QQ斗地主游戏内存数据分析：

已知玩家0出牌数量基址：

0050DEC4



我们首先，对出牌数量下**硬件写入**断点，为了防止中断过长时间，需要操作快一点儿。

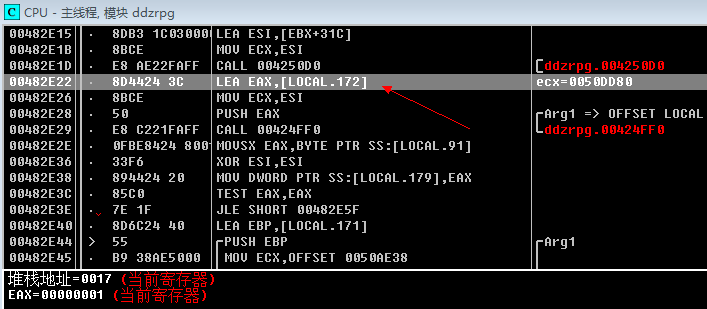


堆栈中的返回地址：

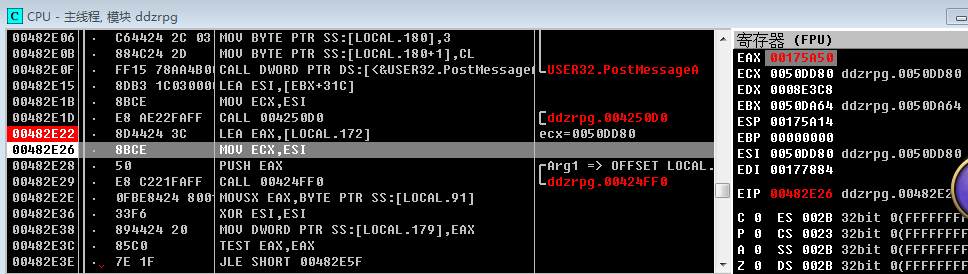
00482E22



然后转到汇编区地址：00482E22处



在此处下F2断点。

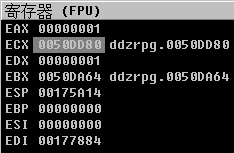


CPU Disasm

地址 十六进制转储 命令 注释

00482E22 |. 8D4424 3C LEA EAX,[LOCAL.172] ; ecx=0050DD80

跟踪寄存器ecx的值为0050DD80 ，然后在数据窗口中



转到这个地址：0050DD80

分析次地址中内存数据，切换成16进制形式



可见，从地址：0050DD80开始每两个字节代表一个牌数，例如上图中

可以读取的第一张牌是0401（注意高低位）表示黑桃4，依次往下每2个字节

表示一张牌。

牌面特点:

黑桃 梅花 红桃 方块

01 03 02 04

牌数特点:

A 2 3 4 5 6 7 8 9 10 J Q K 小王 大王

1 2 3 4 5 6 7 8 9 A B C D E F

两者组合特点：

0A01 – 黑桃A

0A02 – 梅花A

0E00 – 小王

0F00 – 大王

1号玩家



也是00482E22

依次可以跟踪出1号和二号玩家出牌的信息

（为了简便可以自己切换桌位号方法跟踪）

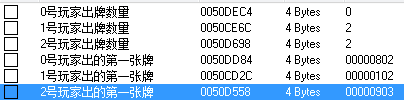
0050CD28

出牌信息的基址：0050CD28

2号玩家

出牌信息的基址：0050D554

下面用CE工具去测试一下：



这里将基址后移1个字节（4byte），然后显示4Byte，

之后的每两个字节显示一张牌

编程指导：

每次获取玩家出牌信息，必须先获取当前玩家出牌数量n，

然后根据n来获取玩家详细的出牌信息，否则遍历出的牌信息

有可能是上一下玩家出牌的信息。

例如：获取n=0，表示玩家当前没有出牌，或者过牌，不要牌；

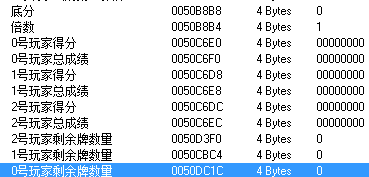
N=1，表示玩家出来一张牌之间取基址+8byte；

N=2，需要过滤出来两张牌信息，之后的牌信息要舍弃掉，

因为是上一次的出牌信息；

依次类推。

CE遍历玩家其他信息





QQ斗地主座位号分布:



在内存中是以 0,1,2数值表示。

