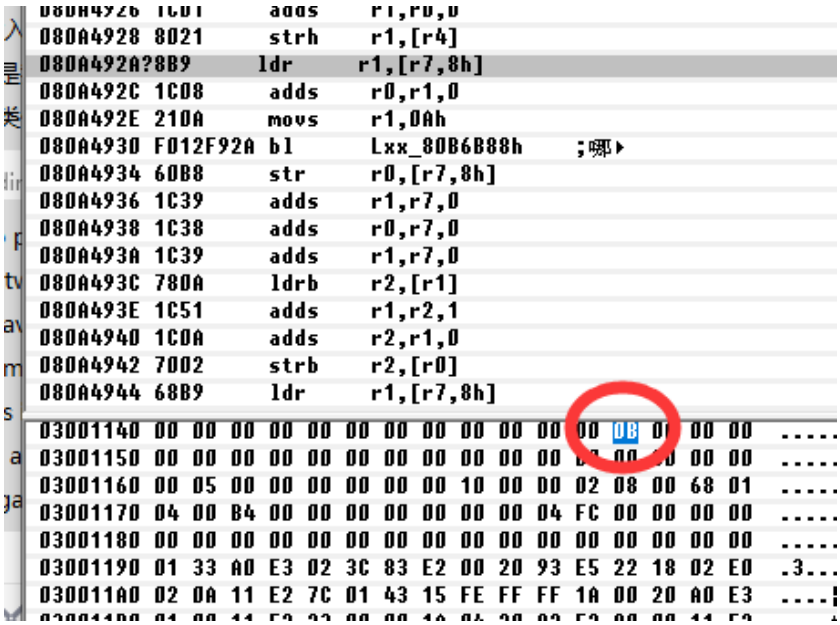
我们拿 0025 为例

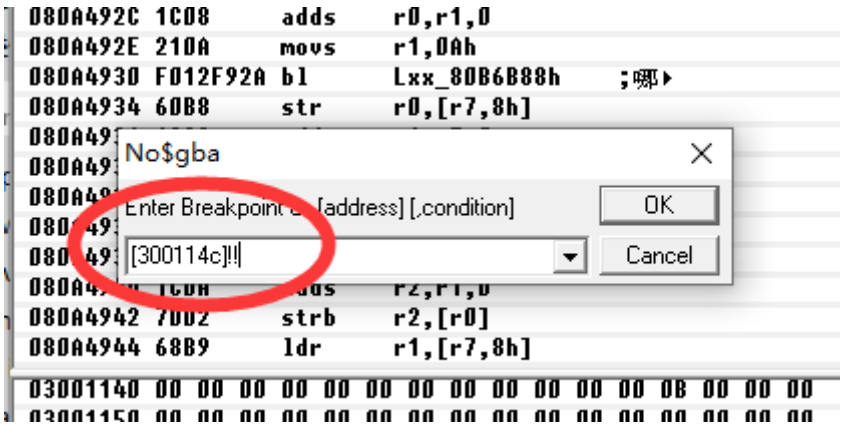
1、打开金手指文件，找到分数项，找到地址，4114C，转换为正确地址为 0x300114C。

```
[SM分数99999990]
ON=4114C,7F,96,98
```

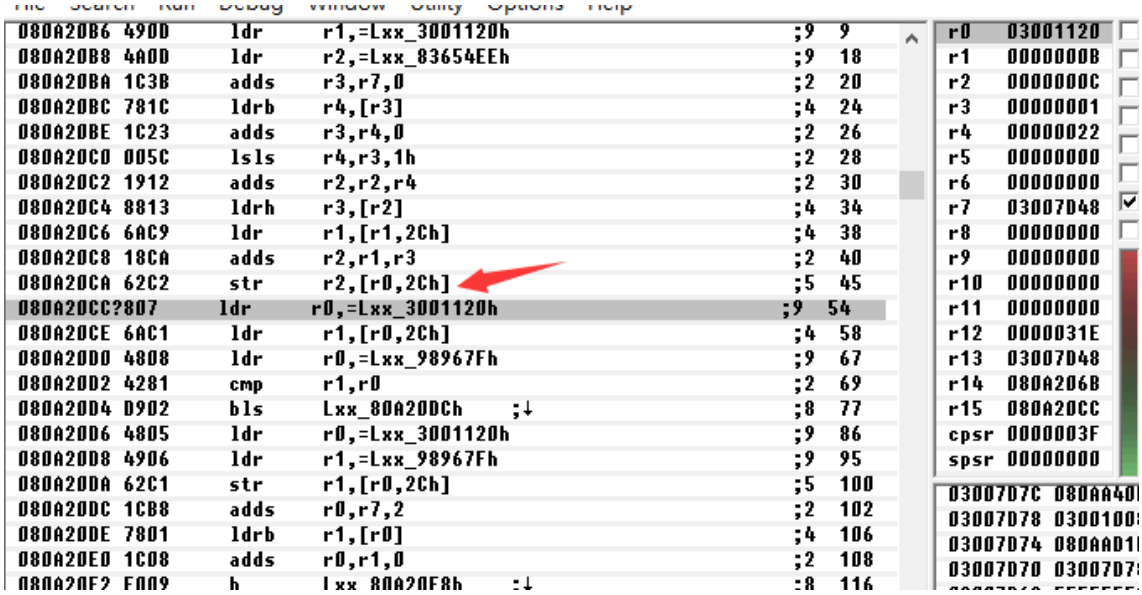
2、用 NO$GBA 打开游戏，定位到数据位置



3、加一个断点，看哪部分代码往这个地址写数据



4、运行游戏，改变积分，可以触发断点



5、 上面的断点地址往上找合适的跳转地址，这里取 080A20C0。修改 patch.s 里面的代码，把代替掉的代码补回来，预先下载安装好 devkitARM，修改好 “makebin.bat” 里面的路径。双击执行 makebin.bat，正确的话生成 patch.bin

```
080A20BE 1C23      adds    r3,r4,0                 ;
080A20C0 00E3      lsls    r4,r3,1h                ;
080A20C2 1912      adds    r2,r2,r4                ;
080A20C4 8813      ldrh    r3,[r2]                 ;
080A20C6 6AC9      ldr     r1,[r1,2Ch]             ;
080A20C8 18CA      adds    r2,r1,r3                ;
080A20CA 62C2      str     r2,[r0,2Ch]             ;
080A20CC?807       ldr     r0,=Lxx_3001120h        ;9
080A20CE 6AC1      ldr     r1,[r0,2Ch]             ;
080A20D0 4808      ldr     r0,=Lxx_98967Fh         ;
080A20D2 4281      cmp     r1,r0                   ;
080A20D4 D902      bls     Lxx_80A20DCh    ;↓      ;
080A20D6 4805      ldr     r0,=Lxx_3001120h        ;
080A20D8 4906      ldr     r1,=Lxx_98967Fh         ;
080A20DA 62C1      str     r1,[r0,2Ch]             ;
080A20DC 1CB8      adds    r0,r7,2                 ;
```

```
  .global main
main:
   LSL   R4, R3, #1
   ADD   R2, R4

  push {r1-r5}
  ldr   r1,=0xD200
```

6、 在游戏 ROM 里面找到一处合适的空地址，这里是 3E7900，把 patch.bin 的内容复制到这里。

```
003E78B0  FF FF FF FF 00 00 00 00  00 00 00 00 00 00 00 00
003E78C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
003E78D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
003E78E0  00 00 00 00 FF FF FF FF  FF FF FF FF FF FF FF FF
003E78F0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
003E7900  5C 00 12 19 3E B4 0D 49  0D 4A 0E 4B 19 80 0E 4B
003E7910  1A 80 0E 4B 19 80 0E 4B  1A 80 0E 4B F1 21 19 80
003E7920  0D 4B 1A 80 0D 4C 02 25  25 70 C0 46 C0 46 C0 46
003E7930  C0 46 00 25 25 70 3E BC  70 47 00 00 00 D2 00 00
003E7940  00 15 00 00 00 00 FE 09  00 00 00 08 00 00 02 08
003E7950  00 00 04 08 00 00 E2 09  00 00 FC 09 00 10 00 08
003E7960  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
003E7970  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
003E7980  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
```

7、 计算跳转地址，即从 0xA20C0 跳转到 0x3E7900。这里要区分 arm32 位的代码还是 thumb16 位的代码。这个游戏是 16bit 的。

0x3E7900-0xA20C0=0x345840

0x345840-4=0x34583C

High=0x34583C>>12=0x345

Low=(0x34583C&0xFFF)/2=0xC1E

machineCode = ((0xFF00 | low) << 16) | (0xF000 | high)= 0xFC1EF345

```
000A20C0  45 F3 1E FC 13 88 C9 6A  CA 18 C2 62 07
000A20D0  08 48 81 42 02 D9 05 48  06 49 C1 62 B8
000A20E0  08 1C 09 E0 E8 5C 00 03  A3 03 00 00 20
000A20F0  EE 54 36 08 7F 96 98 00  01 B0 90 BC 02
000A2100  90 B5 81 B0 6F 46 39 1C  08 70 78 1C 0A
000A2110  3A 1C 13 78 1C 1C 62 00  0B 1C 08 4B C9
000A2120  11 88 0A 1C 02 70 78 1C  01 78 11 29 08
```

8、加载修改好的 ROM，查看修改得对不对

```
080A20BC 781C      ldrb    r4,[r3]
080A20BE 1C23      adds    r3,r4,0
080A20C0 F345FC1E  bl      Lxx_83E790Dh    ;哪
080A20C4 8813      ldrh    r3,[r2]
080A20C6 6AC9      ldr     r1,[r1,2Ch]
```