

ROMHACKING EN MEGADRIVE

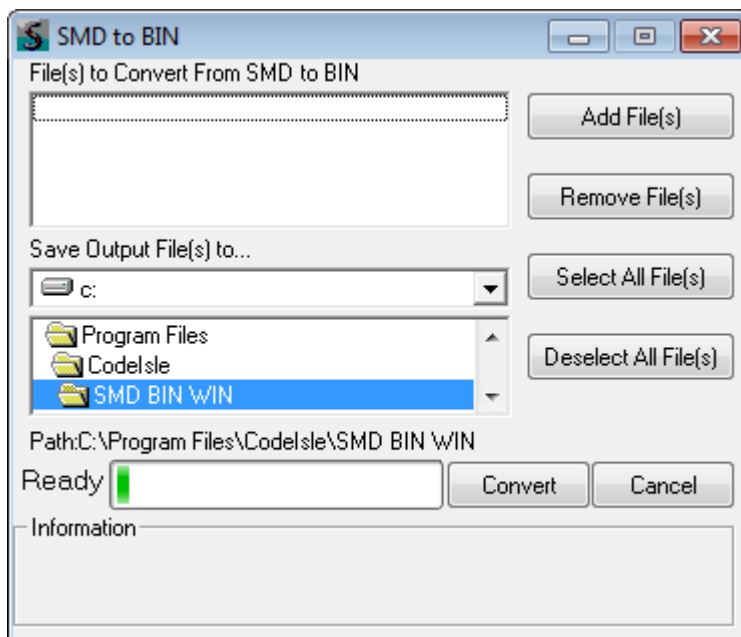
En este tutorial voy a tratar de explicar como conseguir ventajas en juegos de Megadrive modificando la ROM o juego para lo cual vamos a utilizar una serie de herramientas.

Para realizar el proceso necesitaremos los siguientes programas:

- Emulador de Megadrive: Wingens, Megasis o cualquier otro.
- Sega Asm (Ensamblador/Desensamblador de Megadrive).
- GGEncoder (Herramienta que convierte cheats en direcciones de la ROM).
- SMD BIN WIN (Utilidad para convertir entre varios formatos de ROM de Megadrive).
- Editor hexadecimal, tal como Hex Workshop o cualquier otro.
- ROM (Para el ejemplo voy a utilizar el juego "Phelios").

En primer lugar, si el juego o ROM está en formato .SMD en lugar de .BIN debemos convertirlo a este último formato para hacer las modificaciones.

Para ello ejecutamos el SMD BIN WIN y pulsamos sobre el botón "SMD to BIN". En la siguiente pantalla pulsamos sobre "Add File(s)" para seleccionar el fichero .SMD y elegimos el directorio donde se va a guardar el fichero .BIN resultante (tal y como se ve en la parte inferior de la pantalla):



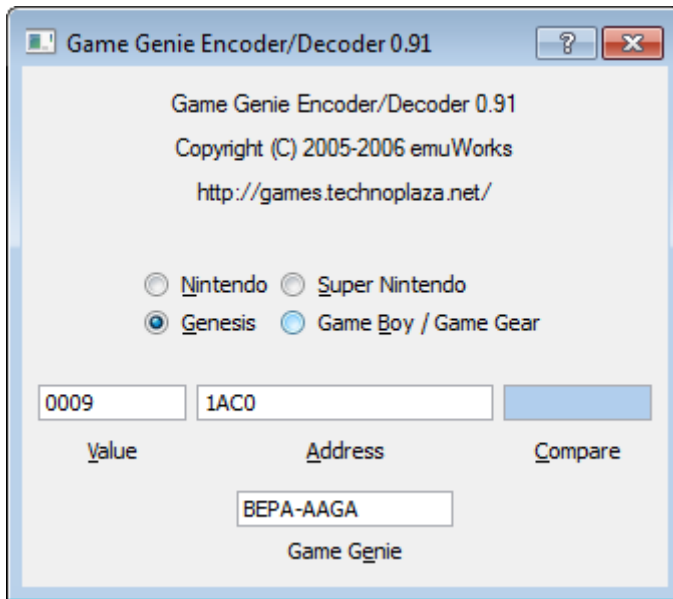
Ya sólo basta con pulsar en "Convert" para obtener dicho fichero.

Ahora que tenemos el fichero .BIN podemos utilizar un código Gamegenie como los que se pueden encontrar en <http://www.gamegenie.com>.

En esta página encontrar una gran cantidad de códigos de diferentes juegos.

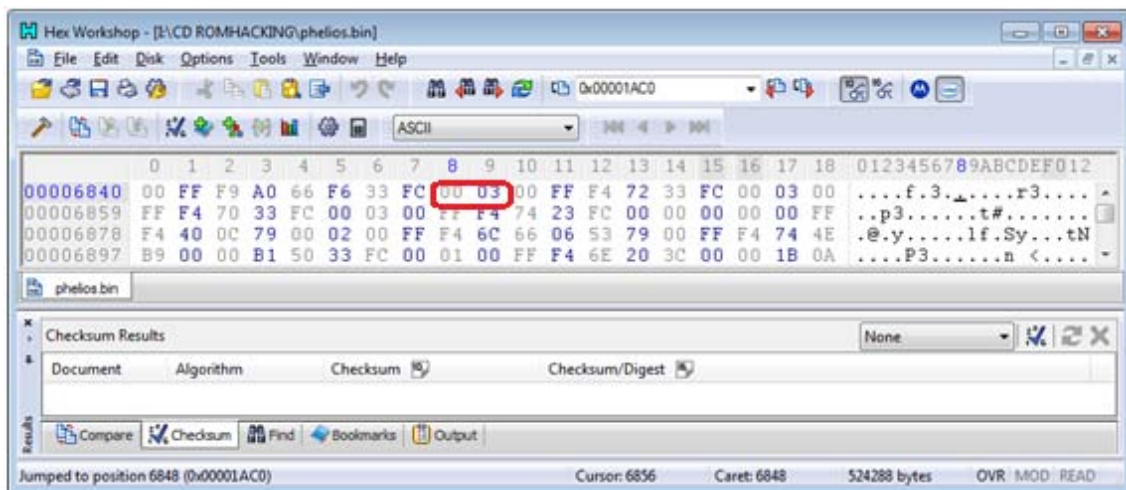
Por ejemplo, el código BEPA-AAGA nos permite tener 9 vidas en el juego.

Podemos ejecutar el programa GGEncoder para convertir el código gamegenie en dirección de la ROM para lo cual seleccionamos Genesis ya que se trata de un código para la Megadrive y lo introducimos en la parte inferior para que nos de la dirección (1AC0, en formato hexadecimal) y el valor (0009) también en este formato.



Con esto ya nos bastaría para poder modificar el juego y tener 9 vidas en lugar de las que tiene originalmente.

Podemos abrir la ROM con el editor hexadecimal y situarnos sobre la posición 1AC0 hexadecimal o 6848 decima; o seleccionando la opción "Goto..." .



Podemos poner el valor 00 09 (en lugar de 00 03) y conseguimos el resultado esperado (tenemos más vidas). Si guardamos la modificación y cargamos el ROM con Wings vemos como si ha surtido efecto.

Con esto ya podría terminar el tutorial ya que hemos conseguido el resultado esperado pero quiero mostrar otros aspectos para intentar comprender a que se debe esto.

Vamos ahora a utilizar otra página que cuenta con información interesante a la hora de conseguir ventajas en juegos. Se trata de www.bsfree.org, donde hay códigos ProAction Replay de Megadrive además de para otras consolas.

También podríamos obtener estos códigos utilizando "Gens Hacking" (una versión modificada del emulador Gens o Wings) que permite la búsqueda de estos códigos.

Estos códigos tiene 2 partes: una primera que corresponde a la dirección y la siguiente que corresponde al valor.

Vidas infinitas: FFF473:0003

Invencibilidad: FFF475:0003

La dirección corresponde a la RAM (memoria donde se guardan valores en la consola) frente a la ROM (Memoria de sólo lectura que es el propio juego y que la consola no puede modificar pero nosotros sí). Esta memoria RAM puede cambiar el valor que contiene en cada dirección que la compone.

Por ejemplo, en la dirección FFF473 al iniciar el juego aparecerá el valor 0003 (tenemos 3 vidas) y cuando perdamos una tendrá el valor 0002.

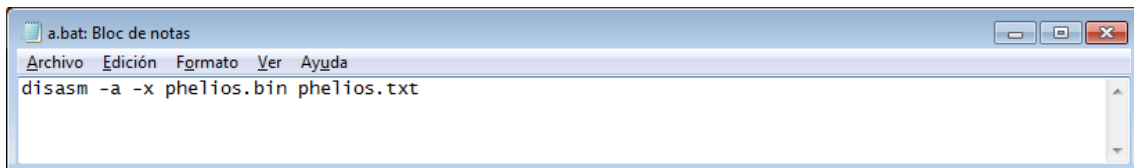
Algunos emuladores permiten introducir estos códigos y se consigue que esta dirección tenga el valor que pongamos de forma perpetua sin afectar a la ROM o juego original.

El código FFF473:0003 (Vidas infinitas) se debe a que en esta dirección siempre aparecerá el valor 0003.

Vamos a tratar por encima un poco de programación de Megadrive para tratar de comprender como funcionan los códigos.

Situamos el programa "Sega Asm" en el mismo directorio que está la ROM (que tiene en mi caso el nombre "Phelios.bin"). Encontraremos un fichero "Disasm.exe" que permite obtener el código fuente del juego.

Creamos un fichero .bat con el siguiente contenido:



```
a.bat: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
disasm -a -x phelios.bin phelios.txt
```

En primer lugar aparecen los parámetros ("-a", "-x") y posteriormente el fichero del juego y del fichero .txt que va a crear con el código fuente.

El fichero ocupa más de 9 megas y contiene bastantes líneas.

Lo abrimos con el "Bloc de notas" de Windows y vamos a buscar el valor FFF472 ya que en este caso se guarda en el juego como un Word (valor de 2 bytes).

El primer resultado que encontramos es el siguiente código:

```
00000B7A 3039 00FFF472      MOVE.W  $00FFF472,D0
00000B80 5340              SUBQ.W  #$1,D0
```

Lo que hace este fragmento de código es poner el valor de la dirección \$00FFF472 en el registro D0 (MOVE.W \$00FFF472,D0) y restarle una unidad (SUBQ.W #\$1,D0).

La W indica que se trata de un Word frente a la B que representaría que se trata de un Byte.

Si cambiamos la siguiente orden por otra tal como:

```
5240              ADDQ.W  #$1,D0
```

Conseguimos que en lugar de disminuir las vidas, éstas aumenten ya que la orden aumenta en una unidad el contenido del registro D0.

El código 5240 es el opcode que representa la orden (ADDQ.W #1,D0) y que aparece en la ROM.

Si nos situamos con el Hex Workshop en la dirección B80 con la ROM abierta y cambiamos el 5340 por 5240 podemos comprobar como se ha conseguido tener vidas infinitas y esta modificación es permanente con lo que podemos ya terminarnos el juego de una forma fácil.

Vamos a continuar con la búsqueda del valor FFF472 en el código fuente con el "Bloc de notas" y encontramos:

```
00001ABE 33FC 0003 00FFF472  MOVE.W  #$0003,$00FFF472
```

```
00001AC6 33FC 0003 00FFF470  MOVE.W  #$0003,$00FFF470
```

```
00001ACE 33FC 0003 00FFF474  MOVE.W  #$0003,$00FFF474
```

Si nos fijamos en lo que habíamos obtenido con el programa GEncoder (teníamos la dirección 1AC0 y el valor 0009 para tener 9 vidas).

El valor 33 corresponde a la dirección 00001ABE, FC a la dirección 00001ABF, 00 a la dirección 00001AC0 y 03 a la dirección 00001AC1.

La primera orden (MOVE.W #\$0003,\$00FFF472) lo que hace es lo siguiente:

Poner el valor \$0003 (Word=2 bytes) en la dirección \$00FFF472=Vidas.

Vimos como se cambiaba el valor \$0003 por \$0009 para tener 9 vidas con lo que la orden sería:

```
00001ABE 33FC 0009 00FFF472  MOVE.W  #$0009,$00FFF472
```

Se guarda el valor \$0009 en la dirección \$00FFF472=Vidas (en la RAM).

Vemos como se ha cambiado la orden y el opcode que la representa.

Antes con 3 vidas el opcode era: 33FC 0003 00FFF472

Después con 9 vidas el opcode es: 33FC 0009 00FFF472

Las siguientes ordenes aunque lo que hacen es poner el valor \$0003 en la dirección \$00FFF470=Número de continues, y el valor \$0003 en la dirección \$00FFF474=Energía.

Cambiando estos valores podemos tener más continues y mayor nivel de energía al inicio del juego. También podríamos buscar donde se disminuyen estos valores y conseguir tener continues y energía infinitos.

Igual que hemos hecho para este juego podríamos hacerlo con cualquier otro de la consola Megadrive.