بسم الله الرحمن الرحيم
السلام عليكم ورحمة الله وبركاتة

العنـوان : كيفية اصطياد او اقتناص السيريال نمبر من البرامج [ Reverse Engennering ]
الكـاتـب : Hakxer – EgY Coders Team

---

اهلا بكم جميعا ان شاء الله في هذه الورقة سوف اشرح كيفية اصطياد و اقتناص السريال نمبر من البرامج التي تطلب سيريال نمبر وكسرها بمنتهى السهولة .

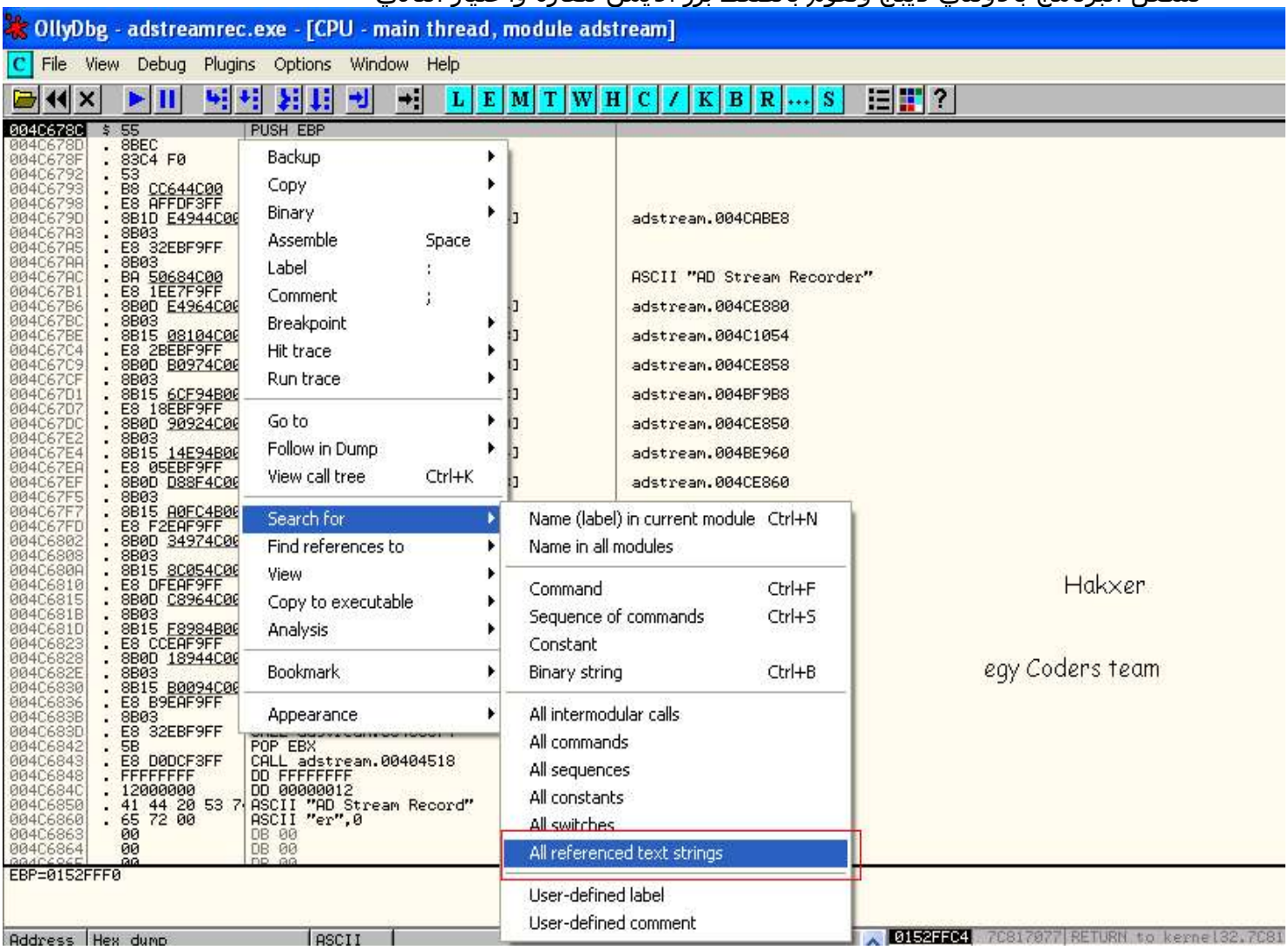
الادوات المستخدمة :
1- برنامج OllyDbg
2-البرنامج المراد كسرة ( AD Stream Recorder )

في البداية هنشغل البرنامج وندخل على منطقة ال Regestration او الريجيستر ( التسجيل ) ونقوم بكتابة بيانات خاطئة لنستخرج محتوى ال MessageBox نقوم بالتالي كما تشاهدون في الصورة


كما ترون المظلل باللون الاحمر هو السيريال نمبر المطلوب الجزء الاول منه والجزء الثاني والمظلل باللون الازرق هي محتوى ال MessageBox والتي هي : Incorrect Code !

الى الاسفل

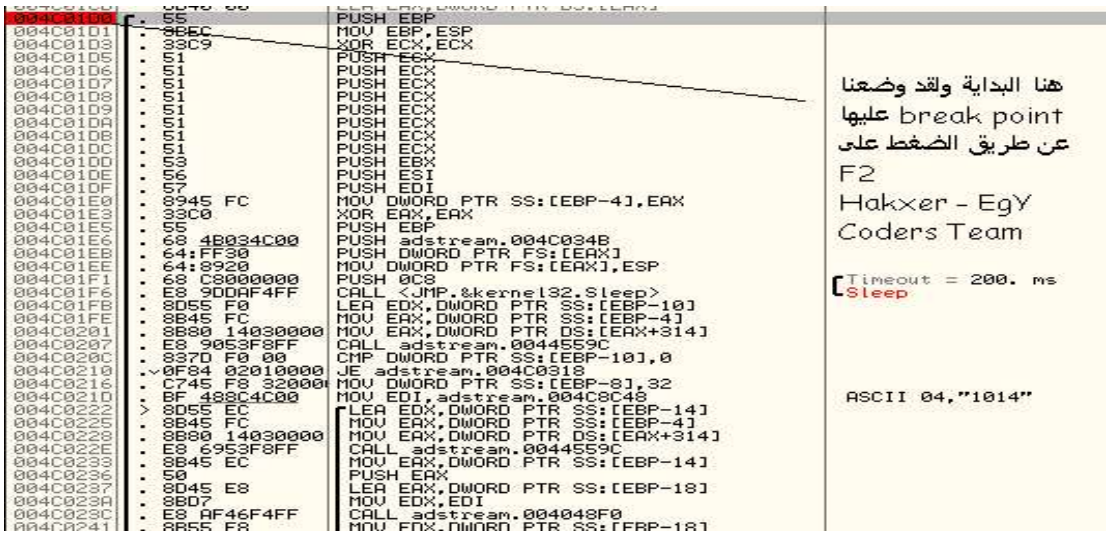
حسنا الان نحفظ هذه الرسالة ونذهب الى صديقنا ال اوللي ديبج للقيام بتنقيح البرنامج
نشغل البرنامج بالاوللي ديبج ونقوم بالضغط بزر الايمن للفارة واختيار التالي




حسنا الان ظهر لنا ال Texts String نقوم بعمل بحث عن الكلمة التي وجدناها في ال MessageBox والتي هي : Incorrect Code!

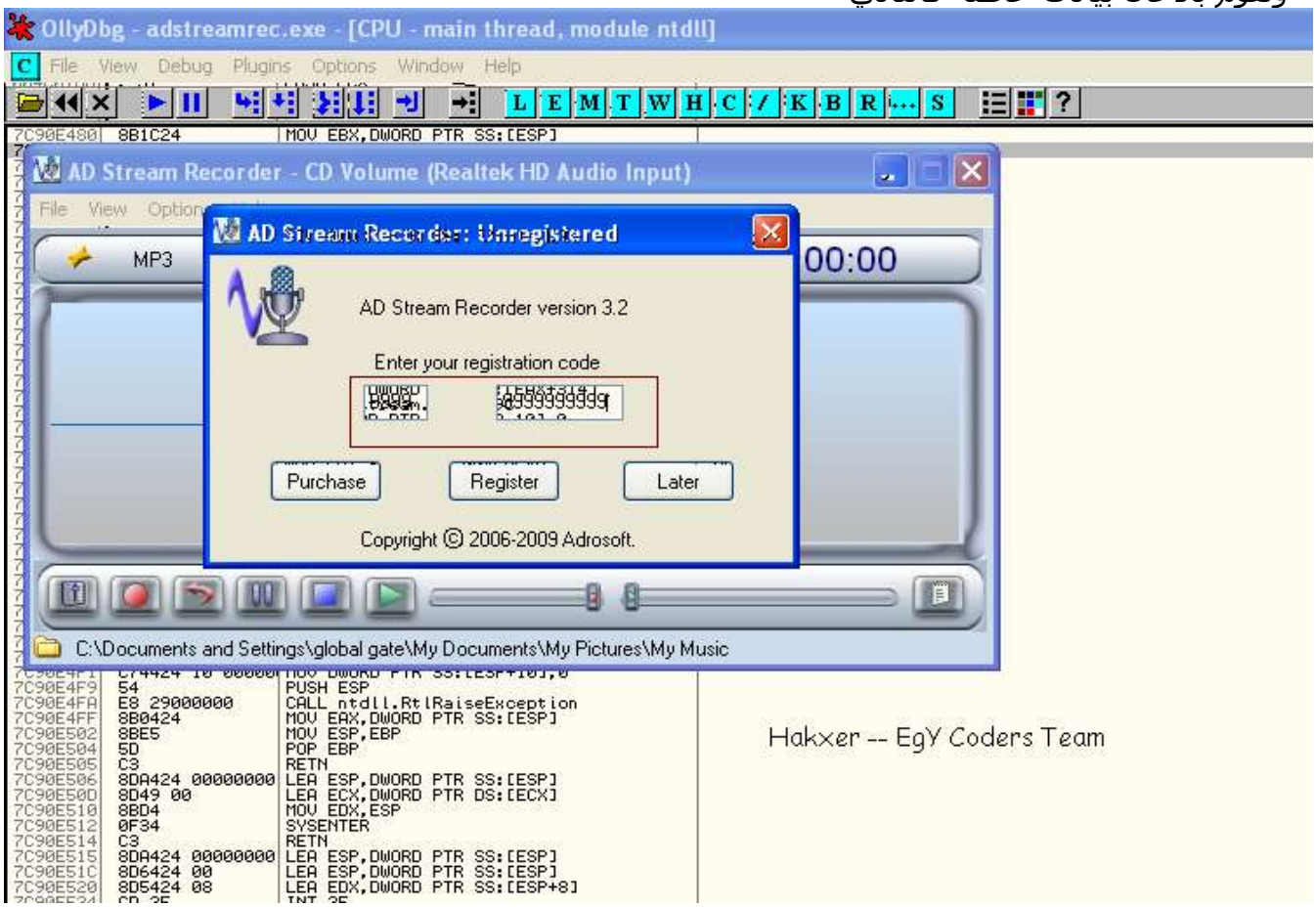

كما تشاهدون لقد وجدنا الجملة التي نبحث عنها حسنا

الان نضغط نقرتين double click




بعدما وضعنا ال Break Point – Toggle نقوم بتشغيل البرنامج من الزر الموجود فوق ( > )

ونقوم بادخال بيانات خاطئة كالتالي




ندخل كمثال 9999999999999999 مثل ماهو في الصورة ونضغط على Register ونقوم بعملية التتبع
وعملية التتبع نقوم بها بالضغط على F8 ومراقبة المكدس ( Stack )
حسنا نتتبع الى ان نجد الجزء الاول من السريال


hakxer - egy coders team

عند 004C0244 لاحظ المكدس ماذا اضيف له انظر الصورة


انظر لقد وجدنا " 1014 " انه الجزء الاول من السيريال ولو قمنا بالتتبع لتغيرت القيمة وظهرت لنا سيريالات جديدة مثلا تتبع مرة اخرى سيظهر لك " 1530 "
حسنا وجدنا الجزء الاول من السيريال يتبقى الجزء الثاني هكذا الحال ايضا مع الجزء الثاني لكن ركز اكتر :D

المهم وجدنا السيريال الثاني ولقد حصلت على اثنين

1222364893
1270287066

طيب الان تعالا نجرب في البرنامج


تمت العملية بنجاح وتم تسجيل البرنامج الى الابد :D

انتهـــت الورقة الى هنـــا

الكـاتب : Hakxer – EgY Coders Team