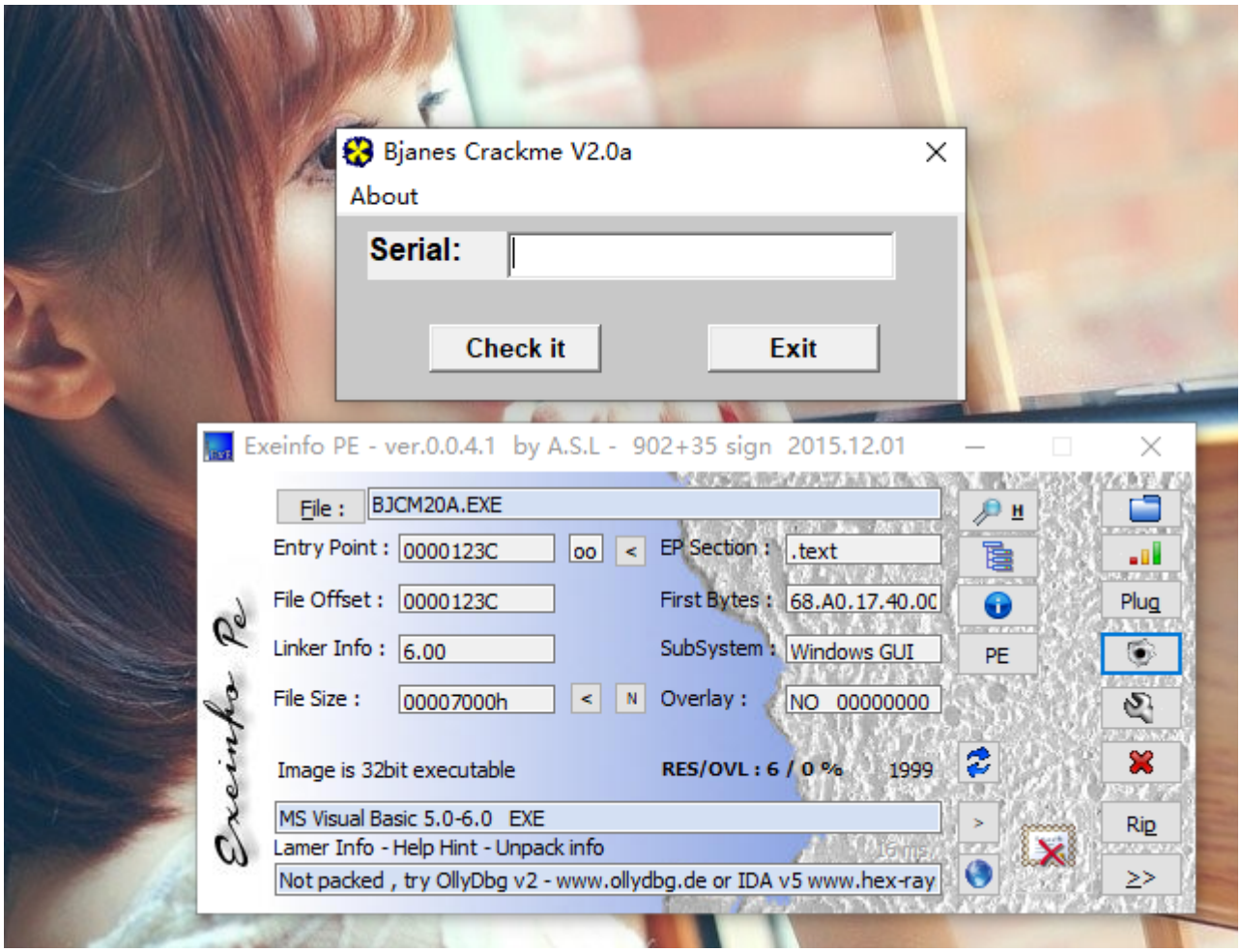
查壳



这个和014那个Crackme是同一个作者，连图标都没换，估计是同一个工程编译出来的，就换了下算法

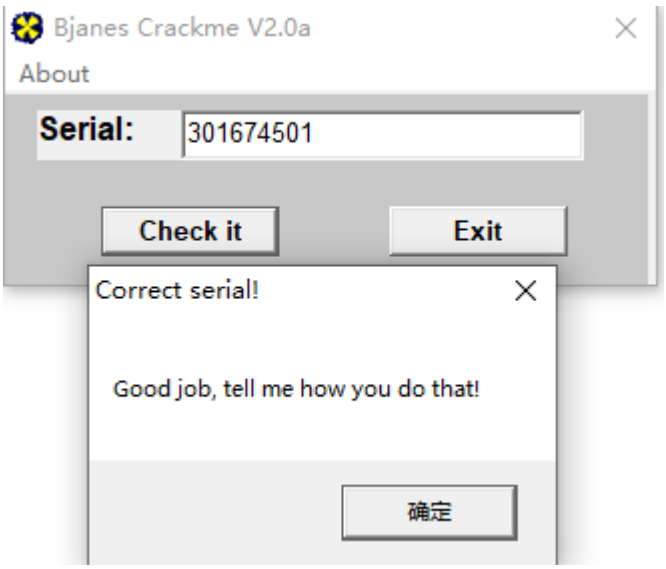
分析程序

```
00403A37   .  894D A8       mov dword ptr ss:[ebp-0x58],ecx
00403A3A   .  BF 08000000   mov edi,0x8
00403A3F   .  8D95 50FFFFFF lea edx,dword ptr ss:[ebp-0xB0]
00403A45   .  8D4D B0       lea ecx,dword ptr ss:[ebp-0x50]
00403A48   .  8945 90       mov dword ptr ss:[ebp-0x70],eax
00403A4B   .  8945 A0       mov dword ptr ss:[ebp-0x60],eax
00403A4E   .  C785 58FFFFFF mov dword ptr ss:[ebp-0xA8],BJCM20A.004022F0  Wrong serial!
00403A58   .  89BD 50FFFFFF mov dword ptr ss:[ebp-0xB0],edi
00403A5E   .  FFD6          call esi                                      ntdll.77C40BA0; <&MSVBVM60.__vbaVa
00403A60   .  8D95 60FFFFFF lea edx,dword ptr ss:[ebp-0xA0]
00403A66   .  8D4D C0       lea ecx,dword ptr ss:[ebp-0x40]
00403A69   .  C785 68FFFFFF mov dword ptr ss:[ebp-0x98],BJCM20A.004022C8  Sorry, try again!
00403A73   .  89BD 60FFFFFF mov dword ptr ss:[ebp-0xA0],edi
00403A79   .  FFD6          call esi                                      ntdll.77C40BA0
00403A7B   .  8D45 90       lea eax,dword ptr ss:[ebp-0x70]
004022C8=BJCM20A.004022C8 (UNICODE "Sorry, try again!")
```

直接来到错误提示的地方，向上跟踪

```
文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H) [+] 快捷菜单 Tools BreakPoint->
运行
地址     HEX 数据    反汇编                                          注释
00403A18   .  8945 E8       mov dword ptr ss:[ebp-0x18],eax
00403A1B   .  33DB          xor ebx,ebx
00403A1D   .^ E9 5AFDFFFF   jmp BJCM20A.0040377C
00403A22   >  33DB          xor ebx,ebx
00403A24   >  8B35 A4104000 mov esi,dword ptr ds:[<&MSVBVM60.__vbaVarDup>]  msvbvm60.__vbaVar
00403A2A   .  B9 04000280   mov ecx,0x80020004
00403A2F   .  894D 98       mov dword ptr ss:[ebp-0x68],ecx
00403A32   .  B8 0A000000   mov eax,0xA
00403A37   .  894D A8       mov dword ptr ss:[ebp-0x58],ecx
00403A3A   .  BF 08000000   mov edi,0x8
00403A3F   .  8D95 50FFFFFF lea edx,dword ptr ss:[ebp-0xB0]
00403A45   .  8D4D B0       lea ecx,dword ptr ss:[ebp-0x50]
00403A48   .  8945 90       mov dword ptr ss:[ebp-0x70],eax
00403A4B   .  8945 A0       mov dword ptr ss:[ebp-0x60],eax
00403A4E   .  C785 58FFFFFF mov dword ptr ss:[ebp-0xA8],BJCM20A.004022F0  Wrong serial!
ebx=00000000
跳转来自 004038AD, 00403A04
```

一共有三个跳转会到这里，这怎么跟014一模一样，输入之前的序列号试试看



好吧 看来两个是重复的了。。。。。。PASS!

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