- xiabee

软件破解实验报告

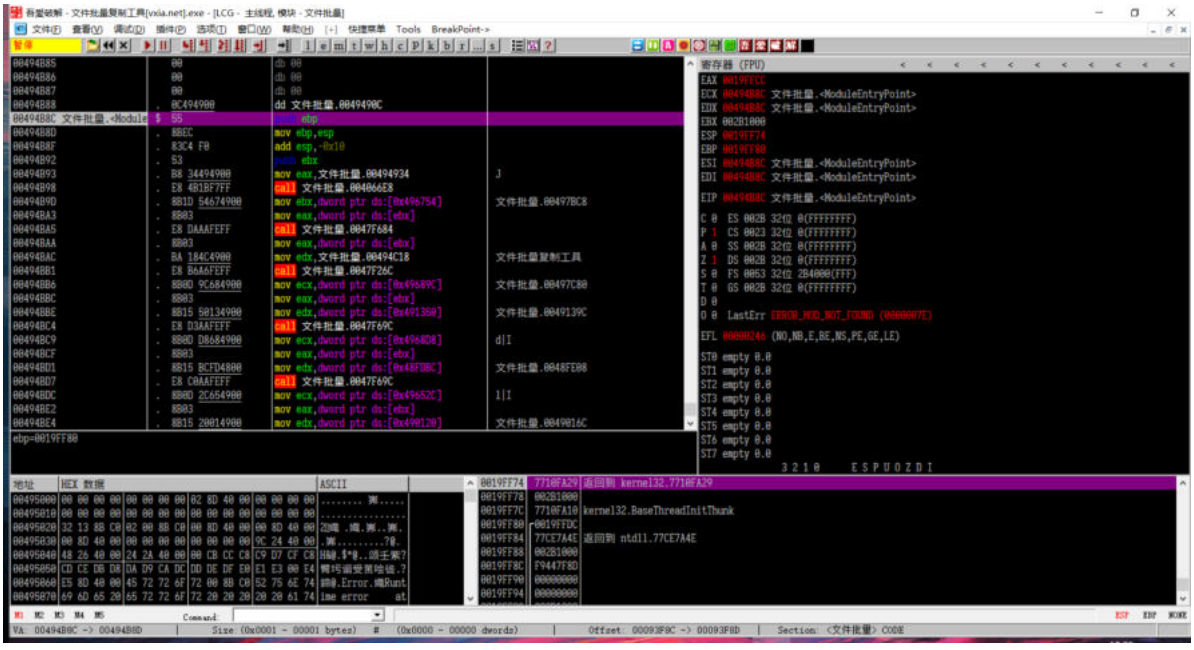
0x00 实验目的

- 学习软件逆向基本过程
- 学习 ollydbg 的使用
- 熟悉汇编程序的运行过程

0x01 实验过程

1、通过Ollydbg进行反汇编

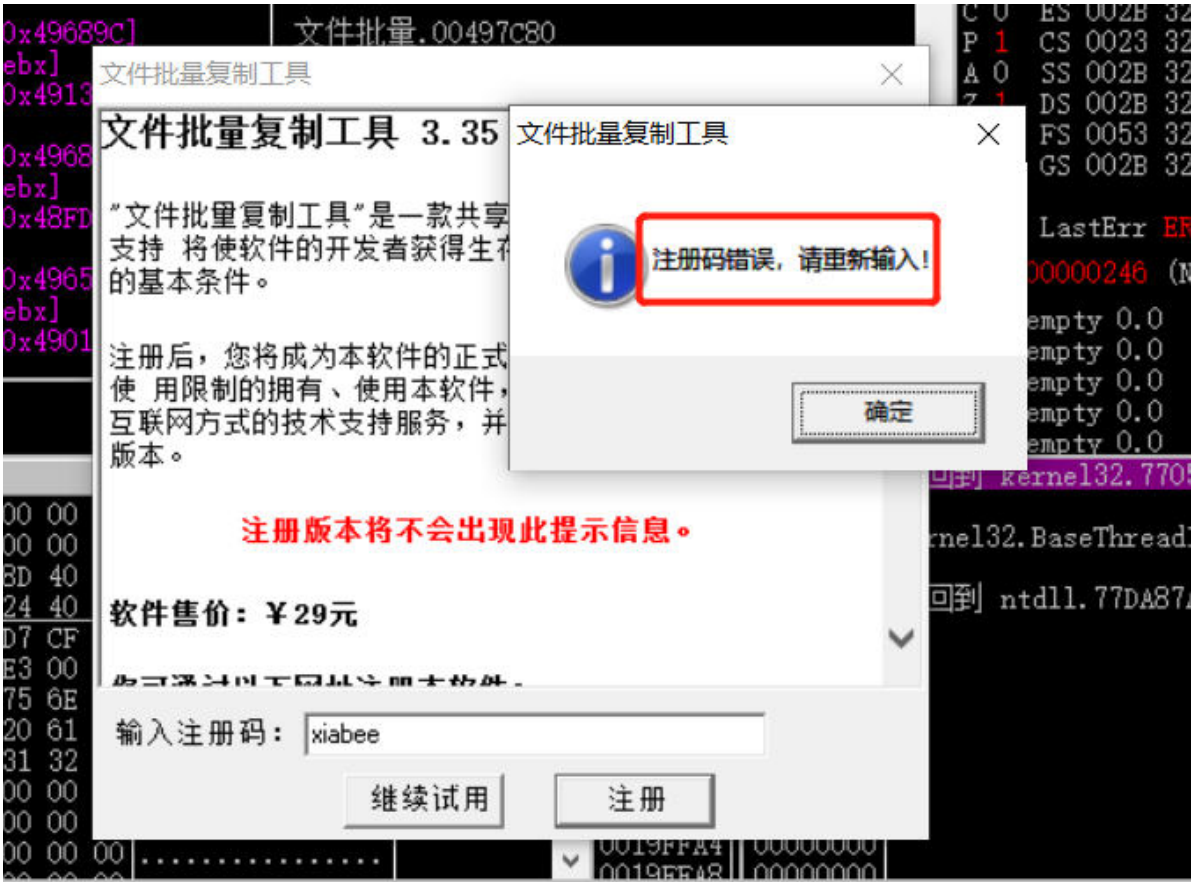
通过ODB打开`文件批量复制工具[vxia.net].exe`，查看其汇编代码：



进入反汇编主窗口，观察程序入口位置

2、动态调试破解软件

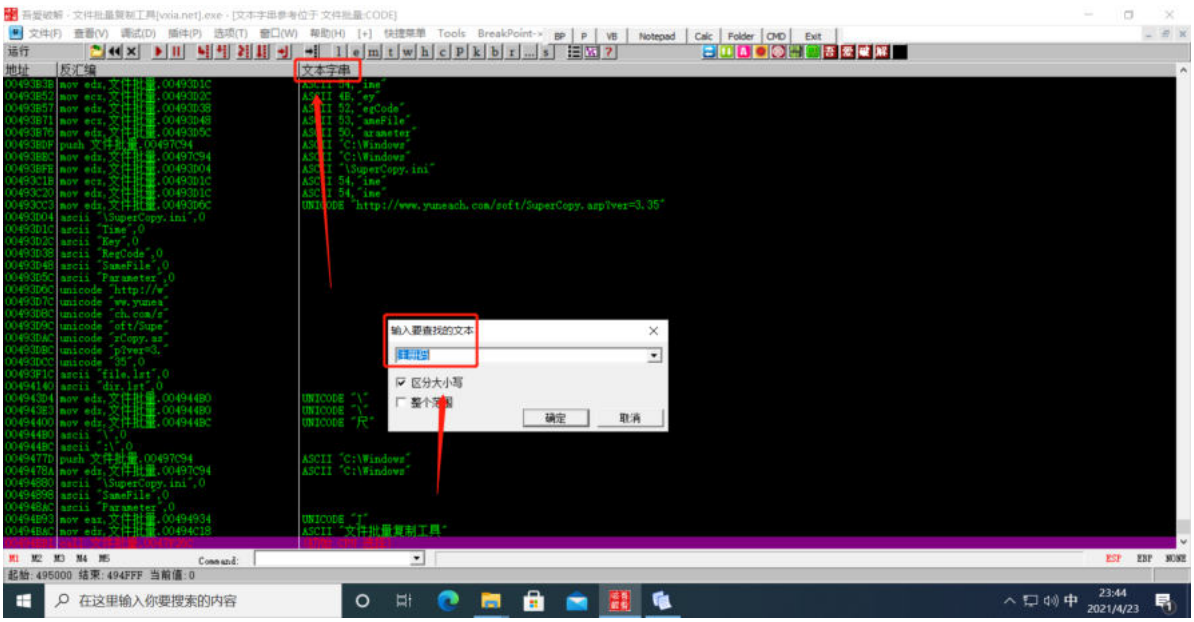
`F9`启动动态调试，开启新进程，进入注册界面；输入注册码`xiabee`，显示注册码错误：



3、寻找注册地址

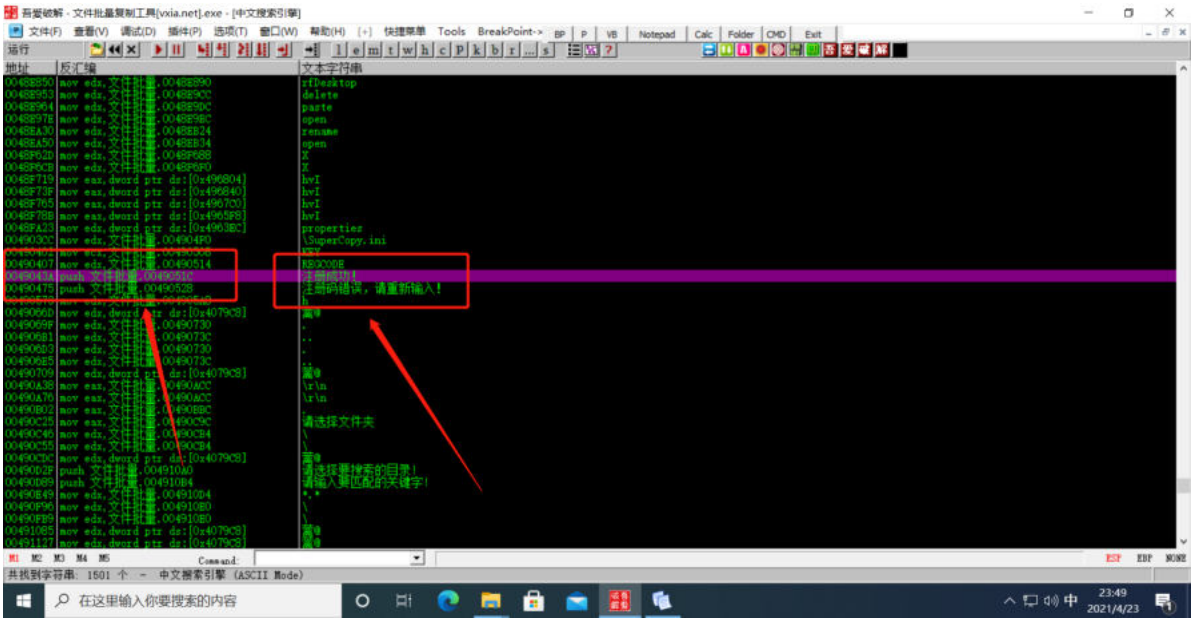
在反汇编窗口查找 `注册码` 相关字符串，定位注册点：

- （反汇编窗口内） `右键` → `查找` → `所有参考文本字串` → `查找文本`



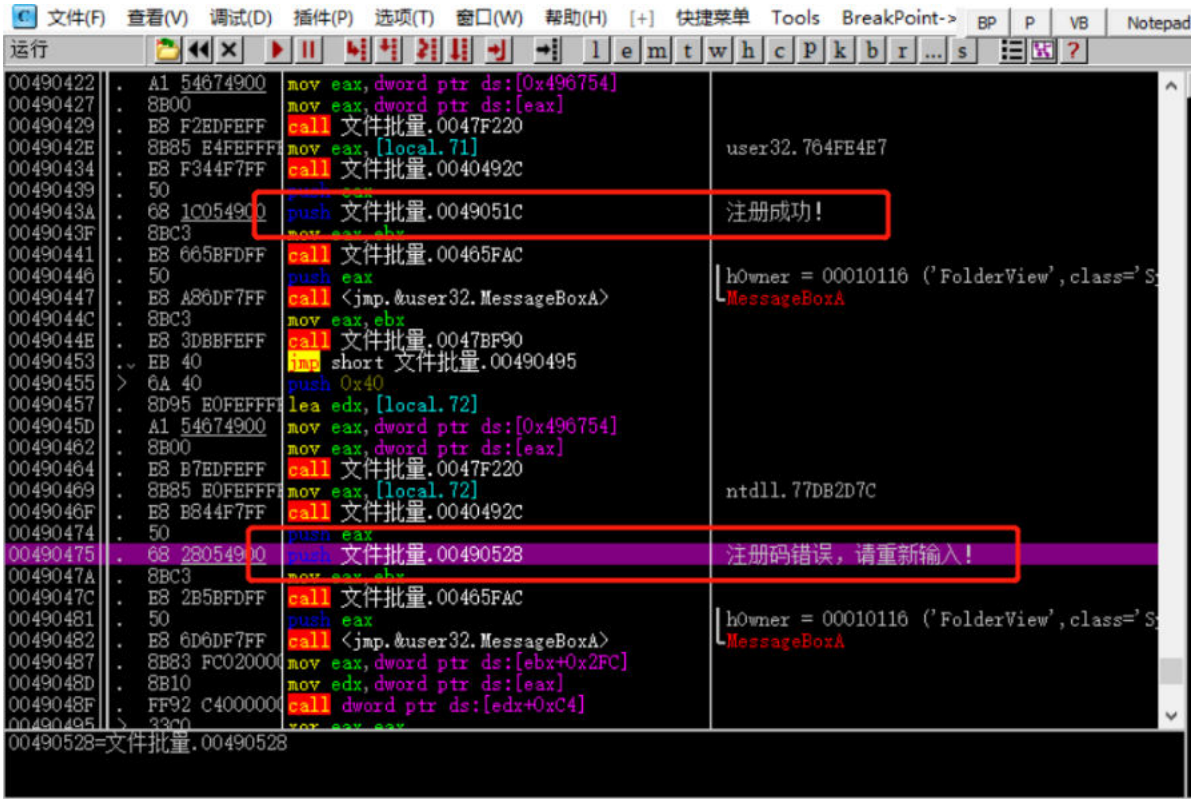
然而因为编码问题，这样搜并不能搜到。

- （回到反汇编窗口） `右键` → `中文搜索引擎` → `搜索ASCII` → `Find`



此时看到，打印 `注册成功` 和 `注册码错误` 的地址分别为 `0049043A` 和 `00490475`

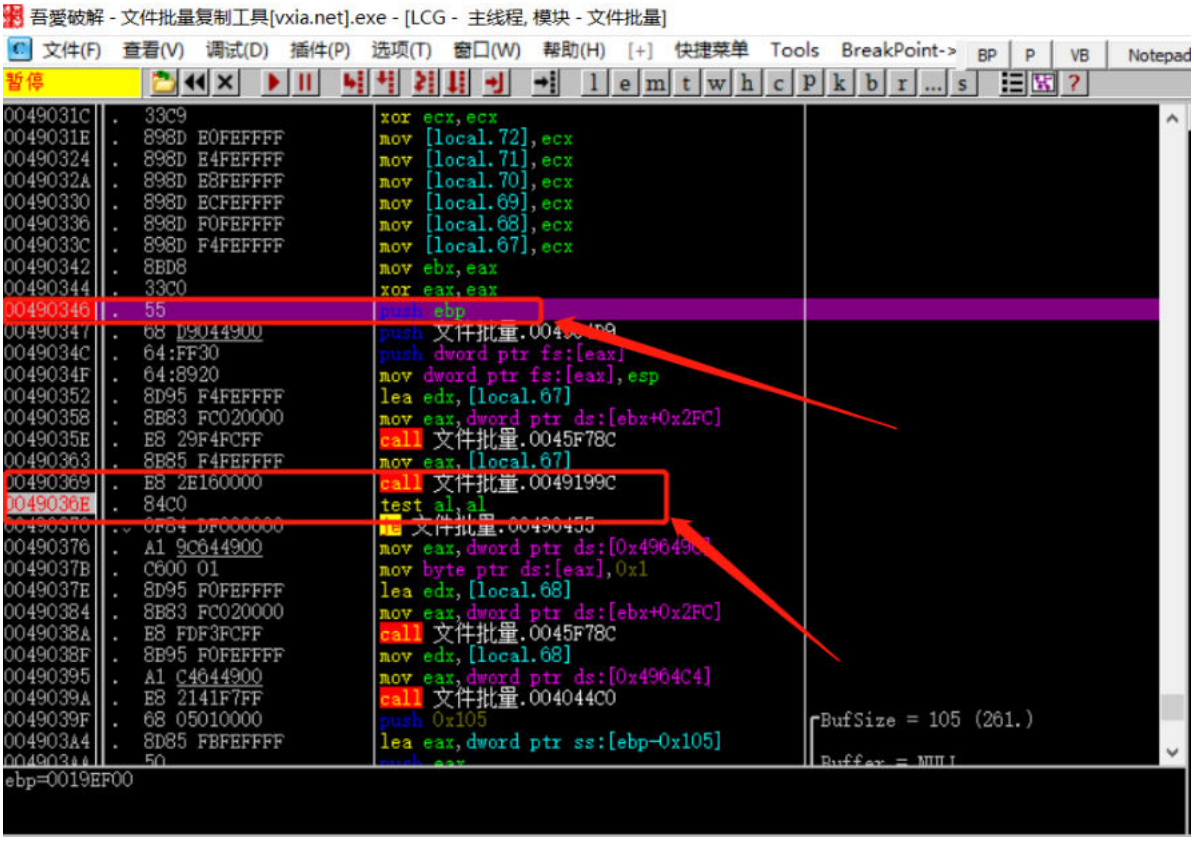
双击 `00490475`，进入该段观察汇编代码：



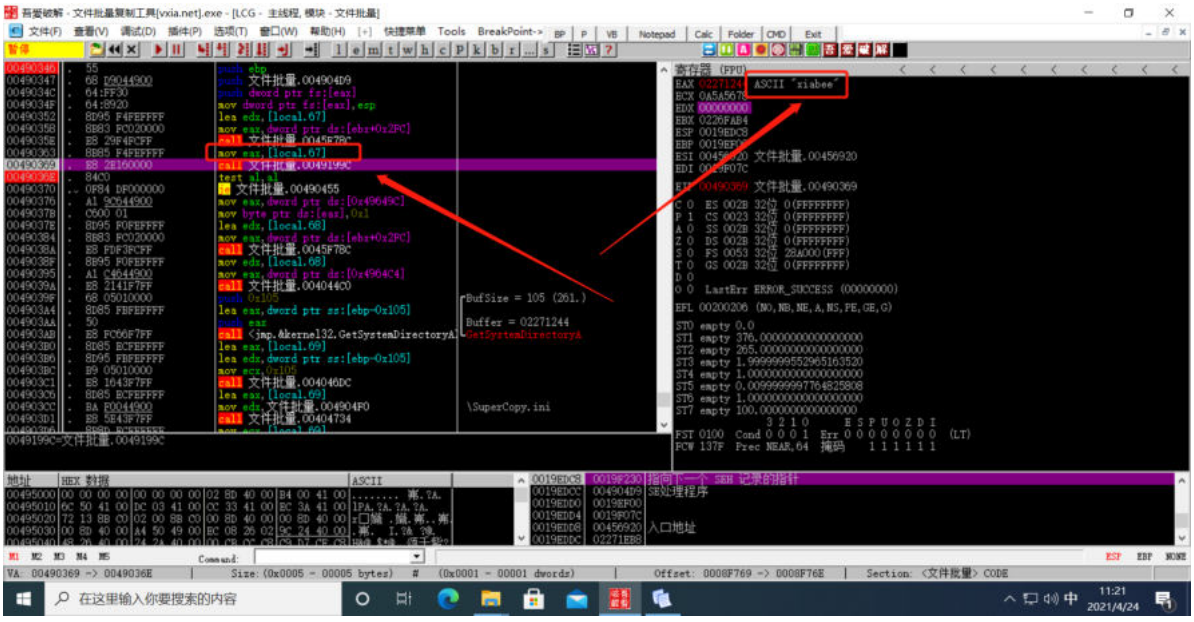
4、设置断点

在 `注册成功` 之前，找到最近的跳转指令 `je`：在 `00490370` 处，不妨假设此跳转为判断注册码的跳转，再不妨假设其上一条指令 `test` 为检验注册码，在此处处设置断点（F2）

同时找到较近的 `push ebp` 指令，在该处设置断点：

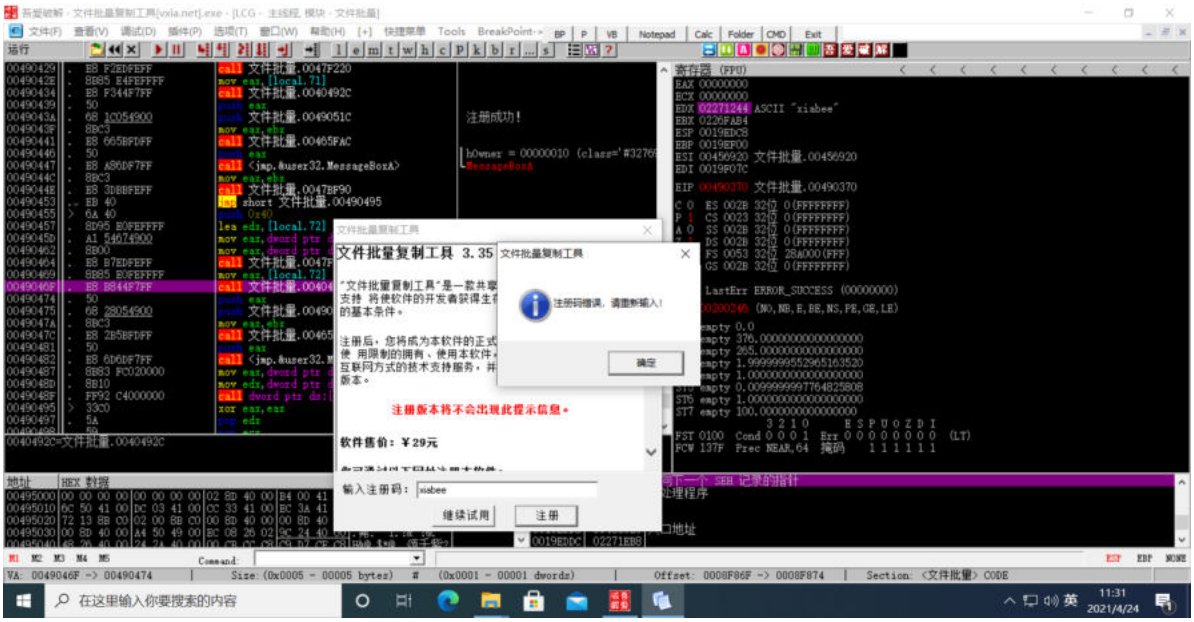


重新载入，`F9`运行到断点处，`F8`进行单步调试，观察寄存器的变化：



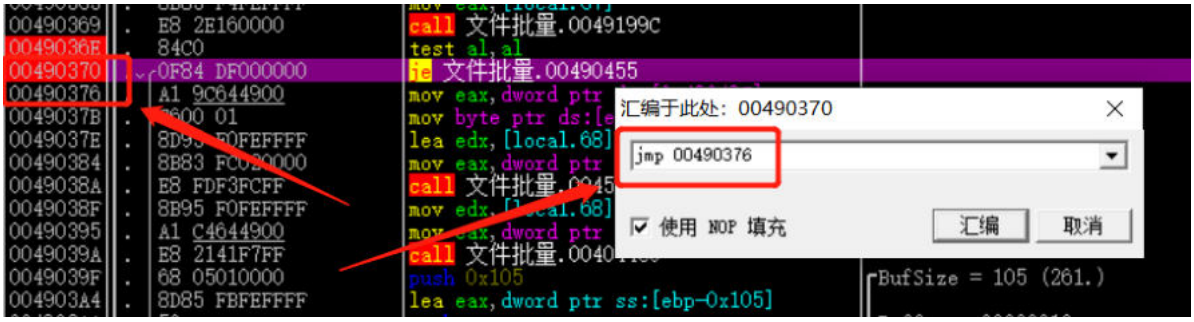
在`00490363`处的`mov`指令执行后，寄存器`EAX`被赋值为`xiabee`；

继续单步调试，发现在`00490370`条件跳转指令`je`执行成功：跳转到`00490455`，执行注册失败部分：



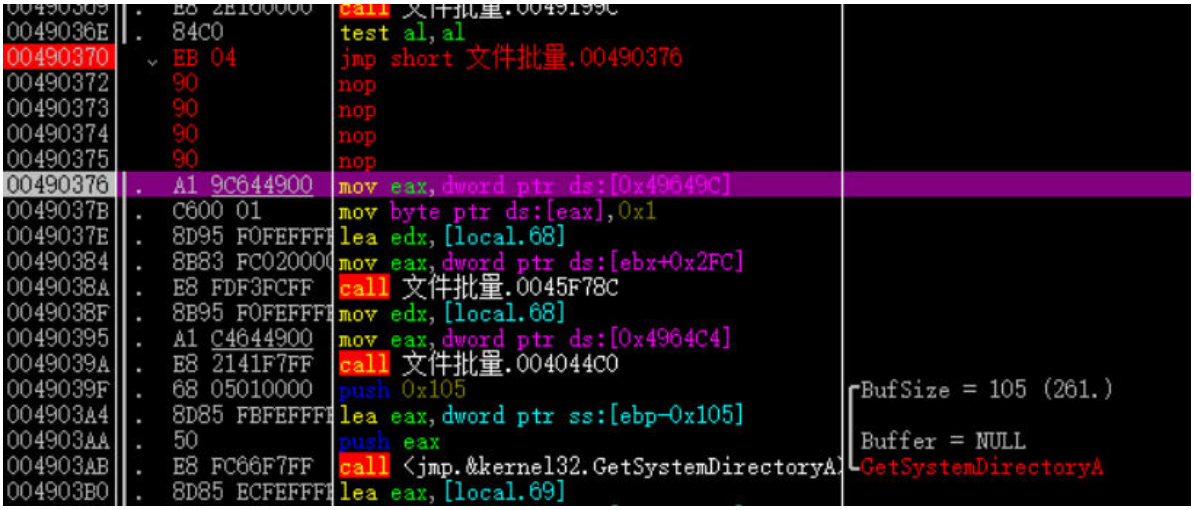
5、修改跳转地址强行破解

由于这个程序逻辑过于简单，没有做跳转验证，我们直接修改跳转地址：不妨假设刚刚跳过的指令为注册成功的指令，我们直接改为跳转到下一条指令`00490376`，并把条件跳转改为无条件跳转`jmp`，同时使用空指令填充空缺：`jmp 00490376`

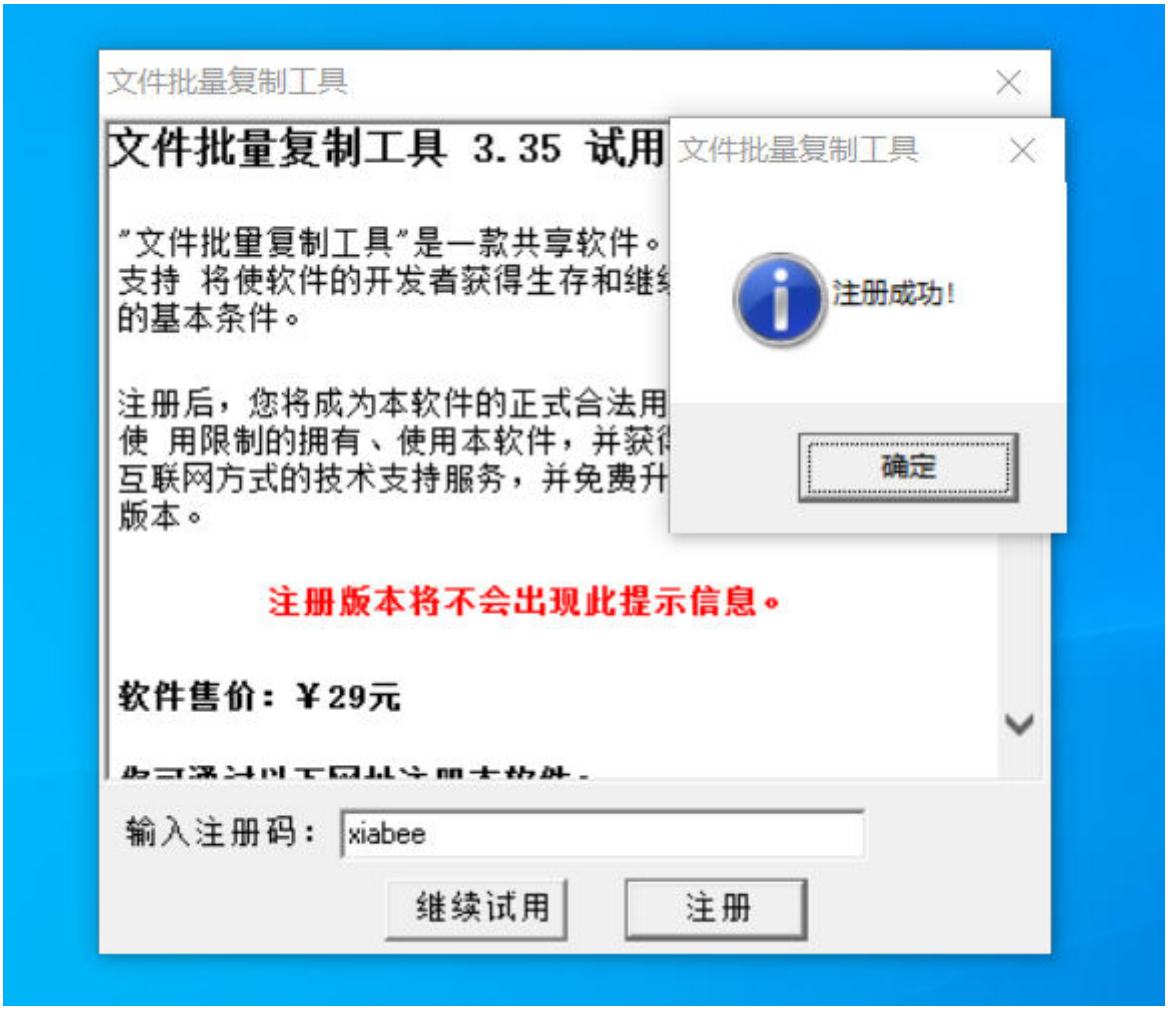


- 此处也可将`JE`设置为`NOP`，直接执行下一步

继续单步调试：此时已经进入`00490376`

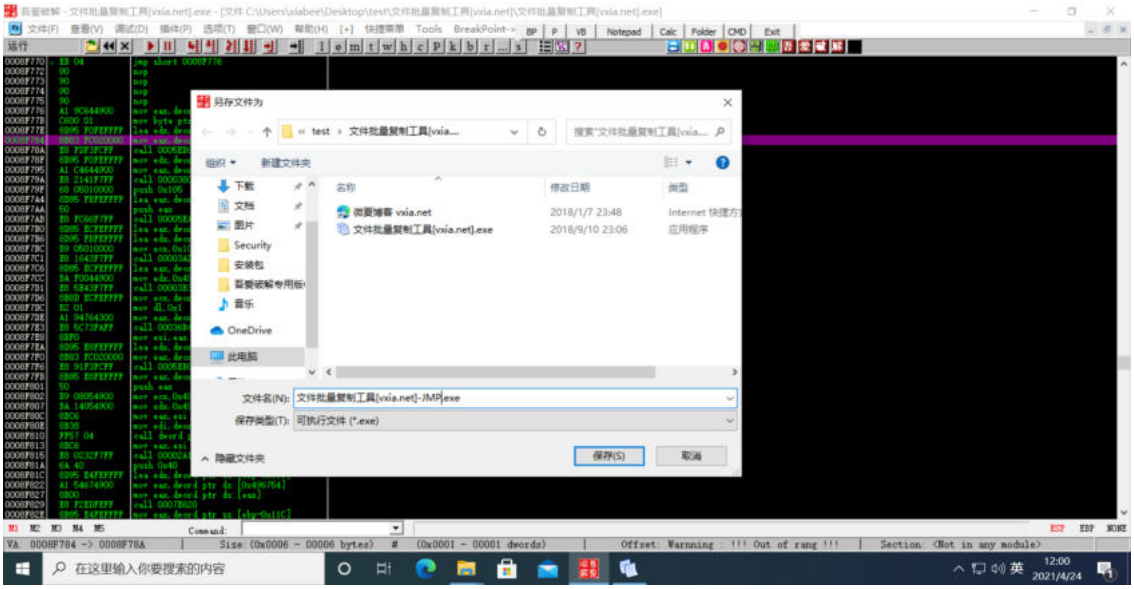


继续执行，注册成功：



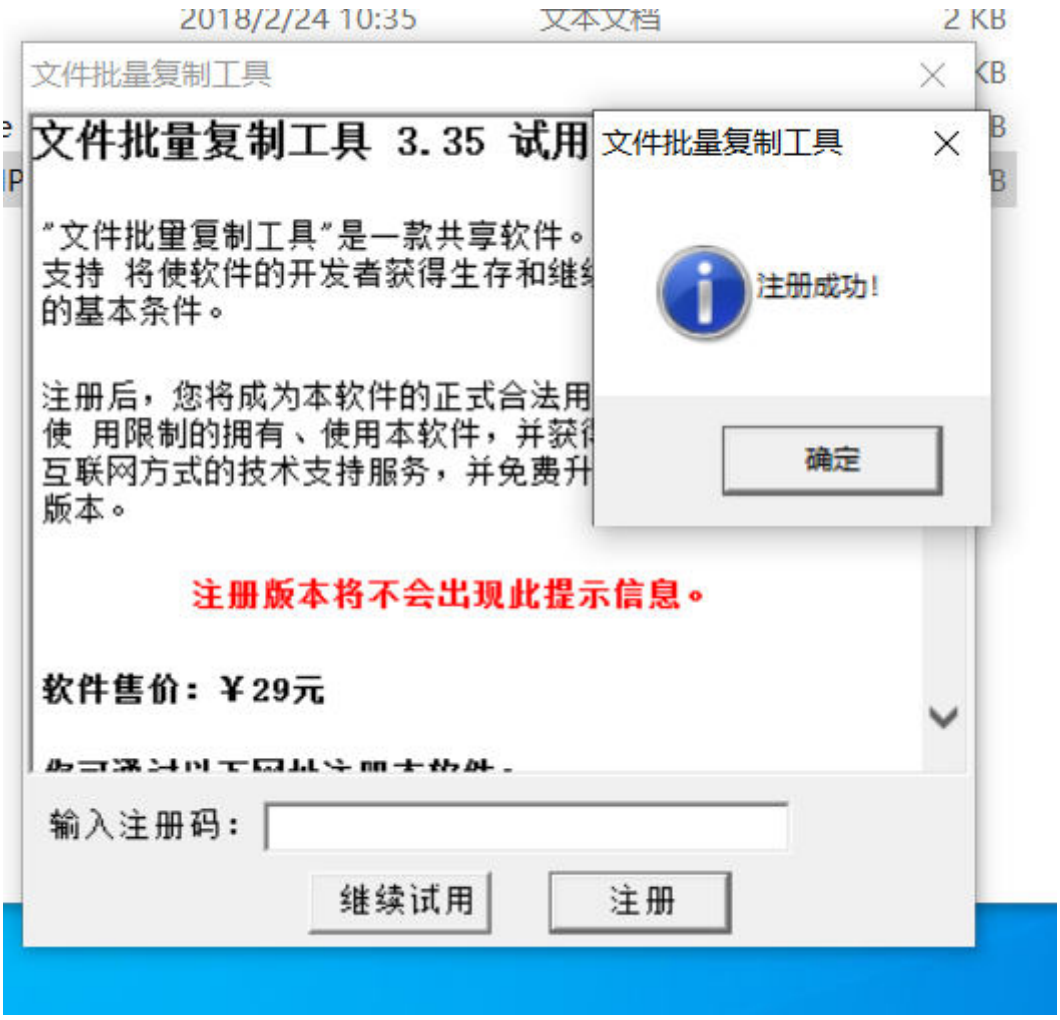
6、保存更改

- 反汇编窗口右键 → 复制到可执行文件 → 所有修改 → 全部复制 → 右键 → 保存文件



####

0x02 实验结果



随意输入注册码，直接注册：注册成功

0x03 实验心得

- 反汇编需要有耐心，汇编代码的阅读以及地址的观察比较费时
- 注册验证不要直接使用`JE`等指令，容易被发现，然后被破解