How to use CWCHEAT Pointer searcher

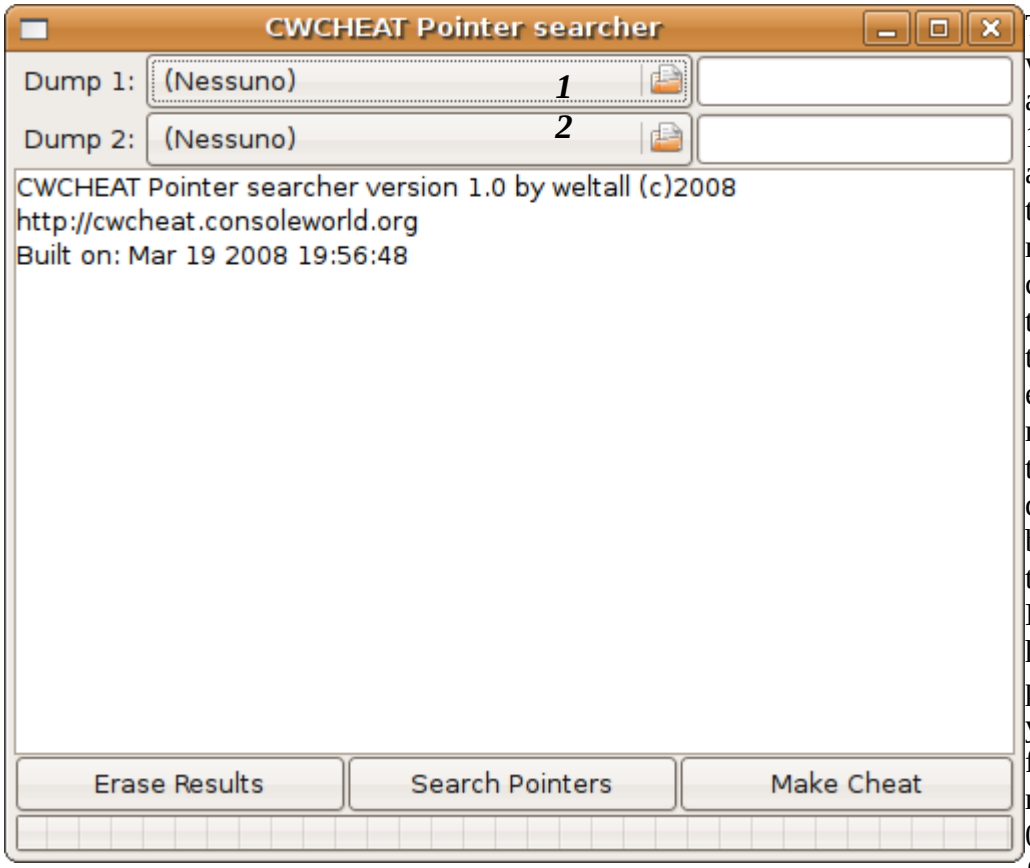
Cwcheat pointer searcher is a new application for your computer to be used as a companion application with cwcheat. It's currently available for windows and linux and will most likely be available for macosx and maybe psp in the future.
This application will permit you to easily search and create cheats for games which uses dinamically allocated adresses or more commonly called in the cheat scene as DMA games (be carefull that the real meaning of DMA is direct memory access and it's a completely different thing).

Cwcheat pointer searcher has currently these functions:

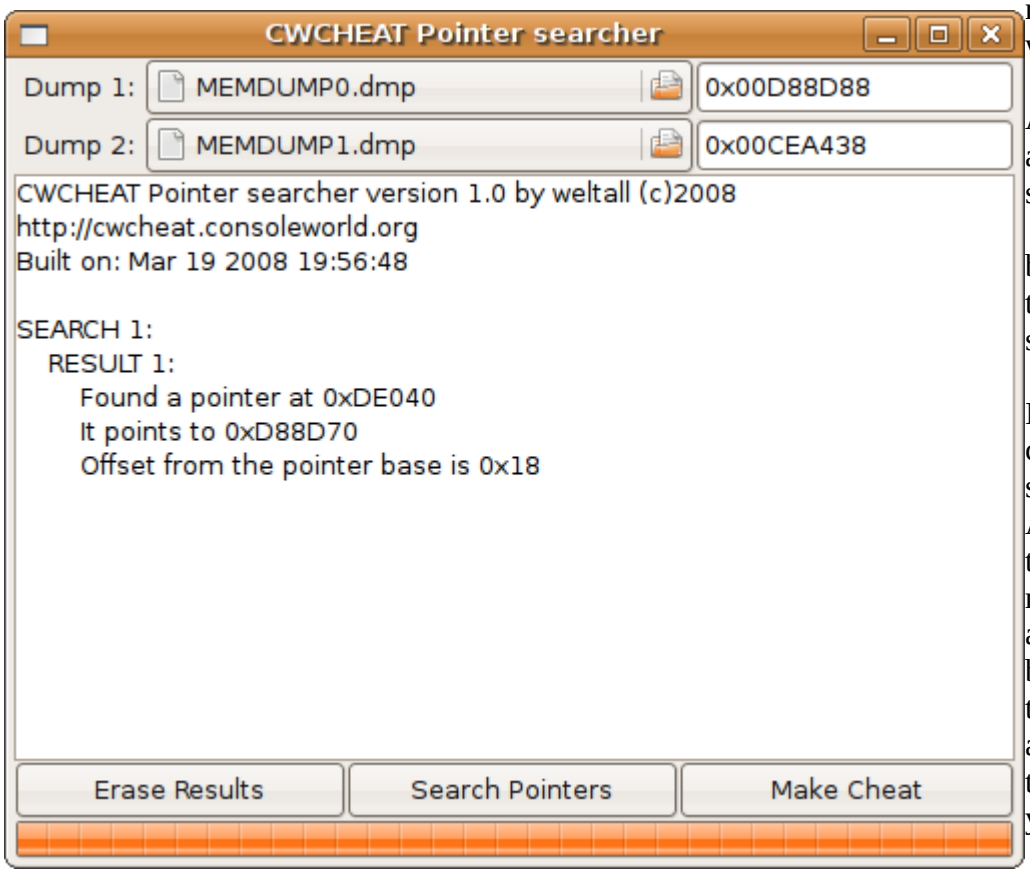
- Search on up to 2 dumps at the same time with the possibility to change them and search only in the results of old searches (so it's possible to continue search with other two dumps or just by changing one dump without keeping track of old results manually)
- Nice graphical, freely scalable and skinnable gtk+ based interface
- It's possible to erase in any moment all the search results and start again from scratch.
- Works entirely with relative adresses so you won't need to do some strange conversions from cwcheat interface to the pointer searcher interface
- Automatic generation of codes starting from adresses: it's needed only to input the value that should be placed in the pointed position and the type of access (8/16/32bit). The generator is capable of generating 8/16/32bit codes and autosensing inverse offset cases and in that case generate inverse offset codes.
- A progress bar to show the search progress

Requirements:

- An x86 computer and operating system or an x64 computer and operating system capable of loading 32bit applications
- 50mb or more free in ram during the searches to load the psp ram dumps
- Windows 2000/XP/2003/VISTA or a never linux distribution (tested with ubuntu gutsy and hardy)



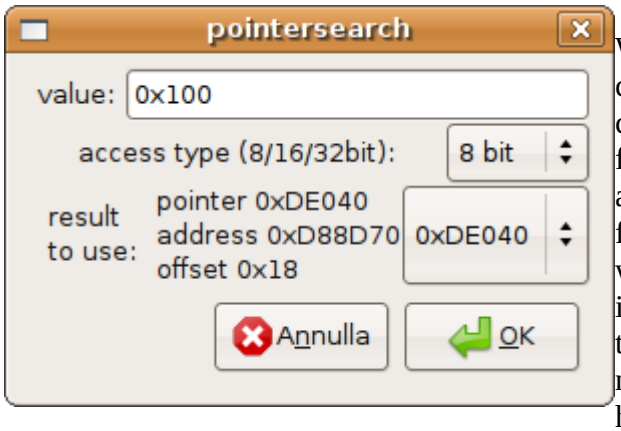
This is the main window of cwcheat as you can see points 1 and 2, if clicked, allows you to choose the various dumps made trough cwcheat (to enable this function enable the enable dump entry in the main menu, as for default the button to make dumps is SQUARE, but it can be changed to something else). Each dump should have a different position in the cheat you are searching. If for example the money is at adress 0x00100000 in the first dump and it's at 0x00120000 in the second dump you have two good dumps to search for pointers, if the position is the same they are pratically useless (or the game doesn't even have dinamically allocated memory). So in order to be able to search for pointers you need first to search for the thing you need for example with the built in cheat searcher and write down the found adress for each dump you do. This value you got by doing normal search will be put in the two text box you can see at the top right part of the window.



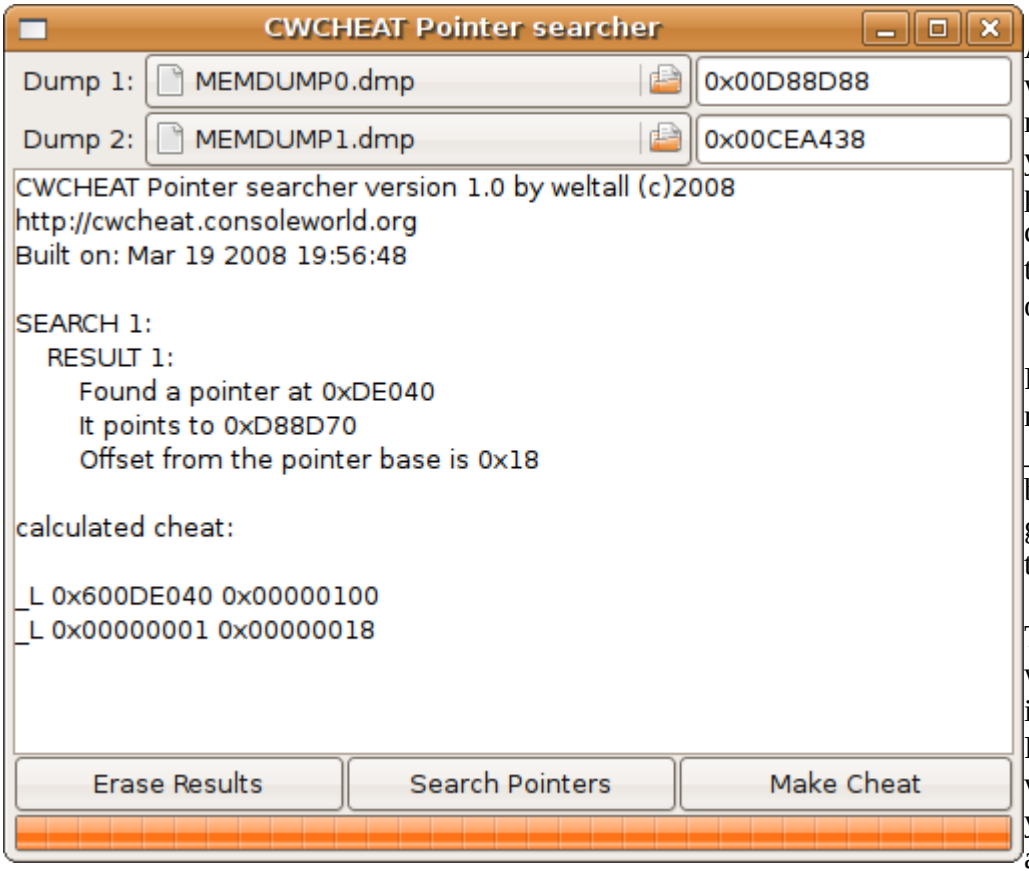
At this point you are ready to start searching press the Search Pointers button and wait for the application to show you the result.

If everything went correctly you will see this window. As you can see, in this case only one result was found and it's most likely be our pointer. If this wasn't the case and you found more than one pointer you might want to

try changing one of the dumps or only one and updating the adress on the top right to adhere the new dump you loaded and at this point click on Search Pointers . Do this till you get one result or at least a decent number of results. If you can't get the results to go down most likely the game has more than one pointer pointing to the same dinamically alloched area so it doesn't matter if you get more than one result.



When you fell satisfied with the results you can click on Make Cheat. You will get the window you can see on the left. This window will ask you in the first text box what value you want to assign to the adress you are searching. The dialog box you can find just under it will allow you to choose if you want to access to an 8, 16 or 32bit adress: pratically it asks if the game stores this data you are making the code for in 8, 16 or 32bit (of which 8bit has a maximum of 0xFF or 255 counting from zero, 16bit has a maximum of 0xFFFF or 65535 and 32bit 0xFFFFFFFF or 4294967295, this isn't always right but it can be a good scheme for most games) Finally the last dialog box asks you the result to use: if you found only one adress you won't need to touch it, else select the result which seems better to you and press OK to confirm the action.



At this point you will return to the main window and you will be presented with the cheat waiting only to be copy & pasted on your database :)

For beginners you need also to add a _C0 cheat name before that if the game is already in the database.

The last function which might be of interest is the Erase Results button which will allow you to delete results and so start searching from scratch, like if you just opened the application.

All the text boxes accepting values can get decimal, hexadecimal and octal values just remember that decimal numbers can be inputted as is, hexadecimal numbers must have 0x before the value and octal numbers must have a 0 before the value.

Last thing: if you want to change the theme of the gui in linux you just have to change the options for the gtk+ engine (which is normally doable trough gnome configuration tools) as for windows

you need to change the included gtkrc with something else. if you have installed the gtk runtimes (for example with gimp) you will only need the .exe and you can just change the theme from the theme selector in your gtk start menu entry.

I think that's all you need to know Enjoy :)