

查壳  
OD脱壳  
修复导入表  
修复程序

## 查壳



首先来查一下壳，是FSG1.33的壳，不过是个变型壳。

## OD脱壳

文件(F) 查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H) 快速菜单 Tools BP VB 记事本 Notepad Calc 快捷菜单 CMD Exit									
暂停									
地址 HEX 数据 反汇编 注释 寄存器									
004307FA	^ 74 F0	je short FSG_1_33.004307EC		EAX 0000					
004307FC	√ 79 05	jns short FSG_1_33.00430803		ECX 7702					
004307FE	46	inc esi	FSG_1_33.004190EA	EDX 0055					
004307FF	AD	lods dword ptr ds:[esi]		EBX 0043					
00430800	50	push eax		ESP 0018					
00430801	√ EB 09	jmp short FSG_1_33.0043080C		EBP 762C					
00430803	FE0E	dec byte ptr ds:[esi]		ESI 0041					
00430805	- 0F84 5B1EFDFF	je FSG_1_33.00402666		EDI 0041					
0043080B	56	push esi	FSG_1_33.004190EA	EIP 0043					
0043080C	55	push ebp	kernel32.762C0000						
0043080D	FF53 04	call dword ptr ds:[ebx+0x4]	kernel32.GetProcAddress	C 0 ES					
00430810	AB	stos dword ptr es:[edi]		P 1 CS					
00430811	^ EB E0	jmp short FSG_1_33.004307F3		A 0 SS					
00430813	33C9	xor ecx,ecx	ntdll.12.770238AA	Z 0 DS					
00430815	41	inc ecx	ntdll.12.770238AA	S 0 FS					
00430816	FF13	call dword ptr ds:[ebx]	kernel32.LoadLibraryA	T 0 GS					
跳转未实现									
00402666=FSG_1_33.00402666									
地址	HEX 数据	ASCII	地址	数值	注释				

关于FSG的壳有一个特点，只要一直往下拉找到一个远跳，这个远跳跟过去就是OEP的位置。然后在这里下断点F7就能到达OEP。

关于如何快速识别远跳，我是通过OpCode的方式。可以看到上图框起来的地方就是目标地址减去当前地址的偏移，当这个地址值比较大的时候，就能确定这是个远跳。

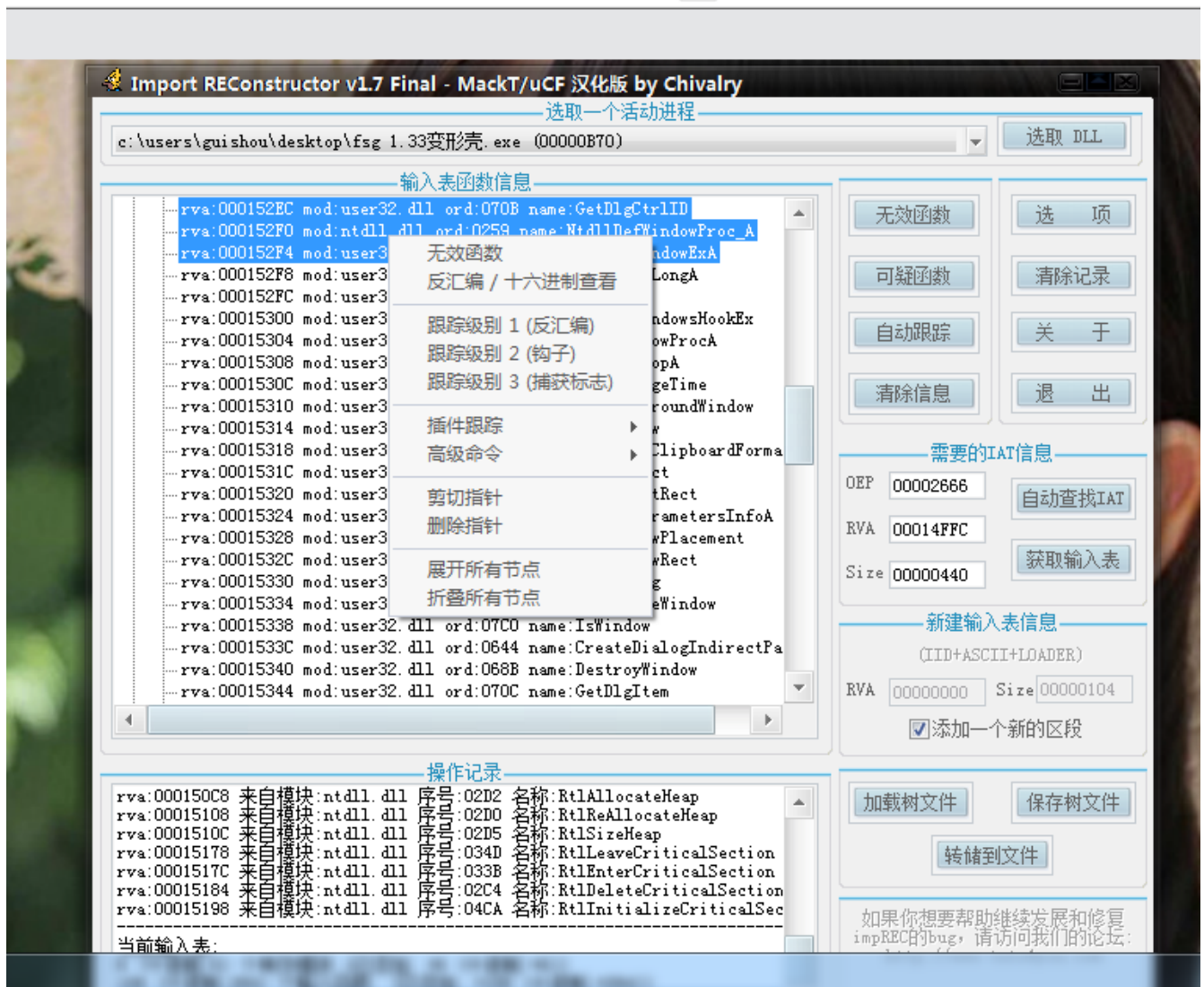
接着再je处按回车键跟随，分析代码 下断点。

地址	HEX 数据	反汇编	注释
00402666	. 55	push ebp	comctl32.72A10000
00402667	. 8BEC	mov ebp,esp	
00402669	. 6A FF	push -0x1	
0040266B	. 68 00674100	push FSG_1_33.00416700	
00402670	. 68 FC504000	push FSG_1_33.004050FC	SE 处理程序安装
00402675	. 64:A1 00000000	mov eax,dword ptr fs:[0]	
0040267B	. 50	push eax	comctl32.72A11700
0040267C	. 64:8925 00000000	mov dword ptr fs:[0],esp	
00402683	. 83EC 58	sub esp,0x58	
00402686	. 53	push ebx	FSG_1_33.00430851
00402687	. 56	push esi	FSG_1_33.00419FCE
00402688	. 57	push edi	FSG_1_33.00415018
00402689	. 8965 E8	mov [local.6],esp	
0040268C	. FF15 14524100	call dword ptr ds:[0x415214]	kernel32.GetVersion
00402692	. 33D2	xor edx,edx	comctl32.72A10000
00402694	. 8AD4	mov dl,ah	

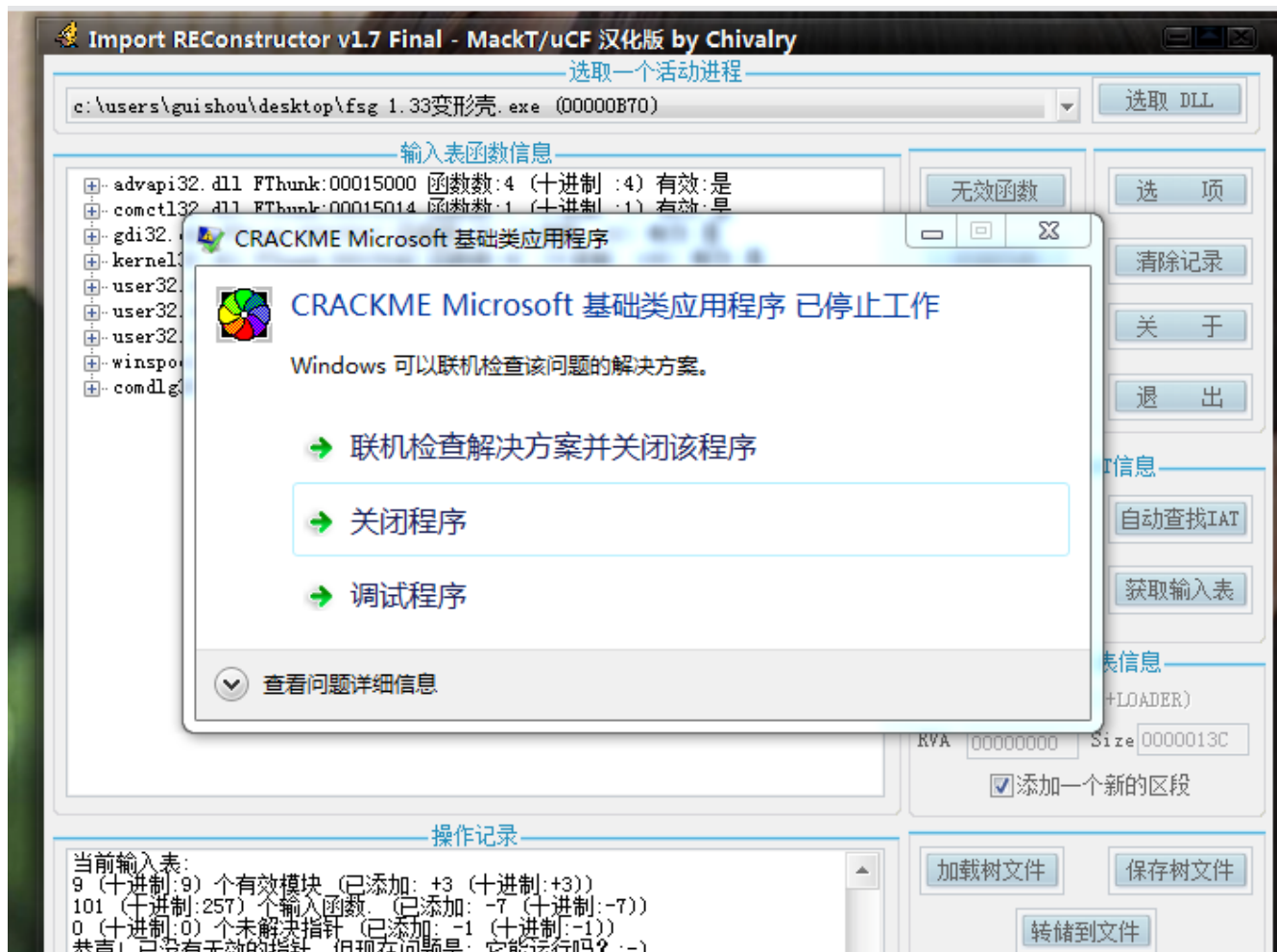
就直接到达OEP了。

## 修复导入表

接下来dump文件，

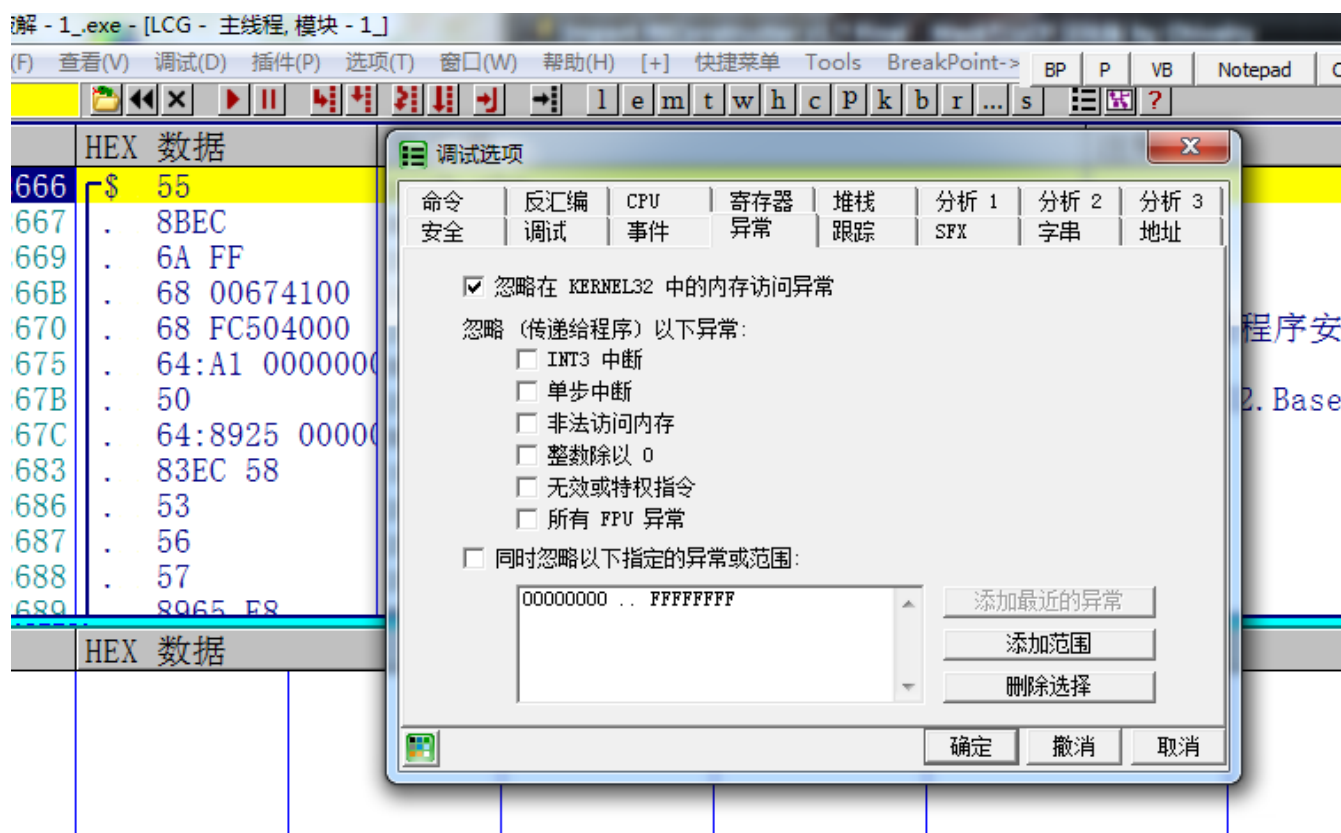


输入OEP，查找IAT，获取输入表，有几个无效函数需要剪切掉。然后转储文件。运行，

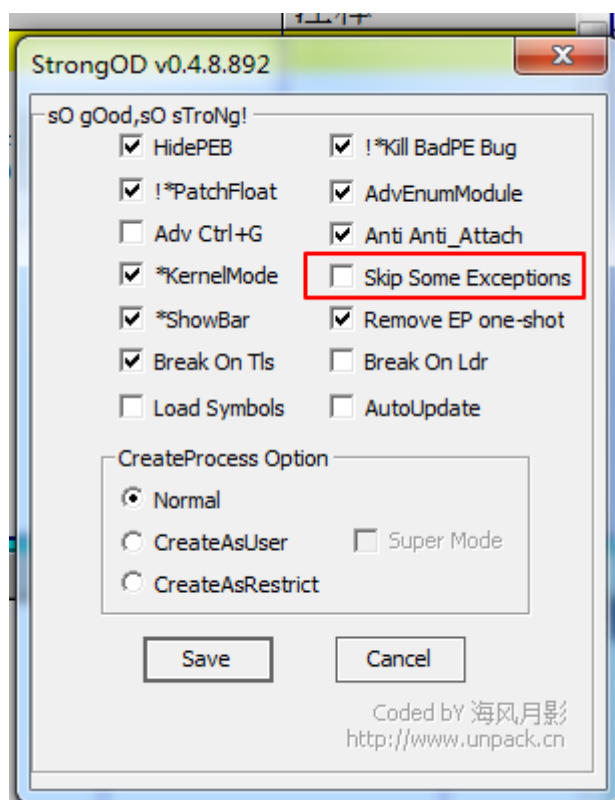


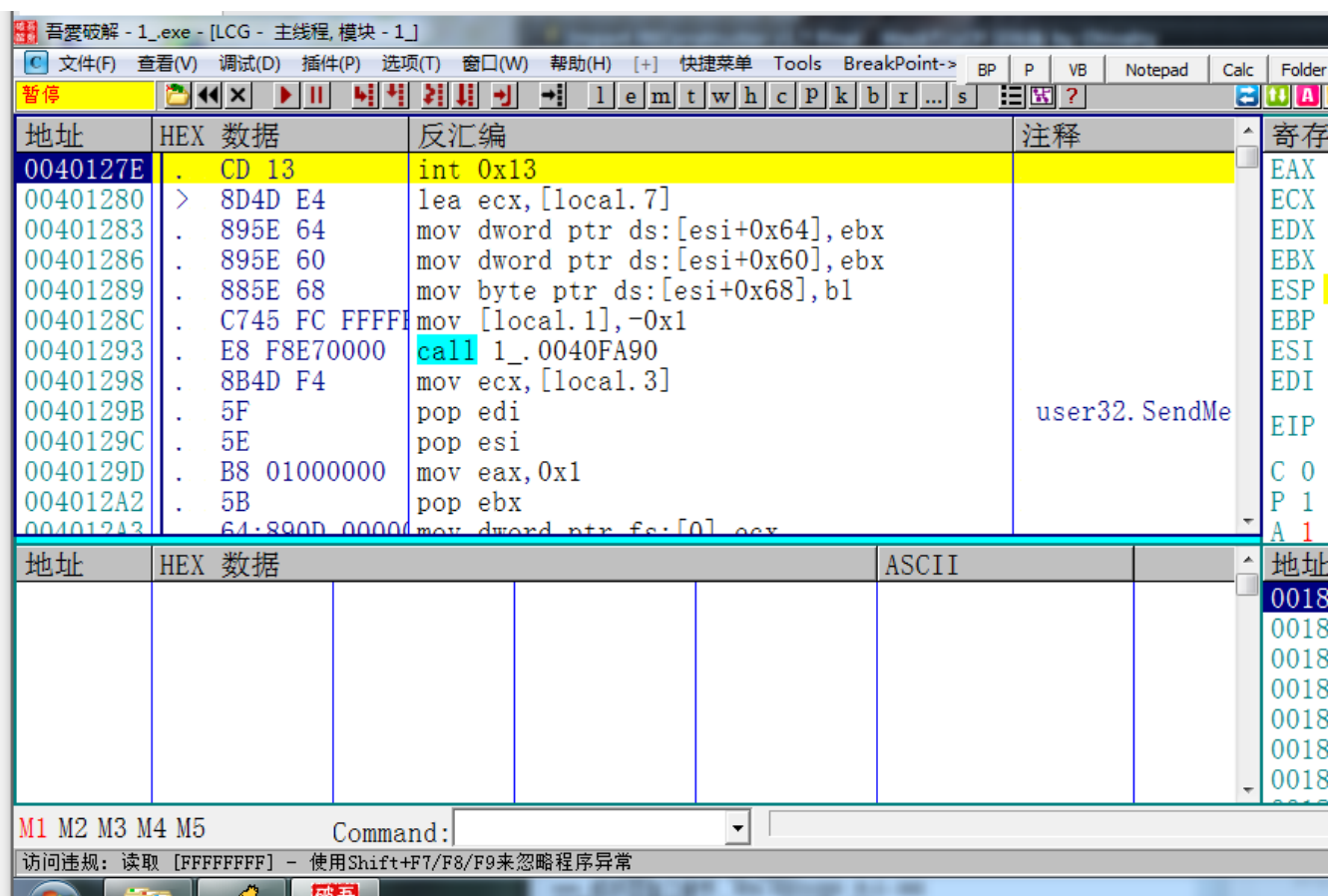
程序居然无法运行，说明肯定是遇到某个异常了，将修复好导入表的程序载入OD，

## 修复程序



设置忽略所有异常，同时要把StrongOD的这个勾给取消掉。直接F9运行。





程序断在了这里，并且显示访问违规，抛出一个异常，而程序本身无法处理这个异常，所以导致直接崩溃。那么只要把这条指令给nop掉就可以了。



nop掉之后，脱壳后的程序是可以正常运行的。

需要相关文件可以到我的Github下载:<https://github.com/TonyChen56/Unpack-Practice>