

Desproteger Monkey Island 2 en 2022

fanta <fanta@56k.es>

RECETA PARA GUSANOS:



MEZCLA 33 MENTA PARA EL ALIENTO
CON 4_ TROCITOS DE QUESO.
AGITAR BIEN.

Sumario

Desproteger Monkey Island 2 en 2022.....	1
Paso 0: Disponer de Dosbox-x.....	2
Paso 1: Obtener los disquetes originales del juego.....	3
Paso 2: Montar los disquetes con dosbox-x e instalar Monkey2.....	4
Paso 3: Desproteger Monkey Island 2.....	8

Hoy es un día de esos en los que **quieres probar como desproteger un juego de MSDOS desde GNU+Linux**. Un día en el que quieres dejarlo documentado pero al final solo dejas notas en un archivo de texto plano.

Y de esas notas estos posts.

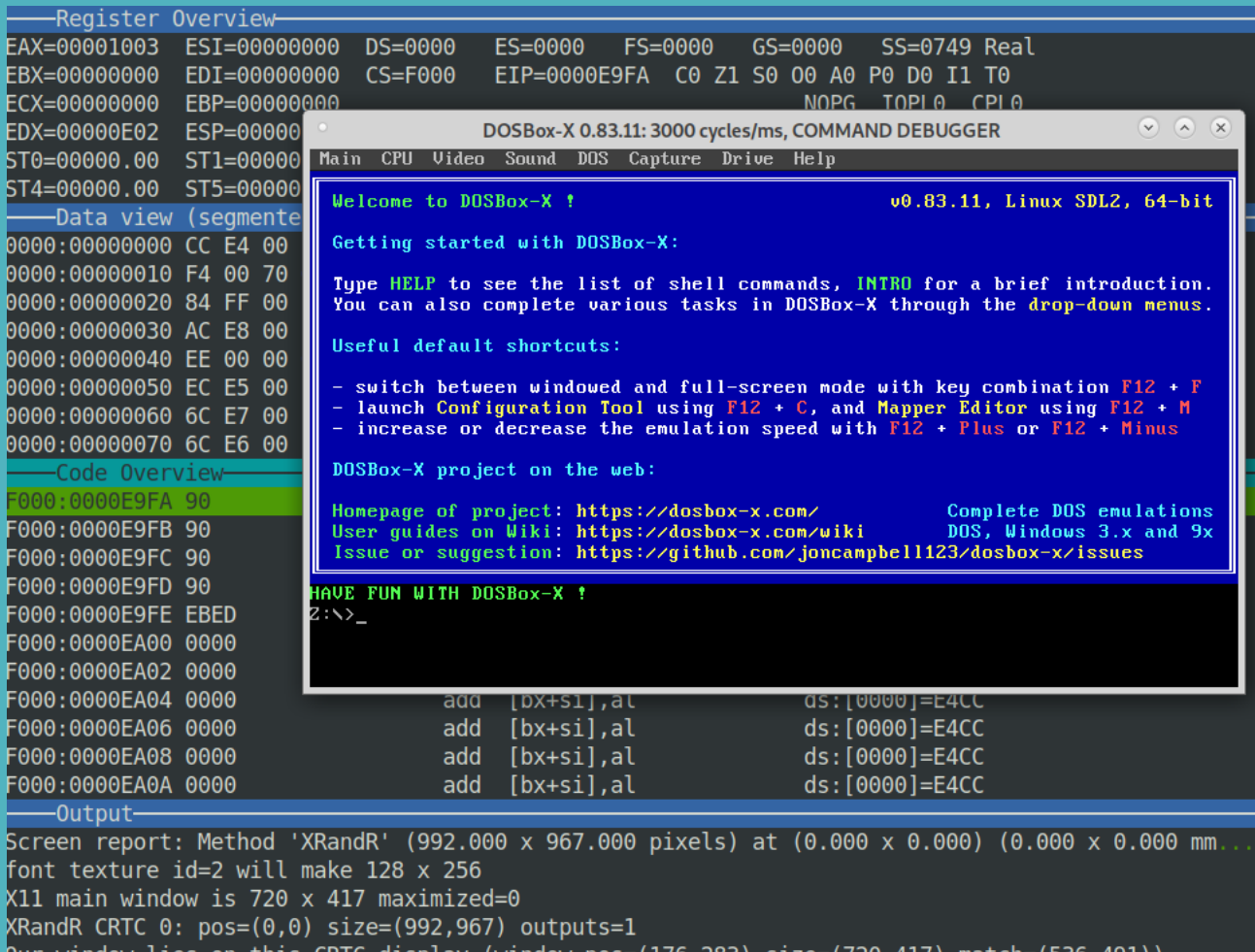
Lo importante no es si al final se alteran 2 bytes o 1 byte. **Lo importante es saber cual cambiar y disfrutar del proceso.**

Paso 0: Disponer de Dosbox-x

Esto se puede hacer compilando dosbox-x en tu distro. Puedes usar este script:

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

El script tendría que funcionar sobre OpenSuse 15.4 Leap, Debian 10, Debian 11, Arch Linux, Ubuntu 20.04.4 y Ubuntu 22.04.1 . Si andas en otra distro mira el script y mira los pasos.



```
Register Overview
EAX=00001003  ESI=00000000  DS=0000  ES=0000  FS=0000  GS=0000  SS=0749  Real
EBX=00000000  EDI=00000000  CS=F000  EIP=0000E9FA  C0 Z1 S0 00 A0 P0 D0 I1 T0
ECX=00000000  EBP=00000000                                NOPG  TOPL 0  CPL 0
EDX=00000E02  ESP=00000000
ST0=000000.00  ST1=000000.00
ST4=000000.00  ST5=000000.00

Data view (segmente)
0000:00000000  CC E4 00
0000:00000010  F4 00 70
0000:00000020  84 FF 00
0000:00000030  AC E8 00
0000:00000040  EE 00 00
0000:00000050  EC E5 00
0000:00000060  6C E7 00
0000:00000070  6C E6 00

Code Overview
F000:0000E9FA  90
F000:0000E9FB  90
F000:0000E9FC  90
F000:0000E9FD  90
F000:0000E9FE  EBED
F000:0000EA00  0000
F000:0000EA02  0000
F000:0000EA04  0000
F000:0000EA06  0000
F000:0000EA08  0000
F000:0000EA0A  0000
                                add [bx+si],al          ds:[0000]=E4CC
                                add [bx+si],al          ds:[0000]=E4CC
                                add [bx+si],al          ds:[0000]=E4CC
                                add [bx+si],al          ds:[0000]=E4CC

Output
Screen report: Method 'XRandR' (992.000 x 967.000 pixels) at (0.000 x 0.000) (0.000 x 0.000 mm...
font texture id=2 will make 128 x 256
X11 main window is 720 x 417 maximized=0
XRandR CRTC 0: pos=(0,0) size=(992,967) outputs=1
Our window lies on this CRTC display (window pos (176,282) size (720,417) match (526,401))

COMMAND DEBUGGER
v0.83.11, Linux SDL2, 64-bit
Getting started with DOSBox-X:
Type HELP to see the list of shell commands, INTRO for a brief introduction.
You can also complete various tasks in DOSBox-X through the drop-down menus.
Useful default shortcuts:
- switch between windowed and full-screen mode with key combination F12 + F
- launch Configuration Tool using F12 + C, and Mapper Editor using F12 + M
- increase or decrease the emulation speed with F12 + Plus or F12 + Minus
DOSBox-X project on the web:
Homepage of project: https://dosbox-x.com/          Complete DOS emulations
User guides on Wiki: https://dosbox-x.com/wiki      DOS, Windows 3.x and 9x
Issue or suggestion: https://github.com/joncampbell123/dosbox-x/issues
HAVE FUN WITH DOSBox-X !
Z:\>_
```

De todos modos **el proceso sería algo así** como cubrir las dependencias, clonar repo y compilar:

```
$ d="/tmp/dosbox-x"
$ sudo apt update
# apt install automake git gcc g++ make libncurses-dev nasm libSDL-net1.2-dev
libSDL2-net-dev libpcap-dev fluidsynth libfluidsynth-dev libavdevice58
libavformat-dev libavcodec-dev libavcodec-extra libavcodec-extra58 libswscale-
dev libfreetype6-dev libxkbfile-dev libxrandr-dev -y
$ git clone "https://github.com/joncampbell123/dosbox-x" $d
$ cd $d
$ bash build-debug-sdl2
$ sudo make install
```

Paso 1: Obtener los disquetes originales del juego

Puedes obtenerlos desde aquí en ENGLISH y en SPANISH así:

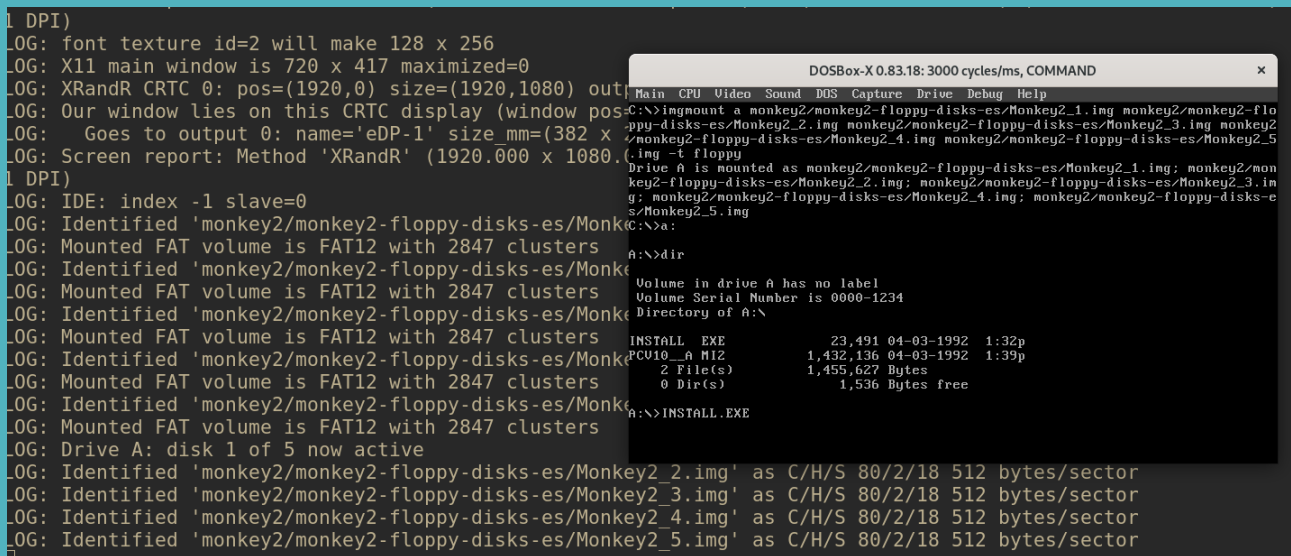
```
$ wget -q "http://fanta.56k.es/games/1990/1991-Monkey_Island_2-LeChucks_Revenge-Spanish-Scummvm/Monkey_island_2-en_and_es-disks/monkey2.tar.gz" -O - | tar xvz
```

```
[fanta@terminator juegos]$ tar xfvz monkey2.tar.gz
monkey2/
monkey2/monkey2-floppy-disks-en/
monkey2/monkey2-floppy-disks-en/Monkey2_1.img
monkey2/monkey2-floppy-disks-en/Monkey2_4.img
monkey2/monkey2-floppy-disks-en/Monkey2_3.img
monkey2/monkey2-floppy-disks-en/Monkey2_5.img
monkey2/monkey2-floppy-disks-en/Monkey2_2.img
monkey2/monkey2-floppy-disks-es/
monkey2/monkey2-floppy-disks-es/Monkey2_1.img
monkey2/monkey2-floppy-disks-es/Monkey2_4.img
monkey2/monkey2-floppy-disks-es/Monkey2_3.img
monkey2/monkey2-floppy-disks-es/Monkey2_5.img
monkey2/monkey2-floppy-disks-es/Monkey2_2.img
[fanta@terminator juegos]$ █
```

Paso 2: Montar los disquetes con dosbox-x e instalar Monkey2

Básicamente podemos hacerlo así:

```
$ mkdir c
$ dosbox-x -c "keyb sp" -c "mount c c" -c "c:" -c "cls" -c "imgmount a
monkey2/monkey2-floppy-disks-es/Monkey2_1.img
monkey2/monkey2-floppy-disks-es/Monkey2_2.img
monkey2/monkey2-floppy-disks-es/Monkey2_3.img
monkey2/monkey2-floppy-disks-es/Monkey2_4.img
monkey2/monkey2-floppy-disks-es/Monkey2_5.img -t floppy" -no-console
```



```
l DPI)
LOG: font texture id=2 will make 128 x 256
LOG: X11 main window is 720 x 417 maximized=0
LOG: XRandR CRT0: pos=(1920,0) size=(1920,1080) out
LOG: Our window lies on this CRT0 display (window pos
LOG: Goes to output 0: name='eDP-1' size_mm=(382 x
LOG: Screen report: Method 'XRandR' (1920.000 x 1080.
l DPI)
LOG: IDE: index -1 slave=0
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monk
LOG: Mounted FAT volume is FAT12 with 2847 clusters
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monk
LOG: Mounted FAT volume is FAT12 with 2847 clusters
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monk
LOG: Mounted FAT volume is FAT12 with 2847 clusters
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monk
LOG: Mounted FAT volume is FAT12 with 2847 clusters
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monk
LOG: Mounted FAT volume is FAT12 with 2847 clusters
LOG: Drive A: disk 1 of 5 now active
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monkey2_2.img' as C/H/S 80/2/18 512 bytes/sector
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monkey2_3.img' as C/H/S 80/2/18 512 bytes/sector
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monkey2_4.img' as C/H/S 80/2/18 512 bytes/sector
LOG: Identified 'monkey2/monkey2-floppy-disks-es/Monkey2_5.img' as C/H/S 80/2/18 512 bytes/sector
```

Abriré una ventana de dosbox-x en la que por defecto apareceremos en C: pero con el disco 1 en la unidad A:

Vamos a movernos por MSDOS para empezar con la instalación así:

```
A:
DIR
INSTALL.EXE
```

Programa de instalación para Monkey Island 2: LeChuck's Revenge
TM & (c) 1991 LucasArts Entertainment Company. All Rights Reserved.

Disco duro para instalar el programa (cursores) C:

Programa de instalación para Monkey Island 2: LeChuck's Revenge
TM & (c) 1991 LucasArts Entertainment Company. All Rights Reserved.

Espacio disponible en el disco: 1966080 k
Espacio necesario para instalar: 9083 k

Leyendo el fichero A:\pcv10__A.mi2

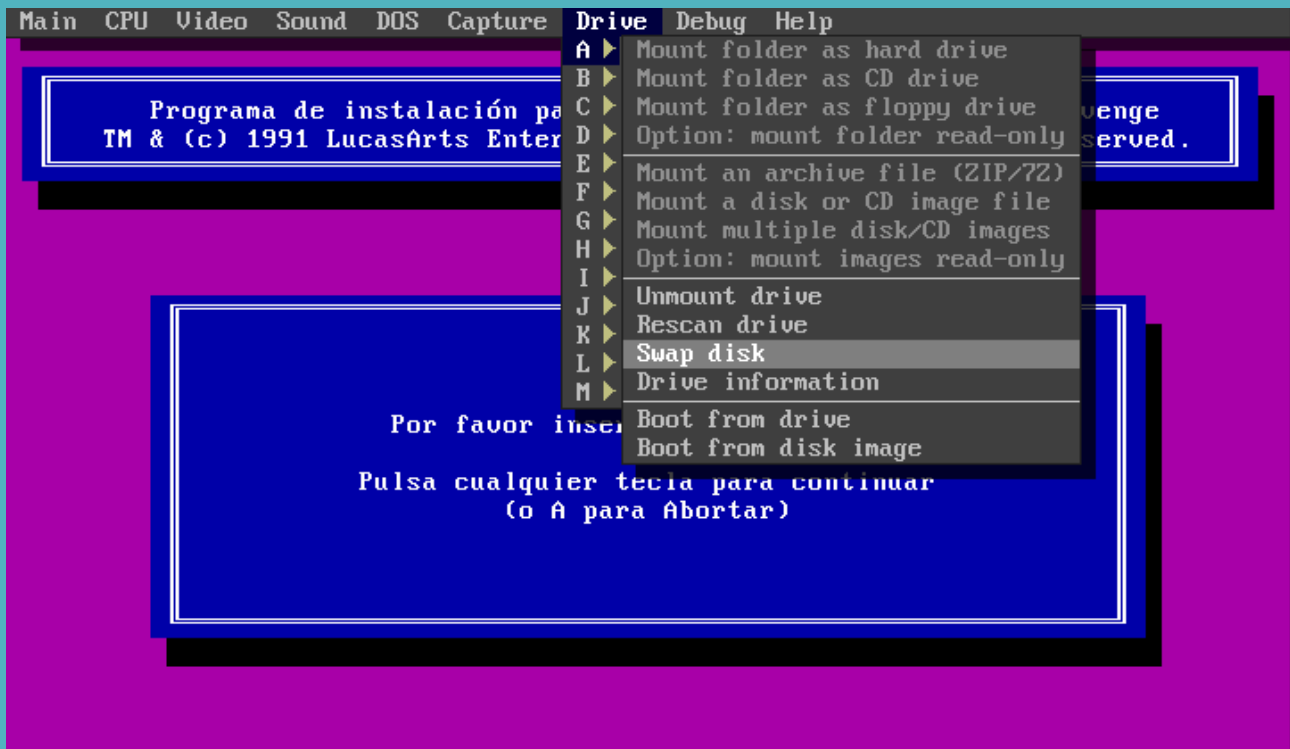
Extrayendo el fichero MONKEY2.001

Comenzará la instalación y en algún momento nos solicitará el disquete 2, el 3, etc ... hasta el 5.

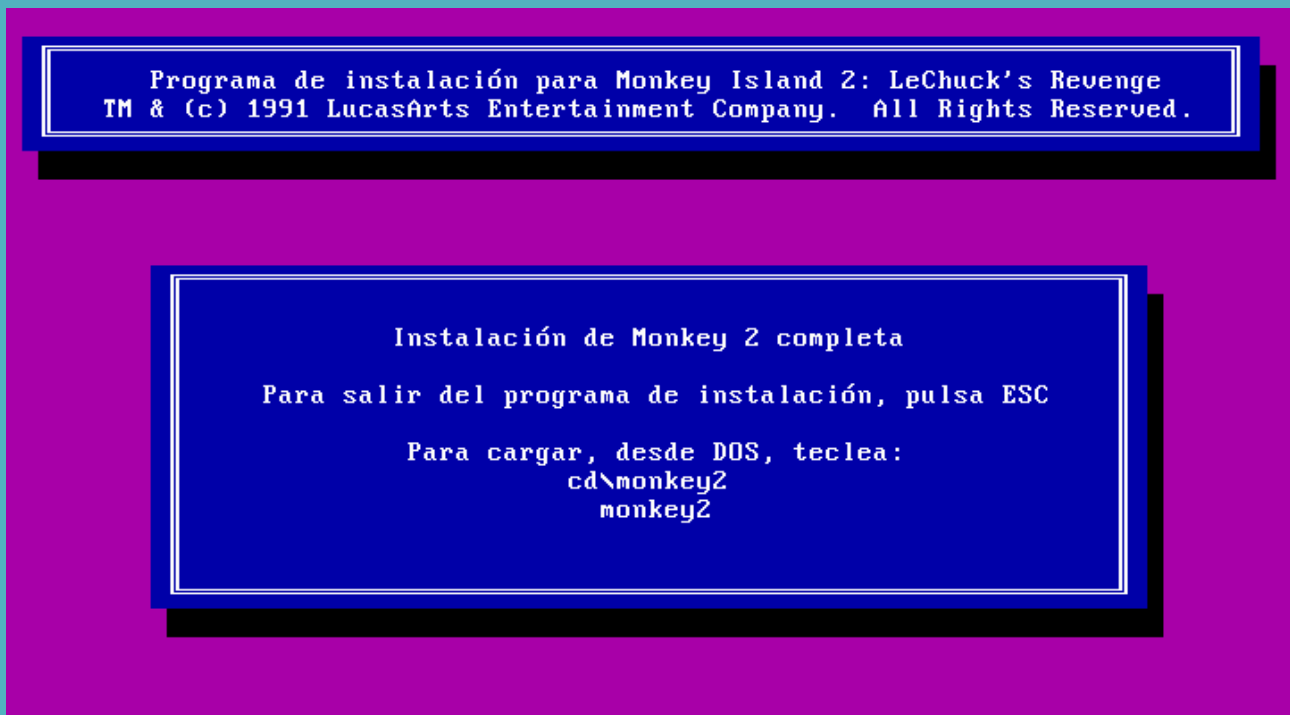
Programa de instalación para Monkey Island 2: LeChuck's Revenge
TM & (c) 1991 LucasArts Entertainment Company. All Rights Reserved.

Por favor inserta el disco No.2
Pulsa cualquier tecla para continuar
(o A para Abortar)

Es entonces cuando en el menú de dosbox-x vamos a cambiar el disquete actual por el siguiente. Eso se hace pinchando en Drive — A — Swap disk una vez. **Al darle cambia el disquete por el siguiente.**



Seguiremos presionando cualquier tecla y tendría que seguir copiando archivos. Hacemos lo mismo con todos los disquetes **hasta terminar la instalación**.



Ya podemos salir de dosbox-x si queremos o podemos probar a ejecutar el juego escribiendo lo siguiente:

```
CD C:/MONKEY2  
MONKEY2.EXE
```

```
C:\MONKEY2>cd c:/monkey2  
C:\MONKEY2>MONKEY2.EXE
```



**PULSA "ENTER" PARA COMENZAR CON LA
PROTECCION.**

Veremos que el juego tiene protección. De modo que cerramos dosbox-x y **ya tenemos que tener en el directorio «c» el juego instalado.**

```
[fanta@terminator juegos]$ ls -la c/MONKEY2/
total 9112
drwxr-xr-x 2 fanta fanta    4096 nov  4 19:54 .
drwxr-xr-x 3 fanta fanta    4096 nov  4 19:46 ..
-rw-r--r-- 1 fanta fanta  20624 nov  4 19:54 ADLIB.IMS
-rw-r--r-- 1 fanta fanta  11135 nov  4 19:54 MONKEY2.000
-rw-r--r-- 1 fanta fanta 9093581 nov  4 19:54 MONKEY2.001
-rw-r--r-- 1 fanta fanta  110811 nov  4 19:54 MONKEY2.EXE
-rw-r--r-- 1 fanta fanta   18976 nov  4 19:54 ROLAND.IMS
-rw-r--r-- 1 fanta fanta   24808 nov  4 19:54 SOUNBLAS.IMS
-rw-r--r-- 1 fanta fanta   20062 nov  4 19:54 SPEAKER.IMS
[fanta@terminator juegos]$ █
```

Paso 3: Desproteger Monkey Island 2

Buscamos la siguiente cadena «**6F 6B 83 68 4B**» dentro del archivo más gordo «MONKEY2.001»

```
$ cat c/MONKEY2/MONKEY2.001 | xxd -u -c 16 -g 1 | grep -i "6F 6B 83 68 4B"
```

```
[fanta@terminator juegos]$ cat c/MONKEY2/MONKEY2.001 | xxd -u -c 16 -g 1 | grep -i "6F 6B 83 68 4B"
00875890: 7D 96 66 49 69 F3 83 68 6A 29 E1 6F 6B 83 68 4B  }.fIi..hj).okokK
[fanta@terminator juegos]$ █
```

Vamos a cambiar «**83 68**» de lo buscado por «**6F 6B**» de modo que quedaría así: «**6F 6B 6F 6B 4B**»

```
$ printf "0087589D: 6F" | xxd -r4 - c/MONKEY2/MONKEY2.001
$ cat c/MONKEY2/MONKEY2.001 | xxd -u -c 16 -g 1 | grep -i "6F 6B 6F 68 4B"
$ printf "0087589E: 6B" | xxd -r4 - c/MONKEY2/MONKEY2.001
$ cat c/MONKEY2/MONKEY2.001 | xxd -u -c 16 -g 1 | grep -i "6F 6B 6F 6B 4B"
```

```
[fanta@terminator juegos]$ cat c/MONKEY2/MONKEY2.001 | xxd -u -c 16 -g 1 | grep -i "6F 6B 6F 6B 4B"
00875890: 7D 96 66 49 69 F3 83 68 6A 29 E1 6F 6B 6F 6B 4B  }.fIi..hj).okokK
[fanta@terminator juegos]$ █
```

Ya hemos desprotegido el juego. Así de simple

Puedes probarlo así:

```
$ dosbox-x -c "keyb sp" -c "MOUNT C c" -c "C:" -c "CLS" -c "C:" -c "CD MONKEY2"
-c "MONKEY2.EXE"
```


Escribes cualquier número y será valido.

RECETA PARA GUSANOS:



**MEZCLA 33 MENTA PARA EL ALIENTO
CON 4_ TROCITOS DE QUESO.
AGITAR BIEN.**

ESCOGE UNO:

MONKEY ISLAND 2

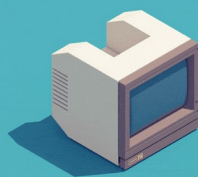
**"¡LO QUIERO TODO! ¡TODOS LOS
ENIGMAS! ¡TODO EL TRABAJO!"**

MONKEY 2 LIGHT

**"NUNCA HE JUGADO UN
JUEGO DE AVENTURAS ANTES.
TENGO MIEDO."**



Disfruta amigo/a/e.



[TWITCH](#) [PEERTUBE](#) [FEDIVERSE](#) [YOUTUBE](#) [TWITTER](#)