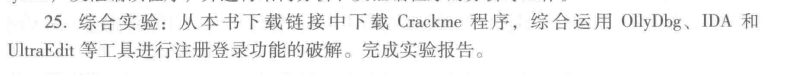
## 选取题目：

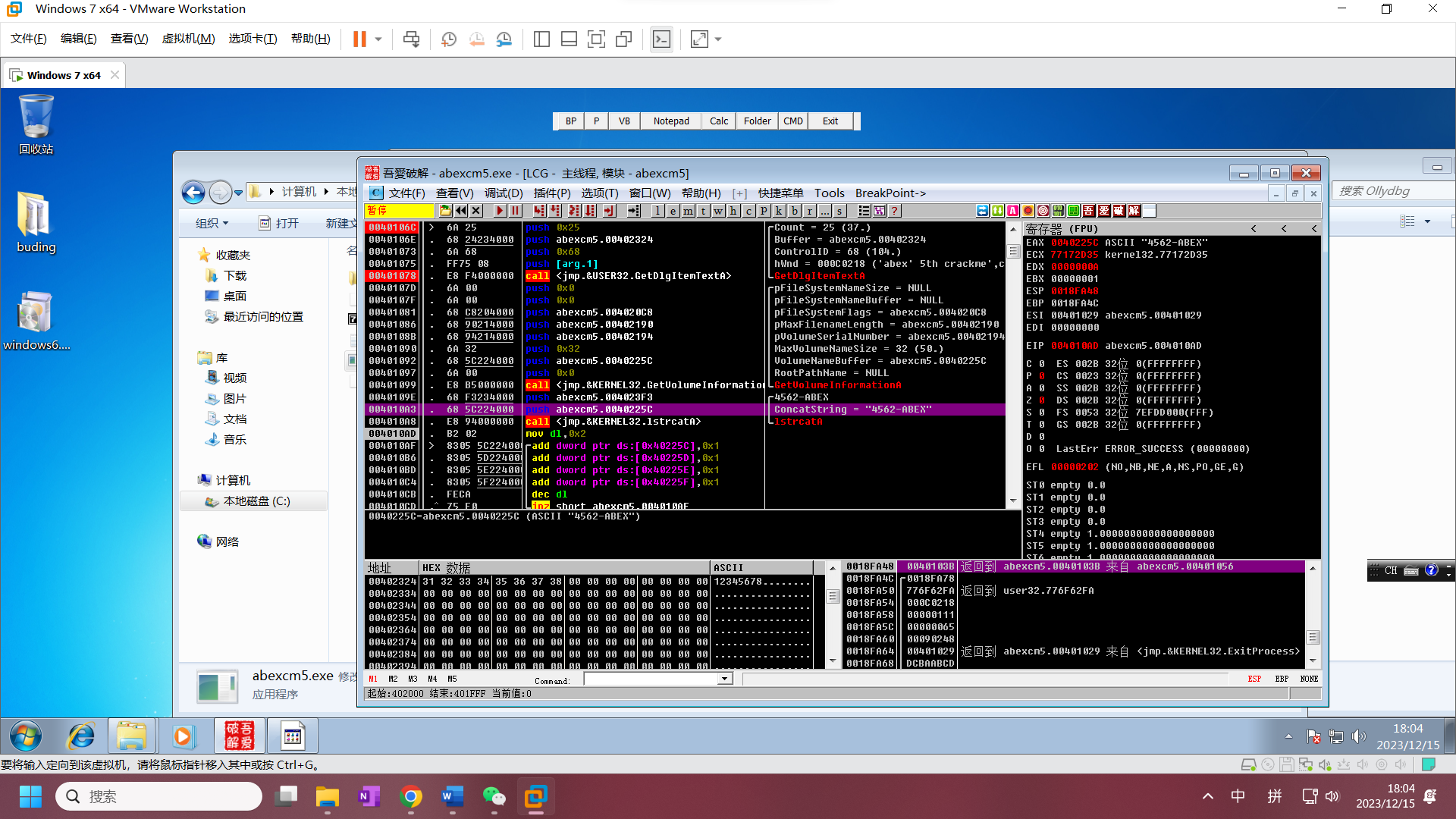
P304 25



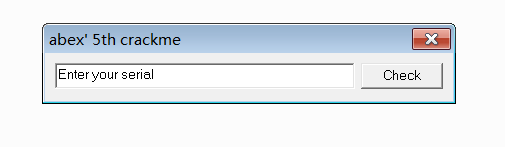
## 软件安装：

没找到题目中说的crackme下载链接，从网上下载了一个crackme程序，由于本机下载类似文件安全中心一直报危险提醒，所以新建一个windows7虚拟机上完成程序的运行和破解

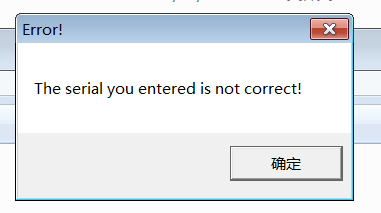
环境：



Crackme程序：



错误提示界面：

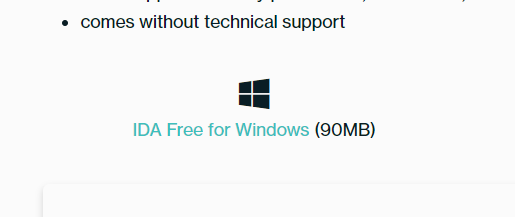


Ollydbg下载：

使用的是国内吾爱破解的版本

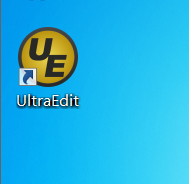


Ida下载：



官网傻瓜式下载即可

Ultraedit：

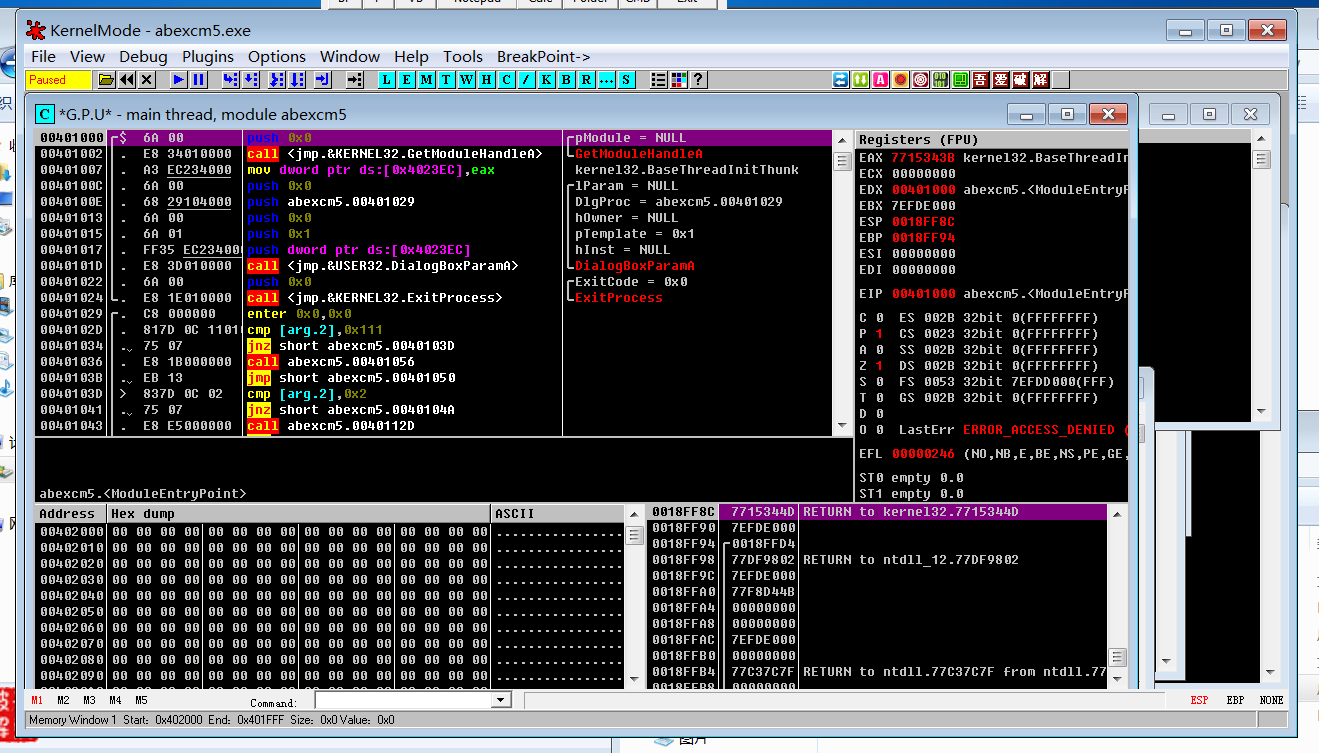


也是官网傻瓜式下载，免费试用三十天

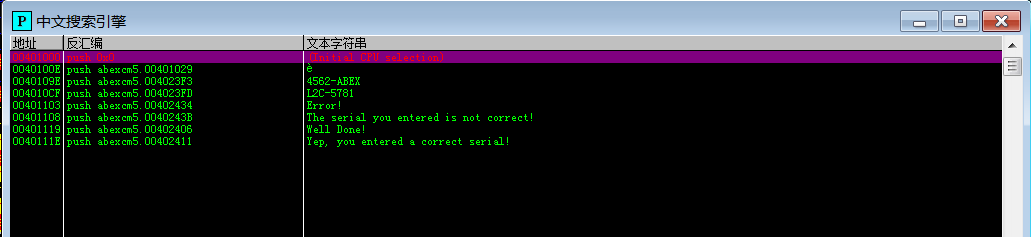
### 分析过程

### Ollydbg

把crackme执行文件拖入ollydbg

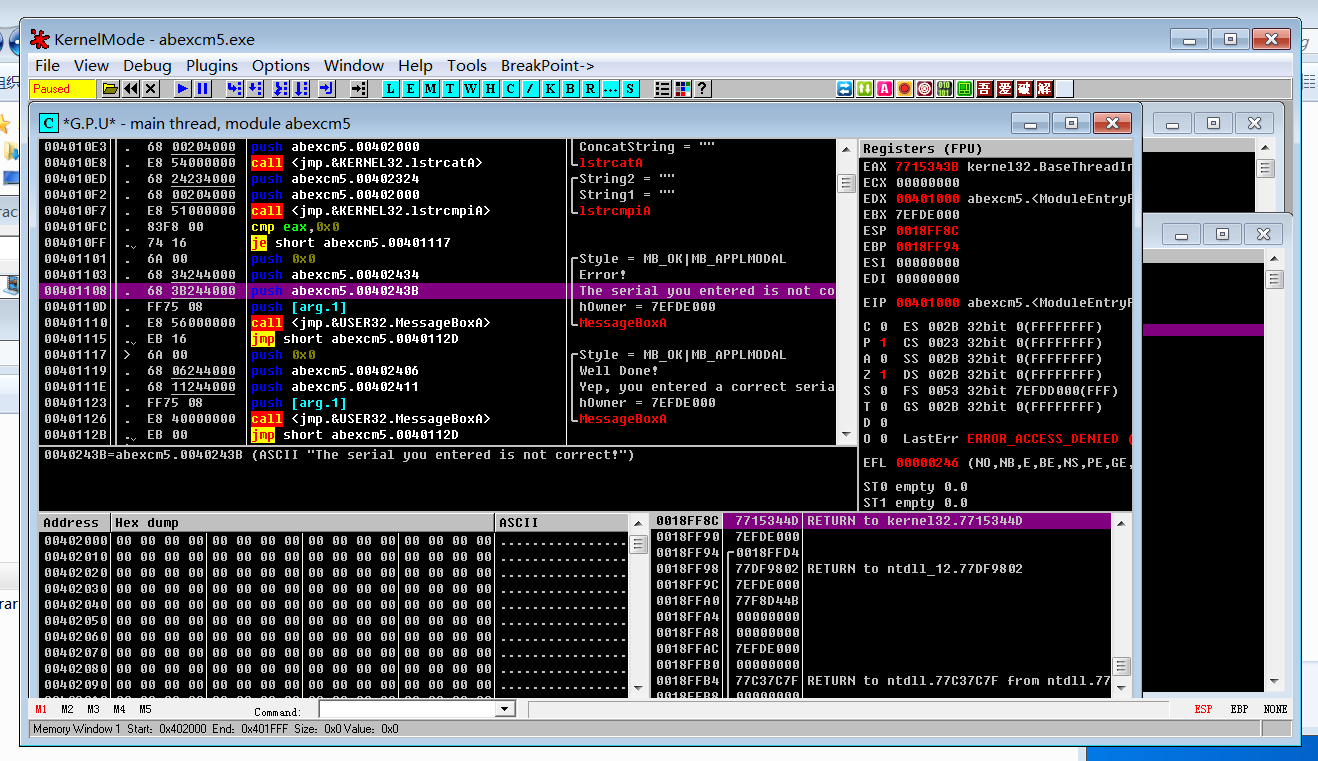


搜索源码中出现的字符串：

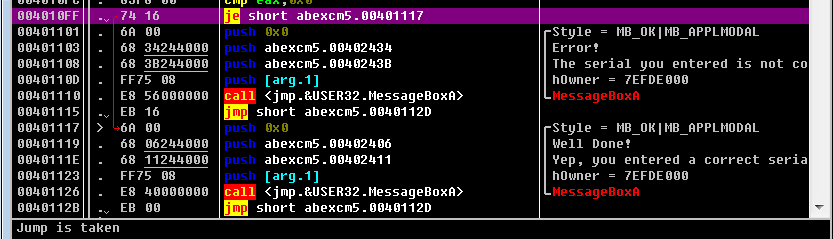


可以看到错误提示的内容，下面的应该是成功时候的提示了

来到出错字符串对应的位置



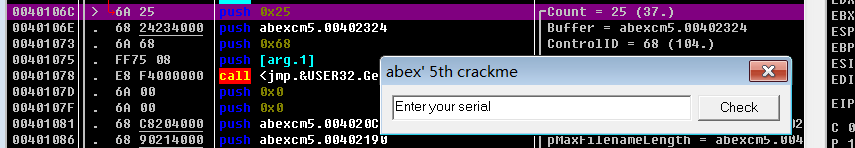
这里有一个跳转和明显的分支，错误正确分别跳转到不同的地方、



这个分支的条件应该就是上一行的eax和0的比较

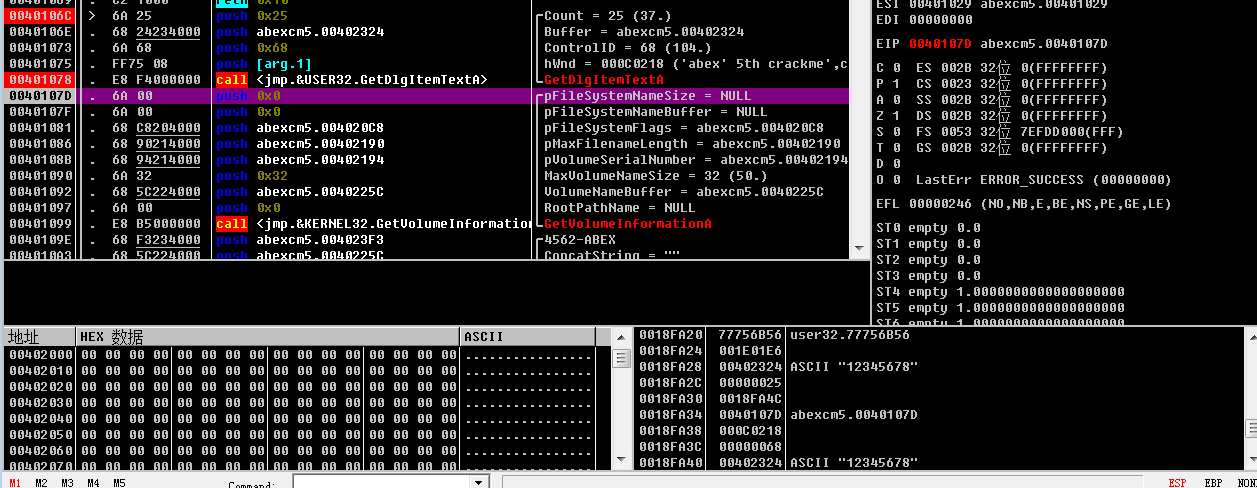


从开头处断点调试



随便输入个12345678，找一下这个输入会到哪

一直单步调试，图里这个GetDlgItemTextA一看就是读取输入内容，继续到下一步看到右下角我们的12345678出来了

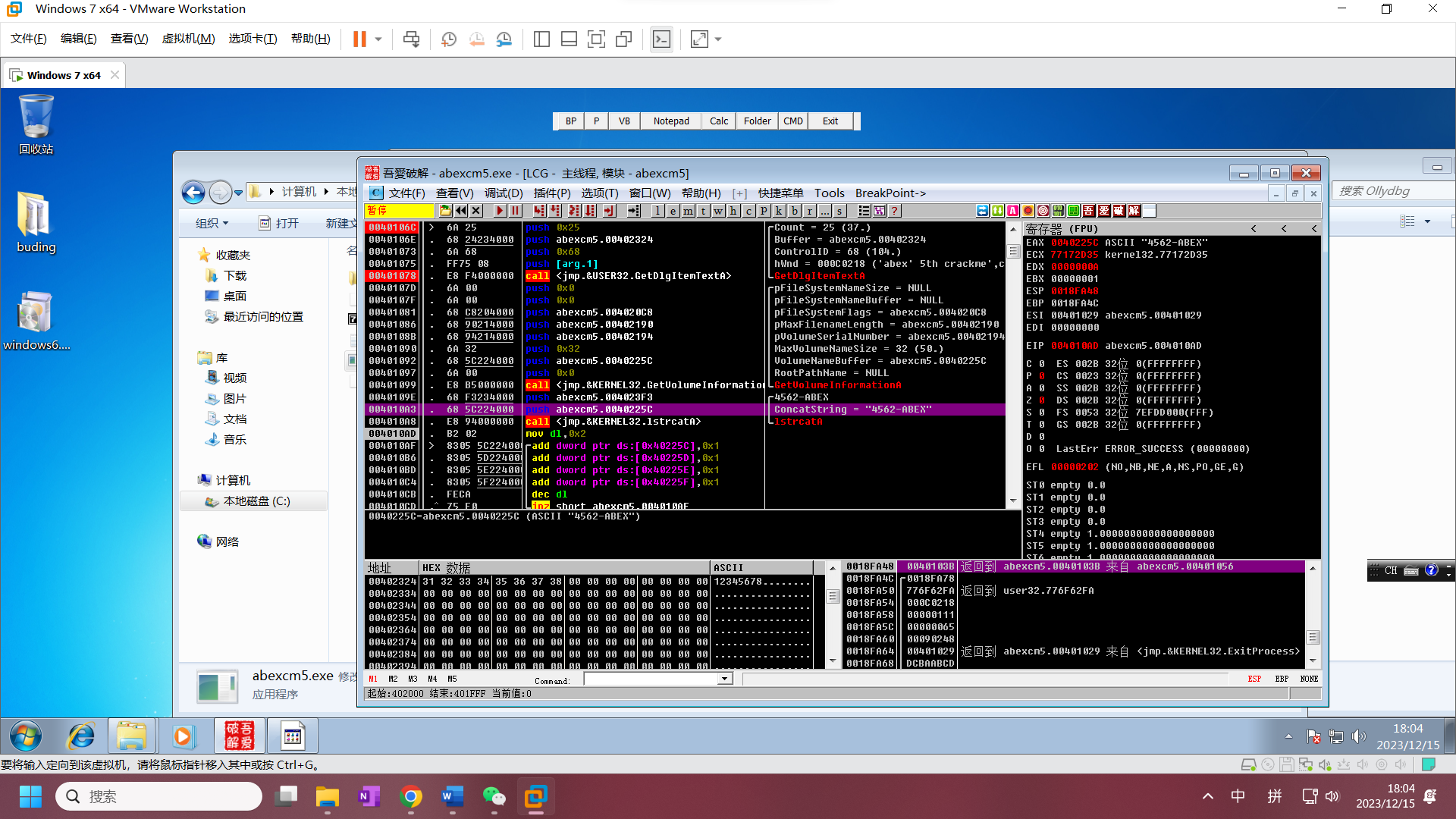


在数据窗口跟随一下这个地址



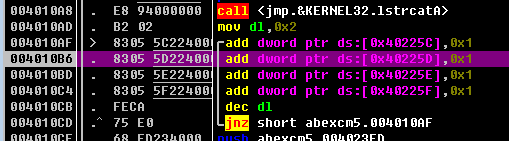
继续调试遇到了下一个函数，叫做GetVolumeInformationA，顾名思义是读取磁盘信息的

但是在我的虚拟机运行时程序好像没有读到磁盘信息，可能是程序只是装作获取了信息没有实际使用，又或者是虚拟机的问题



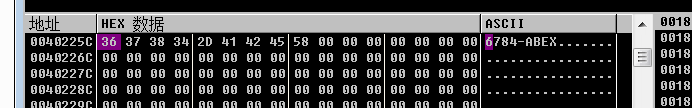


这里的是4562啥玩意的应该是个硬编码，可能有用，继续往下看看吧

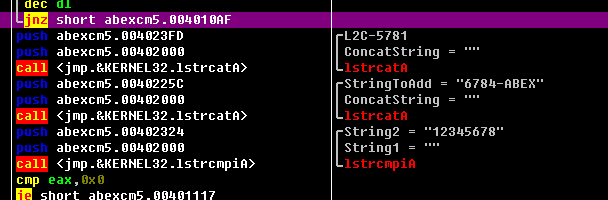


看到这个数据进到了一些add里面，估计对这个数据加加减减应该就是最终的序列号了

一直单步调试到这些加加减减结束（里面是一个两次循环）



下面进行了一系列的字符串合并操作：



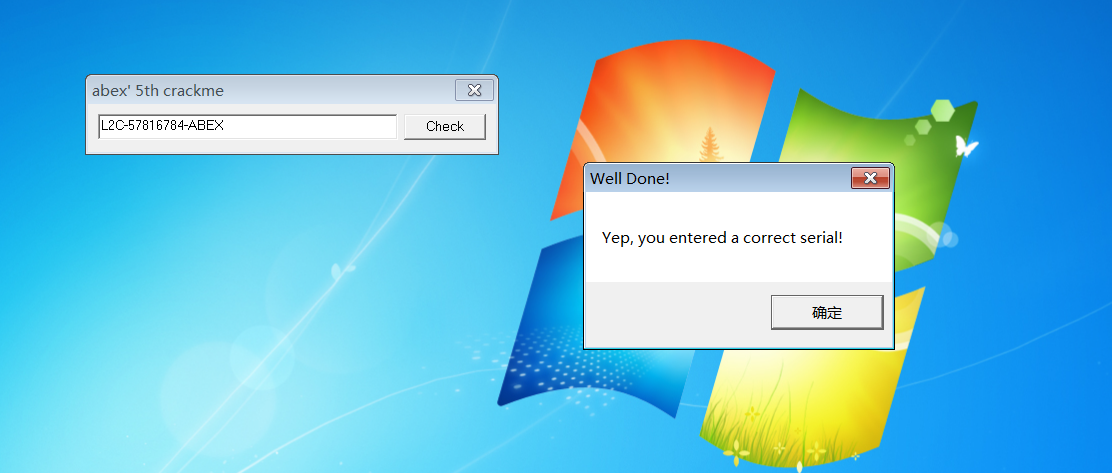
看看最终会变成啥：



最后的得到L2C-57816784-ABEX

再下面就看到一开始分析的eax了，程序基本分析完了

把这个L2C-57816784-ABEX放到crackme里面看看能用不

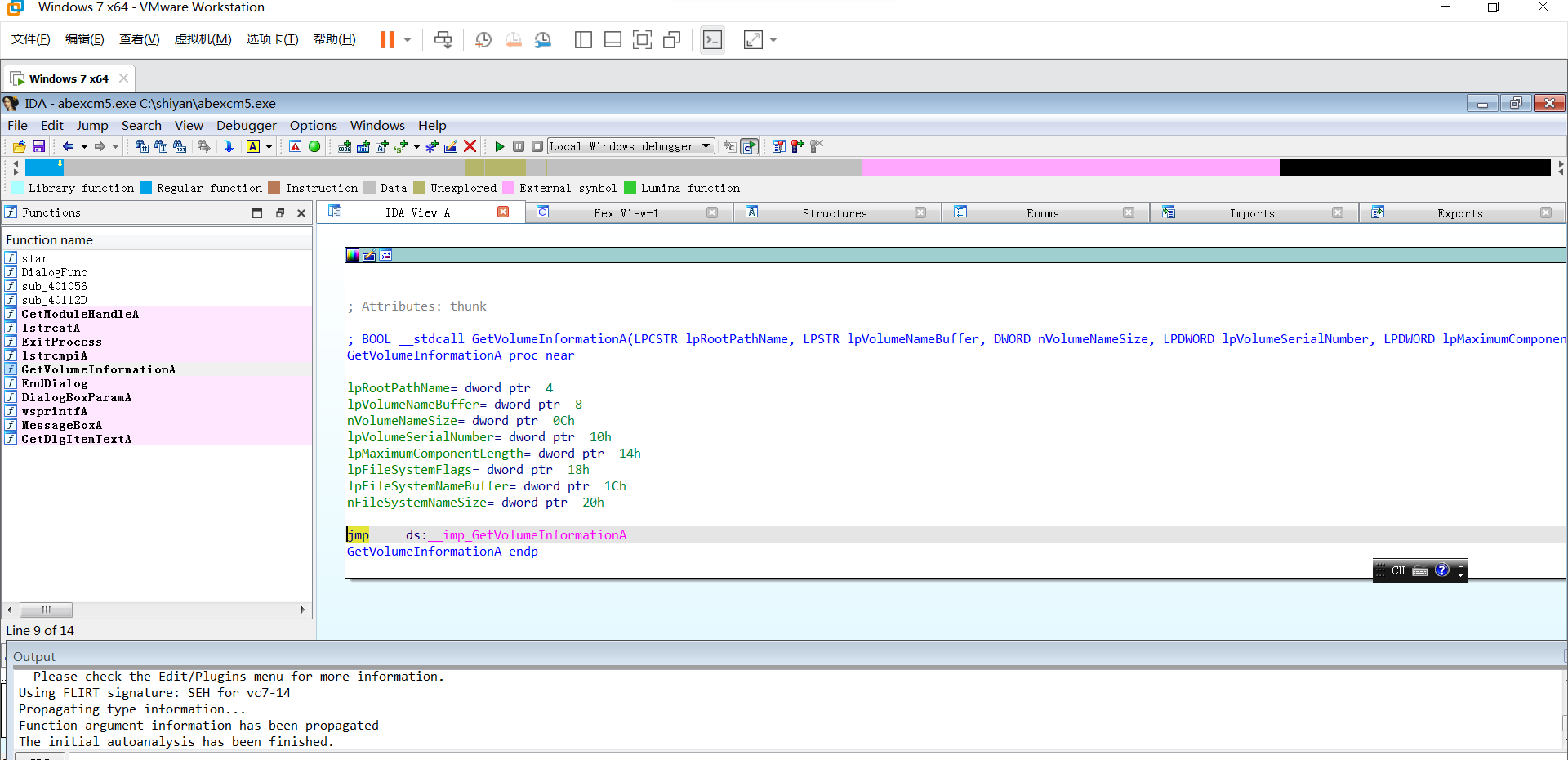


拿下！

### Ida

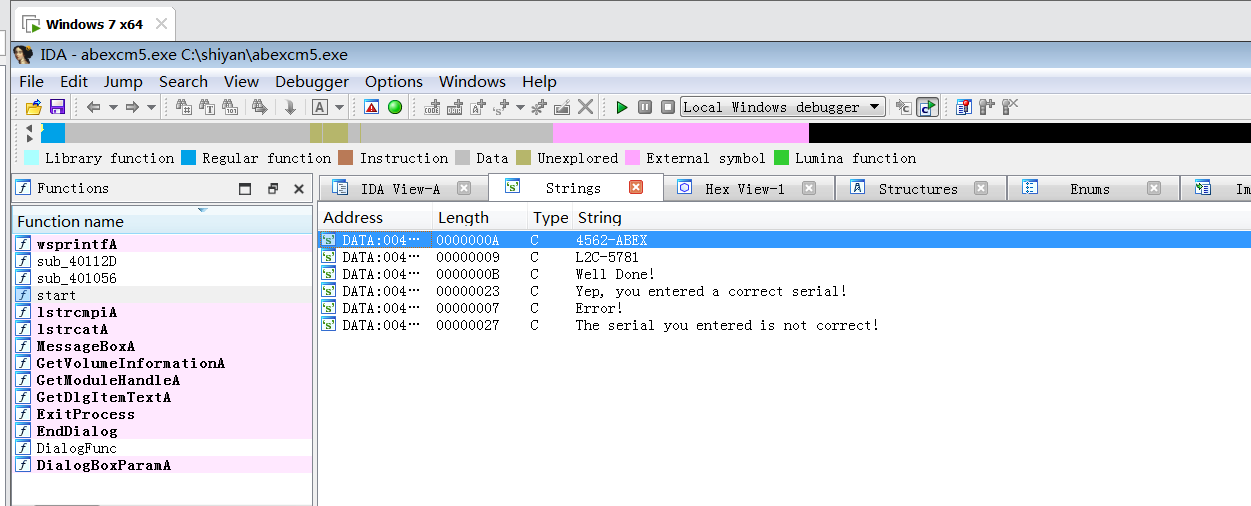
Ollydbg里面已经把程序的算法逻辑理清楚了，剩下两个工具就直接通过修改文件本身让其强制通过：

启动ida，把程序拖到ida里面

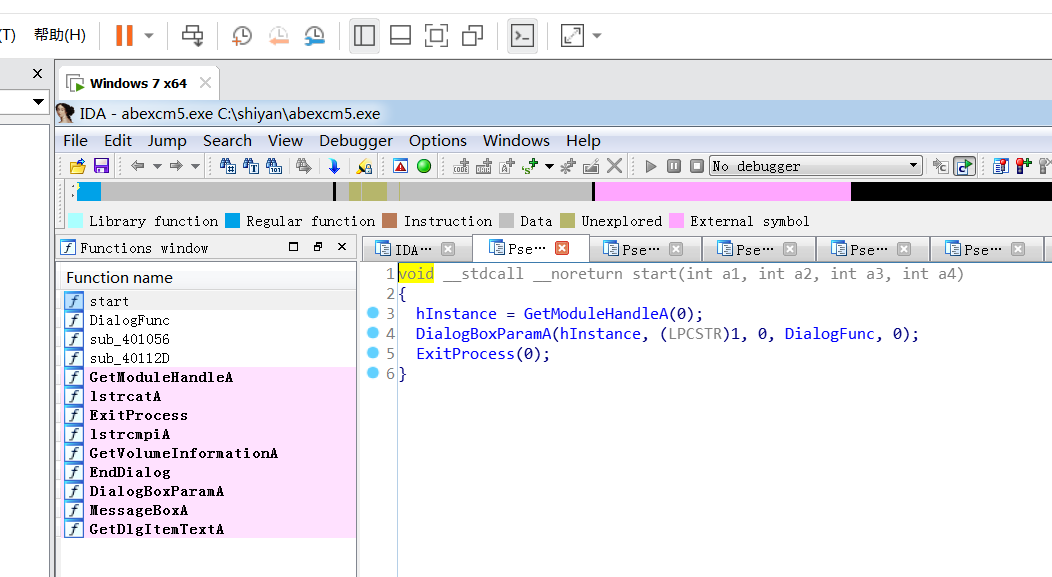


这个ida直接把里面的函数全提取到左边了，好像比ollydbg简单一些

找一下里面出现的字符串：

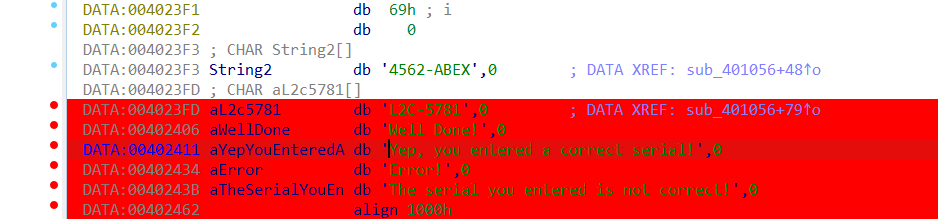


用ida独有的反编译看一下代码逻辑

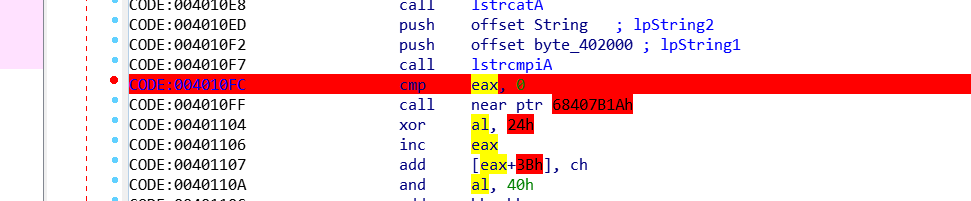


没啥用

找一下上面那些字符串出现的位置：

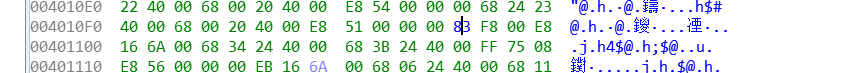


顺着向上找到跳转逻辑



直接把这个cmp eax 0改成0和0比较

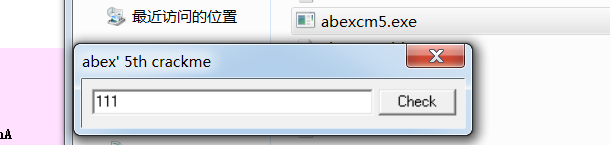
Cmp是83，找一下位置：

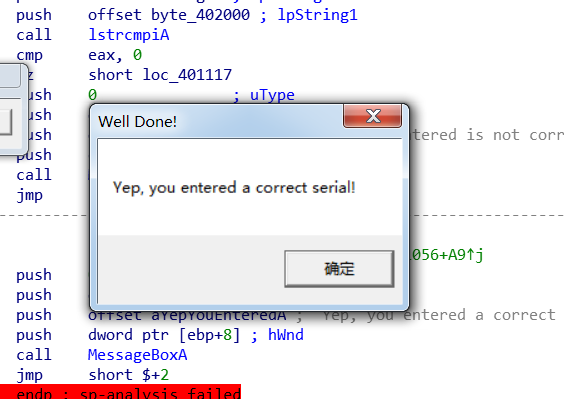


83找到了，后面f8应该就是eax了，改成00



Ok保存看一下是不是输入啥都可以通过





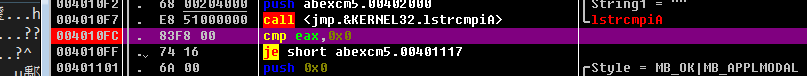
没毛病

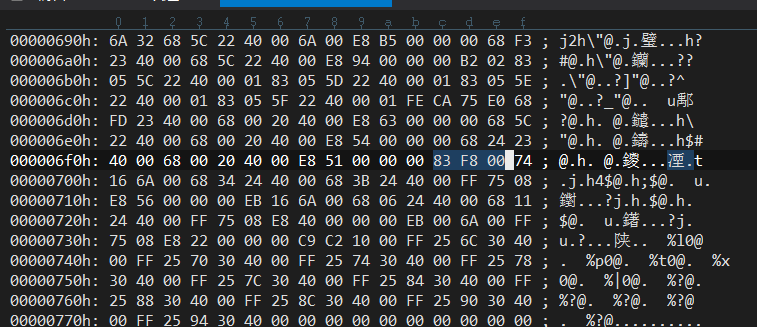
## Ultraedit：

使用这个工具就也不是分析算法和代码流程了，只能改文件本什么

直接把执行文件内部修改让他直接跳转到序列号输入成功界面。

根据ollydbg做过的结果找到跳转的那行：





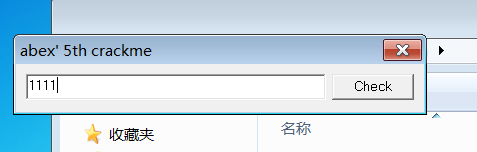
整个文件只有这一个83F800，前后的东西也都对的上，那就是这一句了！

换一种和ida不同的改法：

把他下面那个跳转的je（条件满足跳转）改为jmp直接跳转

Je对应机器码是74，jmp是e8







也是直接拿下了。