




CCIT WORKSHOP
GLITCH THEM ALL

ONE FLAG TO RULE THEM ALL





WHAT I'VE FOUND

```
john@xps15: treasure
```

 **Nostalgia** STAFF PICK
MEDIUM

NO CONNECTION REQUIRED

DIFFICULTY RATING 

40 POINTS 

INFORMATION ACTIVITY CHANGELOG REVIEWS WALKTHROUGHS

SHARE RESULTS

Download Files
Necessary files to play the challenge.

CHALLENGE DESCRIPTION

It's late at night and your room's a mess, you stumble upon an dusty old looking box and you decide to go through it, you start unveiling hidden childhood memories and you find a mesmerising gamebody advanced flash card labeled "Nostalgia", you pop the card in and a logo welcomes you, this strange game expects you to input a cheatcode. Can you figure it out?

```
jo  
$  
SO  
jo  
$  
Vi  
Se  
ZIP PASSWORD  
Searching current directory: /home/john  
Searching home directory: /home/john/.  
Searching system config directory: /etc  
Reading configuration file.  
Color depth: 32
```

A B L R B R L A

```
0000  
0000  
0000  
0000  
0000  
000000000000000000000000  
000000000000000000000000  
SBDPY
```

GB

GB Studio - GB Studio 3

File Edit Game View Window Help

Game World 100%

SCENES

- Cave
- Deep Space
- Deeper Underground
- Dream
- Launch Site
- Logo
- Menu Page 1
- Menu Page 2
- Parallax Example**
- Path to Sample Town
- Player's House
- Sample Town
- Space Battle
- Title Screen
- Top House
- Underground

SCRIPTS

- Init Menu
- Init Weapons

VARIABLES

QUEST LIST

- KEEP ON THE GRASS
- TURNIP TROUBLE
- SNEAK ONBOARD
- HIDDEN TREASURE
- HIDE N SEEK

Player's House

Parallax Example

Space Battle

Underground

Deeper Underground

Search...

Parallax Example

Type: Platformer

Background: parallax (Size: 80x18, Tiles: 191)

Parallax: 3 Layers

1	H	10	Speed 1/16
2	H	3	Speed 1/2
3	H	18	Speed 1

Background Palettes

Sprite Palettes

Player Sprite Sheet: player_platform (Type: Sprite, Tiles: 17)

On Init On Player Hit

Call Script: InitMenu



Hacking della Nintendo GAME BOY™

541.232 visualizzazioni

stacksmashing

In questo video hackerian...

Sottotitoli Inglese

The Checkin...



HO HACKERATO

181.733 visualizzazioni

Otto Climax

In questo video sono riuso...

4K Sottotitoli



Cartuccia Wi-

948.599 visualizzazioni

there oughta be

Ho creato una cartuccia p...

4K Sottotitoli

there.oughta.be/a/wifi-game-boy-cartridge

REVERSING GAMEBOY

The image displays a collection of windows used for reverse engineering a Game Boy ROM. The main window on the left is a listing for 'Tetris (World) (Rev 1).gb', showing assembly code and data. The middle window is a decompiler for 'disable_ppu', showing the corresponding C code. The top-right window is a memory viewer for 'pokecrystal.gbc' showing ROM data. The bottom-left window is a VRAM viewer showing a tilemap. The bottom-right window is a debug console for 'pokecrystal.gbc' showing a breakpoint hit and register values.

```
Listing: Tetris (World) (Rev 1).gb
*****
*                               FUNCTION
*****
void __asm disable_ppu(void)
<VOID> <RETURN>
HASH:13f5880... ly
HASH:13f22d2... lcdc
disable_ppu
2820 f0 ff LDH A,(0xff)
2822 e0 a1 LDH (offset ie_save),A
2824 cb 87 RES 0x0,A
2826 e0 ff LDH (0xff),A

LAB_2828
2828 f0 44 LDH A,(offset LY)
282a fe 91 CP 145
282c 20 fa JR NZ,LAB_2828
282e f0 40 LDH A,(offset LCDC)
2830 e6 7f AND 0x7f
2832 e0 40 LDH (offset LCDC),A
2834 f0 a1 LDH A,(offset ie_save)
2836 e0 ff LDH (0xff),A
2838 c9 RET

data_2839
2839 2f 2f 11 db{80}
12 1d 2f
2f 2f 2f ...

data_2889
2889 1c 12 17 db{181}
10 15 0e
2f 2f 2f ...

data_293e
293e 61 62 62 db{56}
62 62 62
62 63 64 ...

data_2976
2976 19 15 0e db{48}
0a 1c 0e
2f 2f 29 ...

*****
*                               FUNCTION
*****
void __asm update_joypad_state(void)
<VOID> <RETURN>
update_joypad_state
29a6 3e 20 LD A,0x20
29a8 e0 00 LDH (0x0)=>P1,A
29aa f0 00 LDH A,(0x0)=>P1
29ac f0 00 LDH A,(0x0)=>P1
29ae f0 00 LDH A,(0x0)=>P1
29b0 f0 00 LDH A,(0x0)=>P1
29b2 2f 2f 2f ...

Decompile: disable_ppu - (Tetris (World) (Rev 1).gb)
1 void disable_ppu(void)
2 {
3   byte ly;
4   byte lcdc;
5
6   ie_save = IE;
7   IE = ie_save & 0xfe;
8   do {
9     ly = LY;
10    } while (ly != 145);
11    lcdc = LCDC;
12    LCDC = lcdc & 0x7f;
13    IE = ie_save;
14    return;
15 }
16
17
18

Memory
ROM $25 pc+8
Address Space Bank
6770 68 04 C9 CD B0 67 CD C1 67 3E 25 21 08 7E CF CD h...0=g0jg>%! ~æ0
6780 95 67 FA 32 D4 FE 02 C0 CD D1 67 CD B7 67 CD E1 ig'2', z0-g0Σg0·
6790 67 CD F4 67 C9 FA 33 D4 21 90 67 EF C9 A1 67 AE g0Ùg...3'!ùg0...gÆ
67A0 67 CD 1F 68 CD CB 66 3E 25 21 5E 6C CF C9 C9 02 g0 h0Àf>%!^!æ...
67B0 FA AF 67 EA B1 CF C9 FA B1 CF A7 C8 4F CD 68 04 '0gI±æ...±æ8»00h
67C0 C9 FA 33 D4 FE 01 C8 CD A7 05 CD 84 09 CD 7E 04 ...'3', »08 0N 0~
67D0 C9 3E 01 21 6A 57 CF 3E 03 21 97 54 CF CD 12 68 ...> !jWæ> !6Tæ0 h
67E0 C9 3E 01 21 20 59 CF 3E 03 21 D2 54 CF 3E 2E 21 ...> ! Yæ> !"Tæ>.!
67F0 98 40 CF C9 FA 50 D1 CB 6F 28 0B CB 77 28 0D CB ò@æ...P-ÀoC ÅwC Å
6800 67 20 09 CD D0 66 3E 00 EA 33 D4 C9 3E 01 EA 33 g 0-f> I3'... I3
6810 D4 C9 21 50 D1 CB 76 C8 3E 02 21 CA 41 CF C9 AF 'IP-Av»> ! Ae...0
3z0%h0gh8 0th
018 0Ih8 0:i8
i8 0...i>%!Vlæ0
0Ik'8', C, C
/-7... 0 60 >
0 gC >A! Hæ8
"8$0 gC 0'*8*
0yky0 gC 0z
0...> 7...%*0T

VRAM Viewer
Effective Palettes Effective Tilemap Effective Tileset Scrolling Grid
[VRAM Viewer content showing a tilemap of a game level]

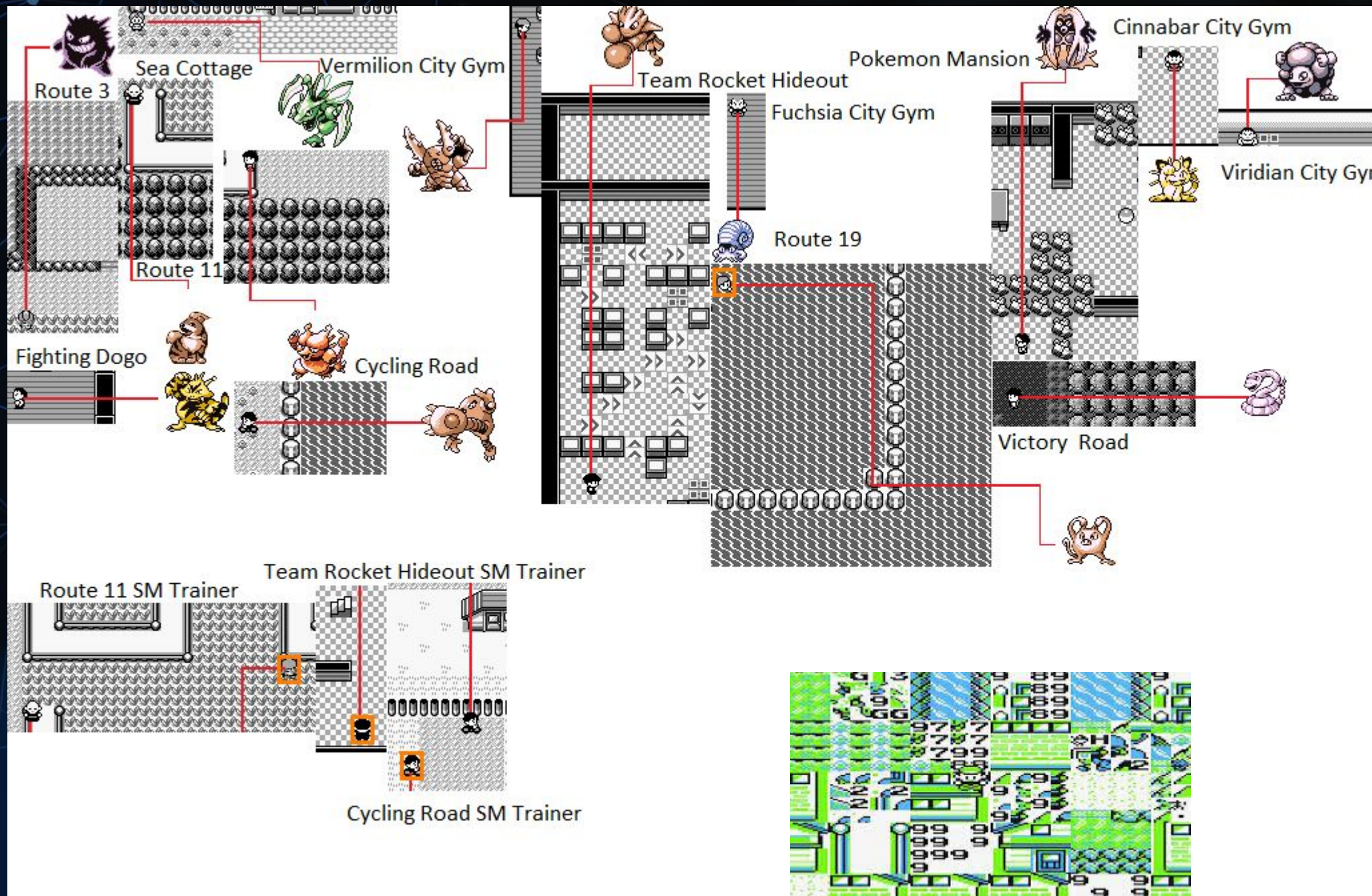
Debug Console - pokecrystal.gbc
>b DelayFrames if a >= 2
Breakpoint set at DelayFrames ($00:$0468)
>c
Breakpoint: PC = DelayFrames ($0468)
DelayFrames:
->0468 <+000>: CALL DelayFrame ;=$045a
046b <+003>: DEC c
046c <+004>: JR nz,.DelayFrames ;.=$0468
046e <+006>: RET

RTC:
046f <+000>: LD a, [$c2ce]
>p de+h1
=$d350 (0TPartyMon5Exp)
>x/32 de+h1
d350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
d360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
>p a=$10
=$0010
>fin
NextOverworldFrame:
->67c0 <+009>: RET

Function967c1:
67c1 <+000>: LD a, [MapEventStatus] ;=$4423

registers
backtrace
registers:
AF = $00c0 (--NZ)
BC = $d600 (ObjectStruct7+$012)
DE = $0200 (Init+$083)
HL = $d150 (CurPartyLevel+$00d)
SP = $c0e7 (RivalTeam+$0c4)
PC = $67c0 (NextOverworldFrame+$009)
backtrace:
1. NextOverworldFrame+$009 ($25:$67c0)
2. HandleMap+$018 ($25:$678b)
3. OverworldLoop+$00a ($25:$66ba)
4. FarCall_hl+$008 ($00:$2d6b)
5. Function5e5d+$018 ($01:$5e92)
6. FarCall_hl+$008 ($00:$2d6b)
7. MainMenu_Continue+$005 ($12:$5ef3)
8. MainMenu+$034 ($12:$5d10)
9. FarCall_hl+$008 ($00:$2d6b)
10. Function5ae8+$018 ($01:$5b1d)
```

GLITCHES



72	Jynx
82	Vulpix
85	Raichu
90	Kabuto
96	Sandshrew
103	Flareon
104	Jolteon
105	Vaporeon
112	Weedle
126	Machop
149	Alakazam
153	Bulbasaur
176	Charmander
177	Squirtle
185	Oddish
188	Bellsprout
55	Koffing



LA LEGGENDA DI MISSING N°



@CentiZen 3 anni fa

MissingNo. was a huge influence on me as a kid, pretty sure it's the main reason I became so interested in coding and hacking as a kid. It was a lot of peoples first exploit.







👍 593 💬 Rispondi




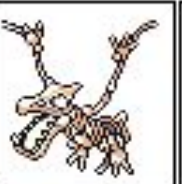

▼ 8 risposte








EVOLUTIONARY RELATIONSHIPS






in the Pokémon Internal ID list





PERIOD 1
PERIOD 5 176-190







					
001	176	177	178	179	180
	CHARMANDER	SQUIRTLE	CHARMELEON	WARTORTLE	CHARIZARD

				
011	181	182	183	184
	MISSINGNO.	MISSINGNO.	MISSINGNO.	MISSINGNO.



						
021	185	186	187	188	189	190
	ODDISH	GLOOM	VILEPLUME	BELLSPROUT	KEEPEINBELL	VICTREBELL





				
033	034	035	036	037


			
072	073	074	075




					
076	077	078	079	080	081



PERIOD 3



				
082	083	084	085	086




				
087	088	089	090	091

				
092	093	094	095	096









				
097	098	099	100	101






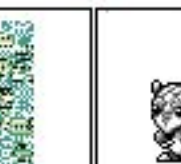


			
102	103	104	105









				
106	107	108	109	110







			
111	112	113	114







PERIOD 3a







							
082	083	084	085	086	087	088	089
VULPIX	NINETALES	PIKACHU	RAICHU	MISSINGNO.	MISSINGNO.	DRATINI	DRAGONAIR

							
090	091	092	093	094	095	096	097
KABUTO	KABUTOPS	HORSEA	SEADRA	MISSINGNO.	MISSINGNO.	SANDSHREW	SANDSLASH

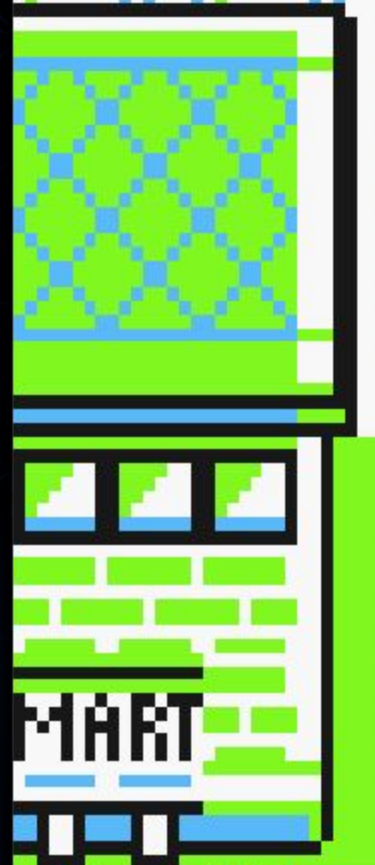
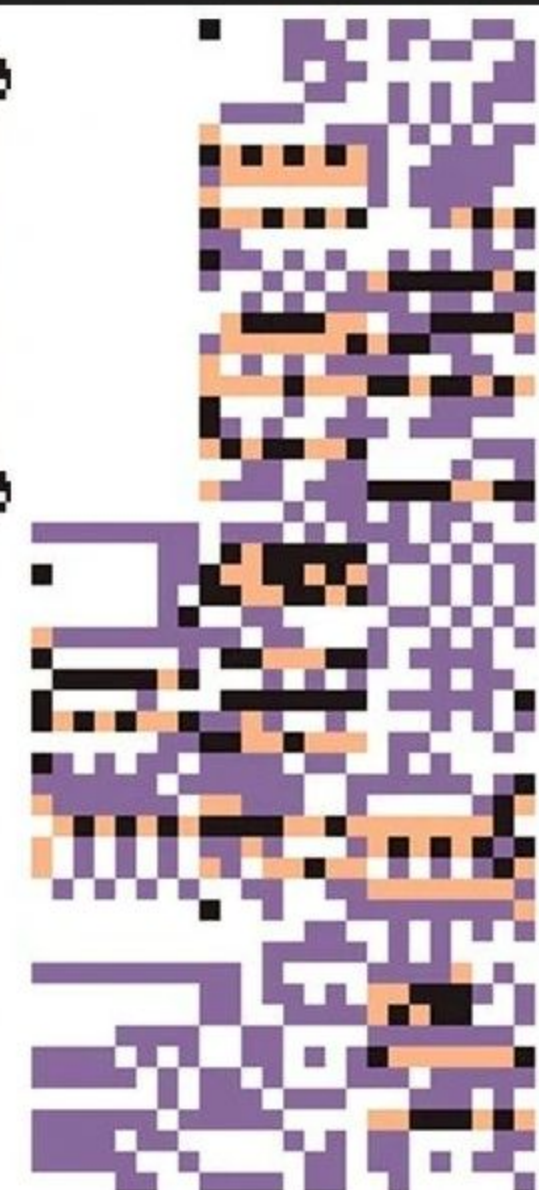
							
098	099	100	101	102	103	104	105
OMANYTE	OMASTAR	JIGGLYPUFF	WIGGLYTUFF	EEVEE	FLAREON	JOLTEON	VAPOREON

					
145	146	147	148	149	150

					
151	152	153	154	155	156

					
185	186	187	188	189	190

Wild MISSINGNO.
appeared!



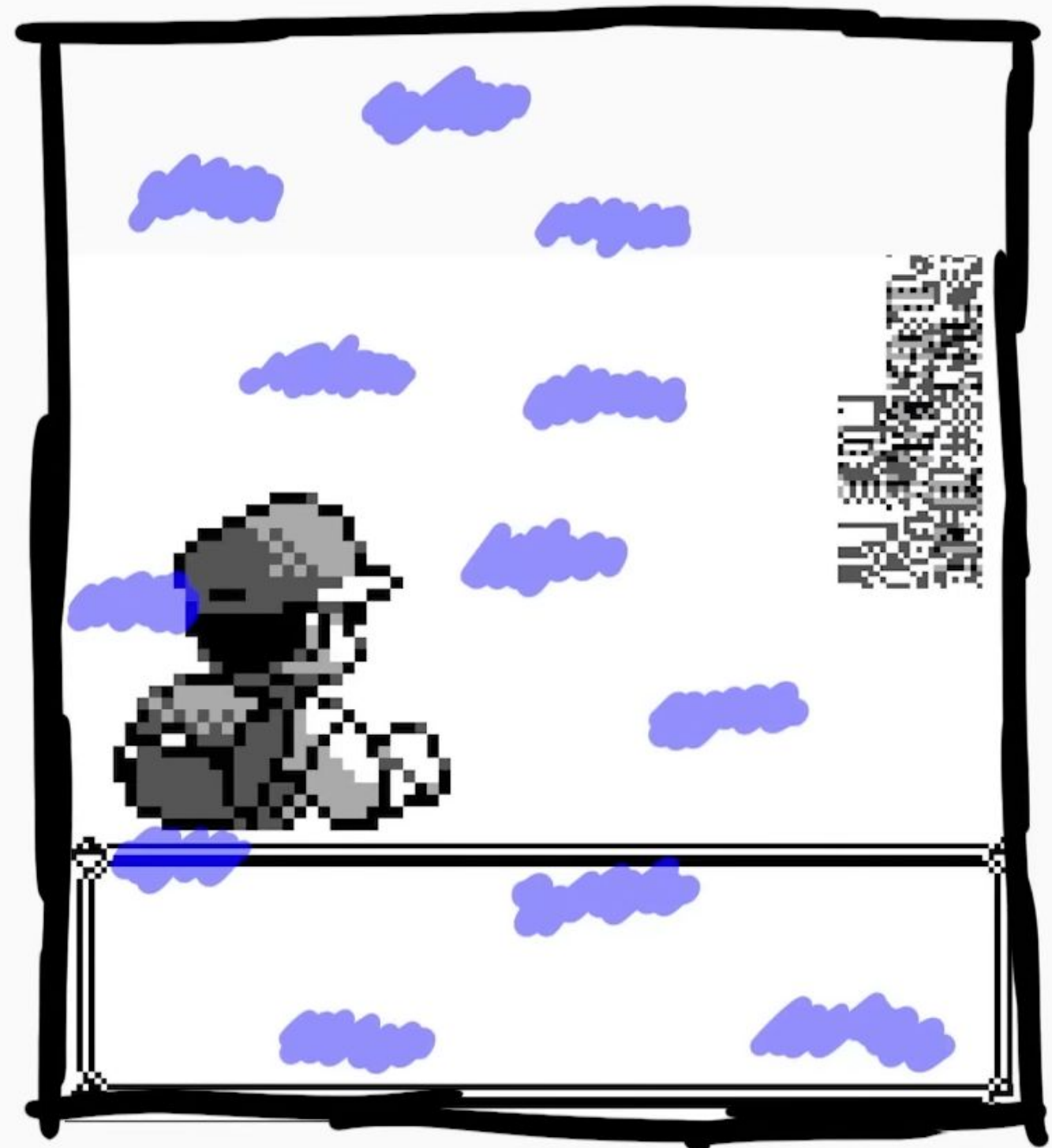
COME SI

A?

writes 



reads 



TENTACOOL

DMG-GBC Debugger

I/O	Palettes	Memory	Disassembly	OBJ Tiles	BG Tiles
0xD7E0	FE 07 0E 00	FE 07 FE C7	FE 03 60 00	7F 7E FF 80~..
0xD7F0	FF FB 7C 00	FE BE 00 00	00 00 00 00	00 00 00 300.
0xD800	00 00 1F 00	1E 00 1E 00	7E 00 00 00	00 00 00 00
0xD810	00 00 5E 00	3E 00 02 00	06 00 D5 00	00 00 00 00^>.....
0xD820	00 00 00 00	3C E0 0C 03	1C 03 3C 07	C0 81 E1 71<.....<...q
0xD830	1C 01 1C 0F	06 01 30 A1	00 00 00 00	00 00 00 000.....
0xD840	00 00 00 00	00 00 02 00	06 00 06 00	00 00 00 00
0xD850	00 00 00 00	00 00 01 00	00 00 00 00	00 00 00 02
0xD860	00 00 00 00	00 00 00 00	06 00 00 00	00 00 00 00
0xD870	00 00 00 00	00 00 00 00	00 00 FE 01	03 03
0xD880	03 04 00 00	00 00 00 00	89 80 82 8A	50 8DP...P.
0xD890	84 3C 4C 3A	BA 3A BD 3A	BD 01 06 61	95 0A 8B	..<L:..<:..a..
0xD8A0	53 68 FF 05	05 18 0A 18	0F 18 05 18	0A 18 0F 18	Sh.....
0xD8B0	14 18 1E 18	23 18 28 18	00 00 00 00	00 00 98 88	...#.(.....
0xD8C0	14 23 15 0F	3D 00 AC 00	89 00 94 00	5E 00 51 95	..#..=.....^..0.
0xD8D0	00 00 00 00	18 18 32 3C	69 5E 86 43	1A 03 0D 3F2<i^.C...?
0xD8E0	00 00 00 00	00 00 00 00	00 00 98 88	14 14 0A 14
0xD8F0	3B 00 8F 00	4A 00 43 00	9C 00 AD 0A	00 00 00 00	;...J.C.....
0xD900	16 18 2D 8C	5F 17 49 43	1A 04 54 4E	00 00 00 00	..._.IC..TN...
0xD910	00 00 00 00	00 00 98 88	14 14 14 00	3D 00 C4 00=.....
0xD920	83 00 76 00	51 00 A7 8B	00 00 00 00	15 19 3C 3A	..v.Q.....<:
0xD930	80 3E 83 43	1A 04 54 4E	00 00 00 00	00 00 00 00	..>.C..TN.....
0xD940	00 00 98 88	14 0A 14 0F	3D 00 8D 00	83 00 EA 00	d.vS.....Km'bSC
0xD950	64 00 76 53	00 00 00 00	14 14 4B 6D	27 62 53 43?...p.m...h
0xD960	1A 03 D0 BF	00 00 00 00	00 00 00 00	00 00 98 88*VbWC..0.
0xD970	19 1E 1E 14	3F 00 AF 00	70 00 6D 00	8D 00 8D 68
0xD980	00 00 00 00	17 17 2D 2A	56 62 57 43	1A 04 30 C1
0xD990	00 00 00 00	00 00 00 00	00 00 98 88	14 14 1E 0A
0xD9A0	41 00 A9 00	65 00 5D 00	B8 00 9E 80	92 87 50 89	A...e.].....P.
0xD9B0	80 82 8A 50	8D 84 80 92	87 50 89 80	82 8A 50 8D	...P....P....P.
0xD9C0	84 80 92 87	50 89 80 82	8A 50 8D 84	80 92 87 50P....P....P
0xD9D0	89 80 82 8A	50 8D 84 80	92 87 50 89	80 82 8A 50P....P....P
0xD9E0	8D 84 80 92	87 50 89 80	82 8A 50 8D	84 00 00 00P....P....
0xD9F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0xDA00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00



ITEM RUN

Refresh Close



0xD880	00 00 00 00	00 00 19 03	4C 04 24 02	A5 03 A5 02
0xD890	4C 03 24 05	24 04 A5 06	4C 07 24 01	7B FF 00 00
0xD8A0	00 00 00 00	00 1E 00 00	07 07 FF 21	51 00 00 81
0xD8B0	83 00 03 E8	00 00 00 00	00 00 00 00	00 00 98 88
0xD8C0	23 28 00 00	0A 00 1E 00	0C 00 0D 00	0F 00 0A 00

0xD880	03 04 00 00	00 00 00 00	92 87 50 89	80 82 8A 50	8D
0xD890	84 3C 4C 3A	BA 3A BD 3C	01 3A 01 06	61 95 0A 8B	
0xD8A0	53 68 FF 00	05 18 0A 18	0F 18 05 18	0A 18 0F 18	
0xD8B0	14 18 1E 18	23 18 28 18	00 00 00 00	00 00 98 88	
0xD8C0	14 23 15 0F	3D 00 AC 00	89 00 94 00	5E 00 51 95	

PERIOD 3a

082	083	084	085	086	087	088	089
VULPIX	NINETALES	PIKACHU	RAICHU	MISSINGNO.	MISSINGNO.	DRATINI	DRAGONAIR
090	091	092	093	094	095	096	097
KABUTO	KABUTOPS	HORSEA	SEADRA	MISSINGNO.	MISSINGNO.	SANDSHREW	SANDSLASH
098	099	100	101	102	103	104	105
OMANYTE	OMASTAR	JIGGLYPUFF	WIGGLYTUFF	EEVEE	FLAREON	JOLTEON	VAPOREON

WHAT'S NEXT?



Wild PIKACHU
appeared!



PRESTARE AT
NIENTE E' DA.

SONO LE PRE
CATTURARE L



MENTALE
-RIEND.

THEM ALL E

[https://github](https://github.com)

TRY ME

[tchThemAll.git](https://github.com/0xFE-AP3/glitchThemAll.git)

<https://github.com/0xFE-AP3/glitchThemAll.git>

I PRIMI 10 SOLVERS ENTRERANNO NELLA HALL OF FAME

6
7
8
9
10