

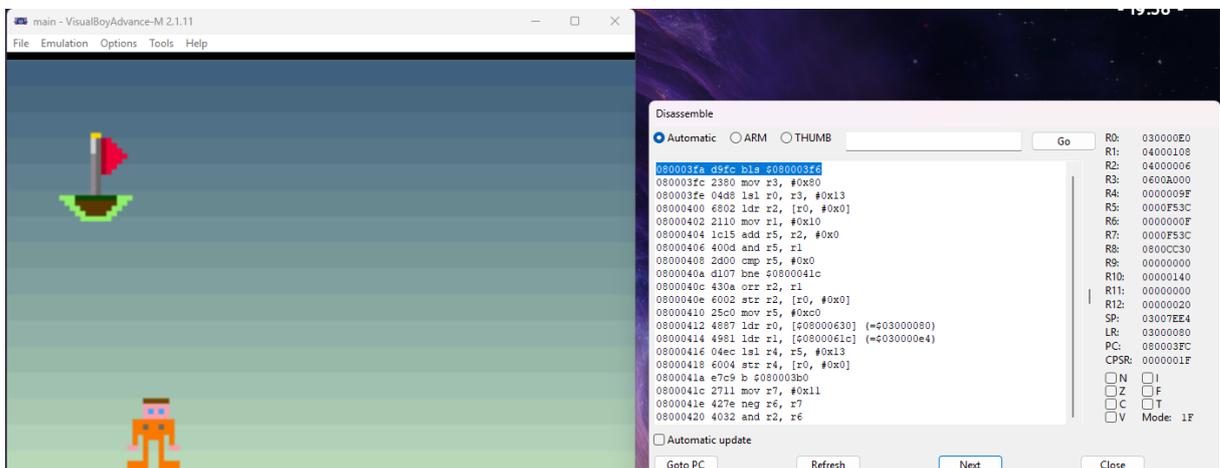
Reverse : JumpBoy (Medium)

Tool Utilisé :

- VisualBoyAdvance (Pour ouvrir le jeu)
- Ghidra (Pour le reverse) avec l'extension [GhidraGBA](#)
- Hexedit (Pour les patches)



- ➔ En premier lieu, 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

```

Bookmark...	Ctrl+D
Clear Code Bytes	C
Clear With Options...	
Clear Flow and Repair...	
Copy	Ctrl+C
Copy Special...	
Paste	Ctrl+V
Comments	
Instruction Info	
Modify Instruction Flow...	
Patch Instruction	Ctrl+Shift+G

→ 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.

```
080003fa fc d9 bls LAB_080003f6
      ↓
080003ba 37 d0 beq LAB_0800042c
```

→ Ouvrez un éditeur hexadécimal et faite la même opération.

```
00000000 2E 00 00 EA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000058 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000084 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000B0 30 31 96 00 00 00 00 00 00 00 00 00 00 F0 00 00 06 00 00 EA 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000DC 00 00 00 00 12 00 A0 E3 00 F0 29 E1 AC D0 9F E5 1F 00 A0 E3 00 F0 29 E1 A4 D0 9F E5 01 00 8F E2
00000108 40 01 0C D3 40 23 1B 03 DA 01 16 1C 91 00 00 F0 3C F8 30 47 40 21 09 03 C8 01 00 F0 2D F8 03 20
00000134 09 1A 00 F0 23 F8 1E 49 1E 4A 1F 4C 00 F0 25 F8 1E 49 1F 4A 1F 4C 00 F0 20 F8 1F 4A 1F 49 53 1A
00000160 1F 4C 00 F0 14 F8 1F 4A 1F 49 53 1A 02 D0 1F 4A 00 F0 0F F8 1E 48 1F 49 8E 46 00 47 C0 46 C0 46
0000018C 70 47 A3 1A 03 D0 01 C9 01 C2 04 3B FB D1 70 47 A0 7F 00 03 00 7F 00 03 00 00 00 08 F0 7E 00 00
000001B8 DC 00 00 03 48 08 00 03 48 CD 00 08 00 00 00 03 7C 00 00 03 30 D5 00 08 30 D5 00 08 48 08 00 03
000001E4 30 D5 00 08 30 D5 00 08 00 00 00 02 31 03 00 08 E0 00 00 08 00 B5 26 48 01 88 10 20 08 40 00 28
00000210 11 0C 00 29 28 D0 1F 4A 11 88 40 20 08 40 02 04 11 0C 00 29 16 D0 1B 4A 11 88 80 20 08 40 00 28
0000023C 02 88 03 88 00 BD 15 4A 50 68 02 30 50 60 40 28 F1 DD 40 21 51 60 EE E7 11 48 02 68 00 2A E4 D0
00000268 0B 4A 10 68 02 38 10 60 00 28 02 DB 0B 49 D1 60 CD E7 11 60 FA E7 06 4A 11 68 02 31 11 60 68 29
00000294 30 01 00 04 90 00 00 03 00 01 00 03 F8 00 00 03 30 30 00 08 30 32 00 08 10 B5 1A 49 1A 48 8C 68
000002C0 00 DD 8B 60 48 68 8B 68 C4 18 4C 60 40 2C 1E DD 40 20 00 22 48 60 8A 60 12 49 01 24 0C 60 0E 48
000002EC 0E DA CB 1C 9A 42 0B DD 41 68 62 68 08 1C 0D 30 82 42 05 DA C8 1C 82 42 02 DD 09 49 02 23 0B 60
00000318 90 00 00 03 F4 00 00 03 FC 00 00 03 00 01 00 03 88 00 00 03 EC 00 00 03 F0 B5 57 46 46 46 C0 B4
00000344 D1 04 0D 4E 08 80 0D 4B 2F 80 04 35 2E 80 0D 49 EE 3D 0D 48 2B 80 0F 22 06 35 2B 80 14 24 4A 60
00000370 09 25 13 E0 82 00 00 00 05 04 00 00 84 00 00 00 80 00 00 00 0A 01 00 04 90 00 00 03 30 32 00 08
0000039C 18 24 37 60 77 60 05 60 44 60 82 60 9B 48 00 21 01 60 9B 49 9B 4F 3E 88 0C 68 35 0B A5 42 37 D0
```

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

