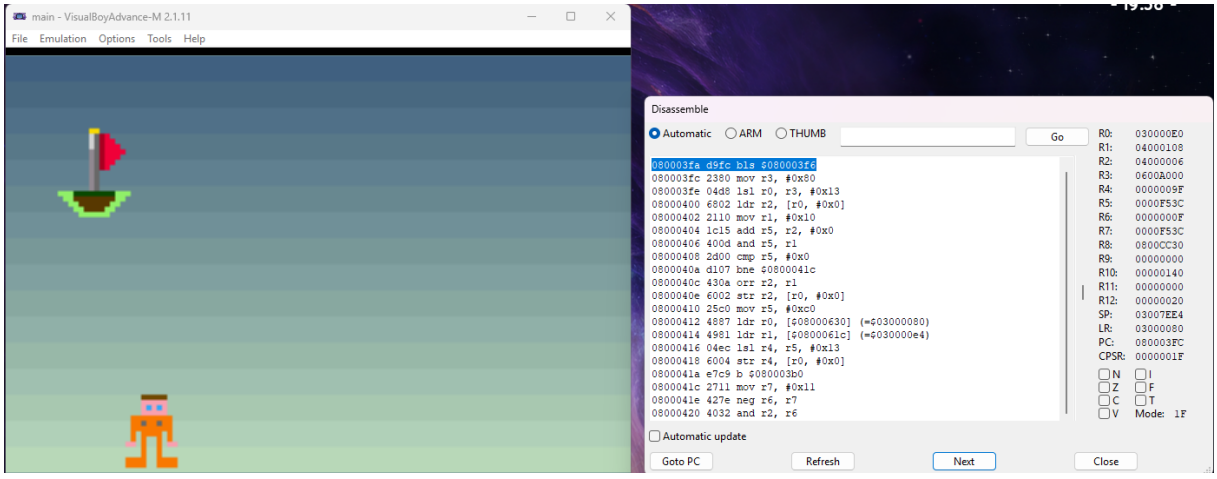
Reverse : JumpBoy (Medium)

Tool Utilisé :

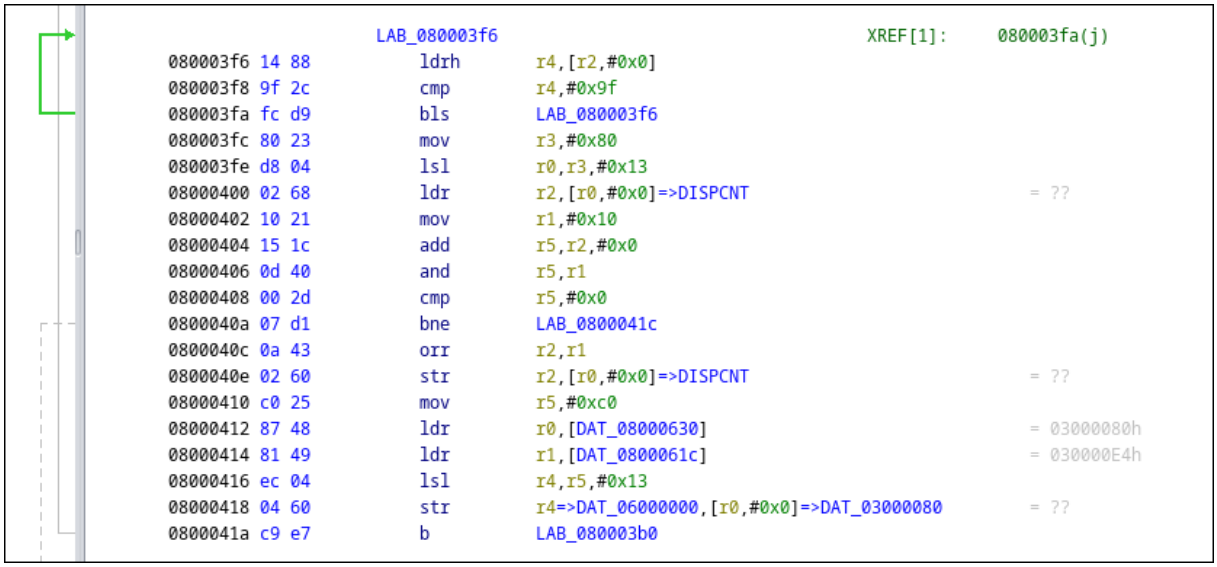
- VisualBoyAdvance (Pour ouvrir le jeu)
- Ghidra (Pour le reverse) avec l'extension GhidraGBA
- Hexedit (Pour les patchs)

➔ En premier lieux, ouvrez le jeu afin de pouvoir comprendre ce qu'il en est. Celui-ci, vu allez vite vous en rendre compte, est actuellement impossible.

➔ Avec « VisualBoyAdvance » vous pouvez, pendant que vous jouez, avoir un aperçut désassemblé. En faisant, « Next », vous pouvez donc apercevoir très rapidement la boucle infinie qui fait tourner le jeu. Le « BLS », vous guidera.



➔ Ouvrez donc maintenant le .gba avec ghidra afin de pouvoir en explorer le contenu. Une fois ceci fait, cherchez la fonction du while trouvée (080003fa, dans mon cas).

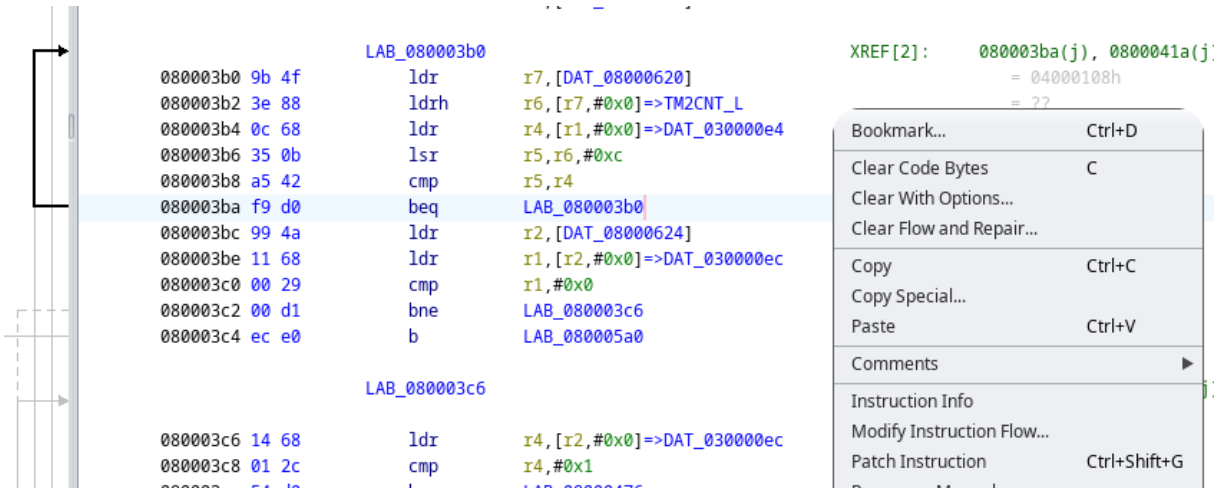


```
                        LAB_080003f6                                    XREF[1]:     080003fa(j)
080003f6 14 88          ldrh    r4,[r2,#0x0]
080003f8 9f 2c          cmp     r4,#0x9f
080003fa fc d9          bls     LAB_080003f6
080003fc 80 23          mov     r3,#0x80
080003fe d8 04          lsl     r0,r3,#0x13
08000400 02 68          ldr     r2,[r0,#0x0]=>DISPCNT                   = ??
08000402 10 21          mov     r1,#0x10
08000404 15 1c          add     r5,r2,#0x0
08000406 0d 40          and     r5,r1
08000408 00 2d          cmp     r5,#0x0
0800040a 07 d1          bne     LAB_0800041c
0800040c 0a 43          orr     r2,r1
0800040e 02 60          str     r2,[r0,#0x0]=>DISPCNT                   = ??
08000410 c0 25          mov     r5,#0xc0
08000412 87 48          ldr     r0,[DAT_08000630]                       = 03000080h
08000414 81 49          ldr     r1,[DAT_0800061c]                       = 030000E4h
08000416 ec 04          lsl     r4,r5,#0x13
08000418 04 60          str     r4=>DAT_06000000,[r0,#0x0]=>DAT_03000080 = ??
0800041a c9 e7          b       LAB_080003b0
```

➔ C'est ici que nous devons injecter notre saut nous permettant de gagner au jeu sans réussir à attraper le drapeau. En observant le code décompilé, et les fonctions associés, vous devriez tomber sur une fonction étrange, car celle-ci n'est remplie que dans certaines condition (la condition de victoire).

```
                        LAB_0800042c                                    XREF[1]:     080003d0(j)
0800042c 80 4b          ldr     r3,[DAT_08000630]                       = 03000080h
0800042e 82 4a          ldr     r2,[DAT_08000638]                       = 08003630h
08000430 9c 46          mov     r12,r3
08000432 a0 23          mov     r3,#0xa0
08000434 5e 00          lsl     r6,r3,#0x1
08000436 96 46          mov     lr,r2
08000438 00 25          mov     r5,#0x0
0800043a f0 27          mov     r7,#0xf0
0800043c b0 46          mov     r8,r6
```

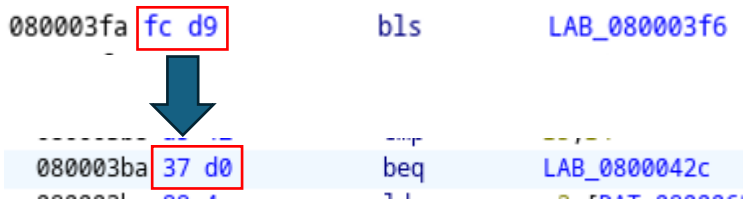
➔ Sélectionnez maintenant la ligne que vous souhaitez patcher et faites : « Patch Instruction », remplacez ensuite la fonction par celle de victoire (42c).



```
                        LAB_080003b0                                    XREF[2]:     080003ba(j), 0800041a(j)
080003b0 9b 4f          ldr     r7,[DAT_08000620]                       = 04000108h
080003b2 3e 88          ldrh    r6,[r7,#0x0]=>TM2CNT_L                  = ??
080003b4 0c 68          ldr     r4,[r1,#0x0]=>DAT_030000e4
080003b6 35 0b          lsr     r5,r6,#0xc
080003b8 a5 42          cmp     r5,r4
080003ba f9 d0          beq     LAB_080003b0
080003bc 99 4a          ldr     r2,[DAT_08000624]
080003be 11 68          ldr     r1,[r2,#0x0]=>DAT_030000ec
080003c0 00 29          cmp     r1,#0x0
080003c2 00 d1          bne     LAB_080003c6
080003c4 ec e0          b       LAB_080005a0

                        LAB_080003c6
080003c6 14 68          ldr     r4,[r2,#0x0]=>DAT_030000ec
080003c8 01 2c          cmp     r4,#0x1
```

➔ Afin d'éviter tout addons ghidra complexe pour exporter les modifications de quelques données hexadécimales, il vous suffit d'analyser les modifications (en hexa), une fois celle-ci effectué sur ghidra.



➔ Ouvrez un éditeur hexadécimal et faite la même opération.

➔ Enregistrez vos modifications et ouvrez le jeu avec un émulateur. Félicitation ! Vous avez le Flag !