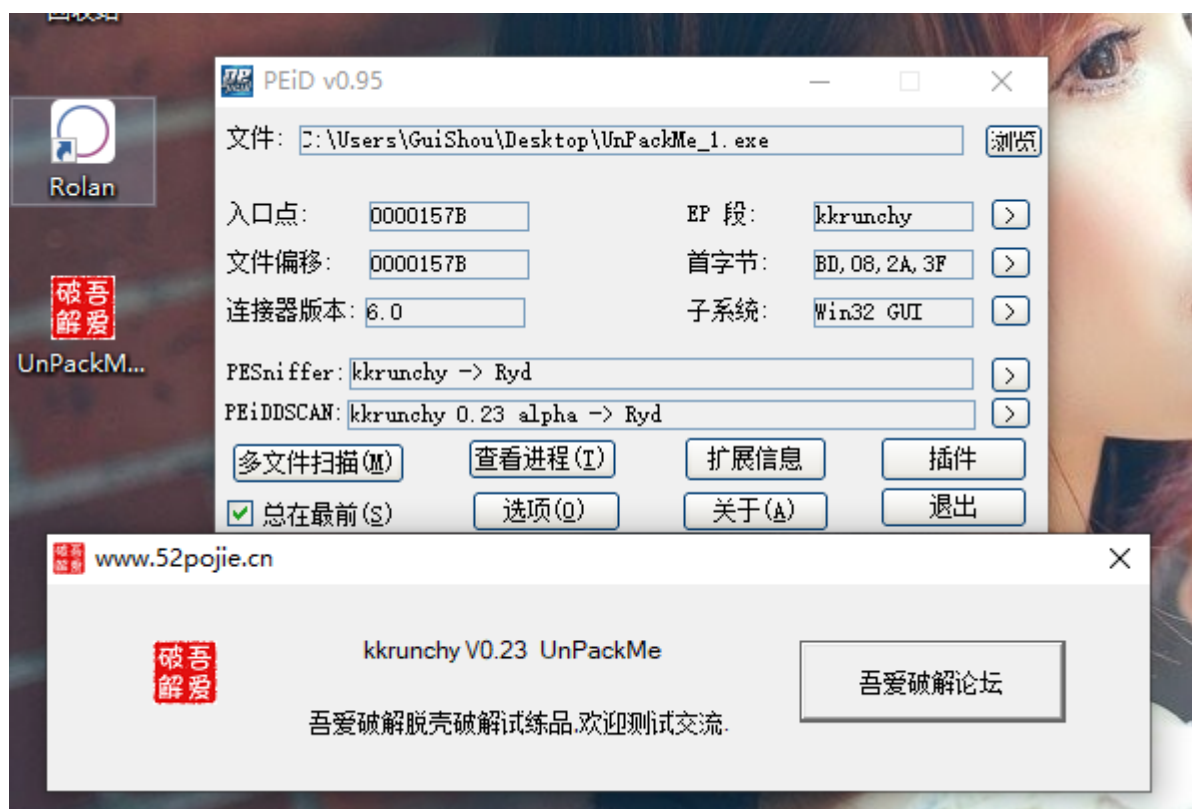


前言  
查壳  
OD脱壳  
修复导入表

## 前言

最近一直在看脱壳系列的教程，国内能找到的脱壳视频几乎都看了个遍，大部分由于年代实在是太久了，附带的示例程序完全不能运行，或者是某些未知原因用相同的步骤中间总是会出差错，后来找到了 **吾爱破解脱壳练习系列动画**，主讲人是论坛的小生大神，感觉这个系列的教程是最适合我的，这个例子是 **吾爱破解脱壳练习系列动画**的第一课，一个有点类似的FSG的压缩壳。

## 查壳



目标程序是这个，一个不怎么常见的压缩壳吧，直接脱壳

## OD脱壳

载入到OD，



吾爱破解 - UnPackMe\_1.exe - [LCG - m主线程, 模块 - UnPackMe]

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->

暂停

地址	HEX 数据	反汇编	注释
00401700	0000	add byte ptr ds:[eax],al	
00401702	0000	add byte ptr ds:[eax],al	
00401704	0000	add byte ptr ds:[eax],al	
00401706	0000	add byte ptr ds:[eax],al	
00401708	0000	add byte ptr ds:[eax],al	
0040170A	0000	add byte ptr ds:[eax],al	
0040170C	0000	add byte ptr ds:[eax],al	
0040170E	0000	add byte ptr ds:[eax],al	
00401710	0000	add byte ptr ds:[eax],al	
00401712	0000	add byte ptr ds:[eax],al	
00401714	0000	add byte ptr ds:[eax],al	
00401716	0000	add byte ptr ds:[eax],al	
00401718	0000	add byte ptr ds:[eax],al	
0040171A	0000	add byte ptr ds:[eax],al	
0040171C	0000	add byte ptr ds:[eax],al	
0040171E	0000	add byte ptr ds:[eax],al	

al=00

寄存器: EAX, ECX, EDX, EBX, ESP, EBP, EDI, ESI, EIP, C 1, P 1, A 1, Z C, S 1, T C, D C

接着重新载入程序，直接F9

吾爱破解 - UnPackMe\_1.exe - [LCG - 主线程, 模块 - UnPackMe]

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->

暂停

地址	HEX 数据	反汇编	注释
00401700	55	push ebp	UnPackMe.003F2A08
00401701	8BEC	mov ebp,esp	
00401703	6A FF	push -0x1	
00401705	68 00254000	push UnPackMe.00402500	
0040170A	68 86184000	push UnPackMe.00401886	
0040170F	64:A1 00000000	mov eax,dword ptr fs:[0]	
00401715	50	push eax	
00401716	64:8925 00000000	mov dword ptr fs:[0],esp	
0040171D	83EC 68	sub esp,0x68	
00401720	53	push ebx	UnPackMe.003FFF3D
00401721	56	push esi	UnPackMe.00400B3B
00401722	57	push edi	UnPackMe.00402000
00401723	8965 E8	mov dword ptr ss:[ebp-0x18],esp	
00401726	33DB	xor ebx,ebx	UnPackMe.003FFF3D
00401728	895D FC	mov dword ptr ss:[ebp-0x4],ebx	UnPackMe.003FFF3D
0040172B	6A 02	push 0x2	

就到达OEP了

## 修复导入表

接着dump文件，自动查找IAT，获取输入表，转储文件



转储之后，文件正常运行



脱壳完成

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