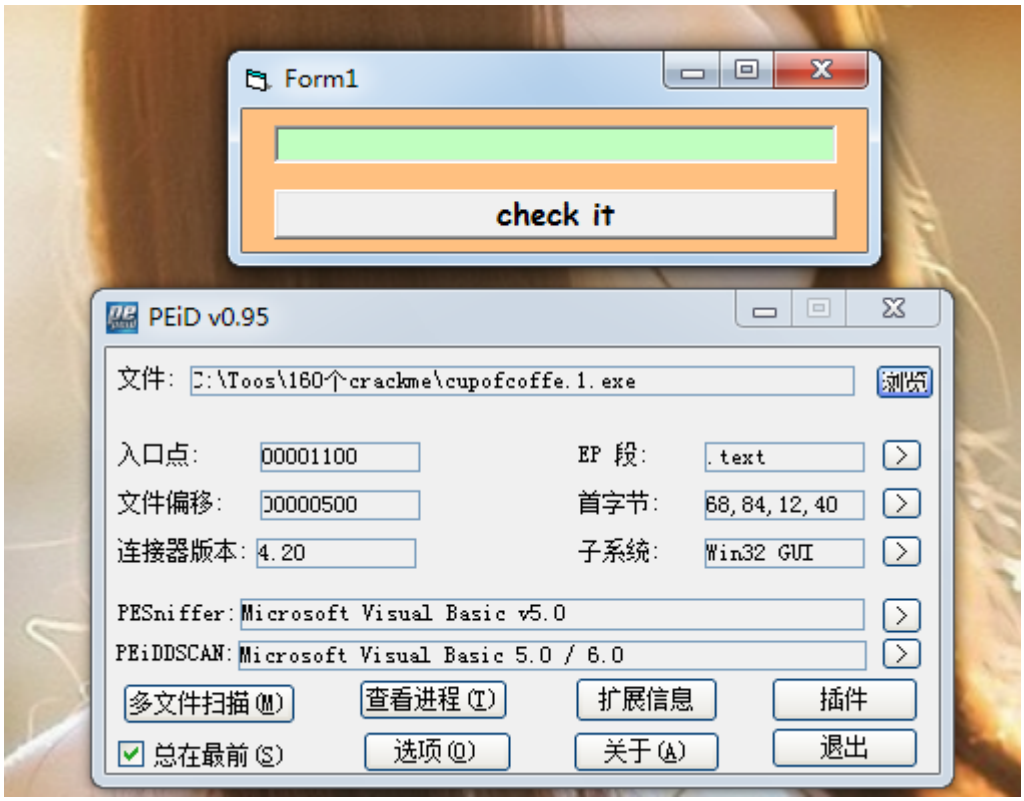
查壳

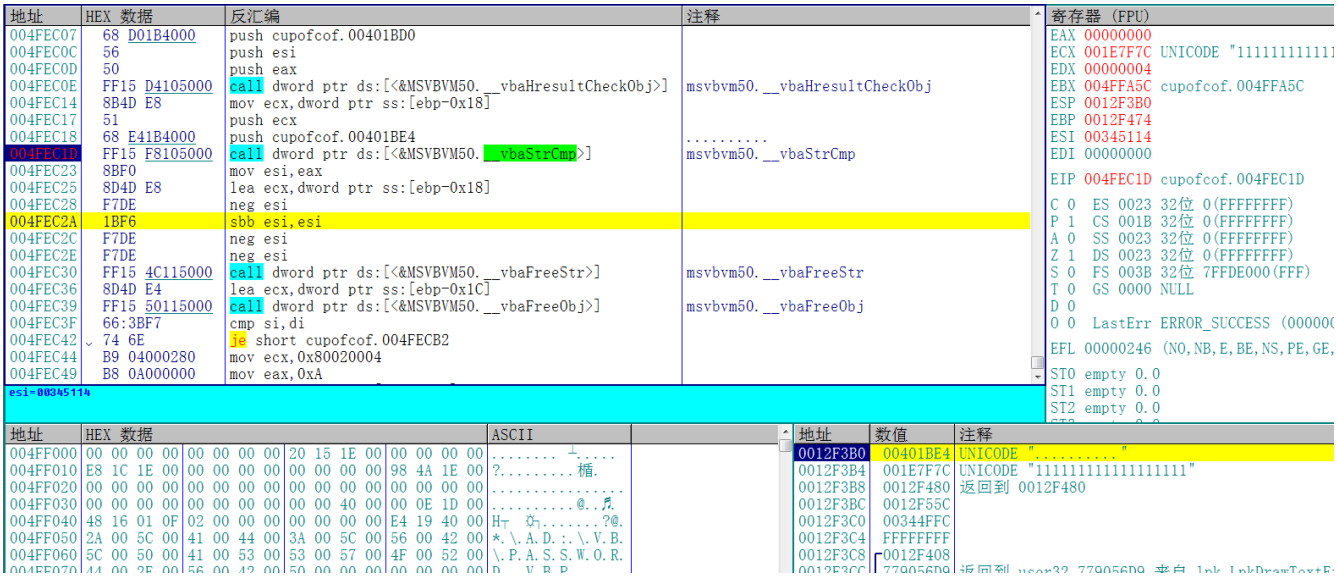


目标程序是一个VB写的，没有加壳。单纯的序列号保护

分析程序

```
004FEC42   74 6E          je short cupofcof.004FECB2
004FEC44   B9 04000280    mov ecx,0x80020004
004FEC49   B8 0A000000    mov eax,0xA
004FEC4E   894D AC        mov dword ptr ss:[ebp-0x54],ecx
004FEC51   894D BC        mov dword ptr ss:[ebp-0x44],ecx
004FEC54   894D CC        mov dword ptr ss:[ebp-0x34],ecx
004FEC57   8D55 94        lea edx,dword ptr ss:[ebp-0x6C]
004FEC5A   8D4D D4        lea ecx,dword ptr ss:[ebp-0x2C]
004FEC5D   8945 A4        mov dword ptr ss:[ebp-0x5C],eax   kernel32.BaseThreadInitThunk
004FEC60   8945 B4        mov dword ptr ss:[ebp-0x4C],eax   kernel32.BaseThreadInitThunk
004FEC63   8945 C4        mov dword ptr ss:[ebp-0x3C],eax   kernel32.BaseThreadInitThunk
004FEC66   C745 9C 001C40 mov dword ptr ss:[ebp-0x64],cupofcof.00401C00   Incorrect password
004FEC6D   C745 94 0800000 mov dword ptr ss:[ebp-0x6C],0x8
004FEC74   FF15 38115000  call dword ptr ds:[<&MSVBVM50.__vbaVarDup>]   msvbvm50.__vbaVarDup
004FEC7A   8D55 A4        lea edx,dword ptr ss:[ebp-0x5C]
004FEC7D   8D45 B4        lea eax,dword ptr ss:[ebp-0x4C]
004FEC80   52             push edx                          cupofcof.<ModuleEntryPoint>
004FEC81   8D4D C4        lea ecx,dword ptr ss:[ebp-0x3C]
004FEC84   50             push eax                          kernel32.BaseThreadInitThunk
00401C00=cupofcof.00401C00 (UNICODE "Incorrect password")
堆栈 ss:[0012FF30]=00000000
地址  HEX 数据  ASCII  地址  数值  注释
```

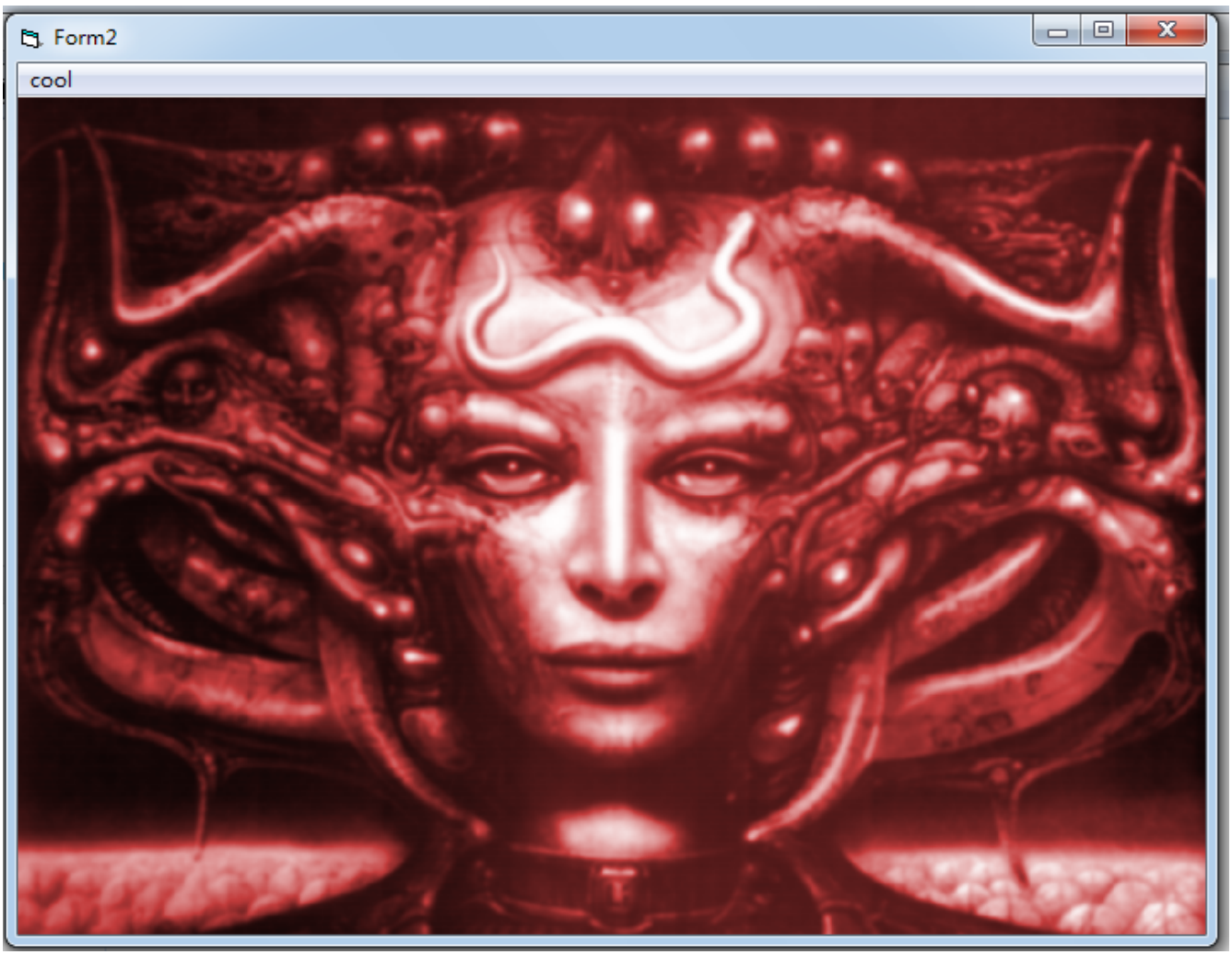
根据字符串的错误提示，跟进去，然后接着向上找。在上面你会发现一个比较函数，下断点，随便输入一个序列号等待程序断下。



看堆栈中有一个自己输入的序列号和一个字符串，这个字符串是十个英文状态下的点(.)。这个作者还是挺有意思的

验证结果

输入刚刚看到的序列号：十个点，记得把输入法调成英文



提示cool，成功了。

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