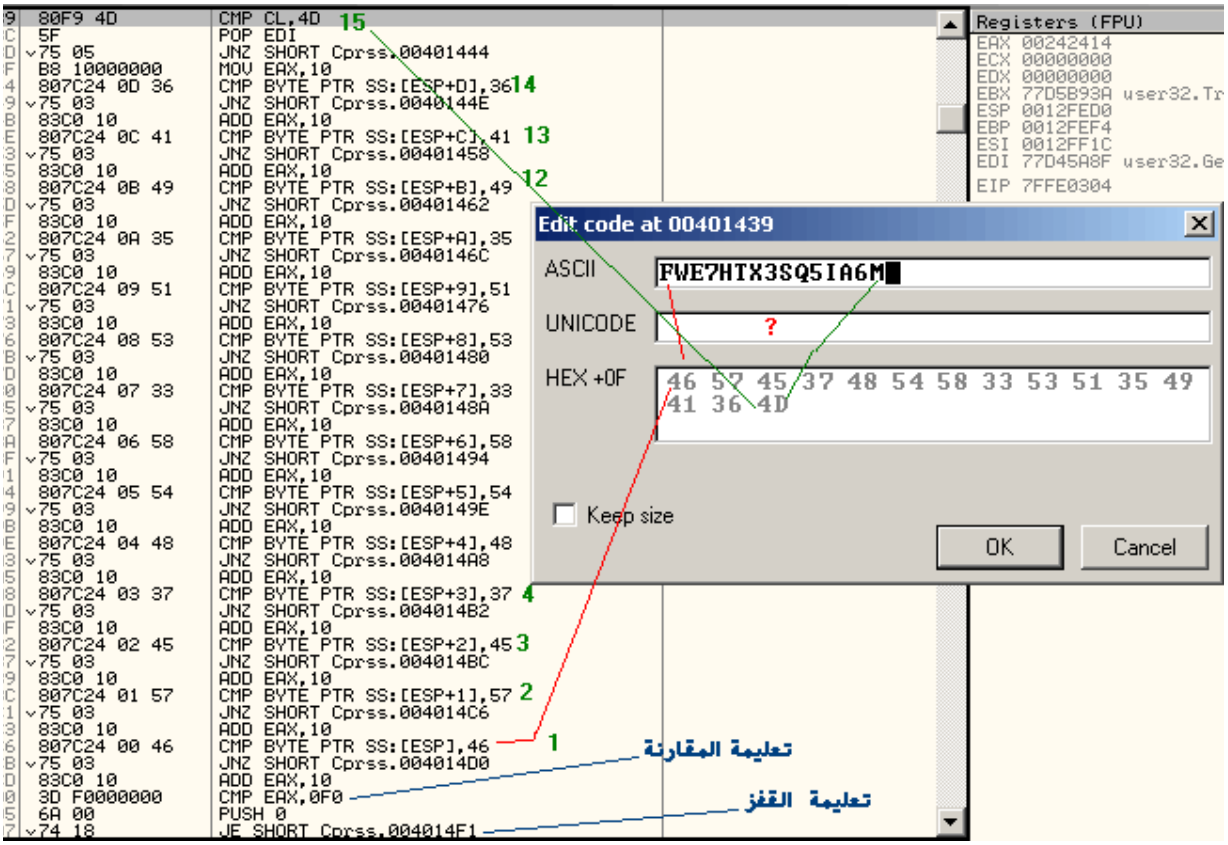
ويضع نقطة توقف وينفذ البرنامج ستلاحظ أن Olly أو قف البرنامج عند تعليمة قد تكون غريبة

وهي للكتابة فوق قسم البرنامج حدد العنوان الذي تقرأ منها التعليمة البيانات المشفرة لكتابتها عند تعليمة القفز

وإصنع باتش يقوم بتغيير هذة التعليمة من Je إلى JNE بصيغة هكس طبعا وبذلك تغير في البرنامج وهو مشفر

وصناعة الباتش ستكون بطريقة يدوية عن طريق تحديد العنوان والقيمة التي ستغيرها.

والطريقة الأشهر هي بإظهار السيريل نمبر أو الرقم السري - وتكون تعليمة المقارنة فوق تعليمة القفز مباشرة




أدخل المفتاح : FWE7HTX3SQ5IA6M وجرب

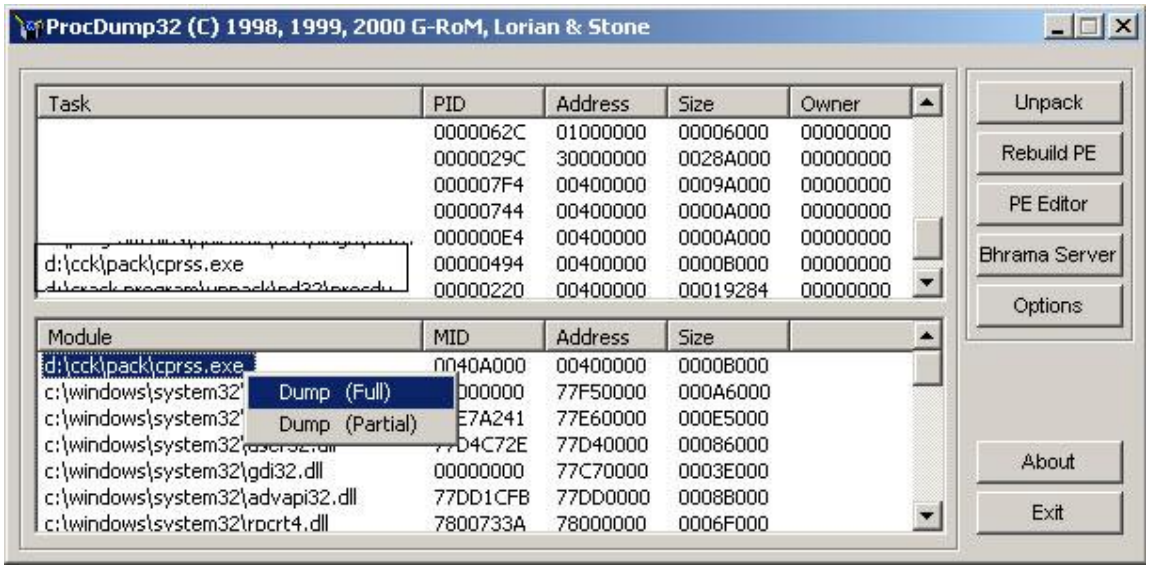
---

ولكن قد يرغب البعض بتعلم:

**فك تشفير البرنامج وإعادتة كما كان بطريقة يدوية**

سنحتاج في هذا الدرس أداة إضافية : ProcDump32 http://www.exetools.com/unpackers.htm

شغل البرنامج المشفر ثم شغل الأداة ( وإختر البرنامج المشفر )




ستظهر لك نافذة لحفظ الملف حدد إسم الملف وليكن xxcprss بعد أن تحفظ الملف راجع حجمة لترى

أنة أكبر بكثير من الملف المشفر والسبب لأننا حفظنا الملف مباشرة من الذاكرة ( بعد أن فك تشفيرة)

بقي الآن أن نعيد ترتيب عدد من النقاط بشكل يدوي

مثل : ١ - عناوين أقسام البرنامج ( ومحتواها )

٢- عنوان بداية تنفيذ البرنامج الأصلي قبل التشفير

٣- عنوان جدول الدوال المستوردة + عنوان جدول ملف المصادر

في الحقيقة لكل هذة العناوين قوانين ثابتة - وأعتقد أنها ليست بجديدة أو غريبة عليك

راجع موضوع ( تعلم كيف تعمل مترجمات لغات البرمجة ) في المنتدى

هل تذكر هذة النقاط : أساسيات الدوال المستوردة + أساسيات ملف المصادر + تروسة الملف والأقسام

وهذا الدرس بإختصار تطبيق لما قرأتة في موضوع المترجمات

الآن يوجد لدينا ملفين وهما : Cprss وهو الملف المشفر مضغوط (تأكد من حجمة )

ولدينا xxcprss وهو الملف المشفر ولاكن بعد فك ضغطة في الذاكرة (راجع حجمة )

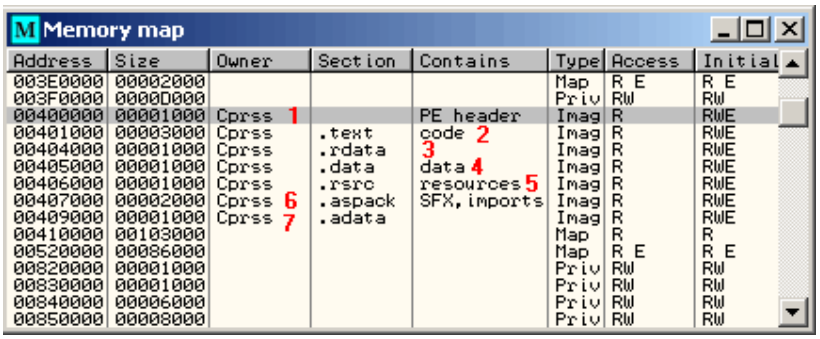
قم بتشغيل الملف Cprss ثم قم بتشغيل **نسختين** من برنامج Olly

في النسخة الأولى من Olly من قائمة File ثم Attach وأدخل الملف Cprss

وفي النسخة الثانية من Olly من قائمة View ثم File وإختر xxcprss (لتفتح الملف بمحرر هكس )

أول شيء سنقوم بة نقل محتويات الأقسام بعد فك تشفيرها

في نسخة Olly الخاصة بـCprss أعمل تخطيط للذاكرة عن طريق الأمر M

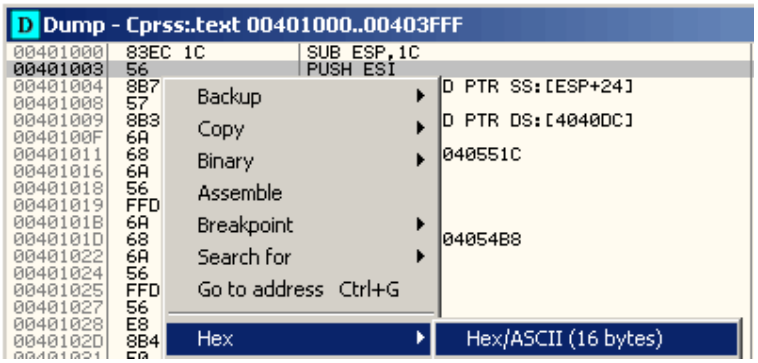


Memory map

| Address | Size | Owner | Section | Contains | Type | Access | Initial |
|---|---|---|---|---|---|---|---|
| 003E0000 | 00002000 | | | | Map | R E | R E |
| 003F0000 | 0000D000 | | | | Priv | RW | RW |
| 00400000 | 00001000 | Cprss 1 | | PE header | Imag | R | RWE |
| 00401000 | 00003000 | Cprss | .text | code 2 | Imag | R | RWE |
| 00404000 | 00001000 | Cprss | .rdata | 3 | Imag | R | RWE |
| 00405000 | 00001000 | Cprss | .data | data 4 | Imag | R | RWE |
| 00406000 | 00001000 | Cprss | .rsrc | resources 5 | Imag | R | RWE |
| 00407000 | 00002000 | Cprss 6 | .aspack | SFX, imports | Imag | R | RWE |
| 00409000 | 00001000 | Cprss 7 | .adata | | Imag | R | RWE |
| 00410000 | 00103000 | | | | Map | R | R |
| 00520000 | 00086000 | | | | Map | R E | R E |
| 00820000 | 00001000 | | | | Priv | RW | RW |
| 00830000 | 00001000 | | | | Priv | RW | RW |
| 00840000 | 00006000 | | | | Priv | RW | RW |
| 00850000 | 00008000 | | | | Priv | RW | RW |

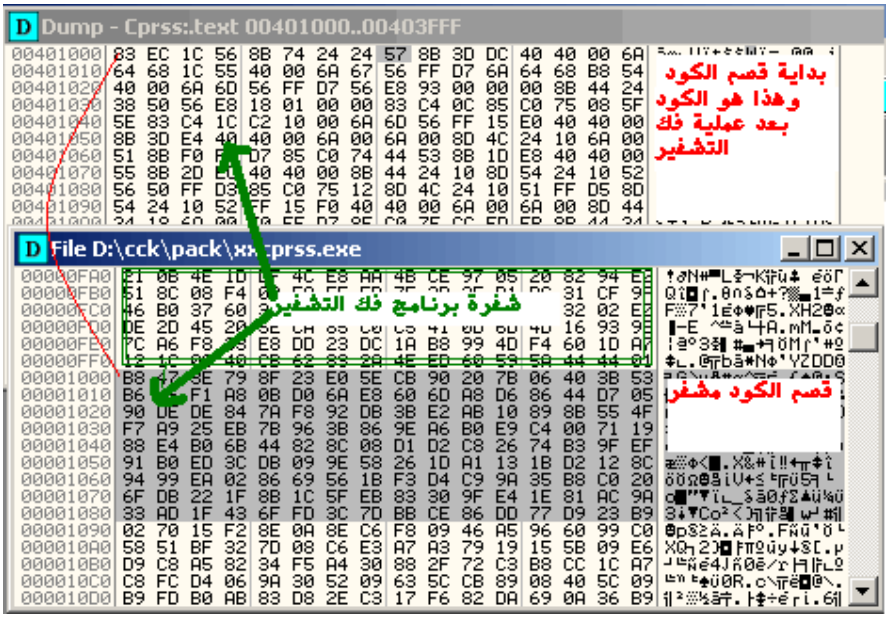
إضغط على قسم الكود (القسم الثاني ) بالزر الأيمن وإختر أمر Dump

ستظهر لنا النافذة وبها معلومات بلغة الإسمبلي ( حولها للترميز الهكس ١٦ بت )



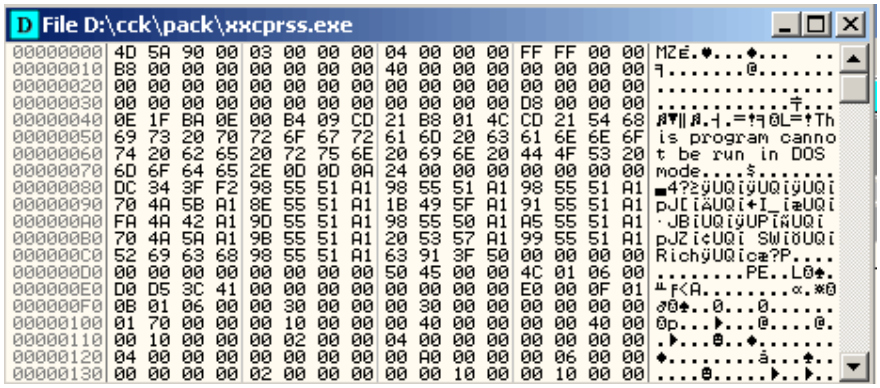

ثم إذهب إلى النسخة الثانية لبرنامجOlly الخاصة ب xxcprss (إنتقل للعنوان ١٠٠٠)

عن طريق Ctrl +G ثم أدخل ١٠٠٠ ثم Ok ماذا تلاحظ




الآن عرفنا بداية قسم الكود=١٠٠٠ وعرفنا محتواة بعد فك التشفير

إذهب إلى برنامجOlly نسخة xxcprss ثم توجهة إلى بداية الكود




والآن سنراجع ترتيب البرنامج عن طريق ملاحظة الفراغات إن صح التعبير

نبدأ من عنوان نهاية الترويسة وهو x02C0 وهو العنوان الذي يلي أسماء الأقسام مثل adata ,code

أول قانون سنطبقة ( أن قسم الكود يأتي مباشرة بعد ترويسة الملف ) بمعنى أنة من العنوان x02c0

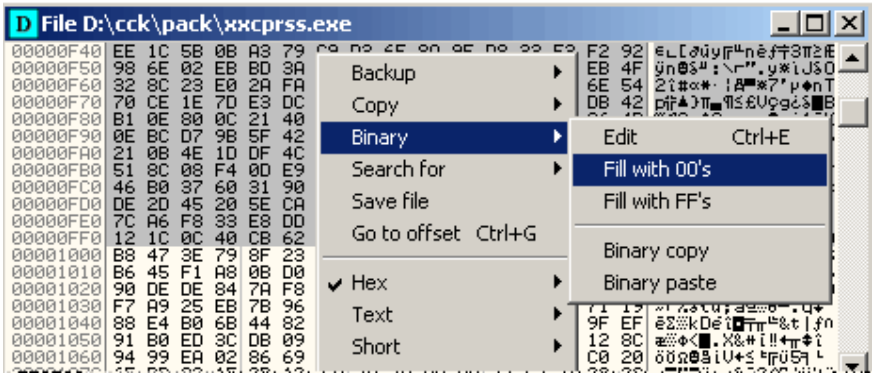
إلى بداية الكود وهو العنوان x01000 سيكون أصفار ( لايحتوي أي معلومات )

وإذا حبيت أن تعرف ماذا نريد أن نحذف بهذة الطريقة

لاحظ العنوان: x0400 وهنا يوجد توقيع للبرنامج ProcDump32 (يخبرك بأنة هو من قام بفك ضغط الملف)

وعند العنوان :x600  يبدأ كود برنامج فك التشفير

المهم : إختر أو علم على كل البيانات من العنوان x2C0  إلى فوق العنوان x1000 وصفرها- بهذة الطريقة

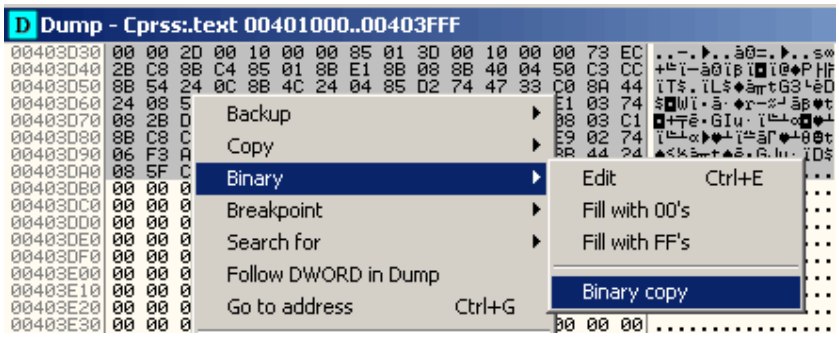



ثم إرجع للنسخة الأولى لبرنامج Olly للملف Cprss  (وإختر قسم الكود ثم Dump  ثم حول الكود للهكس)

كما فعلنا سابقا ولكن الآن نريد نسخ قسم الكود  بهذة الطريقة

من أول بايت عند العنوان x401000  علم على الكود وإنزل للأسفل حتى يأتيك أول فراغ

ثم قم بنسخ هذة البيانات -بهذة الطريقة

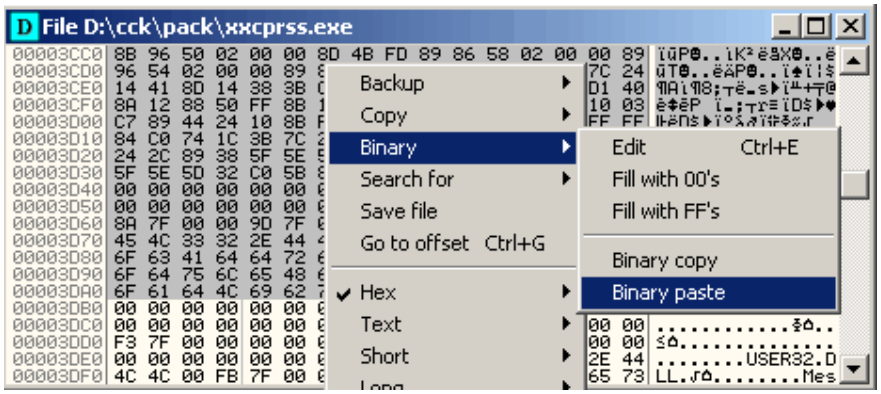



لاحظ توقفنا عند العنوان x403DA0

ملاحظة : في الدرس بشكل عام لا أستخدم العنوان الوهمي مثل x403DA0  ستتحول إلى x3DA0

لكي أسهل عملية التعرف على العنوان الحقيقي في محرر الهكس

نرجع لمحرر الهكس ونبدأ في إختيار البايت من العنوان x1000 إلى x3DA0 ونلصق الكود




والآن نريد حفظ بعض المعلومات عن هذا القسم:

١- يبدأ قسم الكود عند العنوان ١٠٠٠

٢- الحجم الفعلي لقسم الكود =x2DB0

في البداية ماهو الحجم الفعلي للقسم : بإختصار هوعدد البايتات في القسم (بدون الفراغات 000)

نلاحظ بأن الكود يبدأ عند العنوان x1000 وينتهي عند x3DB0 كم الفرق بين العددين هو الحجم الفعلي

وإذا أردت تحديد الحجم الفعلي للكود بدقة فإنة =x2DAE لأنك تلاحظ أنة في نهاية الكود

الذي علمنا علية توجد ٣ بايتات تساوي الصفر -المهم أن الفكرة وصلت

٣ - الحجم الوهمي للكود =x3000

في البداية ماهو الحجم الوهمي : هو الحجم الفعلي للكود+ الفراغ أو الأصفار في نهاية الكود

والفراغ هو عبارة عن مجموعة من الأصفار تفصل بين الأقسام مثل قسم الكود والبيانات

وأسهل طريقة لمعرفة الحجم الوهمي :

لو ترجع لنافذة تخطيط الذاكرة وتلاحظ عنوان القسم الذي يأتي بعد قسم الكود لوجدتة x404000

وطبعا نحذف منة العنوان الوهمي ليصبح ٤٠٠٠ وننقص منة بداية الكود ١٠٠٠ والنتيجة ٣٠٠٠

ملاحظة : يجب أن تكون كل البايتات من العنوان x3DB0 إلى العنوان x4000 تساوي صفر

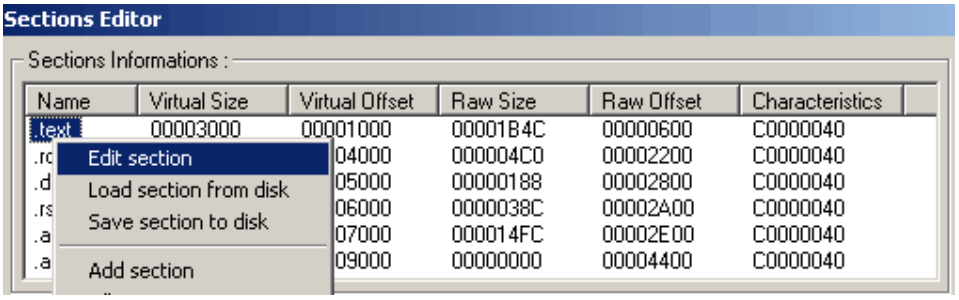
وبهذا نكون قد أوجدنا القسم الفعلي(وهو ماقمنا بنسخة) + القسم الوهمي (وهي الأصفار في نهاية الكود)

و الآن سنقوم بحفظ الملف (إضغط بالزر الأيمن للماوس في أي مكان في محرر الهكس للملف xxcprss )

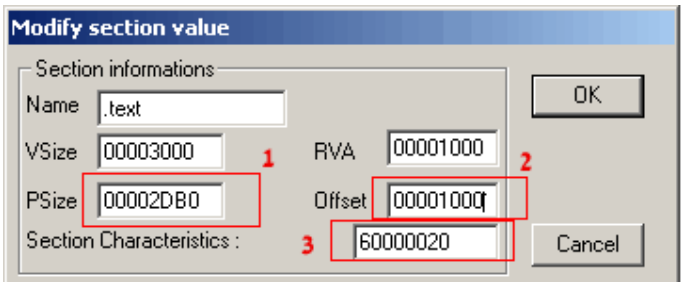
وإختر Save file ثم إحفظ الملف وقم بحذف الملف القديم xxcprss و ضع بدلة الملف الجديد بنفس الإسم

ثم أغلق كل برامج Olly وشغل برنامج ProcDump32 ثم إختر الأمر PE Editor

وأدخل الملف الجديد xxcprss  تظهر لك نافذة إختر منها Sections وعدل قسم الكود




تظهر لك نافذة التعديل  غير هذة القيم




١-الحجم الفعلي لقسم الكود

٢- بداية قسم الكود

٣- خصائص القسم ( وهذة القيمة لقسم الكود متشابهة في كل البرامج )

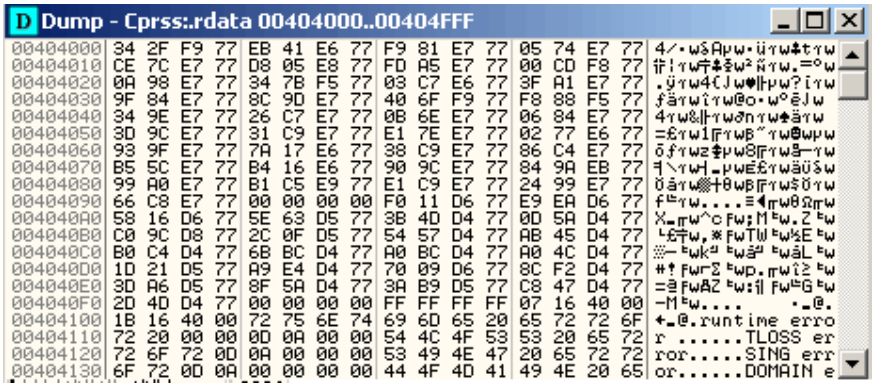
والحمد لله إستطعنا إرجاع قسم الكود كما كان عندما كتبة المترجم وبدون تشفير

**القسم الثاني : قسم البيانات والدوال المستوردة**

قسم الدوال المستوردة وهو القسم rdata - وقسم البيانات في البرنامج هو data

نبدأ في rdata  هذا القسم نطبيق كل الخطوات في القسم السابق ولكن في بعض التغييرات

جرب نفس الطريقة السابقة في نسخ قسم البيانات ستلاحظ هذة النافذة




هذة العناوين في القسم يكتبها النظام بعد تحميل الملف إلى الذاكرة

كما درسنا سابقا وخاصة في موضوع المترجمات وبالتحديد طريقة تحميل الملف التنفيذي للذاكرة

وقلنا بأن النظام يقرأ عنوان إسم الدالة في الملف ثم يستخدم الدالة GetProcAddress لمعرفة عنوان الدالة

ويكتبها في نفس العنوان ( بإختصار هذة البيانات التي تراها ليست في الملف الأصلي وإنما كتبها النظام )

والذي نريد معرفتة الآن بالضبط هو محتوى هذا القسم بعد مايقوم برنامج فك التشفير بكتابتة هذا القسم

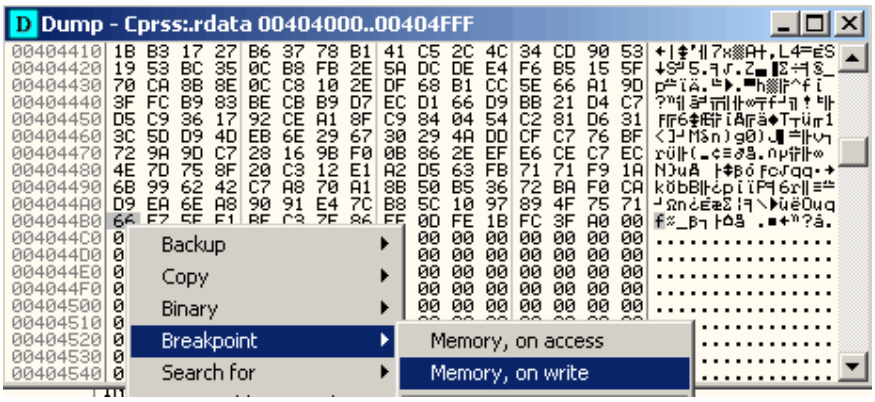
وقبل أن يقوم نظام التشغيل بتحويل هذة البيانات إلى عناوينها في الذاكرة

بمعنى نريد معرفة بيانات هذة القسم كما كتبها مترجم لغة البرمجة

والطريقة سهلة (شغل برنامج Olly ثم File ثم Open وإختر الملف Cprss )

ثم أظهر نافذة تخطيط الذاكرة وإختر القسم rdata ثم إختر الأمر Dump(لاحظ محتوى القسم مشفر)

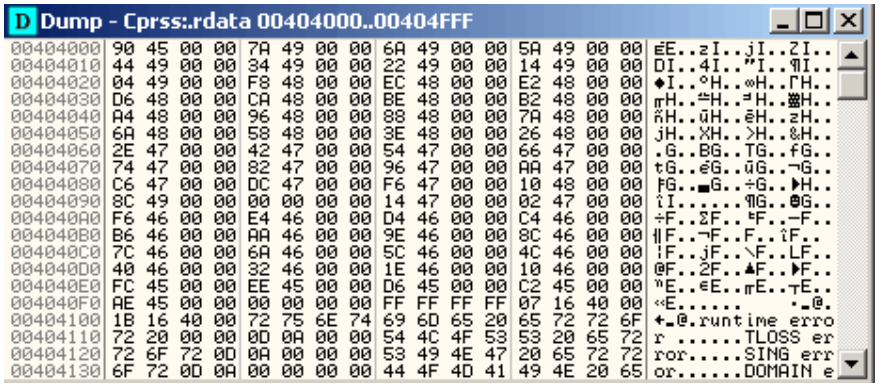
ثم نزل النافذة إلى أسفل حتى تجد أول فراغ - ثم حدد نقطة توقف للبايت - بهذة الطريقة




طلبنا من برنامج Olly بإقاف البرنامج عندما يكتب أول مرة على هذا العنوان

وبعد ذلك نفذ البرنامج F9 ستلاحظ أن البرنامج توقف + لاحظ ماكتبة Olly في شريط الحالة

ثم إذهب إلى نفس القسم ونفذ أمر Dump ولاحظ التغير




هذة البيانات بإختصار هي محتوى القسم كما كتبها المترجم

والآن شغل نسخة أخرى من برنامج Olly وأدخل نفس الملف بواسطة أمر Attach

وإنسخ العناوين الحقيقة للدوال بمعنى نغير في القسم إلى العنوان x4040F0 فقط وباقي القسم

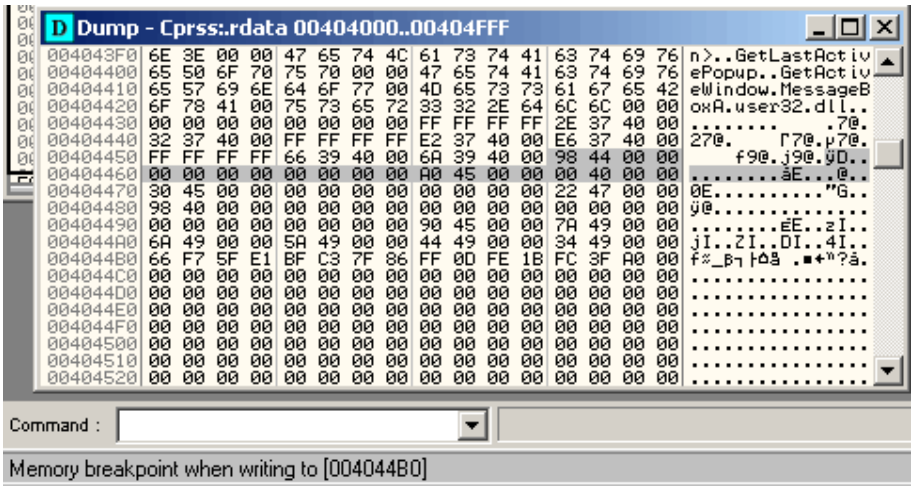
فهو القسم الحقيقي ( ثم إنسخ كل هذا القسم إلى محرر هكس وغير أحجام القسم كما فعلنا في قسم الكود)

وبهذا نكون قد أرجعنا قسم الدوال المستوردة + قسم الكود إلى ماكان علية قبل التشفير

بقي نقطة مهمة وهي عنوان الدوال المستوردة وهو :x0445C

كيف عرفتة ؟؟ عن طريق قانون ٢٠ بايت لكل مكتبة ربط ( وللمرة ١٠ راجع موضوع المترجمات في المنتدى)

وبطريقة عملية لاحظ الصورة




وتمكننا هذة ٢٠ بايت من معرفة إسم المكتبة وعناوين الدوال المستوردة

وإذا لم تستطع تحديد العنوان يمكنك البحث عن إسم مكتبة مثلا user32.dll ثم تحديد عنوانها ونطبق

قانون قلب العنوان وبعد ذلك تبحث عن هذا العنوان ليدلك على ٢٠ بايت الخاص بهذة المكتبة

وحجم جدول الدوال =x3C لأن عدد المكاتب في البرنامج ٢ *٢٠ بايت (عدد البايتات لكل مكتبة )

ونضيف لة ٢٠ بايت وهي عبارة عن البايتات التي تحمل القيمة٠ في نهاية الجدول

وبهذا نكون قد أوجدنا (عنوان جدول الدوال المستوردة + حجم الجدول )

**قسم بيانات البرنامج data**

هذا القسم مثل أول قسم ( شغل Olly ثم File ثم Attach وأدخل الملف Cprss )

ثم حدد القسم data ثم Dump وإنسخ كل محتوى القسم وقم بلصقة في محرر الهكس

ثم غير في أحجام القسم ( طبق ما قمنا بعملة في قسم الكود )

**قسم ملف المصادر rsrc**

هذا القسم ولا أسهل ( شغل Olly ثم File ثم Attach وأدخل الملف Cprss )

ثم حدد القسم rsrc ثم Dump وإنسخ كل محتوى القسم وقم بلصقة في محرر الهكس

وعنوان جدول المصادر = عنوان بداية القسم كما هو x6000

وحجم جدول المصادر = x9D0 نفسة الحجم الفعلي للقسم (بمعنى عدد البايتات التي لا تساوي٠ في القسم)

أما عن بقية الأقسام فهي تخص البرنامج الثاني - برنامج فك التشفير

وهي aspack + adata

وتمثل قسم الكود وقسم البيانات .. أكيد إحذفها Delete بواسطة ProcDump32

---

وبهذة الطريقة نكون قد أكملنا كل البرنامج وقمنا بإرجاعة إلى الصيغة القياسية قبل التشفير

بقي فقط نقطة واحد وهي عنوان بداية تنفيذ البرنامج

وهذا العنوان لايوجد لة قانون ( ولكنة ينعرف من شكلة ) فهو يأتي قبل دوال تشغيل البرنامج الأساسية

وإذا لم تستطع معرفتة (تتبع برنامج فك التشفير وحاول معرفة متى ينقل التنفيذ إلى البرنامج الأصلي)

وفي مثالنا ستجد العنوان التالي : x401530 ويساوي x1530 وهو بالضبط عنوان بداية التنفيذ

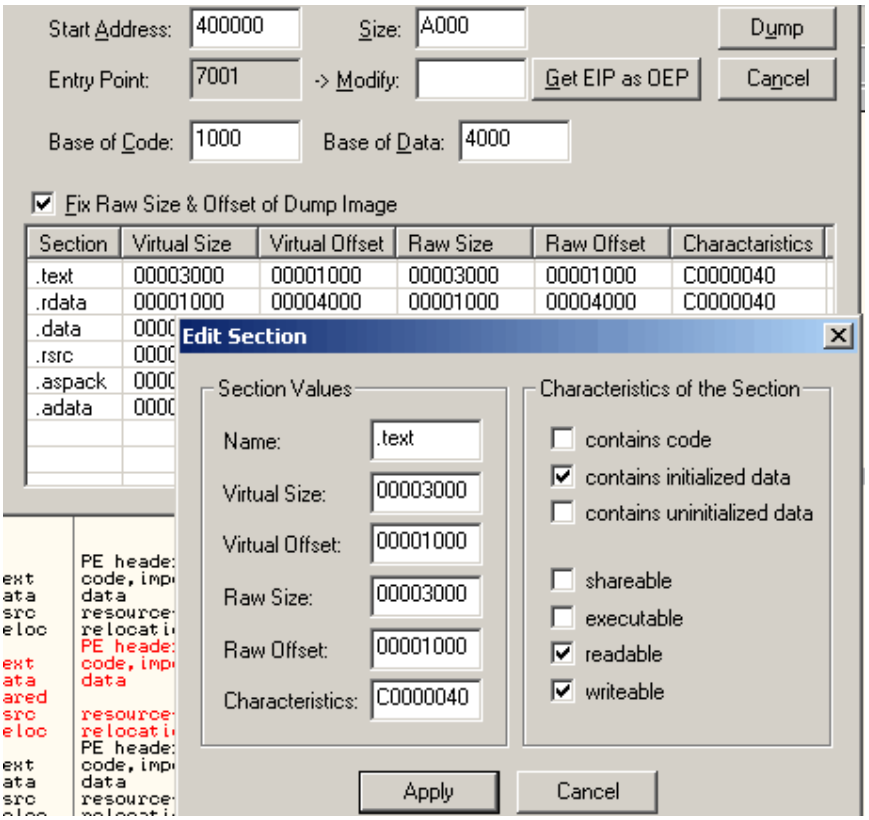
وبهذا نكون قد أنهيناء الأساسيات المهمة في موضوع - البرمجة العكسية للملفات التنفيذية -

وبقي فقط إكتساب الخبرة والخبرة بشكل عام تأتي بكثرة تتبعك للبرامج ومعرفة الأفكار الجديدة

وبكل صراحة القصد من هذا الدرس هو التعرف على أدوات جديدة + فهم بنية الملف التنفيذي

وتلاحظ أن لكل شغلة إستخدمت برنامج وفي الحقيقة أن برنامج Olly فقط يحتوي على أغلب الأدوات

التي أستخدمتها في الدرس لاحظ هذة النافذة في أولي ( ولا أسهل )

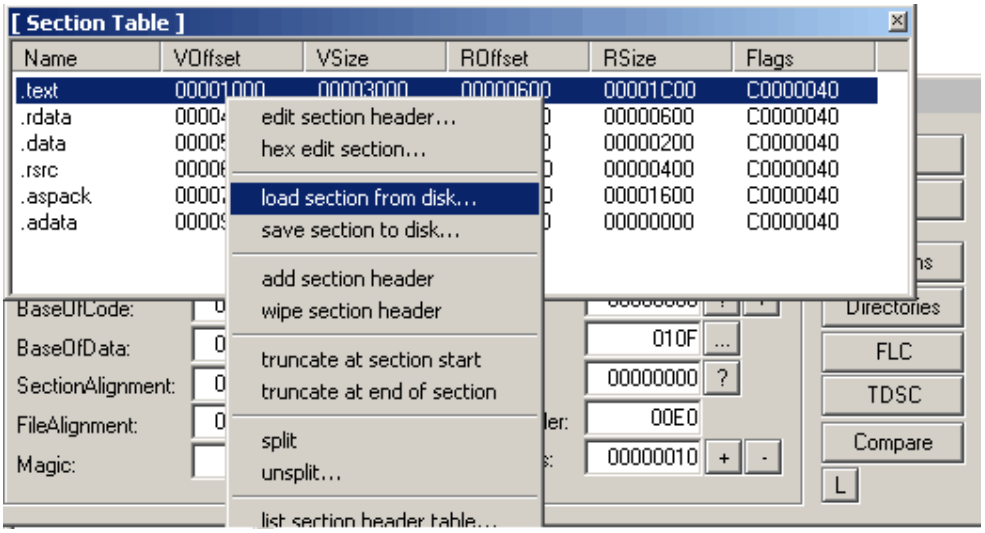



وبكل بساطة تحدد الذي قمنا بتغييرة في كل قسم

وتوجد أدوات كثيرة (تعرف ب Plug in تجدها في موقع Olly ) وهي عبارة عن مكاتب ربط تقوم بوضعها

في ملف البرنامج ثم إذهب إلى قائمة Plugins وتجد أداة جديدة ظهرت ..وهكذا مع كل الأدوات

والنقطة الثانية أن كل ما قمنا بة من مراحل ( تقوم بة بعض البرامج بكبسة زر ) لاحظ




وهذا البرنامج : Lord PE موقع : www. y0da.cjb.net

وتوجد أدوات تسهل الشغلة بشكل كبير ( ولكن ليس موضوع الدرس " فك تشفير البرامج بكبسة زر " )

---

**وأتمنى أن يكون الدرس واضح لا غبار علية**

**هذا والله أعلم**

**٢٠٠٤/٩/٨**