

MANUALE CW CHEAT 0.1.3
For devhook

Sommario

<i>Uso Cw Cheat Installer</i>	3
<i>Uso cw cheat prx</i>	6
<i>Uso cheat searcher</i>	17
<i>Appendice: codici controller</i>	19

Gli ultimi aggiornamenti sono disponibili su <http://www.consoleworld.org> e <http://weltall.consoleworld.org>

Gli ultimi aggiornamenti del database sono disponibili su <http://cwcheat.zioale.it> o su <http://cwcheat.consoleworld.org> .

Uso Cw Cheat Installer

Questo programma si preoccupa di installare e disinstallare automaticamente cwcheat, è utile anche per aggiornare cwcheat nelle prossime release.

Una volta avviato (su 1.50) apparirà questa schermata:



In questa schermata ci sono 4 pulsanti selezionabili con <- -> e attivabili con X.

Iniziamo ad esaminare install (che è uguale a recover con l'unica differenza che install è da usare solo se non è presente cwcheat! Mentre recover si usa per aggiornare, ripristinare dati corrotti o installare cwcheat su firmware diversi da quello della prima installazione).

Premendo X su install apparirà questa schermata.



Qua è possibile selezionare un'installazione tipica o una personalizzata.

L'installazione tipica installa il prx, il database e attiva il prx solo in game.

L'installazione personalizzata permette di selezionare dove attivare il prx tra "in game" e nella vsh.

Chi sceglie l'installazione tipica salti il prossimo passaggio.

Una volta selezionata l'installazione personalizzata apparirà questa schermata:



Qua è possibile attivare e disattivare il prx in alcune locazioni del firmware premendo X si attiva disattiva la locazione premendo su continue si continua l'installazione.

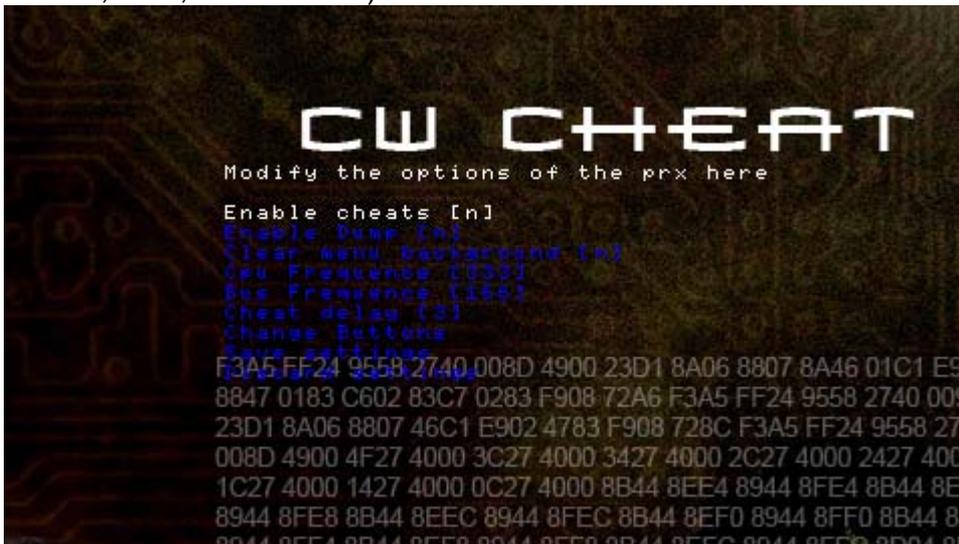
Sia che si sia scelto installazione tipica che personalizzata poi apparirà questa schermata:



Qua è visualizzata una lista delle cartelle di firmware presenti nella cartella dh ed è possibile scegliere il firmware dove installare cwcheat (se si vuole installare il prx in più firmware usare la funzione restore dopo aver completato l'installazione e selezionare il secondo firmware).

Premendo X su un firmware si inizia l'installazione.

Ritornando al menu principale la seconda opzione che esaminiamo (configure) permette di configurare il prx: è possibile configurare tutto meno i tasti kernel mode (vol+/vol-, note, screen, hold, remote hold)

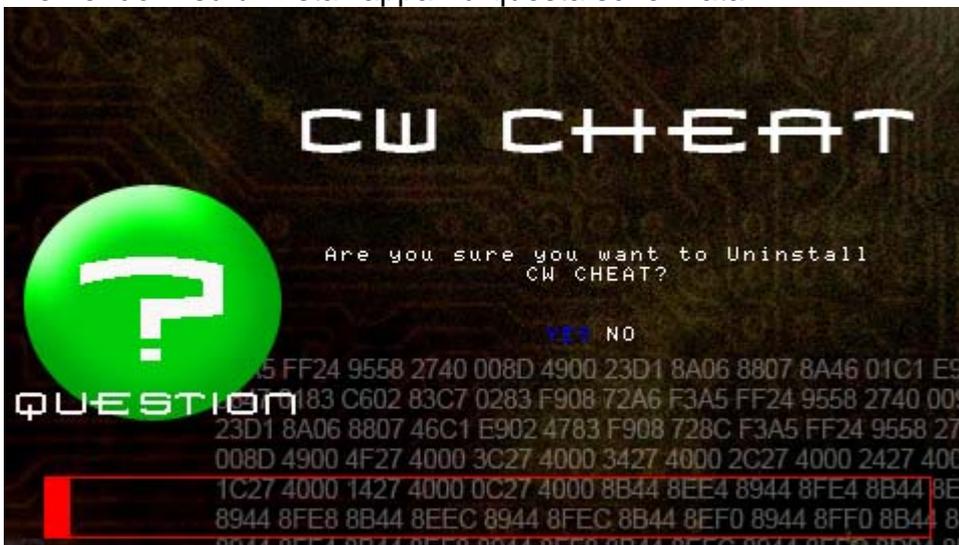


I tasti sono gli stessi del prx, save settings salva la configurazione su file, discard settings non modifica la configurazione.

NB per usare questa funzione è necessario prima avere già salvato una configurazione all'interno del prx.

Infine l'ultima opzione è uninstall che cancella ogni riferimento del prx dai file del firmware, rimuove il prx, il database e lascia solo i dati di configurazione.

Premendo X su uninstall apparirà questa schermata:



Selezionando YES con <- e premendo X inizierà la disinstallazione

NOTE: In questo programma è sempre possibile tornare al menu principale con O e se ci si trova già nel menu principale si torna alla VSH della psp.

Uso cw cheat prx

Il prx viene caricato ad ogni avvio del gioco o della vsh secondo il metodo di installazione usato e viene attivato dopo il rilevamento di un umd inserito.

Una volta attivato è possibile accedere a tutte le funzioni del prx che automaticamente avrà caricato il database e se presente la configurazione.

Per accedere al menu basta premere SELECT (tasto configurabile in seguito) per circa 3 secondi (tempo configurabile).

Entrati nel menu si presenterà questa schermata:

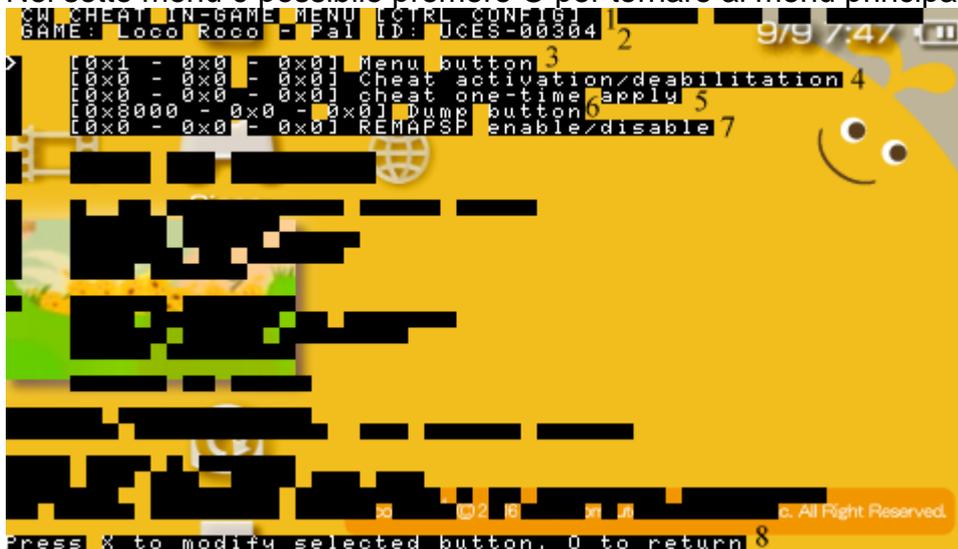


- 1- Nome del programma, nei sottomenu visualizza il menu in cui ci si trova.
- 2- Visualizza dopo game il nome del gioco (se inserito nel database) a destra l'id del gioco (è lo stesso numero che si trova sulla custodia e sul dischetto).
- 3- Permette di applicare i trucchi attivati
- 4- Attiva la funzione di dump assegnata di default al tasto quadrato (modificabile)
La funzione di dump permette di scrivere su un file nella root MEMDUMP.dmp tutto il contenuto della ram user per poter poi trovare trucchi.
- 5- Cancella lo sfondo prima di aprire il menu, è utile se mantendo l'immagine del gioco (come nell'immagine soprastante) non è possibile leggere il menu.
- 6- Abilita la funzione USB MASS
- 7- Abilita remaPSP e carica la mappa dei tasti selezionata di default o quella associata al gioco
- 8- Permette di cambiare la frequenza della cpu (0 = nessun cambiamento).
- 9- Permette di cambiare la frequenza del bus (0 = nessun cambiamento).
- 10-Permette di selezionare i tasti controllati (per esempio per accedere ai menu) è possibile selezionare da 1 a 10 secondi.
- 11-Apre un sottomenu che permette di attivare/disattivare i trucchi disponibili e fare altre operazioni sul database.
- 12-Applica manualmente i trucchi per una sola volta.

- 13-Apre il menu di remaPSP che permette di scegliere una mappa dei tasti tra quelle nella cartella ms0:/remaps/
- 14-Un piccolo text reader legge il file ms0:/chatlog.txt nello spazio disponibile su schermo.
- 15-Apre un sottomenu che permette di configurare i tasti.
- 16-Salva tutte le opzioni e la configurazione dei tasti come default che sarà caricato ad ogni avvio (NB: per le configurazioni del clock è data la precedenza alla configurazione di devhook quindi sono applicate in automatico solo se devhook è configurato su 0 (nessun cambiamento).
- 17-Ricarica il database dalla memory stick (utile se si trovano nuovi trucchi per provarli senza uscire e rientrare nel gioco).
- 18-Permette di accedere a funzioni di ricerca di codici direttamente dalla psp: sono supportate la ricerca per valori precisi (fixed value search) e per differenze (diif search)
- 19-Esce dal menu e torna al gioco
- 20-Sotto questa scritta sono disponibili alcune informazioni del sistema.
- 21-Se non è presente la batteria visualizza quello che si può vedere in figura, in caso contrario visualizza se la psp è collegata alla corrente di rete, se sta ricaricando la batteria, la percentuale di carica, il tempo di carica rimasto e il voltaggio.
- 22-Visualizza in mb quanto è lo spazio disponibile e quello totale.
- 23-Visualizza i mhz a cui va la cpu e il bus
- 24-Visualizza la versione di devhook e quella del firmware attualmente caricato
- 25-Visualizza la versione, la data e l'ora di build del cwcheat.prx.
- 26-Visualizza un aiuto rapido sulla funzione scelta.

Si può usare SU e GIU per spostarsi nei menu e X per confermare.

Nei sotto menu è possibile premere O per tornare al menu principale.

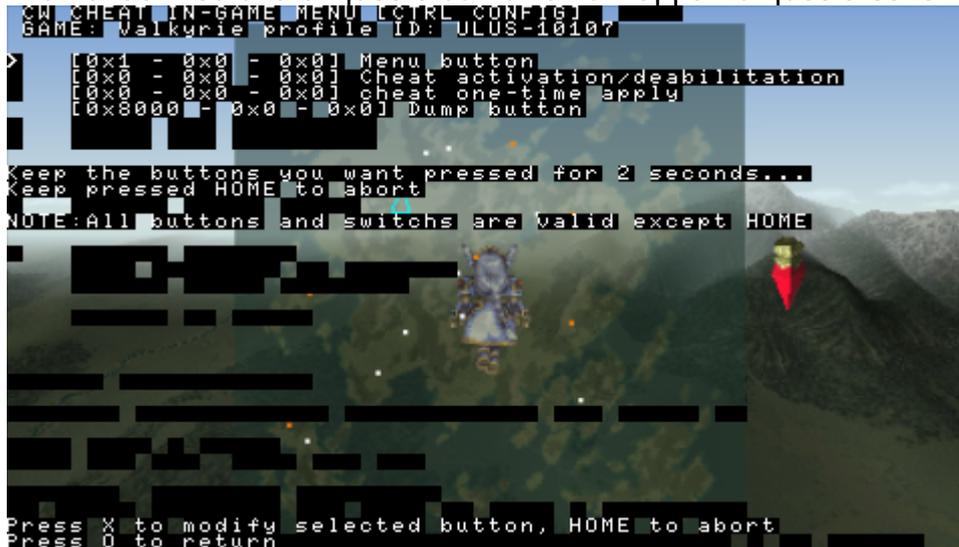


Questo menu permette di modificare la configurazione dei tasti, è possibile scegliere combinazioni fino a 3 tasti e menu che col "menu button" è possibile disabilitare la combinazione.

- 1- Intestazione del menu indica che ci si trova nel menu CTRL CONFIG
- 2- Informazioni sul gioco e l'id del gioco
- 3- Questo permette di modificare il tasto per accedere al menu, non è possibile disabilitare questa combinazione, se si tenterà di annullarlo sarà ripristinato il valore di default (SELECT).

- 4- Questa combinazione ha lo stesso risultato di abilitare/disattivare la voce n. 3 nel menu principale e permette di abilitare o disabilitare l'applicazione dei trucchi.
- 5- Questa combinazione permette di applicare quando premuta i codici. Ha lo stesso effetto dell'opzione n. 12 nel menu principale.
- 6- Questa combinazione permette di dumpare la ram e scriverla su file nella memory stick. L'opzione di default è quadrato, ma è possibile disattivare questa combinazione.
- 7- Questa combinazione permette di attivare/disattivare remaPSP. Ha la stessa funzione della voce n.7 nel menu principale
- 8- Visualizza un aiuto rapido

Premendo X su una di queste combinazioni apparirà questa schermata:



Che invita di tenere premuti i tasti per 2 secondi (fino a quando non spariscono le scritte apparse premendo X) che si vogliono usare per attivare la funzione selezionata.

Una volta trascorso questo tempo sarà cambiata la combinazione con quella nuova, se non viene premuto nulla la combinazione viene annullata e disattivata (esclusa quella del menu che in questo caso viene configurata come select).

Se non si vuole cambiare la configurazione basta tenere premuto HOME e non sarà cambiata.

Premendo O è possibile tornare al menu principale.

Un'altro menu è il menu select cheat accessibile dal menu principale.



In questa schermata è possibile attivare/disattivare i vari trucchi presenti nel db premendo X, ogni trucco ha a sinistra un box [x] con scritto y o n a seconda se il trucco è attivato o meno e a destra una piccola descrizione del trucco.

Premendo O è possibile tornare al menu principale.

Premendo TRIANGOLO è possibile attivare/disattivare tutti i trucchi in lista.

Premendo SELECT è possibile salvare il gioco nel database con le selezioni di attivazione/disattivazione dei trucchi, le modifiche ai valori e i nuovi cheat aggiungi

Premendo QUADRATO è possibile accedere a una schermata in cui è possibile modificare il valore di un trucco



Premendo Quadrato Apparirà questa schermata da cui è possibile cambiare i valori di un cheat:

Premere SINISTRA/DESTRA per togliere/aggiungere 100

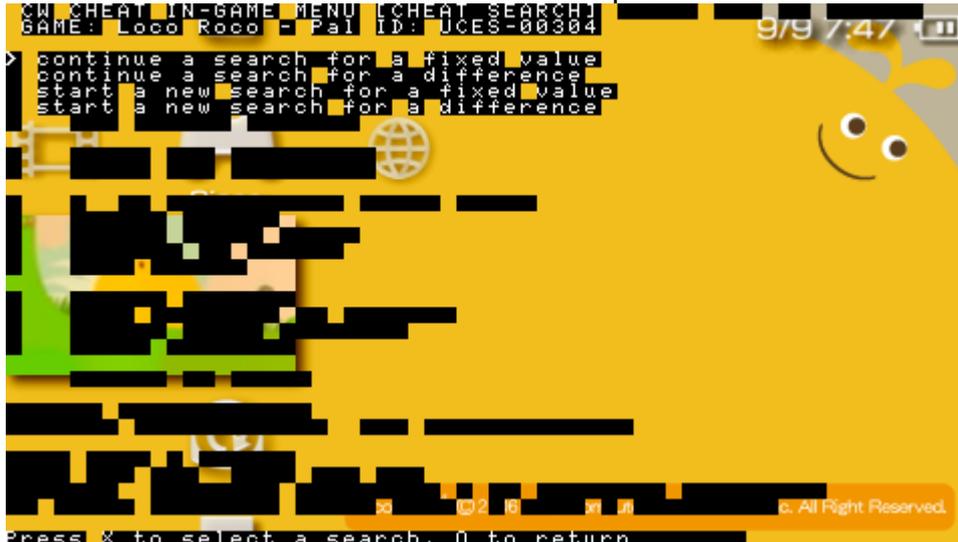
Premere SU/GIU per aggiungere/togliere 1

Premere L/R per togliere/aggiungere 1000

Premere QUADRATO/TRIANGOLO per cambiare codeline

Premere X per accettare il valore e O per uscire senza accettare il nuovo valore

Infine c'è il menu di ricerca dei trucchi che prevede varie sezioni:



Per iniziare una ricerca si usa la 3^a e la 4^a voce

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

La prima di queste permette di cercare nella memoria un valore che si conosce, per esempio i soldi. La seconda invece permette la ricerca di una differenza di valore (uguale, differente, maggiore, minore).

Dopo aver fatto il primo passaggio di ricerca e ritornando a questo menu dopo aver modificato il valore scegliere una delle prime due voci a seconda se si stava facendo una ricerca per un valore conosciuto o una differenza

Iniziamo con la fixed value search (spazio su ms richiesto da 1 a 5mb normalmente):

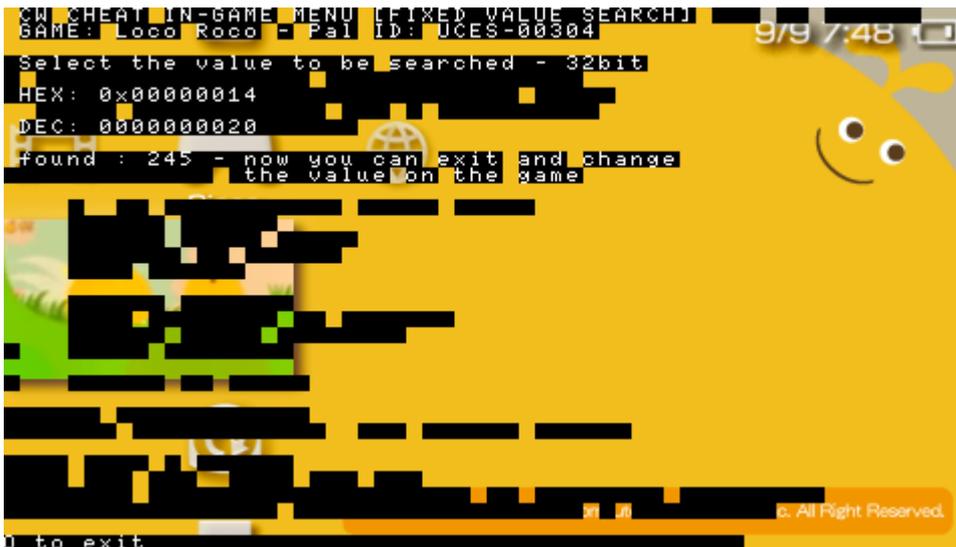


Premendoci verrà presentata una schermata simile a questa.

Prima cosa da fare è selezionare i bit del valore da cercare! Questo si può fare con QUADRATO e cambia tra 8, 16 e 32bit

Tenere a mente questa cosa quando si fa una ricerca: se un valore sembra poter arrivare arrivare come massimo a 255 usare l'8bit, invece se può arrivare al massimo a 65535 usare i 16bit e infine per i valori più alti usare i 32bit (normalmente i soldi sono 32bit per esempio)

Una volta fatto questo si può usare il DPAD, L e R per cambiare il valore (vedere la sezione sulla modifica dei valori dei trucchi per maggiori informazioni) e premere X per iniziare la ricerca.



Una volta finita verrà presentato il numero di valori trovati.

A questo punto si ritorna al menù principale con O, si esce dall'ingame menu e si modifica il valore.

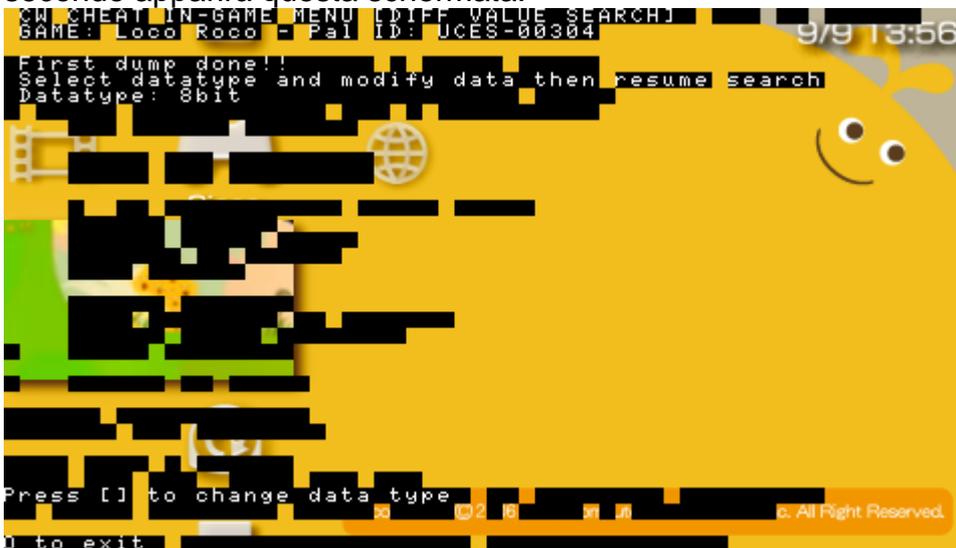
Dopo aver modificato il valore si sceglie Continue fixed value search



In questa schermata è possibile fare due cose.

Continuare la ricerca immettendo un nuovo valore e rifacendo lo stesso procedimento del primo passaggio o controllare il valore che hanno assunto i primi 10 valori trovati e se molto probabilmente sono quelli giusti con TRIANGOLO è possibile scegliere un indirizzo e aggiungerlo alla lista dei codici con X. Verrà automaticamente aperta la schermata di modifica valore che permette di scegliere il valore da assegnare al trucco. Per ulteriori informazioni guardare la funzione di modifica cheat in questo manuale.

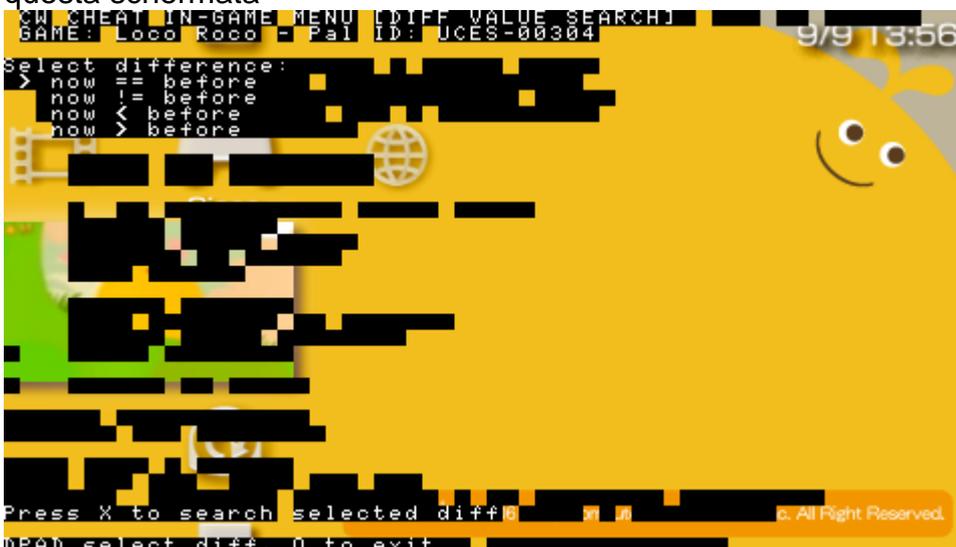
Invece ora passiamo alla ricerca per le differenze o diff search (richiedi 512KB di kernel ram libera, 25MB di spazio su ms per il dump e fino a 10mb per passo a seconda dei risultati) Premendo su start diff search verrà effettuato il dump preliminare della ram e dopo qualche secondo apparirà questa schermata:



Qua bisogna scegliere il tipo di ricerca 8 / 16 / 32 bit premendo QUADRATO e poi uscire e cambiare il valore.

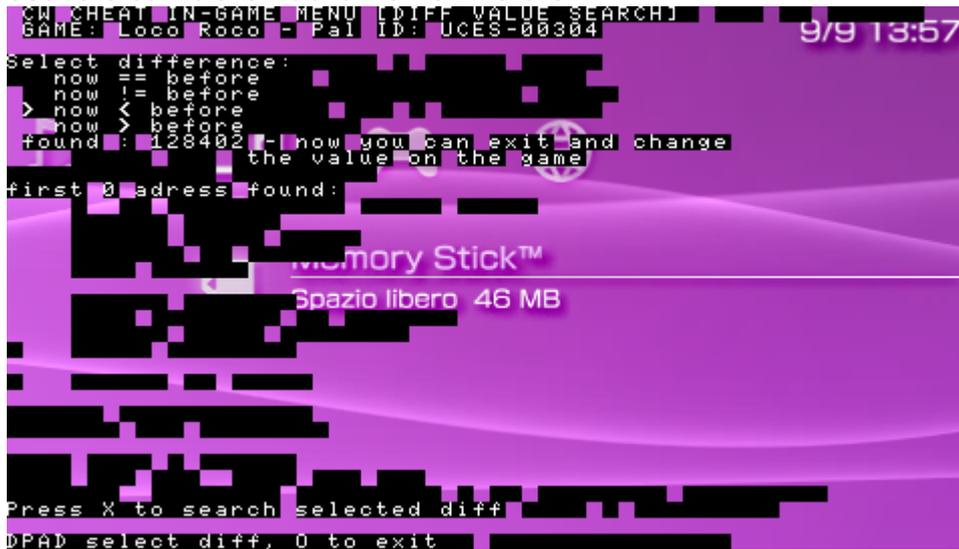
Ulteriori informazioni sul tipo di ricerca sono presenti nella sezione sul fixed value search

Dopo aver modificato il valore basta premere su continue diff search e verrà presentata questa schermata

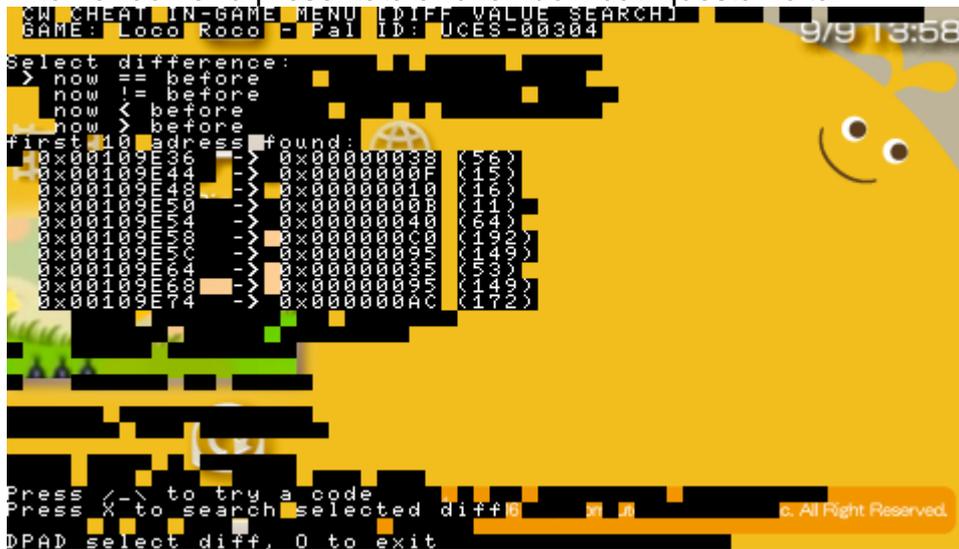


Qui si sceglie il tipo di differenza tra ==, !=, < e > e si preme X

Dopo un po' di tempo verrà presentata la schermata dei risultati. A questo punto si può solo uscire e cambiare nuovamente il valore.



Ritornando verrà presentata anche nuovi dati questa volta:



Questo permette di controllare i valori nei primi 10 indirizzi trovati e poter, come trattato aggiungere un trucco con gli indirizzi trovati da provare subito o continuare la ricerca come fatto prima

Sia il database sia il file di configurazione sono messi nella cartella ms0:/dh/ e sono editabili semplicemente con un editor di testo.

Il database (chiamato cheat.db) può essere in qualunque formato UNIX/DOS/MAC, contenere valori e indirizzi in decimale (123), esadecimale (0x0000007B) e ottale (0173) e viene comunque letto e interpretato correttamente e ha questo formato:

_S signature del gioco: è un codice come ULUS—10041 ed è possibile reperirlo in alto a destra nel menu principale dopo la scritta ID.

Esempio: _S ULUS-10041

_G nome del gioco: è il nome del gioco di massimo 30 caratteri.

Esempio _G GTA LCS (US)

_C0 nome del trucco: una piccola descrizione per il trucco massimo 30 caratteri (il massimo di trucchi supportati per gioco sono 400 gli altri saranno ignorati). Lo 0 vicino a _C indica lo stato di attivazione/disattivazione del trucco

Esempio: _C0 \$9999999

_L identifica una linea di codice per il trucco è formata da due numeri in formato esadecimale che cambiano significato a seconda del tipo di trucco (guardare il sito linkato nel readme per ulteriori informazioni) i due numeri devono avere davanti lo 0x che identifica un numero esadecimale. Di questi ce ne possono essere 29 per trucco.

Esempio: _L 0x20389ACC 0x05F5E0FF

Un esempio completo:

_S ULUS-10022

_G Legend Of Heroes 2

_C0 max Pia

_L 0x202E4874 0x0001869F

_C0 max G

_L 0x202E4878 0x0001869F

NB: se trovate dei trucchi fatti senza 0x sono in formato assoluto quindi per poterli usare bisogna sottrarre l'indirizzo (normalmente è il primo numero, ma può cambiare a seconda del tipo di codice) di 0x08800000. Quindi se si fanno trucchi per cw cheat basta prendere l'indirizzo nel dump e usare quello senza ulteriori operazioni.

Un'altra nota alcuni trucchi vecchi fatti con l'uso di mph game loader hanno un errore di offset causato da mphgl quindi su devhook bisognerà sottrarre 0x4300 da ogni indirizzo.

La configurazione invece può essere così:

CHEAT ENABLE = 0 -> 1 per abilitare all'avvio i trucchi, 0 per disabilitare.

DUMP ENABLE = 0 -> 1 per avere già attivo il dump all'avvio, 0 per non averlo attivo

CLEAR ENABLE = 0 -> 1 per abilitare la cancellazione dello schermo prima di aprire il menu

USB ENABLE = 0 -> 1 per abilitare l'USB MASS, 0 per disabilitare

REMAP ENABLE = 0 -> 1 per abilitare all'avvio il remapsp, 0 per disabilitare

USB DUMP = 0 -> 1 per abilitare il dump su usbhostfs0:/, 0 per dumpare su ms0:/

CPU CLOCK = 333 -> scrivere qua i mhz che si desidera impostare alla cpu all'avvio

NB: le impostazioni di devhook hanno la precedenza, qua è possibile impostare anche frequenze non supportate nel menu.

BUS CLOCK = 166 -> scrivere qua i mhz che si desidera impostare al bus all'avvio.

Valgono le note di CPU CLOCK

DELAY TIME = 3 -> imposta il delay tra ogni controllo dei tasti

Questi tre sono i bottoni della combinazione del menu potete trovare i codici a questo indirizzo (svn.ps2dev.org).

MENU BTN1 = 0x1

MENU BTN2 = 0x0

MENU BTN3 = 0x0

Questi tre sono i bottoni della combinazione dell'attivazione/disattivazione dei trucchi.

CHEATEN BTN1 = 0x0

CHEATEN BTN2 = 0x0

CHEATEN BTN3 = 0x0

Questi tre sono i bottoni della combinazione dell'applicazione immediata dei trucchi.

CHEATAP BTN1 = 0x0

CHEATAP BTN2 = 0x0

CHEATAP BTN3 = 0x0

Questi tre sono i bottoni della combinazione per dumpare la ram su file.

DUMP BTN1 = 0x8000

DUMP BTN2 = 0x0

DUMP BTN3 = 0x0

REMAP DFILE = ms0:/remaps/DEFAULTS.TXT -> il file che remaPSP carica se non trova un file specifico per il gioco

NB: Questo file deve essere tassativamente in formato UNIX.

Uso cheat searcher

Questa applicazione per windows permette di cercare i trucchi in vari dump cercando valori precisi o differenze nel valore.

Una volta avviato appare questa schermata



Da qua è possibile scegliere se cercare un valore preciso o cercare un aumento/diminuzione di un valore.

Qua è possibile pure scegliere tra l'italiano e l'inglese

Premendo su ricerca di un valore apparirà questa schermata:

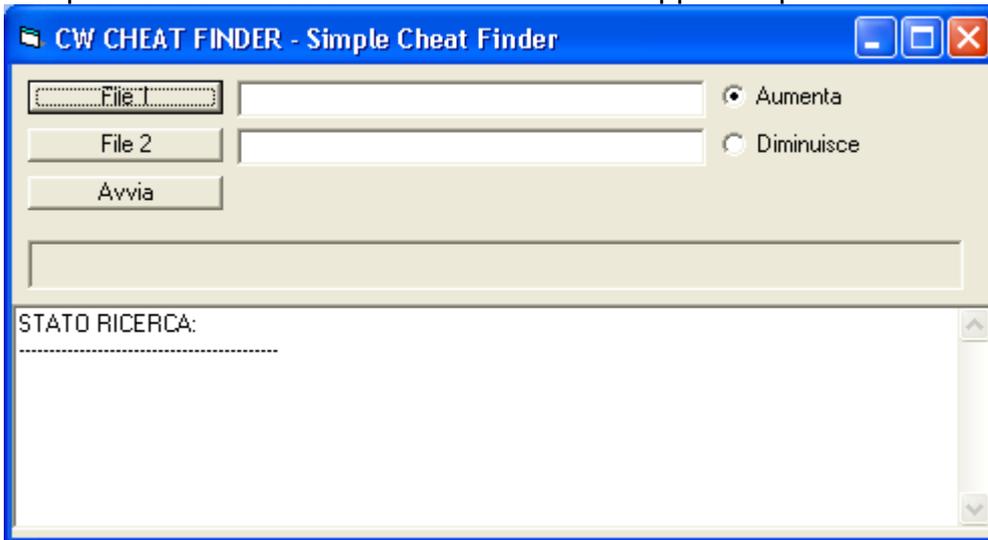


Qui nella text box in alto a sinistra si inserisce il valore che si vuole cercare e si preme cerca, sarà richiesto un file di dump della psp e inizierà la ricerca è possibile fare questo processo teoricamente all'infinito fino a che non si trova il valore.

A quel punto premendo fine ricerca sarà mostrato uno stub da inserire nel database con gli indirizzi trovati.

Se è selezionato AUTO viene automaticamente scelta la quantità di bit da cercare a seconda del valore. Se si vuole forzare la ricerca basta scegliere 8/16/32 bit

Ora premendo ricerca aumento diminuzione apparirà questa schermata:



Da questa schermata è possibile cercare differenze tra due file in modo da trovare trucchi come le barre della vita o simili.

Premendo file 1 e file 2 si selezionano due dump da comparare e selezionando aumenta si ricerca un aumento di valore tra il dump 1 e il dump 2, invece con diminuisce una diminuzione di valore tra il file 1 e il file 2.

Premendo Avvia si inizia la ricerca. Una volta completata è possibile continuare a comparare altri dump cercando solo negli indirizzi precedentemente trovati.

Appendice: codici controller

Questi sono i codici disponibili per impostare a mano i controlli e per controllarli nella schermata di impostazione:

```
/*
 * 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,
```

```
};
```