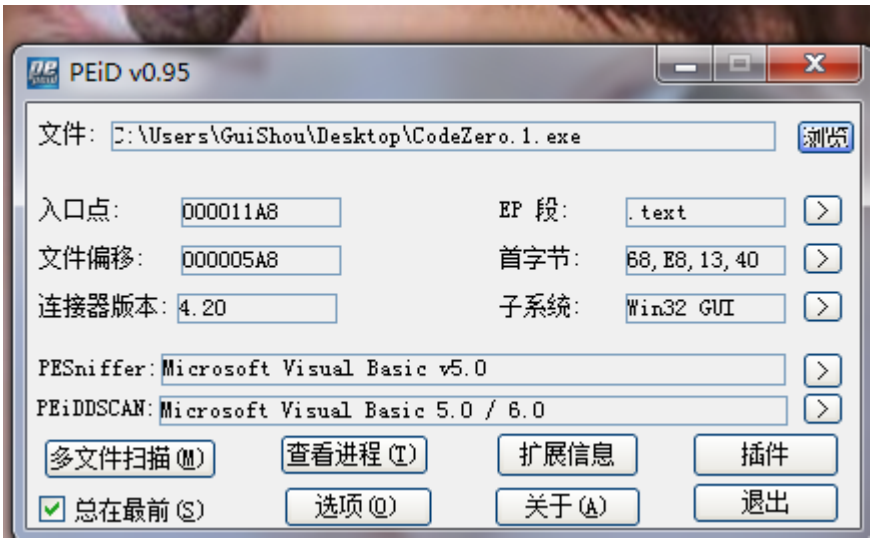
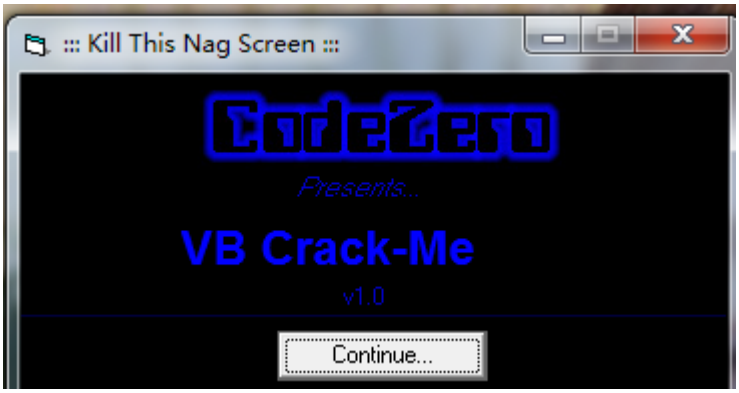
查壳



这个Crackme是VB5写的 没有壳

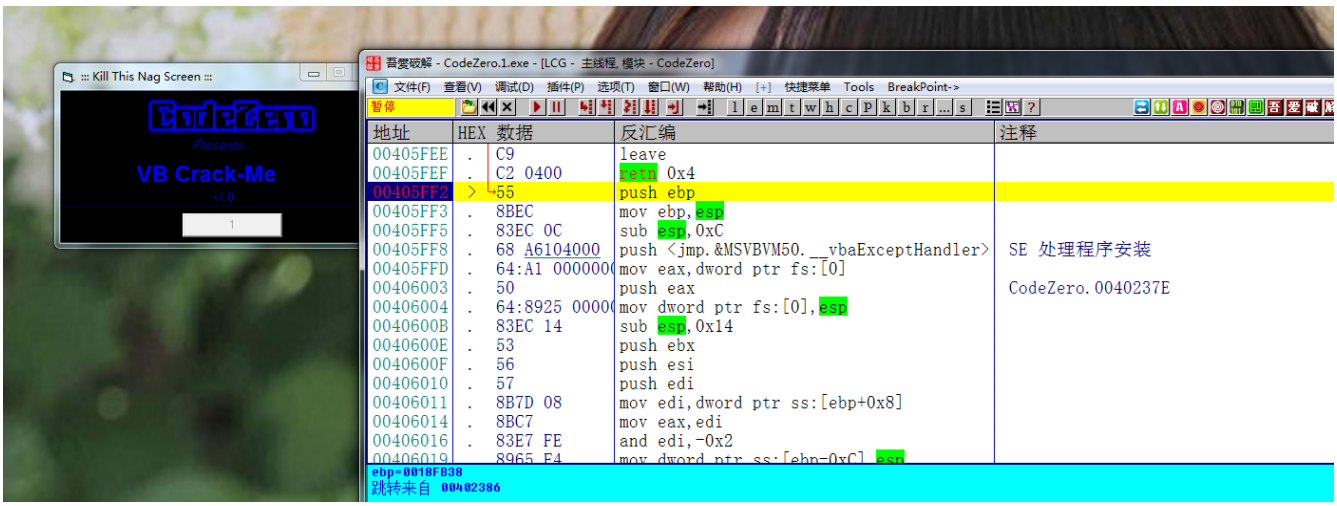
去Neg



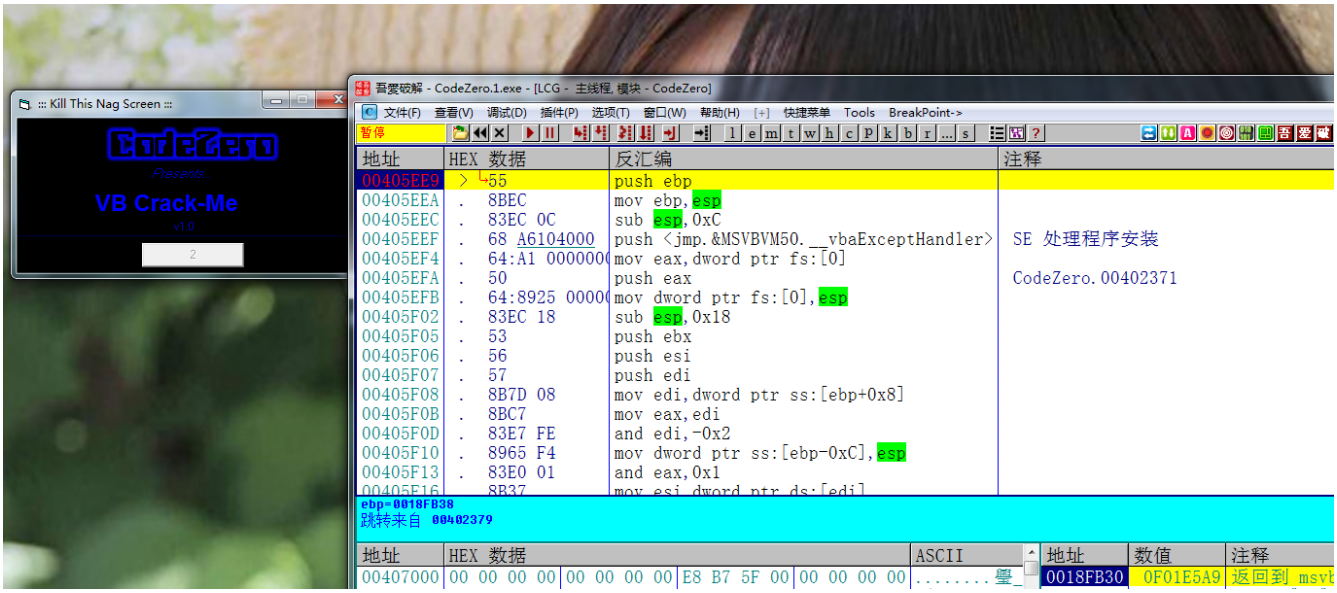
第一个任务就是去除这个倒计时五秒的Neg窗口，去除的思路就是通过字符串的提示向上找到窗体一的加载事件，然后去除

```
0406032  .   8B86 00030000  mov eax,dword ptr ds:[esi+0x300]
0406038  .   8365 E8 00     and dword ptr ss:[ebp-0x18],0x0
040603C  .   57             push edi
040603D  .   FFD0           call eax                          CodeZero.00401DA2
040603F  .   50             push eax                          CodeZero.00401DA2
0406040  .   8D45 E8        lea eax,dword ptr ss:[ebp-0x18]
0406043  .   50             push eax                          CodeZero.00401DA2
0406044  .   E8 17B1FFFF    call <jmp.&MSVBVM50.__vbaObjSet>
0406049  .   8BD8           mov ebx,eax                       CodeZero.00401DA2
040604B  .   68 B0294000    push CodeZero.004029B0            Continue...
0406050  .   53             push ebx
0406051  .   8B03           mov eax,dword ptr ds:[ebx]
0406053  .   FF50 54        call dword ptr ds:[eax+0x54]
0406056  .   85C0           test eax,eax                      CodeZero.00401DA2
0406058  .v  7D 0E          jge short CodeZero.00406068
040605A  .   6A 54          push 0x54
040605C  .   68 8C294000    push CodeZero.0040298C
0406061  .   53             push ebx
```

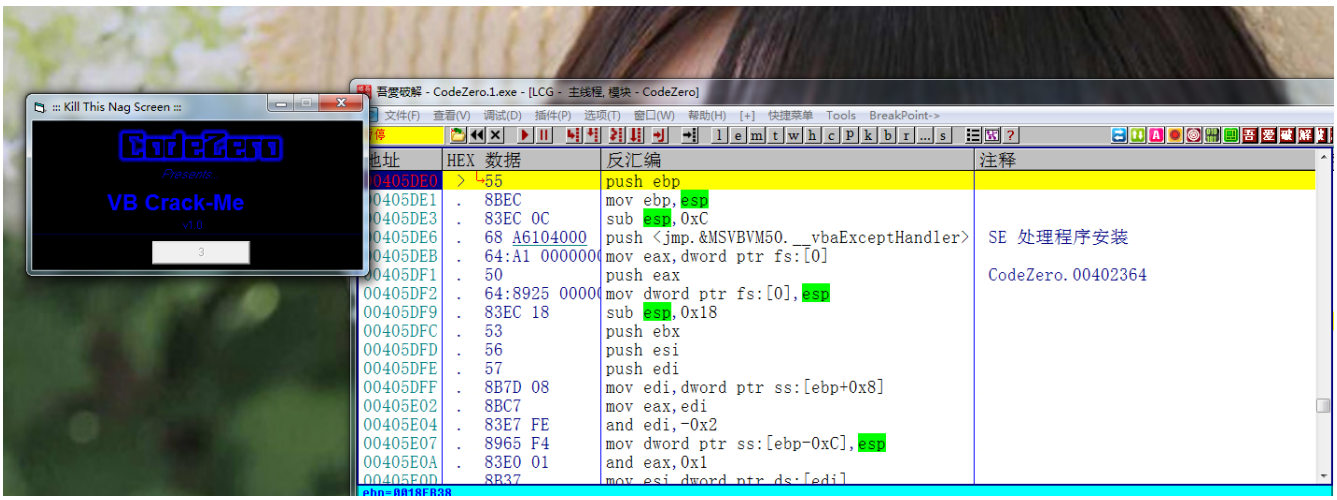
首先来到字符串的提示的地方，向上滚找到函数开头，下断点



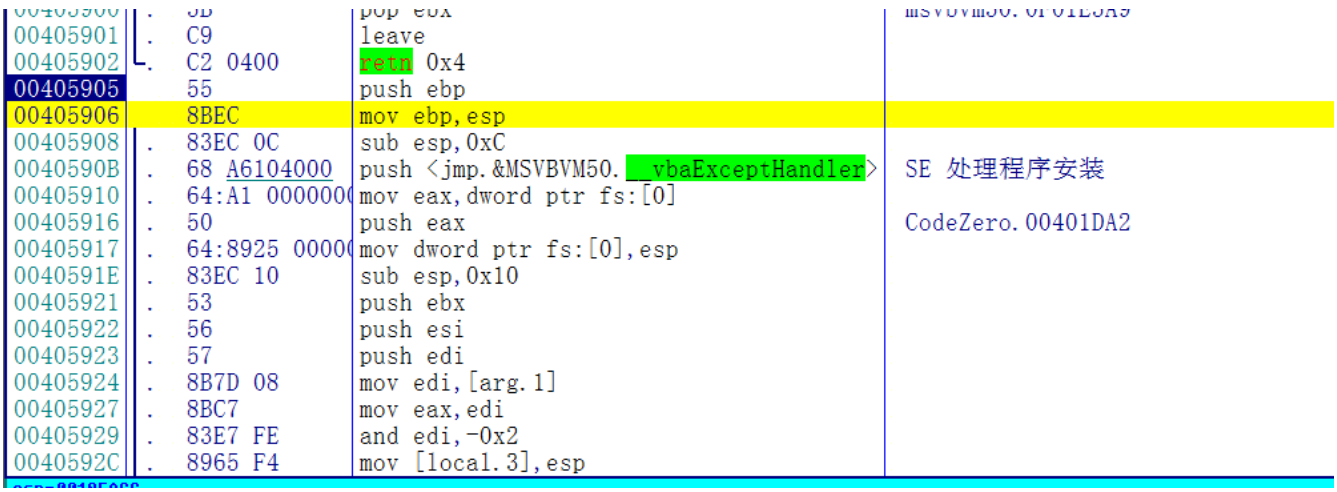
程序断下来时倒计时为1秒，窗体加载完成，所以这里肯定不是，所以我们需要继续往上翻，再找到上一个函数，下断点



断下之后，倒计时为2秒，继续往上找函数头，下断点



断下之后，倒计时为3秒，也不是这，但是我们显然已经找到了规律，每经过一个函数，倒计时减一，继续往上找，直到达到这个地方，程序断下时，窗体还没有加载出来



函数尾的位置是ret 0x4

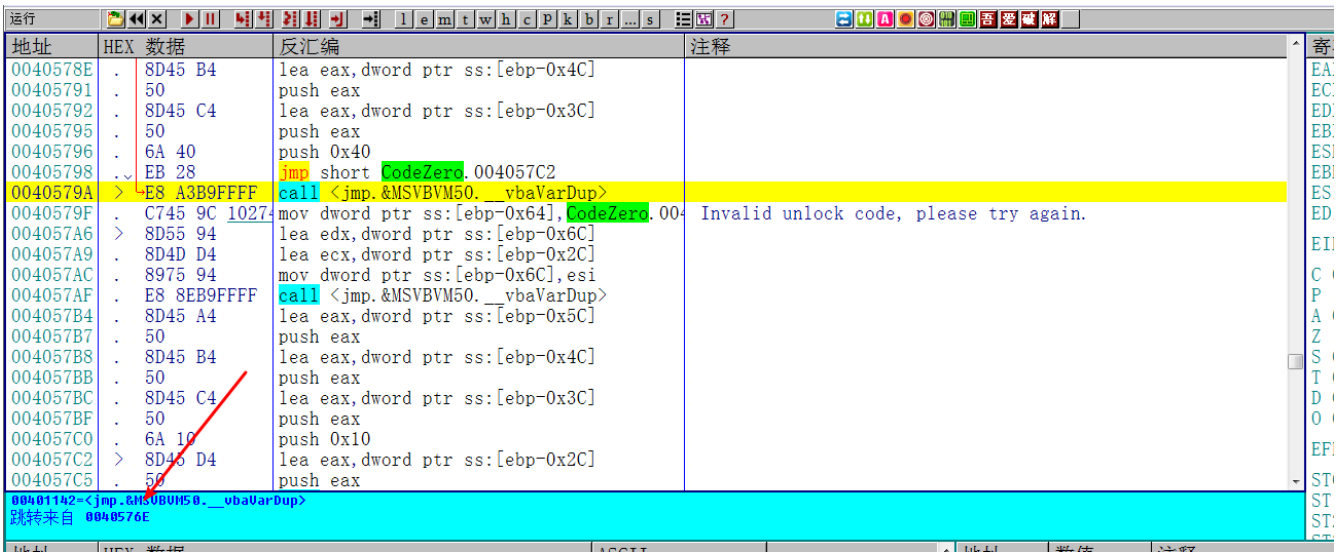
```
地址      HEX 数据        反汇编                                  注释
004059A5  .   8B45 08     mov eax,[arg.1]
004059A8  .   50          push eax                                CodeZero.00
004059A9  .   8B08        mov ecx,dword ptr ds:[eax]
004059AB  .   FF51 08     call dword ptr ds:[ecx+0x8]
004059AE  .   8B4D EC     mov ecx,[local.5]                       CodeZero.00
004059B1  .   8B45 FC     mov eax,[local.1]
004059B4  .   5F          pop edi                                 msvbvm50.0F
004059B5  .   5E          pop esi                                 msvbvm50.0F
004059B6  .   64:890D 0000mov dword ptr fs:[0],ecx
004059BD  .   5B          pop ebx                                 msvbvm50.0F
004059BE  .   C9          leave
004059BF  .   C2 0400     retn 0x4
```

所以只要把函数头的位置修改位retn 0x4，保存文件即可，修改后如下

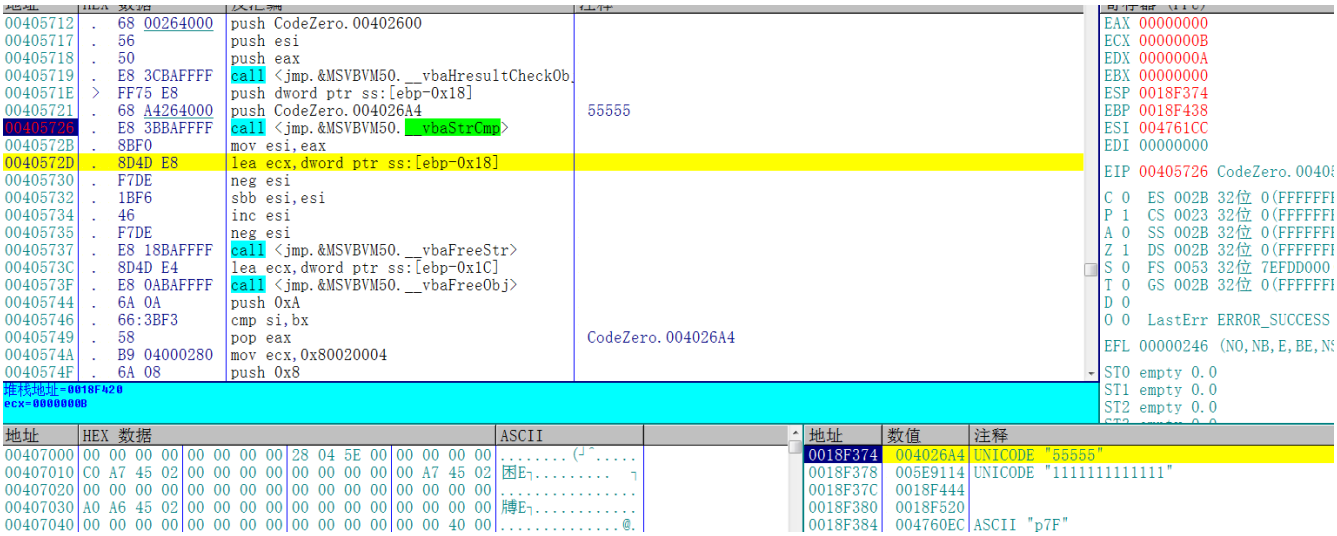
```
地址      HEX 数据        反汇编                                  注释
004058E8  .   8B45 08     mov eax,[arg.1]
004058EB  .   50          push eax                                CodeZero.00402364
004058EC  .   8B08        mov ecx,dword ptr ds:[eax]
004058EE  .   FF51 08     call dword ptr ds:[ecx+0x8]
004058F1  .   8B4D EC     mov ecx,[local.5]                       CodeZero.00401050
004058F4  .   8B45 FC     mov eax,[local.1]
004058F7  .   5F          pop edi                                 msvbvm50.0F01E5A9
004058F8  .   5E          pop esi                                 msvbvm50.0F01E5A9
004058F9  .   64:890D 0000mov dword ptr fs:[0],ecx
00405900  .   5B          pop ebx                                 msvbvm50.0F01E5A9
00405901  .   C9          leave
00405902  .   C2 0400     retn 0x4
00405905      C2 0400     retn 0x4
00405908  .   83EC 0C     sub esp,0xC
0040590B  .   68 A6104000 push <jmp.&MSVBVM50.__vbaExceptHandler>  SE 处理程序安装
00405910  .   64:A1 000000mov eax,dword ptr fs:[0]
00405916  .   50          push eax                                CodeZero.00402364
00405917  .   64:8925 0000mov dword ptr fs:[0],esp
0040591E  .   83EC 10     sub esp,0x10
00405921  .   53          push ebx
00405922  .   56          push esi
返回到 0F01E5A9 (msvbvm50.0F01E5A9)
```

Neg完美去除

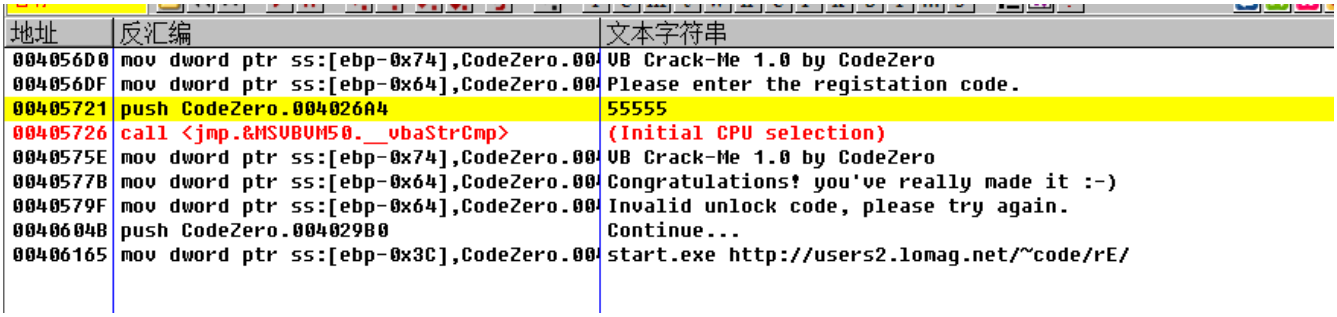
追踪Serial



根据字符串提示找到跳转到错误提示的地址，跟进去



找到这个比较函数，下断点，看参数，那么序列号已经很明显了，就是55555



其实一开始在字符串里就搜到了，只不过不确定而已 哈哈

最后，需要相关文件的可以到我的Github下载：https://github.com/TonyChen56/160-Crackme