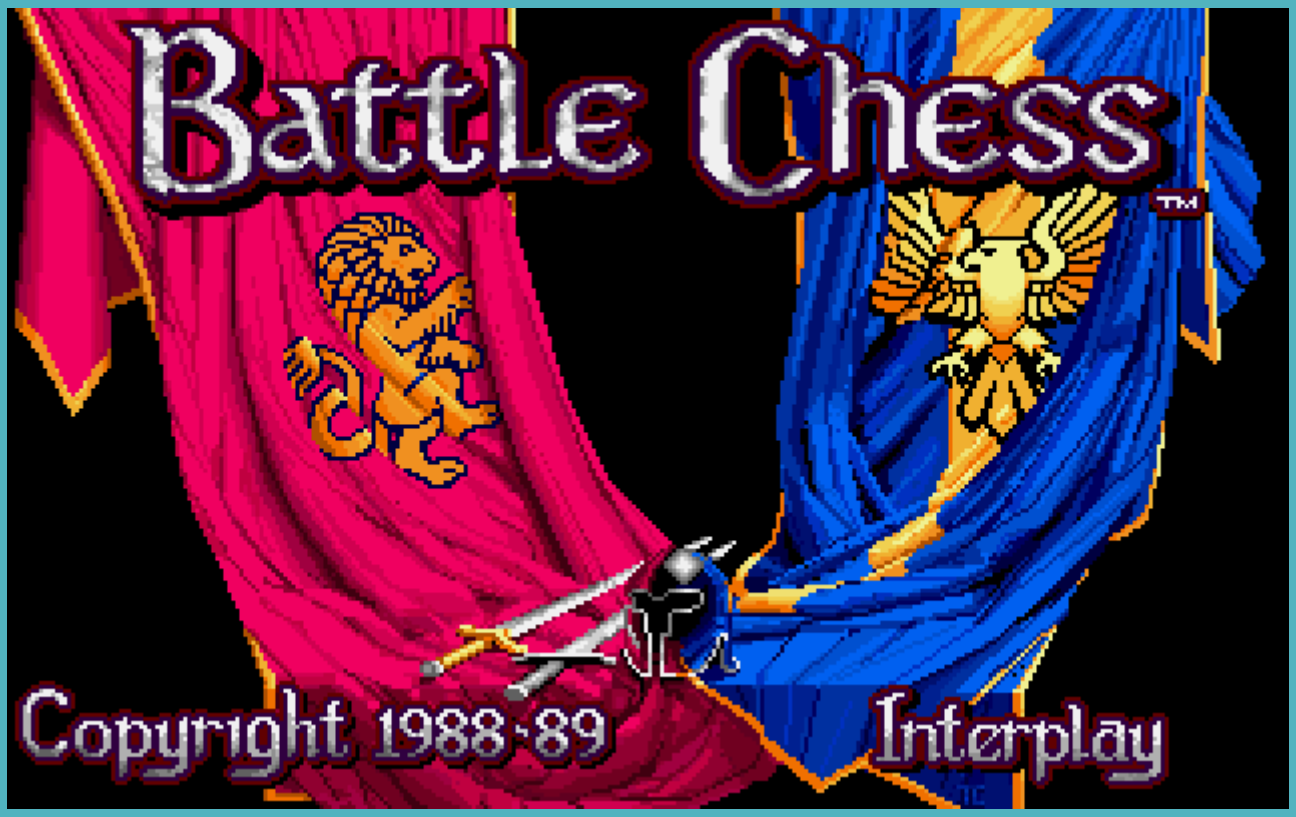
Crackear Battle Chess en 2022

fanta <fanta@56k.es>



Sumario

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
```

Descargar Battle Chess y ejecutar por primera vez

```
$ wget http://fanta.56k.es/games/1980/1988-Battle_Chess/Battle_Chess.tar.gz
$ tar xfvz Battle_Chess.tar.gz
$ cd Battle_Chess/original
$ dosbox-x -fastlaunch -c "mount c ." -c "c:" -c "CHESS.EXE"
```

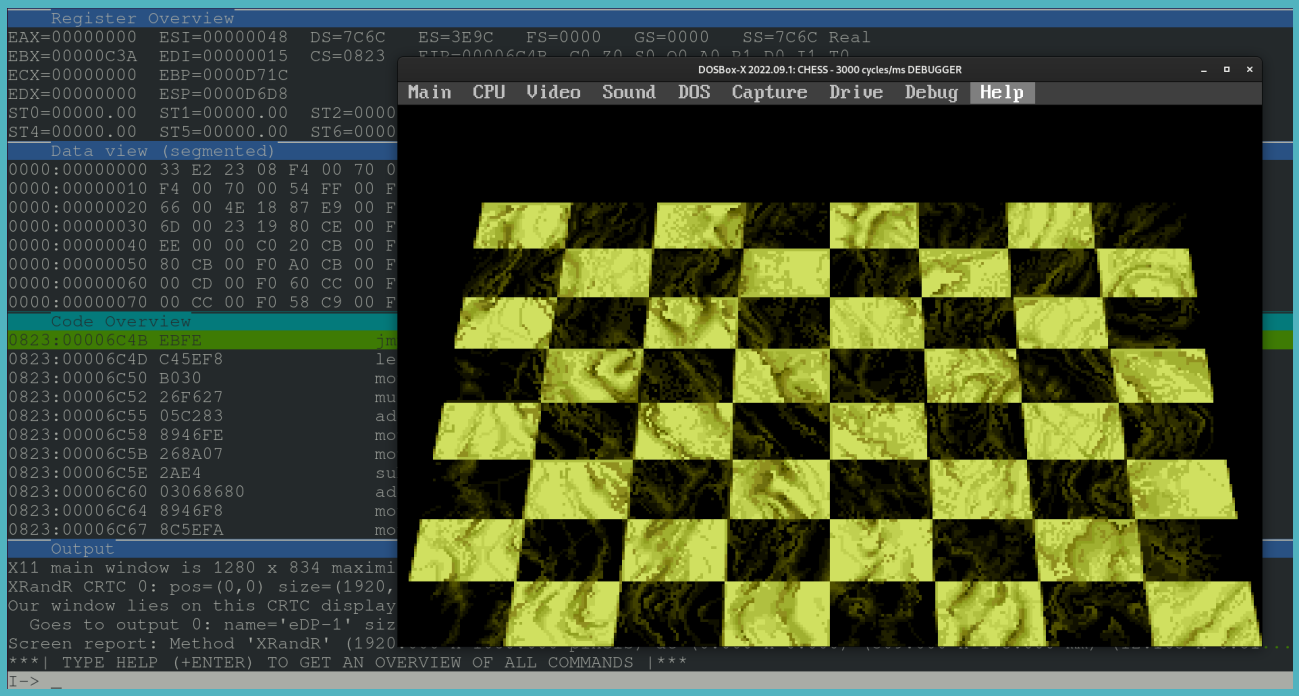
Nada más ejecutar el juego nos pedirá que miremos el manual e indiquemos la posición de una famosa jugada. Esto es un suplicio y la idea es no tener que andar mirando nada cada vez que queremos jugar una partida.

La idea es saltarnos esa protección utilizando para ello dosbox-x y el modo debug.

Desprotegiendo el juego con dosbox-x en modo debug

Ejecutamos el juego con dosbox-x y damos enter todo el rato hasta que se quede en la pantalla que se ve el tablero. Podemos si queremos escribir posiciones inventadas sin sentido y le damos a ENTER.

La idea es fallar todo y que se quede bloqueado. En ese momento pinchamos en Debug → Start dosbox-x debugger (alt + pause)



En la ventana del debugger vamos a ver en Code Overview:

0823:00006C4B EBFE

Tenemos que cambiar en esa posición de memoria EBFE por 9090 (dos nop).

Esto se puede hacer así desde la línea de comandos del debugger:

SM 0823:00006C4B 9090
RUN

Cerramos por tanto el juego y lo abrimos de nuevo. Entonces antes de nada entramos en modo debug y seteamos en memoria los 2 nop (9090).

Cuando luego nos pregunte le damos a todo para adelante con enter o escribimos algo y enter.

Al final en vez de quedarse bloqueado tendría que entrar en el juego.

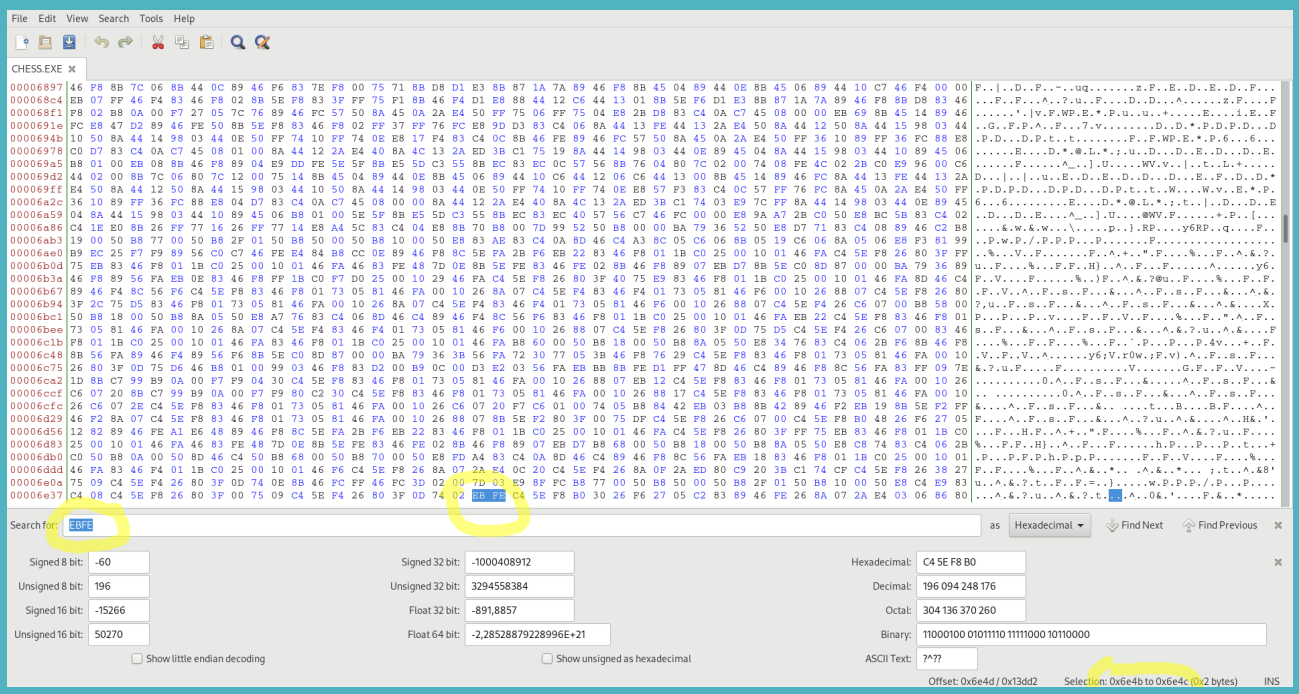
Esto es buena cosa pero tenemos que una vez comprobado que funciona alterar CHESS.EXE para no tener que andar haciéndolo cada vez.

Crackeando el ejecutable alterando lo necesario

Ahora ya por fin vamos a alterar el ejecutable del juego para que directamente siempre podamos empezar a jugar sin tener que andar mirando el manual.

Yo recomiendo usar el programa “bless” que se podrá encontrar seguramente en los repositorios de tu distro GNU+Linux.

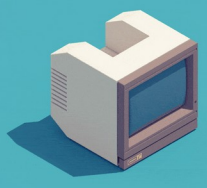
```
$ bless CHESS.EXE
```



Básicamente es buscar EBFE y cambiarlo por 9090. Puede que salgan varias coincidencias pero los valores que nos interesan estarán en 6C4B y 6C4C

A la hora de editar es importante pulsar la tecla insert para que inserte y no desplace.

Se guarda y ya tenemos nuestro Battle Chess listo para poder jugarlo siempre que queramos sin esperas.



TWITCH PEERTUBE FEDIVERSE YOUTUBE TWITTER