Happy Hacking con Sid Meier's Colonization

fanta <fanta@56k.es>

Sumario

Obtener el juego

Para trastear con este juego se ha de **obtener primero el juego** y también disponer de dosbox-x .

Con el que he estado trasteando yo es este: Sid_Meiers_Colonization.tar.gz

```
http://fanta.56k.es/games/1990/1994-Sid_Meiers_Colonization-Spanish/
Sid_Meiers_Colonization.tar.gz
```

Compilar la última versión de dosbox-x

```
$ git clone http://git.56k.es/fanta/compile-Dosbox-x
$ cd compile-Dosbox-x/
# bash compileDosBox-x.sh
```

Activar los cheats en el juego

Cuando andas jugando puede **activarse un menú oculto** tal y como se ve en la captura.

Puede activarse pulsando **alt y luego W I N** . No confundir con Alt + tecla windows, se trata de alt y la W, luego la I, lueo la N .

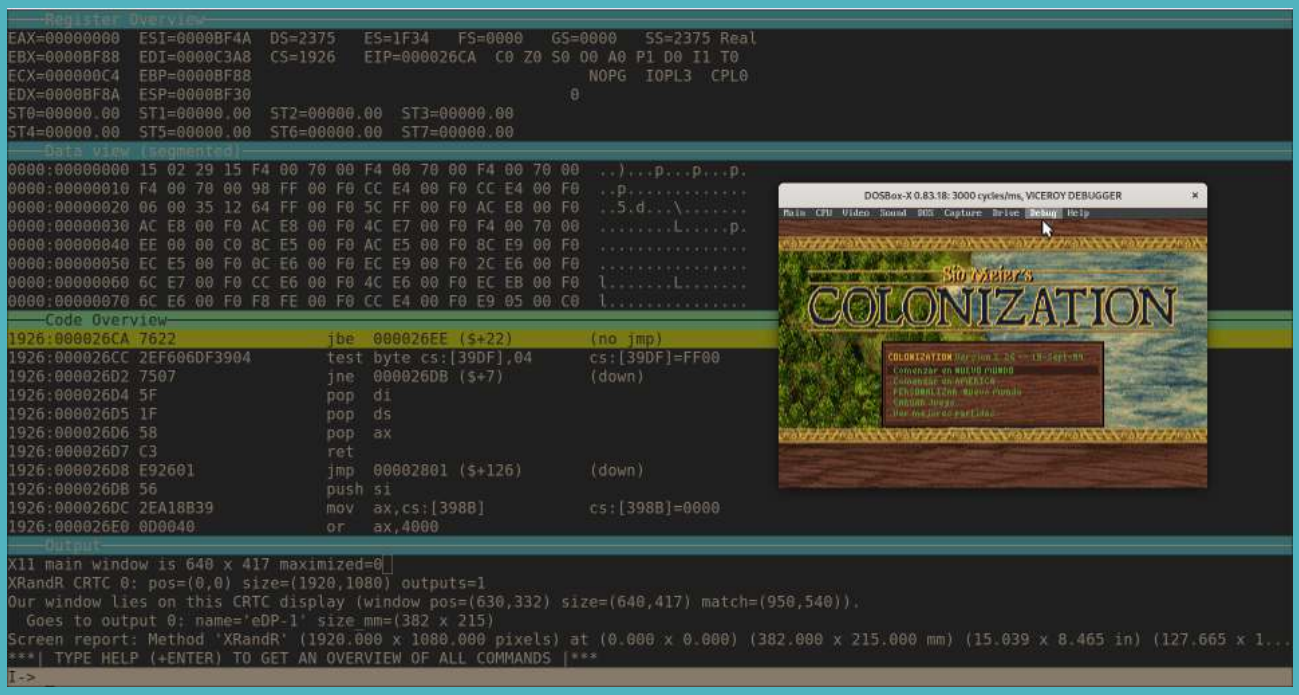
Para desactivar simplemente **alt + W** . No necesariamente las letras en mayúsculas.

Comprobar cuando cambia una zona de memoria en el juego

Nuestra intención será simplemente **colocar un breakpoint en una zona de la memoria que esté a 0x00 y que cuando ese no sea su valor nos avise.**

En el caso de ejemplo es la zona de memoria donde se coloca el primer carácter del nombre que vamos a darle al explorador que seleccionemos en el juego.

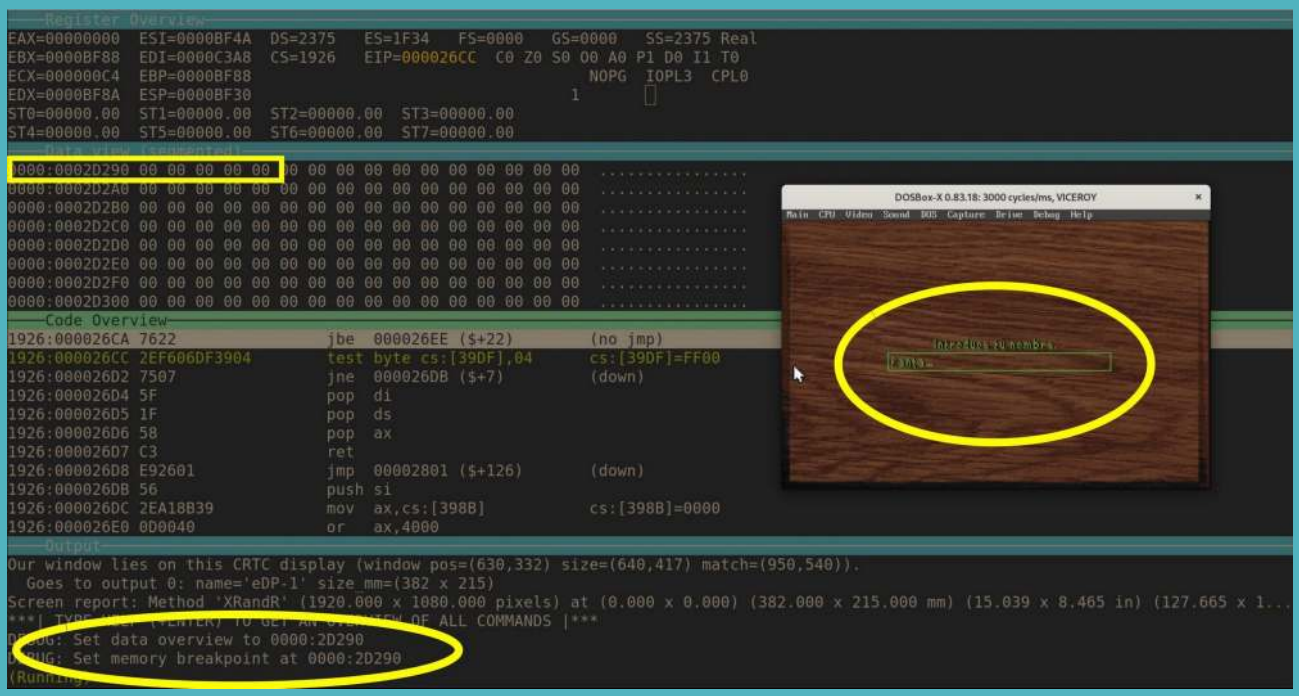
Nada más arrancar el juego activamos el modo debug (pinchando en debug).



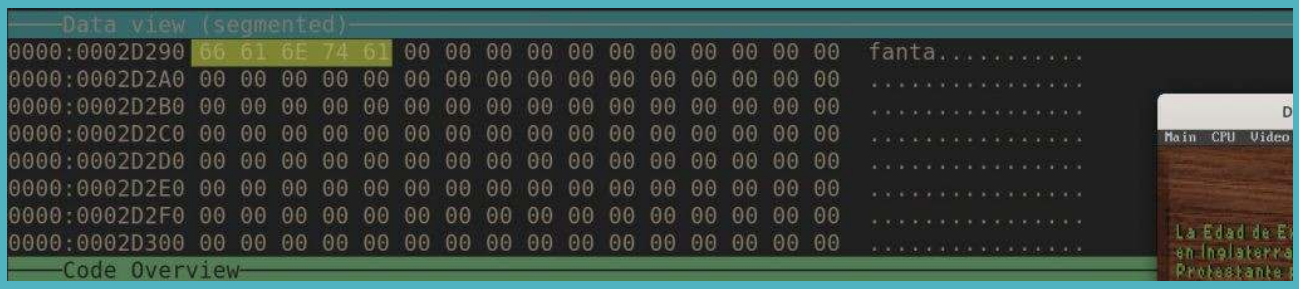
Vamos a proceder a escribir las siguientes ordenes para crear un break point memory **en la posición 0000:0002D290**

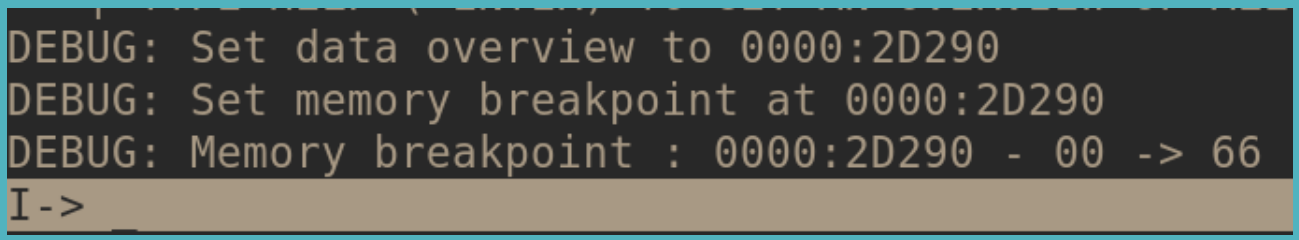
```
bpm 0000:2D290
d 0000:2D290
run
```

Con «bpm» seteamos el break point y con «d» vamos a mostrar esa zona de memoria.



Una vez marcado el breakpoint en 0000:2D290 seguimos con el juego en marcha (run) hasta llegar a la zona de introducir el nombre. **En mi caso voy a poner fanta y darle a intro.**
En el momento de darle a intro tendría que **cambiar el valor de esa posición de memoria de 00 a 66.**





El motivo de cambiar de 00 a 66 es que **la «f» minúscula en hexadecimal sería 66**. La «a» sería 61 y así hasta terminar fanta.

El juego almacenará 23 caracteres ASCII consecutivos desde la posición: **0000:2D290**

Cambiar valores en los archivos de partidas guardadas

Por defecto al **iniciar una nueva partida empezaremos con 1000 de oro** y cosas como que tenemos el mapa oculto (tenemos que ir descubriendo el mapa)

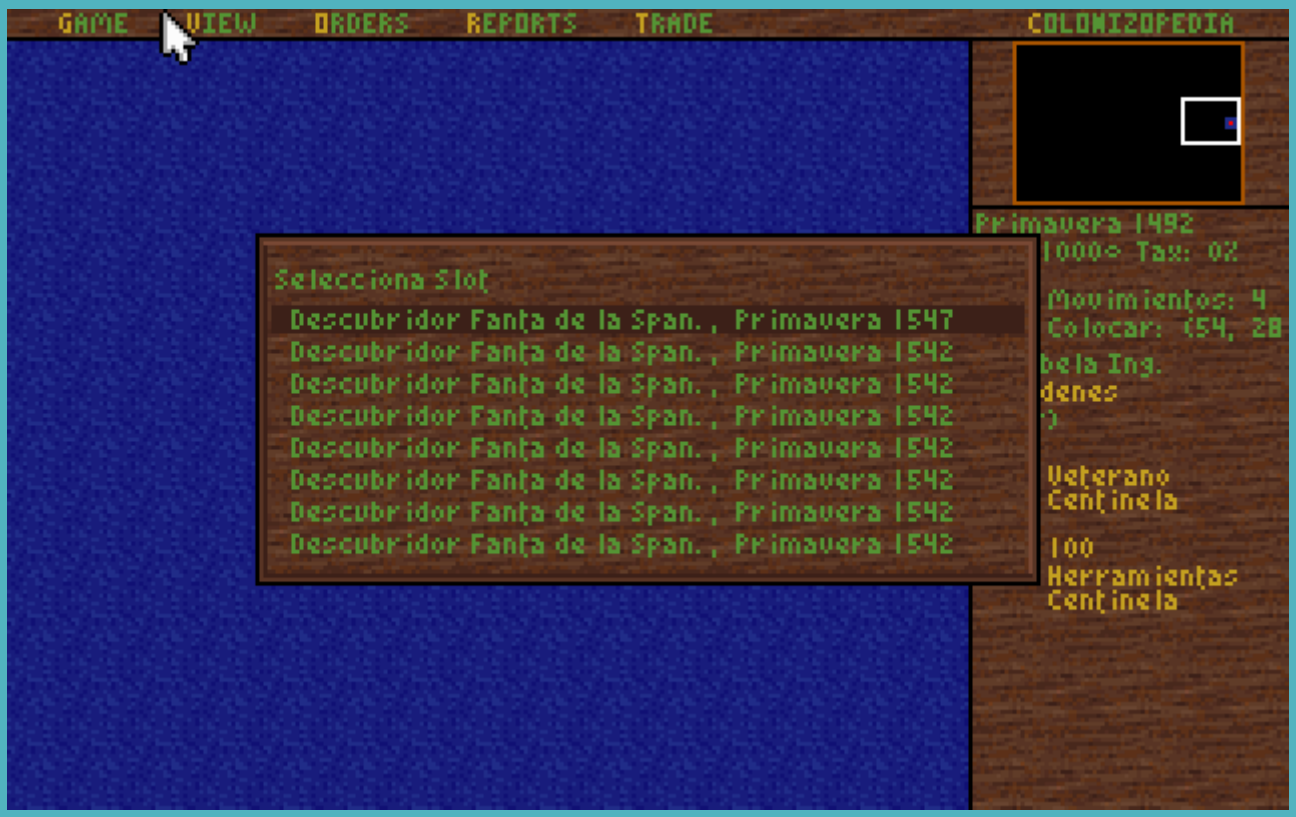
Se puede ver en la siguiente captura.

El juego tiene 8 slots para guardar partida y 10 para cargar. El motivo de que tenga 2 slots más cuando cargas partida es porque esos 2 son de guardado automático.

Por tanto tienes **los slots de guardado** siguientes que se corresponden con los archivos siguientes:

– SLOT 01 – COLONY00.SAV
– SLOT 02 – COLONY01.SAV
– SLOT 03 – COLONY02.SAV
– SLOT 04 – COLONY03.SAV
– SLOT 05 – COLONY04.SAV
– SLOT 06 – COLONY05.SAV
– SLOT 07 – COLONY06.SAV
– SLOT 08 – COLONY07.SAV
– SLOT 09 – COLONY08.SAV – **AUTOGUARDADO** (al final de cada década del juego)
– SLOT 10 – COLONY09.SAV – **AUTOGUARDADO** (al final de cada turno, cambia año)

PANTALLA DE SAVE (GUARDAR) – 8 SLOTS



PANTALLA DE LOAD (CARGAR) – 10 SLOTS

Una forma de **encontrar cambios en los archivos guardados** es grabar en el slot1 una partida nada más comenzar el juego. Luego cargamos esa partida y realizamos un cambio solamente (por ejemplo activar los cheats y mostrar el mapa).

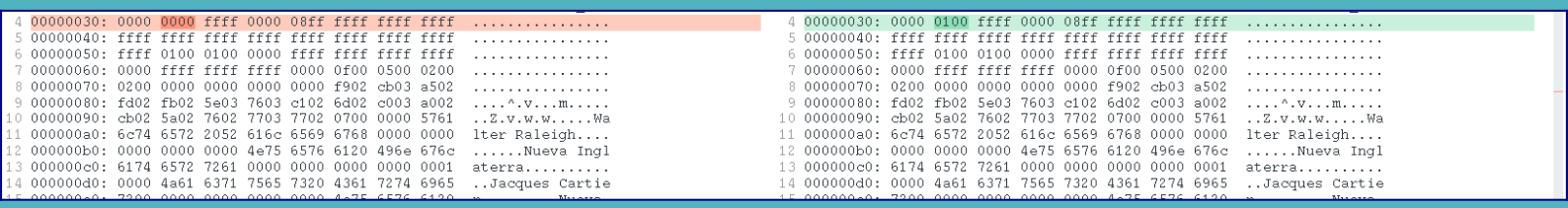
El tema es realizar un cambio y guardar de nuevo pero en el slot 2 esta vez.

De esta forma podemos guardar como archivos 00 y 01 (en texto plano hex ascii) y buscar diferencias entre ambos archivos:

```
xxd COLONY00.SAV > 00
xxd COLONY01.SAV > 01
```

De esta forma encontraremos en que bytes se almacenan los datos.

Un ejemplo:



En esa captura se ve que ha cambiado el byte 33 .

Una de las formas de hacerlo es así para no precisar de un editor hexadecimal.

```
$ cat COLONY00.SAV | xxd -u -c 16 -g 1 | head -4 | tail -1
$ printf "00000032: 01" | xxd -r4 - COLONY00.SAV
$ cat COLONY00.SAV | xxd -u -c 16 -g 1 | head -4 | tail -1
```

```
[fanta@terminator Sid_Meiers_Colonization]$ cat COLONY00.SAV | xxd -u -c 16 -g 1 | head -4 | tail -1
00000030: 00 00 00 00 FF FF 00 00 08 FF FF FF FF FF FF FF  ................
[fanta@terminator Sid_Meiers_Colonization]$
[fanta@terminator Sid_Meiers_Colonization]$
[fanta@terminator Sid_Meiers_Colonization]$ printf "00000032: 01" | xxd -r4 - COLONY00.SAV
[fanta@terminator Sid_Meiers_Colonization]$
[fanta@terminator Sid_Meiers_Colonization]$
[fanta@terminator Sid_Meiers_Colonization]$ cat COLONY00.SAV | xxd -u -c 16 -g 1 | head -4 | tail -1
00000030: 00 00 01 00 FF FF 00 00 08 FF FF FF FF FF FF FF  ................
[fanta@terminator Sid_Meiers_Colonization]$
```

Y una vez alterado ese byte veremos como al cargar de nuevo el slot 1 **veremos todo el mapa despejado.**

Archivos del juego editables fácilmente

Esto lo he encontrado aquí: 562685-sid-meiers-colonization

```
closing.txt -- contains info on the closing animation
colony.txt -- has the names of all the colonies for the 4 nations
debug.txt -- contains MOTD plus the menu information for the cheat menu
game.txt -- containts all the messages plus the menus as well
labels.txt -- has the labels of the game, which is pretty much every word used by the game!
menu.txt -- containts nothing but game menus
names.txt -- discussed in depth below...
opening.txt -- the opening information, what it says and how it animates
pedia.txt -- has ALL the Encyclopedia information
tribe.txt -- only used on America maps, for historical purposes
woodcut.txt -- has the Picture Messages (Creating a Colony, Discovering the Pacific)
```

Más cantidad de oro editando los archivos de partidas

Creo que hasta 4 bytes pueden ocupar los valores de oro en los archivos de guardado de partidas. He creado una pequeña lista en la que se ve que el valor que se ha de añadir para tener 500 de oro es F401.

500 en hexadecimal es 01F4 que si invertimos el orden de los bytes es F401

decimal	hex	invertido
500	01F4	F401
1000	03E8	E803
2000	07D0	D007
10000	2710	1027
50000	C350	50C3
65535	FFFF	FFFF
100000	0186A0	A08601
999999	0F423F	3F420F
9999999	98967F	7F9698

Colocar en el slot 2 (COLONY01.SAV) **9999999 de oro** se podría hacer así:

```
$ cat COLONY01.SAV | xxd -u -c 16 -g 1 | grep -i "0F50"
$ printf "00000f56: 7F" | xxd -r4 - COLONY01.SAV
$ printf "00000f57: 96" | xxd -r4 - COLONY01.SAV
$ printf "00000f58: 98" | xxd -r4 - COLONY01.SAV
$ cat COLONY01.SAV | xxd -u -c 16 -g 1 | grep -i "0F50"
```

De esta forma podemos tener mucho oro. Es hacer trampas.

Un saludo cordial.

Notas finales

Comentar que el juego va a ir más fino con dosbox-x si se marca como cpu core == full core y como cpu type «Pentium pro».

El paso para reproducirlo adecuadamente es:

Para reproducir el tema con el tar.gz limpio que he puesto para descargar. El tema de deshabilitar la niebla del mapa (quitar la oscuridad y todo abierto)

1. cambiar dosbox por dosbox-x en el start.sh e iniciar nueva partida.
2. Para que funcione rápido full core y pentium pro CPU (ya con dosbox-x)
3. Guardar en el slot 1 (COLONY00.SAV) la partida nada más comenzar. Salir y hacer el cambio.
4. El cambio: printf «00000032: 01» | xxd -r4 – COLONY00.SAV
5. Ejecutar de nuevo, cargar el primer slot de partida y a disfrutar el mundo abierto sin oscuridad.