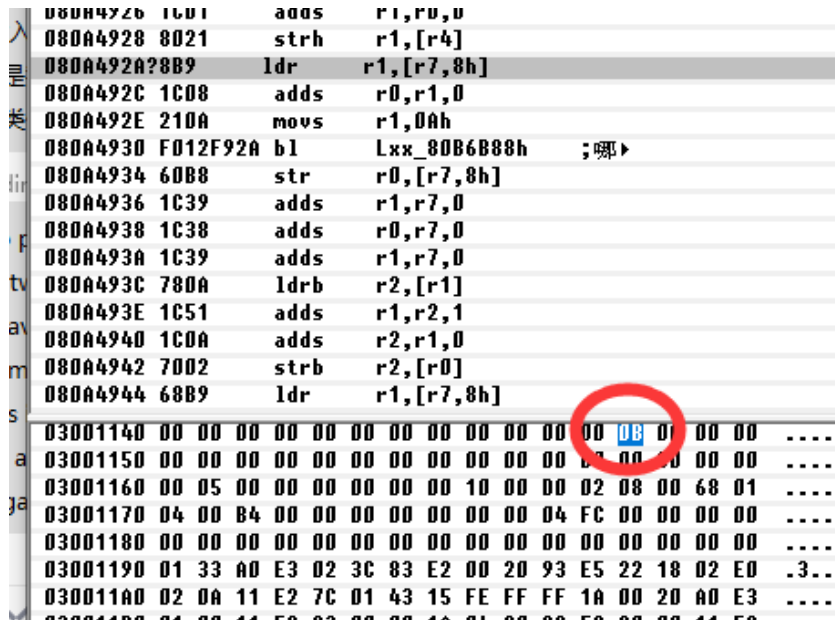


Let us use 0025 Super Mario Advance EU for example.

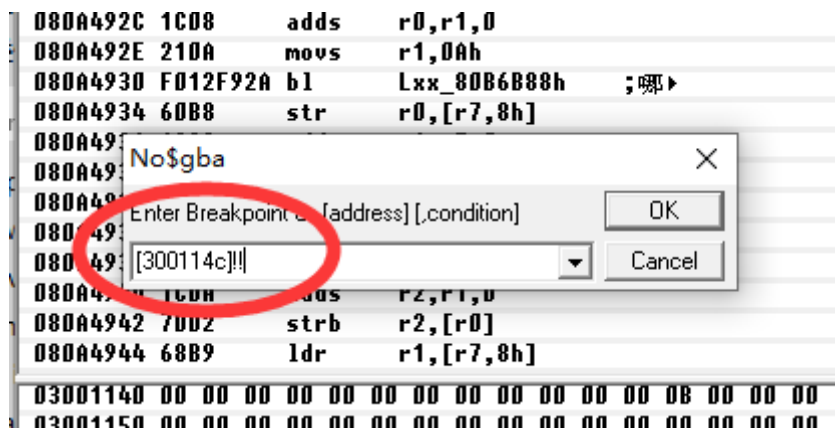
1. Open the corresponding CHT file. Find the Score option, address is 4114C, convert to normal address 0x300114C

[SM分数99999990]
ON=4114C,7F,96,98

- 1、 Use NO\$GBA open the game, locate to the address



- 2、 Add a breakpoint, looking for which code write data to this address



- 3、 Run the game, change the score, it can trigger the breakpoint.

080A20B6	490D	ldr	r1,=Lxx_3001120h	;9	9	r0	03001120
080A20B8	4A0D	ldr	r2,=Lxx_83654EEh	;9	18	r1	00000008
080A20BA	1C3B	adds	r3,r7,0	;2	20	r2	0000000C
080A20BC	781C	ldrb	r4,[r3]	;4	24	r3	00000001
080A20BE	1C23	adds	r3,r4,0	;2	26	r4	00000022
080A20C0	005C	lsls	r4,r3,1h	;2	28	r5	00000000
080A20C2	1912	adds	r2,r2,r4	;2	30	r6	00000000
080A20C4	8813	ldrh	r3,[r2]	;4	34	r7	03007D48
080A20C6	6AC9	ldr	r1,[r1,2Ch]	;4	38	r8	00000000
080A20C8	18CA	adds	r2,r1,r3	;2	40	r9	00000000
080A20CA	62C2	str	r2,[r0,2Ch]	;5	45	r10	00000000
080A20CC?807		ldr	r0,=Lxx_3001120h	;9	54	r11	00000000
080A20CE	6AC1	ldr	r1,[r0,2Ch]	;4	58	r12	0000031E
080A20D0	4808	ldr	r0,=Lxx_98967Fh	;9	67	r13	03007D48
080A20D2	4281	cmp	r1,r0	;2	69	r14	080A2068
080A20D4	0902	bis	Lxx_80A20DCh ;↓	;8	77	r15	080A20CC
080A20D6	4805	ldr	r0,=Lxx_3001120h	;9	86	cpsr	0000003F
080A20D8	4906	ldr	r1,=Lxx_98967Fh	;9	95	spsr	00000000
080A20DA	62C1	str	r1,[r0,2Ch]	;5	100		
080A20DC	1CB8	adds	r0,r7,2	;2	102		
080A20DE	7801	ldrb	r1,[r0]	;4	106		
080A20E0	1C08	adds	r0,r1,0	;2	108		
080A20F2	F009	h	Lxx_80A20F8h ;↓	;8	116		

- 4、 Use the upper breakpoint find the above jump address. Here is 080A20C0. Modify the code in patch.s, replace the code, if you' d downloaded and installed devkitARM before, modify the path in "makebin.bat, double click to run makebin.bat, the patch.bin will be created if everything correct.

080A20BE	1C23	adds	r3,r4,0	;2	20
080A20C0	005C	lsls	r4,r3,1h	;2	28
080A20C2	1912	adds	r2,r2,r4	;2	30
080A20C4	8813	ldrh	r3,[r2]	;4	34
080A20C6	6AC9	ldr	r1,[r1,2Ch]	;4	38
080A20C8	18CA	adds	r2,r1,r3	;2	40
080A20CA	62C2	str	r2,[r0,2Ch]	;5	45
080A20CC?807		ldr	r0,=Lxx_3001120h	;9	54
080A20CE	6AC1	ldr	r1,[r0,2Ch]	;4	58
080A20D0	4808	ldr	r0,=Lxx_98967Fh	;9	67
080A20D2	4281	cmp	r1,r0	;2	69
080A20D4	0902	bis	Lxx_80A20DCh ;↓	;8	77
080A20D6	4805	ldr	r0,=Lxx_3001120h	;9	86
080A20D8	4906	ldr	r1,=Lxx_98967Fh	;9	95
080A20DA	62C1	str	r1,[r0,2Ch]	;5	100
080A20DC	1CB8	adds	r0,r7,2	;2	102

```

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

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

```

- 5、 Find a suitable empty address in the ROM, here is 3E7900, copy the data in patch.bin to here.

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

- 6、 Calculate the jump address. From 0xA20C0 to 0x3E7900. Here it is important to distinguish between arm32bit code or thumb16bit code. This game is 16bit.

$0x3E7900 - 0xA20C0 = 0x345840$

$0x345840 - 4 = 0x34583C$

$\text{High} = 0x34583C \gg 12 = 0x345$

$\text{Low} = (0x34583C \& 0xFFF) / 2 = 0xC1E$

$\text{machineCode} = ((0xFF00 | \text{low}) \ll 16) | (0xF000 | \text{high}) = 0xFC1EF345$

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

- 7、 Load the modified game and check the result.

080A20BC	781C	ldrb	r4,[r3]
080A20BE	1C23	adds	r3,r4,0
080A20C0	F345FC1E	b1	Lxx_83E7900h ; 哪▶
080A20C4	8813	ldrh	r3,[r2]
080A20C6	6AC9	ldr	r1,[r1,2Ch]
080A20C8	10C0	adds	r2,r1,r2

The result is when score changes, will send a rumble signal.