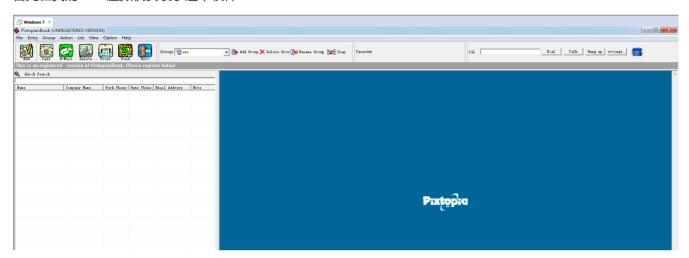
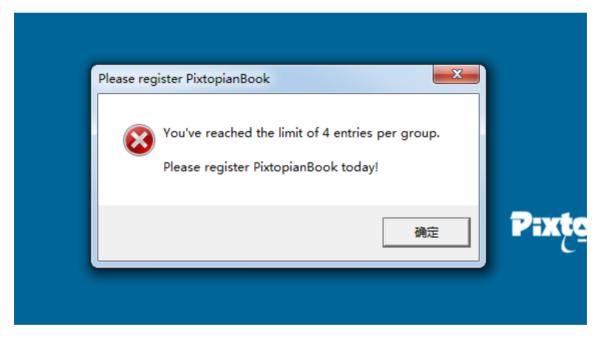
0x01 PixtopianBook

首先在我的win7虚拟机安装了这个软件:



简单操作了一下,发现这个软件是个通讯录,但是只能有4条记录,超过了就会弹窗:



那我就直接OD载入,先用字符串搜索下有没有关键字符,直接搜索上面对话框里的字符串:

```
| DUMONFIED | DUMO
```

先找到了这个,但是这个好像是限制了三个组,不是限制记录,看来这个软件是限制了记录不能超过四条,并且组不 能超过三个,双击跟到引用处:

```
Message = CB GETCOUNT
00408AF9
             68 46010000
                           oush Øx146
00408AFE
                                                                     hWnd = 0x76DA1162
             50
             FF15 D056470
00408B05
             83F8 03
00408B08
             7C 2A
                              short Pixtopia.00408B34
00408B0A
             6A 10
00408B0C
             68 00F74800
                                Pixtopia.0048F700
                                                                     Please register PixtopianBook
00408B11
             68 B4F64800
                                Pixtopia.0048F6B4
                                                                      You've reached the limit of 3 groups.\n\n
00408B16
             RRCR
00408B18
             E8 D0D70400
                                Pixtopia.004562ED
00408B1D
             5E
                               esi
                                                                      kerne132.76DA1174
00408B1E
             5B
                                                                     kerne132.76DA1174
                           oop ebx
00408B1F
             8B8C24 34010 mov ecx, dword ptr ss:[esp+0x134]
```

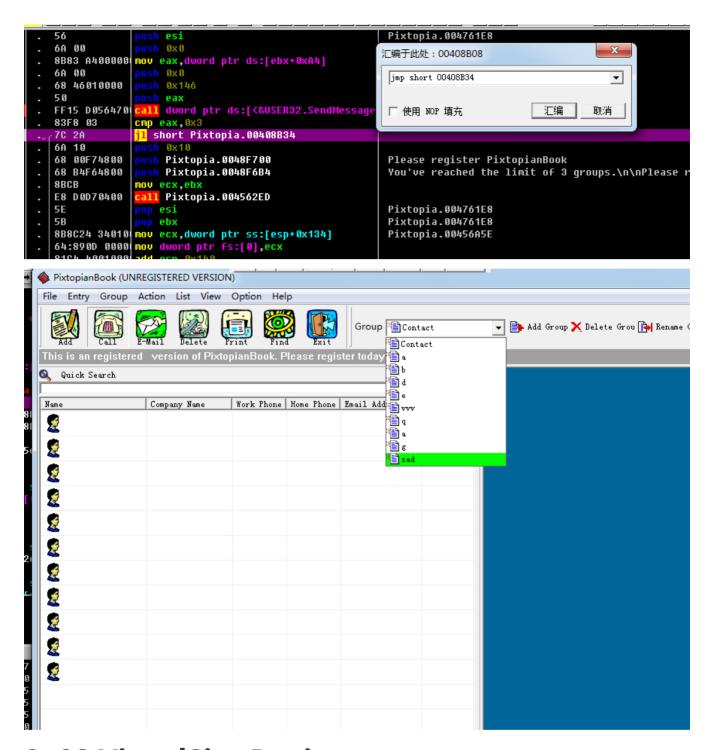
在call messagebox的地方下断,同理在限制四条的地方下断:

```
hWnd = 0x76DA1162
00412DB7 . 50
            8B8E BC01000
00412DBE
                            ov ecx,dword ptr ds:[esi+0x1BC]
             kernel32.BaseThreadInitThunk
00412DC4
             8BF8
00412DC6
00412DC9
00412DD0
             83F8 04
00412DD3
             7C 1A
                              short Pixtopia.00412DEF
                               ecx,dword ptr ss:[esp+0x10]
88412005
             884C24 18
00412DD9
             6A 10
                               Pixtopia.0048F700
Pixtopia.0048FC68
Pixtopia.004562ED
                                                                      Please register PixtopianBook
You've reached the limit of 4 entries per group.\n\nPlease register
00412DDB
             68 00F74800
00412DE0
             68 68FC4888
```

f9运行,需要在此处把il跳转指令,改为imp无条件跳转:

```
8D2CFD 000001
                         lea ebp,dword ptr ds:[edi*8]
412DC9
412DD0
           83F8 04
                         cmp eax,0x4
412DD3
           7C 1A
                            short Pixtopia.00412DEF
412DD5
           8B4C24 10
                         mov ecx,dword ptr ss:[esp+0x10]
412DD9
           6A 10
                         push 0x10
                         push Pixtopia.0048F700
412DDB
           68 00F74800
                                                                     Pleas:
                                                                     You'v
412DE0
           68 68FC4800
                         push Pixtopia.0048FC68
412DE5
           E8
              03350400
                              Pixtopia.004562ED
412DEA
           E9 DD000000
                          mp Pixtopia.00412ECC
412DEF
          58D4C24 14
                         lea ecx,dword ptr ss:[esp+0x14]
        >
412DF3
           E8 38610100
                              Pixtopia.00428F30
412DF8
           68 D8784900
                         push Pixtopia.004978D8
          8D2CFD 00000i
                        lea ebp,dword ptr ds:[edi*8]
          83F8 04
                        cmp eax,0x4
          EB 1A
          8B4C24 10
                        mov ecx,dword ptr ss:[esp+0x10]
          6A 10
                        push 0x10
             00F74800
                        push Pixtopia.0048F700
                                                                    Ρ1
          68
                        push Pixtopia.0048FC68
          68
             68FC4800
                                                                    Yo
                             Divtonia AGNEASEN
             02250100
```

之后永远跳过了阻止继续添加记录的check,接着再把添加组的按照相同方式修改,就可以无限添加组和记录了:

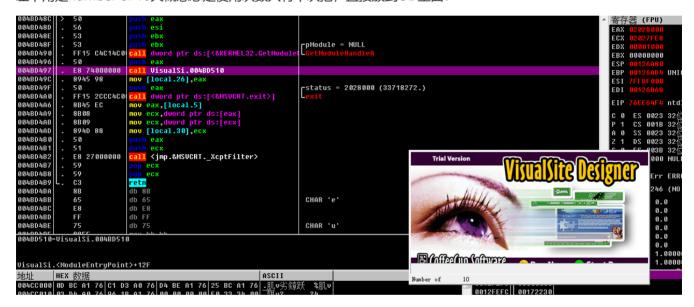


0x02 VisualSite Designer

打开软件,首先是一个这样的窗口:



左下角是number of 10大概意思是使用次数只有十次把,直接放到OD里面:



之后的操作就是找到调用这个窗口的函数,一直下断点就可以,直到mfc的关键位置:

```
visuai51.00489H29
eax,dword ptr ds:[edi+0xE4]
004898E7
004898E7
004898ED
                    8B87 E400000
                    6A 00
85C0
004898EF
004898F1
004898F7
004898FE
                    0F8E A100000
                                              VisualSi.00489998
                    8D8C24 10020
E8 6D240200
                                               ecx,dword ptr ss:[esp+0x210]
VisualSi.004ABD70
                    8D8C24 0C020
C68424 78870
E8 132B0300
                                              ecx,dword ptr ss:[esp+0x20C]
byte ptr ss:[esp+0x8778],0xB
l <jmp.&MFC42.#2514>
00489903
0048990A
                    63F8 01
74 40
8BC
0048991A
                                            short VisualSi.0048995C
0048991C
0048991E
                                                                                                        VisualSi.0058B230
                    E8 ØDF6FFFF
                                                VisualSi.00488F30
                                              ecx,dword ptr ss:[esp+0x2B0]
byte ptr ss:[esp+0x8778],0xD
00489923
0048992A
                    8D8C24 B0020
C68424 78870
00489932
                    E8 81300300
                                                <jmp.&MFC42.#765>
                    8D8C24 70020
C68424 78870
                                              ecx,dword ptr ss:[esp+0x270]
byte ptr ss:[esp+0x8778],0xC
00489937
0048993E
                                               <jmp.&MFC42.#795>
00489946
0048994B
                    E8 DB2B0300
C68424 78870
                                             byte ptr ss:[esp+0x8778],0x5
                    8D8C24 0C020
EB 77
                                              ecx,dword ptr ss:[esp+0x20C]
short VisualSi.004899D3
00489953
0048995A
                    8D8C24 B0020 lea
0048995C
                                              ecx,dword ptr ss:[esp+0x2B0]
  ax=00127958, (ASCII "H新")
```

这个地方返回eax为1,为了去掉这个串口直接把它改为mov eax,1:

```
004878ED
                           push 0x0
             6A 00
                           test eax,eax

jle VisualSi.00489998
004898EF
             85C0
004898F1
             OF8E A100000
004898F7
             8D8C24 10020 lea ecx, dword ptr ss:[esp+0x210]
                                VisualSi.004ABD70
004898FE
             E8 6D240200
             8D8C24 0C020 lea ecx,dword ptr ss:[esp+0x20C]
00489903
0048990A
             C68424 78870 mov byte ptr ss:[esp+0x8778],0xB
00489912
00489917
             83F8 01
                           cmp eax,0x1
             74 40
                              short VisualSi.0048995C
0048991A
0048991C
             8BCF
                           mov ecx,edi
                                                                      VisualSi.0058B230
0048991E
             E8 ODF6FFFF
                                VisualSi.00488F30
00489923
             8D8C24 B0020 lea ecx, dword ptr ss:[esp+0x2B0]
0048992A
             C68424 78870 mov byte ptr ss:[esp+0x8778],0xD
00489932
             E8 81300300
                                <jmp.&MFC42.#765>
```

这样就完成了限制打开软件的去除,软件可无限使用