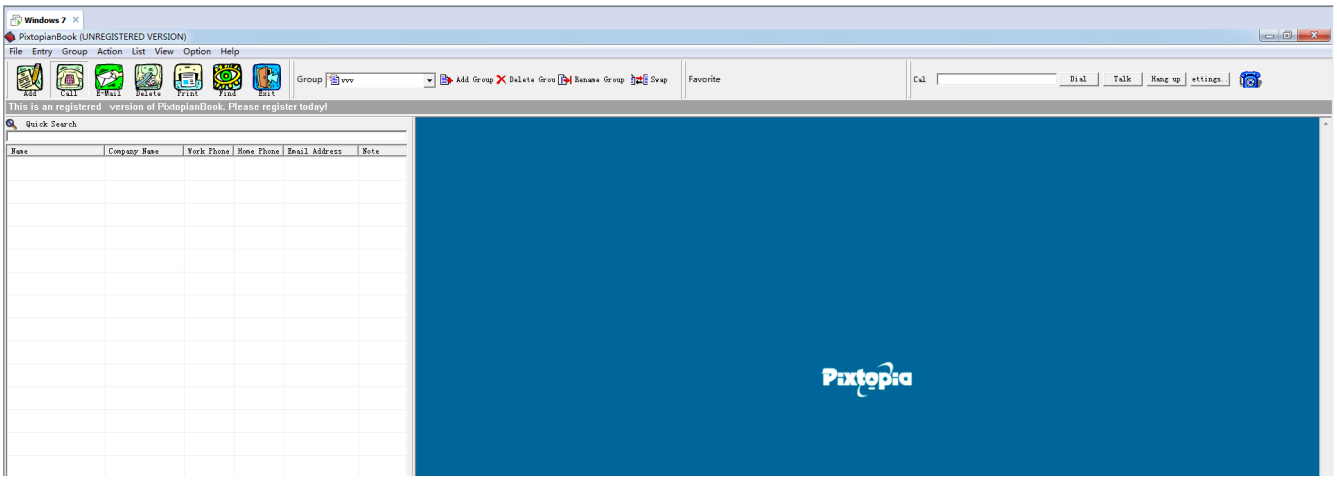
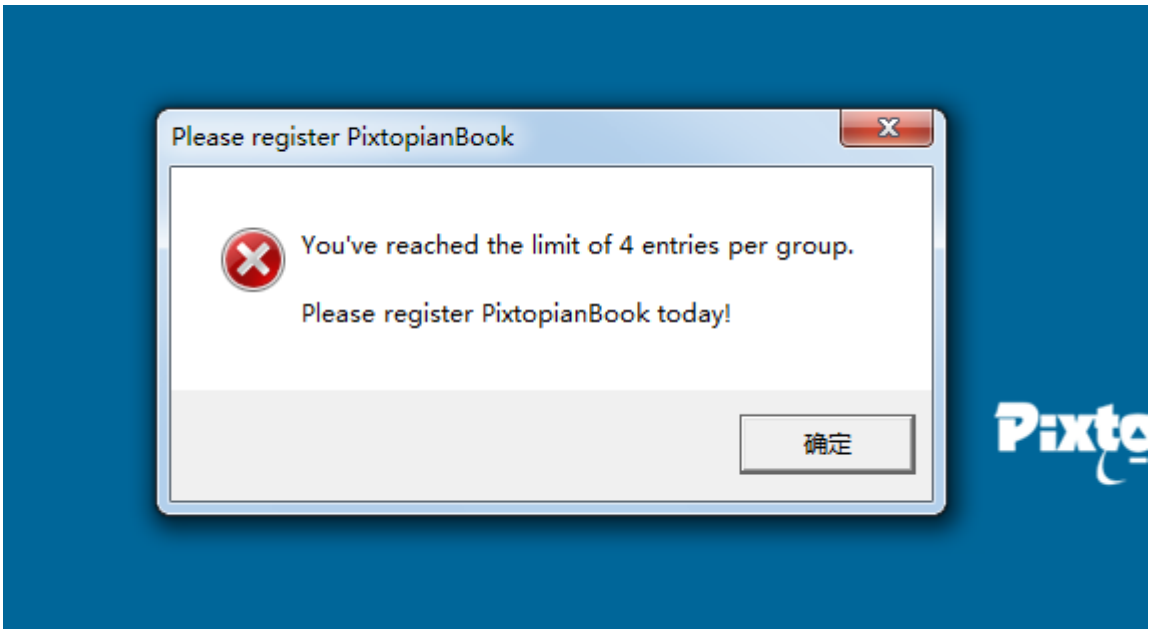
0x01 PixtopianBook

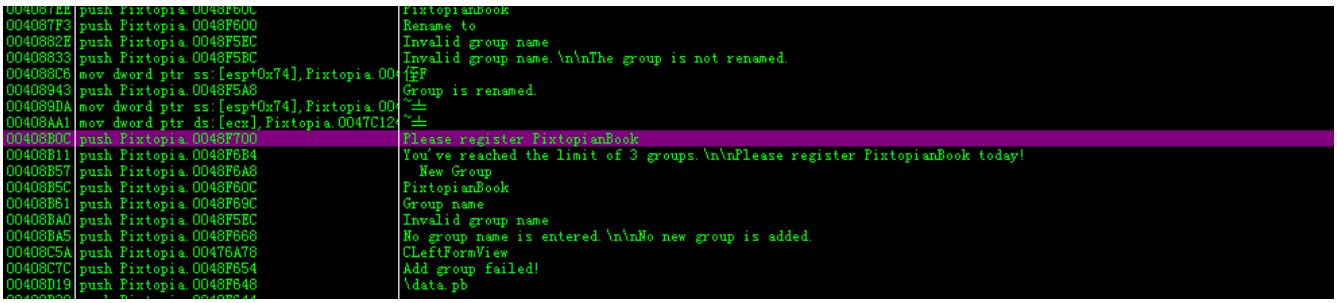
首先在我的win7虚拟机安装了这个软件：



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：



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：

```
00408AF9  .  68 46010000   push 0x146                  Message = CB_GETCOUNT
00408AFE  .  50            push eax                    hWnd = 0x76DA1162
00408AFF  .  FF15 D056470( call dword ptr ds:[<&USER32.SendMessage  SendMessageA
00408B05  .  83F8 03       cmp eax,0x3
00408B08  .v 7C 2A         jl short Pixtopia.00408B34
00408B0A  .  6A 10         push 0x10
00408B0C  .  68 00F74800   push Pixtopia.0048F700      Please register PixtopianBook
00408B11  .  68 B4F64800   push Pixtopia.0048F6B4      You've reached the limit of 3 groups.\n\n
00408B16  .  8BCB          mov ecx,ebx
00408B18  .  E8 D0D70400   call Pixtopia.004562ED
00408B1D  .  5E            pop esi                     kernel32.76DA1174
00408B1E  .  5B            pop ebx                     kernel32.76DA1174
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：

```
mov dword ptr ds:[ecx],Pixtopia.0047C12
mov eax,Pixtopia.00476DC8
mov esi,Pixtopia.0047C124
push Pixtopia.00470620
mov dword ptr ss:[esp+0x18],Pixtopia.00
mov eax,Pixtopia.00476EE8                  CMainDialogBar
mov eax,Pixtopia.00476F00
mov dword ptr ds:[esi],Pixtopia.00477
mov dword ptr ds:[esi],Pixtopia.00477
push Pixtopia.00470746
push Pixtopia.00476A78                     CLeftFormView
push Pixtopia.0048F700                     Please register PixtopianBook
push Pixtopia.0048FC68                     You've reached the limit of 4 entries per group.\n\nPlease register PixtopianBook today!
push Pixtopia.0048FC50                     A new entry is added.
push Pixtopia.004707B3
mov dword ptr ss:[esp+0xDC],Pixtopia.00
mov dword ptr ss:[esp+0x6C],Pixtopia.00
push Pixtopia.00470818
```

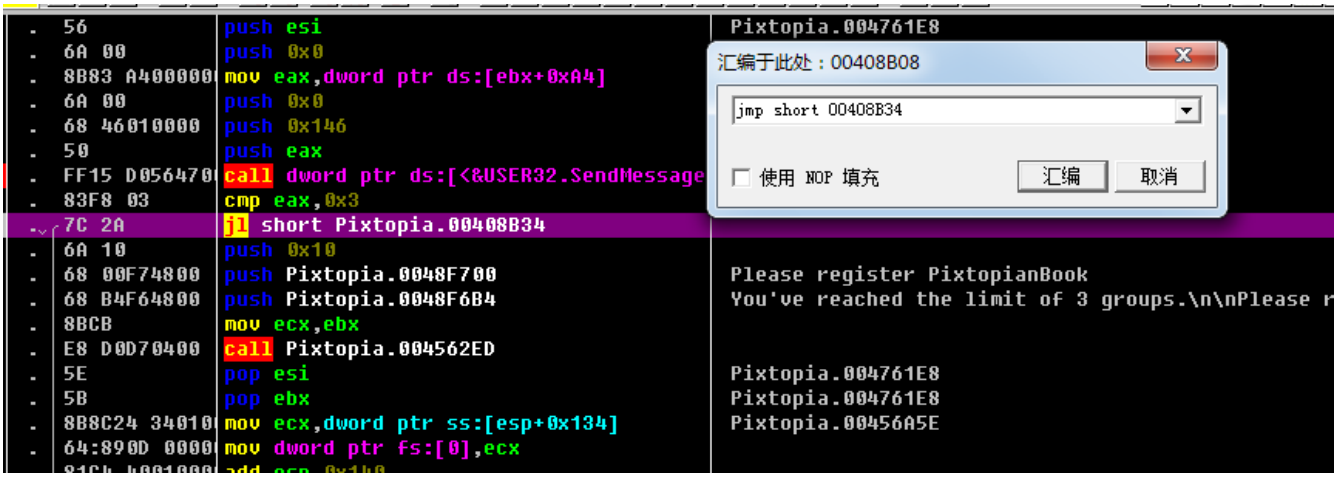
```
00412DB7  .  50            push eax                    hWnd = 0x76DA1162
00412DB8  .  FF15 D056470( call dword ptr ds:[<&USER32.SendMessage  SendMessageA
00412DBE  .  8B8E BC01000( mov ecx,dword ptr ds:[esi+0x1BC]
00412DC4  .  8BF8          mov edi,eax                 kernel32.BaseThreadInitThunk
00412DC6  .  8B04F9        mov eax,dword ptr ds:[ecx+edi*8]
00412DC9  .  8D2CFD 00000( lea ebp,dword ptr ds:[edi*8]
00412DD0  .  83F8 04       cmp eax,0x4
00412DD3  .v 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      Please register PixtopianBook
00412DE0  .  68 68FC4800   push Pixtopia.0048FC68      You've reached the limit of 4 entries per group.\n\nPlease register
00412DE5  .  E8 03350400   call Pixtopia.004562ED
```

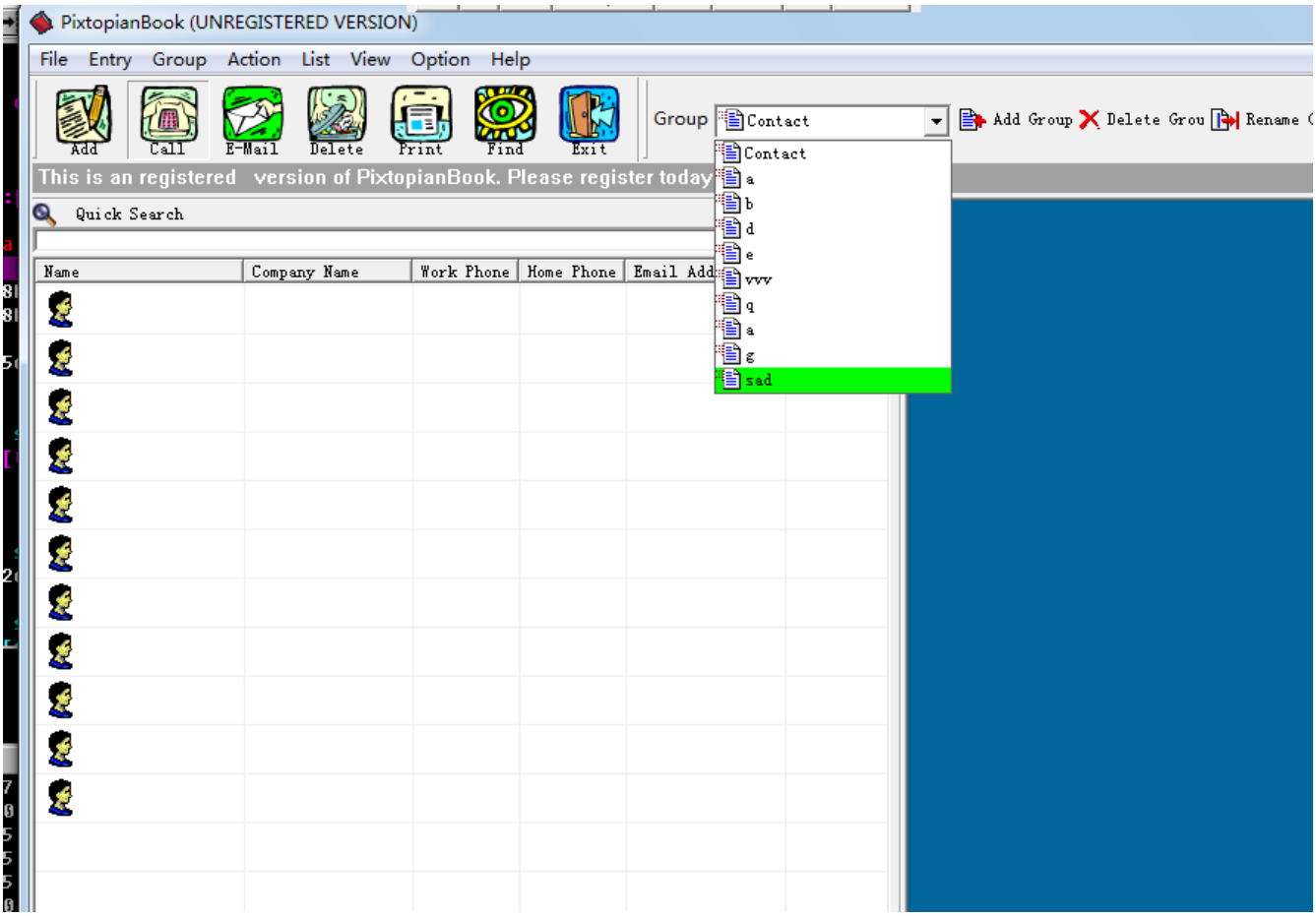
f9运行，需要在此处把jl跳转指令，改为jmp无条件跳转：

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

```
   .  8D2CFD 00000( lea ebp,dword ptr ds:[edi*8]
   .  83F8 04       cmp eax,0x4
   .v EB 1A         jmp short Pixtopia.00412DEF
   .  8B4C24 10     mov ecx,dword ptr ss:[esp+0x10]
   .  6A 10         push 0x10
   .  68 00F74800   push Pixtopia.0048F700      Pl
   .  68 68FC4800   push Pixtopia.0048FC68      Yo
   .  E8 03350400   call Pixtopia.004562ED
```

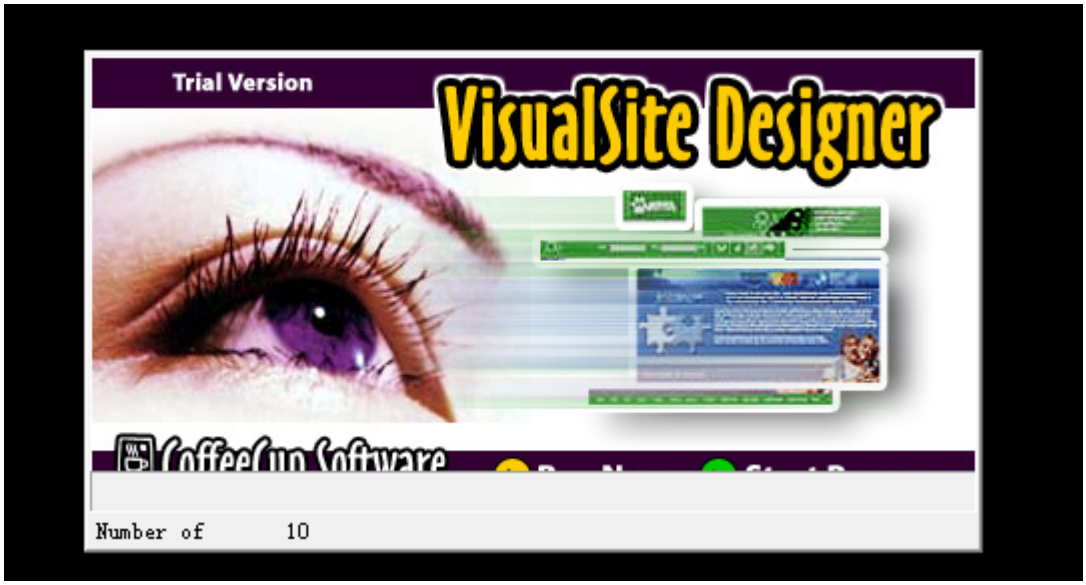
之后永远跳过了阻止继续添加记录的check，接着再把添加组的按照相同方式修改，就可以无限添加组和记录了：



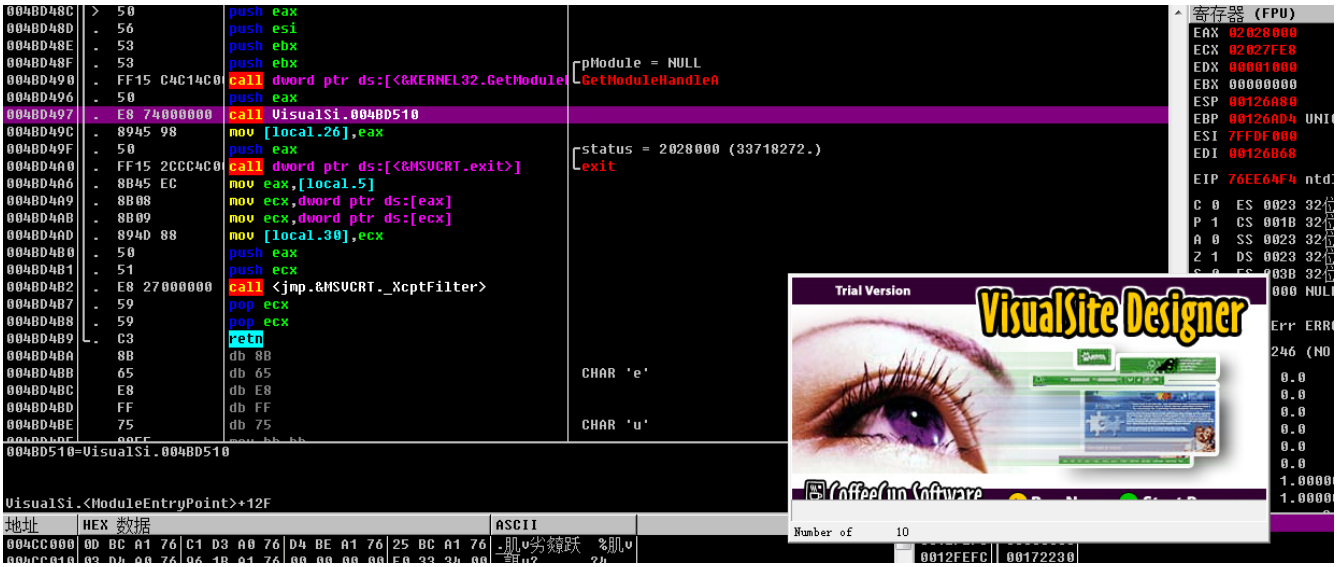


0x02 VisualSite Designer

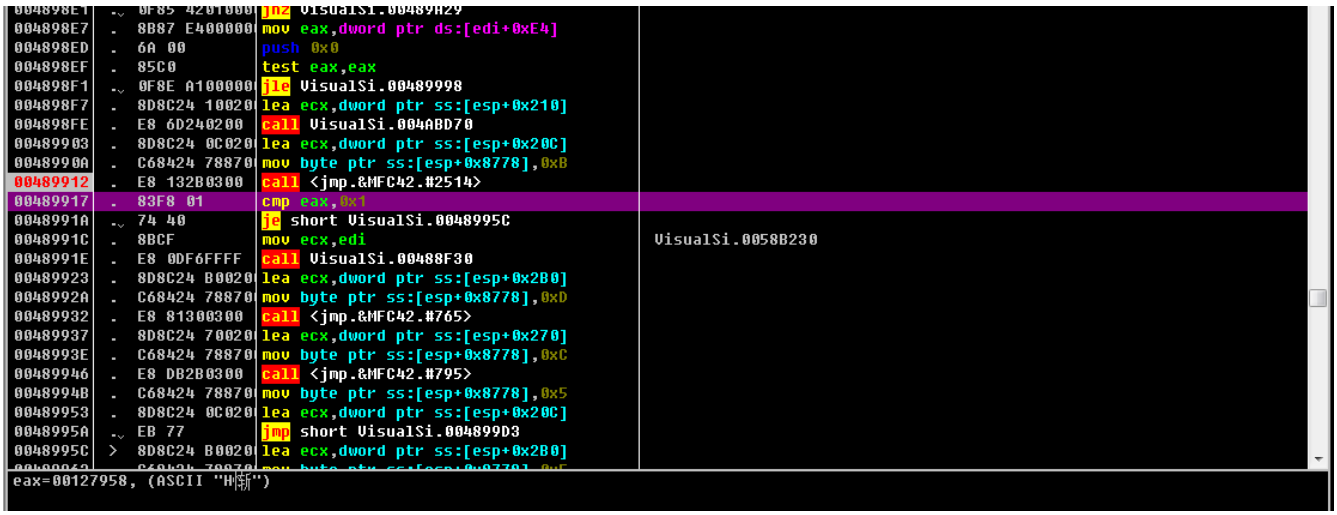
打开软件，首先是一个这样的窗口：



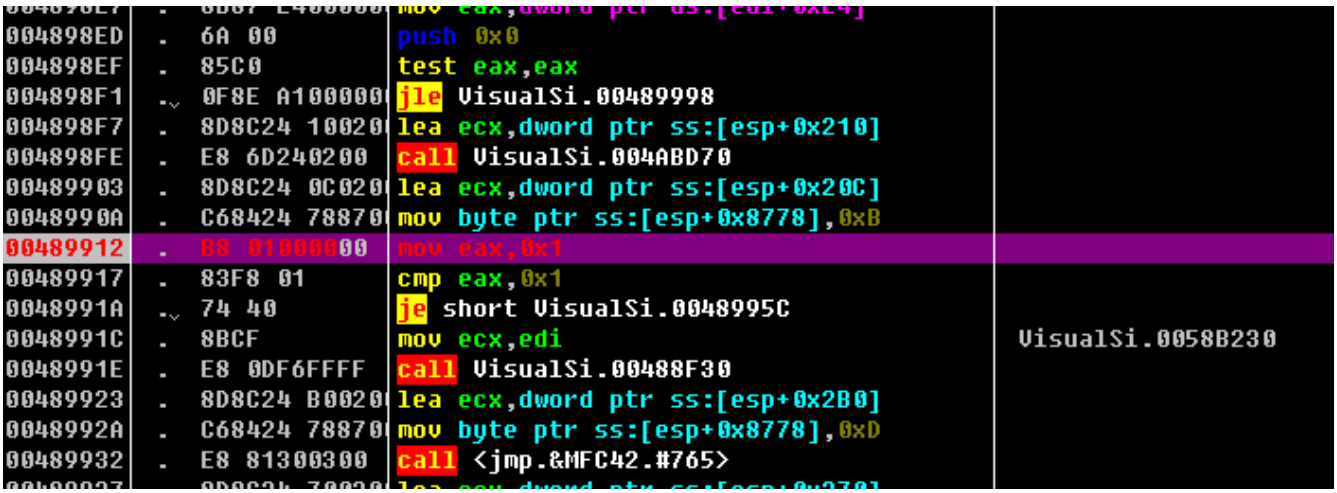
左下角是number of 10大概意思是使用次数只有十次把，直接放到OD里面：



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：



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：



这样就完成了限制打开软件的去除，软件可无限使用