VisualSite Designer破解教程

0x1，次数破解：

1，首先

在原文件中

有Number字符，看来是因为次数会限制，那么我们就先来破解它。

2，由于无壳，就直接上OD了：

```
004BD497   .  E8 74000000   call VisualSi.004BD510
004BD49C   .  8945 98       mov [local.26],eax
```

下断点：

3，ctrl+F2，F9到断点，F7进入函数

```
004BD51C   .  FF7424 10     push dword ptr ss:[esp+0x10]
004BD520   .  E8 43000000   call <jmp.&MFC42.#1576>
004BD525   .  C2 1000       retn 0x10
```

4，老规矩，继续：

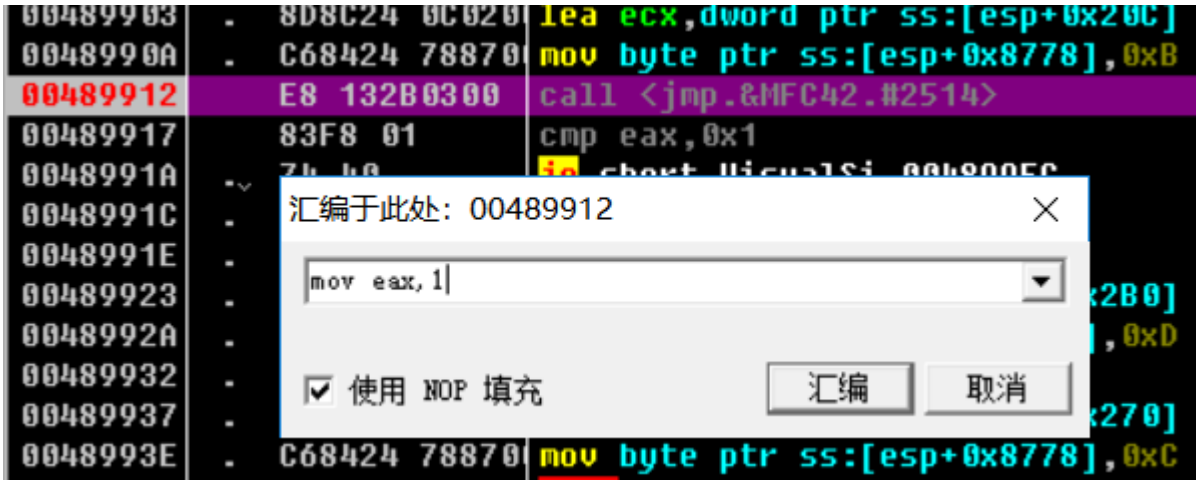
```
0FC86241   8BCF             mov ecx,edi
0FC86243   FFD6             call esi
0FC86245   85C0             test eax,eax
```

5，再次就有点意思了，eax与1比较，然后跳转，这是关键所在，严谨其间还是在进去一次吧；

```
00489912   .  E8 132B0300   call <jmp.&MFC42.#2514>
00489917   .  83F8 01       cmp eax,0x1
```

6，又找到了一个：

7，发现入口，但是OD并不会停下，所以这个就是最终，由于上一个是动态链接库的地址，无法修改，所以在再上一个

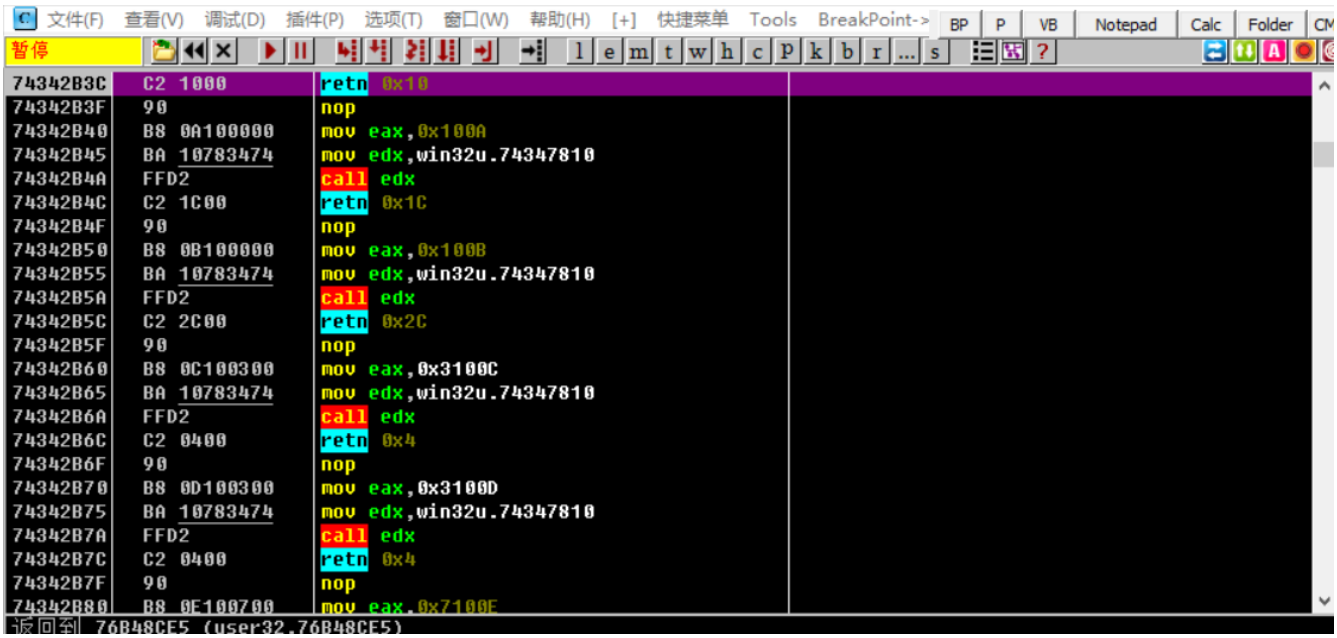


保存到可执行文件后，没有弹窗了；

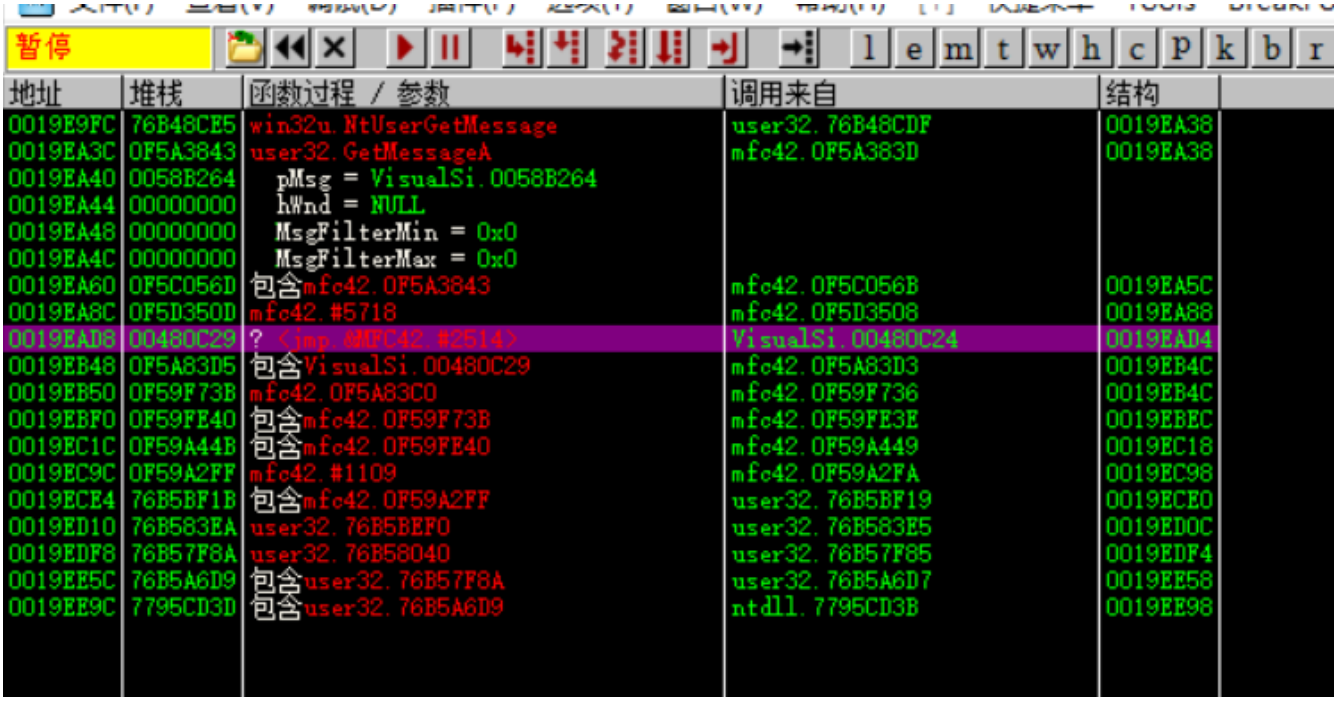
0x2，广告弹窗：

在关闭软件后会显示弹窗，则现在来将他取消掉；

1，在OD中运行程序，再关掉，在OD中点击暂停：



然后进入堆栈段查看调用：



在所选位置，我们看到其他都是mfc的系统调用，只有所选位置是程序自身的，点击进去相应位置：

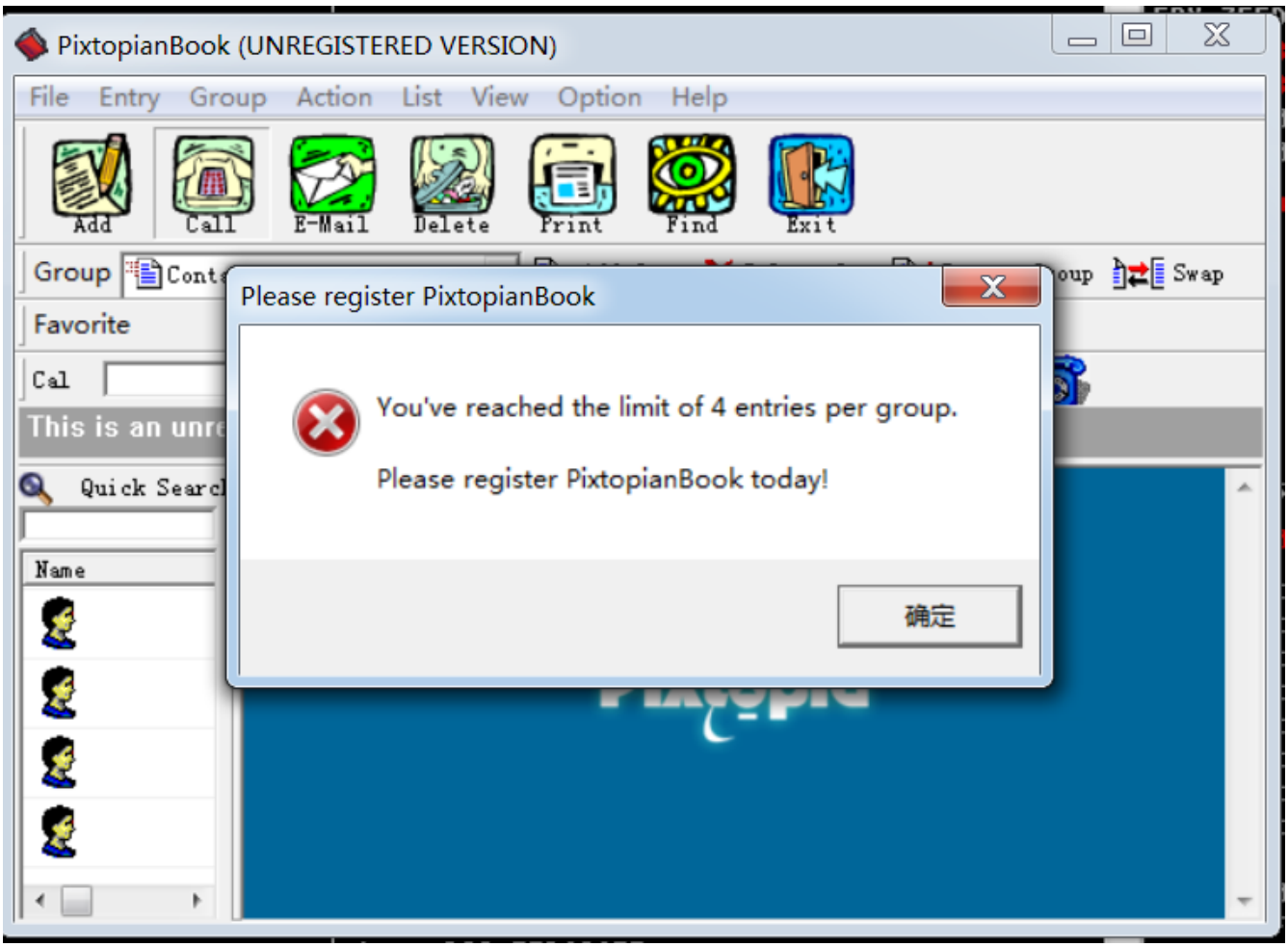
nop填充，保存文件。

这后，就没有广告了。

pixtopianbook107破解教程

0x1，添加联系人限制：

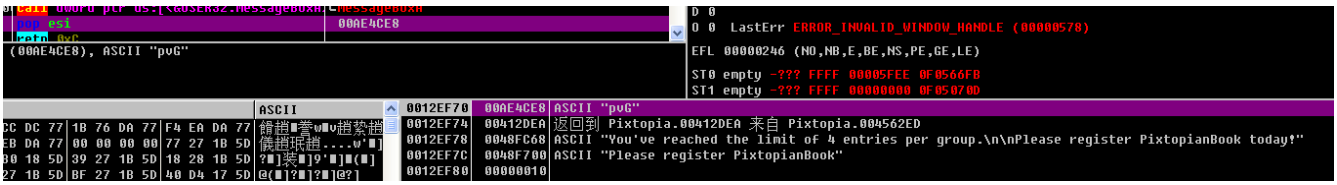
1，原始程序只能添加四个联系人，现在突破限制；



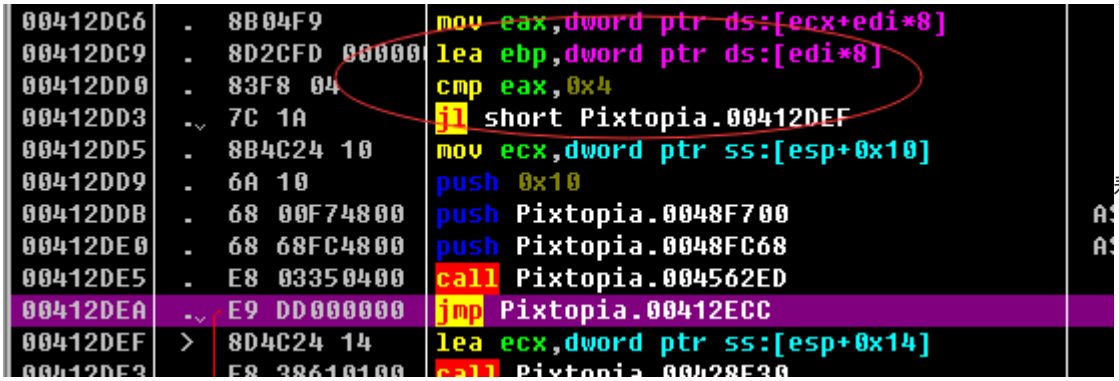
2，现在OD中载入程序，运行程序，添加练习人，当人数到弹窗后在OD中暂停，进入堆栈段：

在用户段看到调用弹窗的地址，重新加载OD，找到对应位置：

3，看反汇编窗口跟随

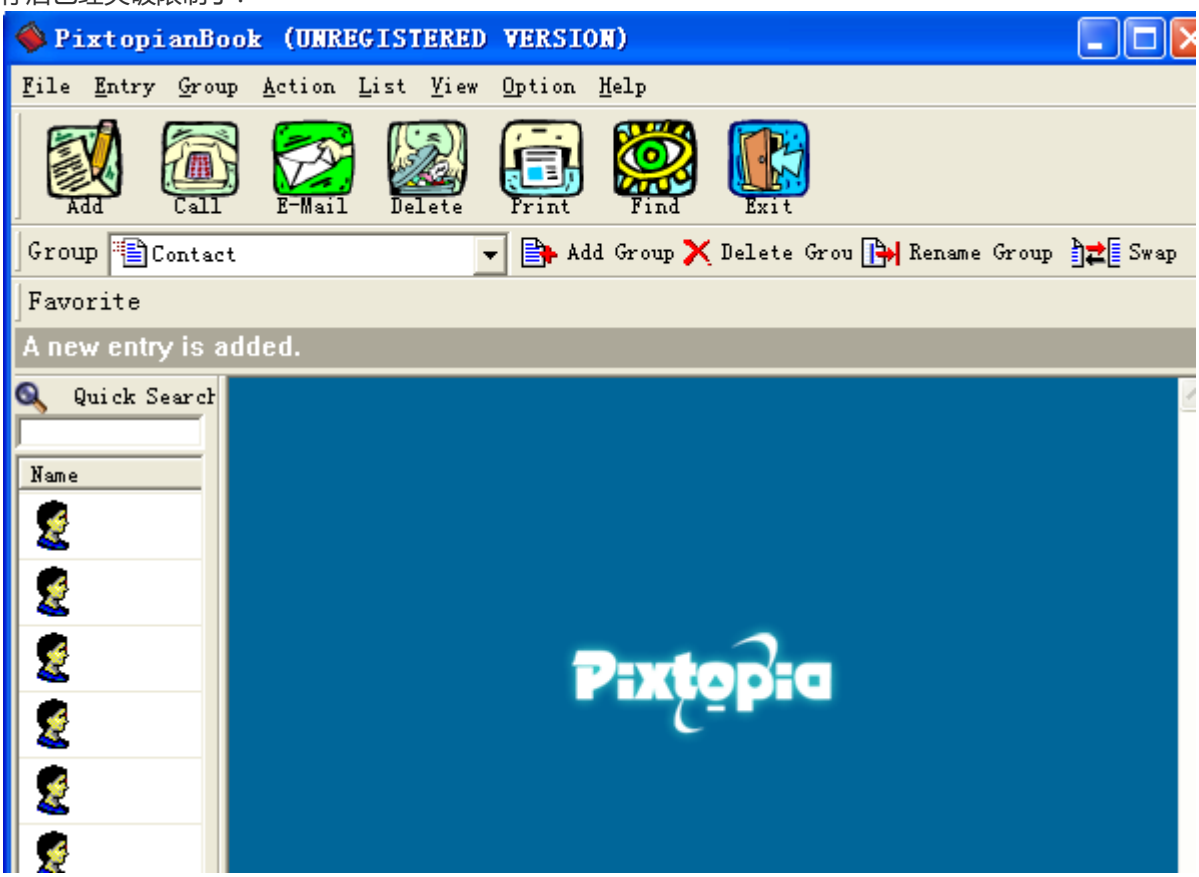


找到此API的位置，现在到此位置来看看，



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：

4，保存后已经突破限制了：

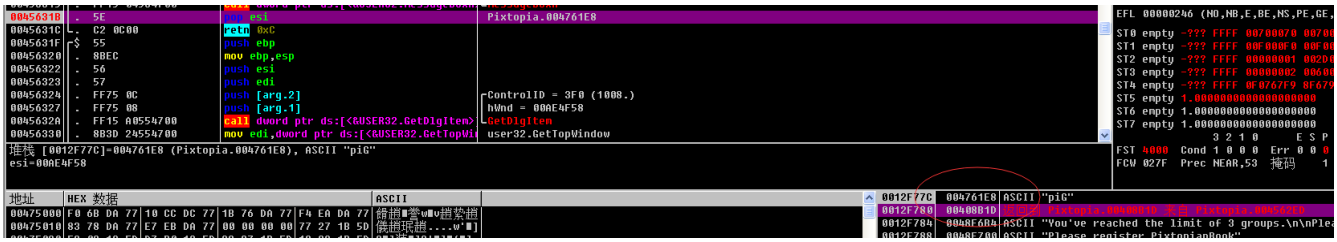


0x2，Add Group限制

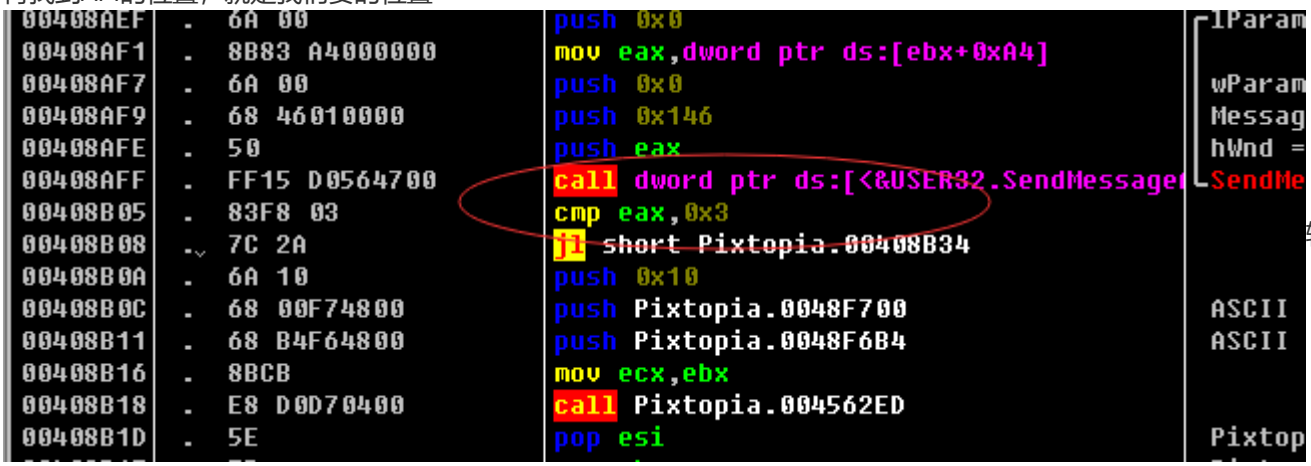
1，现在只能添加两组：

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



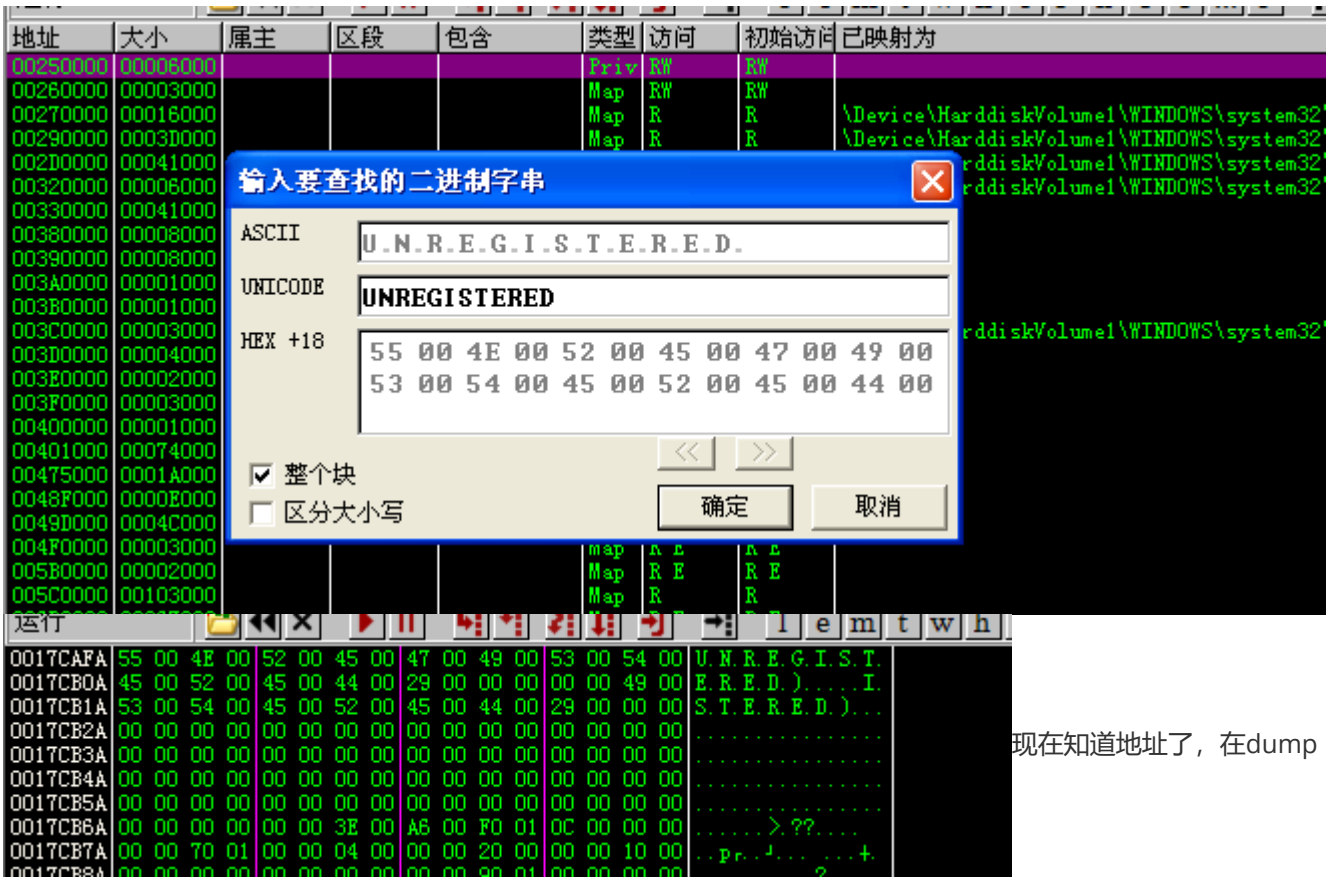
轻车熟路的改成无条件跳转即可，此后Add Group没有限制；

0x3，美观注册破解

1，

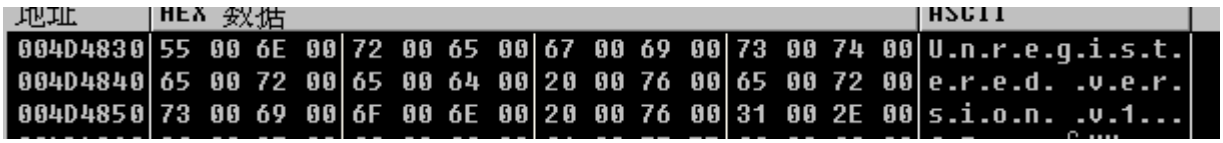
尽管大多部分已经破解完毕，但是有这种未注册的字样，现在我们来破解他们；

2，我们去内存找一下，



现在知道地址了，在dump面板跳转；

3，

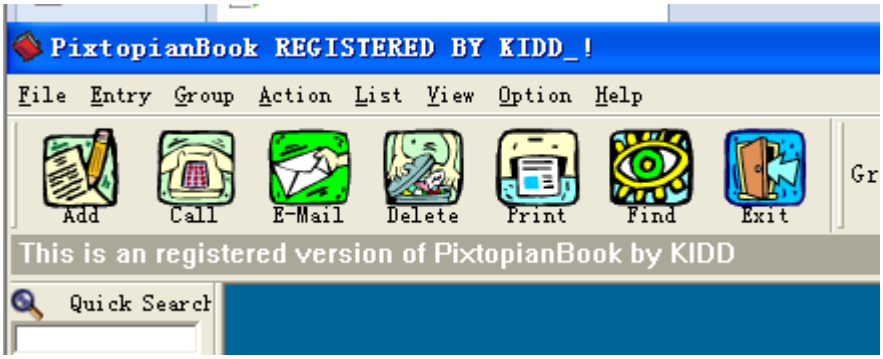


4，这句话

根据

得到地址

然后更改即可：



解决。