

## تشفير وضغط البرامج

السلام عليكم ورحمة الله ،،،

نواصل الحديث في أساسيات البرمجة العكسية للملفات التنفيذية وقد سبق وتحديثنا 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 لأنه يتطلب فهم أغلب لغات البرمجة وفهم كيف تعمل مترجمات هذه اللغات وأفضل طريقة للتعلم هي التجربة والتطبيق العملي على كل البرامج التي في جهازك

وبسم الله نبدأ:

لفهم تشفير وفك تشفير البرامج : يجب أن نعرف

### مافائدة التشفير :

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

أولا : لحماية البرنامج وثانيا : لتصغير حجم البرنامج

**معلومة :** هذه 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 هذه البرامج

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

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

مثال : قمت بإدخال برنامج إلى Olly ( فجأة ظهرت رسالة "الملف مضغوط" أو "لا يوجد دالة رئيسية " )

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

بإختصار : مر عليك برنامج غير قياسي ولا هو 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 اختر أي ملف تنفيذي ليتم عرض معلومات عنه ، بهذه 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 - واجهة وندوز ) وكل الأنواع متشابهة من حيث التشفير

وطريقة إستخدام أغلب برامج التشفير متشابهة .



هذه مقدمة عن التشفير والسؤال الذي يطرح نفسه كيف يتم إعادة برنامج مشفر إلى مكانه عليه

أو بصيغة أخرى كيف أغير في برنامج مشفر وأحفظ هذه التغييرات

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

ولكن 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 تحميله للذاكرة يتم فك تشفيره (ويعود للصيغة القياسية)

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

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

ثم سيقوم بكتابتها بصيغة قانون معين (مثلاً : FFFFCC ستحول إلى : F4C2)

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

القسم الأول وهو البرنامج الأصلي بصيغة مشفرة - والقسم الثاني سيكتب فيه برنامج خاص لفك التشفير  
لاتنسى هذه 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 ويكتبه بنفس الصيغة قبل التشفير ثم ينقل التنفيذ للبرنامج الأصلي وتظهر نافذة  
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 اختر الملف المشفر ستظهر لك رسائل اضغط OK

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

Names in Cprss			
Address	Section	Type	Name
00407F60	.aspack	Import	kernel32.GetModuleHandleA
00407F5C	.aspack	Import	kernel32.GetProcAddress
00407F64	.aspack	Import	kernel32.LoadLibraryA
00407001	.aspack	Export	<ModuleEntryPoint>
00407FF3	.aspack	Import	user32.SendMessageA

هل توجد دالة إظهار المسج (بالتأكيد لا) وبإختصار لا توجد أصلا دوال للإستيراد (وما تراه تمويه فقط)

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

ملاحظة : حتى لو كانت دالة المسج ظاهرة في هذه القائمة (فهي غير موجودة) لتتأكد اضغط على أي دالة بالزر

الأيمن للماوس وإختر من القائمة التي تظهر الأمر Find references to improt لترى أنه لا يوجد

إتصال لهذه الدالة في البرنامج بمعنى أنها غير مستخدمة في البرنامج

إذا البرنامج الذي نراقبه 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 (ل طرق أخرى)

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

ملاحظة : في البرامج المشفرة قد لا يستجيب Olly لمتابعة التنفيذ بإستخدام F8 أو F9 لأنه يخبرك بحدوث

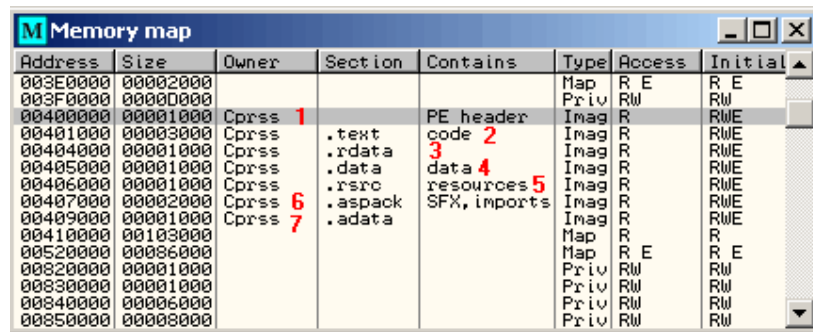
إستثناء ولتتجاوز هذه الإستثناء إضغط مفتاح Shift قبل كل أمر بمعنى Shift+F8 أو Shift+F9 وهكذا

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

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

ليقوم Olly بمراقبته - 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



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	.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 ( إختار قسم الكود وإضغط زر إنتر)

أو إضغط الزر الأيمن للماوس وإختار View in Disassembler

ملاحظة : بعض البرامج المشفرة تظهر بأن قسم الكود هو الرقم ٣ وفي هذه 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 إختار All intermodular calls

Backup	▶	241	
Copy	▶	DC1	user32.LoadStringA
Binary	▶		ASCII "DBG32"
Assemble	Space		
Label	:		
Comment	;		ASCII "DBG32"
Breakpoint	▶		
Run trace	▶		
New origin here	Ctrl+Gray *	381	
Go to	▶		
Thread	▶		
Follow in Dump	▶		
Search for	▶		Name (label) in current module Ctrl+N
Find references to	▶		Name in all modules
View	▶		
Copy to executable	▶		Command Ctrl+F
Analysis	▶		Sequence of commands Ctrl+S
Bookmark	▶		Constant
Dump debugged process			Binary string Ctrl+B
Make Label			All intermodular calls
Appearance	▶		All commands
			All sequences
			All constants

لتظهر لك نافذة الدوال

0040104A	CALL	DWORD	PTR	DS:[4040E0]	user32.LoadAcceleratorsA
00401094	CALL	DWORD	PTR	DS:[4040F0]	user32.DispatchMessageA
0040110A	CALL	DWORD	PTR	DS:[4040D4]	user32.LoadCursorA
0040113E	CALL	DWORD	PTR	DS:[4040D8]	user32.RegisterClassExA
00401180	CALL	DWORD	PTR	DS:[4040C4]	user32.CreateWindowExA
00401194	CALL	DWORD	PTR	DS:[4040C8]	user32.ShowWindow
0040119B	CALL	DWORD	PTR	DS:[4040CC]	user32.UpdateWindow
004011C8	CALL	DWORD	PTR	DS:[4040DC]	user32.LoadStringA
004011F2	CALL	DWORD	PTR	DS:[4040A8]	user32.PostQuitMessage
00401212	CALL	DWORD	PTR	DS:[4040AC]	user32.GetClientRect
004012C8	CALL	DWORD	PTR	DS:[4040B0]	user32.BeginPaint
004012D6	CALL	DWORD	PTR	DS:[4040AC]	user32.GetClientRect
004012F8	CALL	DWORD	PTR	DS:[4040B4]	user32.DrawTextA
00401304	CALL	DWORD	PTR	DS:[4040B8]	user32.EndPaint
00401338	CALL	DWORD	PTR	DS:[4040BC]	user32.DefWindowProcA
00401377	CALL	DWORD	PTR	DS:[4040BC]	user32.DefWindowProcA
004013AD	CALL	DWORD	PTR	DS:[4040C0]	user32.DestroyWindow
004013EE	CALL	DWORD	PTR	DS:[4040A4]	user32.EndDialog
00401427	CALL	DWORD	PTR	DS:[404098]	user32.SendMessageA
0040142D	CALL	DWORD	PTR	DS:[404000]	ntdll.RtlGetLastWin32Error
004014C2	CALL	DWORD	PTR	DS:[40409C]	user32.MessageBoxA
00401506	CALL	DWORD	PTR	DS:[4040A0]	user32.DialogBoxParamA
00401546	CF				ion
00401594	CF	Follow in Disassembler	Enter		andLineA
004015BF	CF				tupInfoA
004015E2	CF				leHandleA
00401658	CF	Toggle breakpoint	F2		cess
004016BE	CF				entProcess
004016C5	CF	Conditional breakpoint	Shift+F2		teProcess
0040173F	CF				cess
00401899	CF	Conditional log breakpoint	Shift+F4		edExceptionf
00401A19	CF				leFileNameA
00401C72	CF	Set breakpoint on every call to MessageBoxA			ronmentStrir
00401D11	CF				ronmentStrir
00401D24	CF	Set log breakpoint on every call to MessageBoxA			ronmentStrir
00401D62	CF				tupInfoA
00401DCE	CF	Remove all breakpoints on call to MessageBoxA			Type
00401E74	CF				andle
00401ECD	CF				Type
00401ED8	CF	Set breakpoint on every command			leCount
00401F12	CF				

لاحظ أن كل دوال البرنامج قد ظهرت في هذه 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 واضغط 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	74 18	JE SHORT Cprss.004014F1	
004014D9	6A 00	PUSH 0	
004014DB	68 48504000	PUSH Cprss.00405048	ASCII "Error in Key"
004014DE	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 هذه 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 هذه 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 )

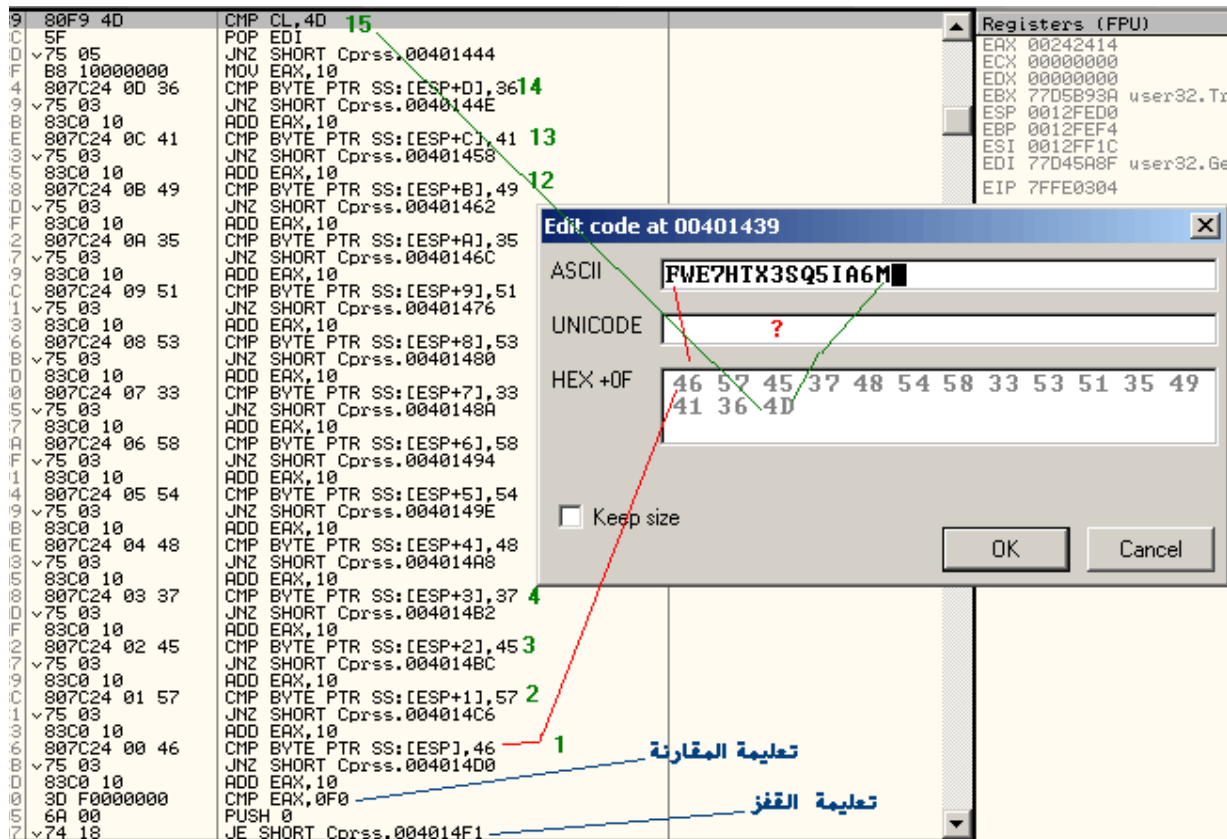
ويضع نقطة توقف وينفذ البرنامج ستلاحظ أن Olly أو قف البرنامج عند تعليمة قد تكون غريبة

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

وإصنع باتش يقوم بتغيير هذه 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

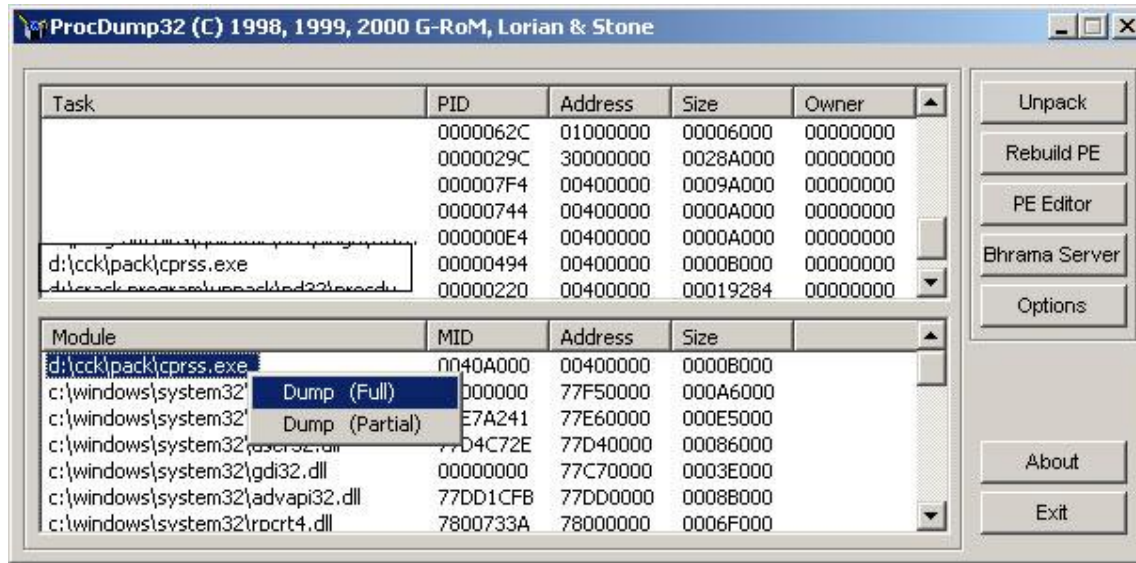
ولكن قد يرغب البعض بتعلم:

فك تشفير البرنامج وإعادة ترميزه 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

أنه أكبر بكثير من الملف المشفر والسبب لأننا حفظنا الملف مباشرة من الذاكرة ( بعد أن فك تشفيره )

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 هذه العناوين قوانين ثابتة - وأعتقد أنها ليست جديدة أو غريبة عليك

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

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

وهذا الدرس باختصار تطبيق لما قرأته في موضوع المترجمات

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

ولدينا xxcprss وهو الملف المشفر ولكن بعد فك ضغطه في الذاكرة (راجع حجمة )

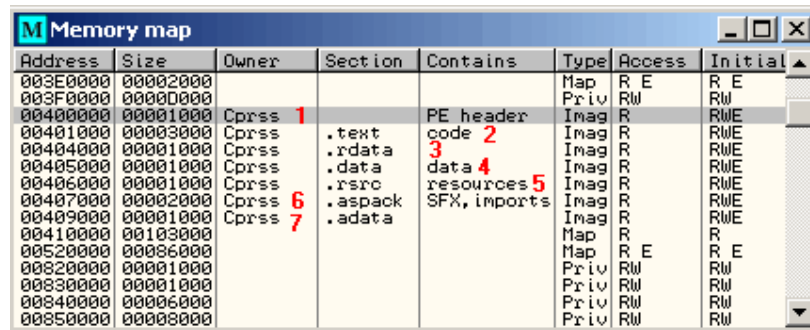
قم بتشغيل الملف Cprss ثم قم بتشغيل نسختين من برنامج Olly

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 (لنتفتح الملف بمحرر هكس )

أول شيء سنقوم به نقل محتويات الأقسام بعد فك تشفيرها

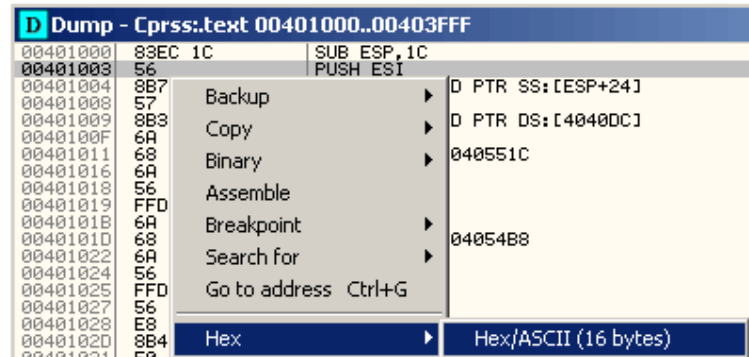
في نسخة Olly الخاصة بـ Cprss أعمل تخطيط للذاكرة عن طريق الأمر M



Address	Size	Owner	Section	Contains	Type	Access	Initial
003E0000	00002000				Map	R E	R E
003F0000	00000000				Priv	RW	RW
00400000	00001000	Cprss	1	PE header	Image	R	RWE
00401000	00003000	Cprss	.text	code	Image	R	RWE
00404000	00001000	Cprss	.idata	3	Image	R	RWE
00405000	00001000	Cprss	.data	data	Image	R	RWE
00406000	00001000	Cprss	.rsrc	resources	Image	R	RWE
00407000	00002000	Cprss	6	SFX, imports	Image	R	RWE
00409000	00001000	Cprss	7	.adata	Image	R	RWE
00410000	00103000				Map	R	R
00520000	00006000				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

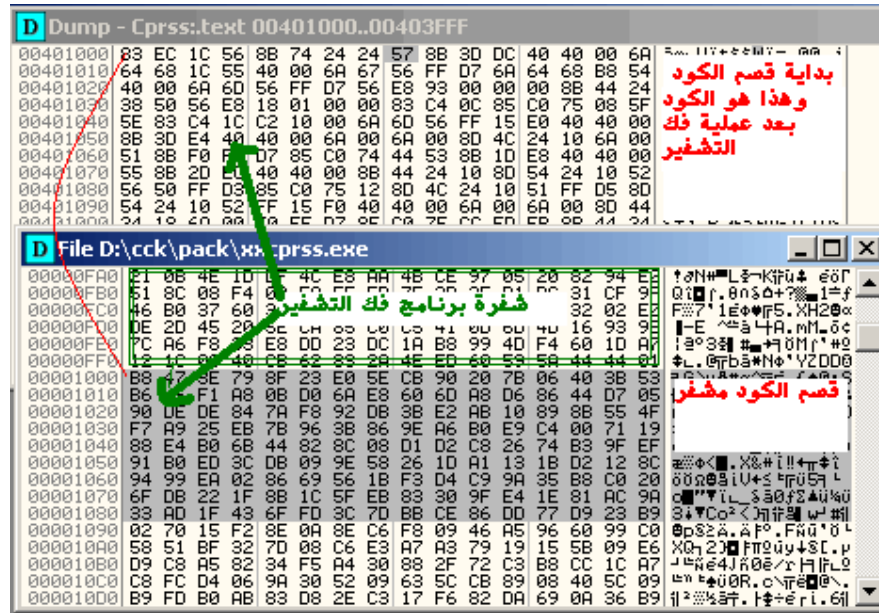
ستظهر لنا النافذة وبها معلومات بلغة الإسمبلي (حولها للترميز الهكس ١٦ بت)



Dump - Cprss:.text 00401000..00403FFF			
00401000	83EC 1C	SUB ESP,1C	
00401003	56	PUSH ESI	
00401004	8B7		D PTR SS:[ESP+24]
00401008	57		D PTR DS:[4040DC]
00401009	8B3		
0040100F	6A		040551C
00401011	68		
00401016	6A		
00401018	56		
00401019	FFD		
00401018	6A		04054B8
0040101D	68		
00401022	6A		
00401024	56		
00401025	FFD		
00401027	56		
00401028	E8		
0040102D	8B4		
00401031	56		

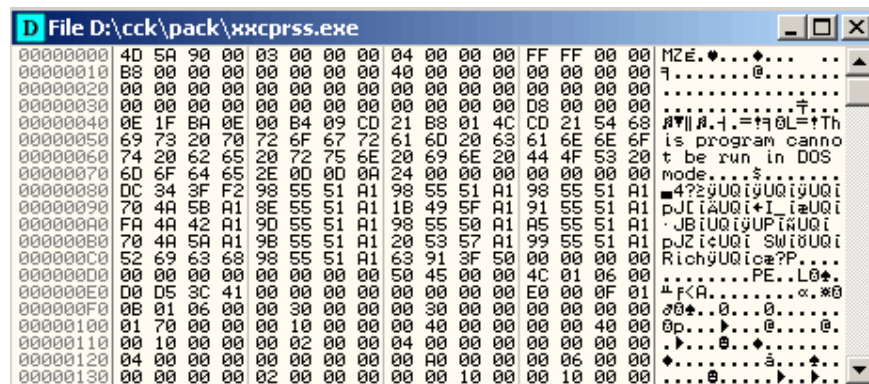
ثم إذهب إلى النسخة الثانية لبرنامج Olly الخاصة بـ xxcprss (إنقل للعنوان ١٠٠٠)

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



الآن عرفنا بداية قسم الكود=1000 وعرفنا محتواة بعد فك التشفير

إذهب إلى برنامج Olly 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 code, adata

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

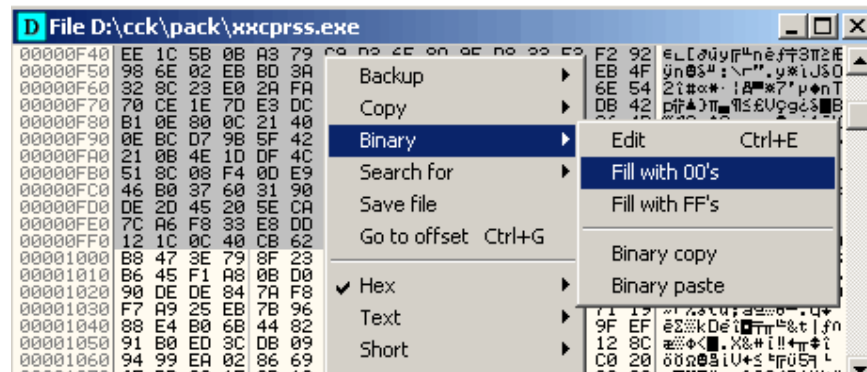
إلى بداية الكود وهو العنوان x01000 سيكون أصفار ( لا يحتوي أي معلومات )

وإذا حبيت أن تعرف ماذا نريد أن نحذف بهذه الطريقة

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

وعند العنوان: x600 يبدأ كود برنامج فك التشفير

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

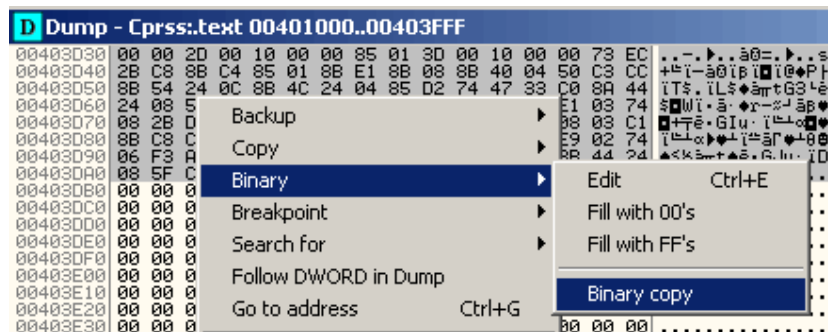


ثم إرجع للنسخة الأولى لبرنامج Olly للملف Cprss (واختر قسم الكود ثم Dump ثم حول الكود للهكس)

كما فعلنا سابقا ولكن الآن نريد نسخ قسم الكود بهذه الطريقة

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

ثم قم بنسخ هذه البيانات بهذه الطريقة

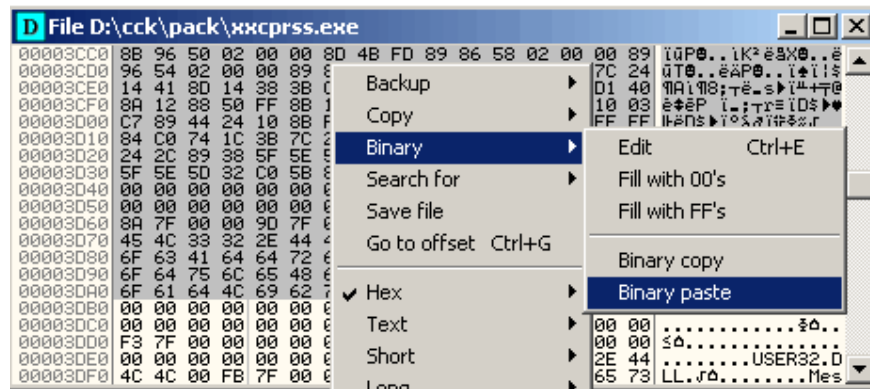


لاحظ توقفنا عند العنوان x403DA0

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 هو عدد 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 أنه في نهاية الكود

الذي علمنا عليه 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

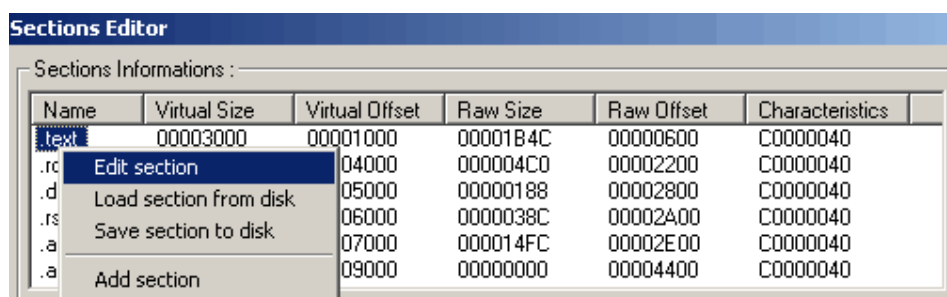
وبهذا نكون قد أوجدنا القسم الفعلي (وهو ما قمنا بنسخة) + القسم الوهمي (وهي الأصفار في نهاية الكود)

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

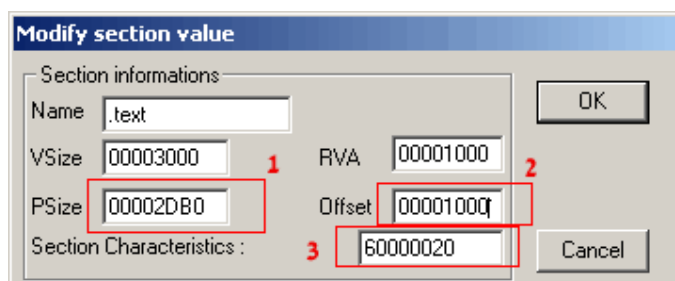
وإختر Save file ثم إحتفظ الملف وقم بحذف الملف القديم xxcprss و ضع بدلة الملف الجديد بنفس الإسم

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

وأدخل الملف الجديد xxcprrs تظهر لك نافذة إختار منها Sections وعدل قسم الكود



تظهر لك نافذة التعديل غير هذه القيم



١- الحجم الفعلي لقسم الكود

٢- بداية قسم الكود

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

والحمد لله إستطعنا إرجاع قسم الكود كما كان عندما كتبه 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 نطبق كل الخطوات في القسم السابق ولكن في بعض التغييرات

جرب نفس الطريقة السابقة في نسخ قسم البيانات ستلاحظ هذه النافذة

```

D Dump - Cprss:rdata 00404000..00404FFF
00404000 34 2F F9 77 EB 41 E6 77 F9 81 E7 77 05 74 E7 77 4/·w$Apw·üryw&tyw
00404010 CE 7C E7 77 08 05 E8 77 FD A5 E7 77 00 CD F8 77 iftyw&zw·üryw.=ow
00404020 0A 98 E7 77 34 7B F5 77 03 C7 E6 77 3F A1 E7 77 üryw4CJw@tyw?tyw
00404030 9F 84 E7 77 8C 9D E7 77 40 6F F9 77 F8 88 F5 77 ftywtyw@·w&Jw
00404040 34 9E E7 77 26 C7 E7 77 08 6E E7 77 06 84 E7 77 4tyw&tyw&nyw&tyw
00404050 3D 9C E7 77 31 C9 E7 77 E1 7E E7 77 02 77 E6 77 =tyw1tyw&tyw&tyw
00404060 93 9F E7 77 7A 17 E6 77 38 C9 E7 77 86 C4 E7 77 ötyw&tyw&tyw&tyw
00404070 B5 5C E7 77 B4 16 E6 77 90 9C E7 77 84 9A E8 77 ftywtyw&tyw&tyw&tyw
00404080 99 A0 E7 77 B1 C5 E9 77 E1 C9 E7 77 24 99 E7 77 ötyw&tyw&tyw&tyw
00404090 66 C8 E7 77 00 00 00 00 F0 11 D6 77 E9 EA D6 77 ftyw.....=4tyw&tyw
004040A0 58 16 D6 77 5E 63 D5 77 38 4D D4 77 0D 5A D4 77 %tyw^tywMtywZtyw
004040B0 C0 9C D8 77 2C 0F D5 77 54 57 D4 77 AB 45 D4 77 &tyw&tyw&tyw&tyw&tyw&tyw
004040C0 B0 C4 D4 77 68 BC D4 77 A0 BC D4 77 A0 4C D4 77 =tyw&tyw&tyw&tyw&tyw&tyw
004040D0 1D 21 D5 77 A9 E4 D4 77 70 09 D6 77 8C F2 D4 77 #tyw&tyw&tyw&tyw&tyw&tyw
004040E0 3D A6 D5 77 8F 5A D4 77 3A B9 D5 77 C8 47 D4 77 =tyw&tyw&tyw&tyw&tyw&tyw
004040F0 2D 4D D4 77 00 00 00 00 FF FF FF FF 07 16 40 00 -tyw.....@.
00404100 1B 16 40 00 72 75 6E 74 69 6D 65 20 65 72 72 6F +@.runtime erro
00404110 72 20 00 00 0A 00 00 54 4C 4F 53 53 20 65 72 r .....TLOSS er
00404120 72 6F 72 00 0A 00 00 53 49 4E 47 20 65 72 72 ror.....SING err
00404130 6F 72 00 0A 00 00 00 44 4F 4D 41 49 4E 20 65 or.....DOMAIN e

```

هذه 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 هذه البيانات التي تراها ليست في الملف الأصلي وإنما كتبها النظام )

والذي نريد معرفة الآن بالضبط هو محتوى هذا القسم بعد مايقوم برنامج فك التشفير بكتابة هذا القسم

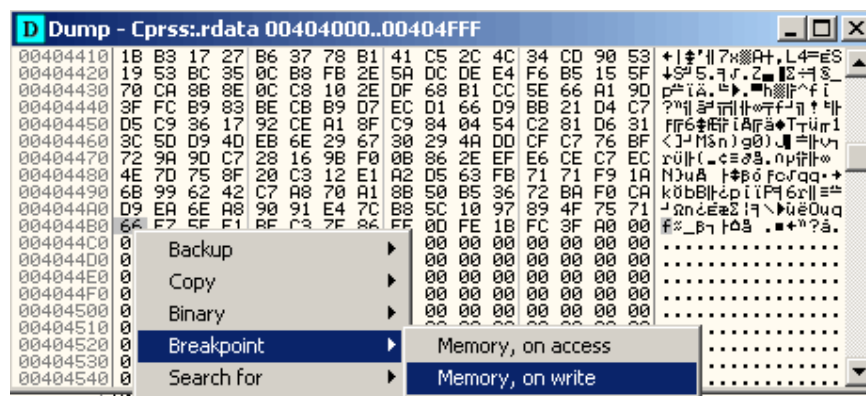
وقبل أن يقوم نظام التشغيل بتحويل هذه البيانات إلى عناوينها في الذاكرة

بمعنى نريد معرفة بيانات هذه 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 - بهذه الطريقة



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

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

ثم إذهب إلى نفس القسم ونفذ أمر Dump ولاحظ التغير



```

D Dump - Cprss:rdata 00404000..00404FFF
00404000 90 45 00 00 7A 49 00 00 6A 49 00 00 5A 49 00 00 eE..zI..jI..ZI..
00404010 44 49 00 00 34 49 00 00 22 49 00 00 14 49 00 00 DI..4I..I..I..
00404020 04 49 00 00 F8 48 00 00 EC 48 00 00 E2 48 00 00 I..H..H..H..
00404030 06 48 00 00 CA 48 00 00 BE 48 00 00 B2 48 00 00 rH..H..H..H..
00404040 A4 48 00 00 96 48 00 00 88 48 00 00 7A 48 00 00 rH..H..H..H..
00404050 6A 48 00 00 58 48 00 00 3E 48 00 00 26 48 00 00 jH..XH..>H..&H..
00404060 2E 47 00 00 42 47 00 00 54 47 00 00 66 47 00 00 .G..BG..TG..fG..
00404070 74 47 00 00 82 47 00 00 96 47 00 00 AA 47 00 00 tG..eG..gG..-G..
00404080 C6 47 00 00 DC 47 00 00 F6 47 00 00 10 48 00 00 fG..mG..+G..H..
00404090 8C 49 00 00 00 00 00 00 14 47 00 00 02 47 00 00 iI.....IG..OG..
004040A0 F6 46 00 00 E4 46 00 00 04 46 00 00 C4 46 00 00 +F..ZF..*F..-F..
004040B0 B6 46 00 00 AA 46 00 00 9E 46 00 00 8C 46 00 00 tF..-F..F..iF..
004040C0 7C 46 00 00 6A 46 00 00 5C 46 00 00 4C 46 00 00 tF..jF..fF..LF..
004040D0 40 46 00 00 32 46 00 00 1E 46 00 00 10 46 00 00 @F..ZF..fF..fF..
004040E0 FC 45 00 00 EE 45 00 00 06 45 00 00 C2 45 00 00 *E..eE..rE..tE..
004040F0 AE 45 00 00 00 00 00 00 FF FF FF FF 07 16 40 00 *E.....E..
00404100 1B 16 40 00 72 75 6E 74 69 6D 65 20 65 72 72 6F *.@.runtime erro
00404110 72 20 00 00 00 0A 00 00 54 4C 4F 53 53 20 65 72 r.....TLOSS er
00404120 72 6F 72 00 0A 00 00 00 53 49 4E 47 20 65 72 72 ror.....SING err
00404130 6F 72 00 0A 00 00 00 00 44 4F 4D 41 49 4E 20 65 or.....DOMAIN e

```

هذه البيانات بإختصار هي محتوى القسم كما كتبها المترجم

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

وانسخ 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 أماكن عليّة قبل التشفير

بقي نقطة مهمة وهي عنوان الدوال المستوردة وهو: x0445C

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

وبطريقة عملية لاحظ الصورة

```

D Dump - Cprss:rdata 00404000..00404FFF
004043F0 6E 3E 00 00 47 65 74 4C 61 73 74 41 63 74 69 76 n>..GetLastActiv
00404400 65 50 6F 70 75 70 00 00 47 65 74 41 63 74 69 76 ePopup..GetActiv
00404410 65 57 69 6E 64 6F 77 00 4D 65 73 73 61 67 65 42 ewindow.MessageB
00404420 6F 78 41 00 75 73 65 72 33 32 2E 64 6C 6C 00 00 oxA.user32.dll..
00404430 00 00 00 00 00 00 00 00 FF FF FF FF 2E 37 40 00 .....7@.
00404440 32 37 40 00 FF FF FF FF E2 37 40 00 E6 37 40 00 27@.
00404450 FF FF FF FF 66 39 40 00 6A 39 40 00 98 44 00 00 f9@.j9@.yD..
00404460 00 00 00 00 00 00 00 00 A0 45 00 00 00 40 00 00 .....aE...@..
00404470 30 45 00 00 00 00 00 00 00 00 00 00 22 47 00 00 0E....."G..
00404480 98 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 y@.....eE..zI..
00404490 00 00 00 00 00 00 00 00 90 45 00 00 7A 49 00 00 jI..ZI..DI..4I..
004044A0 6A 49 00 00 5A 49 00 00 44 49 00 00 34 49 00 00 f%_b1t53..*~?3.
004044B0 66 F7 5F E1 BF C3 7F 86 FF 0D FE 1B FC 3F A0 00 .....
004044C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
004044D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
004044E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
004044F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00404500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00404510 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00404520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Command :

Memory breakpoint when writing to [004044B0]

وتمكننا هذه ٢٠ بايت من معرفة اسم المكتبة وعناوين الدوال المستوردة

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

قانون قلب العنوان وبعد ذلك تبحث عن هذا العنوان ليدلك على ٢٠ بايت الخاص بهذه 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 القيمة ٠ 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 بعمله في قسم الكود )

### قسم ملف المصادر rsrc

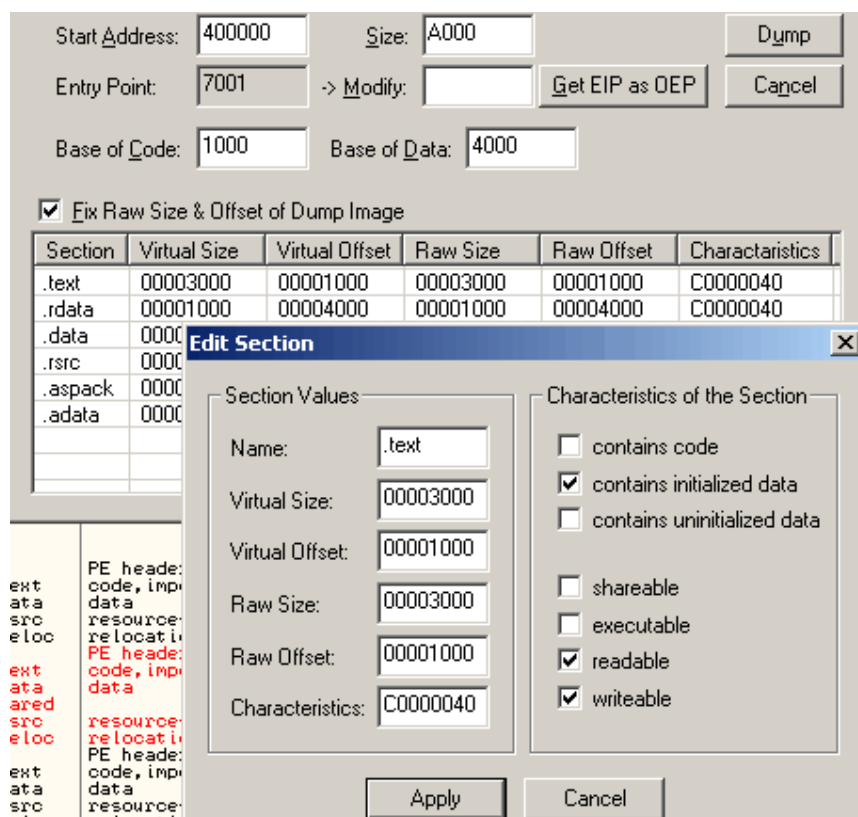
هذا القسم ولا أسهل ( شغل Olly ثم File ثم Attach وأدخل الملف Cprss )  
ثم حدد القسم rsrc ثم Dump وإنسخ كل محتوى القسم وقم بلصقة في محرر الهكس  
وعنوان جدول المصادر = عنوان بداية القسم كما هو x6000  
وحجم جدول المصادر = x9D0 نفسة الحجم الفعلي للقسم (بمعنى عدد البايتات التي لا تساوي ٠ في القسم)  
أما عن بقية الأقسام فهي تخص البرنامج الثاني - برنامج فك التشفير  
وهي aspack + adata  
وتمثل قسم الكود وقسم البيانات .. أكيد إحدفها Delete بواسطة ProcDump32

-----

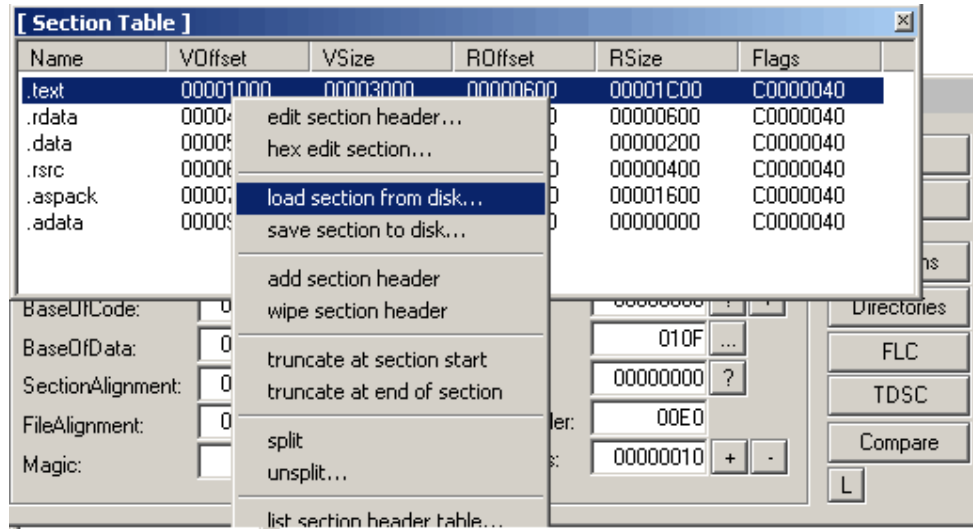
وبهذه الطريقة نكون قد أكملنا كل البرنامج وقمنا بإرجاعه إلى الصيغة القياسية قبل التشفير  
بقي فقط نقطة واحد وهي عنوان بداية تنفيذ البرنامج  
وهذا العنوان لا يوجد لة قانون ( ولكنة نعرف من شكلة ) فهو يأتي قبل دوال تشغيل البرنامج الأساسية  
وإذا لم نستطع معرفة (تتبع برنامج فك التشفير وحاول معرفة متى ينقل التنفيذ إلى البرنامج الأصلي)  
وفي مثالنا ستجد العنوان التالي : x401530 ويساوي x1530 وهو بالضبط عنوان بداية التنفيذ

وبهذا نكون قد أنهينا 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 هذه النافذة في أولي ( ولا أسهل )



وبكل بساطة تحدد الذي قمنا بتغييره 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 الأنواع  
والنقطة الثانية أن كل ما قمنا به من مراحل ( تقوم به بعض البرامج بكسبة زر 🛑 ) لاحظ



وهذا البرنامج : Lord PE موقع : [www.y0da.cjb.net](http://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 عليه

هذا والله أعلم

٢٠٠٤/٩/٨