تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

JAAS @: jaas1001@hotmail.com

السلام عليكم ورحمة الله ،،،

برنامج olly من أفضل الأدوات لتصحيح ومتابعة الملفات التنفيذية (البرامج)

وأفضل ميزة لإختيارة في هذا الشرح سهولة إستخدامة وإمكاناتة المتقدمة في تنقيح البرامج

نبدأ الشرح :

موقع البرنامج : http://home.t-online.de/home/Ollydbg

شغل برنامج olly

كما هو الحال في برامج التنقيح توجد طريقتين لإدخال البرامج ومتابعتها وتنقيحها

من القائمة إختر File تلاحظ الطريقتين وهما (Open - Attach)

الأمر Open : وهي الطريقة القياسية لإدخال أي برنامج لتصحيحة ومراقبتة

من بداية تشغيلة إلى أن تنهي البرنامج.

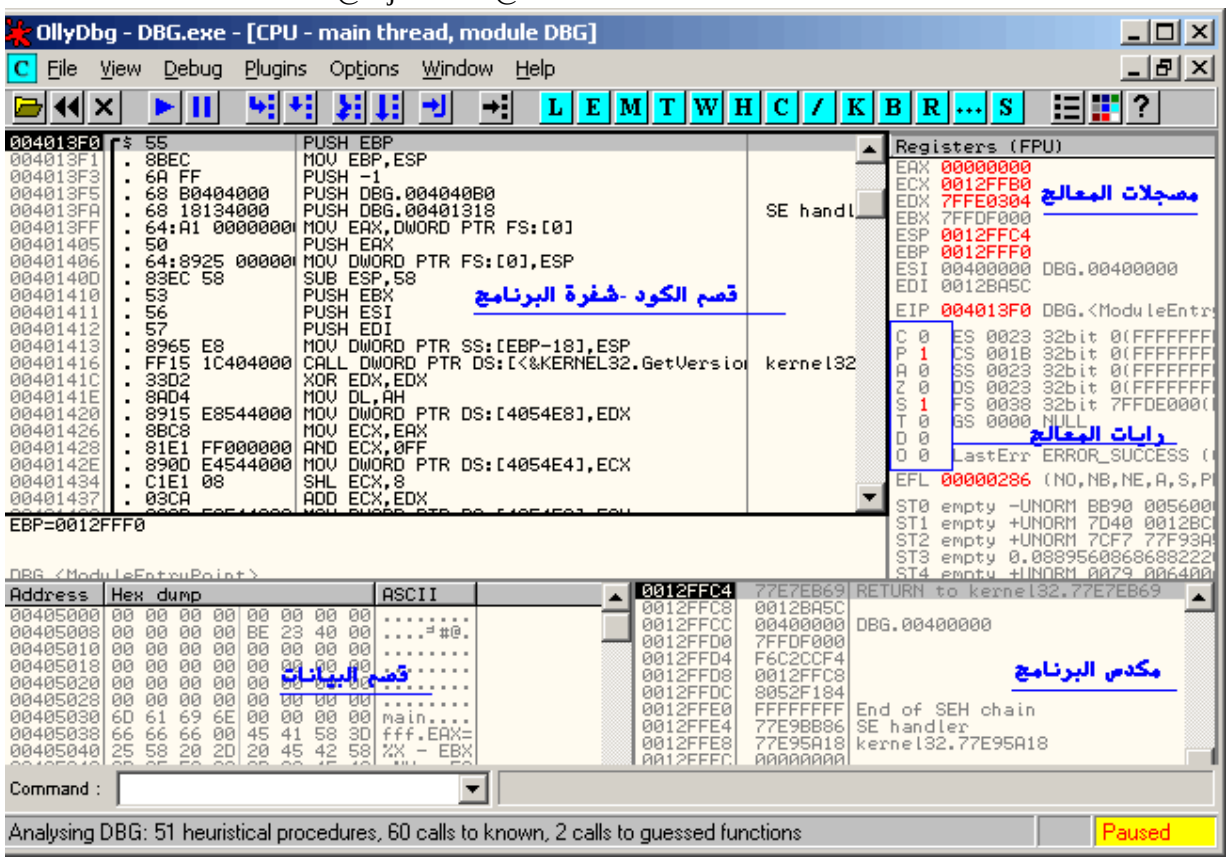
الأمر Attach : وهذة الطريقة لإدخال برنامج يعمل (مقيم في الذاكرة)

ومتابعتة من موقع تنفيذة(هذة الطريقة قد تستخدم في البرامج المشفرة-و البرامج المقيمة في الذاكرة)

إختر Open وتجول في جهازك وإختر أي ملف تنفيذي (ثم لاحظ الصورة)

تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

JAAS @: jaas1001@hotmail.com



هذة الصورة تظهر بعد إختيار البرنامج وتسمى هذة النافذة الرئيسية CPU

ماهي أقسام هذة النافذة (لاحظ العناوين باللون الأزرق)

١ - قسم الكود : وهو القسم التنفيذي من الملف بإختصار هو البرنامج ويشمل الأوامر والدوال والتحكم في سير البرنامج

٢ - قسم البيانات : بإختصار كل الأقسام التي في البرنامج غير قسم الكود تسمى أقسام بيانات

والبيانات مثلا هي مصادر البرنامج - النصوص - عناوين النوافذ إلى آخرة

٣ - مكدس البرنامج : وهو عبارة عن قسم من الذاكرة يعرض ويخزن فية البيانات التي تعالج الآن في الذاكرة

مثلا بارمترات الدوال - عناوين البيانات

٤ - مسجلات المعالج : تنقسم المسجلات إلى نوعين

مسجلات عامة مثل EAX ,EBX ,ECX ,EDX (وهي لنقل المعلومات ومعالجتها)

مسجلات دليلية مثل EDI ,ESI ,ESP , EBP , EIP (وهي تعتبر دليل للأقسام)

مثلا EIP = دليل لقسم الكود (أي أن رقم EIP = السطر الذي ينفذ في قسم الكود)

ESI-EDI = مسجلات دليلية تسهل عملية الوصول للبيانات لقسم البيانات + القسم الموسع(معالجة النصوص)

JAAS @: jaas1001@hotmail.com

ESP = العنوان الذي يعالج حاليا في المكدس - EBP =مساعد لمعالجة البيانات في المكدس

٥- رايات المعالج : ولها إسم ثاني أعلام المعالج وتعبر هذة الرايات عن حالة المعالج

وهذة الرايات هي : (لاحظ الحرف الأول = كما هو موضع في نافذة البرنامج)

CF : تحتوي على محتوى الخانة الأخيرة لعملية إزاحة أو دوران

PF : علم التحقق وهو يتحقق من الخانات الثمانية الأولى يوضع ١ إذا كان ناتج التحقق زوجي و ٠ إذا كان فردي

AF : علم الحمل يفيد في بعض العمليات الحسابية الخاصة وهي تشير إلى وجود الحمل في أحد الخنات

ZF : يوضع في هذا العلم ٠ =إذا كان ناتج آخر عملية مقارنة غير صفري وواحدعندما يكون صفر

SF : يحتوي هذا العلم على إشارة الرقم الناتج عن آخر عملية حسابية ٠= موجب ١= سالب

TF : وتشير هذة الراية للمعالج بالعمل خطوة خطوة لتتبع الأخطاء ومثال برنامج الديبغر يستعمل هذا لعلم

IF : تشير إذا كانت ١ إلى السماح بحدوث طلب مقاطعة خارجي (وهذا غير موجد في ٣٢ بت -فقط برامج دوس)

DF : تحدد إتجاه يسار أو يمين عملية مقارنة السلاسل

OF : وتشير إلى ناتج فيض في إحدى العمليات الحسابية

والسؤال الذي يطرح نفسة (ماذا يمكن أن أستفيد من هذة الرايات)

بكل بساطة تعرف مثلا هل تعليمة القفزة ستنفذ أو لا - تعرف نتيجة مقارنة

مثلا لاحظ هذة القفزات وما هي الشروط لتتحققها (لاحظ رايات المعالج)

مع ملاحظة أن بعض القفزات لها نفس الوظيفة مع إختلافها في طريقة الكتابة

القفزة	الشرح	رايات المعالج
JA	إقفز إذا كان أكبر	ZF=0 - CF=0
JAE	إقفز أذا كان أكبر أو يساوي	CF=0
JB	القفز إذا كان أصغر	CF=1
JBE	القفز إذا كان أصغر أو يساوي	ZF=1 CF=1
JC	القفز في حالة الترحيل	CF=1
JCXZ	القفز في حالةCX=0	-
JECXZ	القفز في حالة ECX=0	-
JZأوJE	القفز إذا كان يساوي	ZF=1
JG	إقفز إذا كان أكبر	ZF=0 SF=OF
JGE	إقفز أذا كان أكبر أو يساوي	OF=SF

JAAS @: jaas1001@hotmail.com

JL	القفز إذا كان أصغر	OF != SF
JLE	القفز إذا كان أصغر أو يساوي	ZF=1 OF!=SF
JNA	القفز إذا لم يكن أكبر	-
JNAE	القفز أذا لم يكن أكبر أو يساوي	-
JNB	القفز إذا لم يكن أقل	-
JNBE	القفز إذا لم يكن أقل أو يساوي	-
JNC	القفز في حالة عدم الترحيل	CF=0
JNZأوJNE	القفز إذا لم يكن يساوي	ZF=0
JNG	القفز إذا لم يكن أكبر	ZF=1 OF!=SF
JNGE	القفز أذا لم يكن أكبر أو يساوي	-
JNL	القفز إذا لم يكن أقل	-
JNLE	القفز إذا لم يكن أقل أو يساوي	-
JNO	القفز في حالة عدم الفيض	OF=0
JNP	القفز في حالة عدم التمثيل	PF=0
JNS	القفز في حالة عدم وجود علامة جبرية	SF=0
JO	القفز في حالة الفيض	OF=1
JP	القفز في حالة التماثل	PF=1
JPE	القفز في حالة التماثل المزدوج	PF=1
JPO	القفز في حالة التماثل المفرد	PF=0
JS	القفز في حالة وجدود علامة جبرية	SF=1

إذا لم تتمكن من حفظ كل هذة القفزات (فعليك حفظ القفزات التي باللون الأحمر فهي المستخدمة بنسة ٨٠ % تقريبا)

كل القفزات التي تم عرضها هي قفزات شرطية وهناك نوع آخر وهي القفزات الغير مشروطة مثل JMP

التحكم في سير البرنامج

بعد أن قمت بتحميل ملف تنفيذي إلى برنامج olly تستطيع أن تتحكم بة بطريقة سهلة (مفاتيح الإختصار)

المفتاح F8 = تنفيذ البرنامج خطوة خطوة بمعنى تنفيذ تعليمة واحدة

المفتاح F9 = تشغيل البرنامج أي تنفيذ كل التعليمات إلى أن تحدث نقطة توقف لتوقف البرنامج

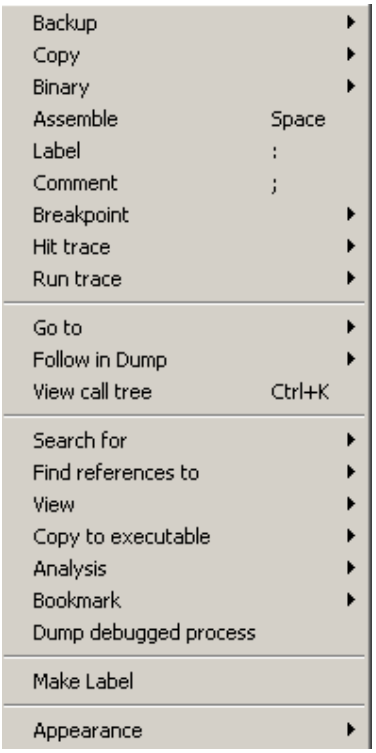
المفتاح F2 = إدراج أو حذف نقطة توقف على العنوان المحدد

الخيارات الأخرى

إختر منطقة الكود وإضغط الزر الأيمن للماوس ولاحظ القائمة

تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

JAAS @: jaas1001@hotmail.com



ملاحظة بعض الأوامر تتغير بحسب التعليمة المؤشر عليها (وهذا هو سبب تميز هذا البرنامج)

سؤحاول شرح بعض أوامر القائمة المهمة للمبتدىء

Backup : تحفظ نسخة إحتياطية للملف كما يمكن إستخدام هذا الأمر في طرق متقدمة مثل مقارنة الملفات والتغيرات

Binary : التغيير في التعليمة بصيغة الترميز الست عشري (هيكس)

Assemble : التغيير في التعليمة بصيغة لغة الإسمبلي

مع ملاحظة أن أي تغيير تجرية داخل نافذة CPU وبواسطة هذان الأمران لايحفظ في الملف

بمعنى أنك عندما تخرج من البرنامج فإن التغيرات لا تحفظ في الملف على القرص (توجد طريقة أخرى لحفظ البيانات)

سيتم شرحها لا حقا.

Go to : هذا الأمر ينقلك إلى العنوان الذي تحددة (هل تعتقد أنة بسيط)

هذا الأمر لة طرق متقدمة في تبديل الأقسام (تبديل الأقسام هي حيلة تستخدمها البرامج المشفرة)

للفائدة هناك قانون يجب أن تعرفة ألى وهو ترتيب الأقسام (يجب أن يكون ترتيب أقسام البرنامج بهذة الطريقة)

١- مكدس ٢- قسم كود ٣- قسم بيانات

تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

JAAS @: jaas1001@hotmail.com

وطبعا البرامج المشفرة تغير في هذا الترتيب مما يجعل برنامج olly غير قادر على معرفة الدوال المستوردة مثلا -أو كود البرنامج

وسيكون لنا شرح منفصل عن هذة الطرق

Search for : عند ملامستك لهذة القائمة تظهر قائمة أخرى مليئة بالأوامر

كل الأوامر هي للبحث فمثلا All Referenced text يعرض كل النصوص الموجودة في قسم البيانات

الأمر All Switches يعرض لك حلقات المقارنة في البرنامج وهكذا كل الأوامر

فقط في ملاحظة على الأمر All intermodualr calls هذا الأمر يظهر لك الدوال المستوردة والمصدرة التي

يستخدمها البرنامج ولاكن فائدة هذا الأمر أنة يعرض الدوال التي داخل القسم المحدد فقط (أعتقد إن فكرة تشفير البرامج صارت مفهومة)

وسنقوم بمناقشة هذة الطرق في دروس مقبلة بإذن الله

بعد ذلك يأتي في القائمة الرئيسية

الأمر **to Find References**

هذا الأمر مهم لتعرف كيف وصل التنفيذ للأمر المؤشر علية (بمعنى ما هي الأوامر المتصلة بهذة التعليمة)

الأمر **View** + الأمر **Copy to executable**

تنقلك هذة الأوامر إلى شفرة البرنامج وأي تغير فيها تستطيع أن تحفظة على القرص(بمعنى كتابة البرنامج + التغيير فية)

هذة أهم الأوامر الواجب معرفتها (بقية الأوامر تأتي بعد التجربة وفهم عمل البرنامج)

نوافذ البرنامج

L : تعرض لك هذة النافذة معلومات عن البرنامج (ماذا يستخدم - كم ثريد - مكاتب الربط....)

E : تعرض لك هذة النافذة الملفات المرتبطة مع البرنامج

M : تعرض لك هذة النافذة تخطيط مفصل عن البرنامج وملفاتة - كما تعرض ترتيب الأقسام وخصائصها

T : الخيوط (ثريد) المستخدمة في البرنامج

W : نوافذ البرنامج والأزرار

H : مقابض البرنامج (هذا الأمر جديد في إصدارات olly الأخيرة)

JAAS @: jaas1001@hotmail.com

C : تعرض لك نافذة CPU النافذة الرئيسية

K : معلومات مكدس الثريد (مصدر إنشائة)

B : قائمة نقاط التوقف التي وضعتها في البرنامج

ملاحظة (الأوامر التي لم أذكرها - هي تكرار لما تم شرحة في قائمة البرنامج الرئيسة)

بعد كل هذة المعلومات بقي أمر مهم عرض دوال البرنامج وهو المفتاح Ctrl+n

أشر على نافذة CPU وإضغط المفتاح Ctrl+N لتظهر لك قائمة الدوال في البرنامج

تطبيق عملي

هذا مثال بسيط جدا للمبتدئين في تنقيح وتغيير البرامج

ستجد برنامج مرفق مع هذا الدرس هذا البرنامج عبارة عن زر أمر يعرض لك مسج

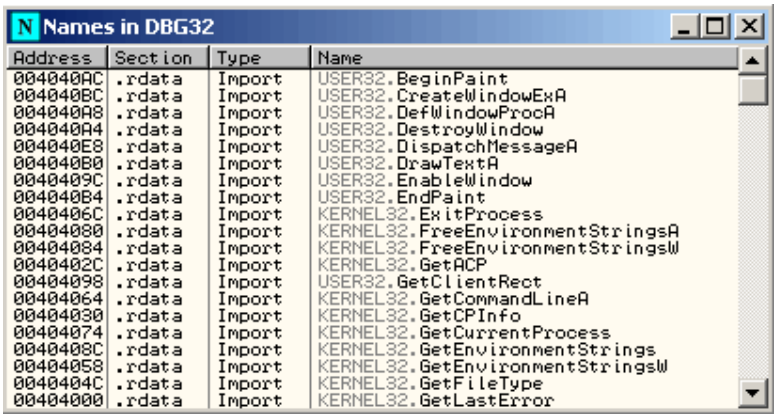
ولاكن هذا الزر غير نشط ونريد في هذا الدرس تطبيق عملي وهو (تنشيط هذا الزر وتنفيذة)

أول خطوة أخرج البرنامج من الملف المضغوط + شغل برنامج olly ثم

Open -> File

إختر البرنامج المرفق مع الدرس ستظهر لك نافذة شبيهة بالصورة الأولى في الدرس

أشر على نافذة CPU على أي عنوان وإضغط مفتاح Ctrl+N ستظهر لك هذة النافذة



هذة هي الدوال المستخدمة في البرنامج (ياترى ماهي الدالة الخاصة بتنشيط الزر أو النافذة)

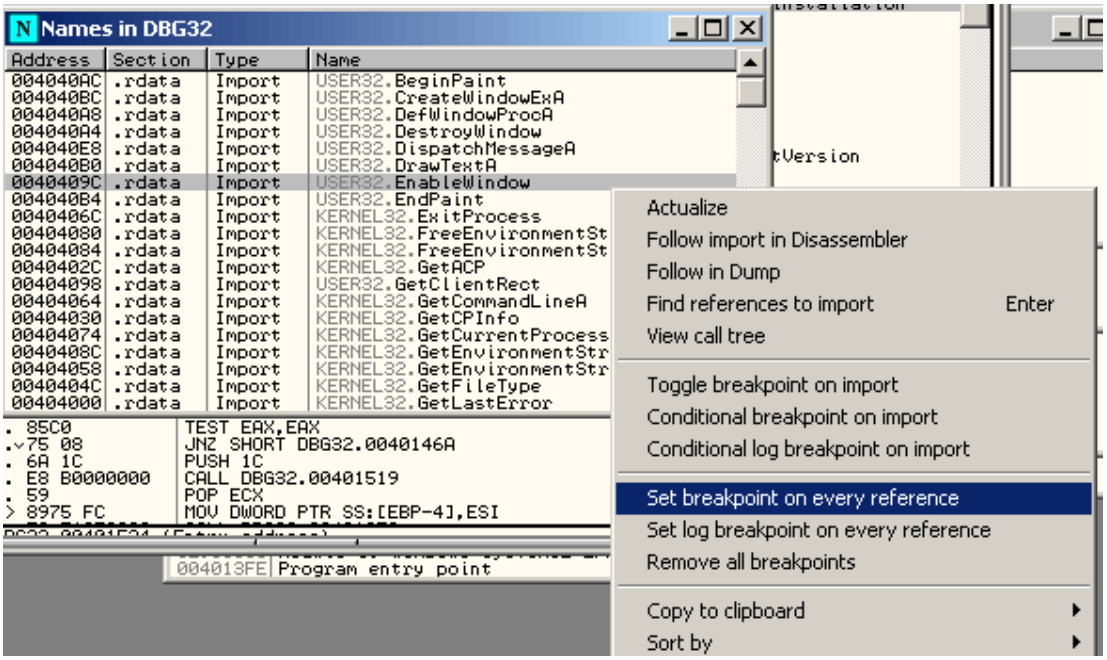
لو كنت مبرمج سي أو تعرف دوال API سيكون تحديد الدالة مجرد لعبة

الى وهي EnableWindow الدالة السابعة في الصورة

تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

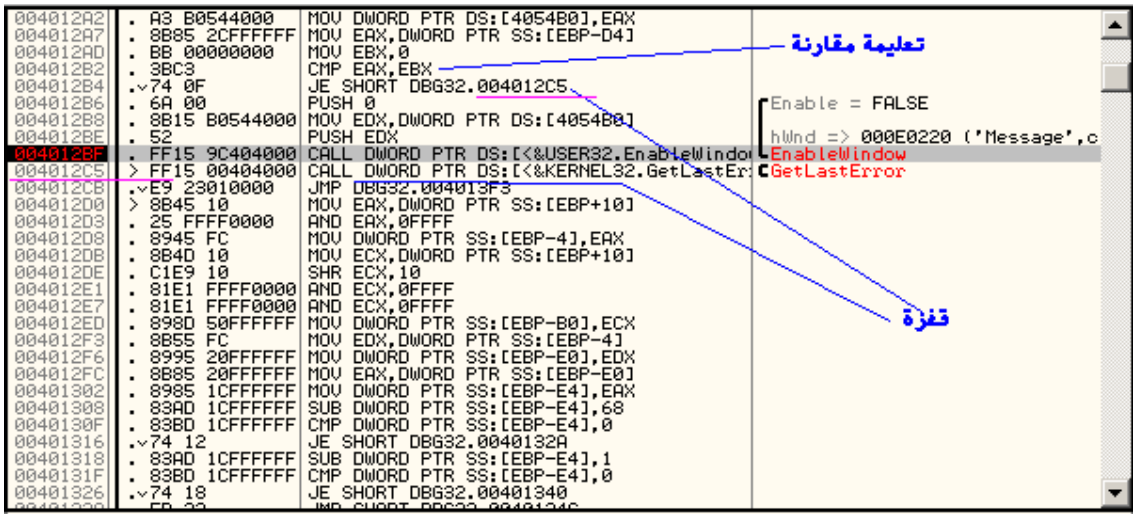
JAAS @: jaas1001@hotmail.com

الآن كيف أضع نقطة توقف على هذة الدالة (أشر على الدالة بالماوس ثم إضغط الزر الأيمن كما هو موضح)



ثم إضغط على الأمر الموضح في القائمة (وهو لوضع نقطة توقف على كل الإتصالات للدالة)

بعد ذلك نفذ البرنامج بالضغط على مفتاح F9 (ماذا تلاحظ - البرنامج توقف عند عنوان بالون الأحمر)



لاحظ مقطع الكود و لاحظ الدالة ماذا جاء قبلها (تعليمة مقارنة)

ودائما بعد تعليمة المقارنة تأتي قفزة وفي مثالنا هي JE (معنى القفزة =إقفز إذا كان يساوي)

و لاحظ إلى أين تقفز (تتعدى نقطة التوقف)

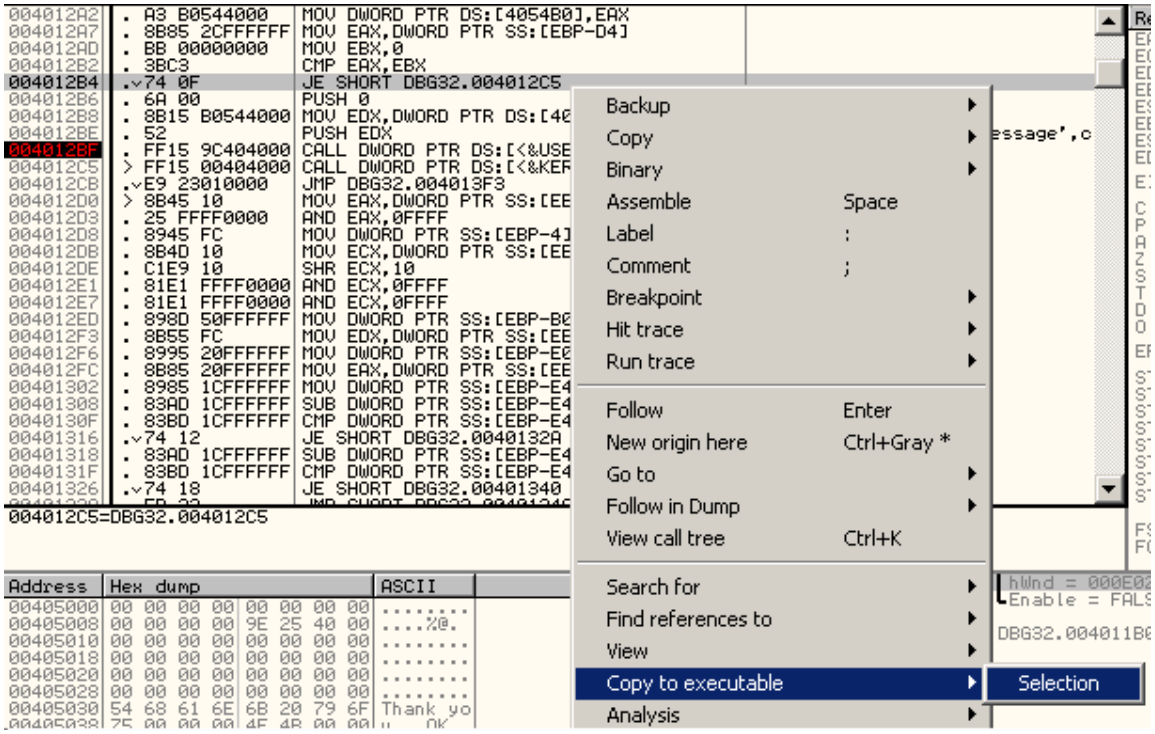
JAAS @: jaas1001@hotmail.com

والملاحظة الثانية هي إسم الزر الممرر للدالة =Message والقيمة FALSE

بمعنى أن هذة الدالة هي التي تجمد الزر (الآن المطلوب تجاوز هذة الدالة) والطريقة بسيطة

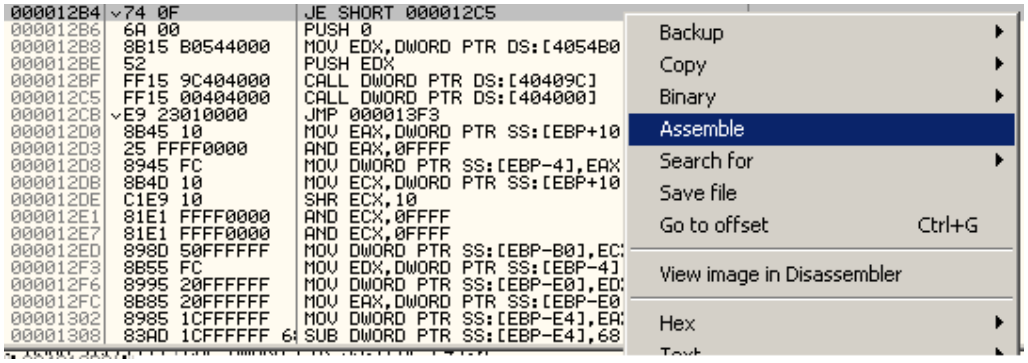
غير JE =إقفز إذا كان يساوي إلى JNE إقفز إذا كان لا يساوي

والطريقة : أشر على تعليمة القفزة وإضغط على الزر الأيمن للماوس



إختر الأمر الموضح في الصورة

تظهر لك النافذة



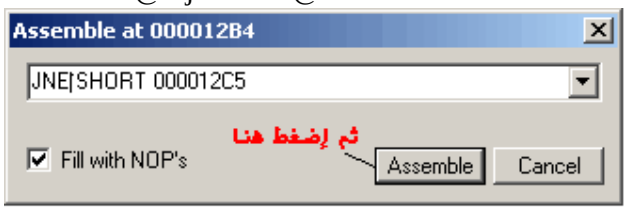
وهي عبارة عن نفس الكود ولاكن تختلف العناوين في الملف (من عناوين وهمية إلى حقيقية)

أشر على نفس التعليمة وإختر الأمر الموضح في الصورة

تظهر لك نافذة تعديل الكود (فقط غير القفزة من JE إلى JNE) بهذا الشكل

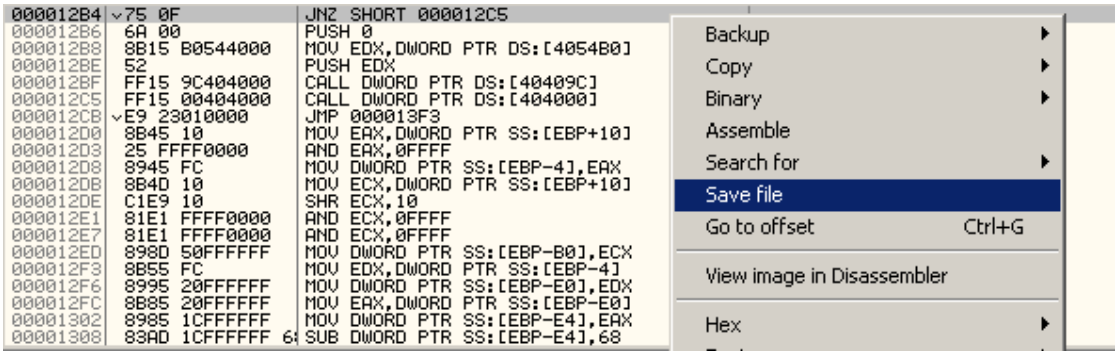
تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

JAAS @: jaas1001@hotmail.com



بعد تغيير أمر القفز إضغط زر Cancel إذا لم تختفي نافذة التعديل

في نفس النافذة إضغط الزر الأيمن للماوس وإختر حفظ الملف



تظهر لك نافذة إستعراض (حدد إسم للملف الجديد وإحفظة)

أغلق برنامج Olly

إذهب للبرنامج الذي غيرتة جرب شغل البرنامج لاحظ زر الأمر إضغط علية (ماذا تلاحظ)

هذة رسالتي لك لتطبيق الدرس

الآن يمكنك النبش والتغيير وزيادة خبرتك في بحر البرمجة العكسية

وبنفس الطريقة مع أي برنامج

وفي ملاحظة : لو وجدت إن الموضوع صعب فإني أقول إن هذا أسهل مثال وجدتة في هذا المجال

وأنصحك بتعلم لغة برمجة مثل سي + فهم تقسيمات البرامج + أساسيات في لغة الإسمبلي

هذا ما يلزمك وبعدها سيفتح المجال بالخبرة وكثرة تصحيح وتغيير البرامج

أتمنى أني قد وفقت في شرح هذا المثال - هذا والله أعلم .

تعلم Olly : أساسيات في تصحيح وتتبع البرامج التنفيذية .....

JAAS @: jaas1001@hotmail.com