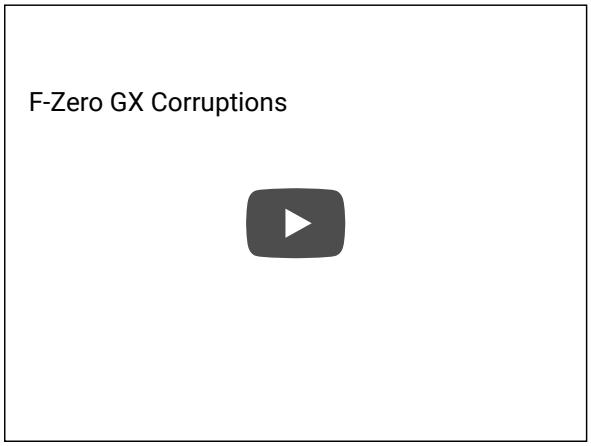
CHEAT ENGINE CORRUPTION GUIDE

Cheat Engine is an MHS (Memory Hacking Software), it scans what a program has loaded on a computer's memory (RAM) when it's running and allows you to edit all the values a program has on memory. Normally Cheat Engine is used to cheat in video games like give you infinite health, thus the name. But it has loads of extra features that allow for all kinds on fun, including the ability to screw up a game so bad that it induces face-hurting hilarity. The kind of hilarity that can only come from Corruptions. Here is my guide on Corrupting with Cheat Engine.

If you've just discovered Corruptions, or don't know what they are, I highly suggest you check out some of CosmoCourtney's corruptions, or some of mine before learning how to do it yourself. Cosmo taught me how to corrupt with Cheat Engine so big props to Cosmo!



PREREQUISITES

Firstly, you're going to need Cheat Engine.

Download it at CheatEngine.org

The second thing you're going to need is a table with some HEX values, I'll get to why these are important soon but keep this list handy:

3c000000 - 3e800000 3e800000 - 3f800000 3f800000 - 40000000 40000000 - 40800000 40800000 - 42000000 42000000 - 47000000 bc000000 - be800000 be800000 - bf800000 bf800000 - c0000000 c0000000 - c0800000 c0800000 - c2000000 c2000000 - c7000000

Optionally, you can download some emulators, seeing as this works on pretty much any game, why rule out emulated games? Here's a list of emulators with download links (this is a list of emulators I've used and have had success corrupting with, they may not be the most accurate but they just work).

- PCSX2, a Playstation 2 emulator.
- XEBRA, for Playstation 1.
- Dolphin, for Wii and Gamecube.
- Project64, for Nintendo 64.
- DEmul, for Dreamcast.
- DeSmuME, for Nintendo DS.
- PPSSPP, for Sony PSP.

Feel like experimenting? You can try a bunch more emulators for different platforms which you can find at the Emulation Gametech Wiki.

Where do I get games for these emulators?

I wouldn't jump to piracy because there are legitimate ways to get games for these platforms, like from a store, Ebay, Amazon, Cragslist, a garage sale or from a friend. But I just can't recommend legitimate purchase for some of these games because getting some of them to run in emulators is a tedious and difficult process.

PCSX2 and Dolphin are easy because they allow you to play the games just by putting them in your DVD drive but for emulators like Project 64 and DeSmuME it involves dumping data off cartridges and cards which is a whole new realm of difficulty. So for those kinds of games I wouldn't hesitate to check out EmuParadise, The IsoZone or FreeROMs. If you're a ROM purist, Google "cartridge dumping guide" for your platform of choice.

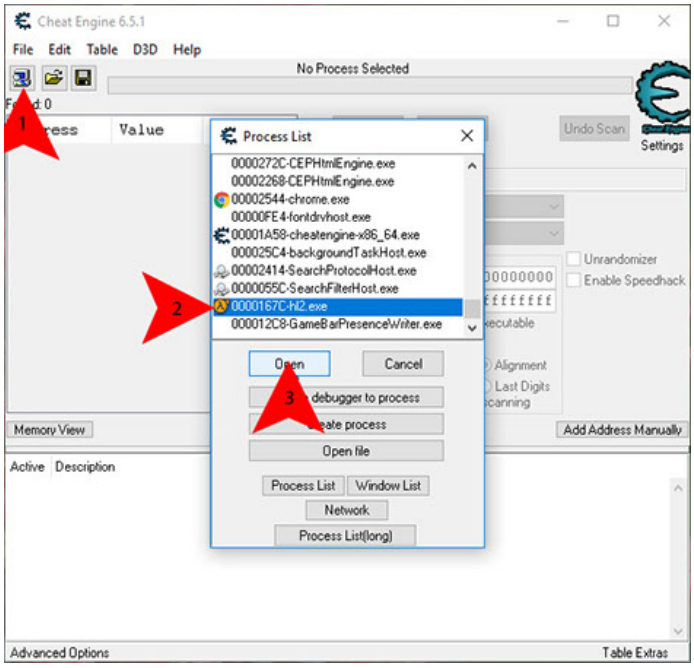
GETTING READY TO CORRUPT

In the main window we use the process list to select the game we want to corrupt. I'll be using Half Life Source for this tutorial.

1. Click the process button in the top left corner.

2. Select the process of your game or emulator.

3. Click open to hook the process for scanning.

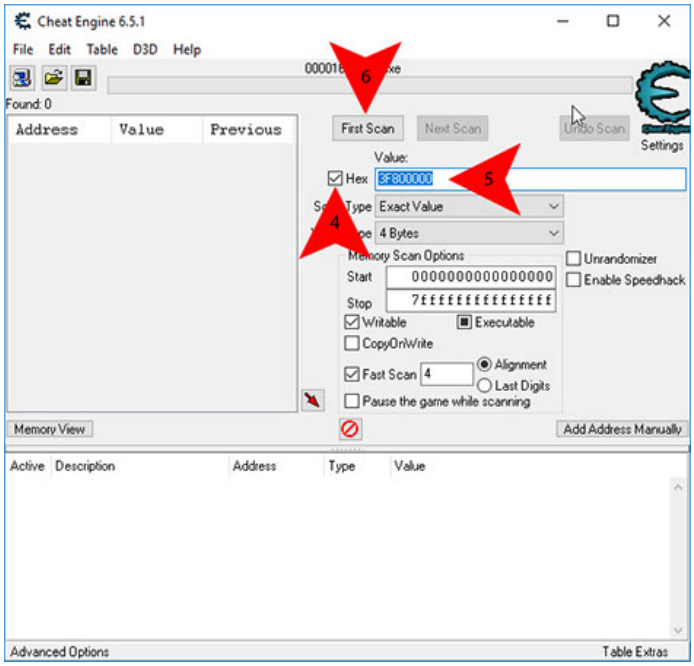


In the main area below the two scan buttons we have a box where we can input our values. 3F800000 is arguably the best value to start off with because it's a value that most games use as a "static value", which means anything that isn't meant to change is set to a value of 3F800000 and changing it to something else with almost certainly result in something interesting.

4. Check the HEX box.

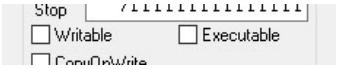
5. Enter 3F800000 as the value.

6. Click on "first scan".



Tip:

You can get more interesting results from scans that you've done with the "Writable" and "Executable" boxes unchecked.

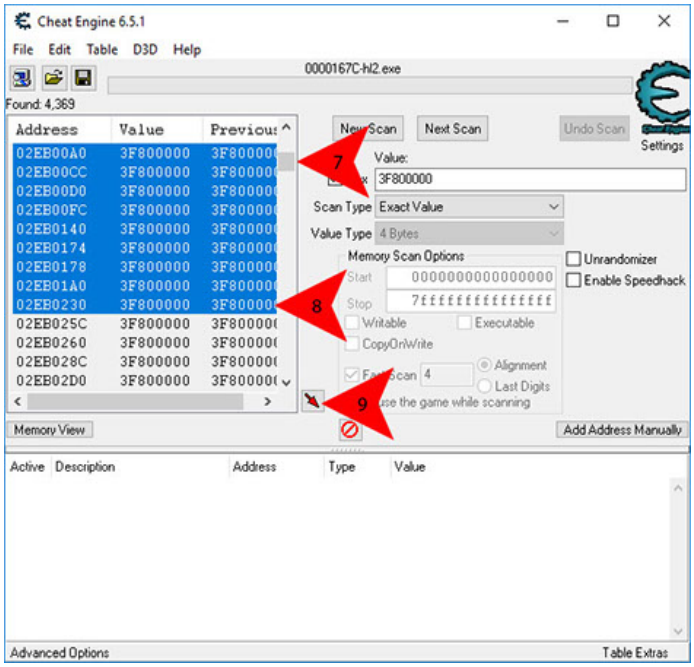


After scanning you will see about 5,000 to 85,000 values depending whether or not you checked the Writable or Executable boxes.

7. Click on the first value and scroll about 2cm down the list.

8. Shift+Click the another value, doesn't matter which value.

9. Click on red arrow pointing down and to the right.



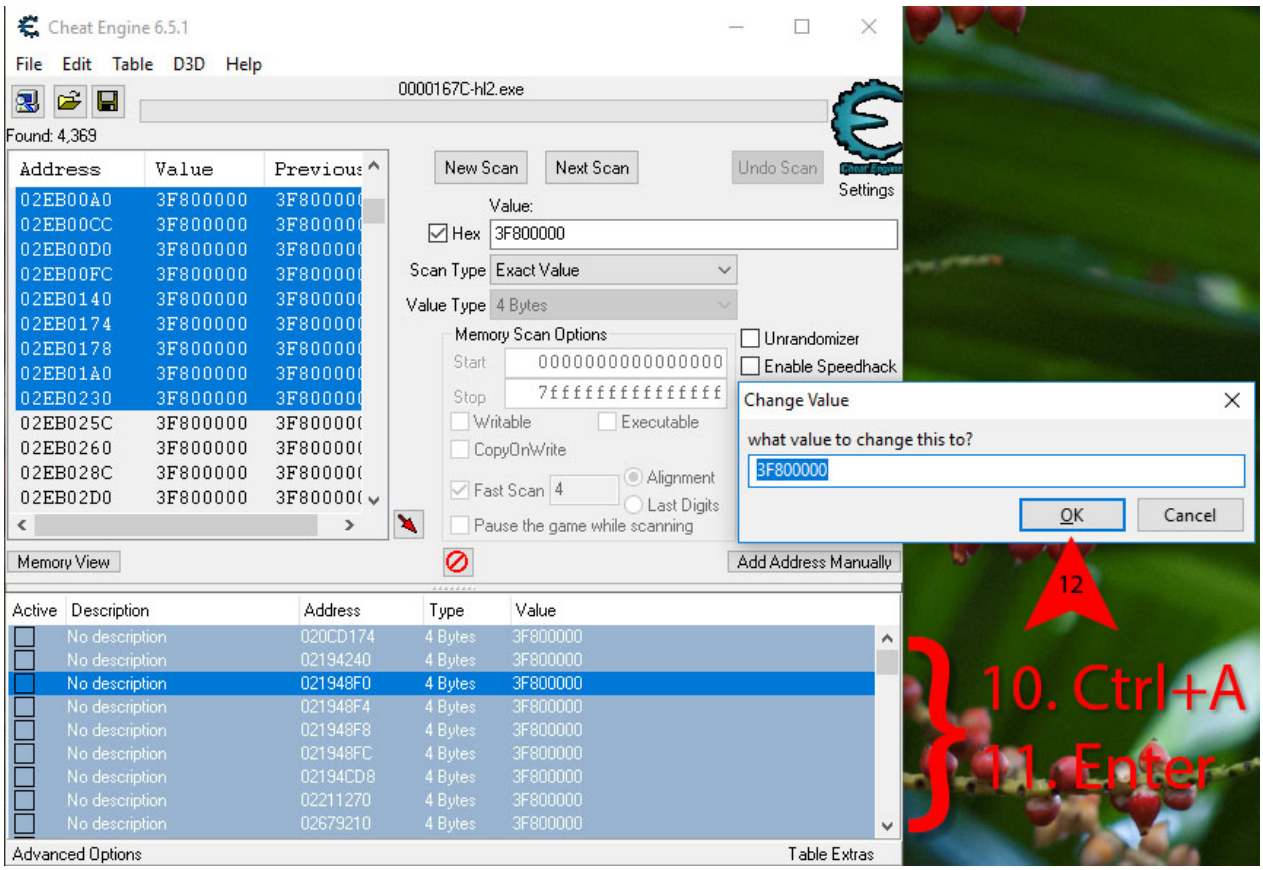
CORRUPTING THE GAME

Now that you've moved all the values to the address list below, we can finally start the corrupting!

10. Click on any value in the address list and select all with Ctrl + A.

11. Hit enter to bring up the "Change Value" dialogue.

12. Change the value incrementally, like 3F900000, and click OK.

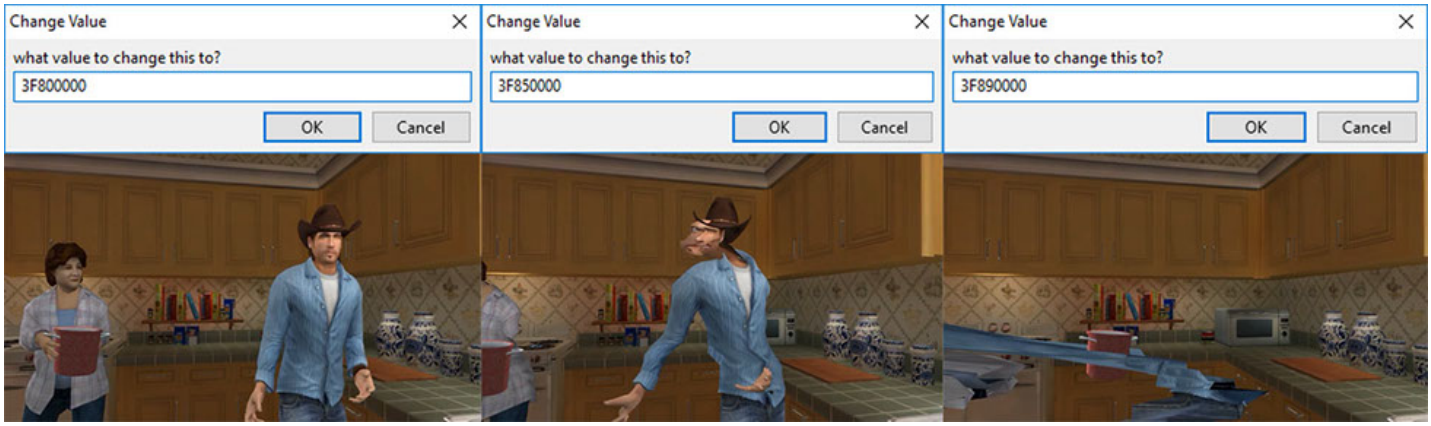


DID IT WORK?

If it did, congrats! You can now try other values, this is where the value list I mentioned earlier becomes useful.

If the change from 3F800000 to 3F900000 was big enough you can try smaller values like 3F810000 to see exactly what is changing, you can also try changing 3F800000 to 3E800000 for the opposite effect of what you have.

3F800000 Isn't the only value you can scan for, you can scan for any of the values listed in the embedded pastebin list and change them to your liking as long as it doesn't crash the game or emulator. For example, you could scan for 40000000 and change it to 3F800000.



Corrupting requires a lot of experimentation, trial, error and lots of crashing. Some games are less susceptible to crashing and some crash at the moment any value is changed, CS:GO for example just crashes to desktop as an anti cheat mechanism if I'm not wrong.

NEVER CORRUPT AN ONLINE GAME

Just don't, you'll get banned from the servers, you might get VAC banned, you might not be able to play online ever again.

Why? The name of the program says it all, Cheat Engine is mostly often used to cheat in games, so most online multiplayer games can tell when a foreign process, i.e, Cheat Engine, is trying to edit the memory of the game, like to change the amont of health you have, for example.

So don't join a CS:GO match and try to corrupt the playermodels because you'll likely get VAC banned and won't be able to play online ever again.

CORRUPTING WITH DOLPHIN

Dolphin is slightly different when corrupting, the Wii and the GameCube use PowerPC architecture which is a type of processor architecture that deals with values in Little Endian format, that means the values are somewhat back to front. So when you are corrupting with Dolphin, use the list of values below instead.

0000803F - 00002040 0000003F - 00000040 0000803E - 00004040 0000C03F - 00004040 00000040 - 00008040 0000A040 - 00000041 00002041 - 00000042 00000042 - 00000043 00000044 - 00000045 0000807F - 0000803F 000080BF- 000040C0 000000BF - 000000C0 000000C0 - 000000C1

QUESTIONS?

If you've got any questions regarding corruptions, shoot me an email at bitrainy@gmail.com

Normally this guide would be on the Vinesauce forum, but it every few months the Vinesauce forum dies and isn't fixed for ages so I've hosted it here instead. Here's an archived version of the Vinesauce forum guide.