

آموزش های R4NDOM - فارسی

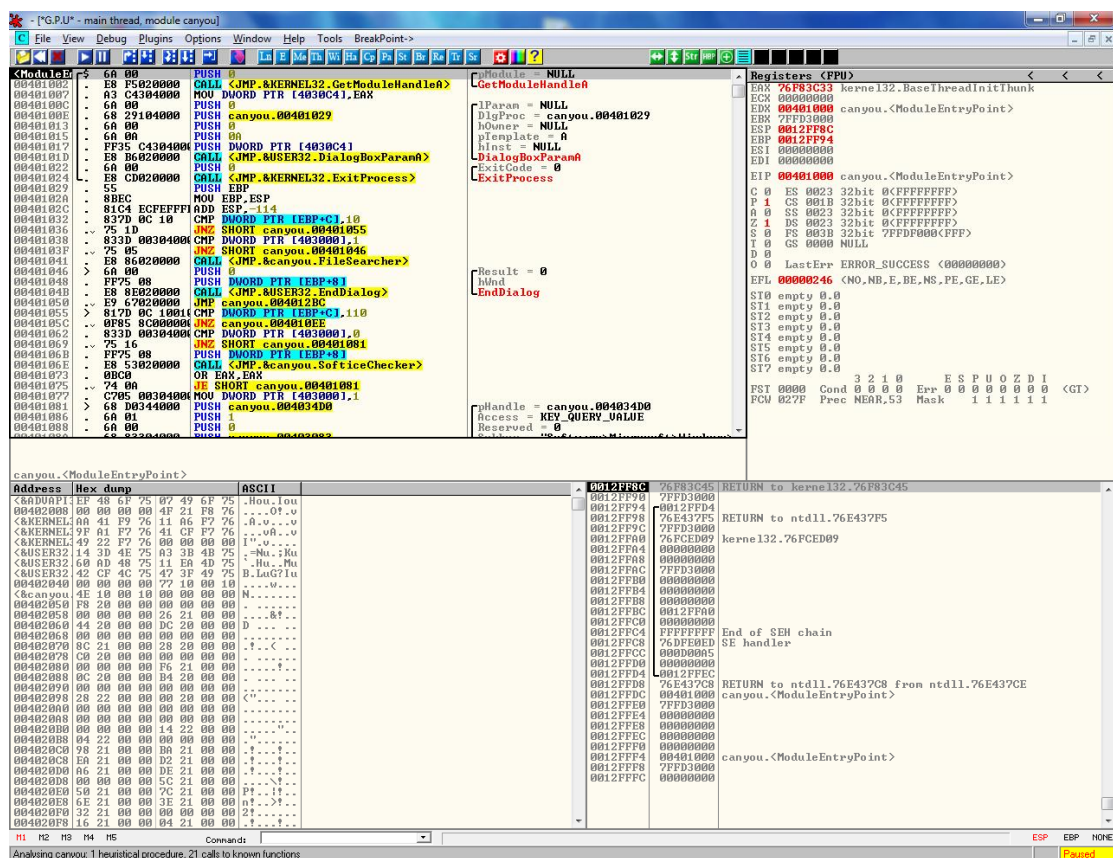
قسمت هفتم - More Crackmes

سلام، به قسمت هفتم از این سری آموزش R4ndom's tutorials on Reverse Engineering خوش آمدید، در این آموزش ما با دو کرک می کار خواهیم کرد، یکی مثله آموزش قبل ا این تفاوت که مانور بیشتری روی آن انجام خواهیم داد و دیگری بیسشتر حالت شونی و سرگرمی دارد ☺

این دو کرک می و همینطور برنامه ی Resource Hacker ضمیمه ی این آموزش شده که از آن در کرک می دوم استفاده میکنیم

بررسی

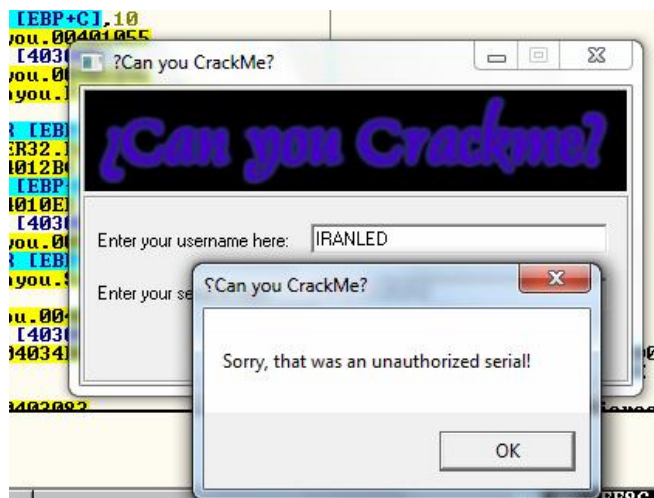
فایل canyou.exe را در Olly باز کنید (مطمئن شوید که فایل canyou.dll در کنارش باشد):



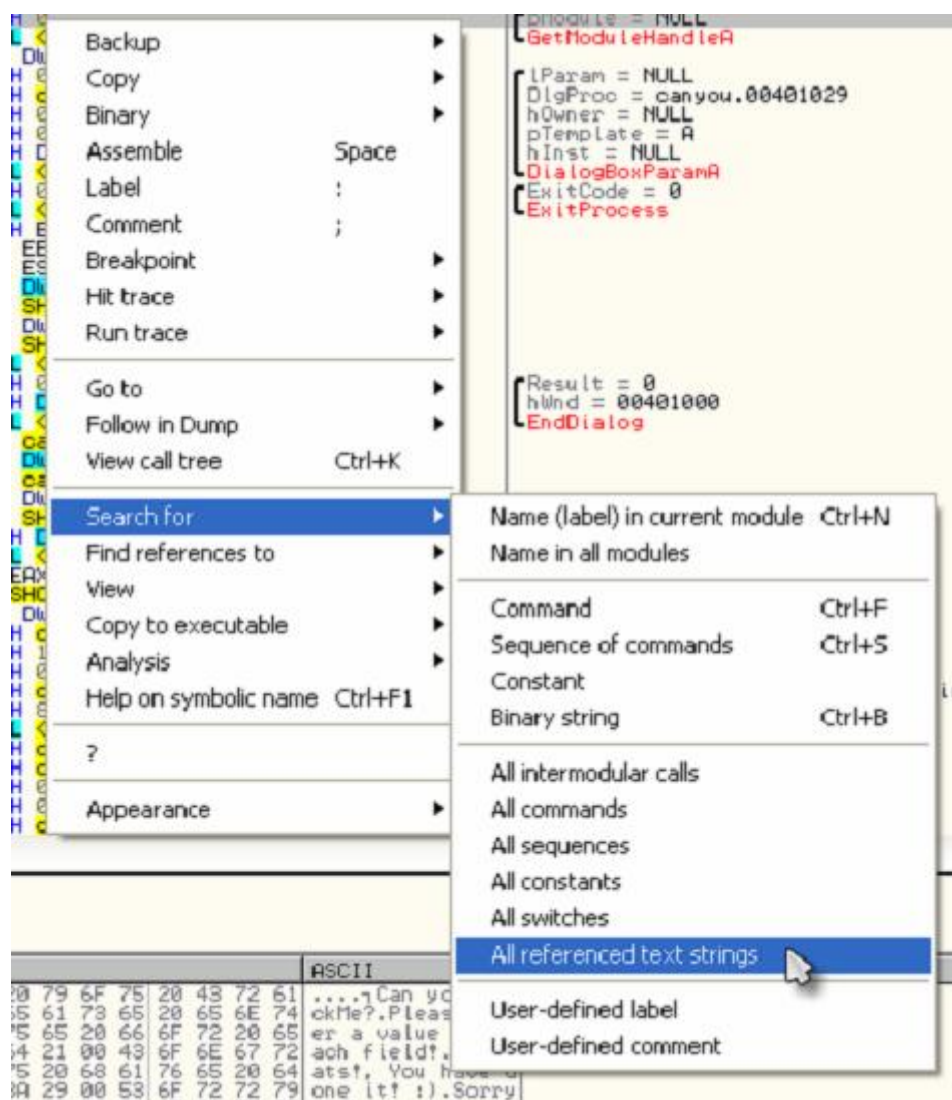
همانطور که قبلا گفتیم، قبل از شروع کردن بهتر است برنامه را واریسی کنیم تا از نحوه ی کارکرد و همینطور نوع حفاظت آن اطلاعاتی بدست بیاوریم :



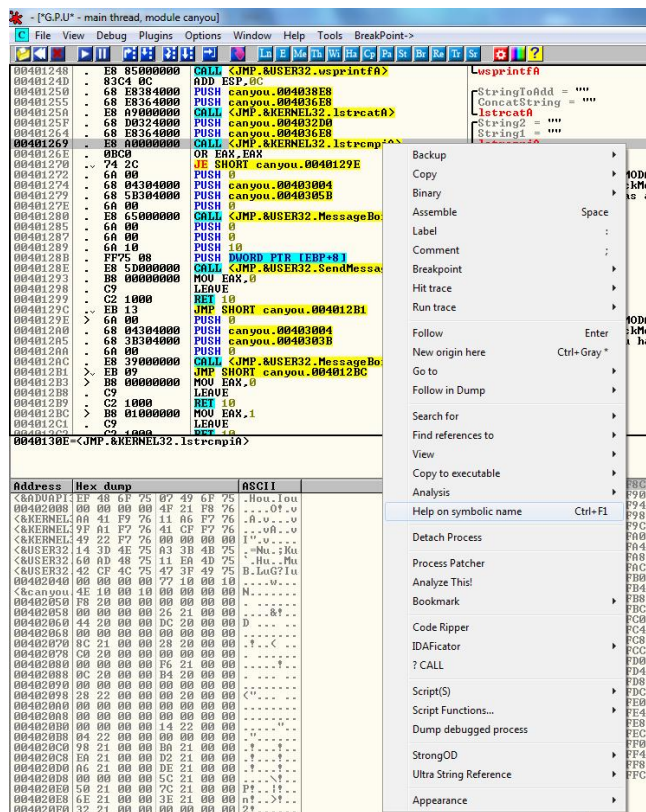
و بعد از وارد کردن اطلاعات داریم :



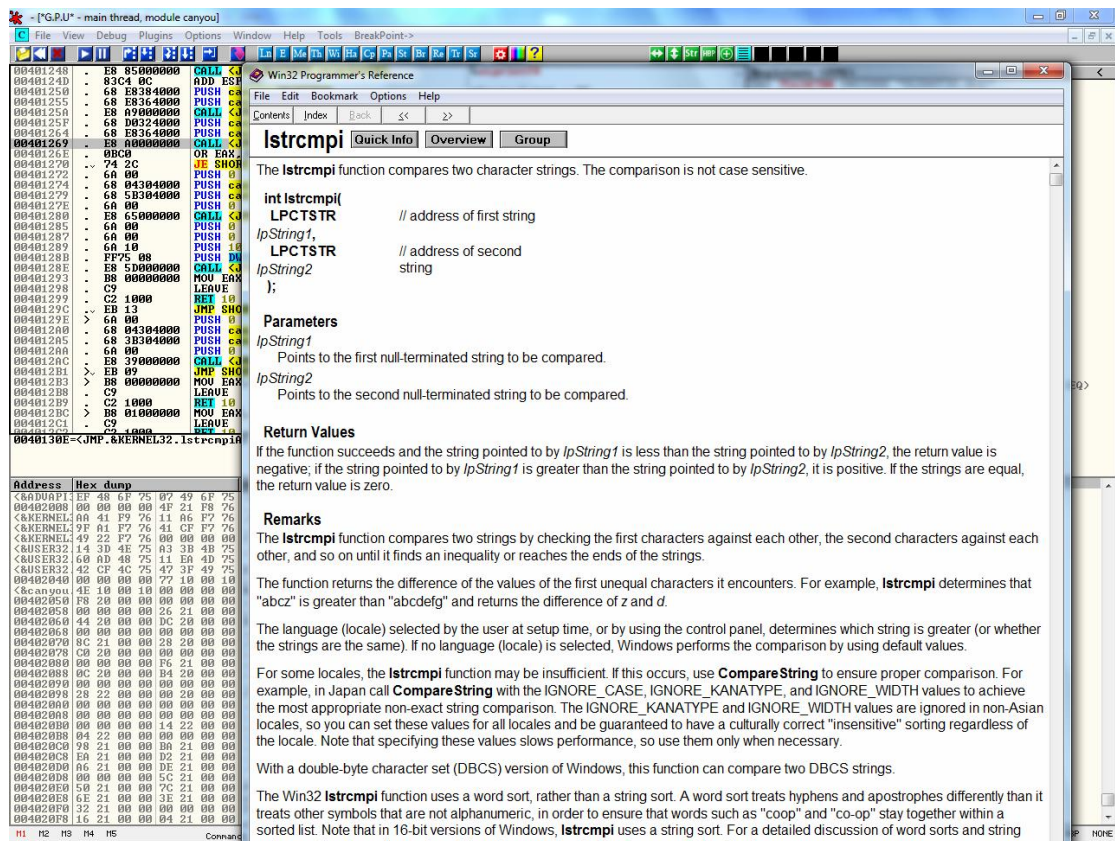
حالا باید حرکت بعدی را فهمیده باشید ،له جستجوی رشته ها:



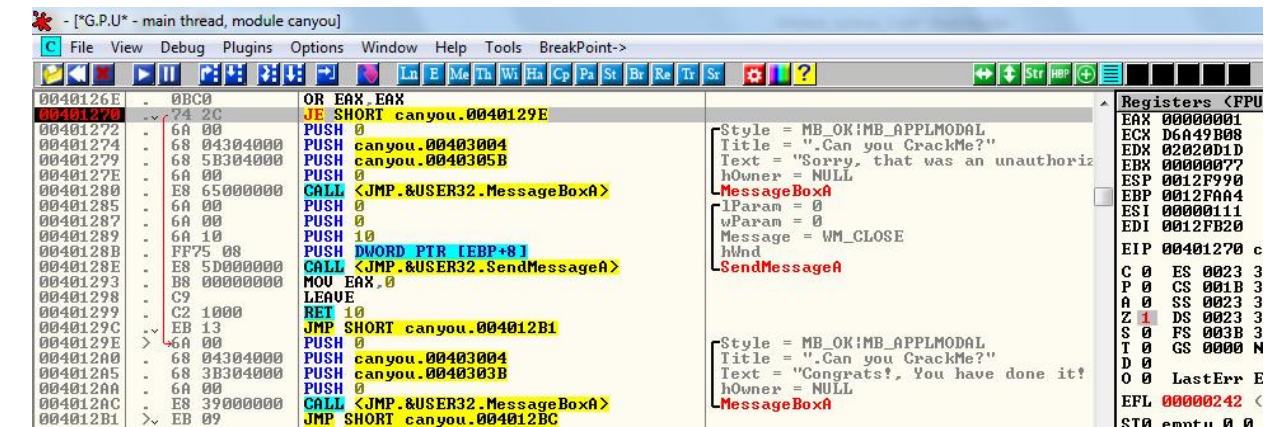
اگر آموزش قبلی را مطالعه کرده باشید ،این شبیه به همان مثال GOODBOY و BAD BOY است ،با همان مقایسه و پرش ،اما قبل از JUMP به فراخوانی Call نگاه کنید که تابع ویندوزی IstrcmpiA را فراخوانی میکند.بروی آم راست کلیک کرده :



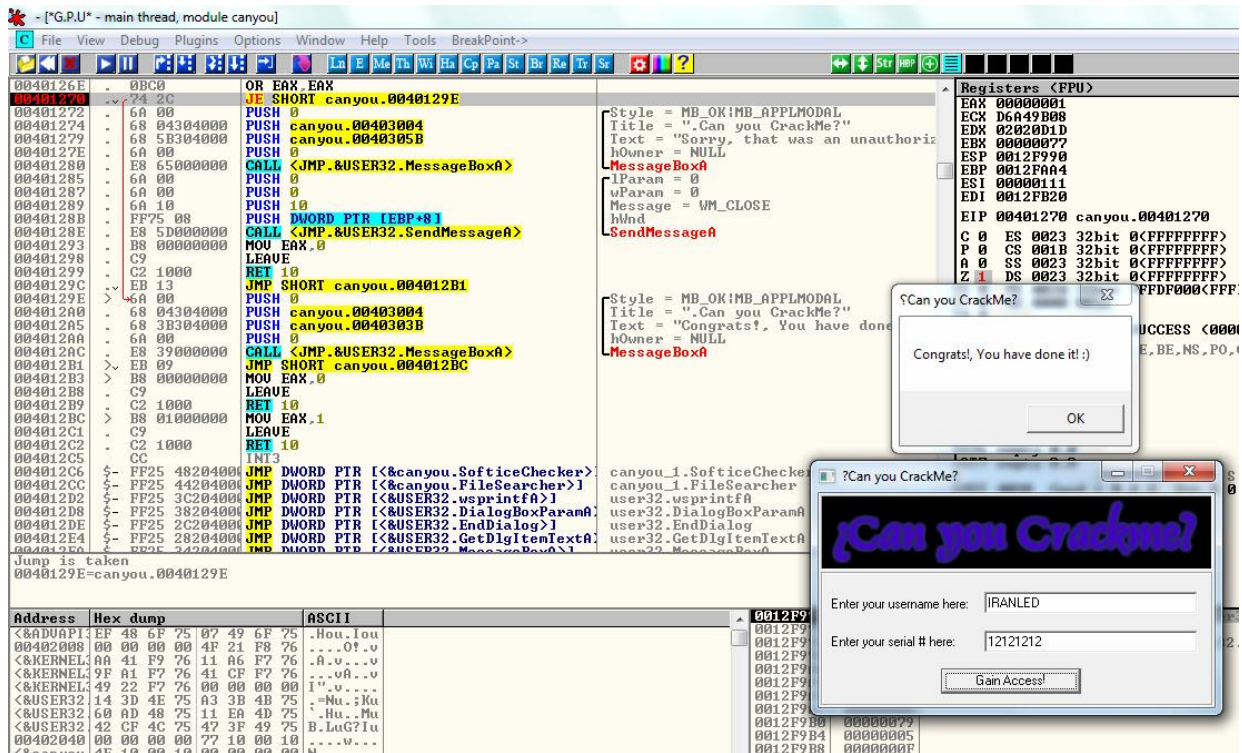
9



همانطور که میبینید این پرش صورت نمی گیرد ، با دبل کلیک کردن بروی پرچم Z مقدار آن را به 1 تغییر دهید :

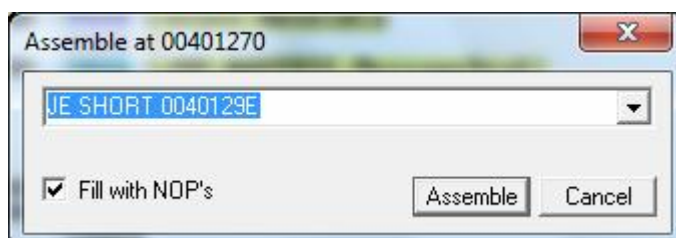


وسپس برنامه را با کلید F9 کامل اجرا کنید :

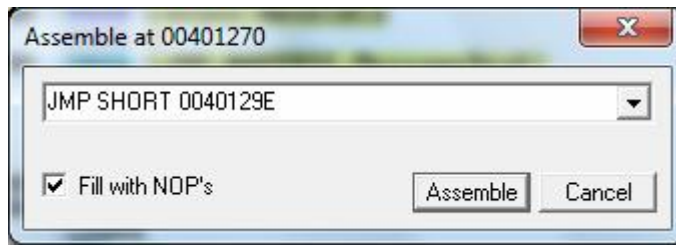


Patch

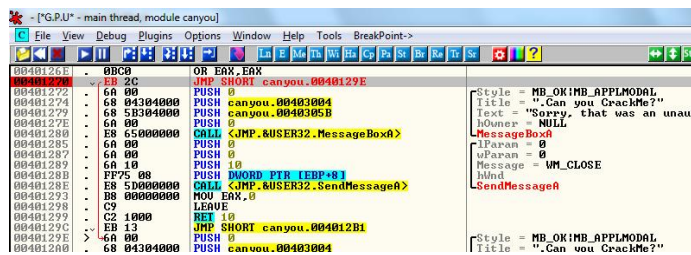
در این قسمت مانند قسمت قبلی میفواهیم تغذیرات را در اعمال کنیم اما این با نه با دستور Nop، دلیل آن هم این است که اگر دستور Nop را جایگزین کنیم برنامه همیشه به قسمت Bad Boy میرود متی با دانستن "یوزرو پسورد" صحیح ☺ ما میفواهیم همیشه برنامه وارد قسمت Good Boy شود برای اینکار بروی دستور عمل JE کلید Space را فشار داده:



و آن را با عبارت JMP تغییر میدهم :

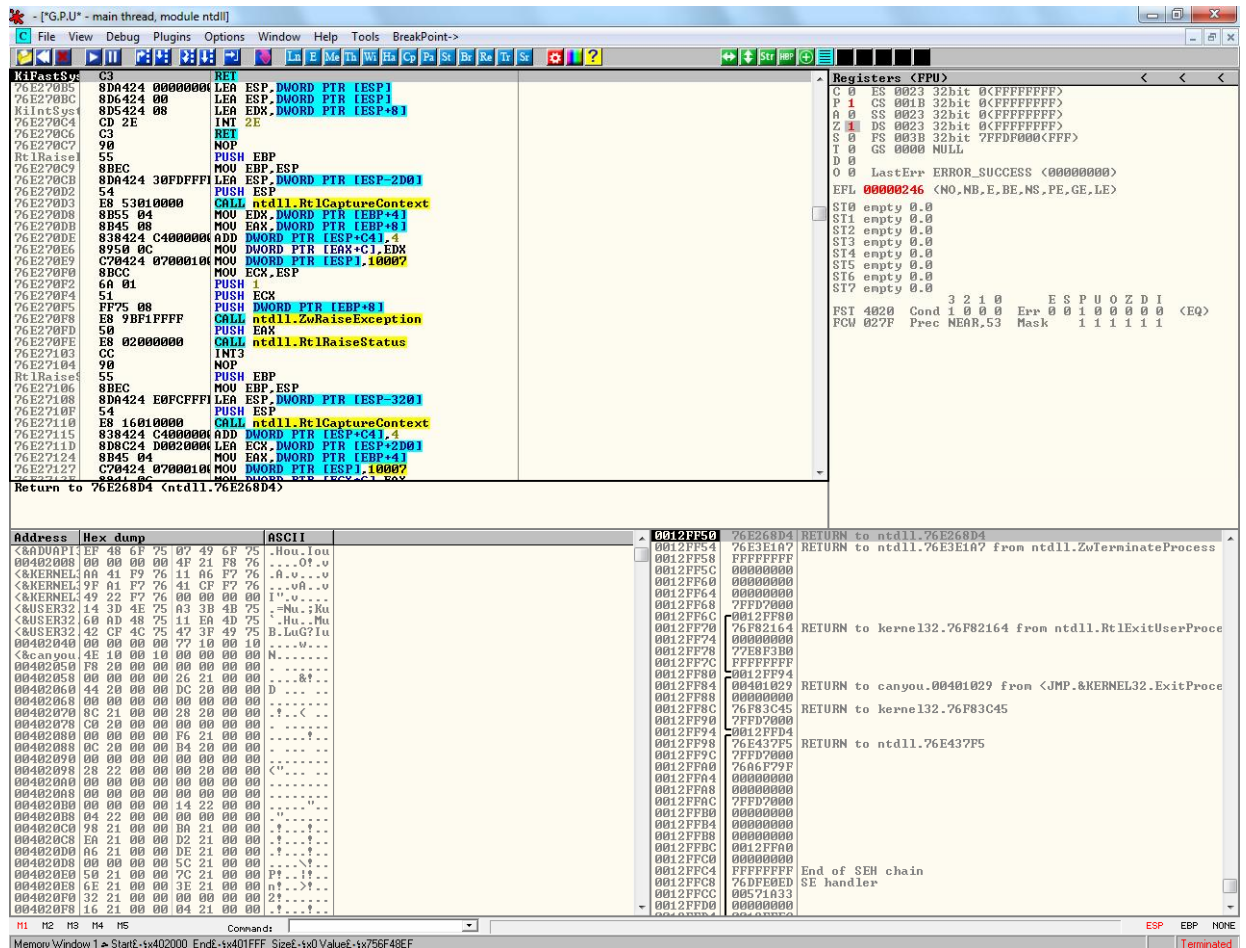


و سپس کلید Assembl را میفشاریم:

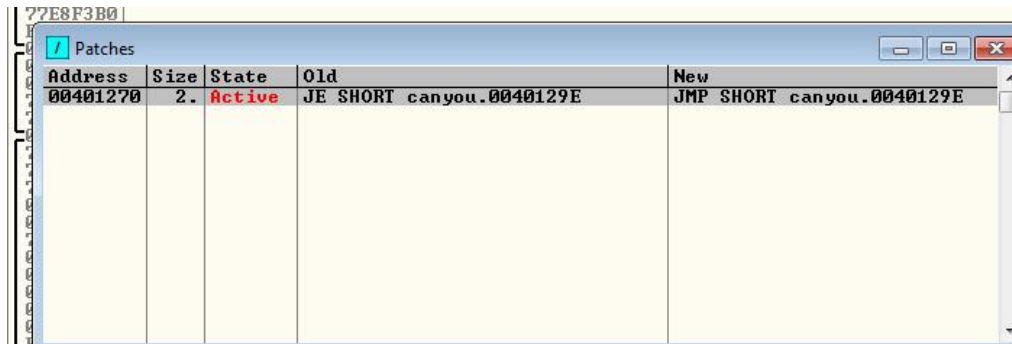


ما درواقع دستور JE به معنی (ببر اگر مساوی است) را با دستور JMP (همیشه ببر) تعویض کرده ایم و برنامه تحت هر شرایطی به قسمت Good Boy میرود ☺

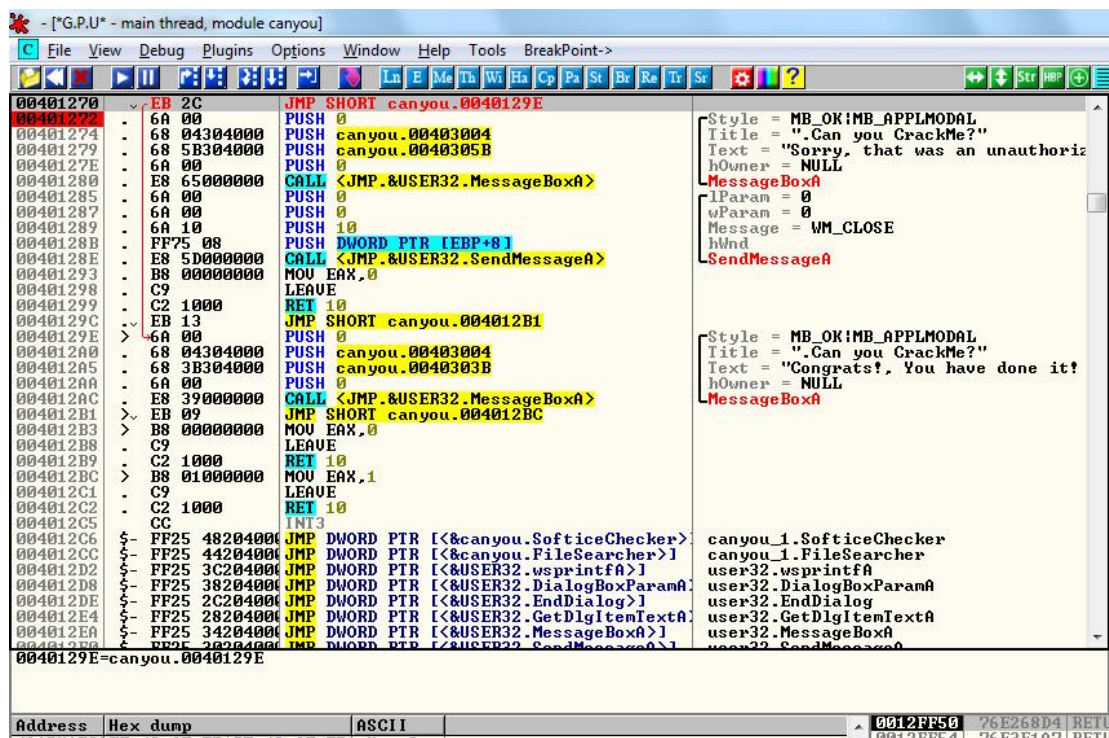
حال نوبت این است که تغییرات را در برنامه ذخیره کنیم، اما قبل از انجام آن میفوام اینبار با استفاده از پنجره ی Patch این کار را انجام دهیم. چگونه؟ باید برنامه را درون ollybinder :



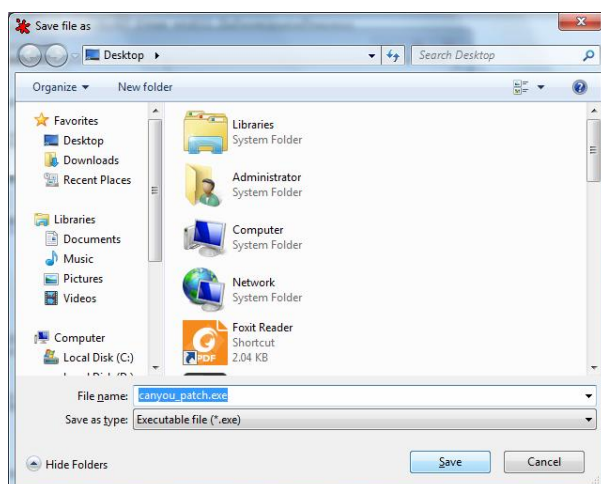
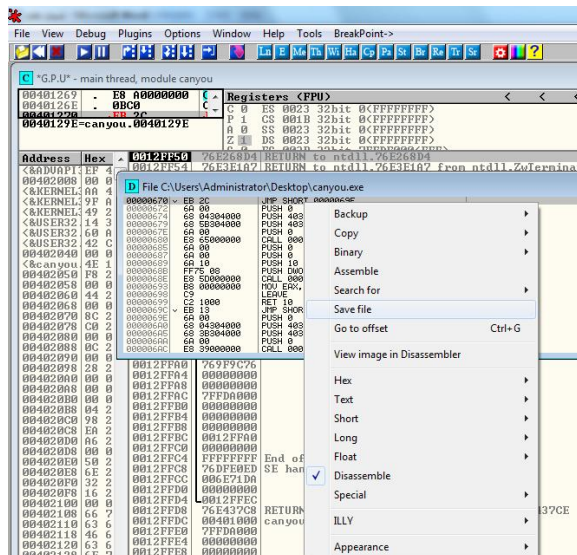
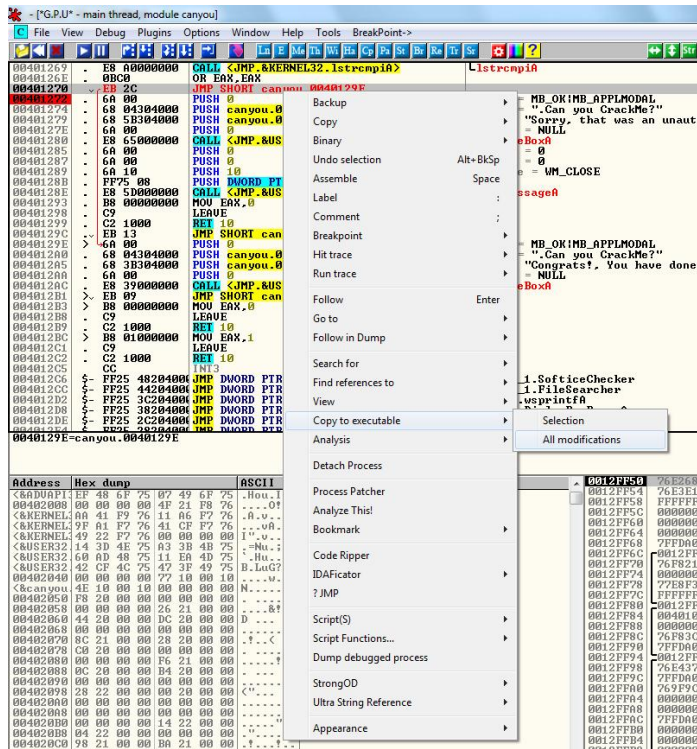
فرض بر این است به هر دلیلی برنامه بعد از انجام کار متوقف شده حال نمیخواهیم دوباره (راند 5) را از پیش بگیریم، پنجره ی Patch را با فشردن کلید Ctrl+P بازکنید:



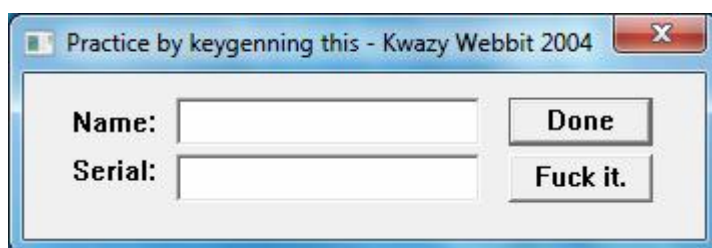
میبینید که تظیری که داده ایم وجود دارد، ولی چون برنامه Terminatted شده قادر نیستیم به برنامه برگردیم مگر ری استارت کنیم، حال بروی دستور العمل در پنجره ی patch دبل کلیک کنید تا به قسمت کد درون برنامه برویم :



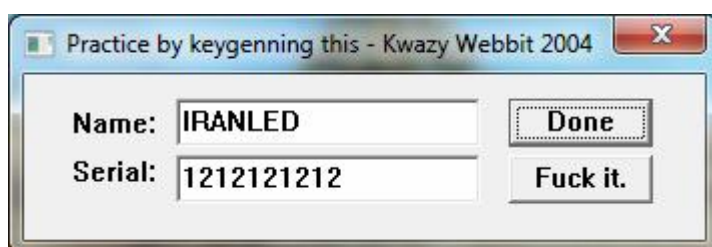
این یکی از قابلیت های ollydbg است ،حال بروی پنجره ی اسمبلی راست کلیک کنید :



برنامه Crackme8.exe ضمیمه شده را اجرا کنید:



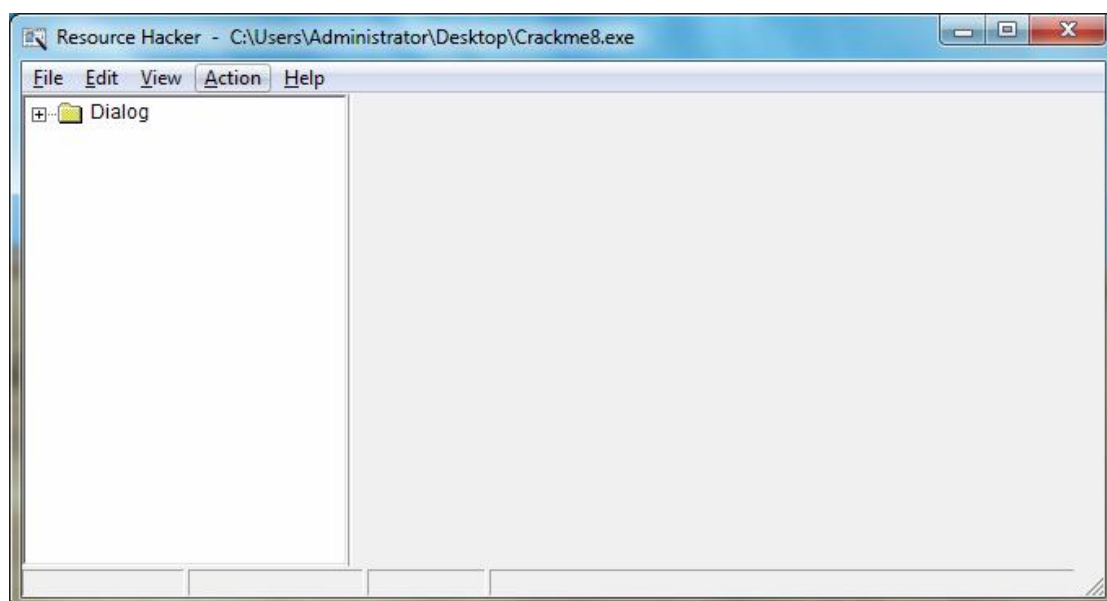
فیلدهای Name و Serial را به دلفواه پر کنید :



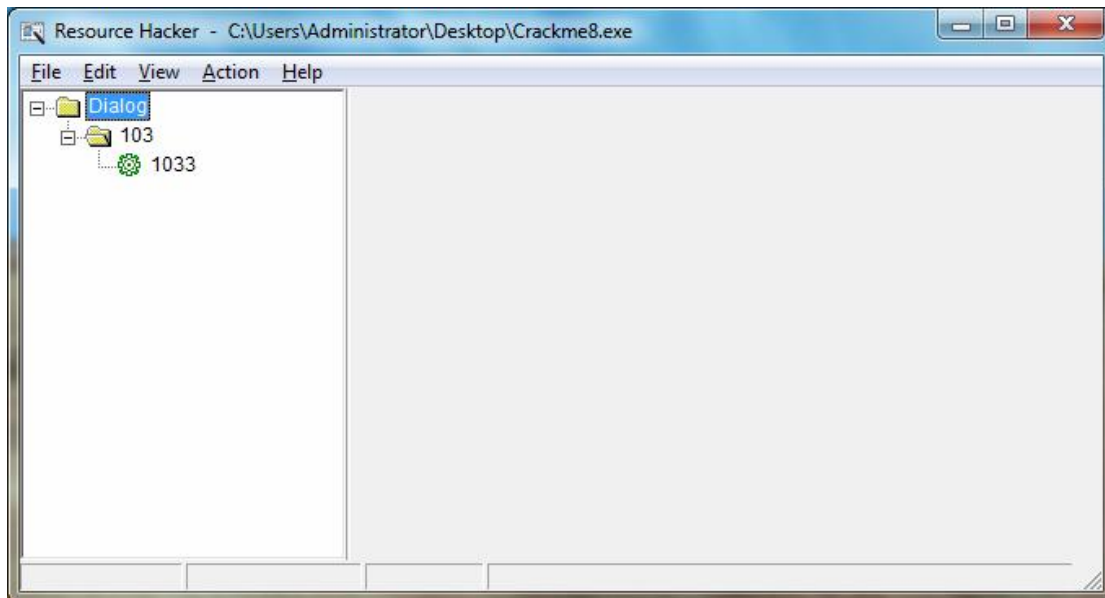
به دکمه ی Done نگاه کنید ،معنی این کلمه معمولا "فروچ" است !! و با کلیک بروی دکمه ی دیگری برنامه فروچ میکند ،حال بهتر نبود بجای Done کلمه ی Enter و FUCK IT کلمه Exit بود؟ بیایید انجامش دهیم

Resource Hacker

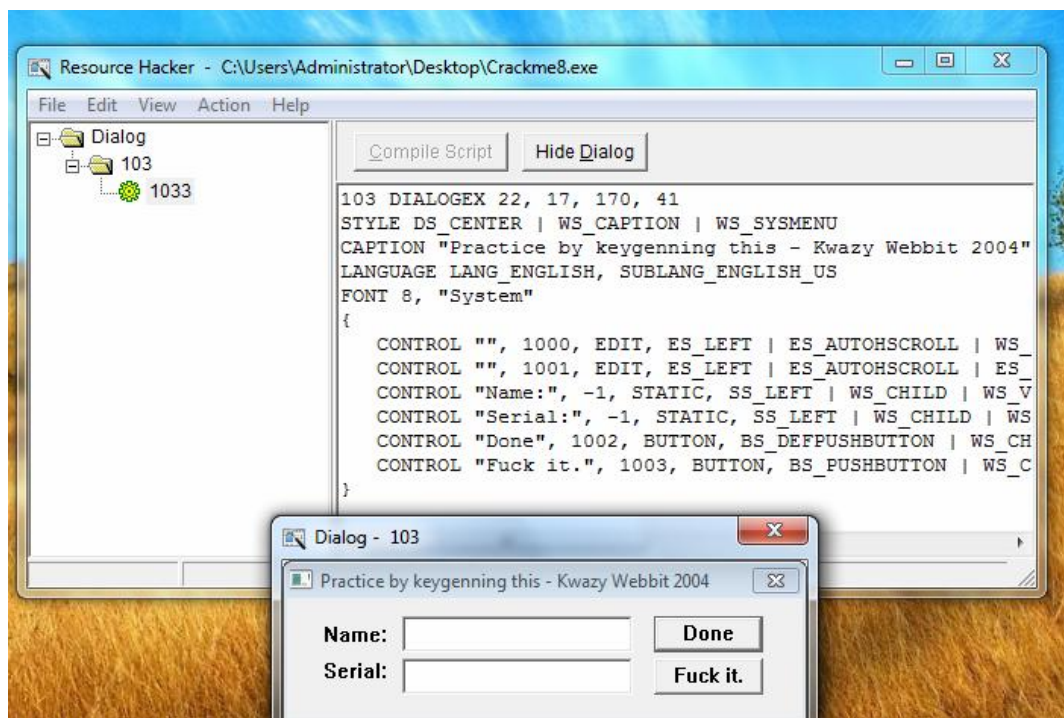
برنامه را اجرا کنید و از منوی File>Open برنامه ی Crackme8.exe را درون آن باز کنید:



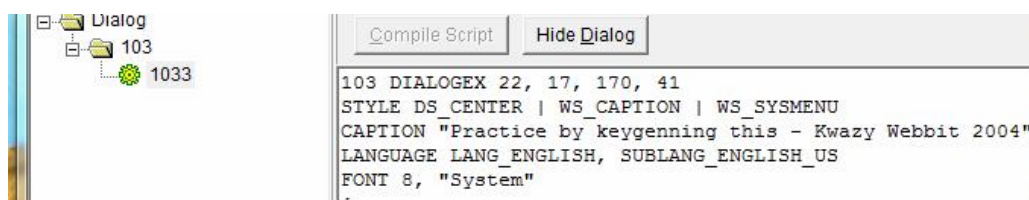
بروی + کلیک کنید و سپس (103) تا گسترش یابد :



حال بروی (103) کلیک کنید ،در پنجره ی سمت راست اطلاعاتی درباره ی پنجره ی برنامه ی Crackme8.exe میبینید :



در قسمت زیر اطلاعاتی درباره ی فونت ،زبان،و همچنین Caption پنجره میتوان دید ،همینطور با فشردن کلید Hide Dialog میتوان نمایش پنجره را مخفی کرد:



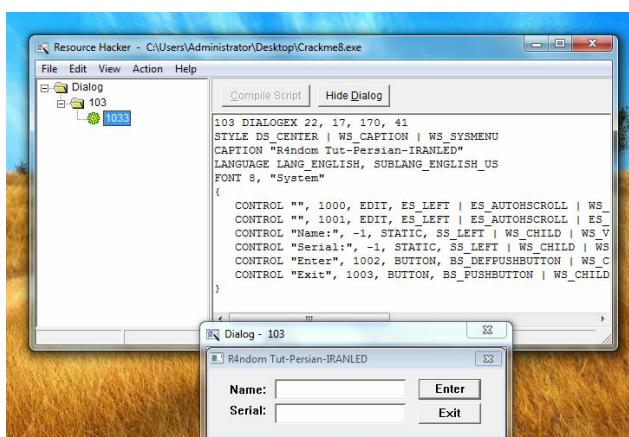
همینطور که در تصویر پائین میبیند تمامی اطلاعات از المان های پنجره قابل رویت است،مانند لیبل Name,Serial و دو دکمه ی Done,Fuck it

```

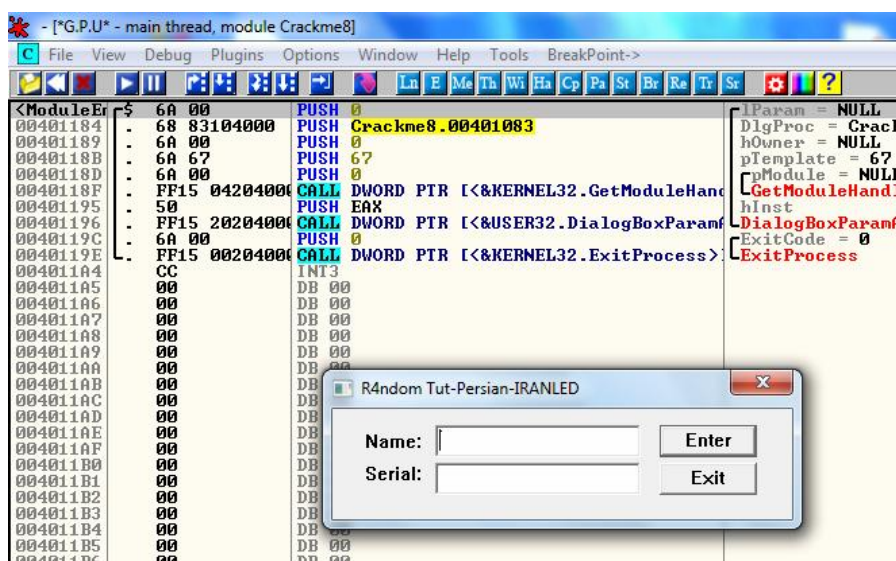
CONTROL "", 1000, EDIT, ES_LEFT | ES_AUTOHSCROLL | WS_
CONTROL "", 1001, EDIT, ES_LEFT | ES_AUTOHSCROLL | ES_
CONTROL "Name:", -1, STATIC, SS_LEFT | WS_CHILD | WS_V
CONTROL "Serial:", -1, STATIC, SS_LEFT | WS_CHILD | WS_
CONTROL "Done", 1002, BUTTON, BS_DEFPUSHBUTTON | WS_CH
CONTROL "Fuck it.", 1003, BUTTON, BS_PUSHBUTTON | WS_C

```

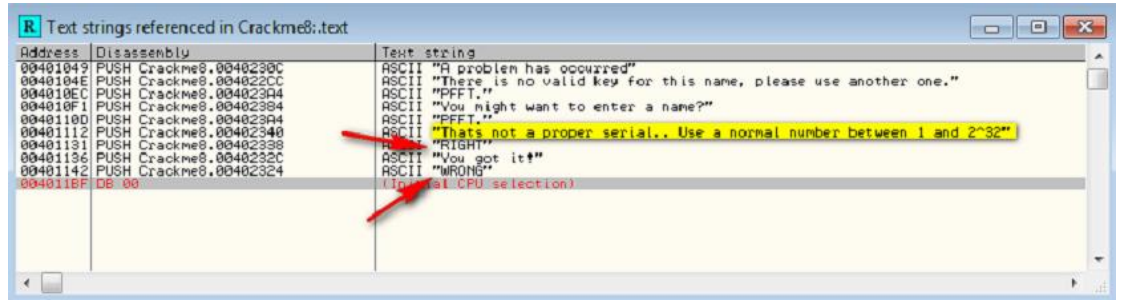
حال متن ها را جایگزین میکنیم و بروی دکمه ی Compile Script کلیک میکنم و نتیجه را ذخیره میکنم :



برنامه را درون Olly باز میکنیم و کلید F9 را میفشاریم :

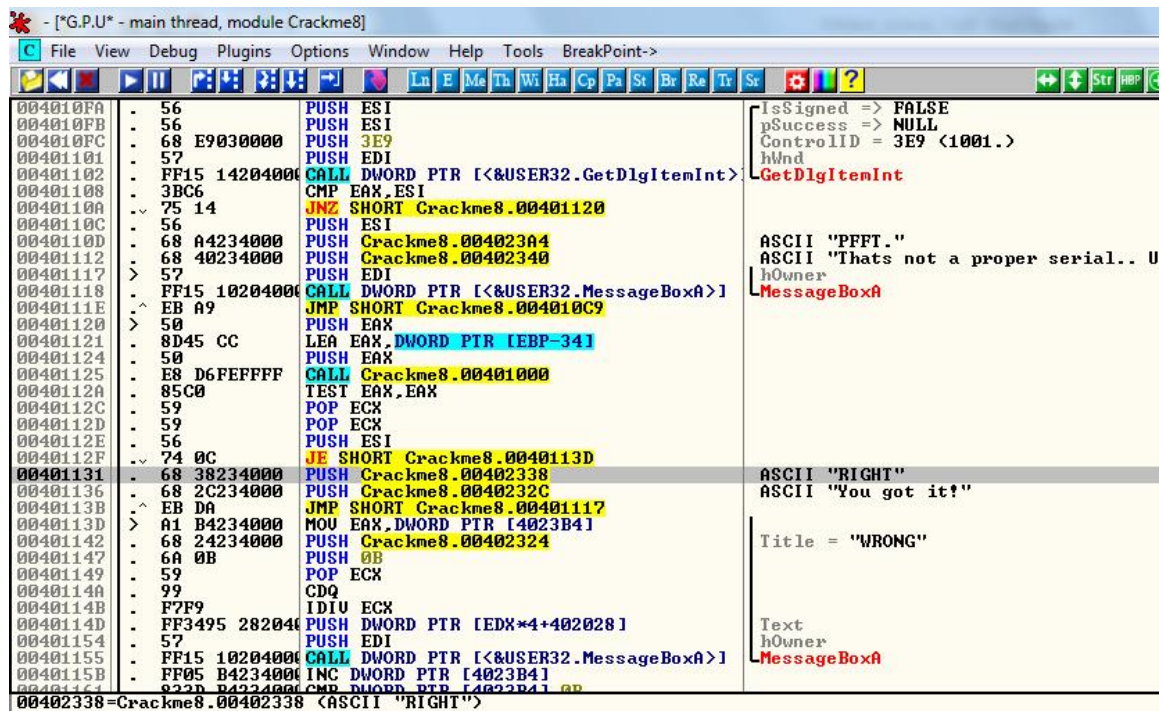


حال رشته های درون برنامه را جستجو میکنم:

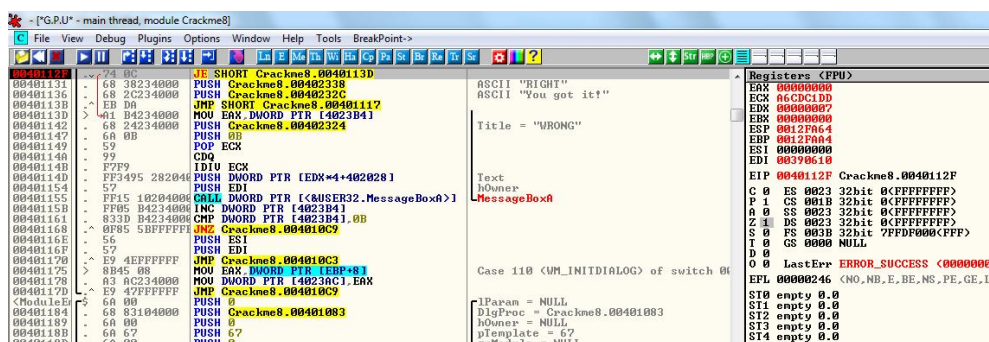


ما دو چیز میدانیم یکی اینکه سریال نامبر باید حاوی اعداد 1,2 باشد و دوم اینکه ما محل Bad Boy و Good Boy را میدانیم ☺
 بیایید به محل Good Boy برویم ،همان(Right)

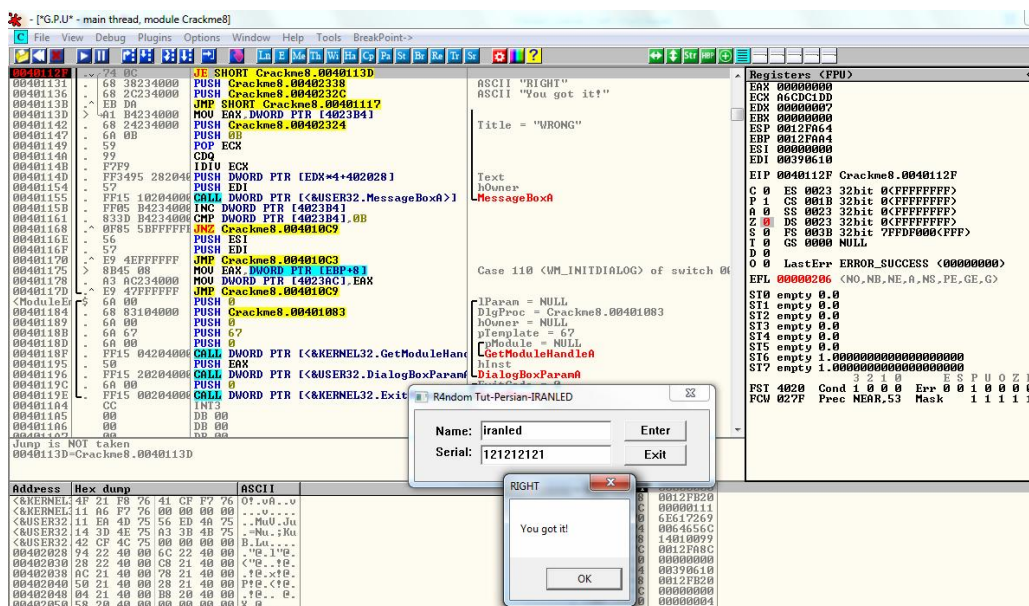
نکته : Good Boy و Bad Boy اشاره به محلی دارد که برنامه پیام را نمایش میدهد ،پیام دلفوا را با اصطلاحا Good Boy و پیام غیر دلفوا را با Bad Boy میشناسیم



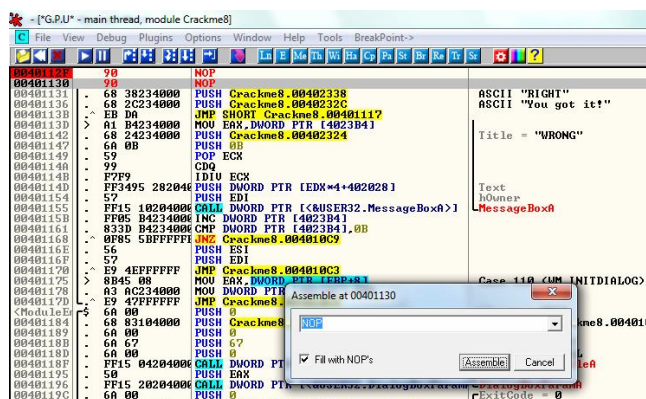
همانطور که میبینید در آدرس 401131 ما روتین Good Boy را داریم و در آدرس 40113D روتین Bad Boy ،و همچنین در آدرس 40112F یک پرش داریم (JE SHORT Crackme8.0040113D) که نتیجه پرش در آدرس 40112A مشخص میشود یعنی دستور: Test EAX,EAX بیایید بروی آدرس 40112F یک BP بگذاریم و برنامه ا سریال و یوزر پر کنیم و نکمه ی Enter را بفشاریم :



طبق آموزش های قبل مقدار پرچم Z را 0 میکنیم :



موفق شدیم ، پس باید این خط هیچ گونه پرشی نداشته باشد که بهترین گزینه Nop است ،روی دستور فوق Space را فشرده و آن را به Nop تغییر دهید و نتیجه را از منوی “All modifications” -> “Save to executable” در فایل ذخیره و ثبت کنید :



نکته ی پایانی :برنامه ی Resource Hacker میتواند تغییرات ظاهری اعم از (strings, icons, labels, buttons, captions) در فایل ها ایجاد کند (در حالت معمول) حتی شما میتوانید دکمه های Olly را برای خودتان سفارشی کنید