

MANUAL CW CHEAT 0.1.3
For devhook

Index

<i>Using Cw Cheat Installer</i>	<i>3</i>
<i>Using cw cheat prx.....</i>	<i>6</i>
<i>Using cheat searcher.....</i>	<i>16</i>
<i>Appendix: controller codes.....</i>	<i>18</i>

The latest updates are available on <http://www.consoleworld.org> and <http://weltall.consoleworld.org>

The latest Database updates are available on <http://cwcheat.zioale.it> and
<http://cwcheat.consoleworld.org> .

Using Cw Cheat Installer

This program install and uninstall automatically cwcheat, it's useful also to update cwcheat in the next releases.

When you start it you will see this:



Here there are 4 buttons selectable with <- -> and you can activate them with X.

First of all there is Install (which is equal to recover with the only difference that install is to be used only if cwcheat isn't installed! Recover is used to update, restore cwcheat or to install cwcheat to different firmware than where it is currently installed).

Press X over install and you will see this:



Here you can select a typical and a custom installation.

The typical installation installs the prx, the database and activates the prx only in-game.

The custom installation permits to select where to enable the prx: in the vsh and/or in-game.

Who choose the typical installation can skip the next pass.

When you select custom installation you will see this:



Here you can select where to enable the prx: in the vsh with the first option and/or in game. Press X to enable/disable the options and press continue to continue with the installation.

If you had chosen typical or custom installation you will see this:



Here you have a list of all the folder of firmware in the dh folder and it's possible to select the firmware where cwcheat will be installed (if you want to install cwcheat in more than one firmware you need to use the restore function when you finish the installation process and select the other firmware).

Press X on a firmware to start the installation.

In the main menu you can also see configure. This function permits to change the prx configuration: it's possible to configure all you can normally configure from the prx except setting kernel buttons to the buttons configuration (vol+/vol-, note, screen, hold, remote hold)

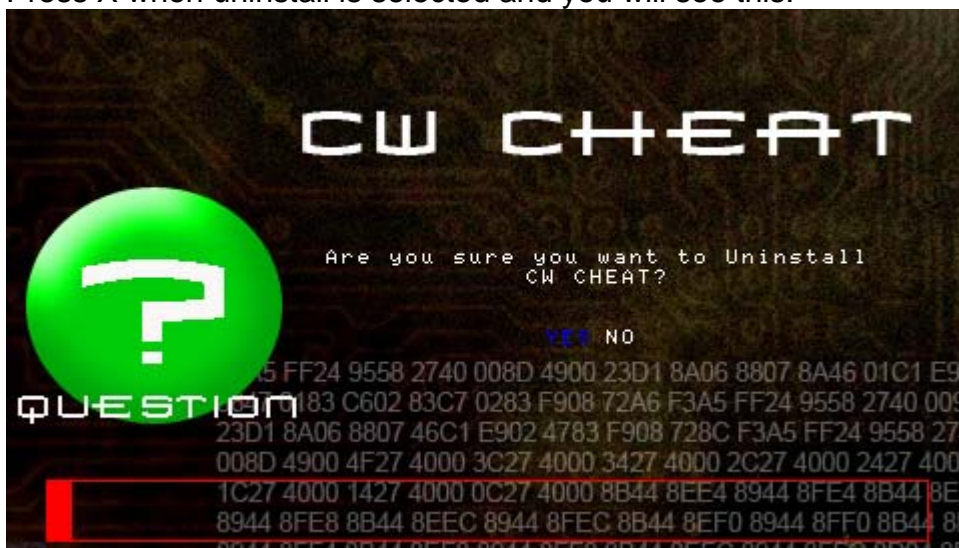


The controls here are the same of the prx.

Save settings saves the new configuration to file, discard settings doesn't save the configuration and returns to the main menu.

The last option is uninstall: this function removes all calls to the prx from the firmware files, removes the prx, the database and leaves the configuration data.

Press X when uninstall is selected and you will see this:



If you select YES with <- and press X the uninstall process will start.

NOTE: In this program you can return to the main menu with O and if you are on the main menu by pressing O you will return to the vsh of the psp.

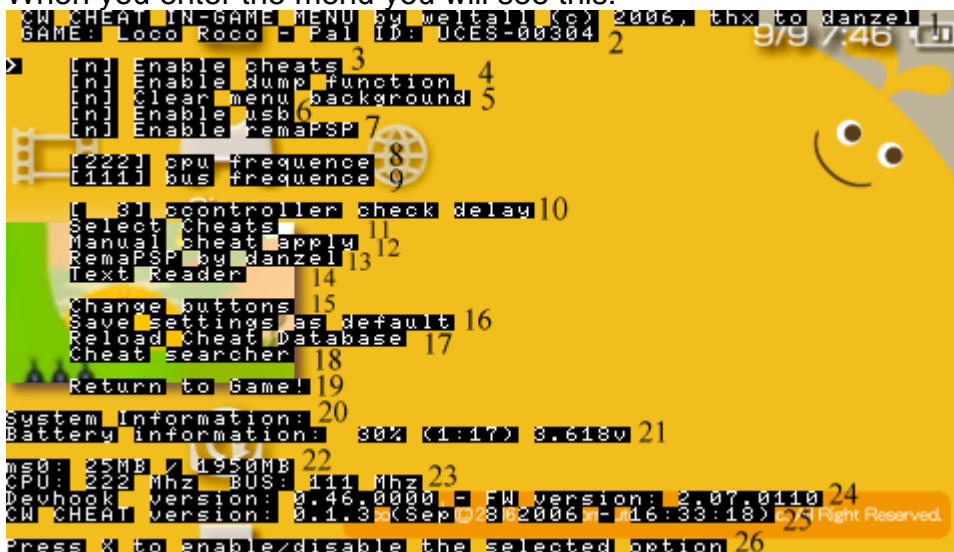
Using cw cheat prx

The prx is loading every time you load the game or the vsh depending on how you installed it and it will accept commands only when the umd is found (also emulated umd).

After this you can access to all the prx function, the database and if present the configurations will be automatically loaded.

To enter the menu press SELECT (button you can configure) for about 3 seconds (which is a configurable time).

When you enter the menu you will see this:



- 1- Application name, in the submenu it shows in which menu you are
- 2- Shows the game name (if present in the database) and the game id (the number you can find in the umd disc)
- 3- This permits to enable cheat apply
- 4- Activates the dump function. You can dump the ram with the square button (customizable)
The dump function writes on the file ms0:/MEMDUMP.dmp all the content of the user ram to find new cheats
- 5- Erases the background before opening the menu, it's useful if you can't see the menu with the background game image
- 6- To enable usb mass function
- 7- Enables remaPSP and loads the keymap selected as default or the one associated to the signature id of the game
- 8- Permits to change the cpu frequency (0 = no change)
- 9- Permits to change the bus frequency (0 = no change)
- 10- Permits to select pad control delay. It's possible to select from 1 to 10 seconds
- 11- This will open a submenu to enable/disable the available cheats and doing other operations to the database
- 12- Manually apply cheats for one time

- 13-Opens the remaPSP menu which permits to select a keymap from the ones in the ms0:/remaps/ folder
- 14-A simple text reader which reads the ms0:/chatlog.txt file in the available screen space.
- 15-This will open a menu to configure buttons
- 16-Saves all the options and button configuration as default and they will be loaded at every startup (NB: the clock configuration of devhook has the precedence over the cwcheat configuration so they are automatically applied only if devhook is set on 0 (no change))
- 17-Reloads the database from the memory stick (useful to test new cheats without reloading the game)
- 18-Permits to access to built in search functionality directly from the psp: fixed value search and difference search are supported
- 19-Exits from the menu and return to the game
- 20-Under this you can find some information about the system
- 21-If the battery isn't present you will see what's on the image, else it shows if the psp is connected to the socket, if it's recharging the battery, the charge percentage, the remaining time, and the voltage
- 22-Shows the available/total memory stick space
- 23-Shows the cpu and bus MHz
- 24-Shows the devhook version and loaded firmware version
- 25-Shows the cwcheat version, and build date and time
- 26-Shows a quick help about the selected option

You can use UP and DOWN to move on the menu and X to confirm, you can press O to return to game.

In the sub menus you can press O to return to the main menu

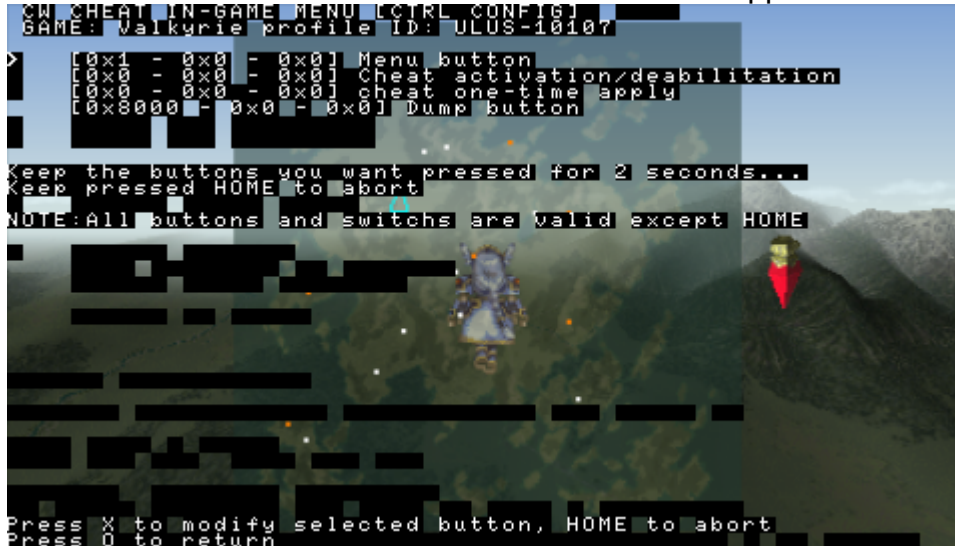


This is the button change menu. You can use this menu to configure the buttons of various functions with combination up to 3 buttons.

- 1- Menu header. It shows we are in the CTRL CONFIG menu
- 2- Game id and name informations
- 3- This permits to modify the button to access the menu you can't disable this by not selecting any combination, if you try to do it, it will restore the default (SELECT)
- 4- This combination it's the same as enabling/disabling the entry n. 3 of the main menu
- 5- This combination it's the same as selecting the entry n. 10 in the main menu

- 6- This combination permits to dump the ram and write it to the memory stick. The default it's SQUARE.
- 7- This combination permits to enable/disable remaPSP. It has the same function of the entry 7 in the main menu
- 8- Shows a quick help

Press X on one of these combinations and this will appear:



This invites you to keep pressed for 2 seconds the combination you want to set for the function.

If you don't want to change the configuration keep pressed HOME.

Press O to return to the main menu

Another menu is select cheats.



Here you can enable/disable the cheats on the db by pressing x, each cheat has a box with written y or n either if enabled or disabled and a short description

You can press O to return to the main menu.

You can press TRIANGLE to enable/disable all the cheats for the game.

You can press SELECT to save the game on the database with codes enabled/disabled status, modifications to the value of the cheats and new cheats.

You can press SQUARE to modify the value of a cheat.



If you press SQUARE when selecting a cheat this screen will appear:

You can press LEFT/RIGHT to add/subtract 100

You can press UP/DOWN to add/subtract 1

You can press L/R to add/subtract 1000

You can press SQUARE/TRIANGLE to change codeline

You can press X to accept the value or O to discard changes

In the main menu another submenu is “remaPSP by danzel” if you press x on it you will access to a menu in which you can select the keymap to be used:

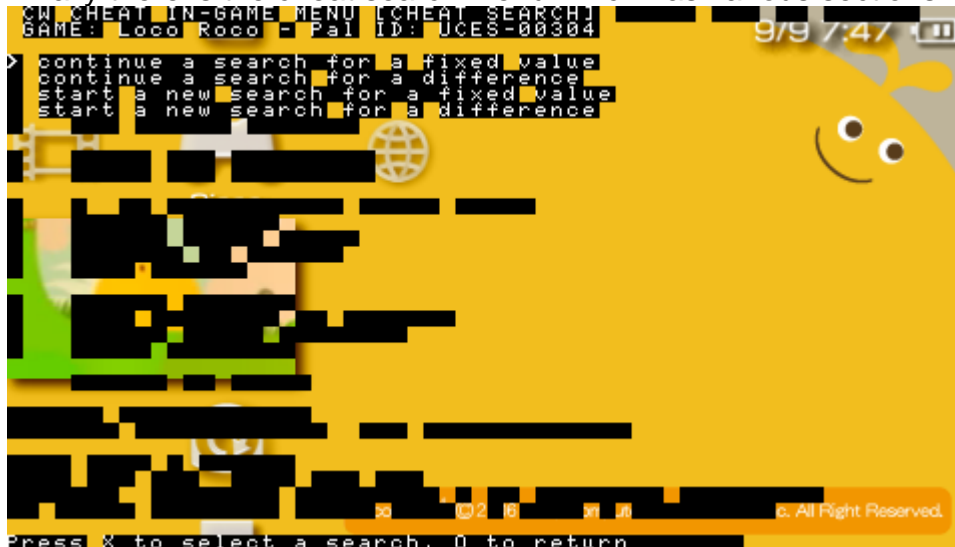


You can press X to select the desired keymap or O to exit without selecting a keymap

NOTE: selecting a new keymap before enabling remaPSP could cause the change of the keymap because it autoloads the game keymap if present.

More information on the included remaPSP documentation by danzel

Finally there is the cheat search menu which has various sections:



To start a search you must use the 3^ and 4^ entry:

Start a new search for a fixed value and Start a new search for a difference.

The first of these permits you to search the memory for an already known value, for example money. The second permits you to search for a difference in the value (equal, different, major, minor)

Let's start with the fixed value search (space required on the memory stick 1-5mb)



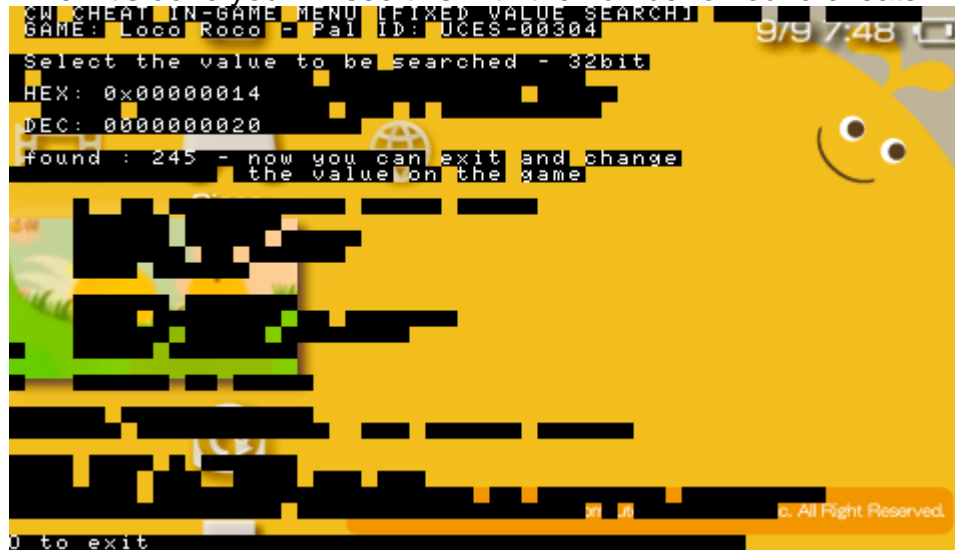
You will see a screen similar to this.

The first thing to do is to set the bit of the value to be searched this can be done with SQUARE and changes in 8, 16 and 32bit.

Keep in mind to select the bit not by the current value but on how much that value can increase: if you think a value can't go upper than 255 select 8bit, if you think a value can't go upper than 65535 select 16 bit for other cases select 32bit (for example money).

When this is done you can change the DPAD and L/R buttons to change the value (see the section about cheat value modification for more information about this) and press X to start the search

When it's done you will see this with the number of found cheats:



Now you can exit the ingame menu and modify the value.

After this select Continue fixed value search:



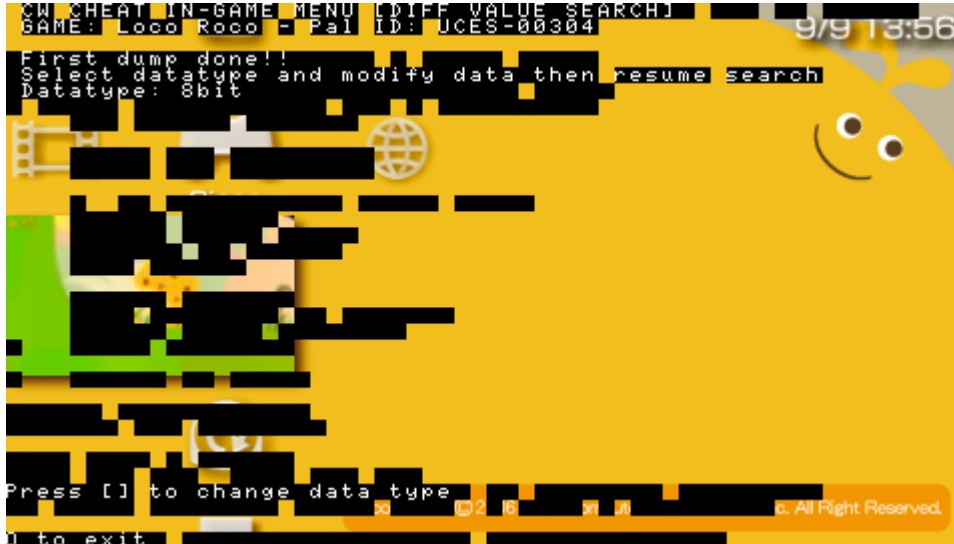
And you will see this screen.

Here you can do two thing. Searching again for a value like before or checking the first 10 address from before for the cheat you want. If you think there is an address which could be right just press TRIANGLE and select the address you want with X.

The cheat will be added to the database in memory (remember to save) and you will be asked for the value to assign to it (check the cheat modification section above for more informations).

Now we will see the difference search or diff search (required 512KB of free kernel ram, 25MB of free memory stick space for the dump and up to 10mb/pass depending on result (normally only the first pass can be so big))

When you will select diff search a memory dump will be make and you will then see this screen:

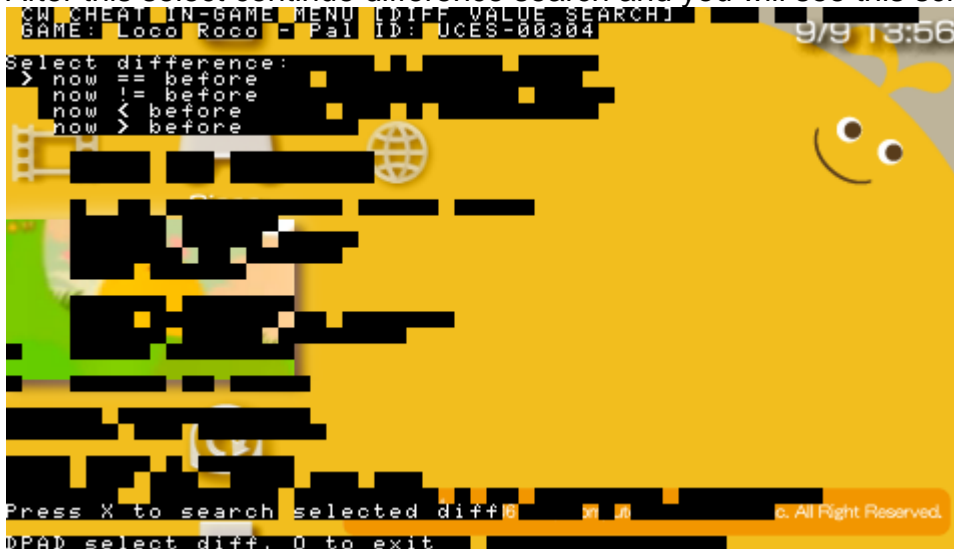


Here like with the fixed value search you have to select the bit to be used for the search by pressing SQUARE.

More information on this in the fixed value search section.

Then you can exit the ingame menu and modify the value.

After this select continue difference search and you will see this screen

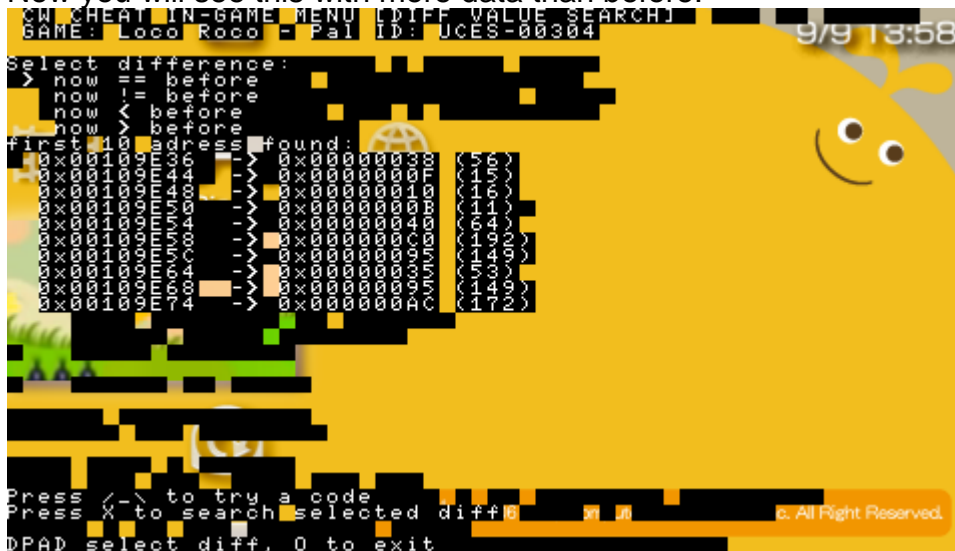


Here you can select how you changed the value: == (equal), != (different), < (less) and > (more). And you can start the first search by pressing X.

After a bit of second you will see a screen with the result. Now you have to change the value again and come back.



Now you will see this with more data than before:



Here you can check the first 10 addresses and add them like with the fixed value search, or continue the search by selecting again the difference.

Both the database and the configuration file are put in the ms0:/dh/ folder and are editable with a text editor.

The database (called cheat.db) can be in UNIX/DOS/MAC format and can contain values and addresses in decimal (123), hexadecimal (0x0000007B) and octal (0173) and it will be read without problems

This is its structure.

_S signature of the game: it's a code like ULUS—10041 and you can find it in the cw cheat main menu on the top right after ID:

e.g.: _S ULUS-10041

_G game name: it's the name of the game (maximum 30 characters)

E.g.: _G GTA LCS (US)

_C0 chat name: a little description for the cheat (maximum 30 characters) (the maximum cheat supported for game is 400). The 0 near _C is the status of enabled/disabled which the cheat will have when loaded

E.g.: _C0 \$9999999

_L this is a code line for the cheat. It's formed of two numbers in hexadecimal format, their meaning changes from cheat type to cheat type (check the site linked in the readme for more information) the two numbers must have 0x before the number: this means the number is in hexadecimal format.

E.g.: _L 0x20389ACC 0x05F5E0FF

A complete example:

```
_S ULUS-10022
_G Legend of Heroes 2
_C0 max Pia
_L 0x202E4874 0x0001869F
_C0 max G
_L 0x202E4878 0x0001869F
```

NB: if you find cheats without the 0x it means they are in absolute format so to use them you need to subtract the address of 0x08800000 (normally the first number but for some cheat types this can change) .

So cheats made for cwcheat have the same address of the dump position you can see on your hex editor without more operations.

Another note: old cheats made with mph game loader have an offset error caused by mphgl itself so with devhook you need to subtract 0x4300 from every address.

This is the configuration file format:

CHEAT ENABLE = 0 -> 1 to enable cheat apply, 0 to disable

DUMP ENABLE = 0 -> 1 to enable dump, 0 to disable it

CLEAR ENABLE = 0 -> 1 to enable screen clearing before opening the menu

USB ENABLE = 0 -> 1 to enable usb mass

REMAP ENABLE = 0 -> 1 to enable remaPSP on startup, 0 to disable.

USB DUMP = 0 -> 1 to dump to usbhostfs0:/, 0 to dump on ms0:/.

CPU CLOCK = 333 -> write here the MHz to apply to the CPU on startup

NB: this is ignored if devhook is set to something different than 0
(no change)

BUS CLOCK = 166 -> write here the MHz to apply to the bus on startup.

The notes of CPU CLOCK are valid also here

DELAY TIME = 3 -> set the delay between every cheat application and buttons check

These are the buttons of the combination to open the menu you can find the codes here
(svn.ps2dev.org)

MENU BTN1 = 0x1

MENU BTN2 = 0x0

MENU BTN3 = 0x0

These are the button of the combination to enable/disable cheats

CHEATEN BTN1 = 0x0

CHEATEN BTN2 = 0x0

CHEATEN BTN3 = 0x0

These are the button of the combination to apply chat for one time

CHEATAP BTN1 = 0x0

CHEATAP BTN2 = 0x0

CHEATAP BTN3 = 0x0

These are the button of the combination to dump the ram

DUMP BTN1 = 0x8000

DUMP BTN2 = 0x0

DUMP BTN3 = 0x0

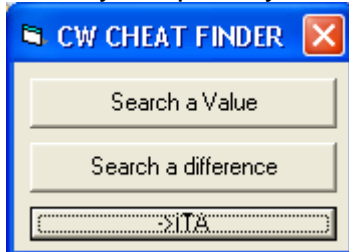
REMAP DFILE = ms0:/remaps/DEFAULTS.TXT -> the keymap which remaPSP if a game specific keymap is not available

NB: This file must be in UNIX format

Using cheat searcher

This windows application permits to search cheats by using ram dumps by searching precise values and difference between values in the various dumps.

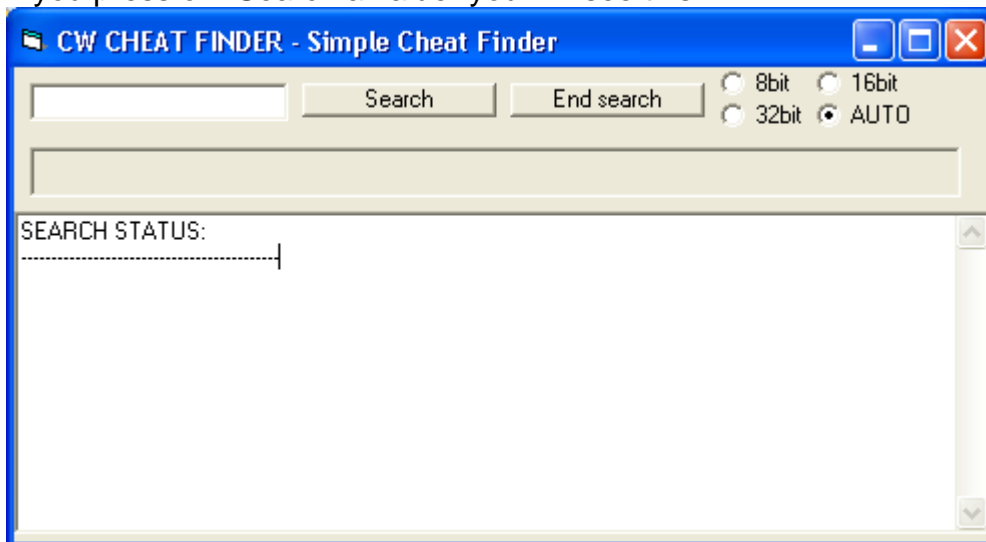
When you open it you will see this:



From here you can select if you want to search for a precise value "search a value" or search for a major or minor value "search a difference".

Here you can also select if you want English or Italian (for English you just need to press once -> ENG)

If you press on "Search a value" you will see this:

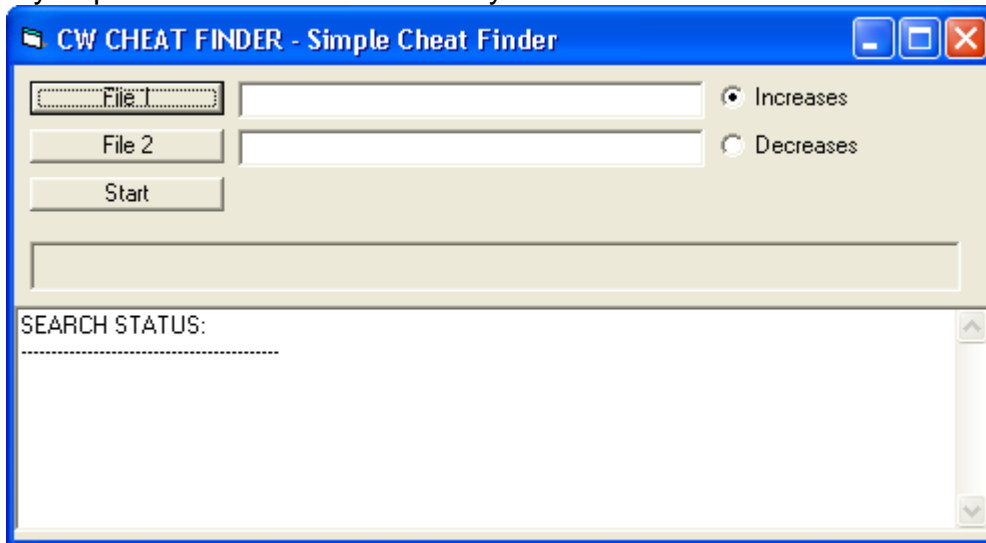


Here in the text box in the top left you can put the value you want to search then to start the search press "Search". You can repeat this till you find the right position. Then by pressing "End Search" you will get a stub to be put in the database.

With AUTO it will determine how much bits is your value and search for it accordingly.

If you want to force 8/16/32bit search you just need to select the correct option

If you press "Search a difference" you will see this:



Here you can search for differences between two dumps for example to find cheats for life bar or similar cheats.

To select the dump you press "File 1" and then "File 2" then you can select if the difference from 1 to 2 is an increase select "Increases" if it's a decrease select "Decreases" then to start the search press "Start" then you can repeat this with another dump.

Appendix: controller codes

These are the codes you can use to manually set cwcheat or to check them in the button configuration screen:

```
/*
 * PSP Software Development Kit - http://www.pspdev.org
 * -----
 * Licensed under the BSD license, see LICENSE in PSPSDK root for details.
 *
 * pspctrl.h - Prototypes for the sceCtrl library.
 *
 * Copyright (c) 2005 Marcus R. Brown <mrbrown@ocgnet.org>
 * Copyright (c) 2005 James Forshaw <tyranid@gmail.com>
 * Copyright (c) 2005 John Kelley <ps2dev@kelley.ca>
 *
 * $Id: pspctrl.h 1964 2006-07-08 19:49:40Z tyranid $
 */
```

```
/* Note: Some of the structures, types, and definitions in this file were
   extrapolated from symbolic debugging information found in the Japanese
   version of Puzzle Bobble. */
```

```
/**
 * Enumeration for the digital controller buttons.
 *
 * @note PSP_CTRL_NOTE, PSP_CTRL_SCREEN, PSP_CTRL_VOLUP,
 * PSP_CTRL_VOLDOWN, PSP_CTRL_DISC, PSP_CTRL_WLAN_UP,
 * PSP_CTRL_REMOTE, PSP_CTRL_MS can only be read in kernel mode
 */
```

```
enum PspCtrlButtons
{
    /** Select button. */
    PSP_CTRL_SELECT    = 0x000001,
    /** Start button. */
    PSP_CTRL_START     = 0x000008,
    /** Up D-Pad button. */
    PSP_CTRL_UP        = 0x000010,
    /** Right D-Pad button. */
    PSP_CTRL_RIGHT     = 0x000020,
    /** Down D-Pad button. */
    PSP_CTRL_DOWN      = 0x000040,
    /** Left D-Pad button. */
    PSP_CTRL_LEFT      = 0x000080,
    /** Left trigger. */
    PSP_CTRL_LTRIGGER  = 0x000100,
    /** Right trigger. */
    PSP_CTRL_RTRIGGER  = 0x000200,
```



```

/** Triangle button. */
PSP_CTRL_TRIANGLE = 0x001000,
/** Circle button. */
PSP_CTRL_CIRCLE   = 0x002000,
/** Cross button. */
PSP_CTRL_CROSS    = 0x004000,
/** Square button. */
PSP_CTRL_SQUARE   = 0x008000,
/** Home button. */
PSP_CTRL_HOME     = 0x010000,
/** Hold button. */
PSP_CTRL_HOLD     = 0x020000,
/** Music Note button. */
PSP_CTRL_NOTE     = 0x800000,
/** Screen button. */
PSP_CTRL_SCREEN   = 0x400000,
/** Volume up button. */
PSP_CTRL_VOLUP    = 0x100000,
/** Volume down button. */
PSP_CTRL_VOLDOWN  = 0x200000,
/** Wlan switch up. – NOT USABLE IN CWCHEAT*/
PSP_CTRL_WLAN_UP  = 0x040000,
/** Remote hold position. */
PSP_CTRL_REMOTE   = 0x080000,
/** Disc present. – NOT USABLE IN CWCHEAT*/
PSP_CTRL_DISC     = 0x1000000,
/** Memory stick present. – NOT USABLE IN CWCHEAT*/
PSP_CTRL_MS       = 0x2000000,

```

```
};
```