《漏洞利用及渗透测试基础》实验报告

姓名：孙蕗 学号：2112060 班级：信安1班

**实验名称：**

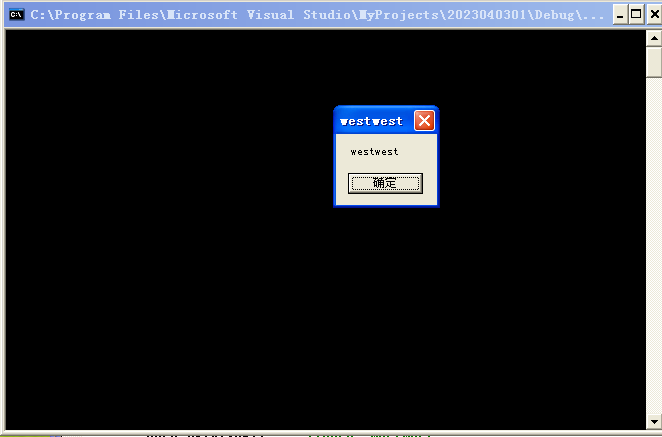
API函数自搜索

**实验要求：**

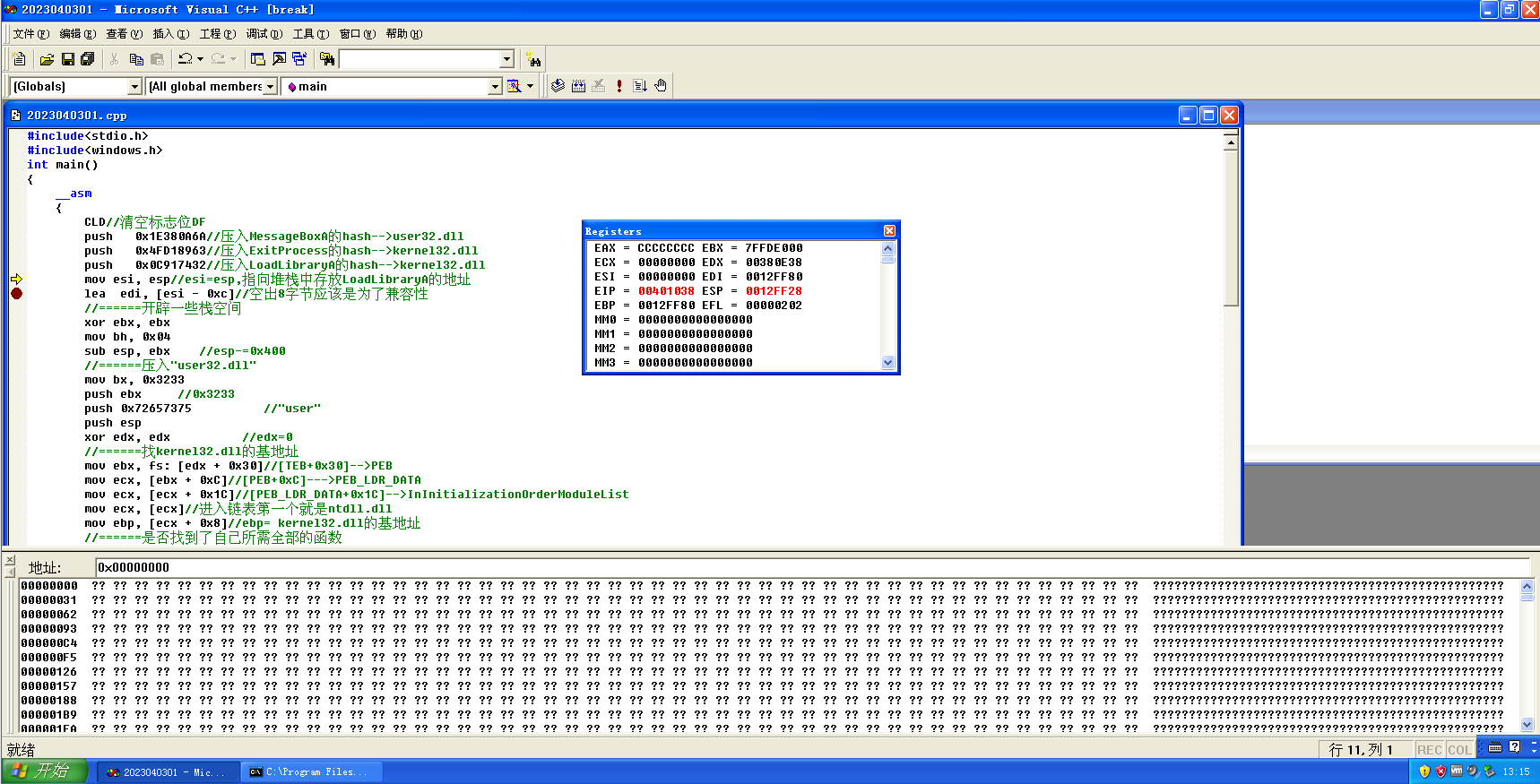
复现第五章实验七，基于示例5-11，完成API函数自搜索的实验，将生成的exe程序复制到windows10操作系统里验证是否成功。

**实验过程：**

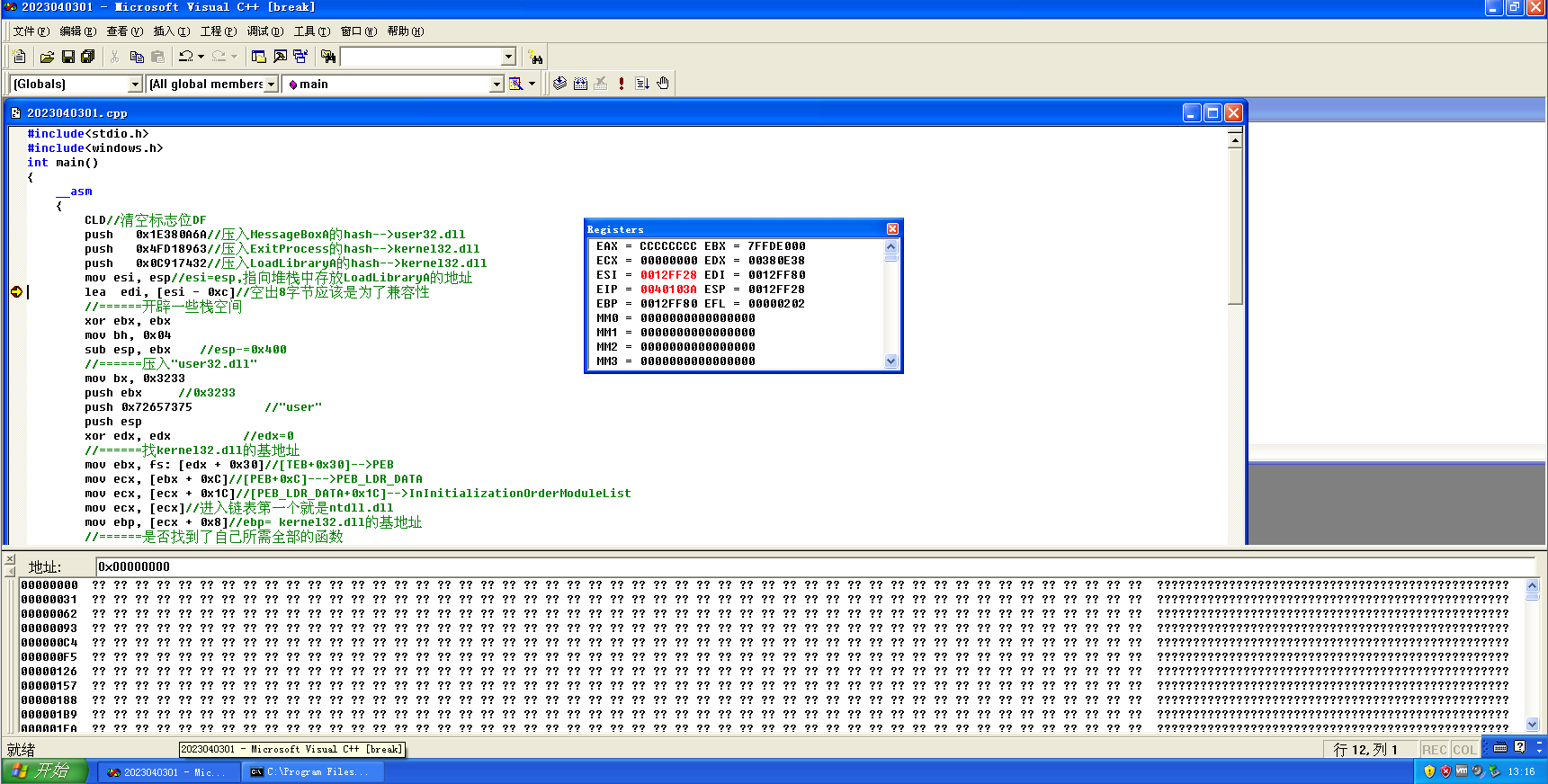
1. Windowsxp运行截图



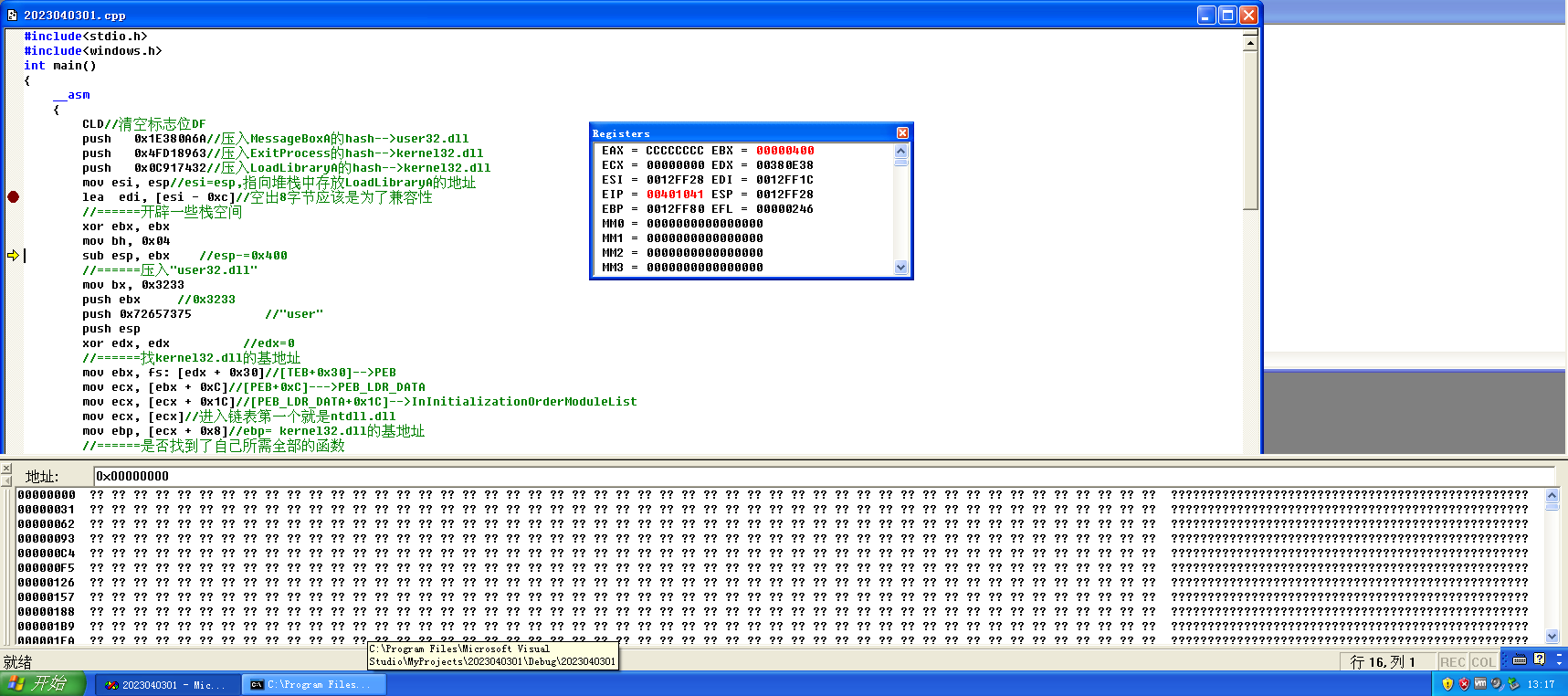
1. F10，3个push哈希值，MessagBoxA、ExitProcess、LoadLibraryA的字符串的hash



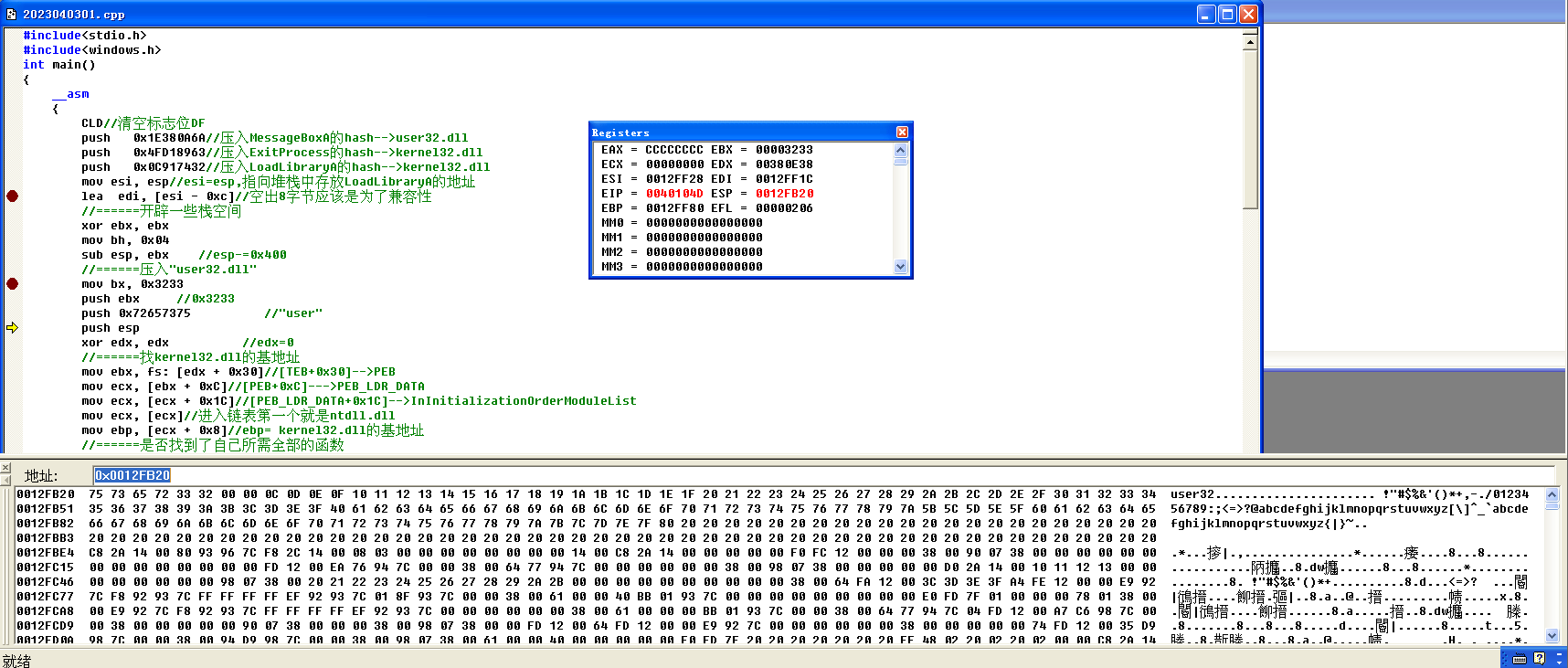
1. F10，找到这些哈希值。esi=0012FF28



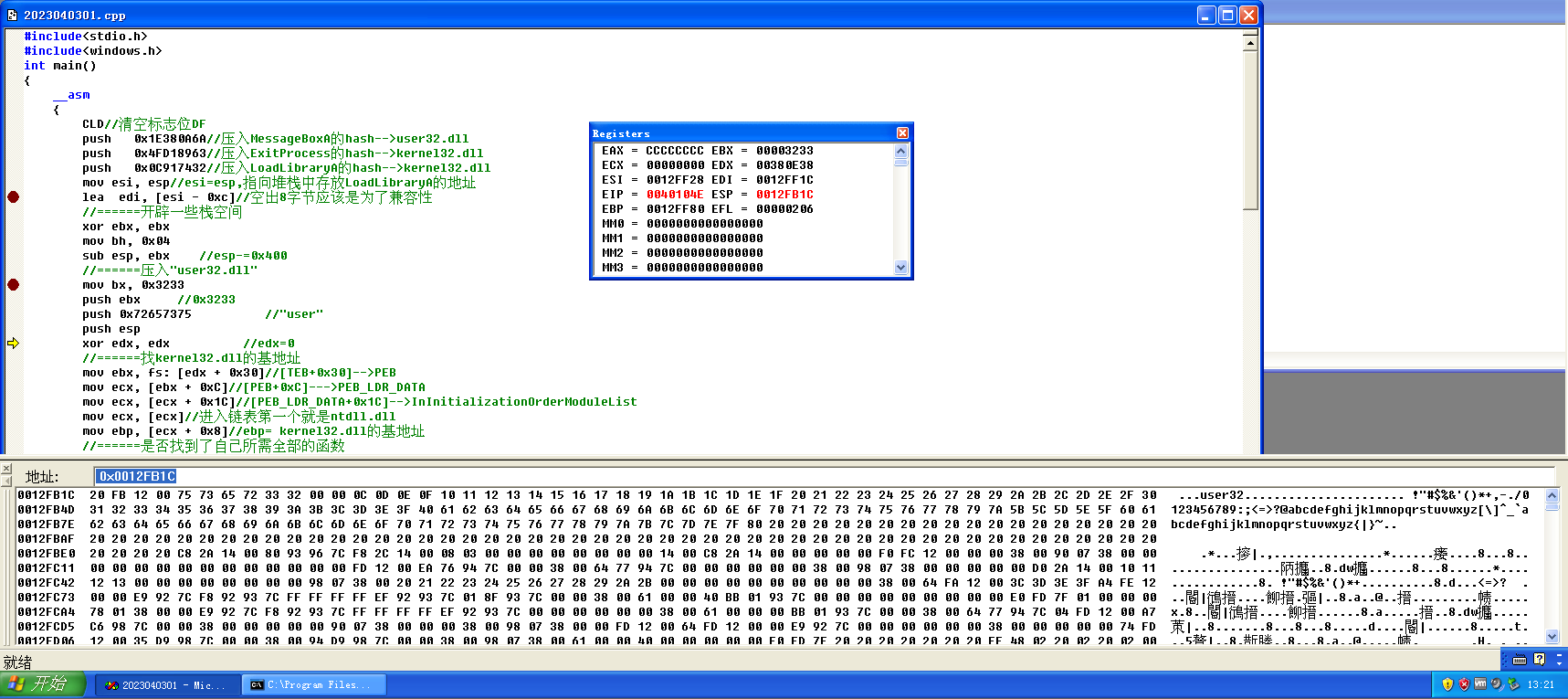
1. F10，esp抬高。ebx=00000400



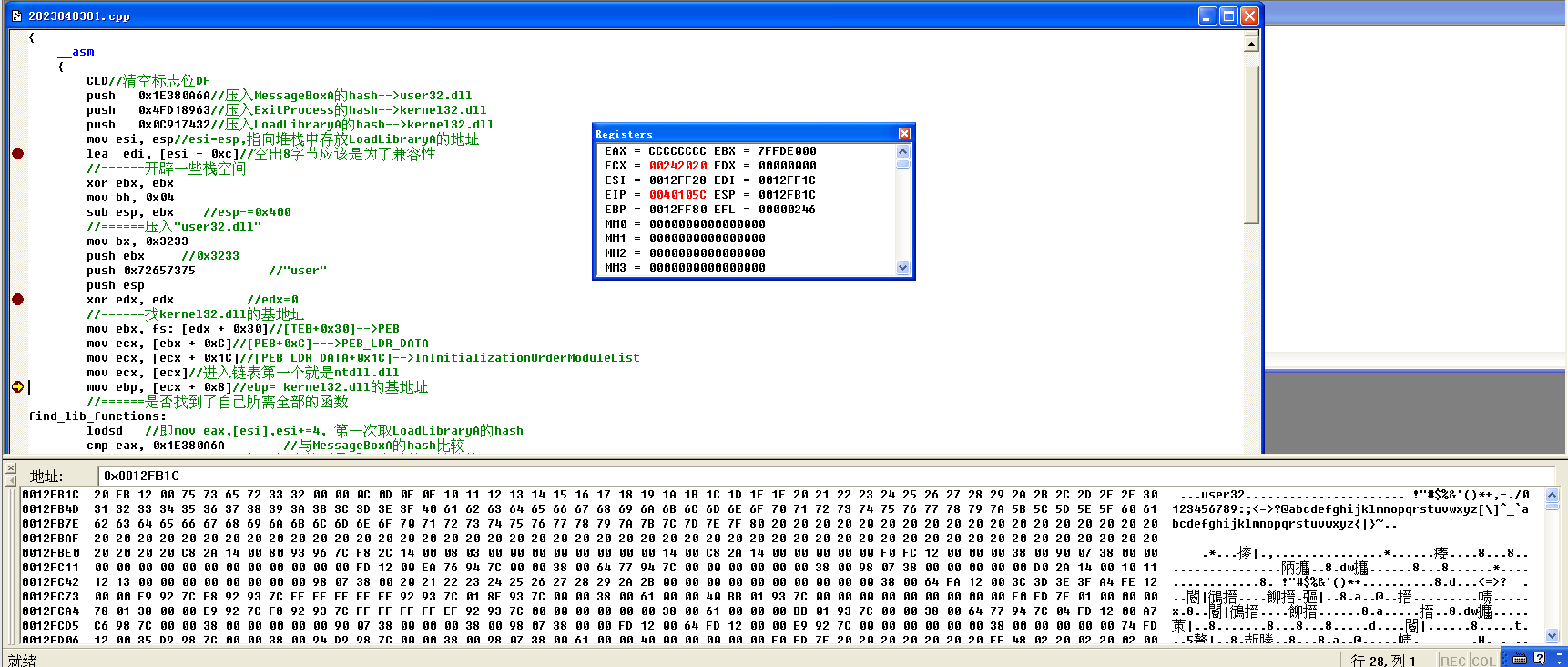
1. F10，push user32。eip里存的就是user32，esp=0012FB20



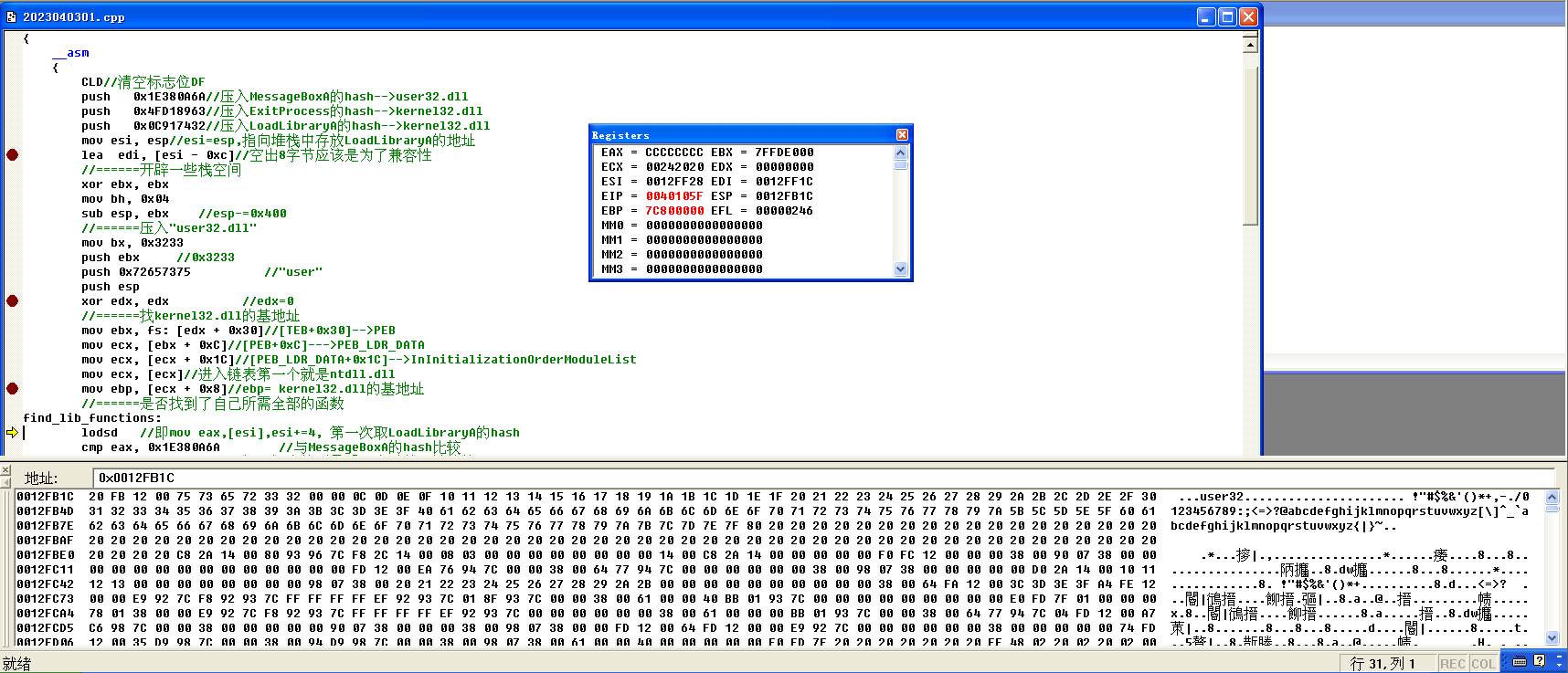
1. F10，esp=0012FB1C，该地址前面存了0012FB20，即user32字符串的地址



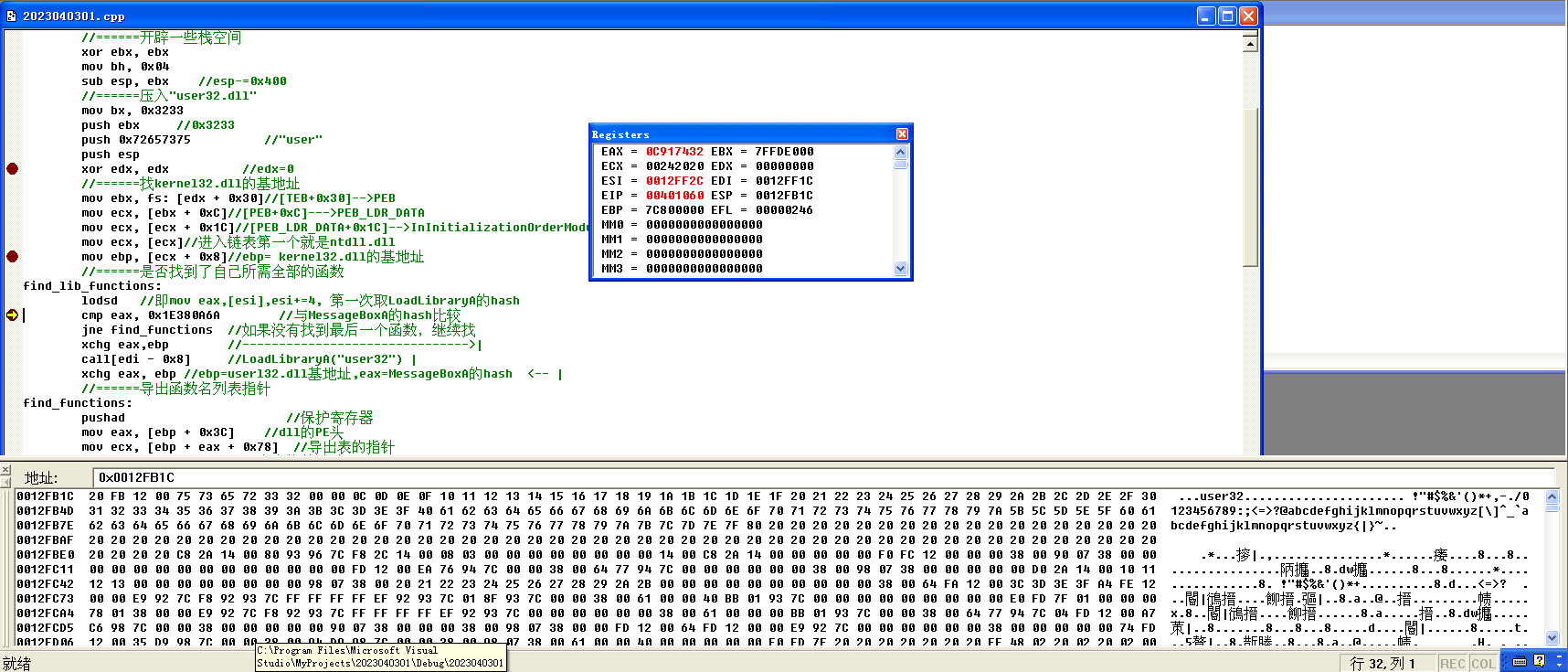
1. F10



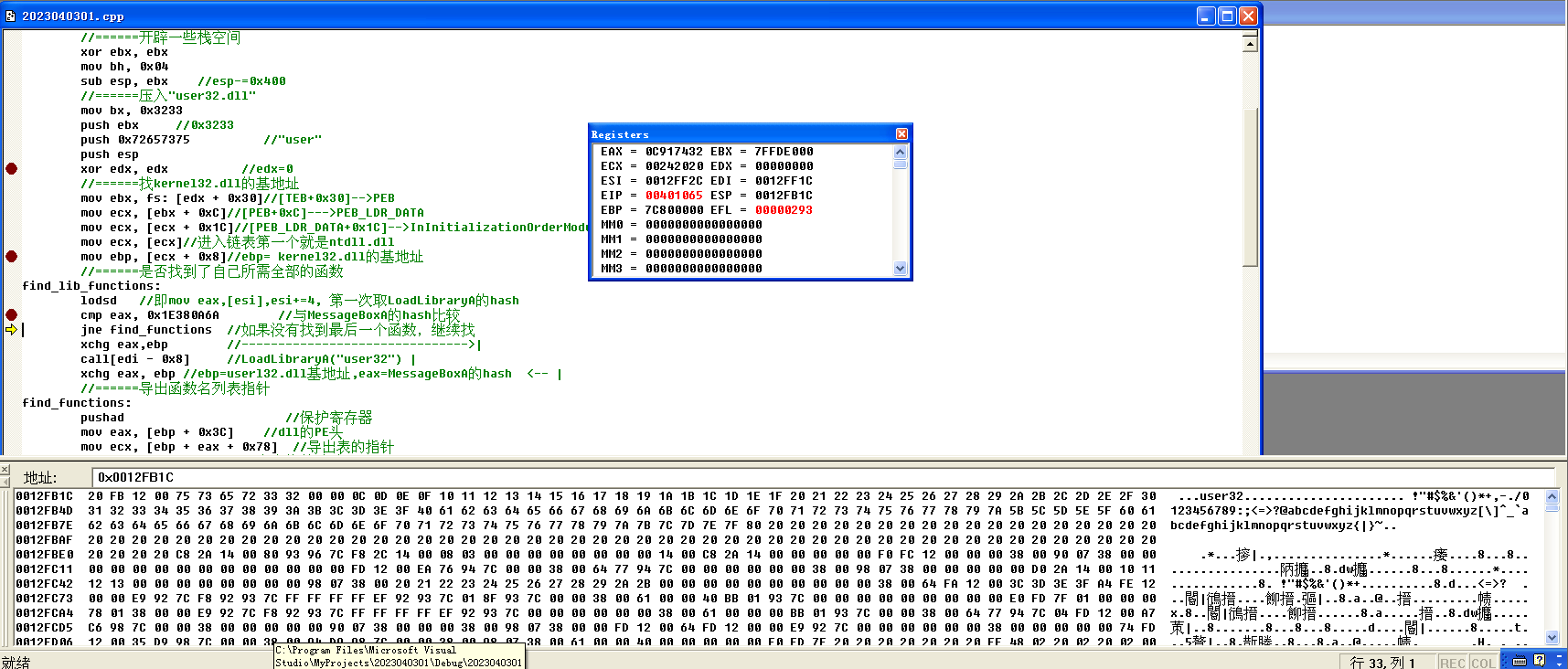
1. F10，ebp=7C800000，存的是kernel.32的地址



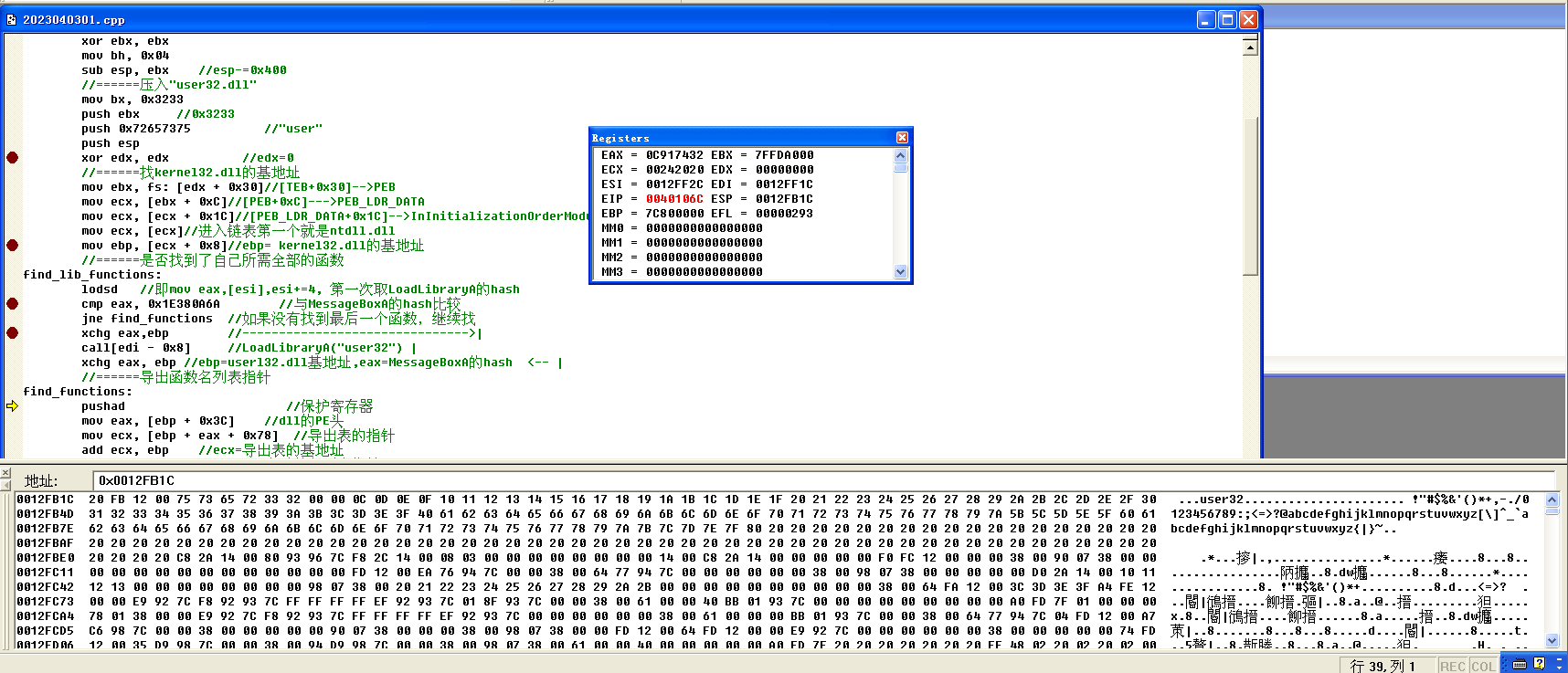
1. F10，lodsd即mov eax,[esi]，esi+=4，第一次取LoadLibraryA的hash



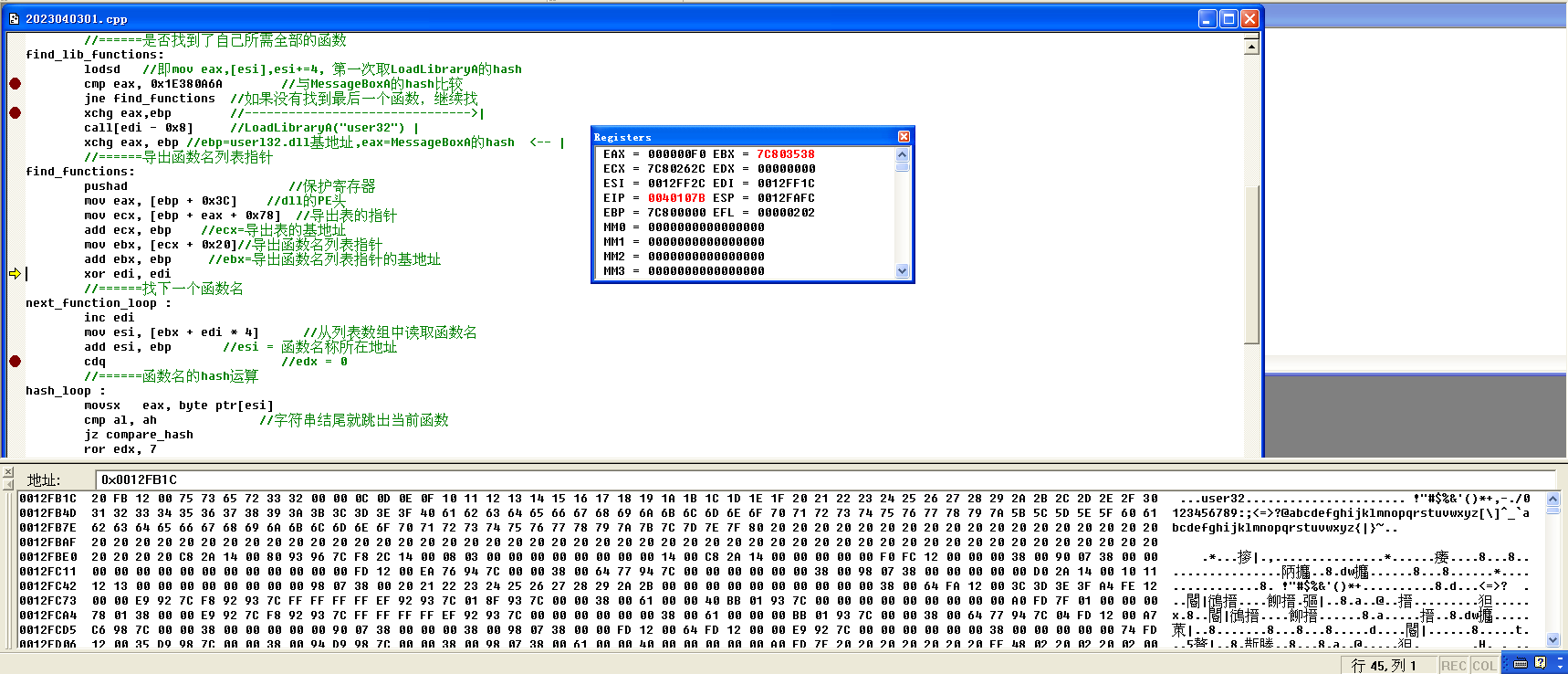
1. F10



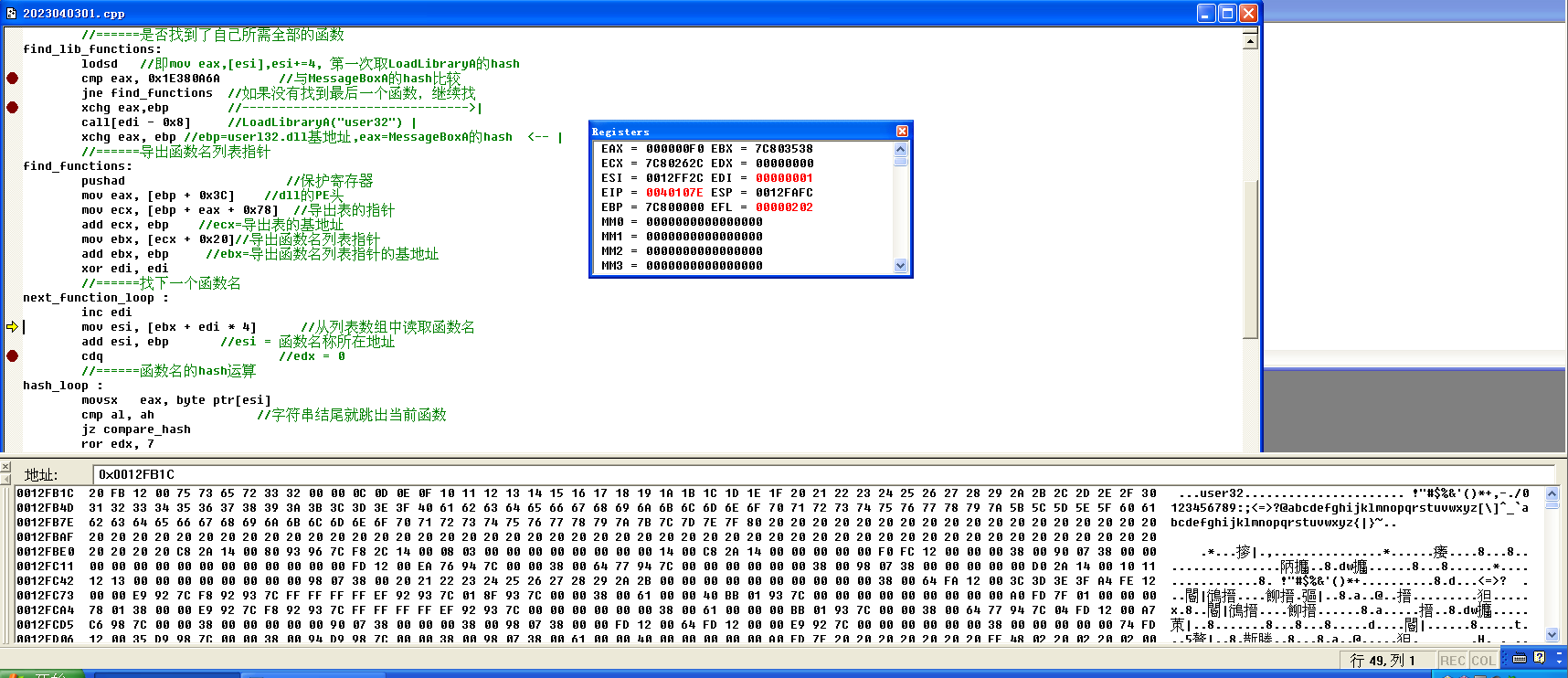
1. F10，条件判断，条件成立转到pushad



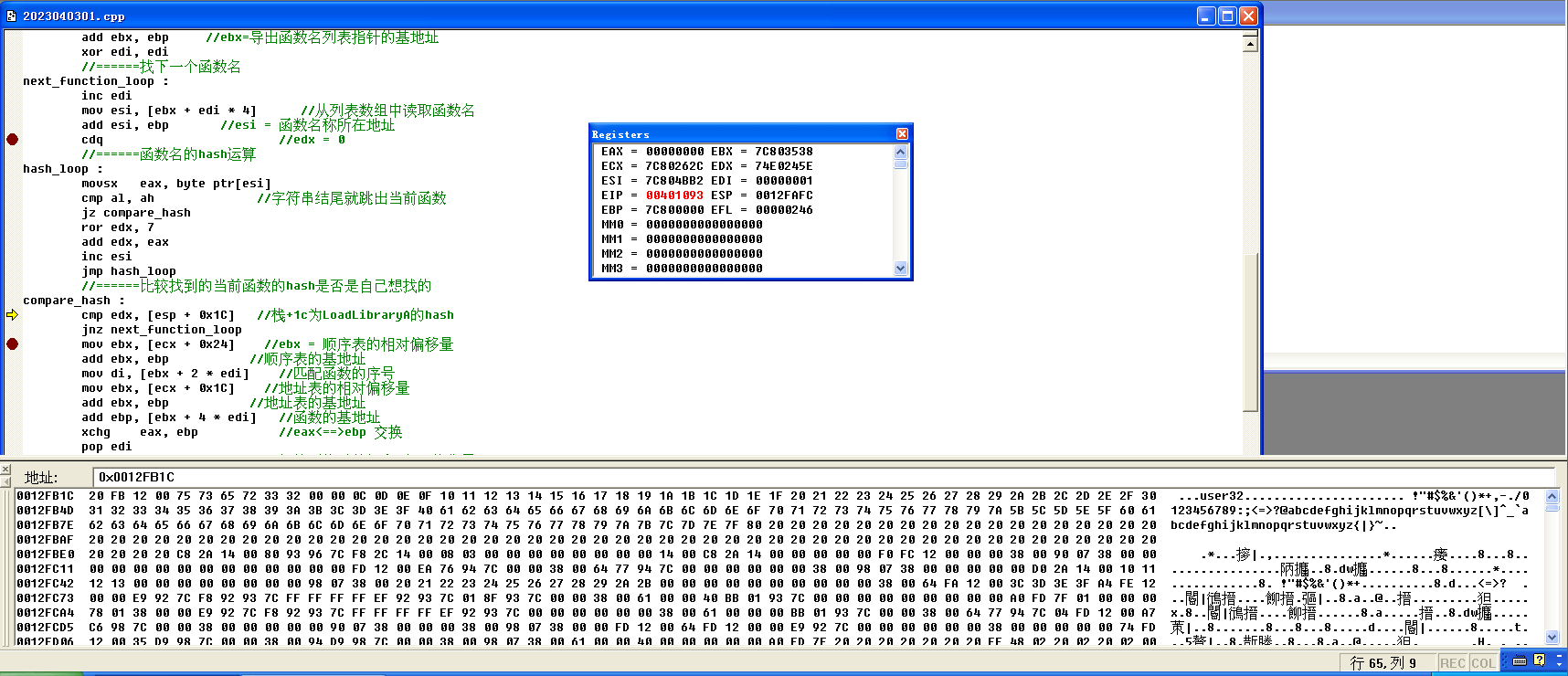
1. F10，dll的PE头，导出表指针，ecx=导出表的基地址，导出函数名列表的指针，ebx=导出函数名列表指针的基地址。



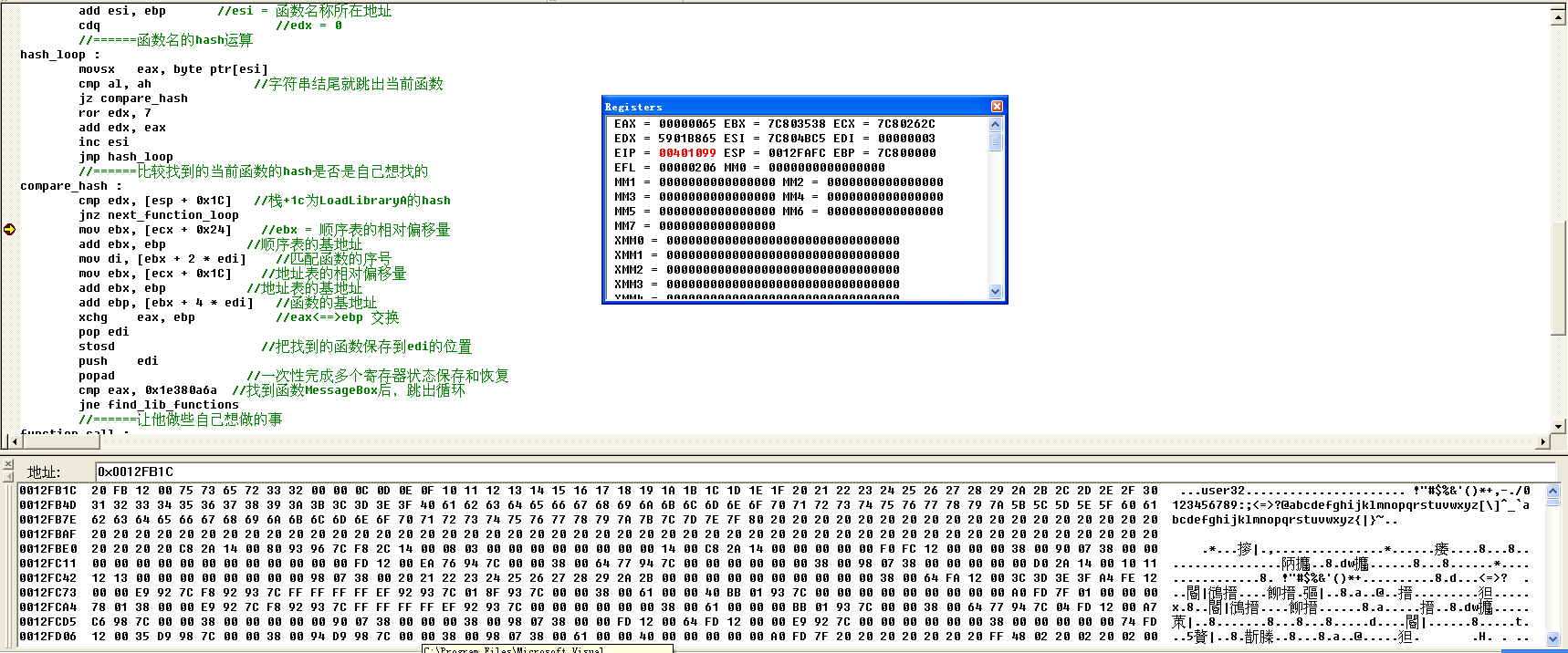
1. F10，取一个函数，然后去计算hash



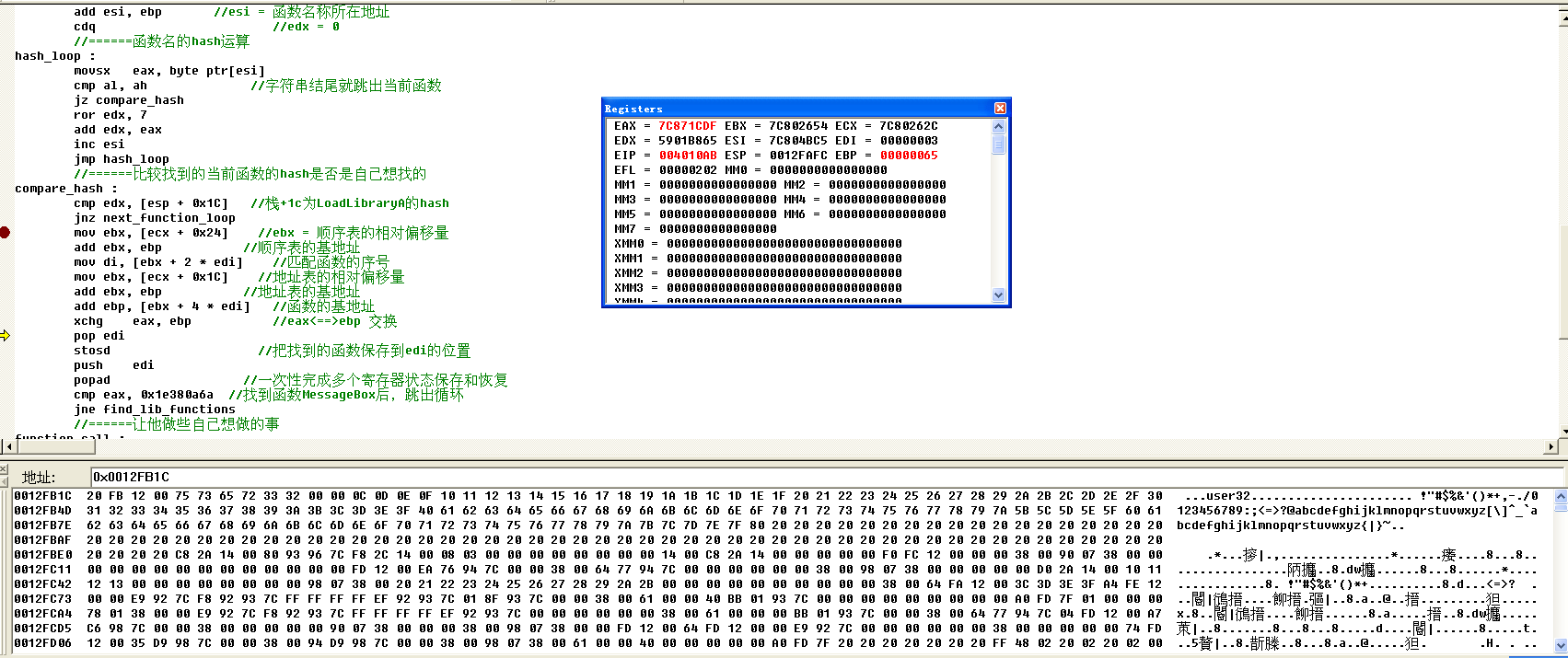
1. F10，hash计算，计算完成好跳转到cmp的位置



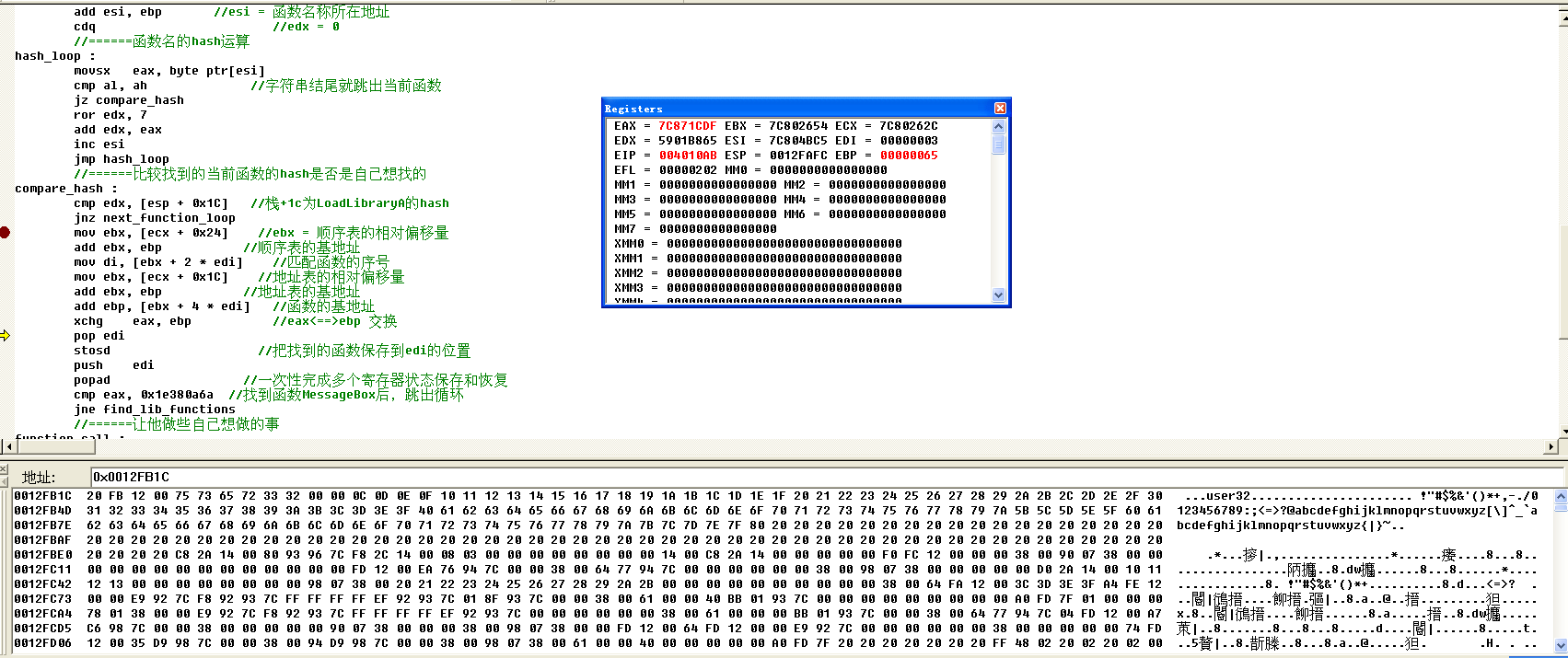
1. F5，找到了



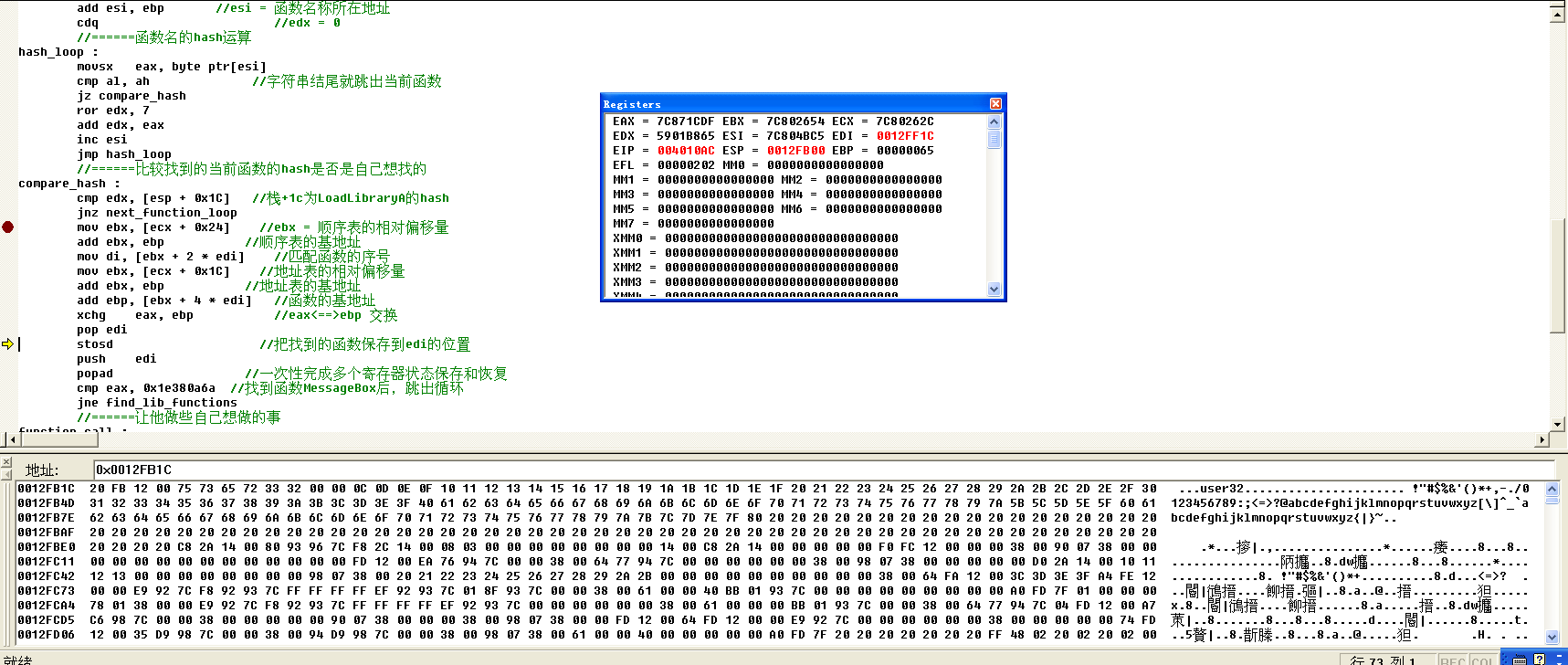
1. F10，相对虚拟地址+基地址-->虚拟地址



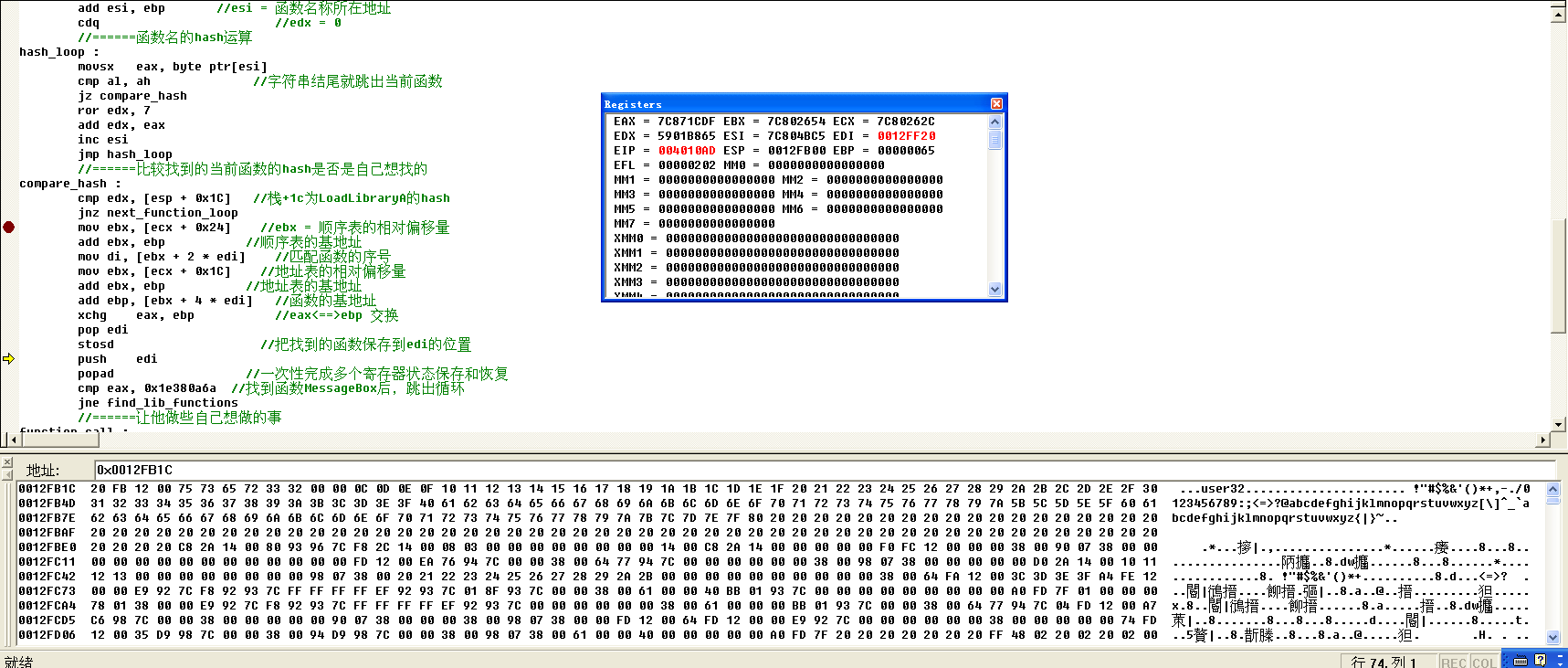
1. F10



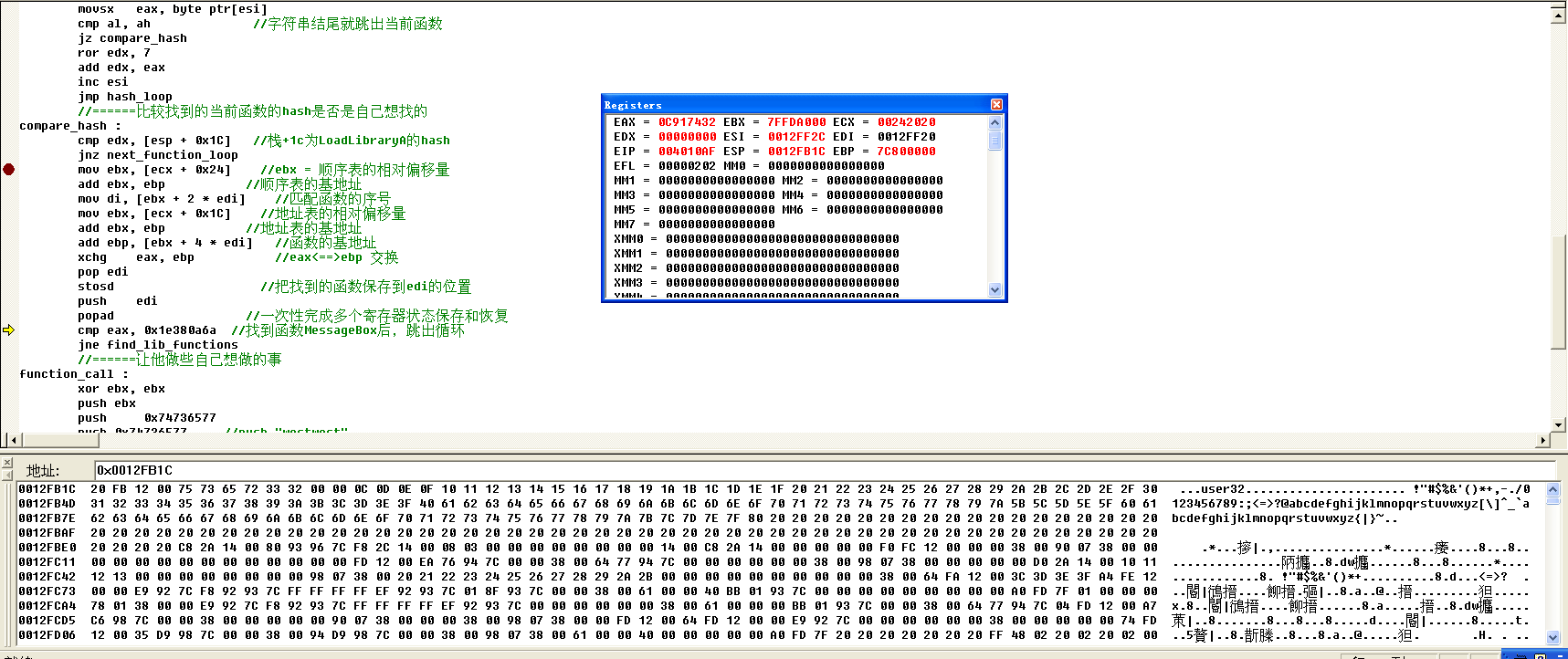
1. F10，edi=0012FF1C。



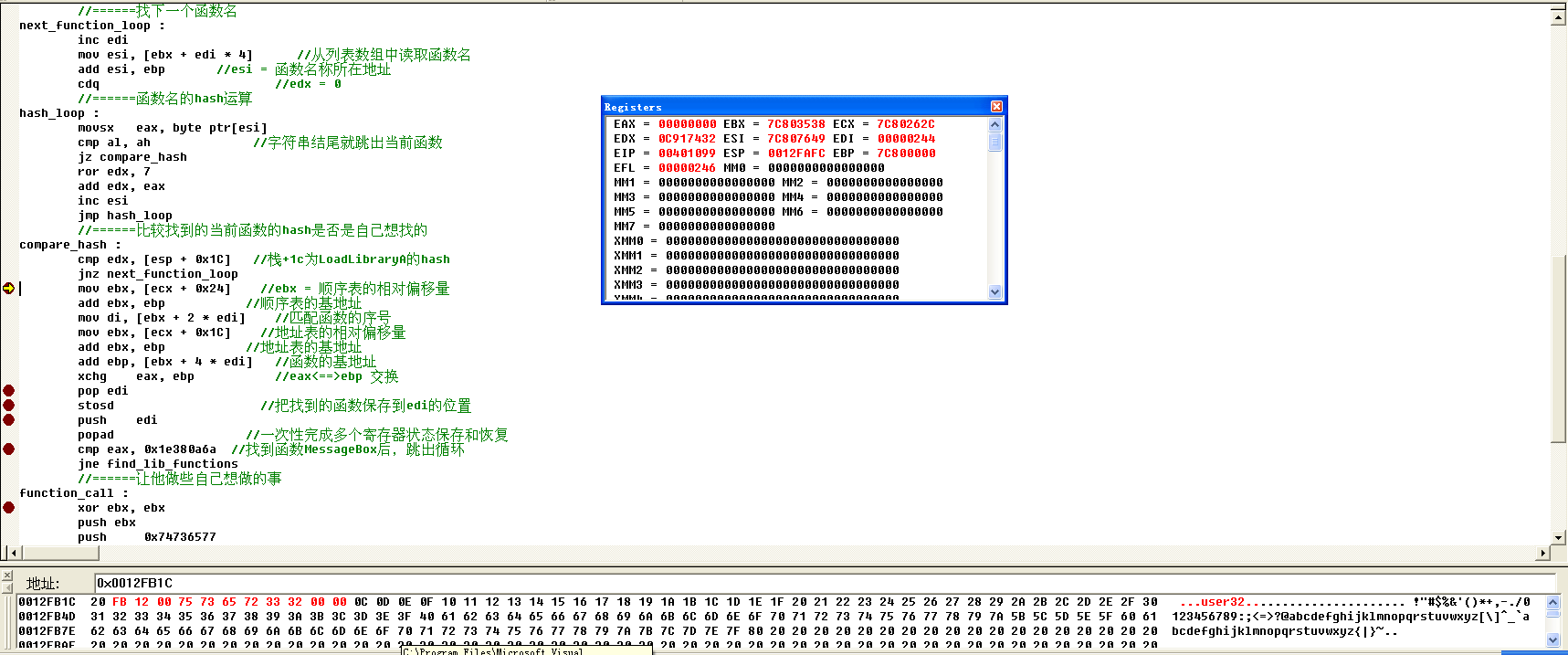
1. F10把找到的函数保存到edi位置上



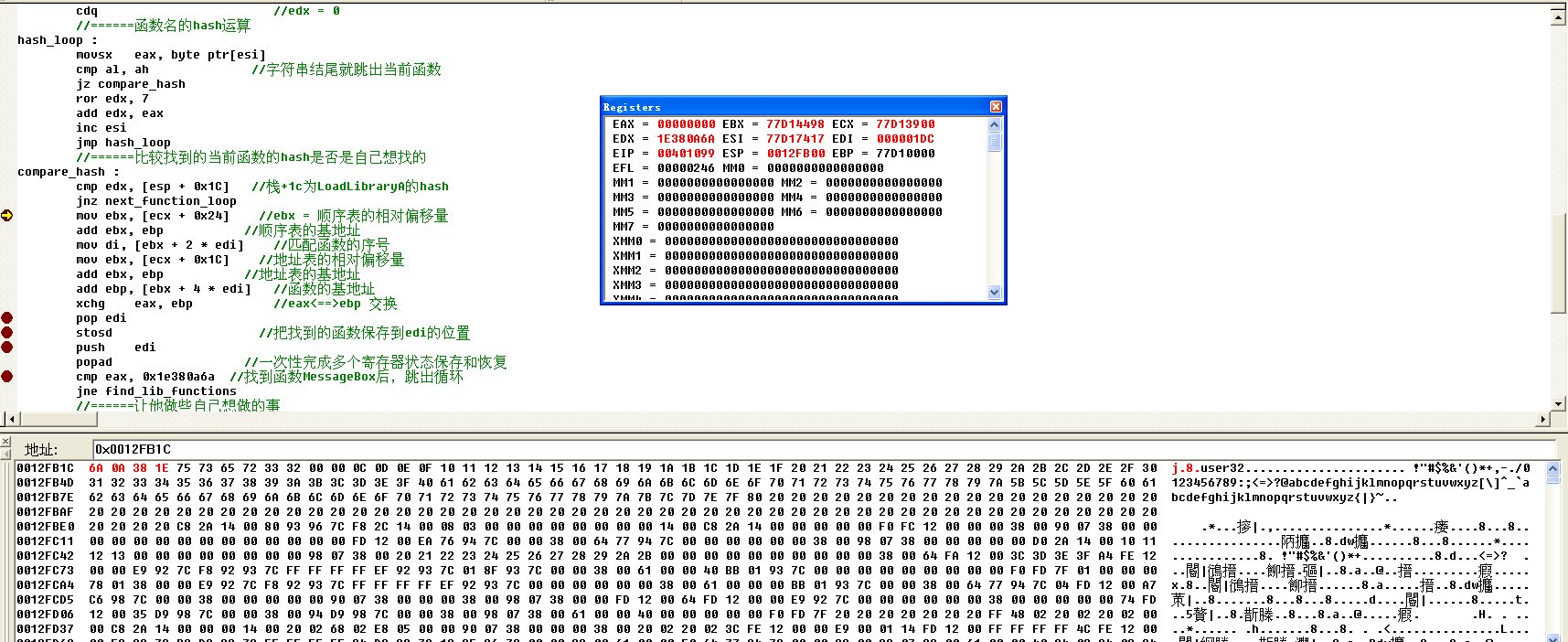
1. F10，找到最后一个函数MessageBox后，跳出循环



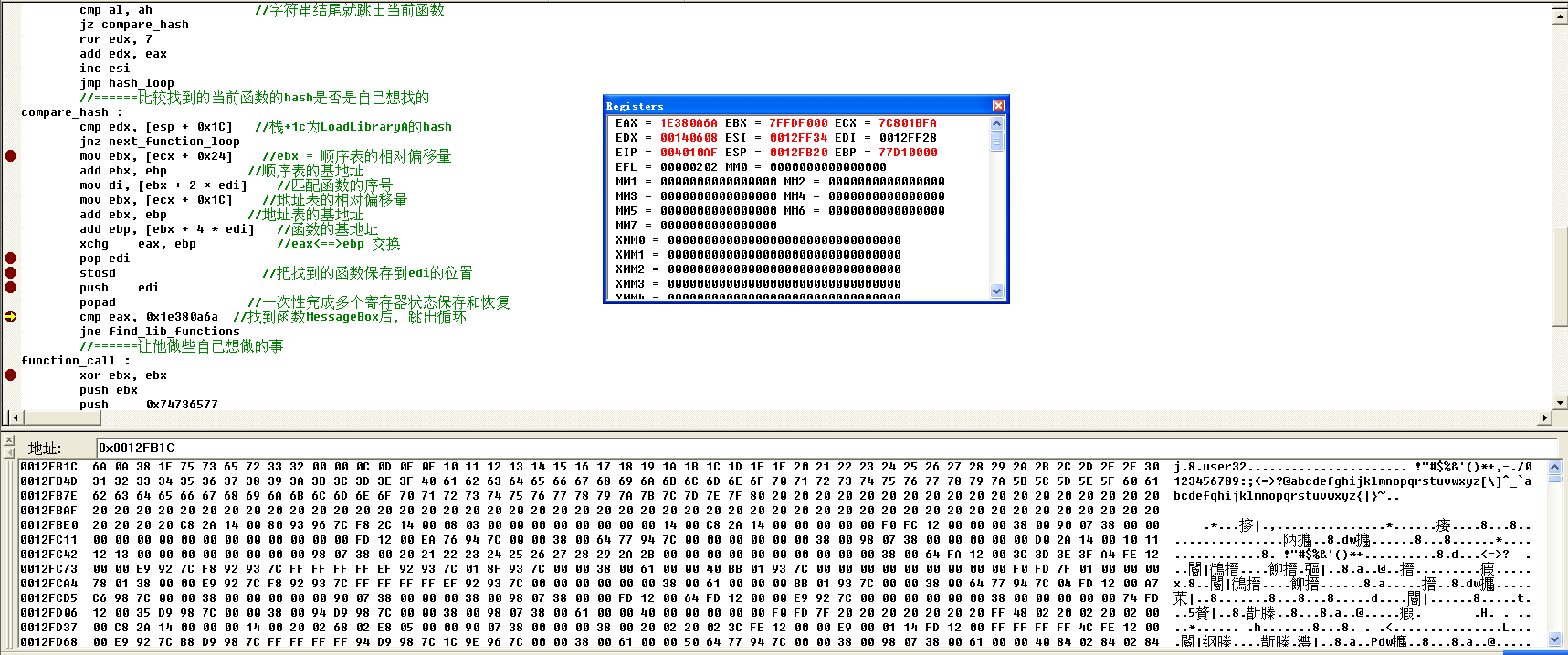
1. F10



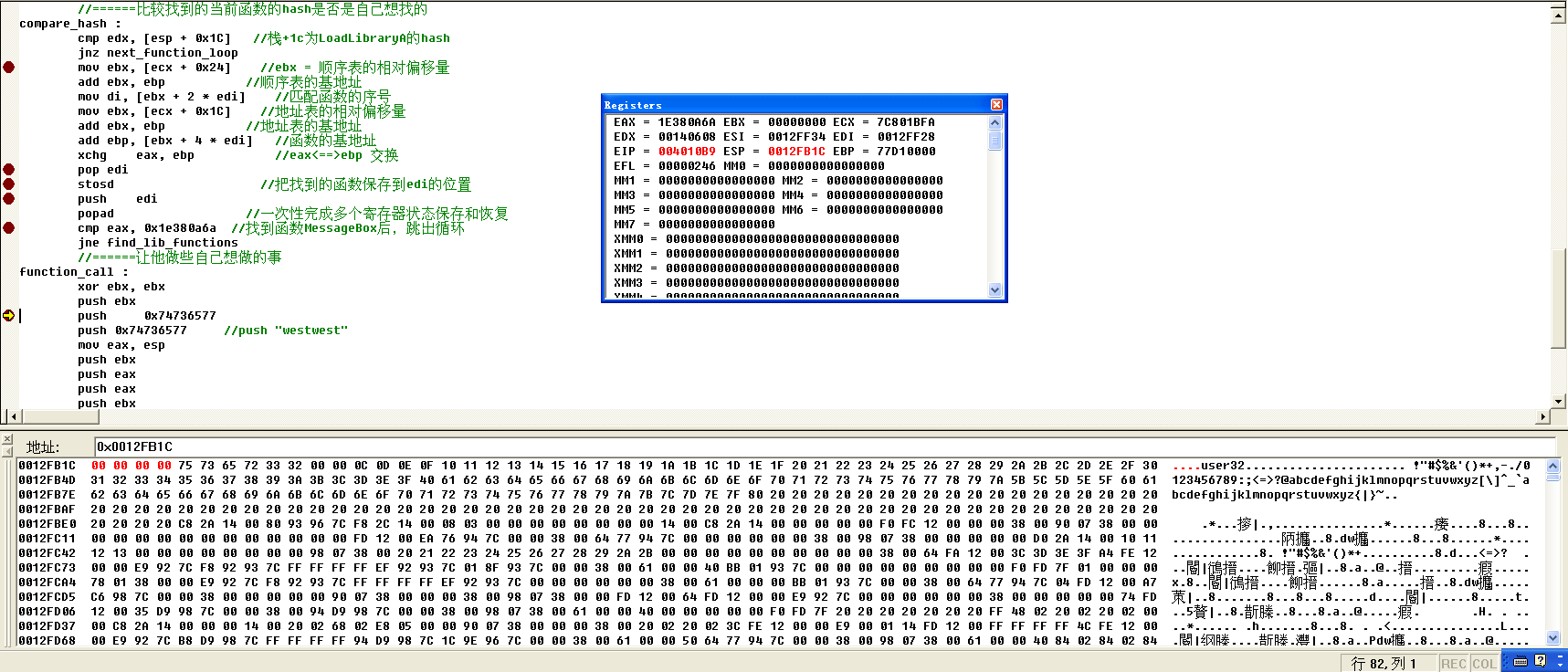
1. F5



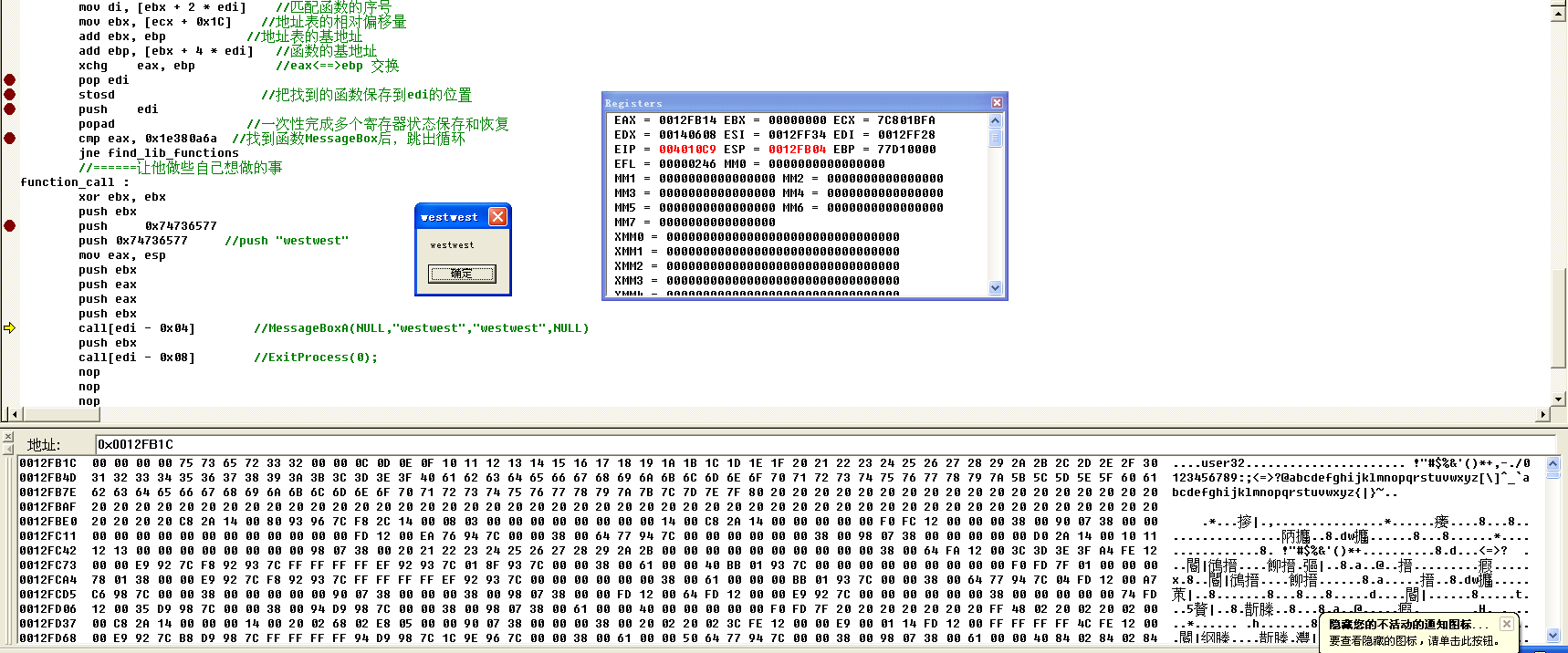
1. F5



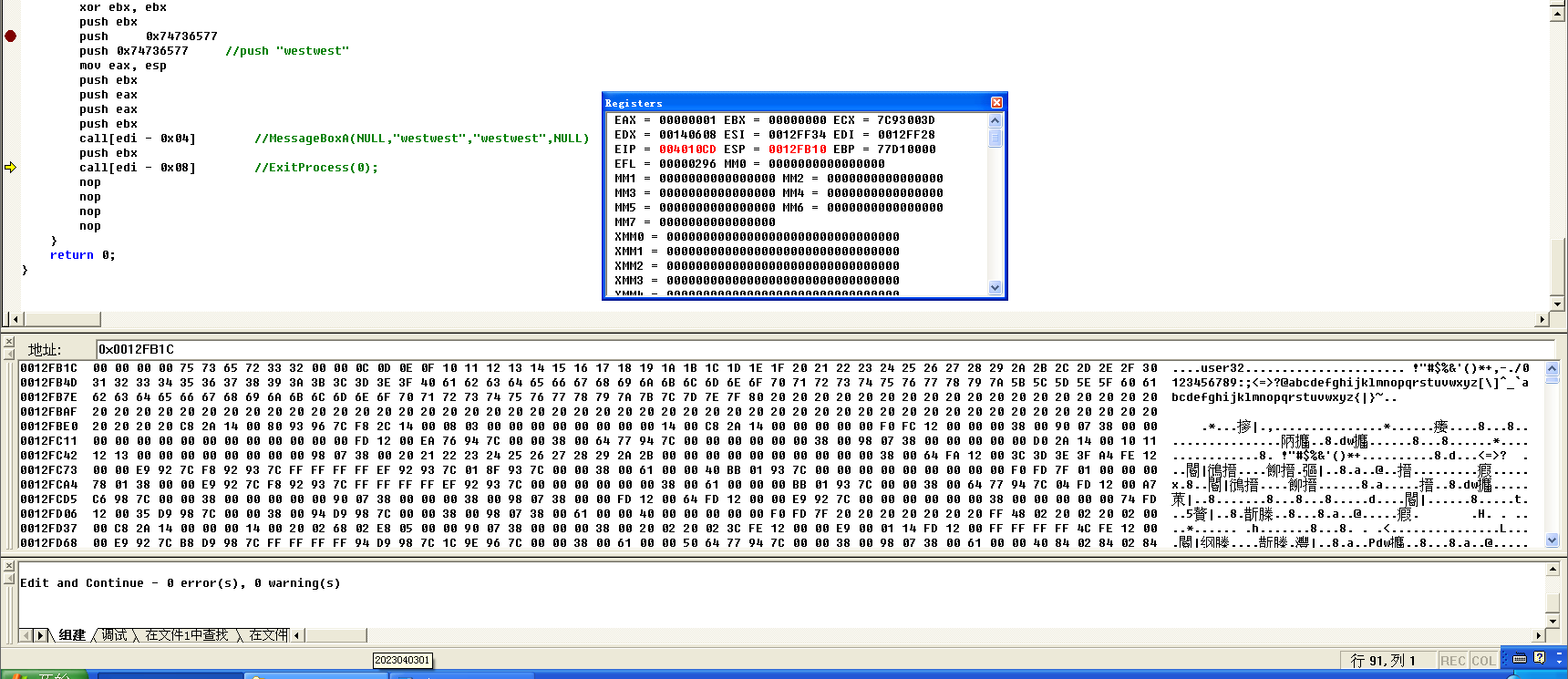
1. F10



1. F10



1. F10



1. Win10验证



**心得体会：**

在实际中为了编写通用shellcode，shellcode自身必须具备动态的自搜索所需API函数地址的能力。先后定位kernel32.dll、kernel32.dll的导出表、搜索定位目标函数，找到函数的入口地址。然后编写自己的shellcode，完成完整API函数自搜索代码。