THEZZAZZGLITCH’S GLITCH RESEARCH ARCHIVES

Arbitrary code execution in Red/Blue using the "8F" item
First found and published on: April 25, 2013, 07:57:48 AM

1.1. WHAT’S 8F?

8F is a Red/Blue equivalent of JP Red/Green's 5 かい - an item executing machine code starting from $D163 (Number of Pokemon) upon use. Its hex identifier is 0x5D, despite its hex-like name. 8F is treated by the game as a key item and it can't be tossed away or sold in the mart.

As address $D163 contains re-writeable data, it is possible to redirect the instruction pointer to the item list with relative jumps and easily run arbitrary code just by spelling the opcodes with items. With enough items, one could also make a program that reads key input continuously, writes it somewhere in the RAM and jumps to it after a while, allowing to even run your own homebrew software (jailbreaking the gameboy, lolz).

1.2. HOW TO OBTAIN IT

There’s still no reliable way to obtain 8F. There are two ways to accomplish this, but they do not always work.

Obtaining 8F using invalid encounter flags:

:: **Prerequisites:**
- A Ditto with a Cooltrainer move, nicknamed "R:u"
- At least 1 Escape Rope
- Good Rod on your 4th item slot
- Exactly 10 Pokemon in your current box (this tremendously increases the chances of Cooltrainer move working properly)
- Preferably a Bicycle, to make things a little bit faster.

:: Execution:
1. Heal your Pokemon in Fuchsia City's Pokemon Center.
2. Do the Safari Zone walk through walls glitch, with only Ditto in your party.
3. After you appear back at the Fuchsia City's Center with noclip activated, walk exactly:
a) 19 steps west
b) 28 steps north
c) 1 step west
d) 29 steps north
e) 11 steps east
4. Open your Pokemon menu and close it (important). You may want to use bicycle now to travel faster - you won't be able to do this later.
5. Go 11 steps west and keep walking south until you find yourself back on Route 18. Do not open your Start menu from now on.

6. Walk/bike to Seafoam Islands and enter the cave.
7. Encounter a wild Pokemon, and continuously try to use the Cooltrainer move. If it does not work after about 15 tries, quit the battle and start a new one. Do not open your Pokemon menu, Item menu or Start menu at all!
8. Eventually, the music will fade out, the move typing will become blank, and name of the opponent will get changed. Catch the resulting Pokemon - the game will state you caught a "98", and your Good Rod will turn into an 8F.
9. Use an Escape Rope, as there's a slight chance the game will crash after exiting the cave normally.

Obtaining 8F with a corrupted item pack (obsolete):

This method is not recommended - it has a lot of side effects and is terribly complicated. Use it only when the encounter flag method does not seem to work for you.

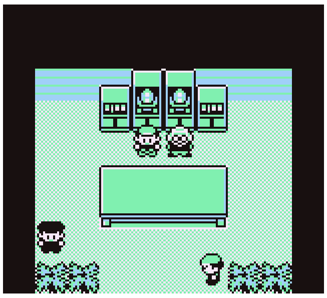
:: **Prerequisites:**
- A Pokemon on the first slot meeting very specific requirements:
  > It needs to have a Super Glitch as a 4th move
  > Its three moves besides the Super Glitch have to contain 25 characters in total
  > One of its three moves needs to be 4 characters long
  > This Pokemon needs to be able to learn Mega Kick through TM05
  An example: ゥ L || ゥ M 4 (hex C6) with moves Body Slam, TM50, Quick Attack, [Super Glitch]
- Any Pokemon on the second slot you don't care about, nicknamed "cccccccc". It will be gone in the process, so don't use your L100 Charizard.
- A Pokemon on the third slot knowing Fly.
- Exactly 3 useless items in your Bag. They will get destroyed again, so don't pick anything important.
- TM05 (Mega Kick), deposited in the PC
- At least one free space in the PC to store your obtained 8F
- An empty Pokemon box currently selected, most likely box 12

:: Side effects:
Sadly, those side effects are actually quite annoying. But also, happily enough, one can fix them with 8F's arbitrary code execution.

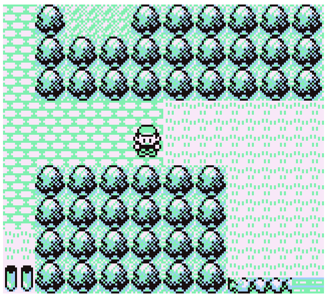
1. Your player name will become blank (the game will save just fine though). However, with 8F's arbitrary code execution capabilities, one can change his name back to something nice.
2. Lower 5 Pokedex bytes will become corrupted, displaying some yet unseen species as caught. There's no easy way to fix this, but it's not a big deal unless you care about your Pokedex progression.
3. Your Pokemon box may get to a state where trying to release the glitch Pokemon inside will crash the game. This side effect does not happen every time, but if it does, again, this can be fixed with 8F's arbitrary code execution.

:: Execution:

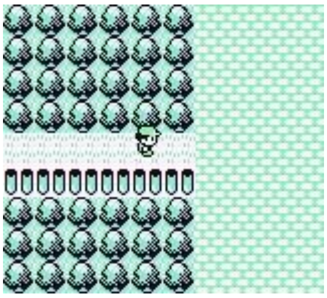
1. Go to the exact spot shown on the screenshot below (second to last house on Celadon's south-east). Open up and close immediately your Pokemon menu while still standing on that spot.



2. Go into a patch of grass and encounter a wild Pokemon. Do not open your start menu while going there.
3. Open and close your fight menu a few times, then run from the battle.
4. Open your Start menu. Your name should be glitched. If it isn't, repeat step 3.
5. Now you should have 16 Pokemon. Go to the Celadon's Pokemon Center and talk to Nurse Joy, but don't heal.
6. Go to the exact spot shown on the screenshot below:

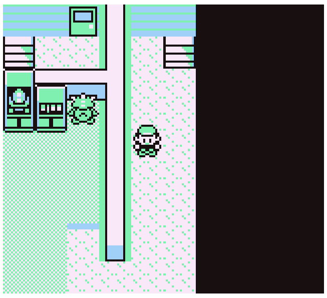


7. Open up your Pokemon menu, swap the 2nd Pokemon with the 10th.
8. Now your item pack should have 162 items, with the first item being "RIVAL's" and the second being Ether.
9. If you have more than 1 Ether on the second position, toss them so only 1 remains.
10. Swap the Ether (2nd item) with the 35th one (for this location this should be a Nugget)
11. Try walking to the right - the map should now loop back to the left side of Celadon City.
12. Keep walking to the right until you find the spot below:

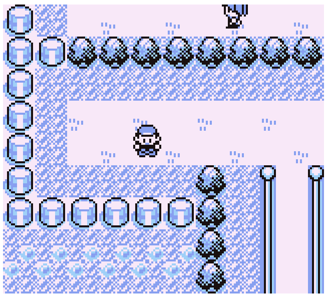


13. Open your item pack here - the Ether should turn into 8F. Switch it back with the second item to keep it.
14. Fly away to any town. Go to the Pokemon Center.
15. Store one of your 8Fs in the PC. 8F is treated like a key item and depositing more than one will clutter your PC.
16. (Optional) You can also deposit "RIVAL's" into the PC to get 2 glitch items for the price of one.
17. Swap the 10th Pokemon back with the 2nd. This will clear all your items.
18. Withdraw TM05 from your PC.
19. Swap the 2nd Pokemon with the 5th to avoid crashing in the next few steps.

20. Swap the 3rd Pokemon with the 2nd so your Pokemon with Fly won't get obliterated by Charizard 'Ms
21. Deposit your LM4 and your Pokemon with Fly.
22. From now on keep depositing Pokemon into your empty box until you're left with just one Pokemon in your party.
23. Withdraw LM4 and the Pokemon with Fly.
24. Exit out the PC and move the first Pokemon (Charizard 'M) to the last slot.
25. Deposit the Charizard 'M. You should now have only LM4 and the flyer in your team.
26. Because of the Super Glitch, your LM4 became an unstable hybrid of Krabby. Fly to Cerulean City, bring your LM4 into Daycare and take it out to change it back to LM4.
27. Fly back to Celadon City, stand in the spot below:



28. Teach your LM4 Mega Kick (use TM05). Replace the move with 4 characters in its name, otherwise stuff won't work as intended.
29. Fly to Cerulean City again, stand in the spot shown below:



30. Open your Pokemon menu here (important). If your LM4 is now the second Pokemon in your party, switch it back to the first slot.
31. Fight a wild Pokemon. Open up and close your fight menu a few times, then run from the battle.
32. Your name should be now blank. If it isn't, repeat step 30.
33. Fly to any Pokemon Center and heal your Pokemon.
34. And finally, you're done! You are now free to save the game if you're brave enough. Withdraw your 8F and have fun.

1.3. BOOTSTRAPPING

8F won't do anything amazing by itself - in order to make it execute code from $D322 (third item), we need to use the party Pokemon to spell out a short bootstrapping program, which will redirect the instruction pointer to your item pack. The requirements are as follows:

1. 6 Pokémon [0xD163 = 0x06]
2. Onix as the first Pokémon [0xD164 = 0x22]
3. Pidgey as the second Pokémon [0xD165 = 0x24]
4. Tentacool as the third Pokémon [0xD165 = 0x18]
5. Meowth as the fourth Pokémon [0xD166 = 0x4D]
6. 24 PP left on the second Pokémon's second move [0xD1B5 = 0x18]
7. 21 PP left on the second Pokémon's third move w/ 1 PP Up used [0xD1B6 = 0x55]
8. 36 PP left on the fourth Pokémon's first move [0xD20C = 0x24]
9. 24 PP left on the fourth Pokémon's second move [0xD20D = 0x18]
10. 20 PP left on the fourth Pokémon's third move [0xD20E = 0x14]
11. Double Team as the fifth Pokémon's first move [0xD223 = 0x68]
12. Double Kick as the fifth Pokémon's second move [0xD224 = 0x18]
13. Strength as the fifth Pokémon's third move [0xD225 = 0x46]
14. Sixth Pokémon's attack stat has to be exactly 233 [0xD26C = 0xE9]

(11/12/13: Hitmonlee is probably the only Pokémon that can learn all of those moves)
/Nope, TheGlitchedUpGlitch proves me wrong: *“double kick is in the level up set for both nidorans and they can both learn hm strength once evolving into Nidoking/queen. They can also both learn tm 32 - double team. Figured this would be helpful for anyone who doesn't have a readily available hitmonlee to save the time of ditto glitching one”*

1.4. USING 8F TO OUR ADVANTAGE

"CATCH 'EM ALL" SCRIPT

This is just K)ry's ASM for JP Red/Green ported on the international release. With those items, 8F will act like an item that forces a Pokemon encounter based on the quantity of item #1, allowing to catch all 151 Pokemon easily.

Video: http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=782s

ITEM LIST (starting from the first slot):

* Preferably Master Balls	
* 8F	
TM50	x31
TM11	x4
TM34	x89
TM08	x201

ALTERNATIVE CATCH 'EM ALL

This version of the Catch 'Em All script requires more items, but gives the Pokemon instead of forcing an encounter (like: BLUE got EEVEE!), and allows for getting normally unobtainable glitch Pokemon without trading. The given Pokemon depends on the quantity of the 3rd item.

Remark: Avoid obtaining Missingno with this method. It will duplicate your 6th item and screw the opcodes up.

Video: http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=865s

ITEM LIST (starting from the first slot):

* Any item
* 8F

Repel	x[SpeciesIndex]
X Speed	x14
Ultra Ball	x64
TM05	x72
Lemonade	x201

FIX THE PLAYER'S NAME

One of the side effects of obtaining 8F is blanking out your name. However, with this setup, you can change your name to the nickname of your first Pokemon. Using 8F will copy one letter from your first Pokemon's nickname to your player name. Use 8F (length of the name+1) times to copy all the name characters and bring your name back to normal.
Warning: This code is self modifying, it will increase quantities of items #3 and #5 every use - remember to set those quantities back to 181 and 88 if you want to reset this. Also use carefully, as there's no memory protection implemented and you may cause save corruption if you're not careful.

Video: http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=918s

ITEM LIST (starting from the first slot):

* Any item
* 8F

TM50	x181
TM10	x64
TM34	x88
TM09	x46
Calcium	x52
X Accuracy	x35
Full Heal	x201

CHANGE THE SECOND ITEM

This easy code uses only 3 basic items, and it increases the first item's index by 1 every time 8F is used. You can obtain normally unobtainable items, glitch items or TMs so you can do other item configurations described.

Video: http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=974s

ITEM LIST (starting from the first slot):

* 8F	
* Item you want to morph	
Burn Heal	x43
Ice Heal	x43
Full Heal	x201

WALK THROUGH WALLS

Jump off a ledge after using 8F to walk through walls.

http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=1020s

ITEM LIST (starting from the first slot):

* Any item	
* 8F	
TM34	x20
TM15	x201

ESCAPE FROM A TRAINER BATTLE

This turns 8F into an item which allows escaping from any battle, including trainer battles.

http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=1048s

ITEM LIST (starting from the first slot):

* Any item	
* 8F	
TM34	x120
TM08	x201

CLEAR A POKEMON BOX

While obtaining 8F there's a slight chance Pokemon at your box will get corrupted and will crash the game upon releasing. One can either deal with it and switch to another box, or make the box empty with this item configuration.

Switch to the corrupted box, use the 8F, done. Be careful though, you don't probably want to clear the box with your L100 legendaries.

Video: http://www.youtube.com/watch?v=Sw0h7ImFsAs#t=1104s

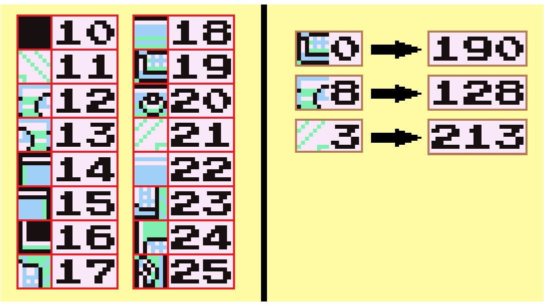
ITEM LIST (starting from the first slot):

* Any item	
* 8F	
Lemonade	x1
Soda Pop	x64
TM34	x128
TM18	x201

1.5. BIG ITEM QUANTITIES?

All of those item lists will have at least one item with quantity bigger than 99. Obviously, it's possible to obtain those big quantities using the Missingno. item duplication glitch (duplicating a 99 item stack will result in a 227 item stack).

However, the numbers bigger than 9 are represented with glitch blobs, so it's normally impossible to read how many items you actually have. This short image guide below will help you with reading quantities of those big item stacks.


10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
0
190
8
128
3
213