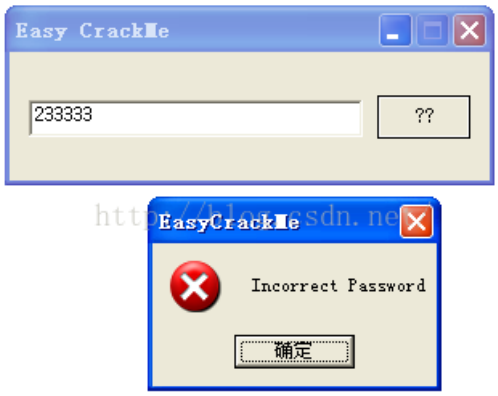
[writeup] reversing.kr - Easy Crack

原创

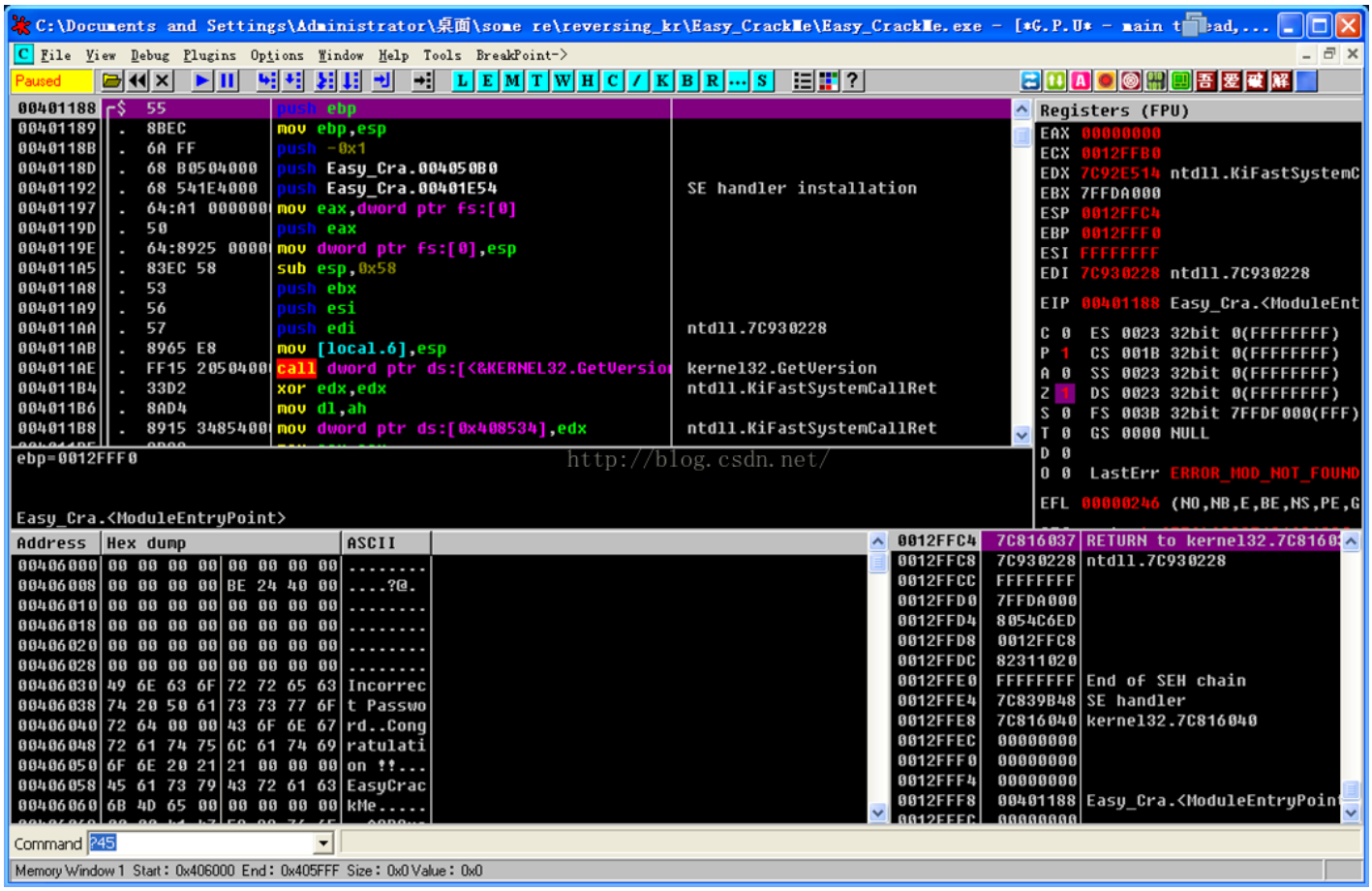
hellotaqini 于 2016-03-12 16:55:56 发布
分类专栏： ctf 文章标签： 逆向 reversing.kr

最近在学习二进制，本文的例子是reversing.kr的Easy Crack，因为之前没写过博客，所以先拿一个简单的题目练练手。。

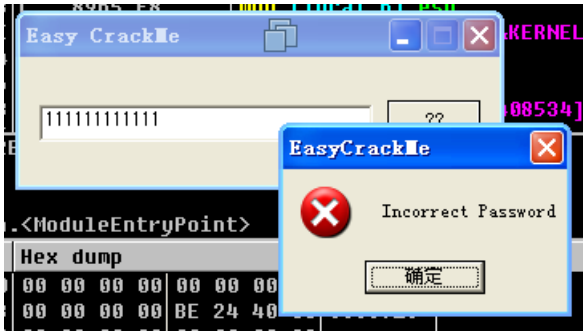
首先运行程序，发现有一个输入框，一个按钮，输入的内容应该就是最后的答案。



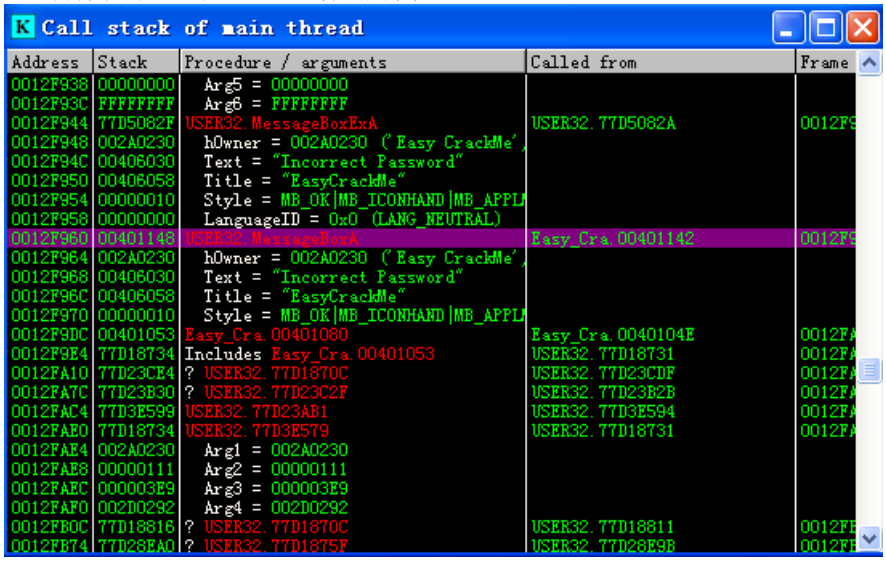
因为是easycrack，所以应该没加壳，直接ollydbg载入，程序停到了入口点，确实没有加壳



接着F9运行程序，随便输入一串字符，点击按钮，程序跳出了密码错误的提示窗

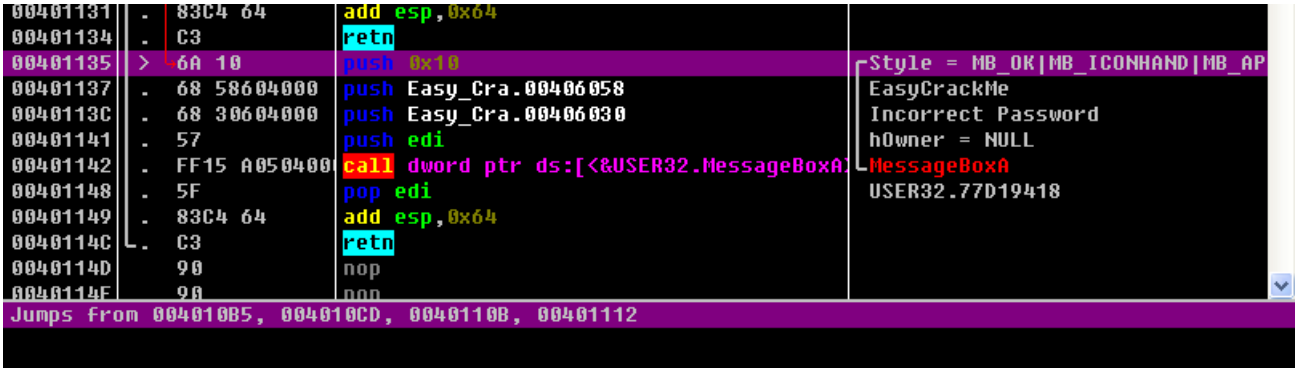


F12暂停程序，然后Alt+K查看调用栈



在MessageBoxA处右键show call，定位到了弹窗所在的程序段

发现一共有四个判断会跳转至密码错误，分别是4010B5，4010CD，40110B，401112

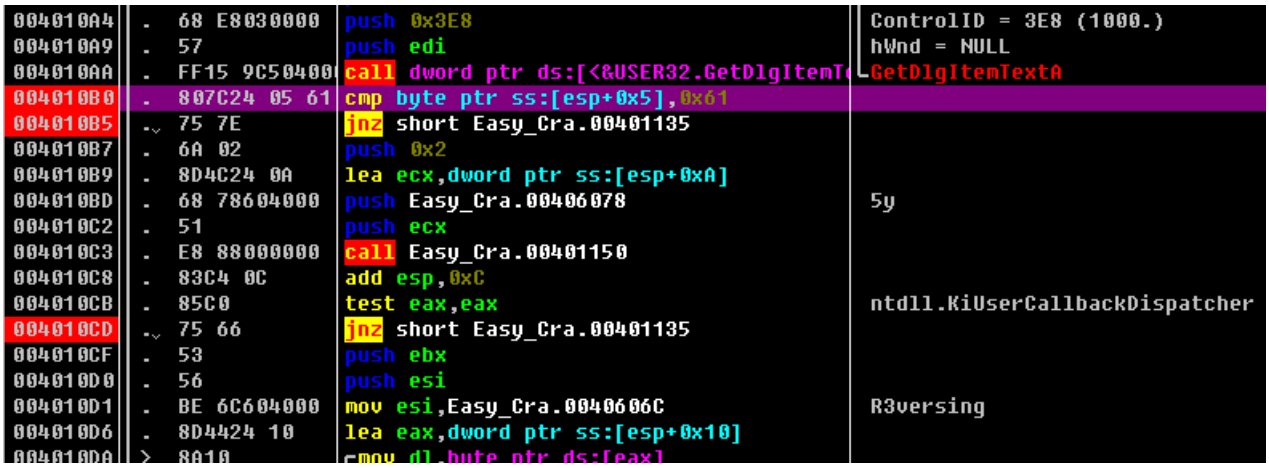


在这四处下断点，再往上看，发现读取输入文本的GetDlgItemTextA，GetDlgItemTextA和第一个跳转之间有一个字符比较的指令，也下个断点

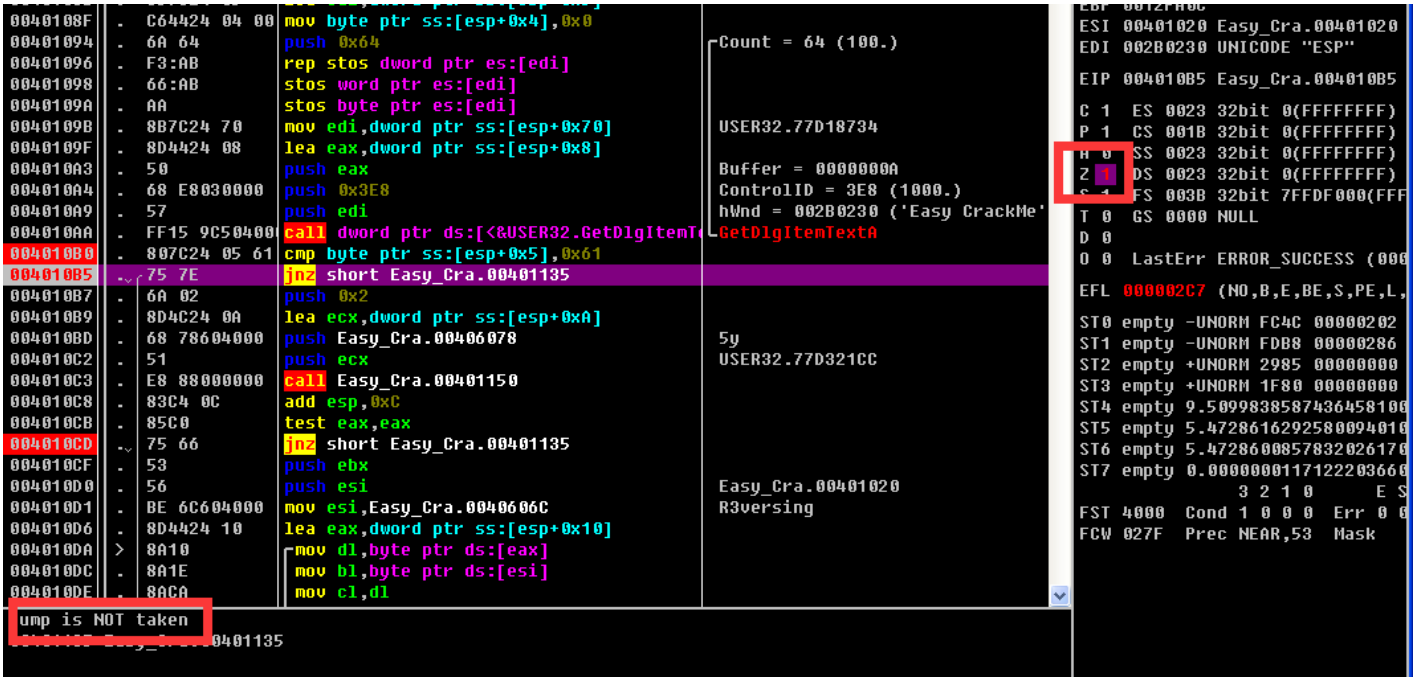
重新载入程序，运行，

这次输入1234567890，然后点击按钮，程序停到了第一个断点处，

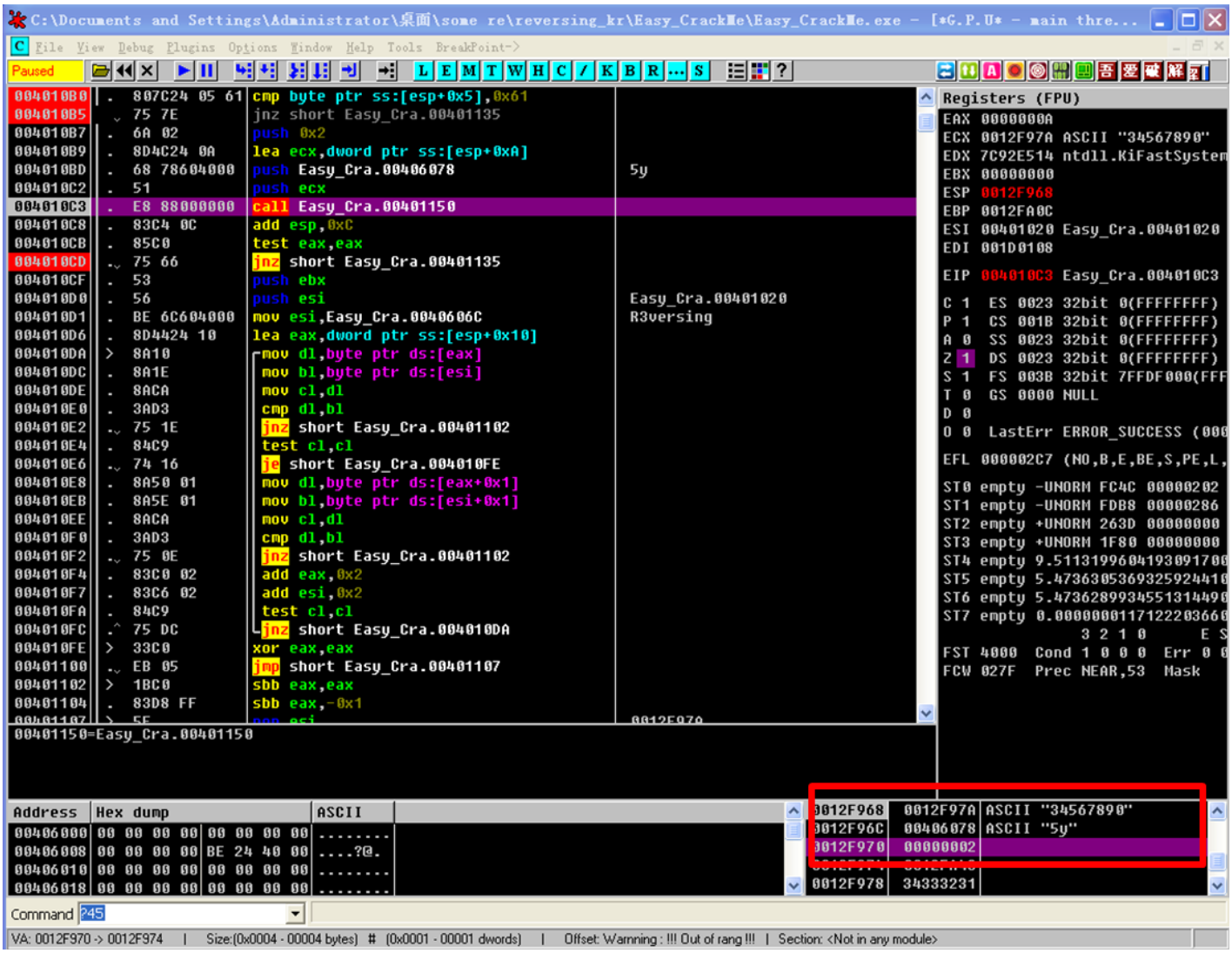
此时进行比较的是输入的第二位'2'和'a'（ASCII=0x61）



F8单步执行程序，遇到跳转时，把Z标志位置1，让跳转不发生，程序进行后续的字符比较

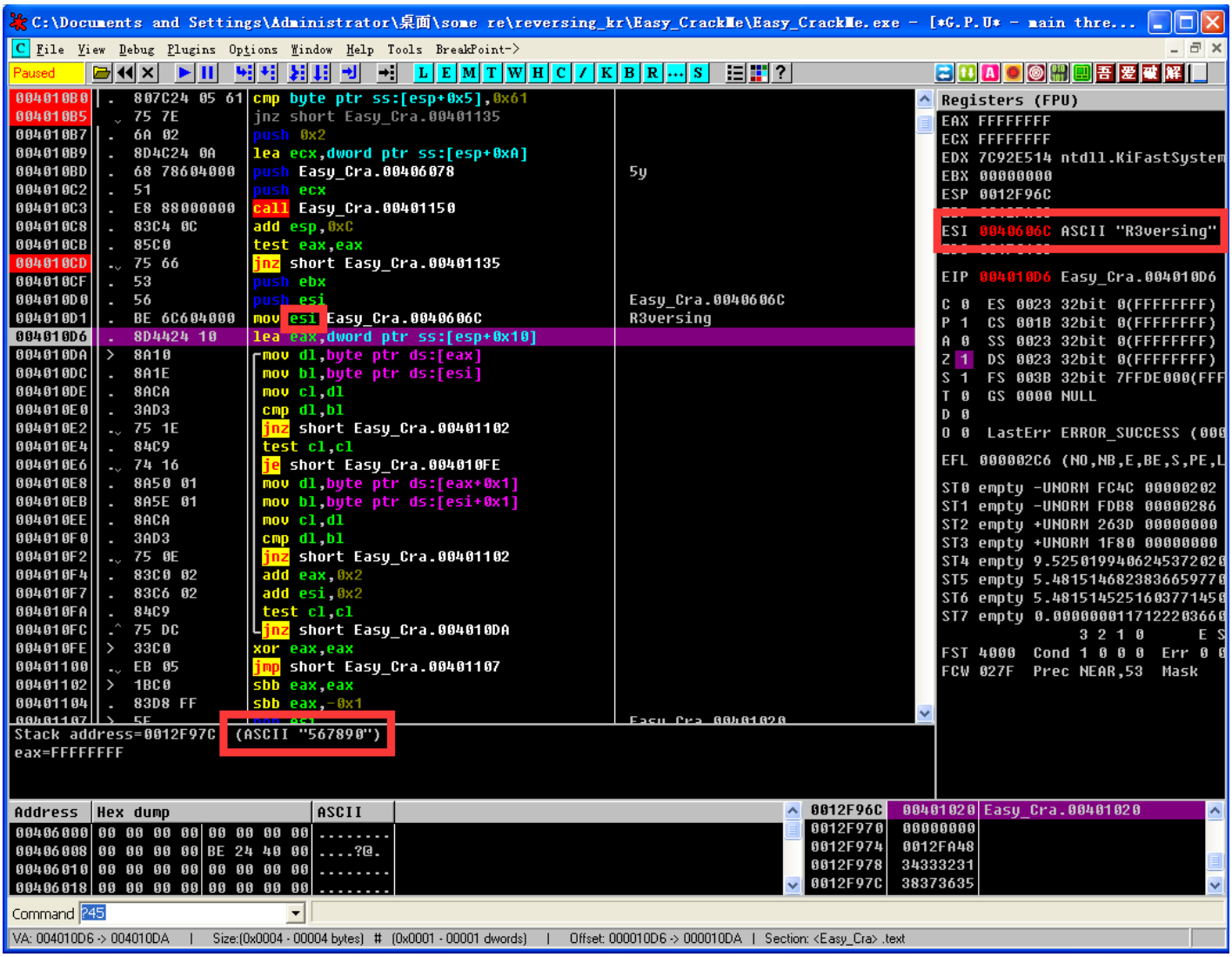


观察堆栈，这时是'34'和'5y'的比较

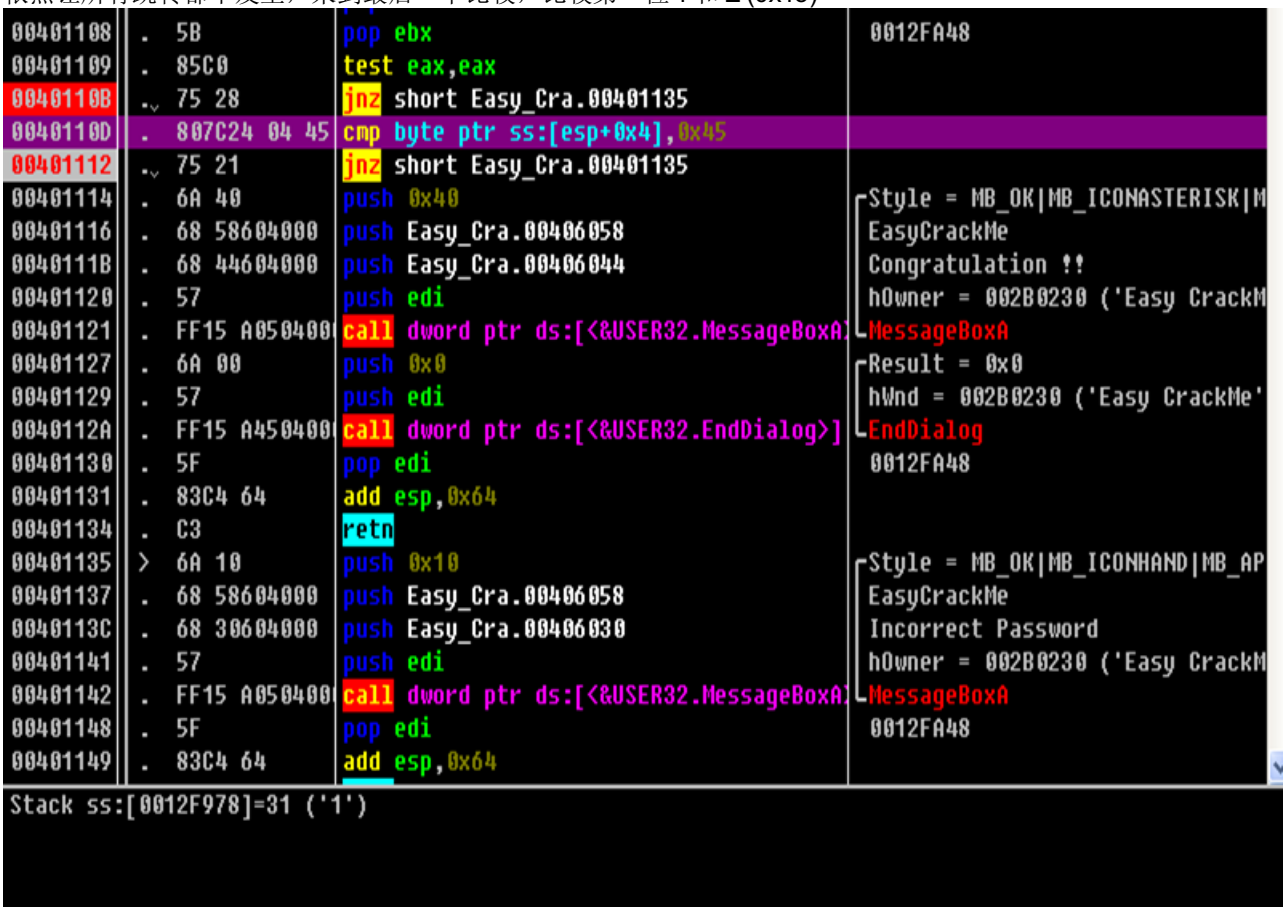


遇到跳转时，把Z置1，让跳转不发生，

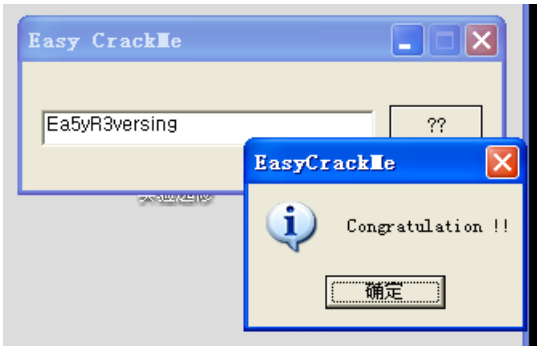
接下来的是比较'567890'和'R3versing'，对应的是密码的5到13位



依然让所有跳转都不发生，来到最后一个比较，比较第一位'1'和'E'(0x45)



于是得出密码第2位是a，3到4位是5y，5到13位是R3versing，第一位是E


Easy CrackMe
Ea5yR3versing
??
EasyCrackMe
Congratulation !!
确定