

# PRESERVING ARCADE GAMES

ANGE ALBERTINI

31C3



```

static MACHINE_CONFIG_START( tokiu, bublbobl_state )

    /* basic machine hardware */
    MCFG_CPU_ADD("maincpu", Z80, MAIN_XTAL/4) // 6 MHz
    MCFG_CPU_PROGRAM_MAP(tokio_map)
    MCFG_CPU_VBLANK_INT_DRIVER("screen", bublbobl_state, irq0_line_hold)

    MCFG_CPU_ADD("slave", Z80, MAIN_XTAL/4) // 6 MHz
    MCFG_CPU_PROGRAM_MAP(tokio_slave_map)
    MCFG_CPU_VBLANK_INT_DRIVER("screen", bublbobl_state, irq0_line_hold)

    MCFG_CPU_ADD("audiocpu", Z80, MAIN_XTAL/8) // 3 MHz
    MCFG_CPU_PROGRAM_MAP(tokio_sound_map)

    MCFG_QUANTUM_TIME(attotime::from_hz(6000))

    MCFG_MACHINE_START_OVERRIDE(bublbobl_state,tokio)
    MCFG_MACHINE_RESET_OVERRIDE(bublbobl_state,tokio)

    /* video hardware */
    MCFG_SCREEN_ADD("screen", RASTER)
    MCFG_SCREEN_RAW_PARAMS(MAIN_XTAL/4, 384, 0, 256, 264, 16, 240)
    MCFG_SCREEN_UPDATE_DRIVER(bublbobl_state, screen_update_bublbobl)

    MCFG_GFXDECODE(bublbobl)
    MCFG_PALETTE_LENGTH(256)

    /* sound hardware */
    MCFG_SPEAKER_STANDARD_MONO("mono")

    MCFG_SOUND_ADD("ymsnd", YM2203, MAIN_XTAL/8)
    MCFG_SOUND_CONFIG(y2203_config)
    MCFG_SOUND_ROUTE(0, "mono", 0.08)
    MCFG_SOUND_ROUTE(1, "mono", 0.08)
    MCFG_SOUND_ROUTE(2, "mono", 0.08)
    MCFG_SOUND_ROUTE(3, "mono", 1.0)
MACHINE_CONFIG_END

```

not everyone understands software

1UP  
34760

HIGH SCORE  
34760

INSERT  
COIN

3

but everyone understand that it's a (good) game!



# HACKING

# EMULATION

# GAMES

that's the cool part of emulation:  
it brings games to everyone !  
(games that might be lost forever)



This talk is about arcade games, the games where you put money to play. That money would go in the operator's pocket, no share to the arcade manufacturer. To be successful, they had to be awesome. "Dedicated" (hardware, controls...) is the key to their success.

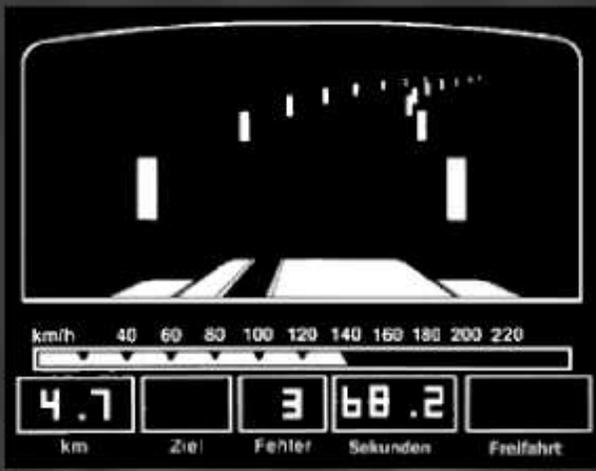


YOUR SCORE 006 TOP SPEED 091  
TIME 035

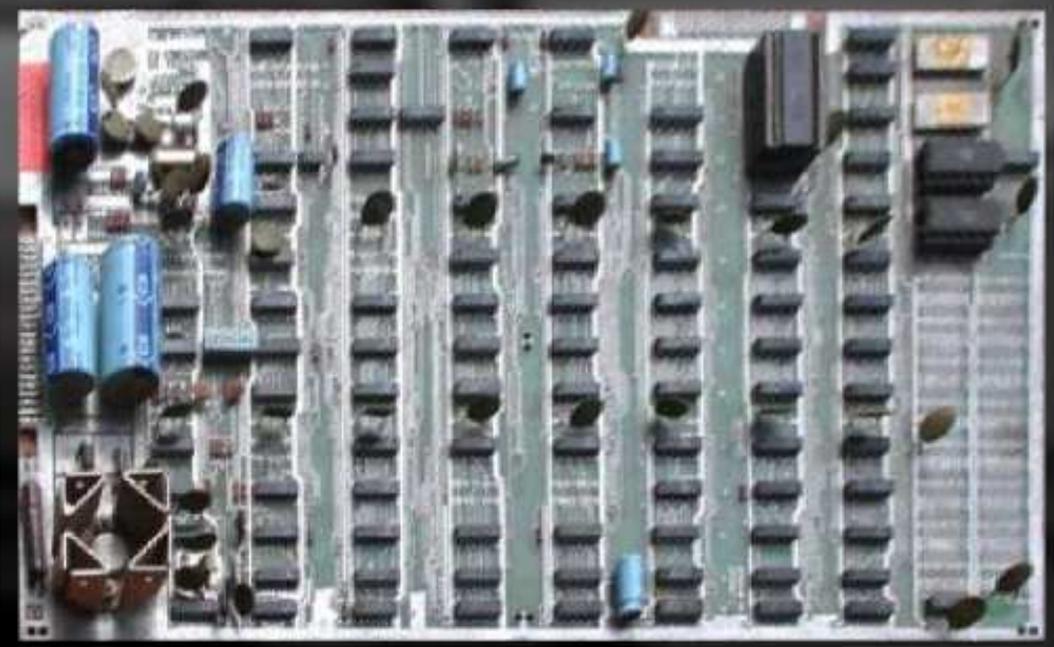
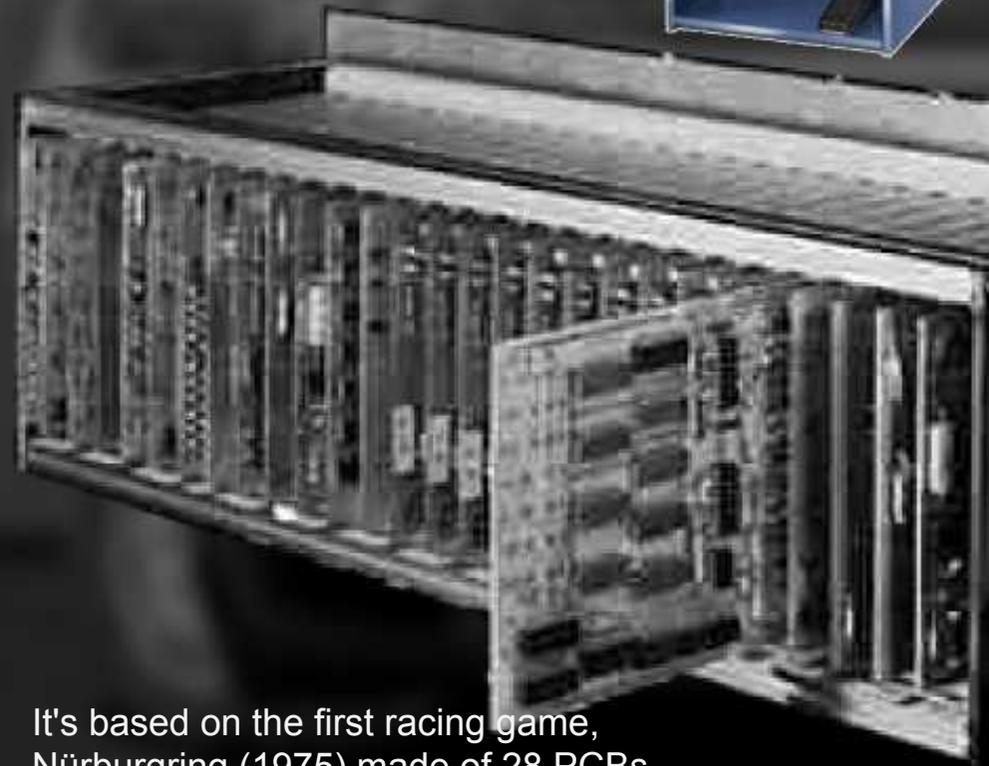
Let's go back in time:  
This is Night Driver (Atari 1976)...



# Nürburgring



# NIGHT DRIVER



It's based on the first racing game, Nürburgring (1975) made of 28 PCBs.



Berzerk was one of the first game with digitized speech.  
It cost 1000 USD / word to be digitized  
(it contained 16 words!)

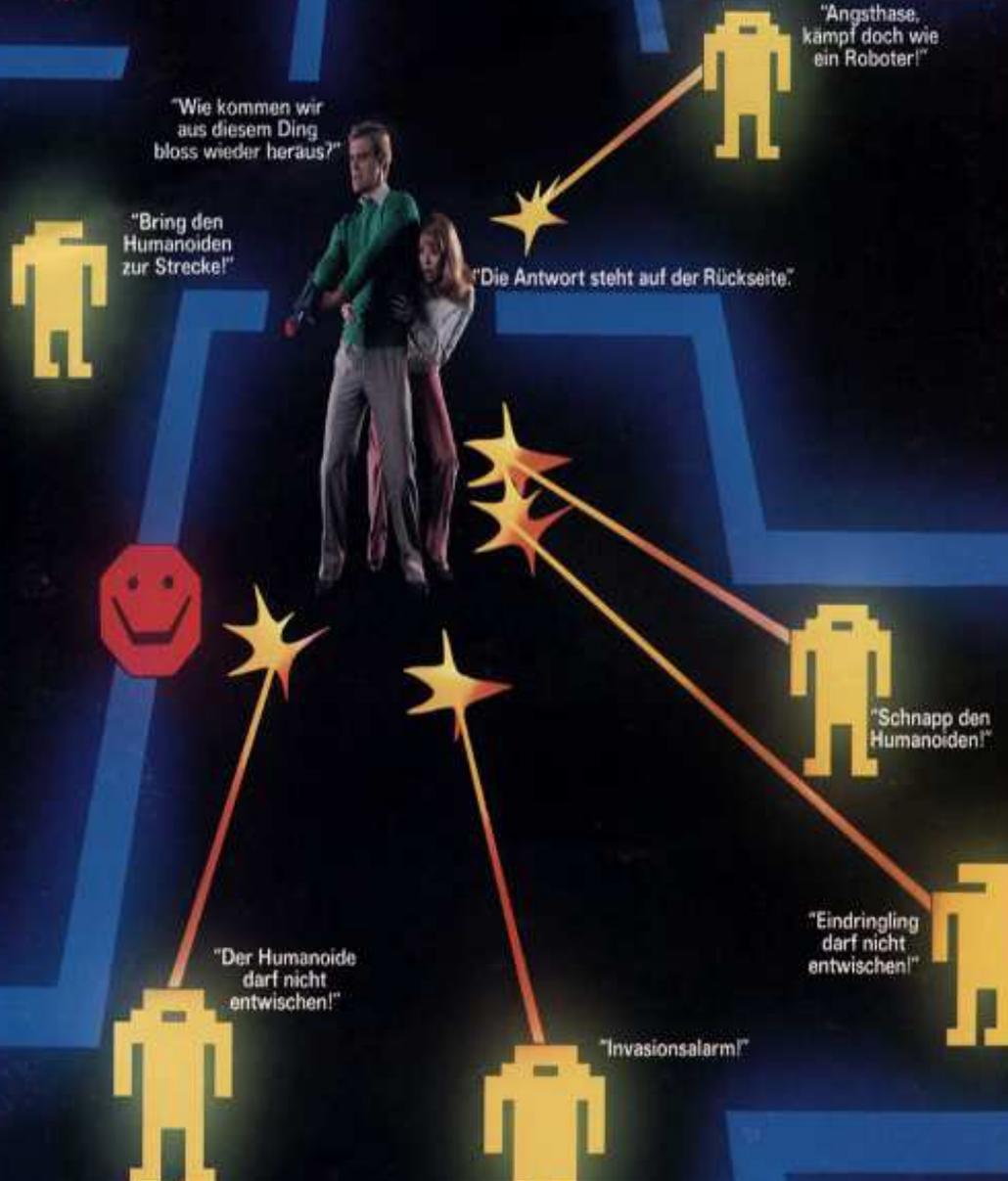
1. Object of game is to shoot as many Robots as possible and escape from room.
2. Player is controlled by control stick and can move in eight directions.
3. Aim with control stick and shoot with either FIRE button.
4. Robots are worth 50 points. Bonus Score for destroying all Robots (even if Robots destroy each other).
5. EVIL OTTO comes out from anytime player started, cannot be destroyed, will go thru walls, and follows player with its object to destroy the player.
6. Extras for score of 5,000.

130-1100

DESIGNED AND PROGRAMMED BY:

*Alan McNa*

# STERN GEHT BERZERK!



"Wie kommen wir aus diesem Ding bloss wieder heraus?"

"Bring den Humanoiden zur Strecke!"

"Die Antwort steht auf der Rückseite."

"Angsthasen kämpfen doch wie ein Roboter!"

"Schnapp den Humanoiden!"

"Der Humanoide darf nicht entweichen!"

"Eindringling darf nicht entweichen!"

"Invasionsalarm!"

...they also made a german version ! same price per word ? ;)

# STERN GEHT BERZERK!

Wenn Sie glauben, dass wir bei der Entwicklung von Berzerk aus dem Häuschen geraten sind, dann haben Sie recht! Wir haben hier erstmals unsere gesamte Technologie und all unser Wissen in ein einzelnes Videospiel gesteckt. Das Ergebnis ist ein Video-Meisterwerk, das nicht nur die Spieler absolut ausser Rand und Band geraten lässt, sondern das auch die Gewinne direkt zu den Operatoren treibt.

## AUFZÄHLUNG INNOVATIVER BESONDERHEITEN VON BERZERK

- Unübertroffener Wortschatz von 30 Wörtern lässt das Spiel zum Spieler Nachrichtenverkehr unterhalten.
- 64.000 beliebig angeordnete Modellvorlagen erscheinen in labyrinthischer Gestaltung für explosive, sich nicht wiederholende Action auf der Video-Platte.
- Ein vor kurzem entworfener Daumenhebel ermöglicht es dem Spieler, das Bild des Humanoiden in 8 verschiedene Richtungen zu bewegen.
- Nach Spielende erscheinen die bis dato erzielten 10 höchsten Punktgewinne auf dem Bildschirm.
- Selbst bei ausgeschaltetem Gerät speichert die bis dato erzielten 5 höchsten Punktgewinne.
- Betriebsart "Anziehung" lockt Spieler mit der zeitlich programmierten Durchsage an: "Münzen in der Tasche entdeckt".
- Alle logischen Tafeln sind in leicht zugänglichem Ausziehfach im Vordergehäuse untergebracht, was mühelose Wartung gewährleistet.
- Hochentwickeltes automatisches Diagnoseprogramm.



## SPIELEIGENSCHAFTEN



Roboter verfolgen Humanoiden (Spieler) durch eine der 64.000 möglichen Modellvorlagen.



Humanoid vermeidet Roboter durch gekonnte Betätigung des Daumenhebels, und er vernichtet sie durch Feuerung seiner Geschosse.



Der "böse Otto", eine unzerstörbare Macht, erscheint aufs Geratewohl am Bildschirm, um den Humanoiden zu verfolgen und zu vernichten. Er muss um jeden Preis vermieden werden!

NEUER

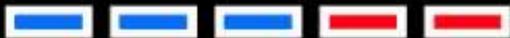
"Dieses Spiel hat wirklich jeden vom Stuhl! Auch Sie!"



Battlezone, the first FPS, in 1980...

**INSTRUCTIONS**

- INSERT COINS
- PRESS START
- YOU LOSE A TANK EACH TIME YOU ARE HIT



**TANK**



1000 POINTS

**MISSILE**



2000 POINTS

**SUPER TANK**



3000 POINTS

**SAUCER**



5000 POINTS

**STRATEGY**

- USE THE **RADAR**
- KEEP MOVING - DON'T STAY IN PLACE OR YOU WILL BE HIT
- USE THE CUBES AND PYRAMIDS AS SHIELDS
- LISTEN FOR THE ENEMY'S TANK SHOTS





...was turned into a military trainer.



Dragon's Lair, an 'interactive' cartoon in 1983, at a time where HDs were 10 Mb and graphics in 16 colors.

# DRAGON'S LAIR



...was using the very recent Laser Disc technology (from 1981).  
But LD drives were quickly worn out, because of frequent scene skipping.

**TIME** 33

**SCORE**

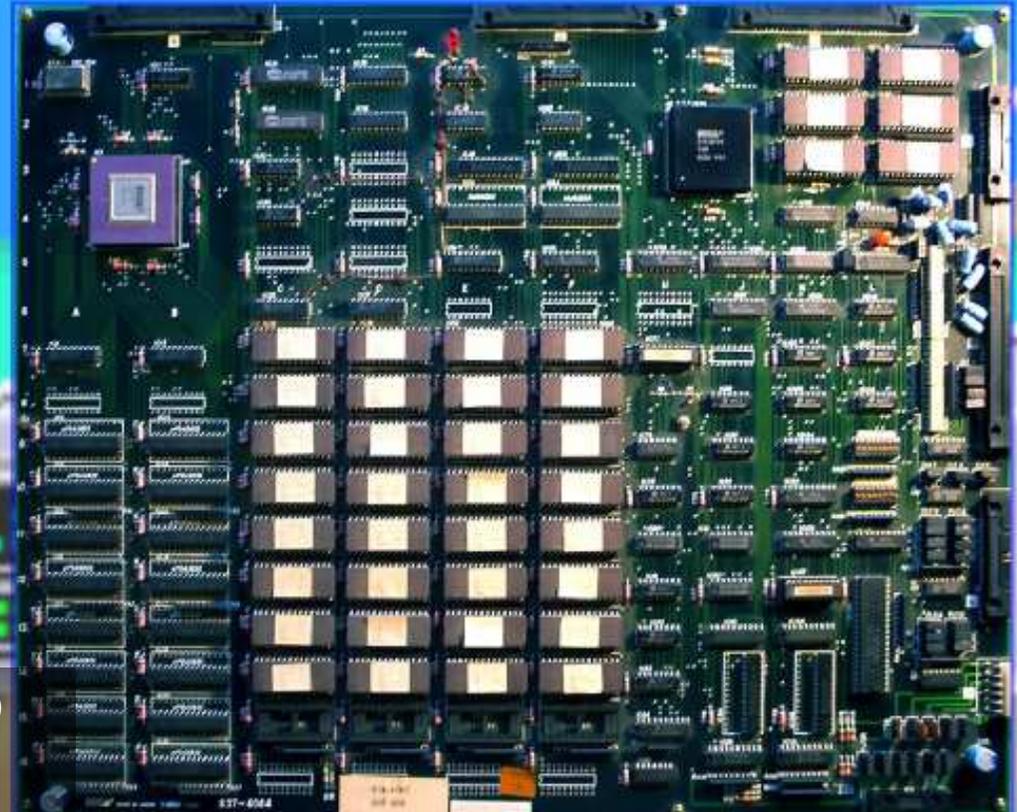
361940

**LAP**

0'40"95

Outrun (Sega 1986), awesome racing game!





...uses 2 main CPUs at 10 Mhz (an Amiga 500 runs at 7 Mhz)  
the 2nd CPU's only task is to display the roads.  
(they're drawn at 30 FPS \*only\*, the rest of the game at 60)



0:35

SCORE 7694
LAP TIME 0:54:08
BEAT 1:38:00 TO CHALLENGE

 RPM
 TMP

RPM

X1000

MPH

0 20 40 60 80 100 120 140

 OIL
 GAS

FUEL
OIL
RMP
TEMP
BELT
HZRD

AUTO


Hard Drivin (1989), a 3d simulation way before modern GPUs existed...

Atari Games presents...

# Hard Drivin'

the world's first driving simulation game!



...used 3 PCBs.

They made a triple screen version of the sequel:

6 PCBs, 4 CPUs, 9 DSPs !!!!

It's emulated since last month (November 14) !



Sometimes, it was the arcade cabinet that was awesome. Hang gliding, bike, car... ass poking ?!?

# R360



Sega's R360 rotates the player on all axis, even upside down !



Sometimes, the screen was the awesome part: almost half spherical...



triple CRT screen (with mirrors) or double widescreen...



...and with awesome games came awesome piracy!

SPACE INVADERS

SRD MISSION

BLOODBROS™

ARCADIA

DONKEY KONG

BOMB JACK TWIN

PLUM POP

CAVEMAN

GYRUSS

POLE POSITION

XAVIUS

奇々怪界

Shock TROOPERS 2nd Squad

THE KING OF FIGHTERS 2002

PHOENIX

BUBBLE BOBBLE

Final Fight

THE KING OF FIGHTERS 2001

MR. DRILLER

BIG STRIKER

METAL SLUG 3™

PPS

As long as a game was good enough and its hardware not too extreme, bootlegs would be made. A few of them were 'creative'.

EARTH  
VADER

FX

WEST STORY

RAPID  
HERO

CRAZY

WONK

VENUS

ATOM



XAVIS

BATTLES



STONE  
ANGLE



NEXT  
PHASE

VANTAGE

CONDOR

GRIFFON

KNIGHT BOY

ようへい  
LANQUENET

SNK  
PLAYMORE

©SNK PLAYMORE 2005 WINTER

Super  
BUBBLE  
BUBBLE

Finch  
GRASSH

臥虎藏龍  
CROUCHING TIGER  
HIDDEN DRAGON  
SUPER PLUS

FENIX

Mr.  
Dig

BEST  
LEAGUE

METAL  
SLUG 6

Space Invaders (text) <-> Darth Vader (gfx)

Metal Slug 3 <-> Metal Slug 6 (!!)

SOOBY KIDS



They went further and were taking a good game, then hacking gfx & sound to create a 'new' game

18066 MONSTERS WORLD  
STAGE 500000



With awesome piracy came awesome protections. once again, dedicated stuff, sometimes tightly integrated with the game internals



In Bee Storm, if the protected CPU is missing, the game works, but the enemies don't shoot anymore.

**TOP** 1000000

**TIME**

**SCORE**

STAGE 1

36

SPE

TOP 1000000 TIME SCORE 988990  
STAGE 1 50 SPEED 278KM



In Hang-on, if the 2nd CPU (sometimes encrypted) is missing, then roads are straight.

1UP

0

HI

1000

TIME 2'54"



P 0

1UP

0

HI

1000

TIME 2'54"

0 2UP

P 0

GAME OVER

STAGE 5

POWER



CREDIT 00



POWER

GAME OVER

STAGE 5



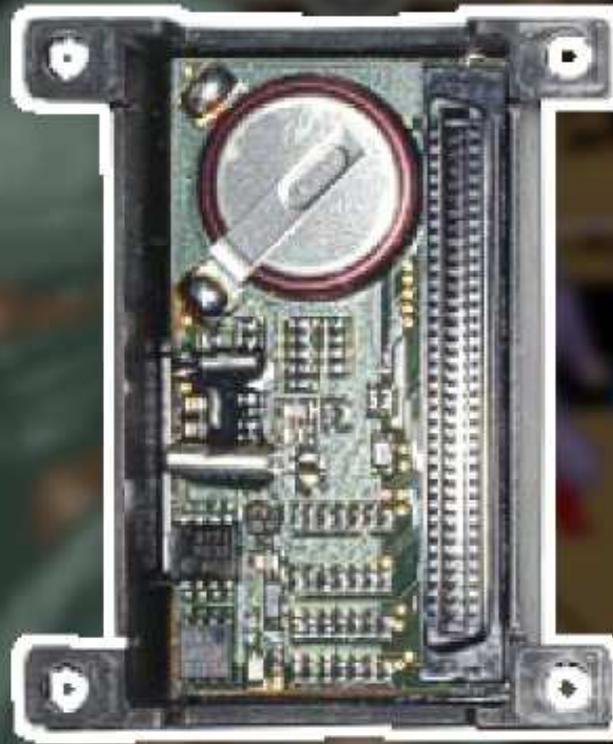
CREDIT 00

00



POWER

in S.P.Y., collisions are handled by a custom chip: without it, you can't hurt and cannot be hurt.



to store protected data, they went further:  
 store data on battery-powered RAM.  
 the battery dies, the game dies.  
 the manual doesn't even mention it!  
 the warranty is void if you open the game's case!



so you're not supposed to open the game, yet all games will eventually die once all batteries are empty. Hacking these games is the only way to preserve them.

SONY

PS4 GAMES & SYSTEMS SIGN IN & CONNECT INSIDE PLAYSTATION® GET HELP Looking for something? 🔍

# Super Street Fighter® II Turbo HD Remix

Buy Download Download Price: \$9.99

Platform: PS3™ Genre: Fighting, Head-to-Head Fighting Out Now



★★★★★

Nintendo Wii U Wii mini Nintendo 3DS Support Search 🔍

# NINJA MASTER'S



Virtual Console Classic Games for Wii

System	Wii
Release Date	1996
No. of Players	2 players simultaneous
Category	Action
Publisher	D4 Enterprise
Wii Points:	900



## Darkstalkers® Resurrection

Capcom U.S.A., Inc.

PSN Game | Released Mar 12, 2013 | ★★★★★ 636 Ratings

\$14.99

Add to Cart

Try Free Demo

Playable On:

PS3

[Click Here to Learn How](#)



Xbox One Xbox 360 Xbox Live Gold Games Entertainment Support

# Marvel vs. Capcom: Origins

Buy Game \$14.99

10 LEVEL 130/150

Chain Reaction ★5 Perform 750 combos of at least 3 hits. 293/750

Fully Charged ★★★ Perform 100 charged moves. 77/100

NEW HERO WAR MACHINE NEW HERO ROLL

JIN MORRIGAN

2 HIT

Images (1 of 10) Overview (2)

it also enables the IP to be re-used commercially later.

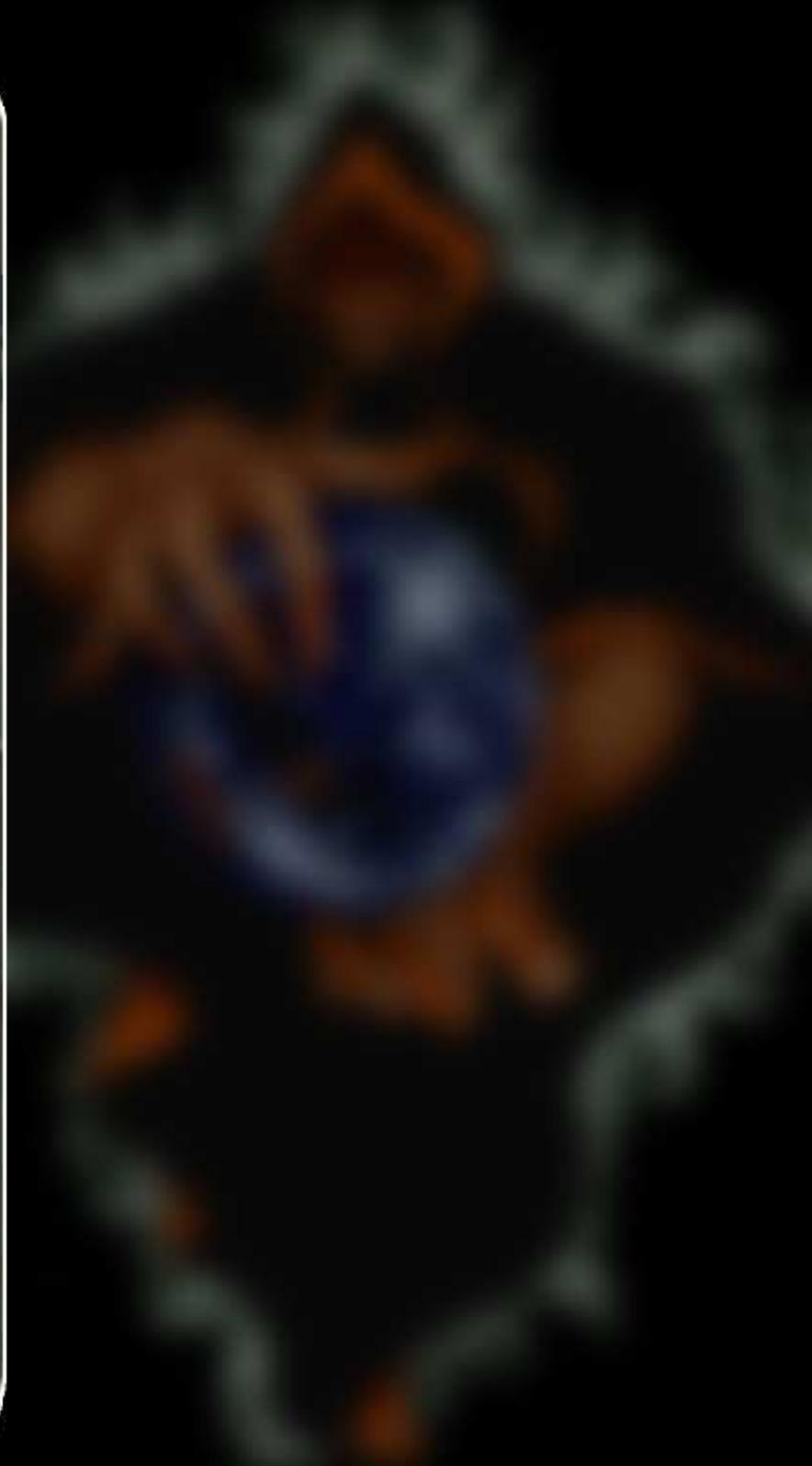
**DEDICATED**

**PIRATED**

**PROTECTED**

**VULNERABLE**

Arcade games had to be awesome. They were often using dedicated parts.  
they were heavily pirated. they were heavily protected.  
So protected that it makes them vulnerable (to time)!  
Hacking is the only way to preserve them.



Let's look at the Capcom Play System, known as CPS1.

# STREET FIGHTER II

The World Warrior

PUSH 1P OR 2P START.

©CAPCOM CO.,LTD.

# STREET FIGHTER II

CHAMPION EDITION

PUSH 1P OR 2P START.

©CAPCOM CO.,LTD. 1991,92

CREDIT= 2

# STREET FIGHTER II

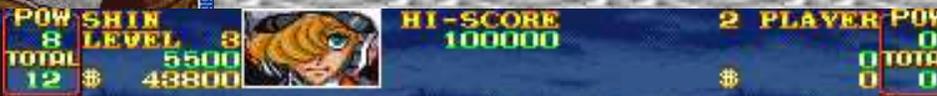
HYPER FIGHTING

PUSH 1P OR 2P START.

1991,92

known mostly for Street Fighter II





and many other good games



the complete list...

including the least known, only emulated in June 2014. It's SF2-based, but it's a mole hitting game !!



1P 1000 YU 99999

KO

RYU

95

DHALSIM



CPS1 was increasingly protected:  
Yet it was completely hacked.  
SF2 bootlegs were common.

# SELECT PLAYER



GUY

CODY

HAGGAR



1 . PLAYER



Height · · 5.87ft. Height · · 5.97ft. Height · · 6.64ft.

Height · · 158lb. Height · · 187lb. Height · · 297lb.



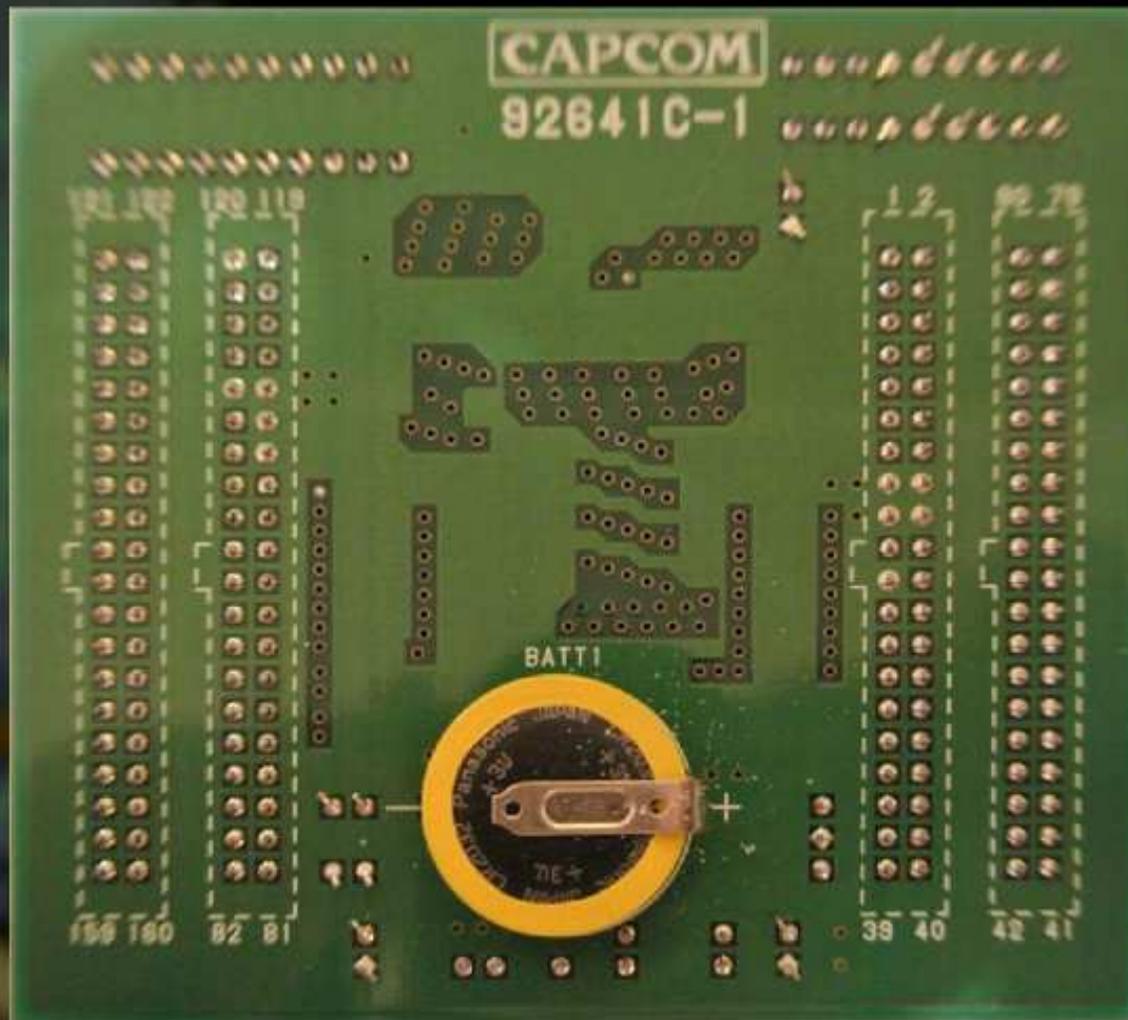
a final fight bootleg, adding extra characters to control.



an original CPS1... (3 PCBs)



and a CPS1 bootleg (nothing in common)



the latest CPS1 generation had custom chip+suicide battery,..

# Cadillacs AND Dinosaurs

Cadillacs & Dinosaurs: Cadillac, Cadillac script, Cadillac crest design, "V" design, various automobile body style designs, are trademarks of General Motors Corporation used under license.

© 1992, Mark Schultz  
© 1992, CAPCOM Co., Ltd

# DINOSAUR HUNTER

TALES BASED UPON THE COMIC  
"DINOSAURS & HUNTERS"

恐龍獵人

# THE PUNISHER

© 1993 MARVEL ENTERTAINMENT GROUP, INC.  
© CAPCOM CO., LTD. 1993

# 飆風戰警

© 2002 MARVEL ENTERTAINMENT GROUP, INC.  
© ALL-IN CO., LTD. 2002

# Warriors of Fate

# 火鳳凰

© CAPCOM CO., LTD. 1988  
本宮之志 M&M 集英社

...but it was defeated nonetheless:  
weak encryption+encrypted data made plaintext attack easy.



**GREAT  
PROTECTED  
COMPLETELY  
HACKED**

CPS1 was great.  
It was protected.  
It was completely hacked.



Capcom released its evolution, the CPS2



it started with this...

# STREET FIGHTER II

SUPER  
STREET FIGHTER 2  
831005  
JAPAN

The New Challengers

# STREET FIGHTER II<sup>TM</sup>

HYPER  
STREET FIGHTER 2  
040202  
USA

The Anniversary Edition

from Super SF2 (1993)  
to Hyper SF2 (2003)  
(how original !)



CPS2 was awesome...



...really awesome!



...plenty of great games...

# I



# II



# III

the real successor to the CPS1  
the last successful hardware from Capcom.



here is the complete list of bootlegs, hacks, swaps...  
(absolutely NOTHING)

1P

1 P00

50000

2P

1

E. Honda

K.O  
98

T. Hawk



they were so desperate that they couldn't hack that...

1UP 0 LEO 50000 INSTER



E-Honda

99

T-Hawk



that they hacked a console version into an arcade game (with typo)



所 有  
CAPCOM  
CP 5294 E  
シムス/ソニー38888  
シムス030112955  
WEB: 8733

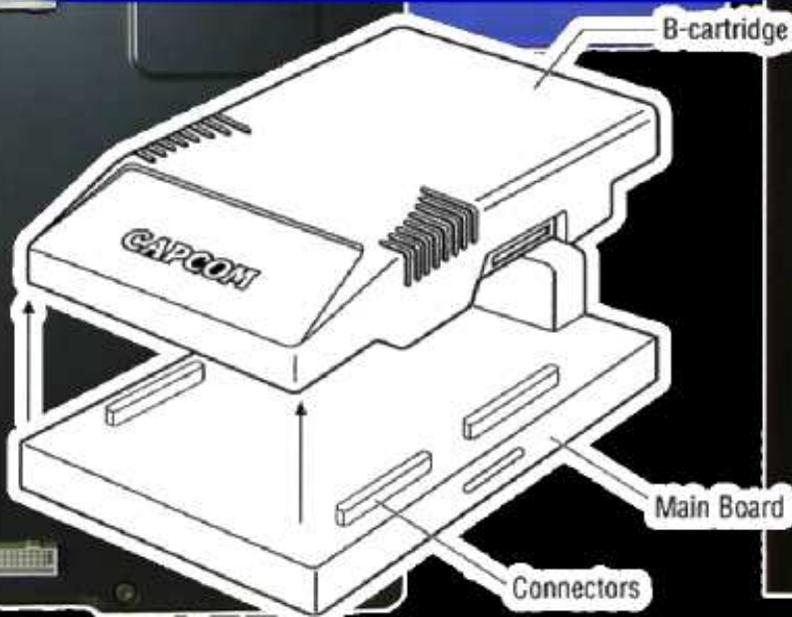


所 有  
CAPCOM  
CP SYSTEM 5  
シムス/ソニー38888  
シムス030112955  
WEB: 8733



所 有  
CAPCOM  
CP 5294 E  
シムス/ソニー38888  
シムス030112955  
WEB: 8733

# CPS II SYSTEM

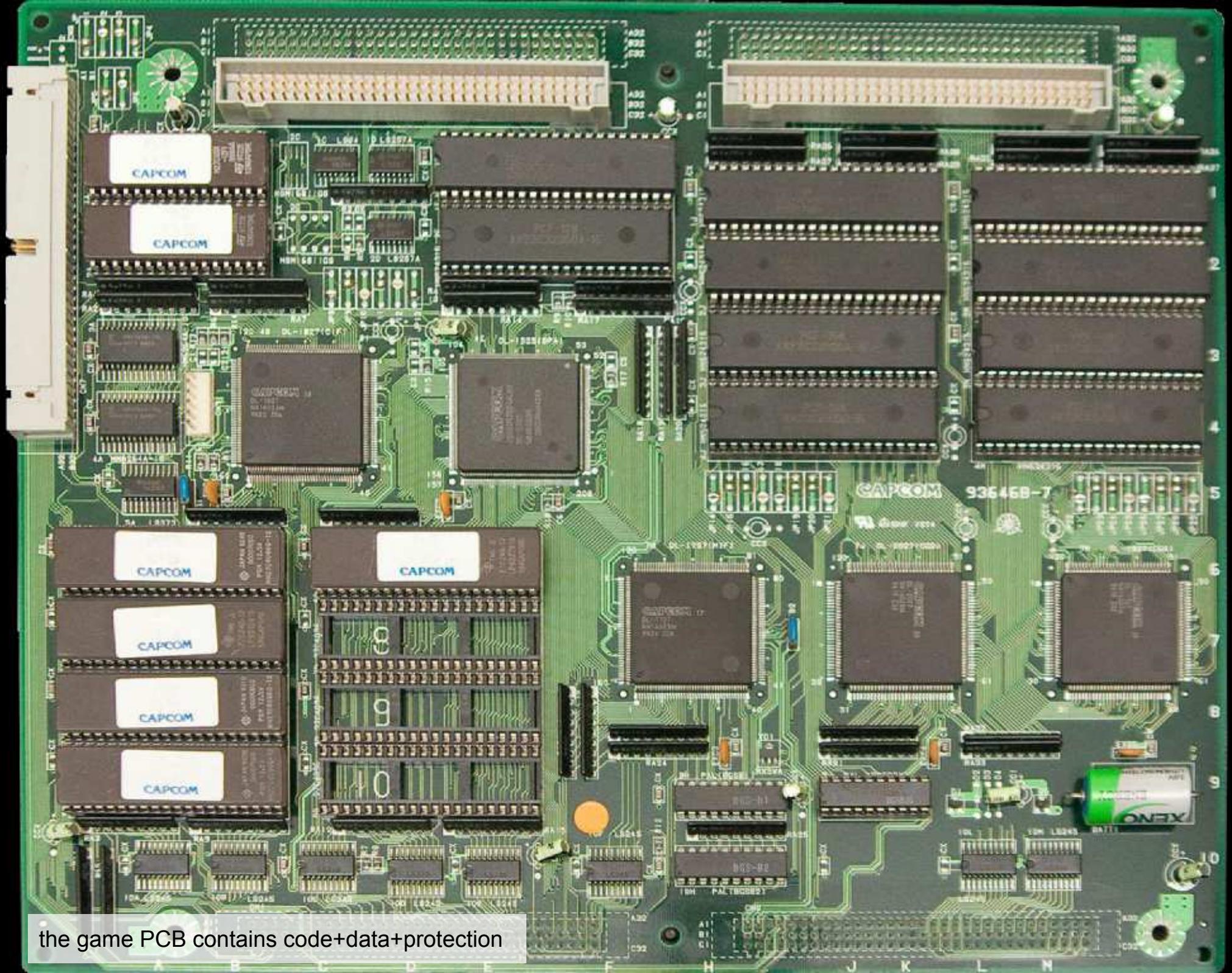


所 有  
CAPCOM  
CP 5294 E  
シムス/ソニー38888  
シムス030112955  
WEB: 8733

警告

- 分解禁止
- 充電注意
- 高温注意
- 取扱い注意

A CPS2 is a sandwich of 2 PCBs (sometimes only 1, sometimes 3)



the game PCB contains code+data+protection

EXPANSION CONNECTOR

SOUND  
CODE

SAMPLES  
(SOUND DATA)

GRAPHICS

SRAM

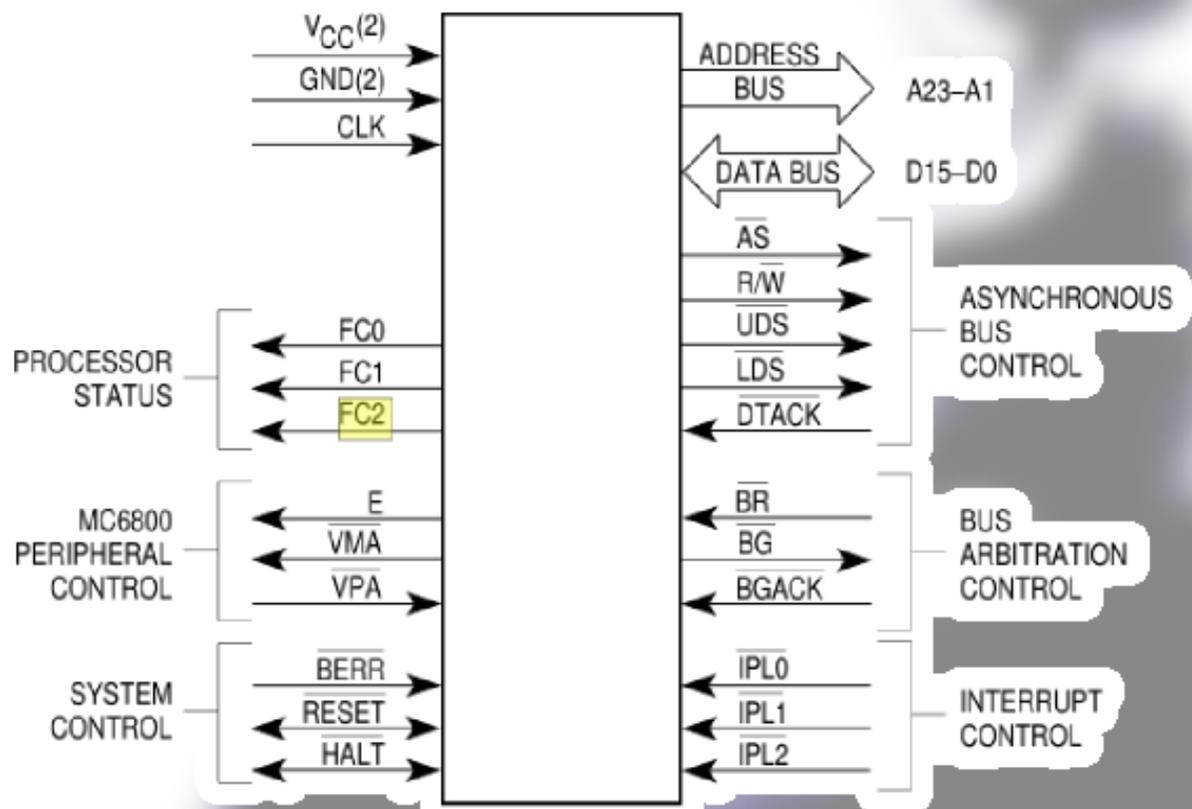
CODE

DATA

PALS

BATTERY

what's in green is in clear,  
in red is encrypted.  
Code and Data are together.  
Code is crypted, data isn't.



**Table 3-3. Function Code Outputs**

Function Code Output			Address Space Type
FC2	FC1	FC0	
Low	Low	Low	(Undefined, Reserved)
Low	Low	High	User Data
Low	High	Low	User Program
Low	High	High	(Undefined, Reserved)
High	Low	Low	(Undefined, Reserved)
High	Low	High	Supervisor Data
High	High	Low	Supervisor Program
High	High	High	CPU Space

**Table 6-2. Exception Vector Assignment**

Vectors Numbers		Address		Space <sup>6</sup>	Assignment
Hex	Decimal	Dec	Hex		
0	0	0	000	SP	Reset: Initial SSP <sup>2</sup>
1	1	4	004	SP	Reset: Initial PC <sup>2</sup>
2	2	8	008	SD	Bus Error
3	3	12	00C	SD	Address Error

assigned these numbers.

Reset vector (0) requires four words, unlike the other vectors which only require two words, and is located in the supervisor program space.

decryption is made on the fly, during memory fetch. read standard memory? as is. read for execution? decrypt.

patch an opcode (unknown encryption)  
→ black screen. game over. retry ?

AWEOSOME

PROTECTED

UNSCATHED  
1993-1999

CPS2 was really awesome.  
it was well protected.  
it was absolutely unscathed for 6 years.

# NEO·GEO®

MAX 330 MEGA  
PRO-GEAR SPEC

**SNK**



the Neo-Geo is known for many games...

an exceptional success and longevity !

# NEO-GEO

## SNK



90

91

92

93

94

95

96

97

98

99

2000

01

02

03

04



a success in arcade AND as an expensive console



So Capcom created something that made the NeoGeo look small and cheap. It was a commercial failure...

STREET FIGHTER ZERO STREET FIGHTER ZERO

950605

JAPAN

WORK	RAM OK
CPS0	RAM OK
CPS1	RAM OK
CPS2	RAM OK
OBJECT	RAM OK
Q SOUND	RAM OK



QSound Chips have been developed by QSound and incorporate QSound's proprietary QSound sound enhancement technology.

CAPCOM

951020

CPS CHANGER

WORK	RAM OK
CPS0	RAM OK
CPS1	RAM OK
CPS2	RAM OK



INSERT COIN

©CAPCOM Co., Ltd. 1995



PRESS START

©CAPCOM Co., Ltd. 1995





but nothing happened. the dragon was still alive.



to defeat a dragon, you need adventurers:  
Razoola, Charles MacDonald, Andreas Naive, Nicola Salmoria, David Haywood, and many others.  
(I worked with Razoola, and helped him on the PC side)





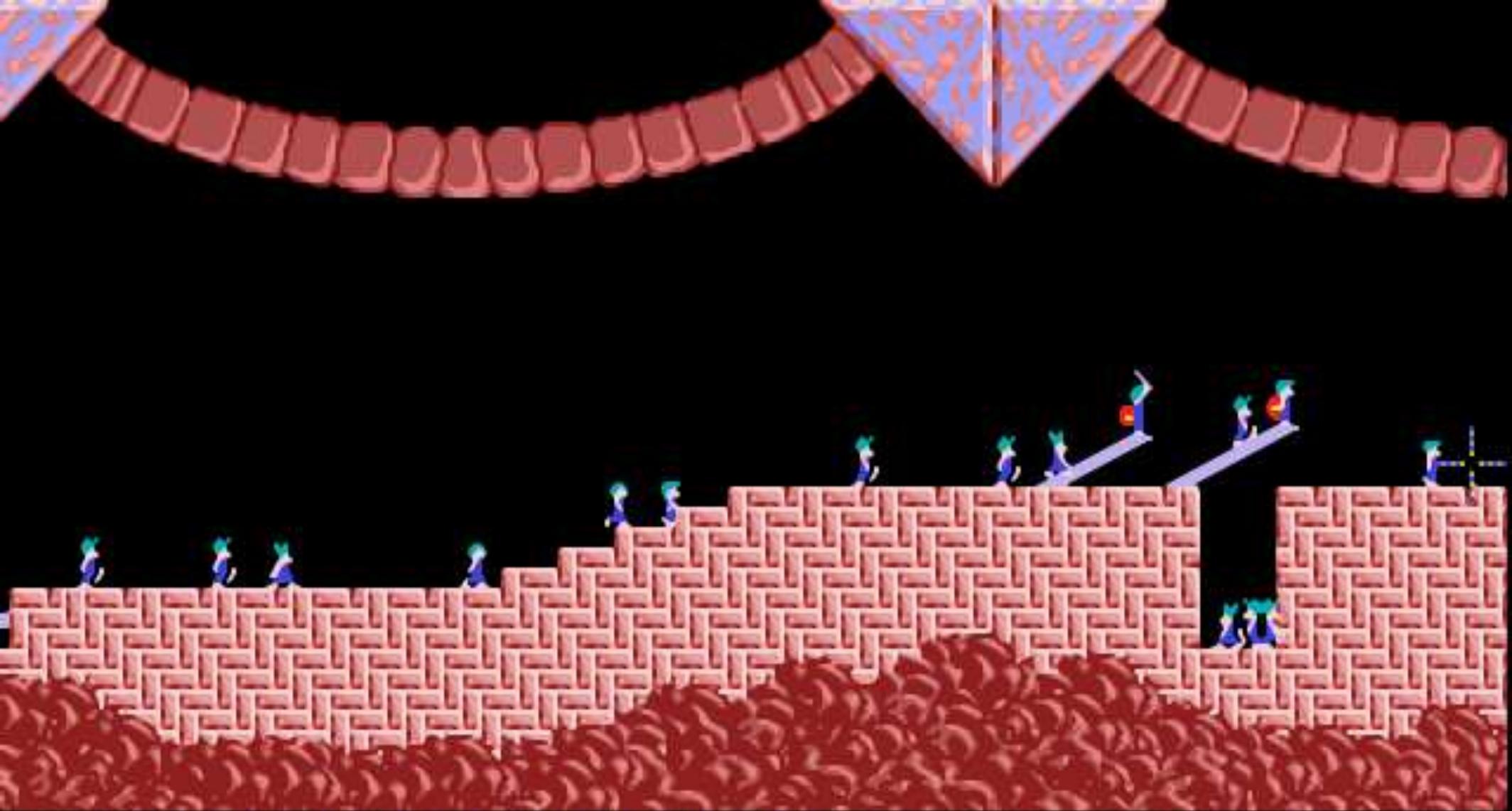
in spring 2000, he found that some specific memory ranges were not using encryption!  
why ? no reason - just a big facepalm !  
→ shellcode execution for a split second.

# FACEPALM

Mode	Generation	Syntax
<b>Register Direct Addressing</b> Data Register Direct Address Register Direct	EA=Dn EA=An	Dn An
<b>Absolute Data Addressing</b> Absolute Short Absolute Long	EA = (Next Word) EA = (Next Two Words)	(xxx).W (xxx).L
<b>Program Counter Relative Addressing</b> Relative with Offset Relative with Index and Offset	EA = (PC)+d <sub>16</sub> EA = (PC)+d <sub>8</sub>	(d <sub>16</sub> ,PC) (d <sub>8</sub> ,PC,Xn)
<b>Register Indirect Addressing</b> Register Indirect Postincrement Register Indirect Predecrement Register Indirect Register Indirect with Offset Indexed Register Indirect with Offset	EA = (An) EA = (An), An ← An+N An ← An-N, EA=(An) EA = (An)+d <sub>16</sub> EA = (An)+(Xn)+d <sub>8</sub>	(An) (An)+ -(An) (d <sub>16</sub> ,An) (d <sub>8</sub> ,An,Xn)
<b>Immediate Data Addressing</b> Immediate Quick Immediate	DATA = Next Word(s) Inherent Data	#<data>
	EA = SR, USP, SSP, PC, VBR, SFC, DFC	SR,USP,SSP,PC, VBR, SFC,DFC

when reading relatively to code (PC),  
memory fetches are actually decrypted !  
Sega prevented that, but Capcom failed.  
→ first CPS2 decryption, word by word

This mode is similar to the mode described in **2.2.7 Address Register Indirect with Index (8-Bit Displacement) Mode**, except the PC is the base register. The operand is in memory. The operand's address is the sum of the address in the PC, the sign-extended displacement integer in the extension word's lower eight bits, and the sized, scaled, and sign-extended index operand. The value in the PC is the address of the extension word. **This is a program reference allowed only for reads.** The user must include the displacement, the PC, and the index register when specifying this addressing mode.



Saved: 00

1:21

so, in Summer 2000, I visited Raz, hoping we'd break the algo. but no success...

Credits: 00

## reset

```
nop
nop
nop
move.b  #80, $800030.1
nop
move.b  #0, $800030.1
cmpi.l  #5642194, D0
lea     ($6,PC), A4
bra     $d82
```

lea (\$6,PC), A2	lea (\$6,PC), A2
bra \$ef6	bra \$d96
jmp (A4)	jmp (A4)
moveq #1f, D7	moveq #1f, D7
move.l #f000f000, D0	move.l #f000f000, D0
cmpi.l #5642194, D0	move.l (A0)+, (A1)
move.l (A0)+, (A1)	or.l D0, (A1)+
or.l D0, (A1)+	move.l (A0)+, (A1)
move.l (A0)+, (A1)	or.l D0, (A1)+
or.l D0, (A1)+	move.l (A0)+, (A1)
move.l (A0)+, (A1)	or.l D0, (A1)+
or.l D0, (A1)+	move.l (A0)+, (A1)
move.l (A0)+, (A1)	or.l D0, (A1)+
or.l D0, (A1)+	move.l (A0)+, (A1)
move.l (A0)+, (A1)	or.l D0, (A1)+
or.l D0, (A1)+	move.l (A0)+, (A1)

in December 2000, Raz noticed that Capcom leaked the key to keep decryption alive.  
→ automated dump is now possible !

```

--- CPS-2 Hacker ---
Currently executing address : 00000174
Using instruction : MOVE.L #$xxxxxxxx,D0

-----
NOW BRUTEFORCING
Address : 00000176      Address :
Encrypted : 363A       Encrypted : B
Nonencrypted : 0080    Nonencrypted : 40

-----
Please wait, this will take some time.

```



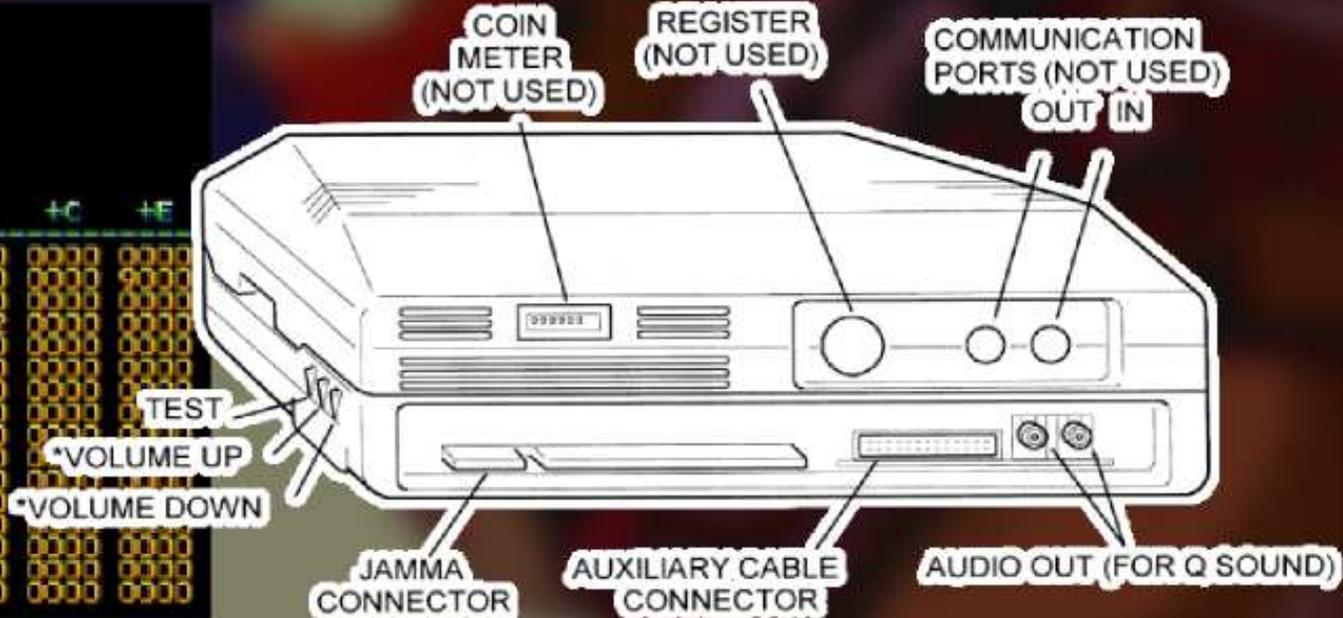
we dumped by connecting the CPS2 to the joystick port of the PC. ugly, clumsy, slow, but worked !

```

--- CPS-2 Hacker ---
Use iup controller.
Button 1 : Fast Move
Button 2 : Step $10000

Offset  +0  +2  +4  +6  +8  +A  +C  +E
00FF8000 0000 0000 0000 0000 0000 0000 0000
00FF8010 0000 0000 0000 0000 0000 0000 0000
00FF8020 9083 90C3 9103 9143 9183 91C3 9203
00FF8030 0000 0000 0000 0000 0000 0000 0000
00FF8040 0000 7FFF 003F 0000 0000 0000 0000
00FF8050 0000 0000 0000 0000 0000 0000 0000
00FF8060 0000 0000 0000 0000 0000 0000 0000
00FF8070 0000 0000 0000 0000 0000 0000 0000
00FF8080 0000 0000 0000 0000 0000 0000 0000
00FF8090 0000 0000 0000 0000 0000 0000 0000
00FF80A0 0000 0000 0000 0000 0000 0000 0000
00FF80B0 0000 0000 0000 0000 0000 0000 0000
00FF80C0 0000 0000 0000 0000 0000 0000 0000
00FF80D0 0000 0000 0000 0000 0000 0000 0000
00FF80E0 0000 0000 0000 0000 0000 0000 0000
00FF80F0 0000 0000 0000 0000 0000 0000 0000

```







stories

submissions

popular

blog

ask slashdot

book reviews

games

idle

yro

## CPS-2 Encryption Scheme Broken

Posted by **Hemos** on Sunday January 07, 2001 @10:44AM  
from the more-roms-for-all dept.



[Acheon](#) writes:

"The CPS-2 arcade board from Capcom uses some hard encryption scheme that has been a very hot issue in emulation for years. Yet finally the code was broken [Final Burn](#), a quite recent arcade emulator, showed concrete results by running previously unsupported games such as Street Fighter Zero using decrypted ROM images. The CPS-2 Shock Team, who managed to reverse engineer the process for scratch, really outdone themselves and it is a very uncommon achievement."

the news didn't get it right, as usual...

# The Register<sup>®</sup>

## CPS2 arcade encryption smashed

Morality debate ensues

By **Lucy Sherriff** • [Get more from this author](#)

Posted in [Business](#), 8th January 2001 19:44 GMT

A group of gaming enthusiasts called the [CPS-2 Shock Team](#) claims to have broken the encryption on the CPS-2 arcade board from [Capcom](#).

While the algorithm itself has not been compromised, the group has managed to extract unencrypted data from the board using the 68k code on the hardware itself, according to a poster on [SlashDot](#). Whether this actually constitutes a break of encryption is a subject under discussion at the aforementioned geek site.



game over for CPS2 ?  
not fully. encryption still unknown, no possible restoration yet.

TOTAL

65200

1P

COM INSERT COIN

45

ROCK HOWARD

NOTARU FUTABA



recent NeoGeo games also featured better protection

CREDIT 00

NEO GEO HACKER by Razoola

Use Joystick and button 1.

- [>] Memory Viewer.
- [ ] Dump data.
- [ ] Verify dump.
- [ ] Music player.
- [ ] Run Loaded Game.

DO NOT DISTRIBUTE THIS SOFTWARE.

NEO GEO HACKER by Razoola

Start PD software & make sure lead connected. (button 1 to continue)

Use joystick to choose a region to dump. (button 1 to continue)

> ROM BANK 1 <

NOW DUMPING PLEASE WAIT.

[XXXX+-----]

Use the Joystick to scroll and the following buttons for extras.

- Button 1 = Speed scroll.
- Button 2 = Jump to bank region.
- Button 3 = Toggle selected bank.
- Button 4 = Quit.

OFFSET	+0	+2	+4	+6	BANK=0
00000000	0010	F300	0000	0402	.....
00000008	00C0	0408	00C0	040F	.....
00000010	0000	0414	0000	0426	.....
00000018	00C0	0426	00C0	0426	.....
00000020	0000	041A	0000	0420	.....
00000028	00C0	0426	00C0	0426	.....
00000030	00C0	0426	00C0	0426	.....
00000038	0000	0426	0000	0420	.....
00000040	00C0	0426	00C0	0426	.....
00000048	0000	0426	0000	0426	.....
00000050	00C0	0426	00C0	0426	.....
00000058	0000	0426	0000	0426	.....
00000060	0000	0432	0000	2536	.....
00000068	0000	2580	0000	0426	.....
00000070	0000	0426	0000	0426	.....
00000078	00C0	0426	00C0	0426	.....

NEO GEO HACKER by Razoola

Use PD tool to create needed files for verify. (button 1 to continue)

Use joystick to choose a region to verify. (button 1 to continue)

> ROM AREA <

VERIFYING ADDRESS #000032F2  
STATUS : GOOD

DO NOT DISTRIBUTE THIS SOFTWARE.

but with 'joystick dumping', that was defeated quickly :p  
(decryption done by Nicola Salmoria)



what about dead CPS2 boards ?

CREDIT

0

?

CODE  
DATA



~~CODE  
DATA~~

if you put back decrypted code on a dead CPS2,  
it still doesn't work.

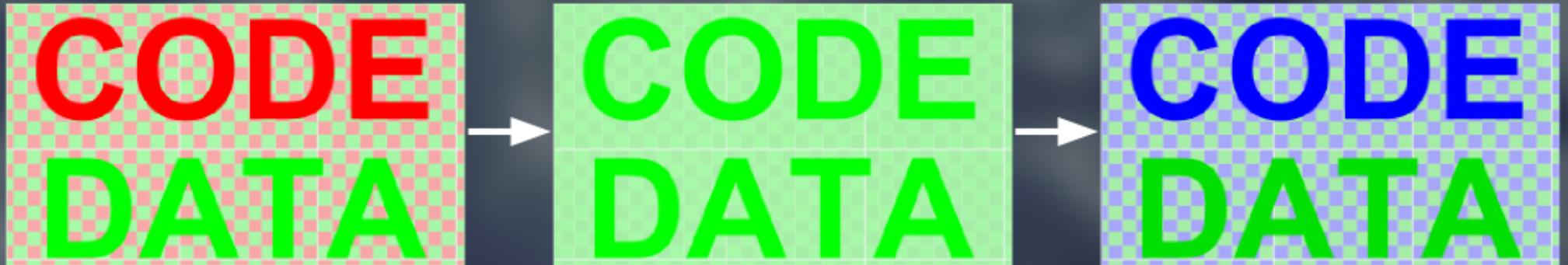


Razoola was donated a working PCB to sacrifice, then found out why.

```
move.w    #$7000, $400000.l
move.w    #$0, $8040a0.l
move.w    #$807d, $400002.l
move.w    #$1234, $400004.l
move.w    #$0, $400006.l
move.w    #$40, $400008.l
move.w    #$10, $40000a.l
move.w    #$f00, $804040.l
cmpi.l    #$5642194, D0
lea       ($6, PC), A4; ($9d6)
bra       $e82
move.w    #$ffc0, $80010c.l
move.w    #$0, $80010e.l
move.w    #$9000, $800100.l
move.w    #$9080, $800102.l
move.w    #$90c0, $800104.l
```

```
move.w    #$7000, $ffffff0.l
move.w    #$0, $8040a0.l
move.w    #$807d, $ffffff2.l
move.w    #$1234, $ffffff4.l
move.w    #$0, $ffffff6.l
move.w    #$40, $ffffff8.l
move.w    #$10, $ffffffa.l
move.w    #$f00, $804040.l
cmpi.l    #$5642194, D0
lea       ($6, PC), A4; ($9d6)
bra       $e82
move.w    #$ffc0, $80010c.l
move.w    #$0, $80010e.l
move.w    #$9000, $800100.l
move.w    #$9080, $800102.l
move.w    #$90c0, $800104.l
```

video and sound registers had a different address on dead games.  
patching these addresses makes them work again !



workflow: decrypt code, merge with data, patch addresses...

SUICIDE CPS2 GAME BOARD TESTER

ON BOARD RAM TEST

WORK RAM = GOOD  
GFX RAM = GOOD  
OBJECT RAM = BAD

SOUND INIT = GOOD  
@ SOUND RAM = GOOD

ERRORS FOUND ON GAME BOARD

(C) RAZOOLA, WWW.CPS2SHOCK.COM

**CAPCOM**  
**PHOENIX EDITION**

> REGION SETUP <

JUKEBOX PLAYER

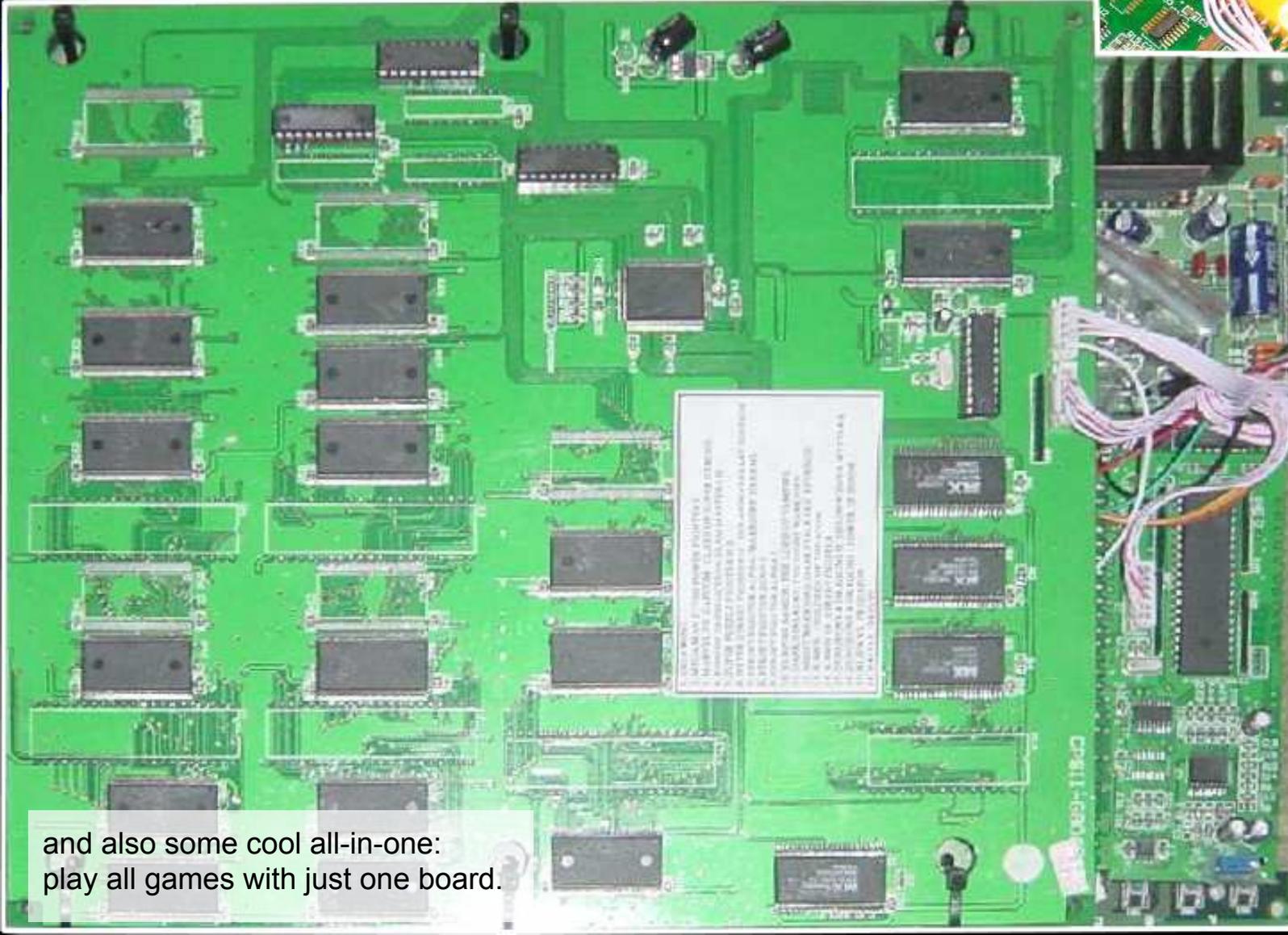
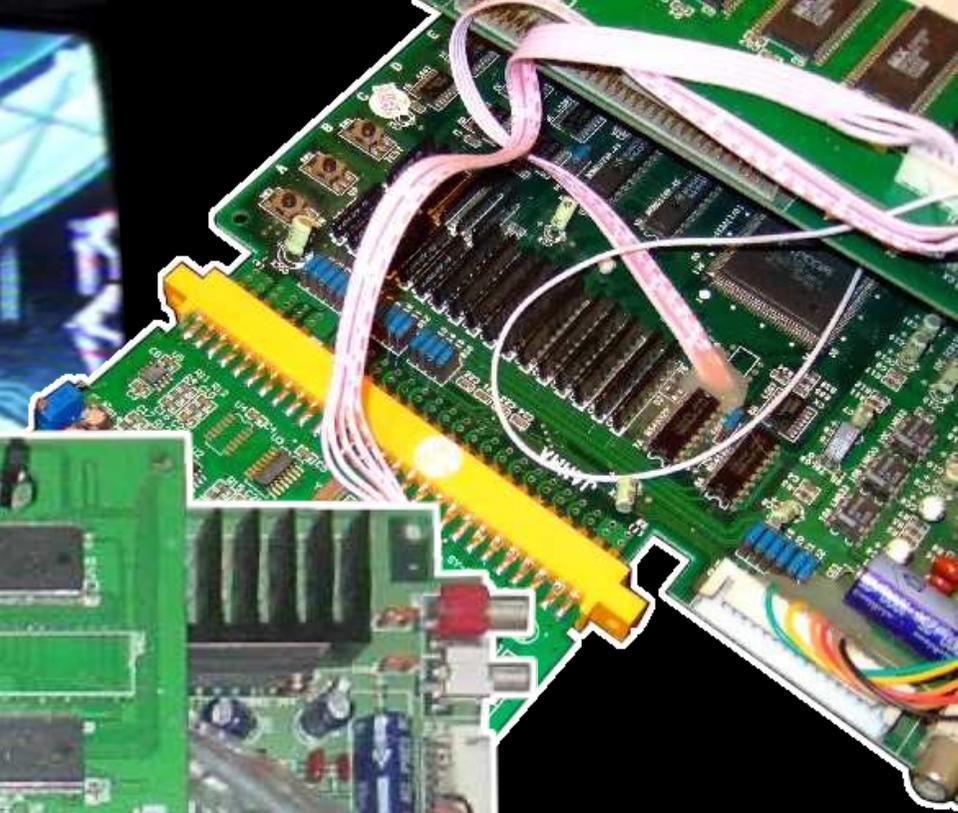
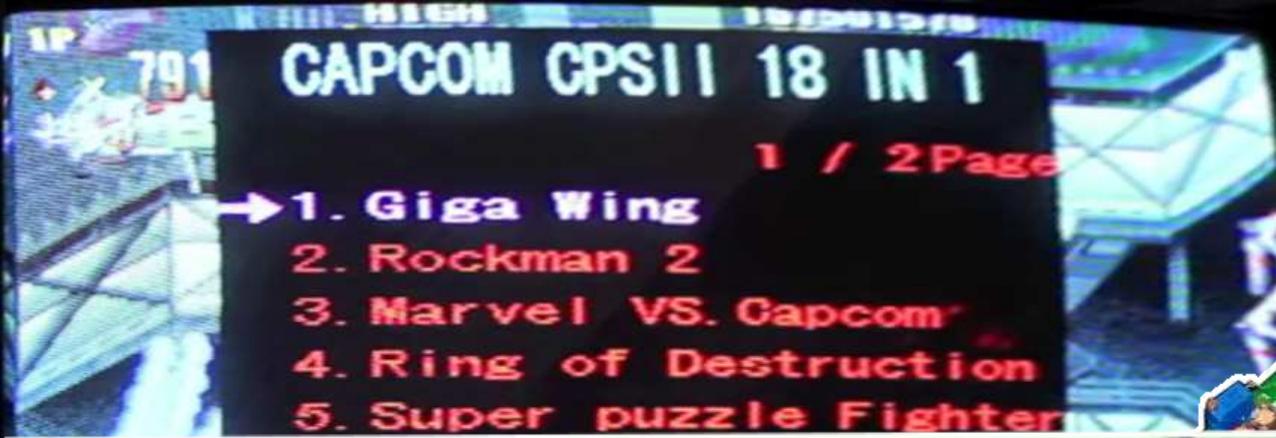
START GAME

Razoola made a universal test ROM,  
and 'no more battery' Phoenix versions.



# GIGAMA 2 THE POWER FIGHTERS

this also made bootlegs possible.  
no more battery...  
from MegaMan to Gigaman :(



and also some cool all-in-one:  
play all games with just one board.



CPS2, 1994



these 2 games look different...

PC, 1999

CPS2  
1994

A L I E N  
VS.  
PREDATOR

however, the IP was the same.  
Some nice lawyer wrote us a letter...  
You see who your friends really are,  
in these cases ;)

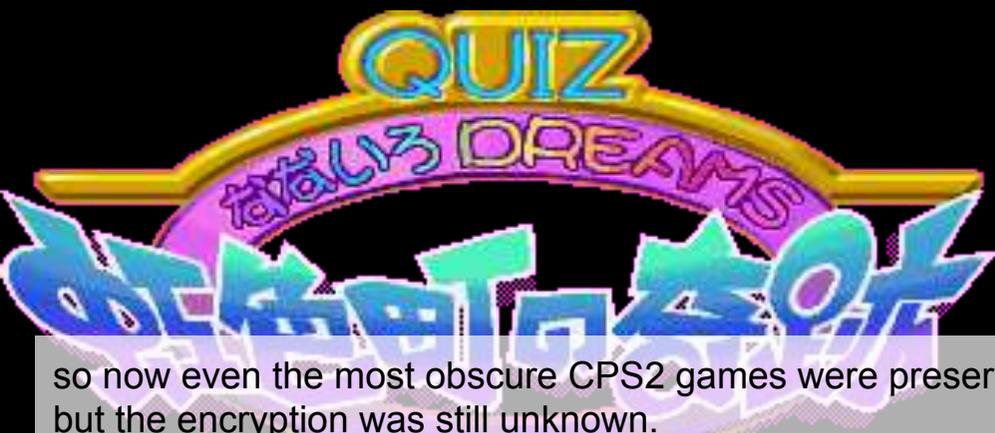
PC  
1999

A L I E N S  
V E R S U S  
PREDATOR



# 雀國志

霸王の采牌



so now even the most obscure CPS2 games were preserved,  
but the encryption was still unknown.  
and it would take us 200 years to dump all possible values for one game...

# CONTINUE 9



so we needed someone else to continue...



Felicia

CHALLENGER

Demitri

51

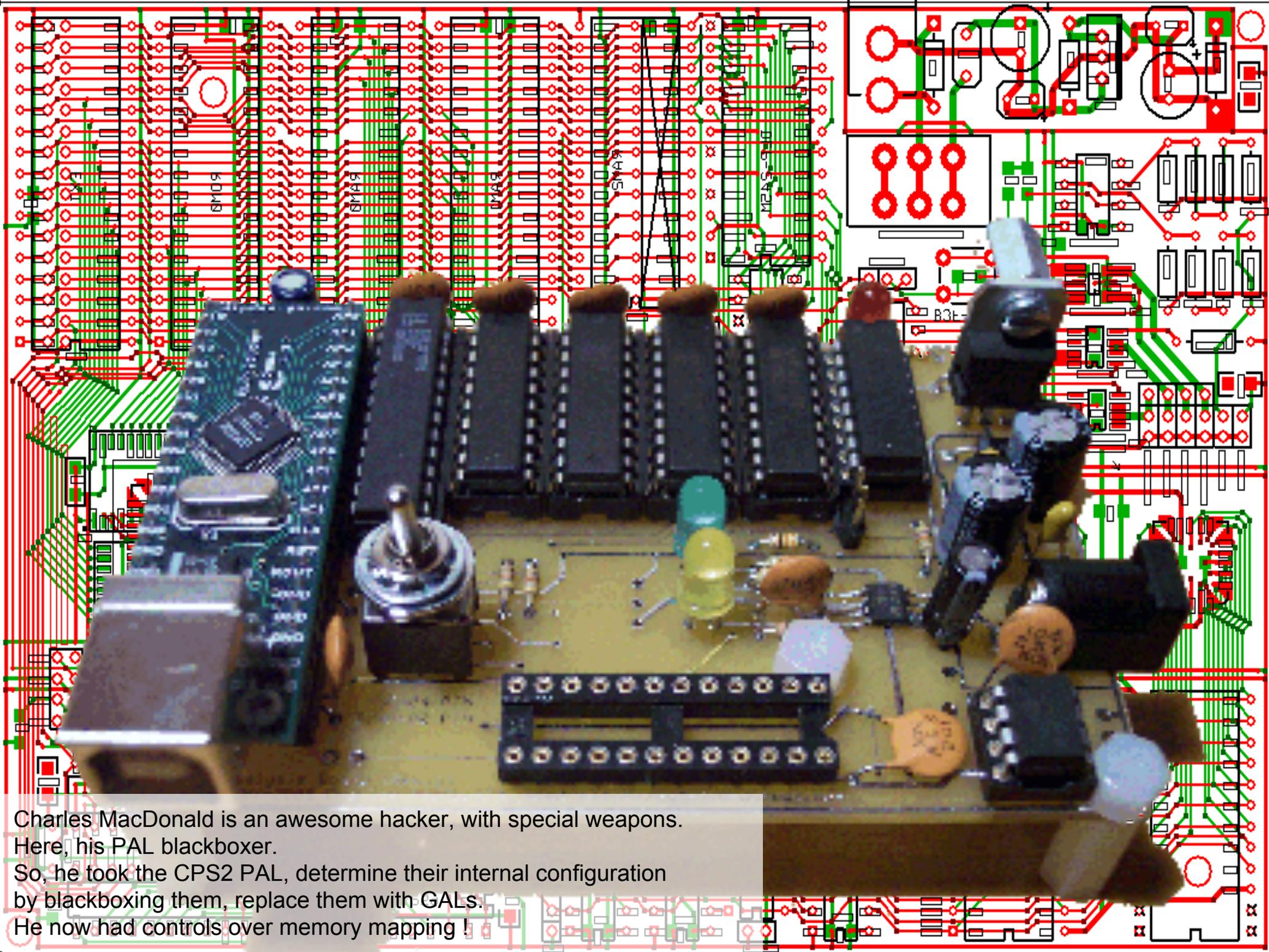
Special

Special

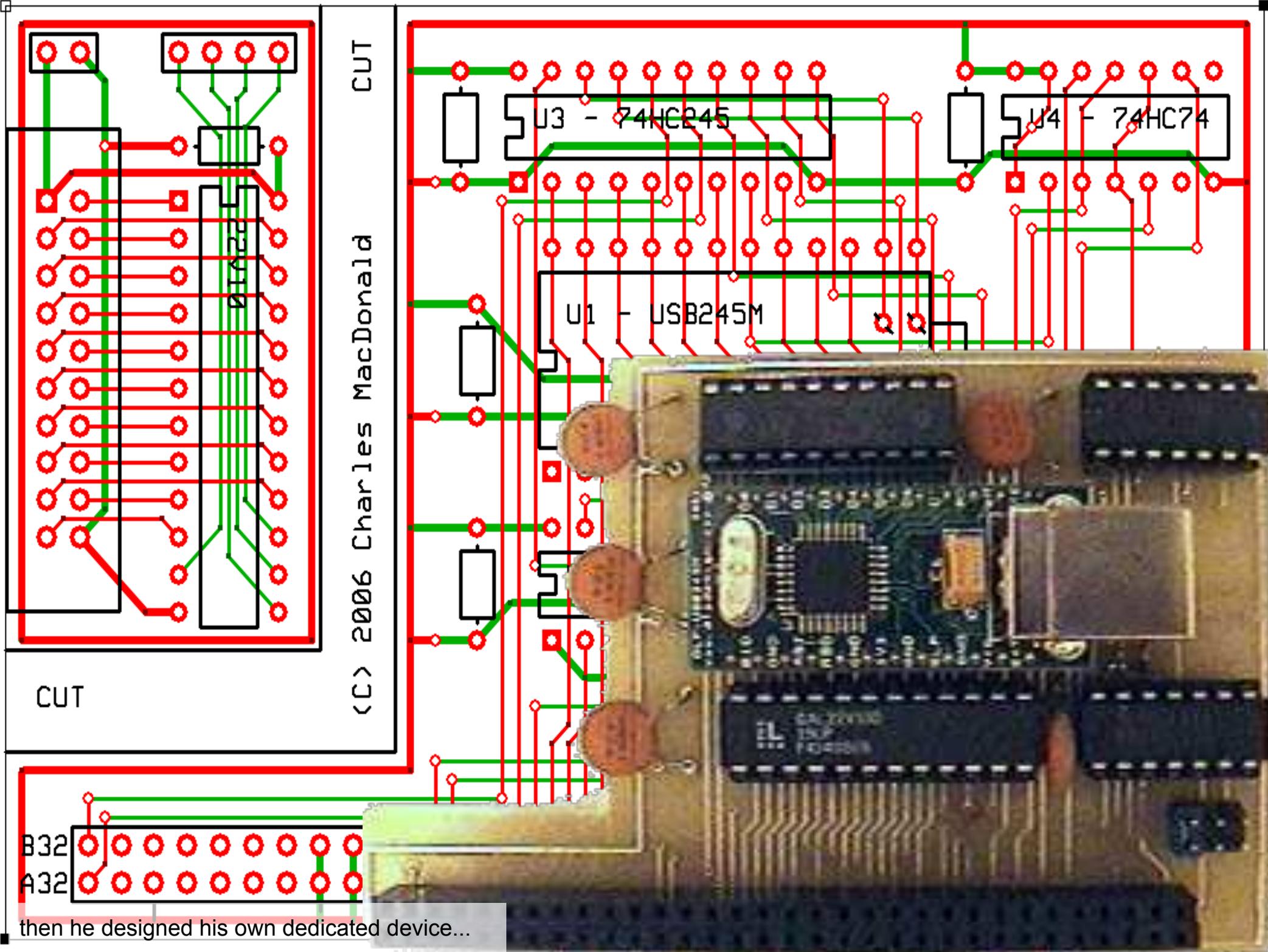
娘々

CAS

if you can't defeat the ennemy, bring your friends.  
In 2005, Charles MacDonald started to work on the CPS2.



Charles MacDonald is an awesome hacker, with special weapons. Here, his PAL blackboxer. So, he took the CPS2 PAL, determine their internal configuration by blackboxing them, replace them with GALs. He now had controls over memory mapping !



CUT

(C) 2006 Charles MacDonald

CUT

B32  
A32

then he designed his own dedicated device...

CPS-2 USB Loader  
© 2005-2006 Charles McDonald  
WWW: [HTTP://C2PM2.EMU1E0S.COM](http://c2pm2.emu1e0s.com)  
PC: 100E1000  
MP: 10001004



to dump CPS2 directly via its expansion port, to USB !!!  
He could dump the 8 Gb set in 17h.  
He did that for several games. but that wasn't enough to understand the algorithm.....



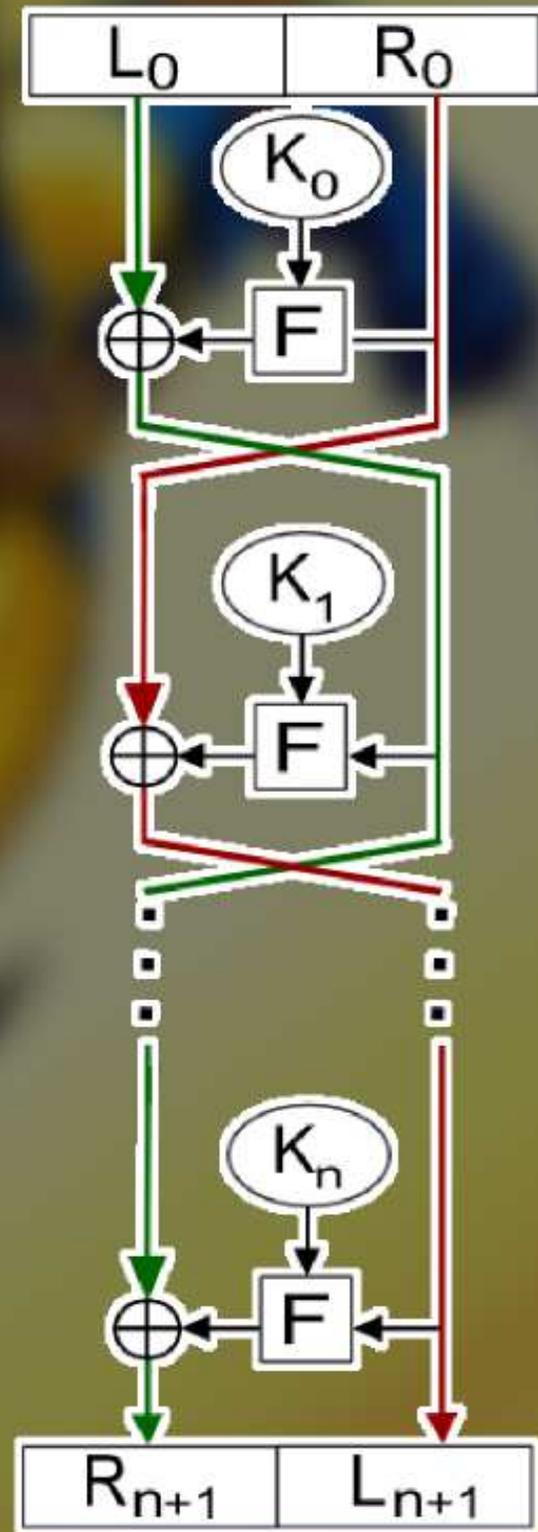
**CONTINUE?**  
**04**

**CONTINUE?**  
**04**



so someone else needed to continue to break the algo...

# PUZZLE FIGHTER II TURBO



that's where Nicola Salmoria and Andreas Naive helped.  
they're awesome to determine encryption algorithm.  
the algo was feistel based, and the key was 64 bits.



so, from one european decrypted dump of a game,  
the key could be determined,  
which could then decrypt the rare japanese version of the game.

# ROCKMAN THE POWER BATTLE

9 5 0 9 2 2

J A P A N

```
WORK      RAM OK
CPS0      RAM OK
CPS1      RAM OK
CPS2      RAM OK
```

```
WORK      RAM OK
CPS0      RAM OK
CPS1      RAM OK
CPS2      RAM OK
OBJECT    RAM OK
@ SOUND   RAM OK
```

## 3 . S O U N D & V O I C E T E S T

SOUND CODE No. 0000

```
CODE +01 == 1P UP
CODE -01 == 1P DOWN
CODE +10 == 1P RIGHT
CODE -10 == 1P LEFT
REQUEST == 1P SHOT1
STOP == 1P SHOT2
```

## 3 . S O U N D & V O I C E T E S T

SOUND CODE No. 0000

```
CODE +01 == 1P UP
CODE -01 == 1P DOWN
CODE +10 == 1P RIGHT
CODE -10 == 1P LEFT
REQUEST == 1P SHOT1
STOP == 1P SHOT2
```

VOLUME

MIN [+++++30+++++] MAX

EXIT = 1P & 2P START

Last, Dave Haywood designed an attack to determine the key just from the ENCRYPTED dump of the game. So even the rarest CPS2 game was preserved !

# ~ Epilogue ~

**UNENCRYPTED VERSION**

**DEBUGGER**

**UNENCRYPTED RANGE**

**ADDRESSING MODE**

**KEY LEAK**

CLUMSY HACKS

JOINT EFFORT

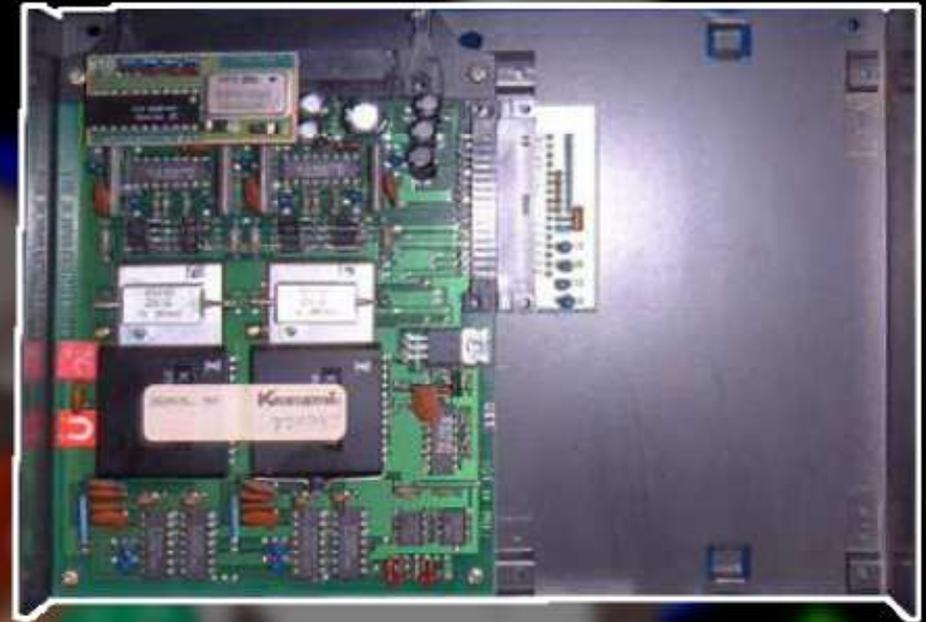
MANY CONTRIBUTIONS

SUCCESS



# AWESOME VICTORY

and overall, an awesome victory !



this is the Bubble Memory system.  
it's **very** fragile.

WARMING UP NOW

99

to work, it needs to warm up to a certain temperature.

to me, this big countdown says:

'all these games are going to disappear if no one hacks or contribute for them'

PRESENTED BY KONAMI

# Last Survivor

Last Survivor, a System X game from 1989, was thought to be lost forever. Someone still had one in working conditions: it was preserved, 20 years later !

SEGA<sup>®</sup>

©SEGA 1989



**before  
it's too late**

**HACKING IS  
PRESERVING**

So, before it's too late: hacking is the only way to preserve these over-protected yet great games...

CPS2Shock

<http://www.cps2shock.com>

[http://web.archive.org/web/\\*/http://cps2shock.retrogames.com](http://web.archive.org/web/*/http://cps2shock.retrogames.com)

Charles MacDonald

<http://cgfm2.emuviews.com/old2005.php>

Nicola Salmoria

<http://mamelife.blogspot.com/2006/01/8gb-2-is-still-4gb.html>

Andreas Naive

[http://andreasnaive.blogspot.com/2006\\_12\\_01\\_archive.html](http://andreasnaive.blogspot.com/2006_12_01_archive.html)

Mame (CPS2 encryption source)

<https://github.com/mamedev/mame/blob/master/src/mame/machine/cps2crpt.c>

DarkSoft

<http://64darksoft.blogspot.com>





yes, this is a CPS2 timeline :p

1P 104100 HI 104100 INSERT COIN

06800

Ryu

25



some bonus ?



SFA3 has a time lock: if you let it run long enough, some special modes are unlocked. the title background tells how many modes are unlocked.





extra characters, extra playing modes



1 . I N P U T T E S T

```

SERVICE  0
TEST      0

COIN      1P      2P
START    00      00
          00      00
          00      00

LEVER     000    000
          000    000
          000    000

SHOT      000    000
          000    000
  
```

LP LP R LK HP (S+LP)

HERE COME NEW CHALLENGERS

4 . C O L O R B A R

```

0 1 2 3 4 5 6 7 8 9 A B C D E F

RED
GREEN
BLUE
  
```

```

P1: LK      MP      U (S+LP)
P2:      HK      MP
  
```

TRADITIONAL FIGHT BEGINS

Hidden in the operator menu, Razoola found the crazy cheat codes in the disassembly to turn on this extras without waiting weeks.

T E S T M E N U

- > 1 INPUT
- 2 OUTPUT
- 3 SOUND & VOICE
- 4 COLOR
- 5 DOT CROSS HATCH
- 6 GAME DATA
- 7 CONFIGURATION
- 8 MEMORY CHECK

6 . G A M E D A T A

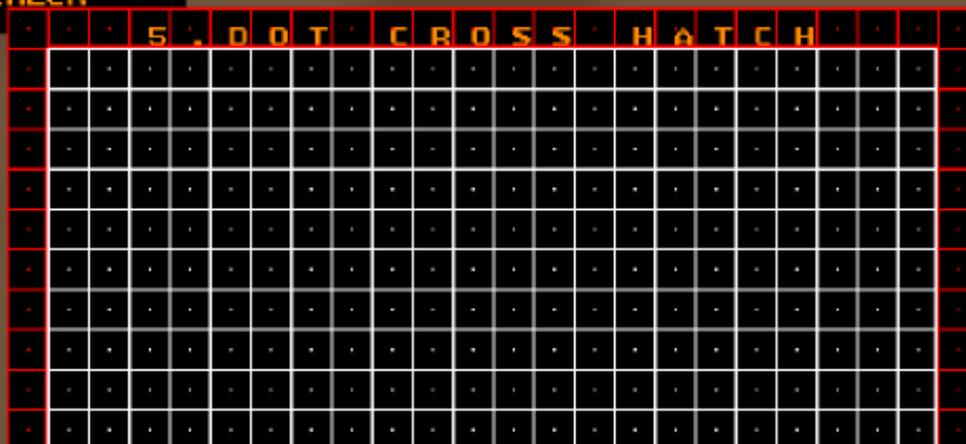
```

COIN      COUNTER  000036
SERVICE  COUNTER  000000
FREEPLAY  COUNTER  000000
  
```

```

P1:      L      R D      U (S+LP)
P2: R D      HK      LP
  
```

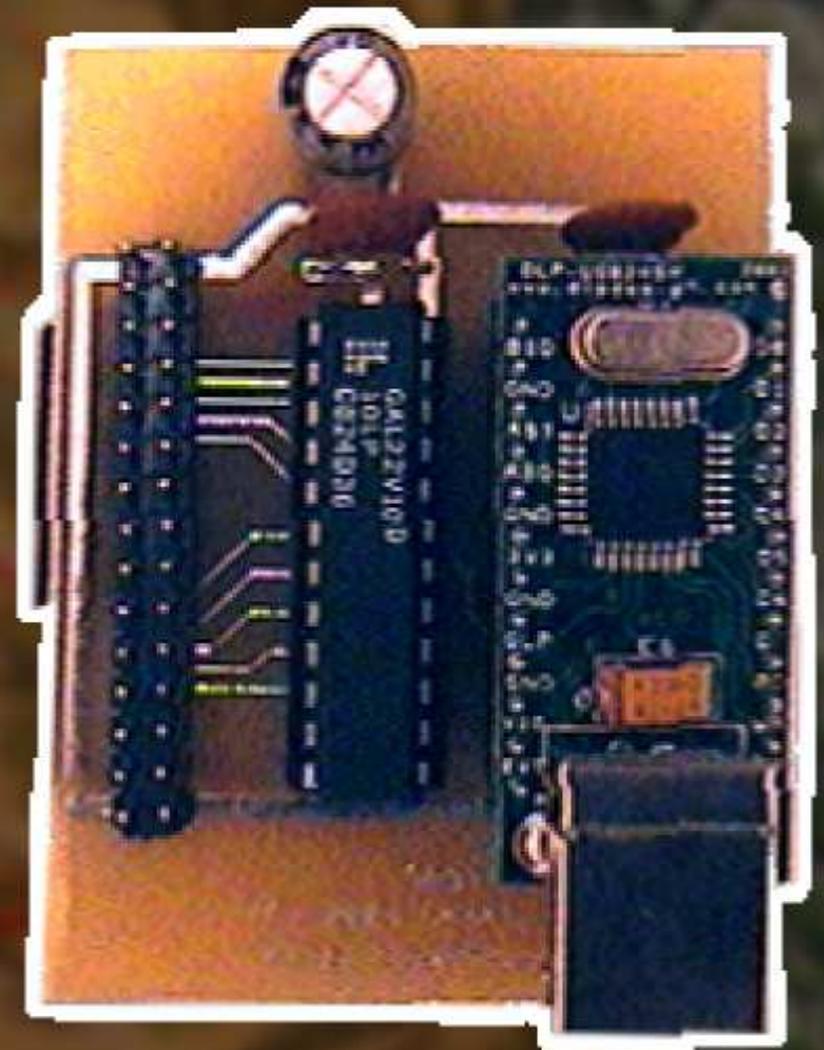
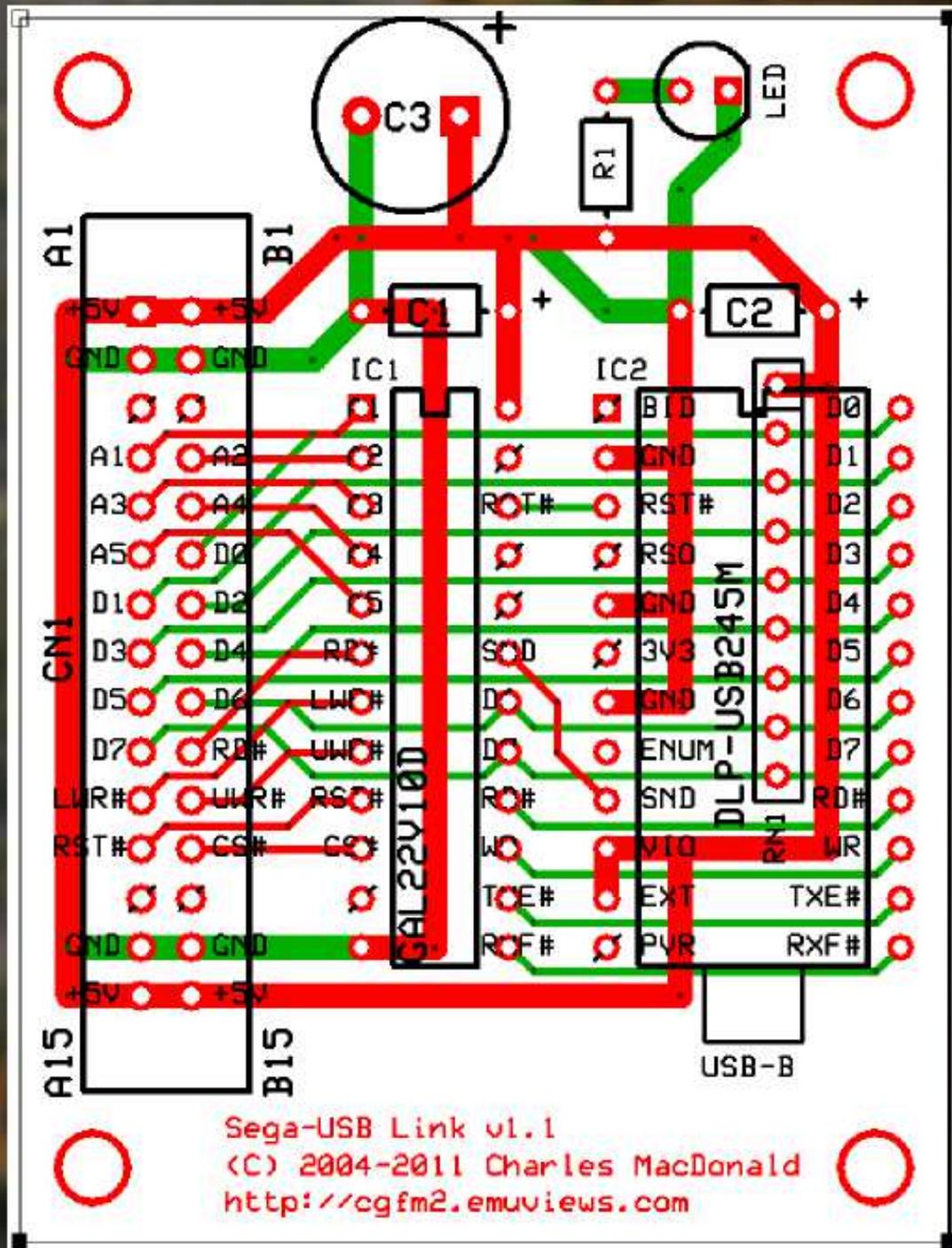
ENJOY NEW FIGHTING STYLE



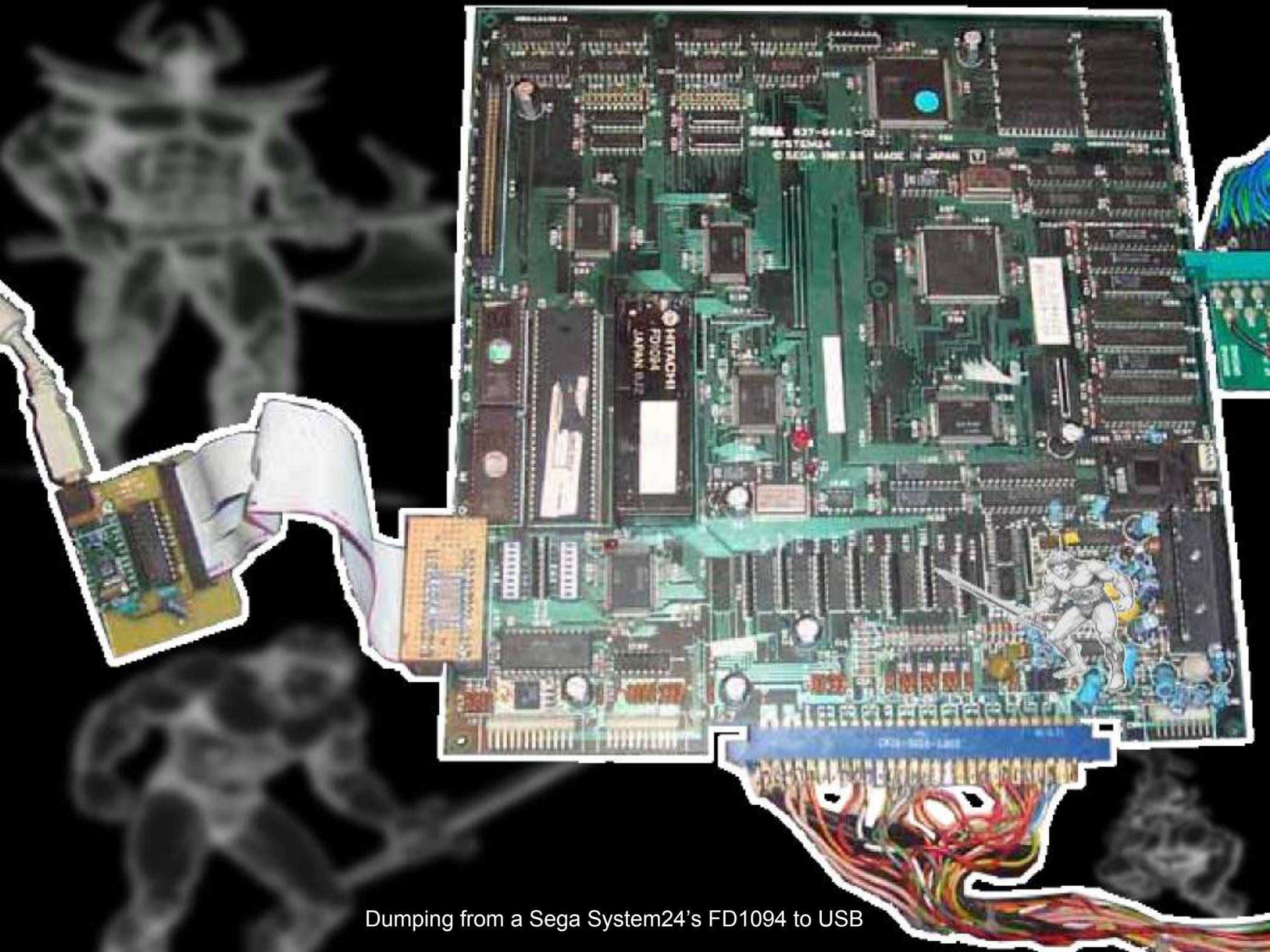
```

P1: MK D      D      MP      U D      LK (S+LP)
P2: D      R      R HP      L      R      MK
  
```

THANK YOU SO MUCH FOR LONG PLAYING



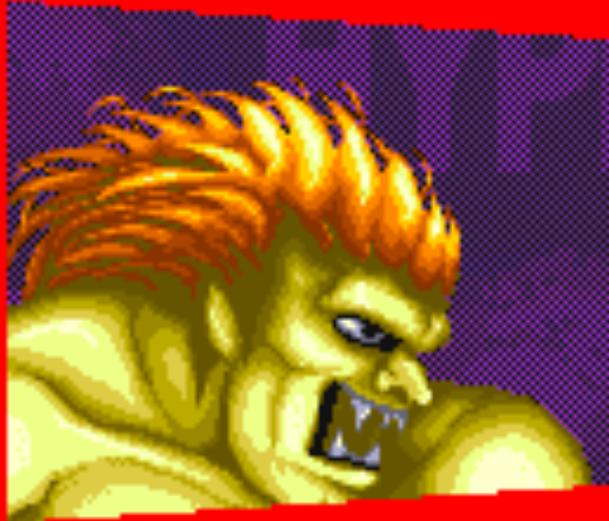
Charles MacDonald also worked on Sega hardware and created his own device for it...



Dumping from a Sega System24's FD1094 to USB



to preserve games from System 16, 24 & System X

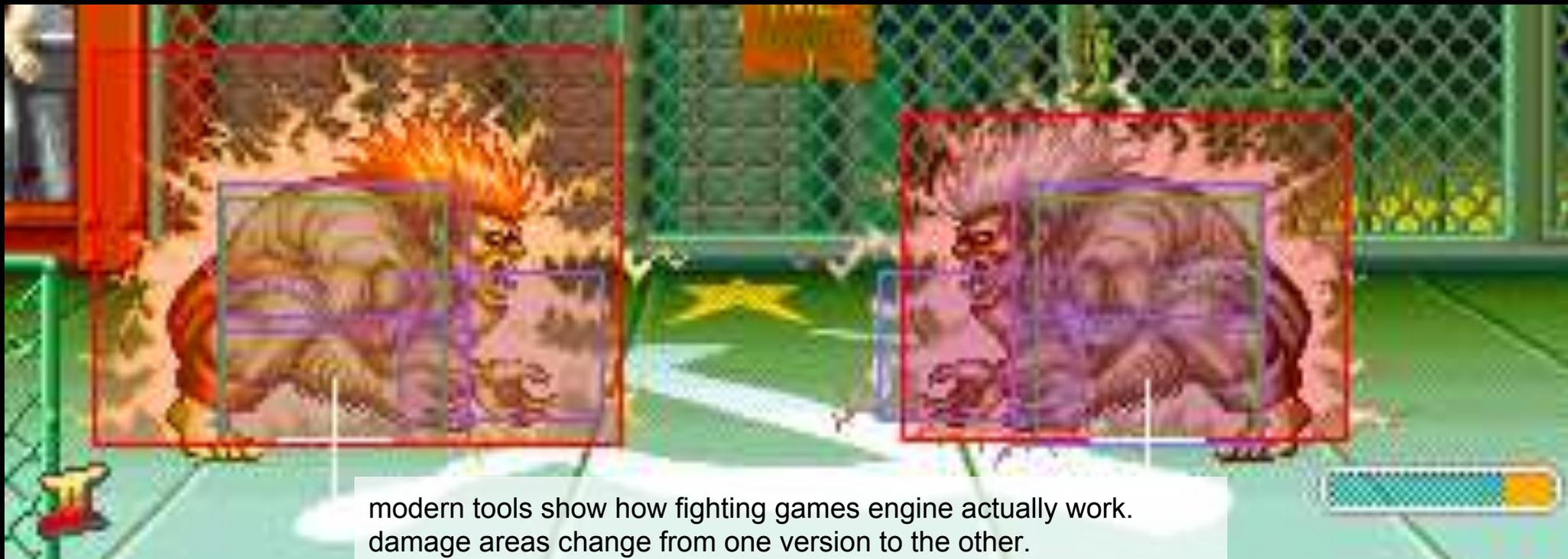


***BLANKA***

***V/S***



***BLANKA***



modern tools show how fighting games engine actually work. damage areas change from one version to the other.



there are bugs in the official releases !



attack behind you, or be hit for no reason...



tools assisted speedruns abuse games via standard controls.





*The End . . . ?*

