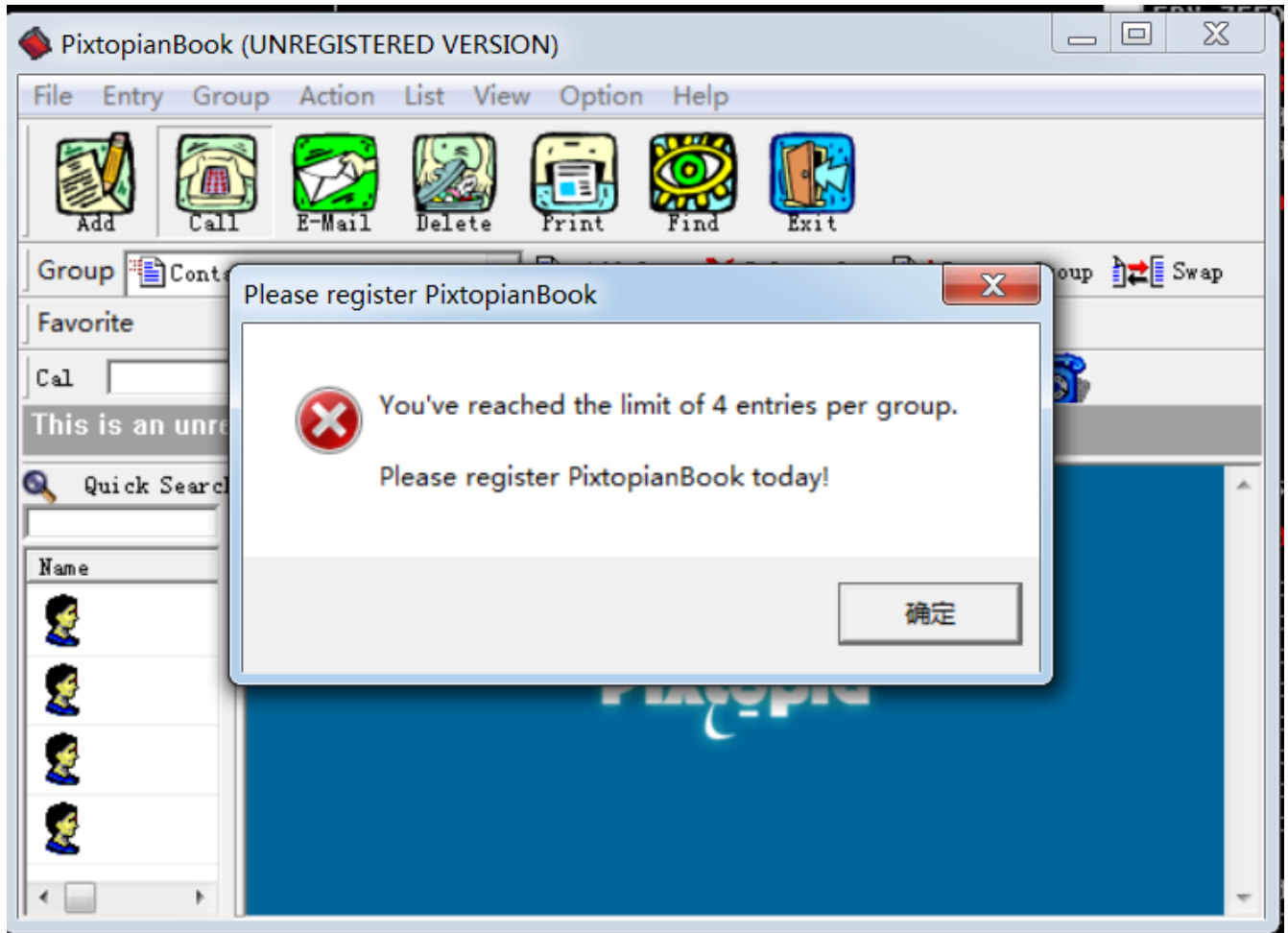


pixtopianbook107破解教程

0x1，添加联系人限制：

1，原始程序只能添加四个联系人，现在突破限制；



2，现在OD中载入程序，运行程序，添加练习人，当人数到弹窗后在OD中暂停，进入堆栈段：

地址	堆栈	函数过程 / 参数	调用来自	结构
0012EA24	77D193F5	包含 ntdll.KiFastSystemCallRet	user32.77D193F3	0012EA58
0012EA28	77D3EA24	user32.WaitMessage	user32.77D3EA1F	0012EA58
0012EA5C	77D2688A	user32.77D3E895	user32.77D26885	0012EA58
0012EA84	77D3B7C5	user32.77D267D4	user32.77D3B7C0	0012EA80
0012ED44	77D3B12B	user32.SoftModalMessageBox	user32.77D3B126	0012ED40
0012EE94	77D65FDF	user32.77D3AFB6	user32.77D65FDA	0012EE90
0012EEEC	77D66084	user32.MessageBoxTimeoutW	user32.77D6607F	0012EEEC
0012EF20	77D50598	? user32.MessageBoxTimeoutA	user32.77D50593	0012EF1C
0012EF40	77D50550	? user32.MessageBoxExA	user32.77D5054B	0012EF3C
0012EF44	000701C4	hOwner = 000701C4 (class= '#32770'		
0012EF48	0048FC68	Text = "You've reached the limit		
0012EF4C	0048F700	Title = "Please register Pixtopia		
0012EF50	00000010	Style = MB_OK MB_ICONHAND MB_APPL		
0012EF54	00000000	LanguageID = 0x0 (LANG_NEUTRAL)		
0012EF5C	0045631B	? user32.MessageBoxA	Pixtopia.00456315	0012EF58
0012EF60	000701C4	hOwner = 000701C4 (class= '#32770'		
0012EF64	0048FC68	Text = "You've reached the limit		
0012EF68	0048F700	Title = "Please register Pixtopia		
0012EF6C	00000010	Style = MB_OK MB_ICONHAND MB_APPL		
0012EF74	00412DEA	? Pixtopia.004562ED	Pixtopia.00412DE5	

在用户段看到调用弹窗的地址，重新加载OD，找到对应位置：

00456315	. FF15 0456470	call dword ptr ds:[<&USER32.MessageBoxA]	LMessageBoxA
0045631B	. 5E	pop esi	
0045631C	. C2 0C00	retn 0xC	
0045631F	. 55	push ebp	

3，看反汇编窗口跟随

call dword ptr ds:[<&USER32.MessageBoxA]		0 0	LastError ERROR_INVALID_WINDOW_HANDLE (00000578)
retn 0xC		EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)	
(00456315), ASCII "puG"		ST0 empty -??? FFFF 00005FEE 0F0566FB	
		ST1 empty -??? FFFF 00000000 0F050700	
ASCII "puG"		0012EF70 00456315	ASCII "puG"
0012EF74 00412DEA		返回到 Pixtopia.00412DEA 来自 Pixtopia.004562ED	
0012EF78 0048FC68		ASCII "You've reached the limit of 4 entries per group.\n\nPlease register PixtopianBook today!"	
0012EF7C 0048F700		ASCII "Please register PixtopianBook"	
0012EF80 00000010			

找到此API的位置，现在到此位置来看看，

00412DC6	. 8B04F9	mov eax,dword ptr ds:[ecx+edi*8]	
00412DC9	. 8D2CFD 000000	lea ebp,dword ptr ds:[edi*8]	
00412DD0	. 83F8 04	cmp eax,0x4	
00412DD3	. 7C 1A	jl short Pixtopia.00412DEF	
00412DD5	. 8B4C24 10	mov ecx,dword ptr ss:[esp+0x10]	
00412DD9	. 6A 10	push 0x10	
00412DDB	. 68 00F74800	push Pixtopia.0048F700	
00412DE0	. 68 68FC4800	push Pixtopia.0048FC68	
00412DE5	. E8 03350400	call Pixtopia.004562ED	
00412DEA	. E9 DD000000	jmp Pixtopia.00412ECC	
00412DEF	. 8D4C24 14	lea ecx,dword ptr ss:[esp+0x14]	
00412E33	. E8 38610100	call Pixtopia.00428E30	

看到这有比较，与

4比较，小于则跳转，那么我们只要将jl改为无条件跳转就可以了：

C 1A	jl short Pixtopia.00412DEF	
B4C24 10	mov ecx,dword ptr ss:[esp+0x10]	
A 10		
8 00F748		
8 68FC48		
8 033504		
9 DD0000		
04C24 14		
8 386101		

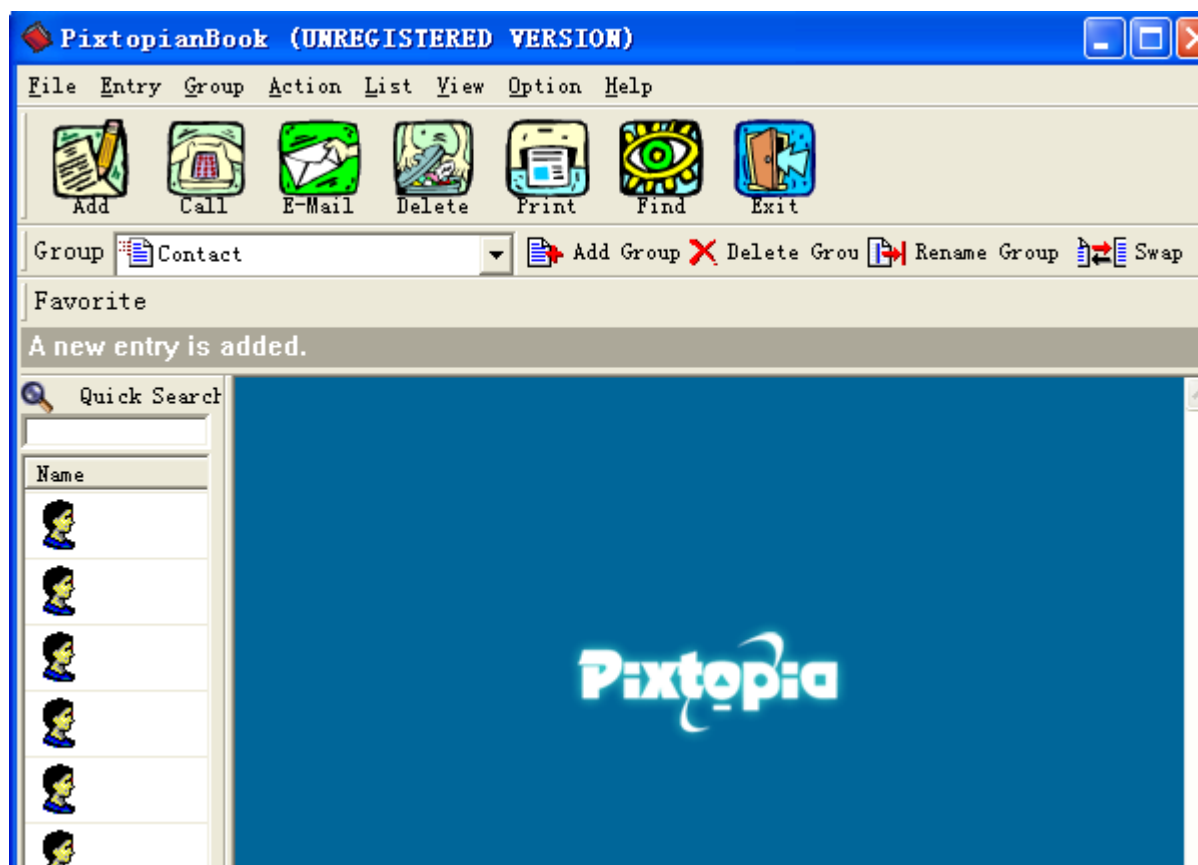
汇编于此处: 00412DD3

jmp short 00412DEF

☒ 使用 NOP 填充

汇编 取消

4，保存后已经突破限制了：



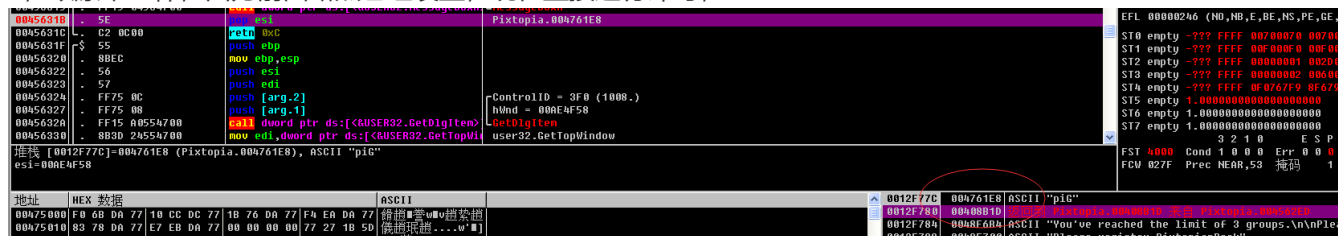
0x2, Add Group限制

1, 现在只能添加两组:

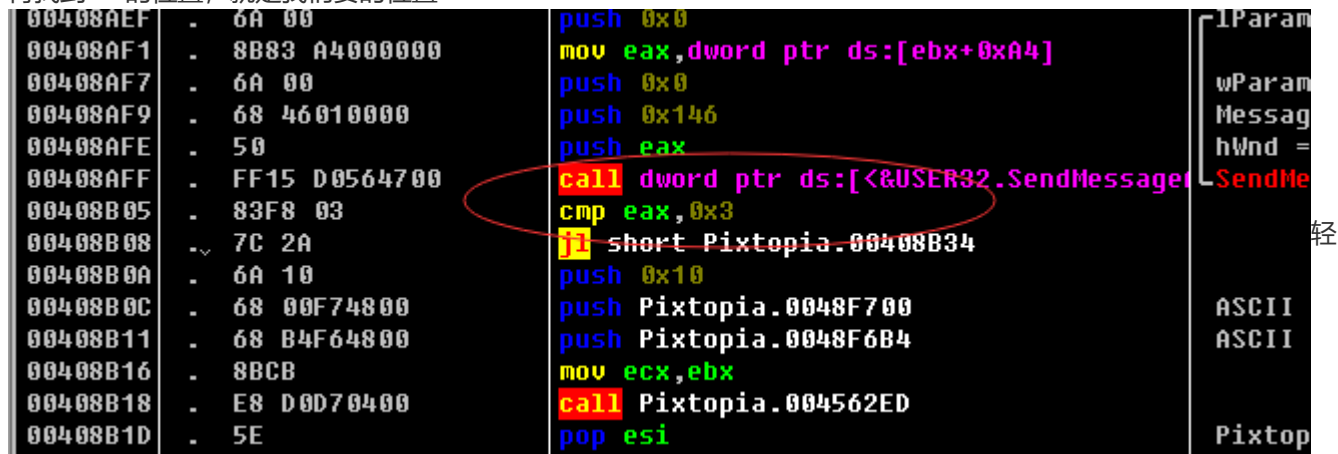


根据上次的来试一试吧;

2, 跟原来一样, 因为前面断点已经设置, 现在直接运行即可,



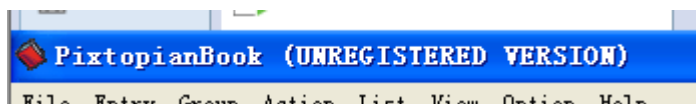
再找到API的位置, 就是我们要的位置



车熟路的改成无条件跳转即可, 此后Add Group没有限制;

0x3, 美观注册破解

1,



尽管大部分已经破解完毕, 但是有这种未注册的字样, 现在我们来破解他们;

2, 我们去内存找一下,

地址	大小	属主	区段	包含	类型	访问	初始访问	已映射为
00250000	00006000				Priv	RW	RW	
00260000	00003000				Map	RW	RW	
00270000	00016000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
00290000	0003D000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
002D0000	00041000							\Device\HarddiskVolume1\WINDOWS\system32\
00320000	00008000							\Device\HarddiskVolume1\WINDOWS\system32\
00330000	00041000							
00380000	00008000							
00390000	00008000							
003A0000	00001000							
003B0000	00001000							
003C0000	00003000							
003D0000	00004000							\Device\HarddiskVolume1\WINDOWS\system32\
003E0000	00002000							
003F0000	00003000							
00400000	00001000							
00401000	00074000							
00475000	0001A000							
0048F000	0000E000							
0049D000	0004C000							
004F0000	00003000				map	R E	R E	
005B0000	00002000				Map	R E	R E	
005C0000	00103000				Map	R	R	

输入要查找的二进制字符串

ASCII: U.N.R.E.G.I.S.T.E.R.E.D.

UNICODE: UNREGISTERED

HEX +18: 55 00 4E 00 52 00 45 00 47 00 49 00 53 00 54 00 45 00 52 00 45 00 44 00

☒ 整个块 ☐ 区分大小写

确定 取消

运行

0017CAFA	55 00 4E 00	52 00 45 00	47 00 49 00	53 00 54 00	U.N.R.E.G.I.S.T.
0017CB0A	45 00 52 00	45 00 44 00	29 00 00 00	00 00 49 00	E.R.E.D.)...I.
0017CB1A	53 00 54 00	45 00 52 00	45 00 44 00	29 00 00 00	S.T.E.R.E.D.)...
0017CB2A	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0017CB3A	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0017CB4A	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0017CB5A	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0017CB6A	00 00 00 00	00 00 3E 00	A6 00 F0 01	0C 00 00 00>??...
0017CB7A	00 00 70 01	00 00 04 00	00 00 20 00	00 00 10 00	..pr... ..+
0017CB8A	00 00 00 00	00 00 00 00	00 00 00 01	00 00 00 002

现在知道地址了, 在dump

面板跳转;

3,

地址	HEX 数值	ASCII
004D4830	55 00 6E 00 72 00 65 00 67 00 69 00 73 00 74 00	U.n.r.e.g.i.s.t.
004D4840	65 00 72 00 65 00 64 00 20 00 76 00 65 00 72 00	e.r.e.d. .v.e.r.
004D4850	73 00 69 00 6F 00 6E 00 20 00 76 00 31 00 2E 00	s.i.o.n. .v.1...

4, 这句话



根据

0040C002	push Pixtopia.0046FD08	有MH
0040C237	push Pixtopia.0046F974	This is an unregistered version of PixtopianBook. Please register today!
0040C3B8	push Pixtopia.0046FD73	街NH
0040C712	push Pixtopia.0046FDE7	街NH
0040CD48	push Pixtopia.0046FEA8	赴OH

得到地址

然后更改即可:



解决。