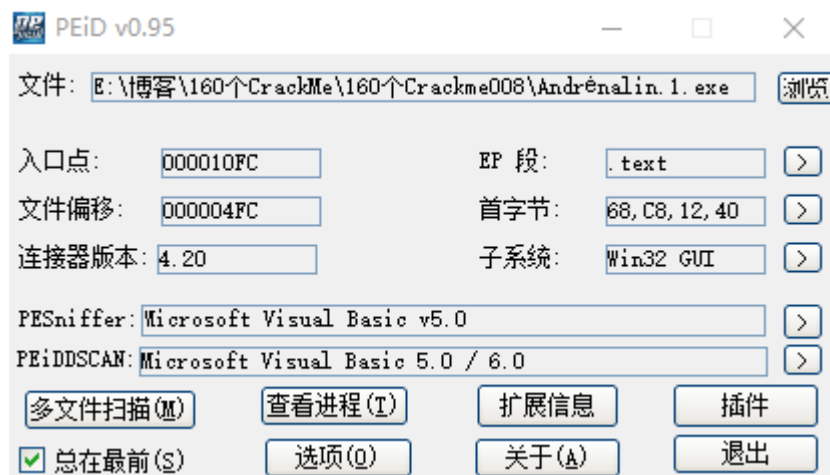


查壳
OD分析
校验密码

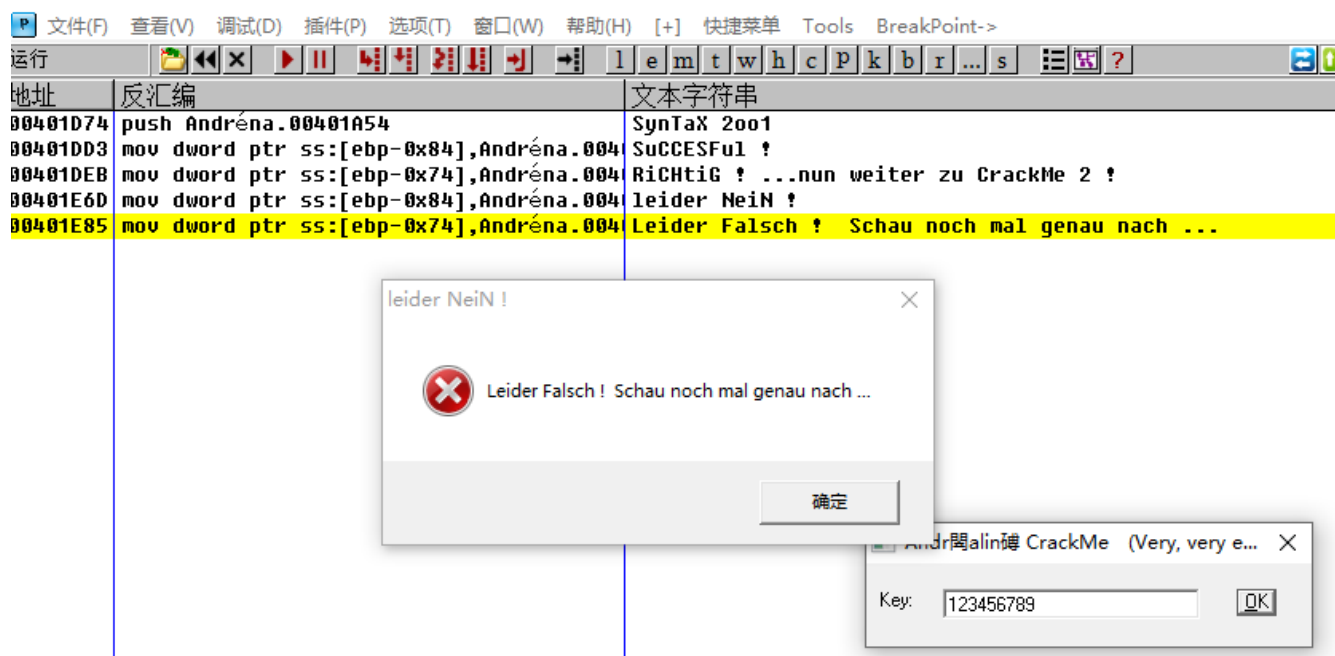
接下来分析008这个crackme，难度是一颗星

查壳



VB写的 没有壳。既然是VB写的程序，那IDA就帮不上什么忙了，VB的反编译工具反编译出来的源码我也看不懂，算了直接上OD吧。

OD分析



首先根据错误提示查找到字符串跟进去，

地址	HEX 数据	反汇编	注释
00401E67	. 8945 94	mov dword ptr ss:[ebp-0x6C],eax	
00401E6A	. 8945 A4	mov dword ptr ss:[ebp-0x5C],eax	
00401E6D	. C785 7CFFFFFF	mov dword ptr ss:[ebp-0x84],Andréna.004	leider Nein !
00401E77	. 899D 74FFFFFF	mov dword ptr ss:[ebp-0x8C],ebx	
00401E7D	. FFD7	call edi	<MSVBVM50.__vbaVarDup>
00401E7F	. 8D55 84	lea ecx,dword ptr ss:[ebp-0x7C]	
00401E82	. 8D4D C4	lea ecx,dword ptr ss:[ebp-0x3C]	
00401E85	. C745 8C E01A	mov dword ptr ss:[ebp-0x74],Andréna.004	Leider Falsch ! Schau noch mal genau
00401E8C	. 895D 84	mov dword ptr ss:[ebp-0x7C],ebx	
00401E8F	. FFD7	call edi	错误提示
00401E91	. 8D4D 94	lea ecx,dword ptr ss:[ebp-0x6C]	
00401E94	. 8D55 A4	lea ecx,dword ptr ss:[ebp-0x5C]	
00401E97	. 51	push ecx	

edi=02261D8C

这里是报错的地方，一步一步往上跟，看看到底是什么地方跳转到这里的。

地址	HEX 数据	反汇编	注释
00401E3D	. 50	push eax	
00401E3E	. E9 95000000	jmp Andréna.00401ED8	
00401E43	. 8B3D 48314000	mov edi,dword ptr ds:[<MSVBVM50.__vbaVarDup>]	MSVBVM50.__vbaVarDup
00401E49	. B9 04000280	mov ecx,0x80020004	
00401E4E	. 894D 9C	mov dword ptr ss:[ebp-0x64],ecx	
00401E51	. B8 0A000000	mov eax,0xA	
00401E56	. 894D AC	mov dword ptr ss:[ebp-0x54],ecx	
00401E59	. BB 08000000	mov ebx,0x8	
00401E5E	. 8D95 74FFFFFF	lea edx,dword ptr ss:[ebp-0x8C]	
00401E64	. 8D4D B4	lea ecx,dword ptr ss:[ebp-0x4C]	
00401E67	. 8945 94	mov dword ptr ss:[ebp-0x6C],eax	
00401E6A	. 8945 A4	mov dword ptr ss:[ebp-0x5C],eax	
00401E6D	. C785 7CFFFFFF	mov dword ptr ss:[ebp-0x84],Andréna.004	leider Nein !
00401E77	. 899D 74FFFFFF	mov dword ptr ss:[ebp-0x8C],ebx	

ds:[00403148]=741C0C68 (MSVBVM50.__vbaVarDup)
edi=001B0792
跳转来自 00401D9D

地址	数值	注释
00401D9D	00000000	

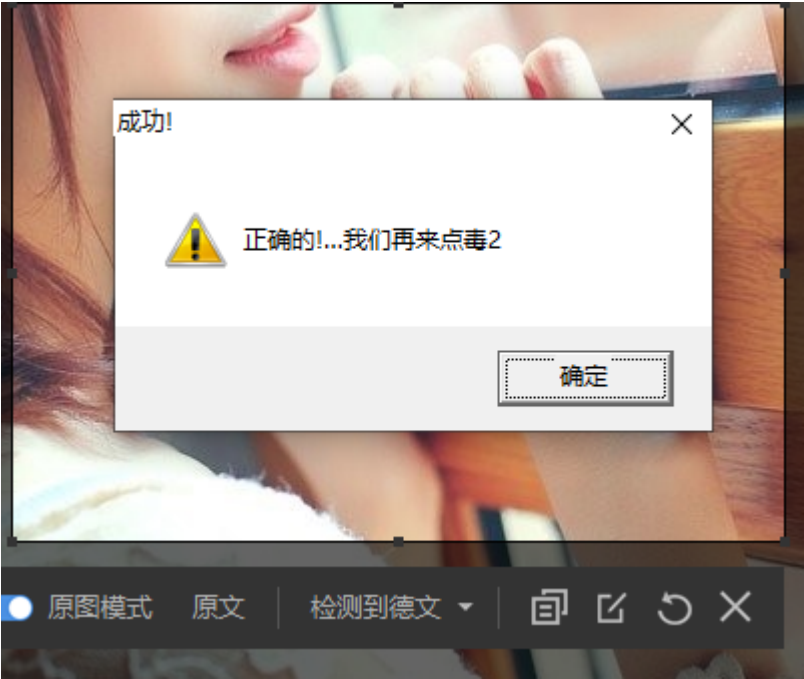
紧接着就看到这个地址的跳转是来自00401D9D，OK继续跟来到00401D9D

地址	HEX 数据	反汇编	注释
00401D88	. 47	inc edi	
00401D89	. F7DF	neg edi	
00401D8B	. FF15 5C314000	call dword ptr ds:[<MSVBVM50.__vbaFreeStr>]	MSVBVM50.__vbaFreeStr
00401D91	. 8D4D D4	lea ecx,dword ptr ss:[ebp-0x2C]	
00401D94	. FF15 60314000	call dword ptr ds:[<MSVBVM50.__vbaFreeObj>]	MSVBVM50.__vbaFreeObj
00401D99	. 66:3BFE	cmp di,si	
00401D9D	. 0F84 A0000000	je Andréna.00401E43	
00401DA3	. FF15 2C314000	call dword ptr ds:[<MSVBVM50.#rtcBeep>]	MSVBVM50.rtcBeep
00401DA9	. 8B3D 48314000	mov edi,dword ptr ds:[<MSVBVM50.__vbaVarDup>]	MSVBVM50.__vbaVarDup
00401DAF	. B9 04000280	mov ecx,0x80020004	
00401DB4	. 894D 9C	mov dword ptr ss:[ebp-0x64],ecx	
00401DB7	. B8 0A000000	mov eax,0xA	
00401DBC	. 894D AC	mov dword ptr ss:[ebp-0x54],ecx	
00401DBF	. BB 08000000	mov ebx,0x8	

跳转未实现
00401E43=Andréna.00401E43

地址	数值	注释
00402000	00000000	

这里会比较di和si，手动把ZF标志位修改下不让程序跳转，看看什么情况

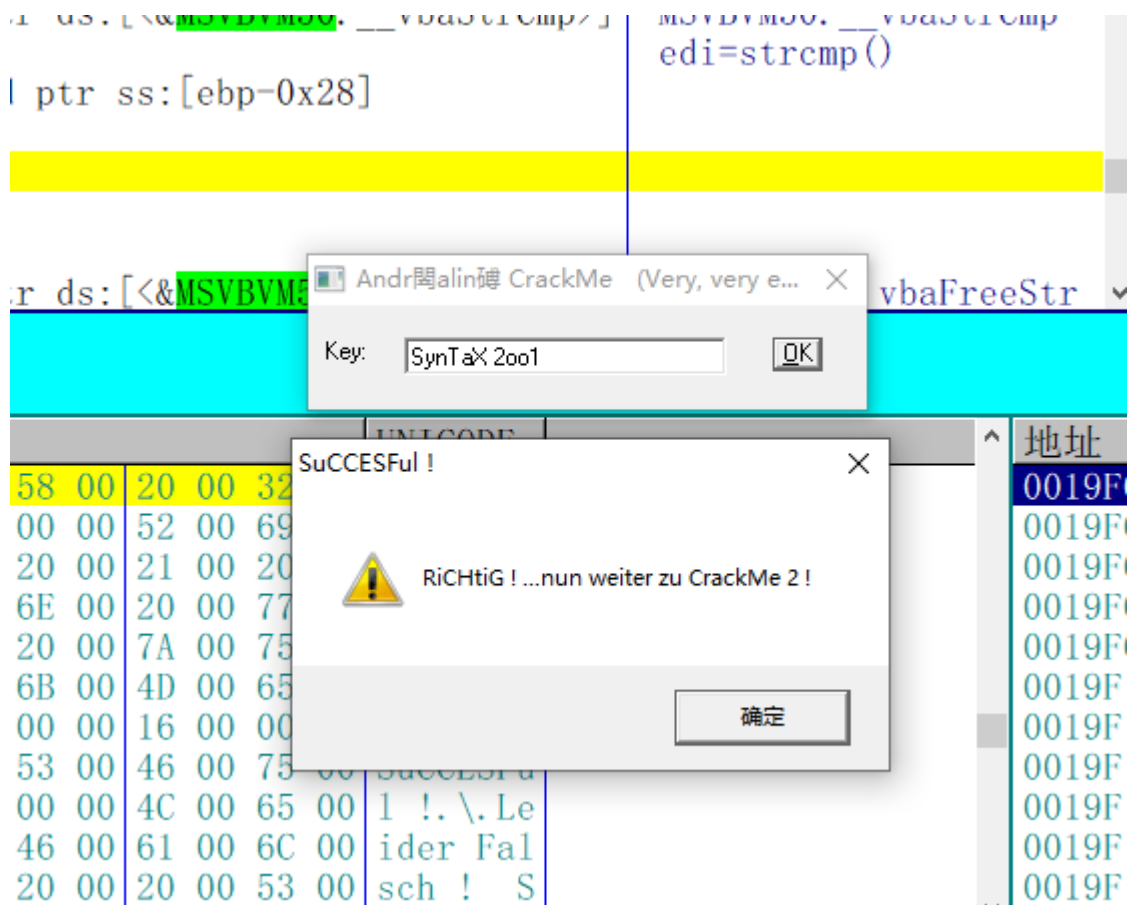


OK，提示成功了，那么再往上跟

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 BreakPoint->									
[图标] [

这里有一个比较，将ecx也就是输入的密码和硬编码的一个字符串SynTaX 2ool做比较，再将结果保存到edi，基于刚刚看到的di和si的比较，那么基本就可以确定这个字符串就是密码了。

校验密码



输入拿到的字符串，点击OK，提示成功。这个crackme也就完成了。果然是一星难度，没有坑我。

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