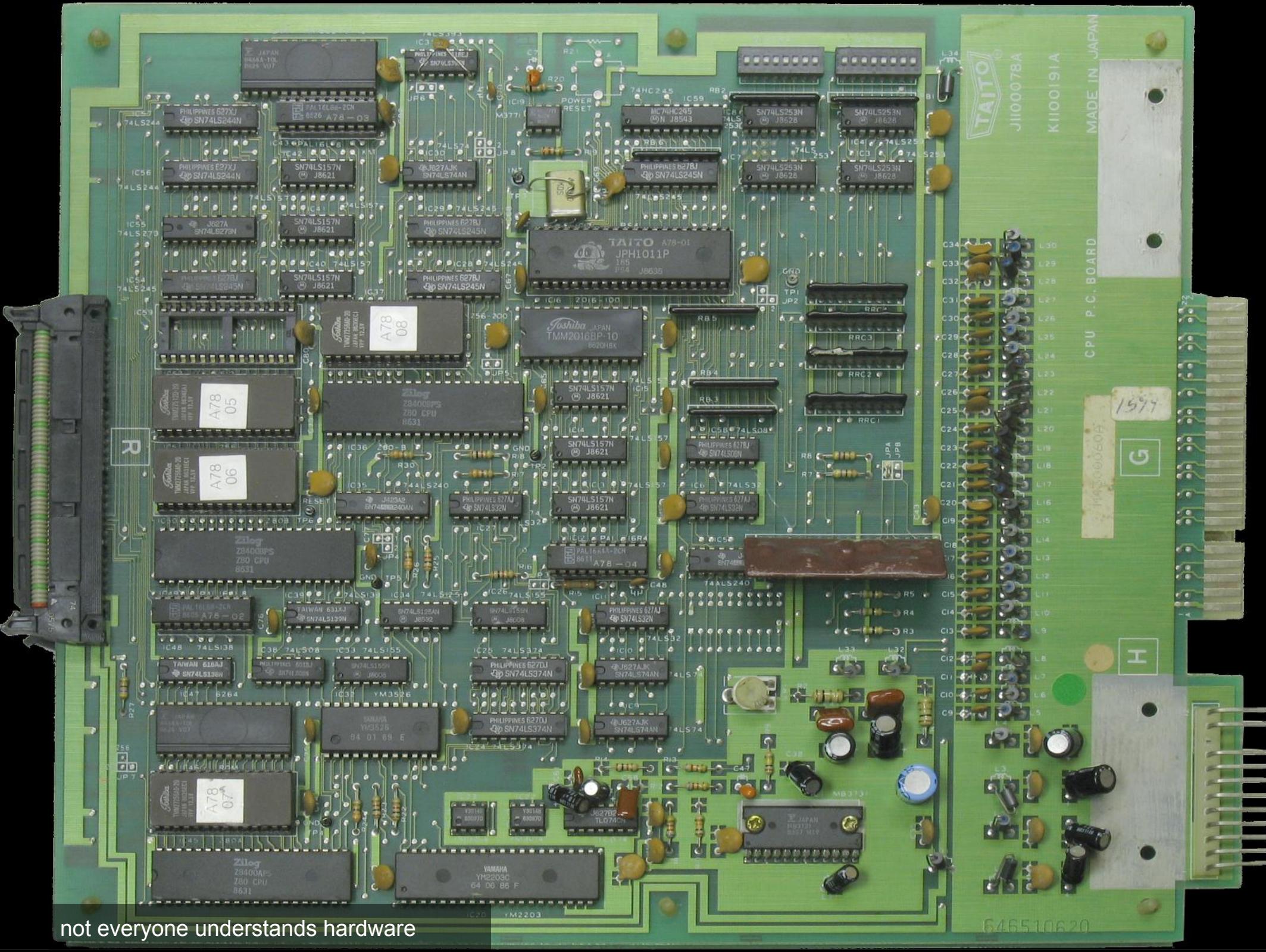


PRESERVING ARCADE GAMES

ANGE ALBERTINI
31C3



not everyone understands hardware

```
static MACHINE_CONFIG_START( tokio, bub1bob1_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", bub1bob1_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", bub1bob1_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(bub1bob1_state,tokio)
    MCFG_MACHINE_RESET_OVERRIDE(bub1bob1_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(bub1bob1_state, screen_update_bub1bob1)

    MCFG_GFXDECODE(bub1bob1)
    MCFG_PALETTE_LENGTH(256)

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

    MCFG_SOUND_ADD("ymsnd", YM2203, MAIN_XTAL/8)
    MCFG_SOUND_CONFIG(ym2203_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
```

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 successfull, they had to be awesome.
"Dedicated" (hardware, controls...) is the key to their success.

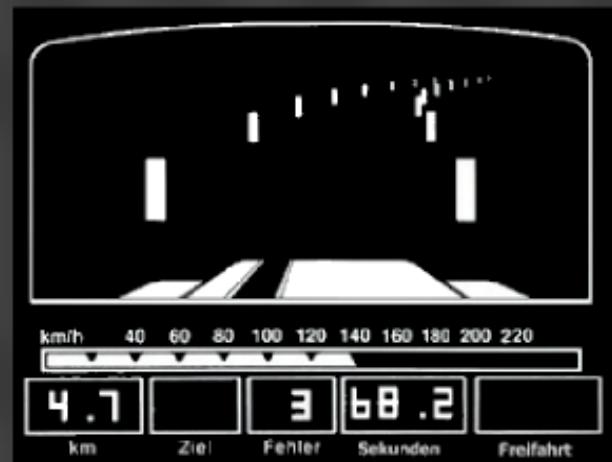
YOUR SCORE 006

TOP SPEED 035

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

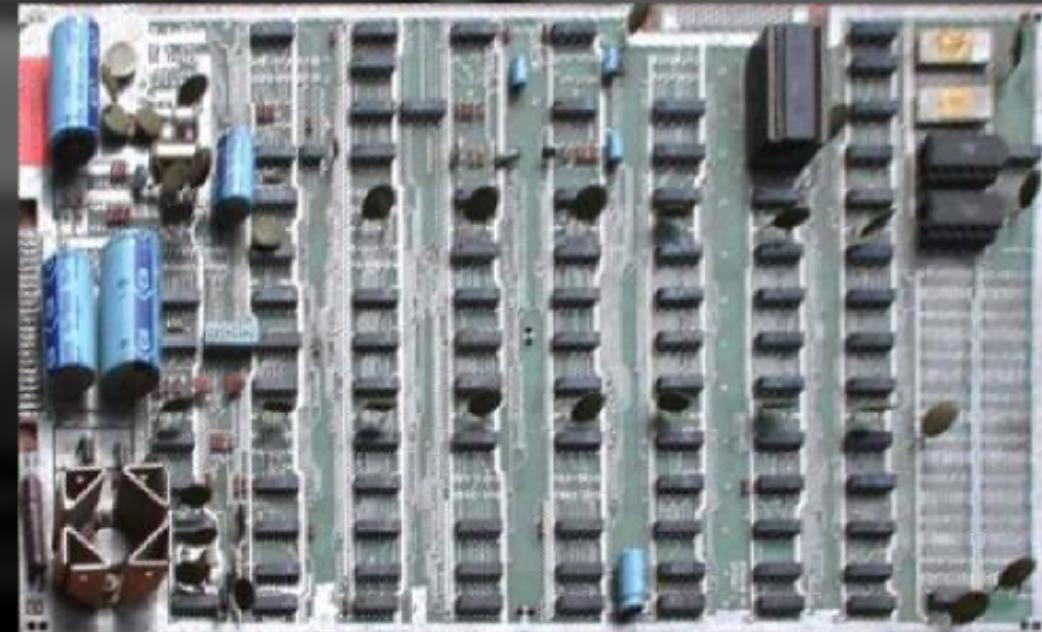


Nürburgring



NIGHT DRIVER

HIGH SCORE 000 GAME OVER ATARI
YOUR SCORE 000 TOP SPEED 000



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.

NOTE: Player stops moving when shot is fired.

4. Robots are worth 50 points. Bonus Score for destroying all Robots (even if Robots destroy each other).
5. The OTTO comes out from position player started, cannot be destroyed, will go thru walls, and follows player with its object to destroy the player.

Extremen for score of 5,000.

DESIGNED AND PROGRAMMED BY:

Alan McNair

STERN GEHT BERZERK!

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

"Bring den Humanoiden zur Strecke!"

"Die Antwort steht auf der Rückseite."

"Angsthase, kämpft doch wie ein Roboter!"

"Der Humanode darf nicht entwischen!"

"Eindringling darf nicht entwischen!"

"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 Video-Spiel 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

- Unübertragbarer 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 Spielen erscheinen die bis dato erzielten 10 höchsten Punktgewinne auf dem Bildschirm.
- Selbst bei ausgeschaltetem Gerät speichert die Informationsdatei 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 mühelos Wartung gewährleistet.
- Hochentwickeltes automatisches Diagnoseprogramm.



SPIELEIGENSCHAFTEN



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



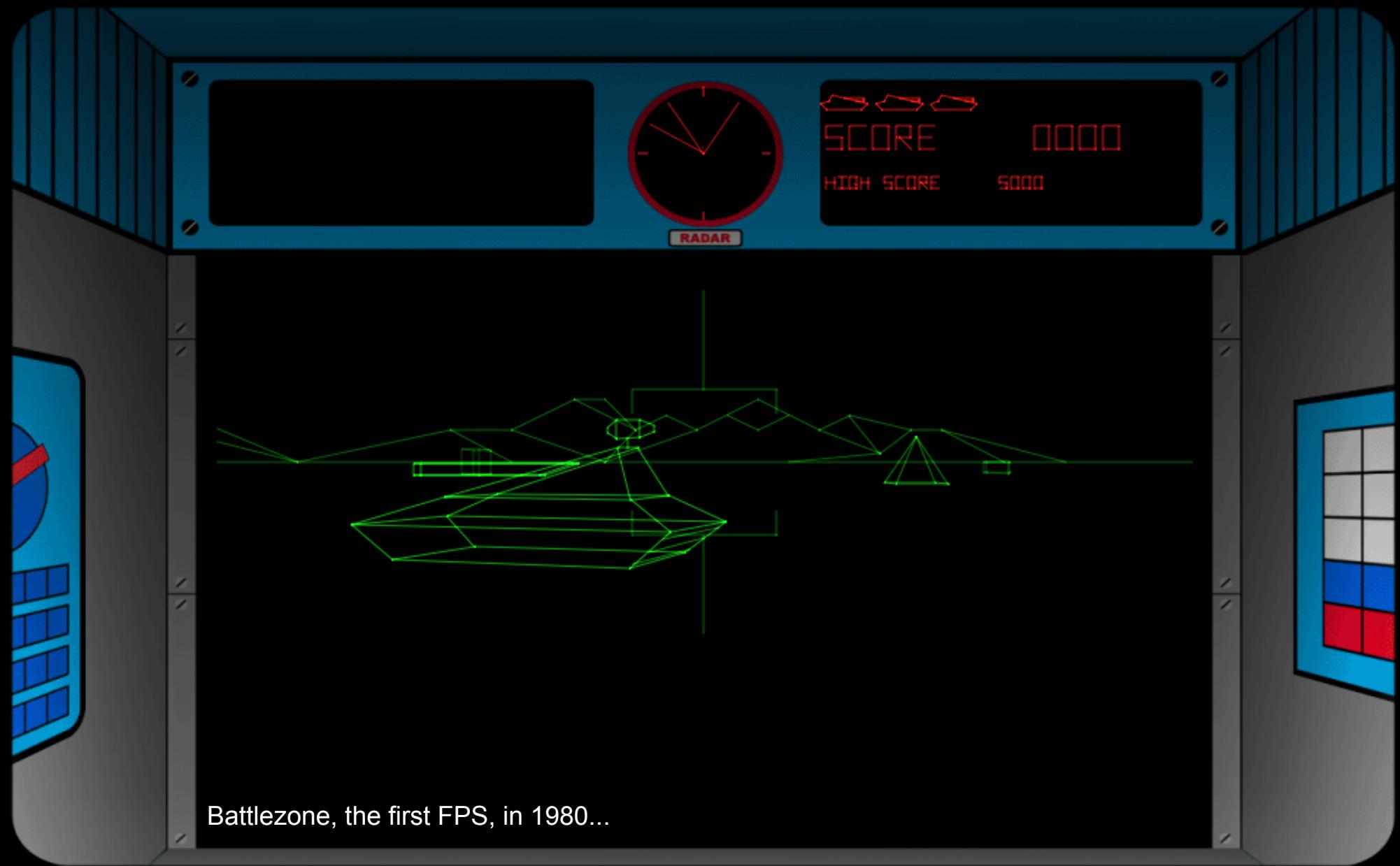
Humanoid vermeidet Roboter durch gekonnekte Betätigung des Daumenhebels, und er vernichtet sie durch Feuerung seiner Geschosse.



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

STERN
BERZERK

„Dieses Spiel haut wirklich jedem 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.

000000



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



...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

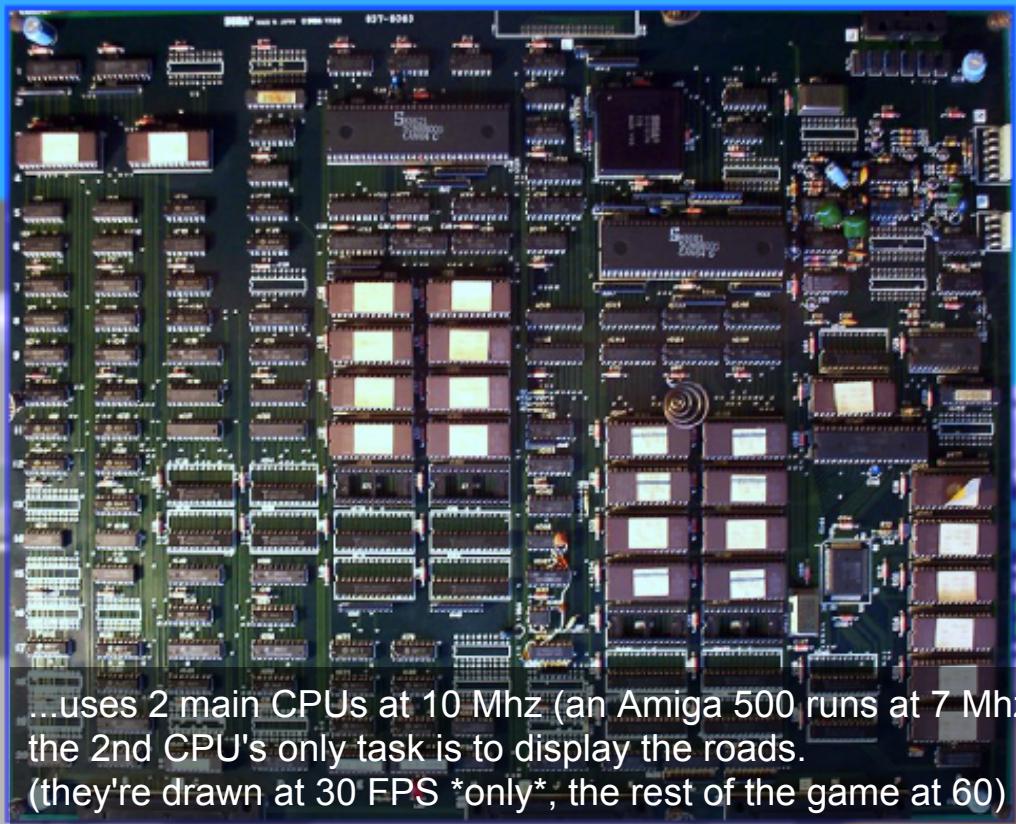
361940

LAP

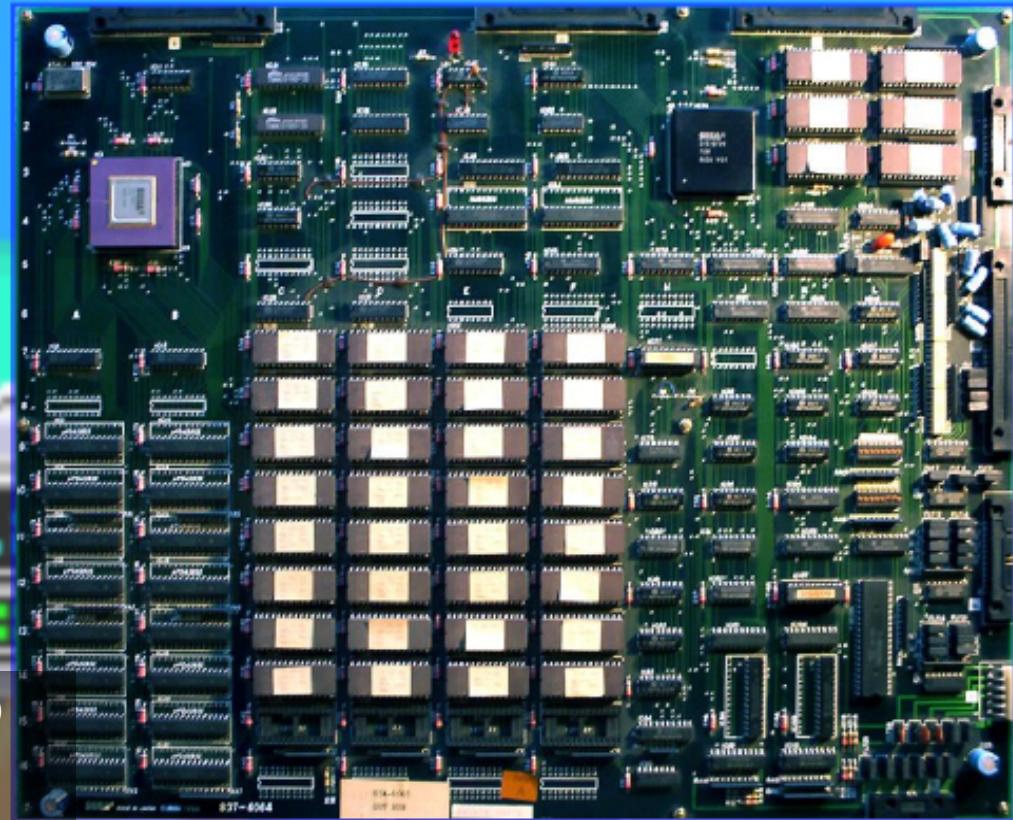
0' 40"95

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)





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

DONKEY KONG

KONG

GYRUSS

XENON

S.R.D.
mission

BOMBACK
TWIN

POLE POSITION

奇々怪界

PHOENIX

BUBBLE
BOBBLE

MR.
DRILLER

PPS.

BLOODBROS.

PLUMA
POP

CAKEMAN

SHOCK
TROOPERS
2nd Squad

Final
Fight

BIG
STRIKER

Arcadia

THE KING OF FIGHTERS™
CHALLENGE TO ULTIMATE BATTLE
2002

THE KING OF FIGHTERS
2001

METAL SLUG 3™

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





They went further and were taking a good game,
then hacking gfx & sound to create a 'new' game
1E066 MONSTERS WORLD

AMI 9122M JL
C012294B-01
C03051
©
PHILIPPINES

137412-105
© ATARI 1984
8551

TAITO 817B
TC0030CMD

COPX-D2
©1992 RISE CORP.
9248 E

ALPHA-8201
44BD1A75
2H15 JAPAN

TAITO A87-01
JPH1021P
126
PS4 38648

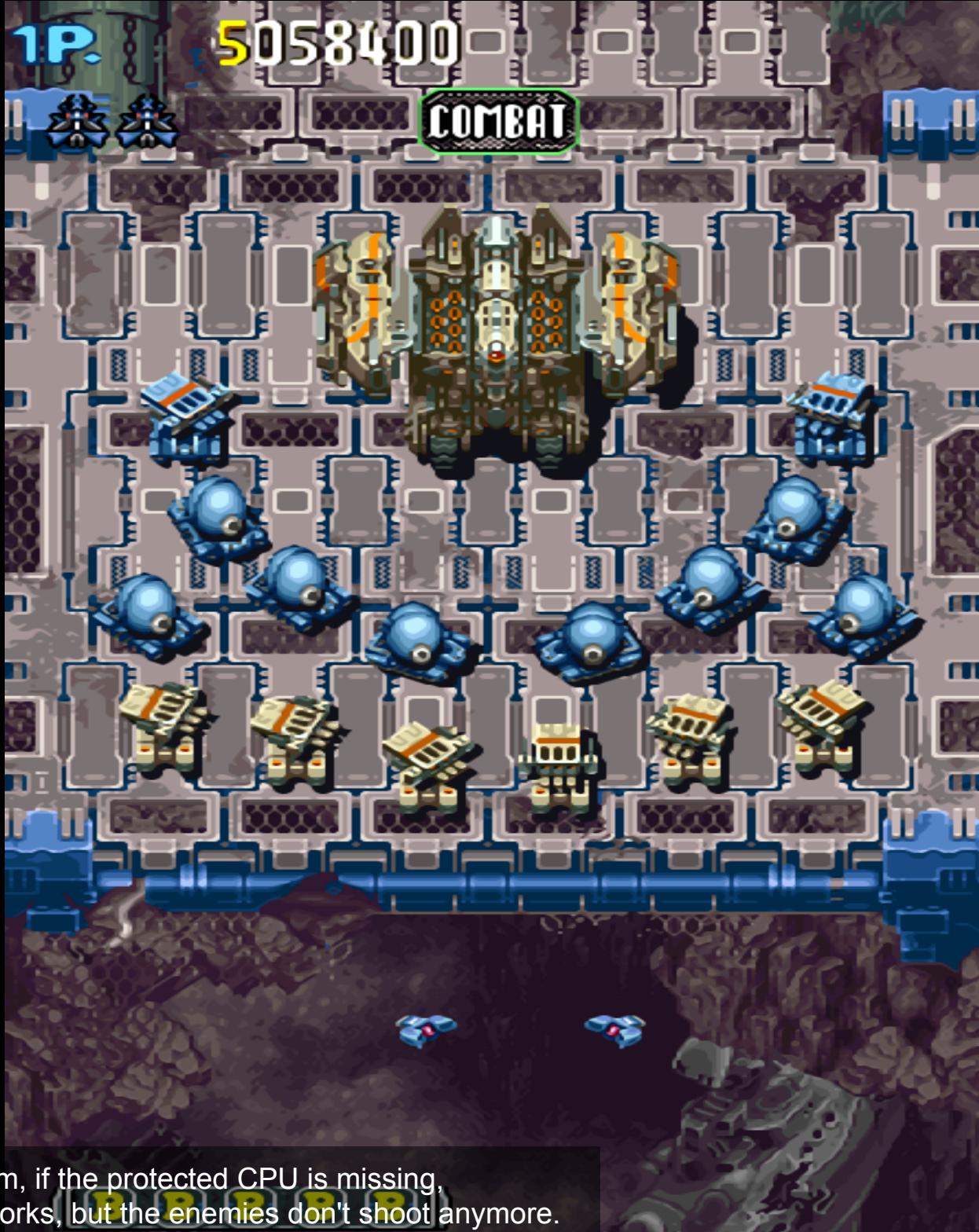
KANEKO® JAPAN
Mermaid
© KANEKO 1988
882011

KANEKO® JAPAN
Beast
© KANEKO 1988
932009

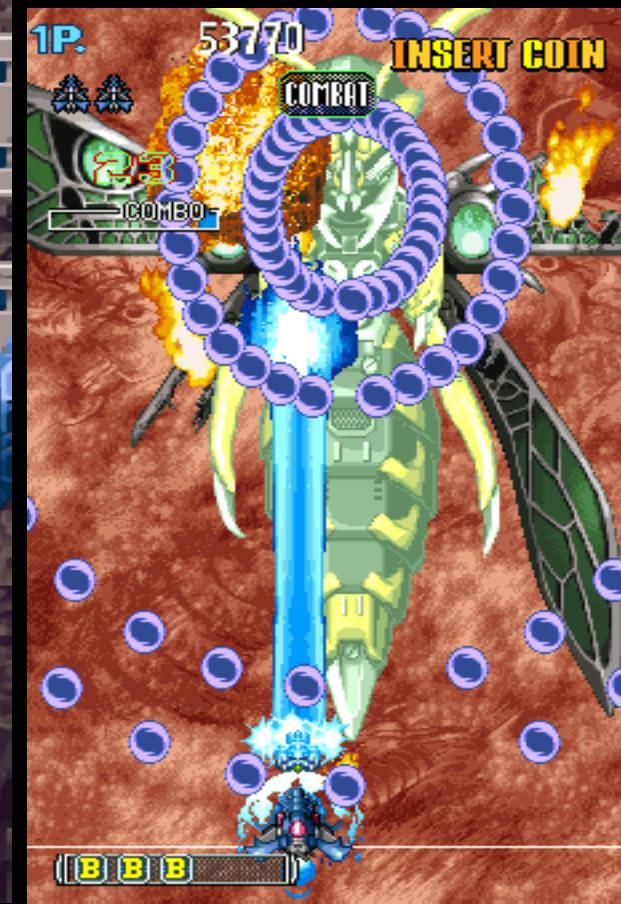
NITRO
TOA PLAN 509
9248NK700

C76
JAPAN
206 448600

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

STAGE 1

TIME

36

SCORE

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

P 0

TIME 2'54"



GAME OVER

STAGE 5



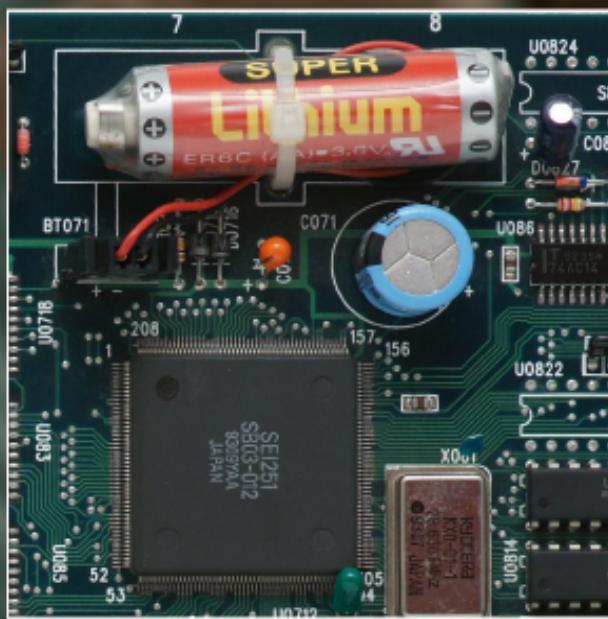
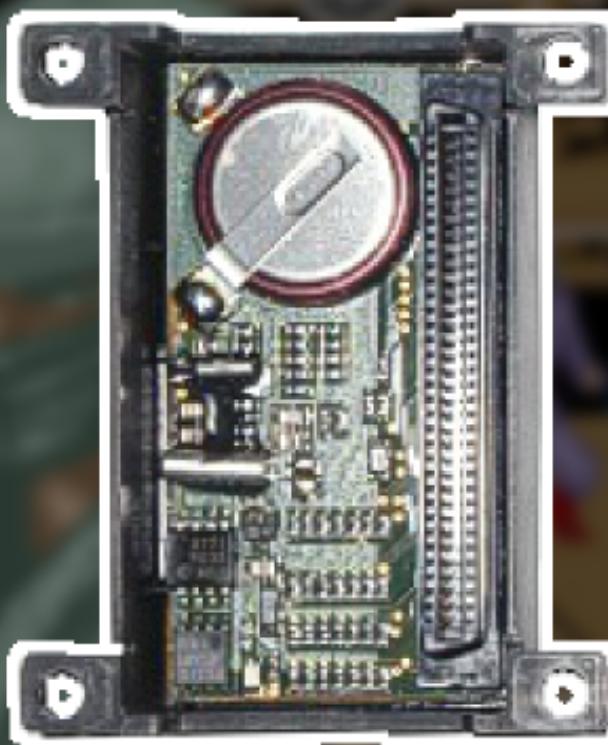
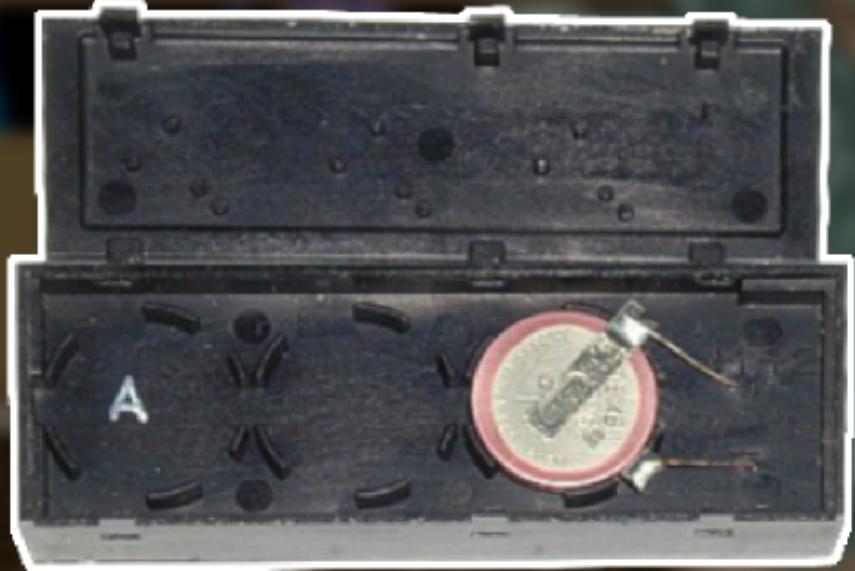
in S.P.Y., collisions are handled by a custom chip:
without it, you can't hurt and cannot be hurt.

POWER

CREDIT 00



POWER



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.



Super Street Fighter® II Turbo HD Remix

[Buy Download](#)

Download Price: \$9.99



★★★★★



Platform: PS3™

Genre: Fighting, Head-to-Head
Fighting

Out Now



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

Sony
Entertainment
Network


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:

[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

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







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

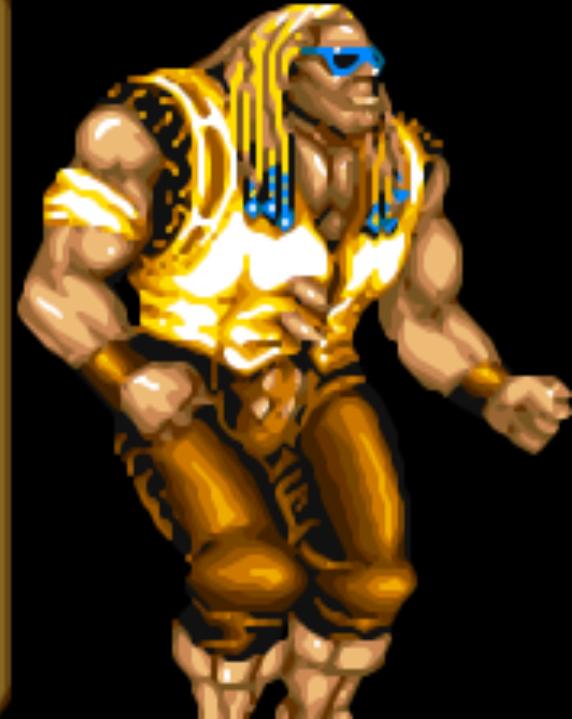
95

DHALSIM



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

SELECT PLAYER



Height ... 5.87ft

Height ... 5.97ft

Height ... 6.64ft

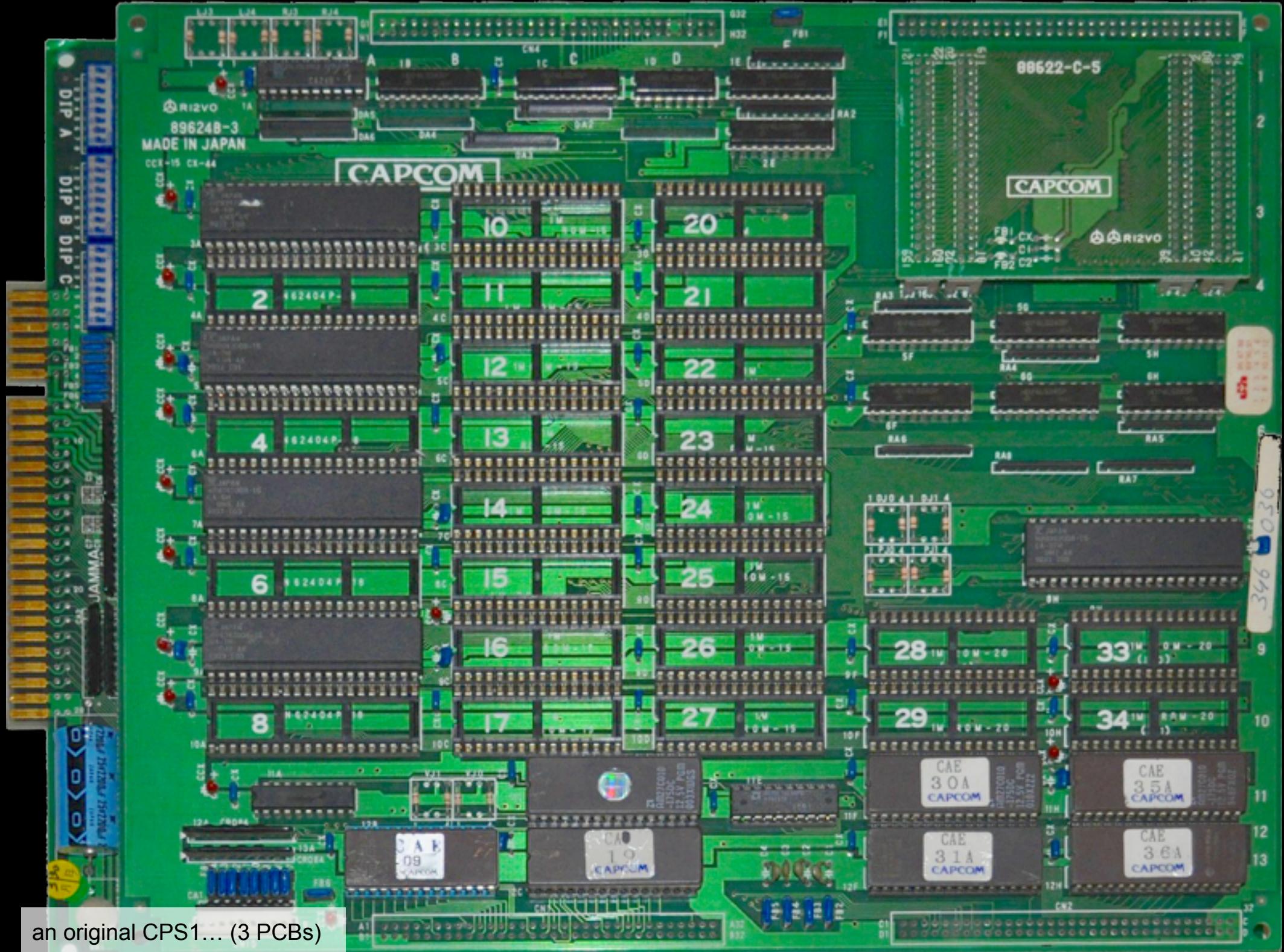
Weight ... 158lb

Weight ... 187lb

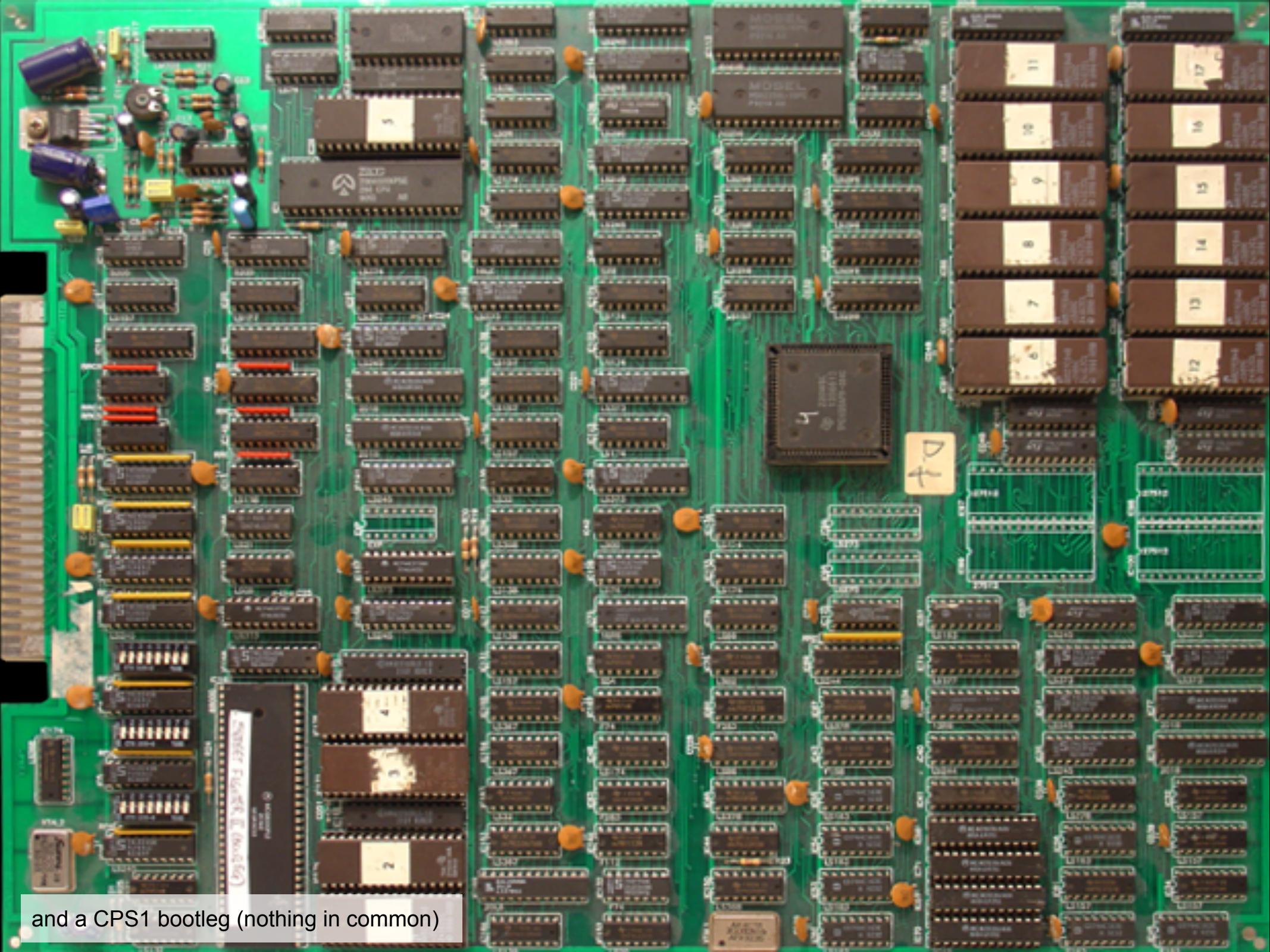
Weight ... 297lb

SELECT PLAYER

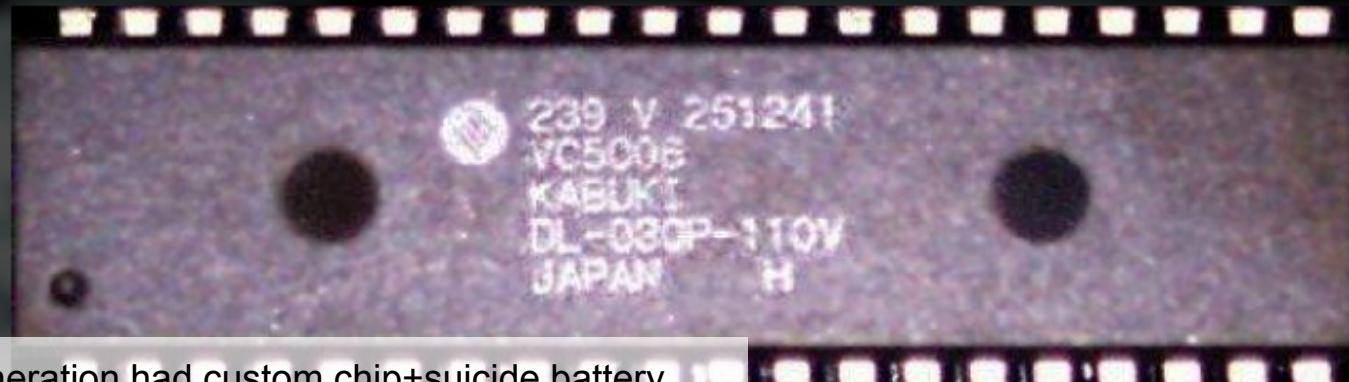
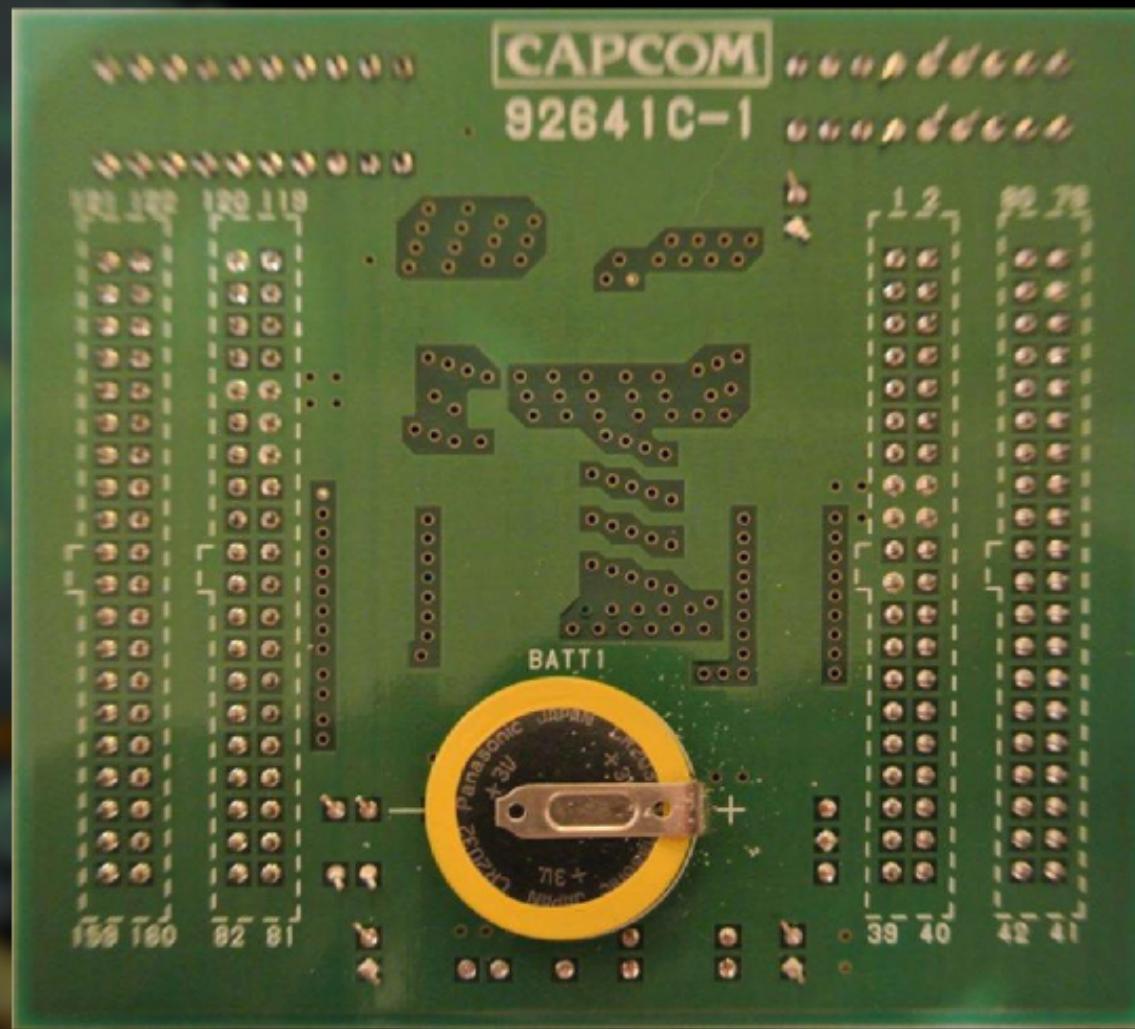
a final fight bootleg, adding extra characters to control.



an original CPS1... (3 PCBs)



and a CPS1 bootleg (nothing in common)



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



...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...



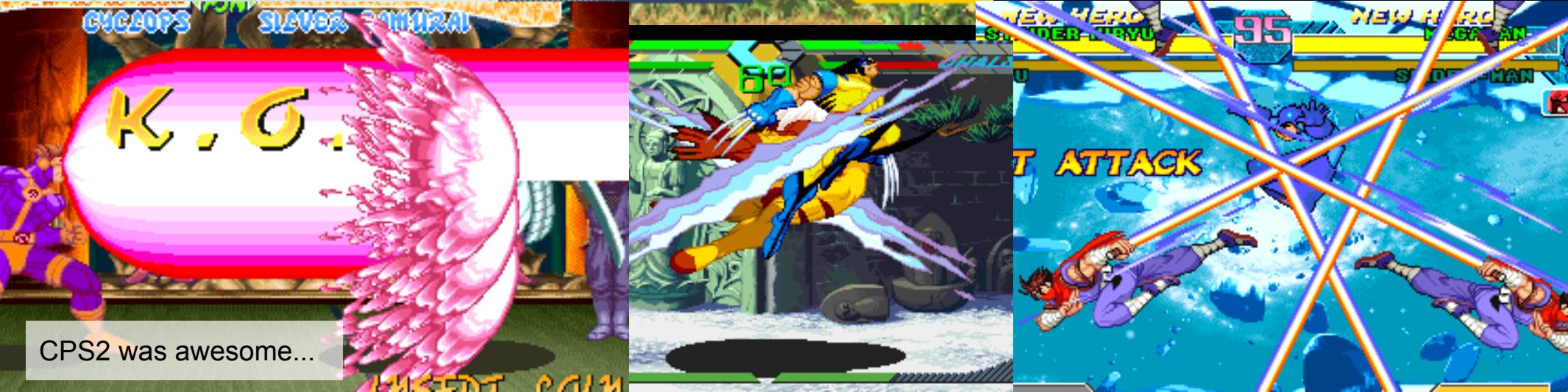
SUPER
STREET FIGHTER II
931005
JAPAN

The New Challengers

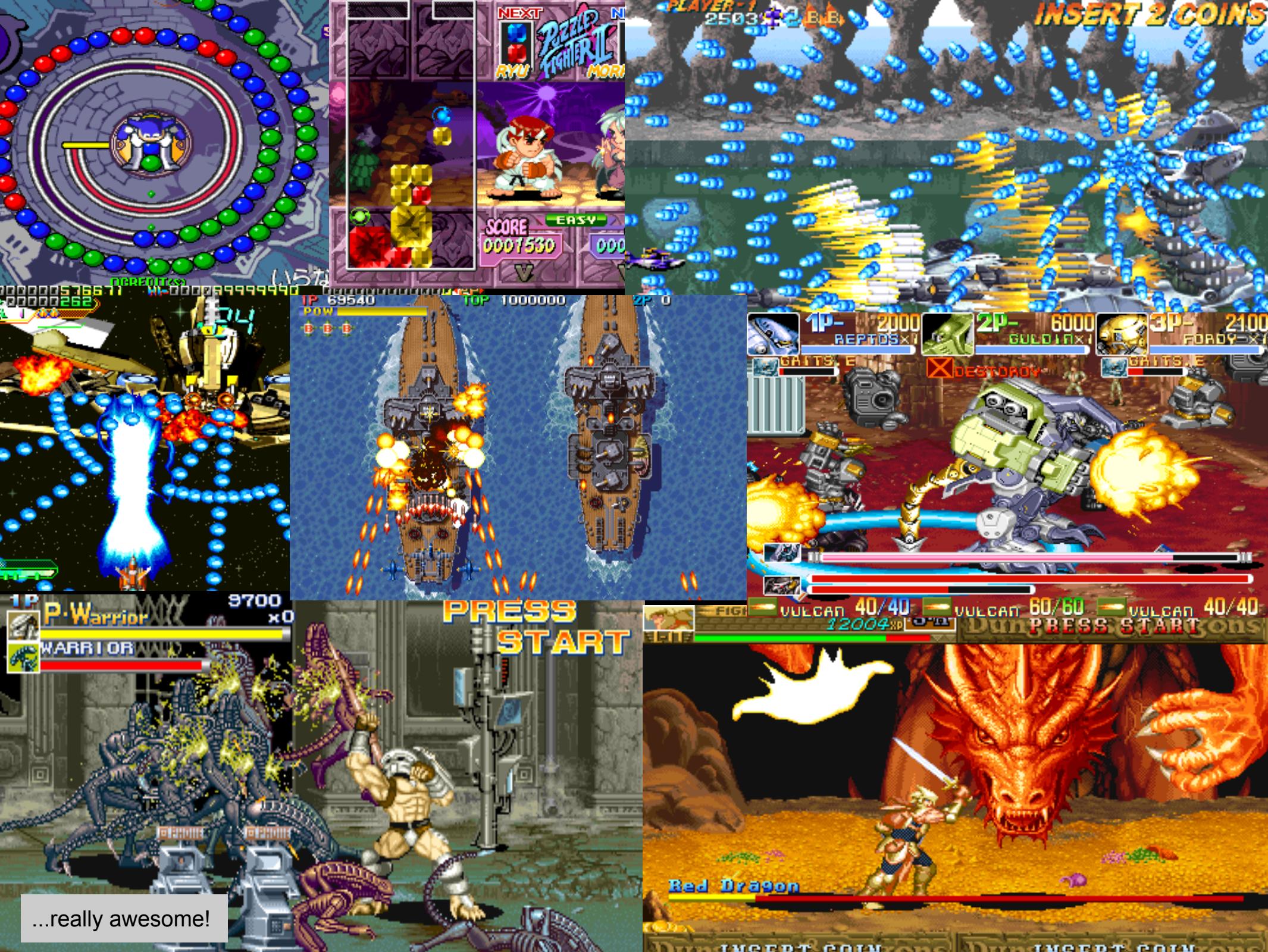
HYPER
STREET FIGHTER II
040202
U.S.A.



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



CPS2 was 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

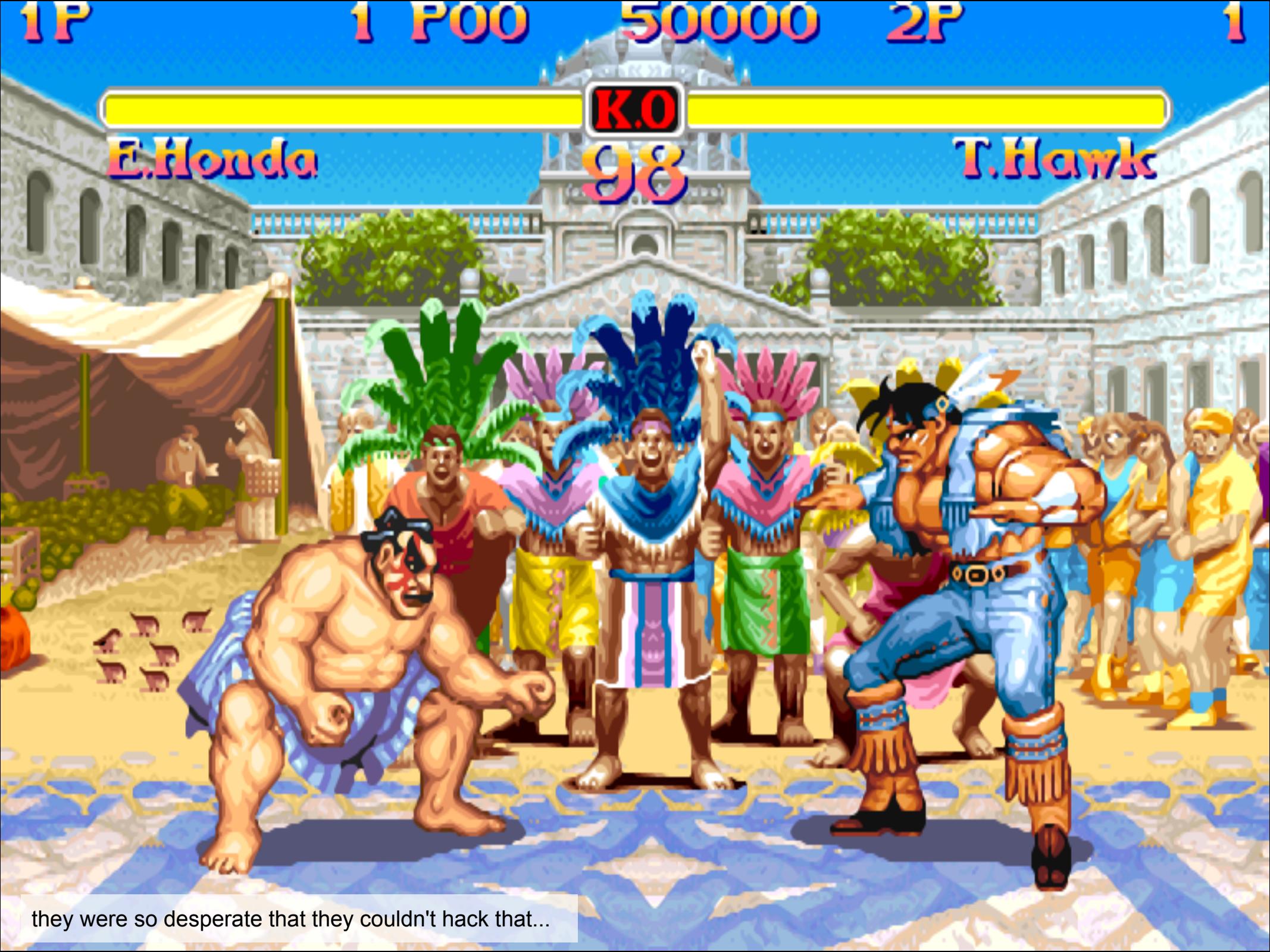
1

E.Honda

K.O

98

T.Hawk



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

1UP

O LEO

50000

INSTER

KO

E Honda

99

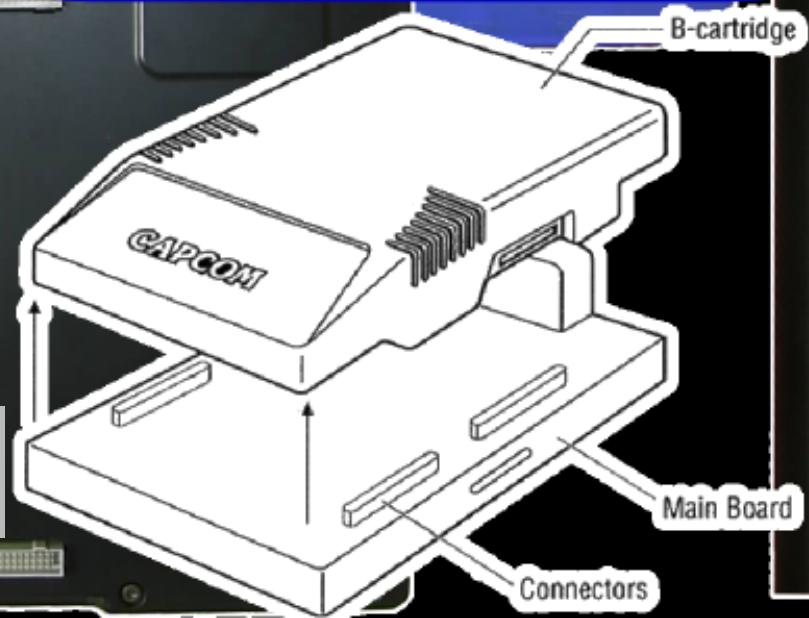
T-Hawk

FIGHT
BATTLE ON



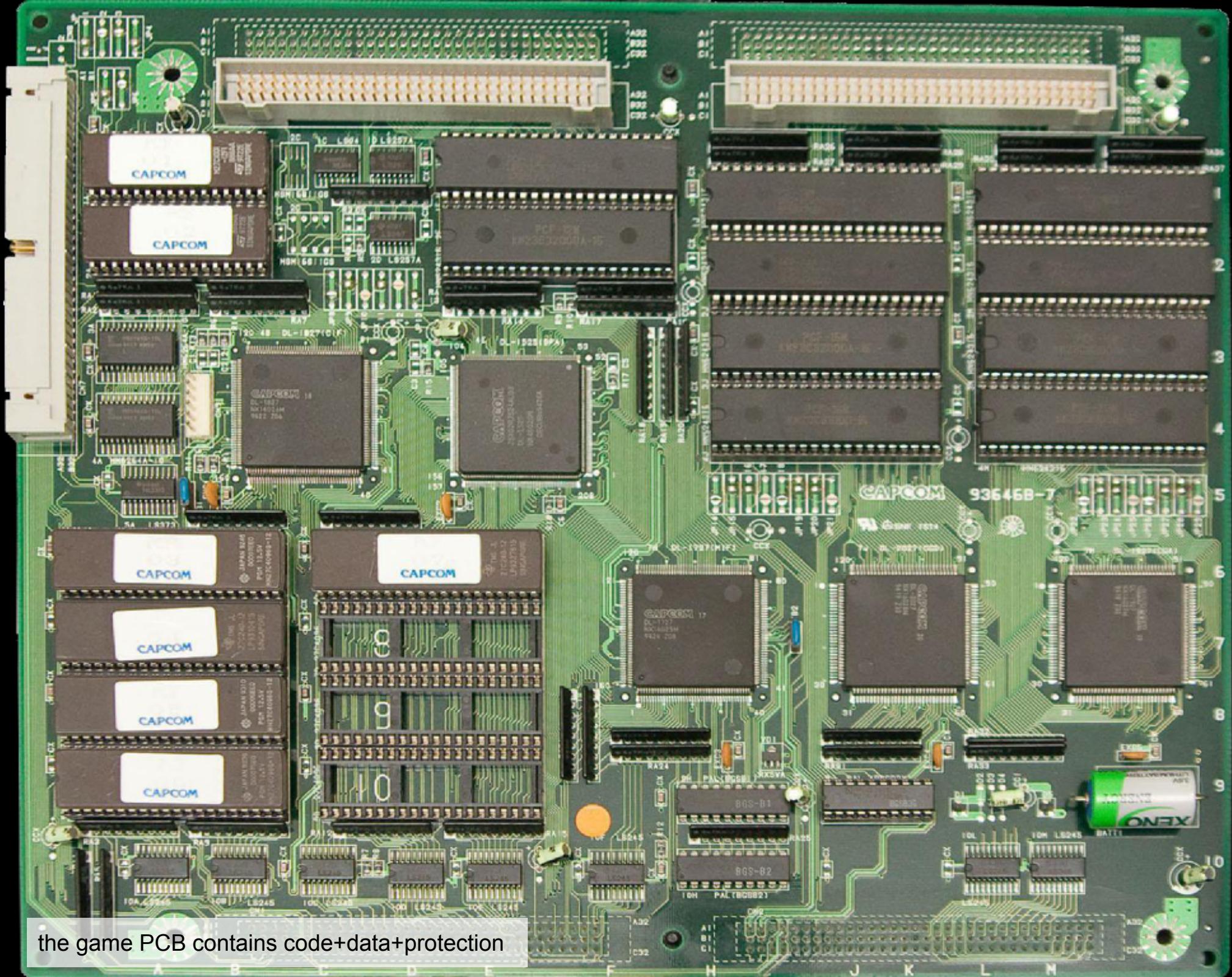
that they hacked a console version into an arcade game (with typo)

CPS II SYSTEM



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)

SRAM

CODE
DATA

GRAPHICS

PALS

BATTERY
ON/OFF

what's in green is in clear,
in red is encrypted.

Code and Data are together.
Code is crypted, data isn't.

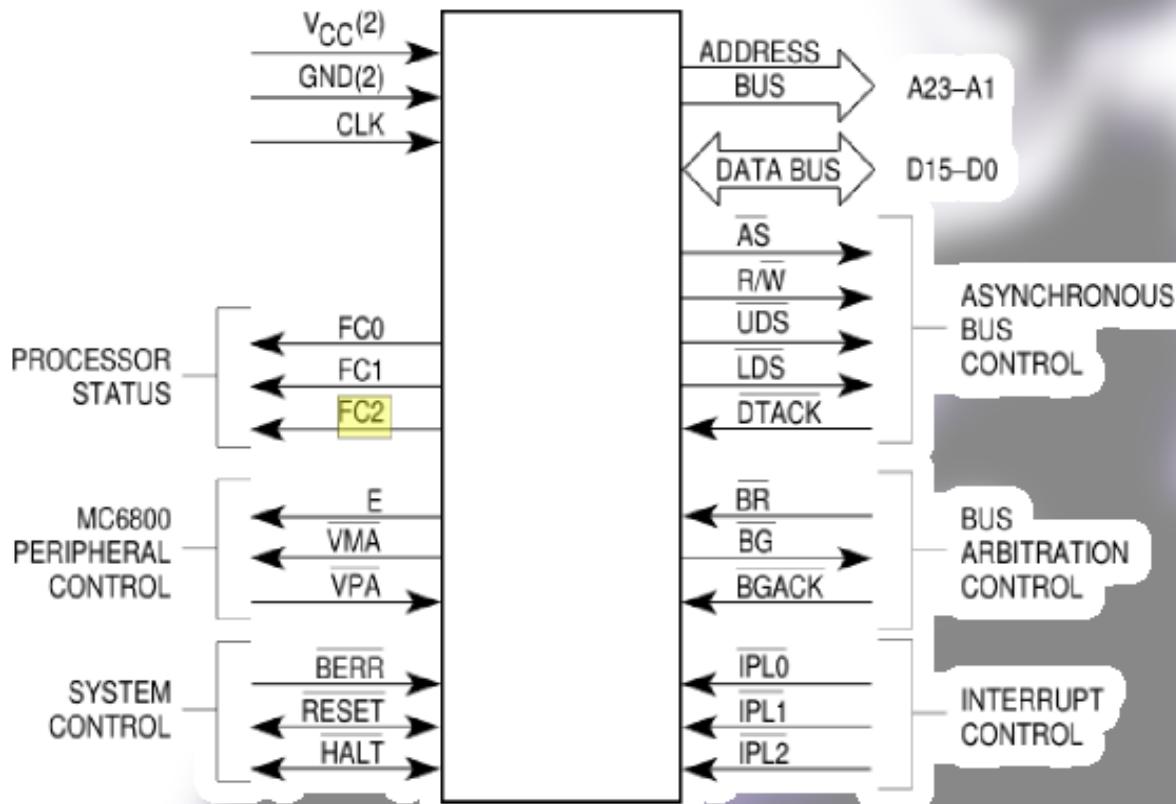


Table 3-3. Function Code Outputs

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 ⁶	Assignment
Hex	Decimal	Dec	Hex		
0	0	0	000	SP	Reset: Initial SSP ²
1	1	4	004	SP	Reset: Initial PC ²
2	2	8	008	SD	Bus Error
3	3	12	00C	SD	Address Error

assigned these numbers.

decryption is made on the fly, during memory fetch.
reset vector (0) requires four words, unlike the other vectors which only require two words, and is located in the supervisor program space.
read standard memory? as is.
read for execution? decrypt.

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

AWESOME
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

Capcom had a major competitor.



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



an exceptional success and longevity !



NEO-GEO

SNK



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

9 5 0 6 0 5

9 5 1 0 2 0

J A P A N

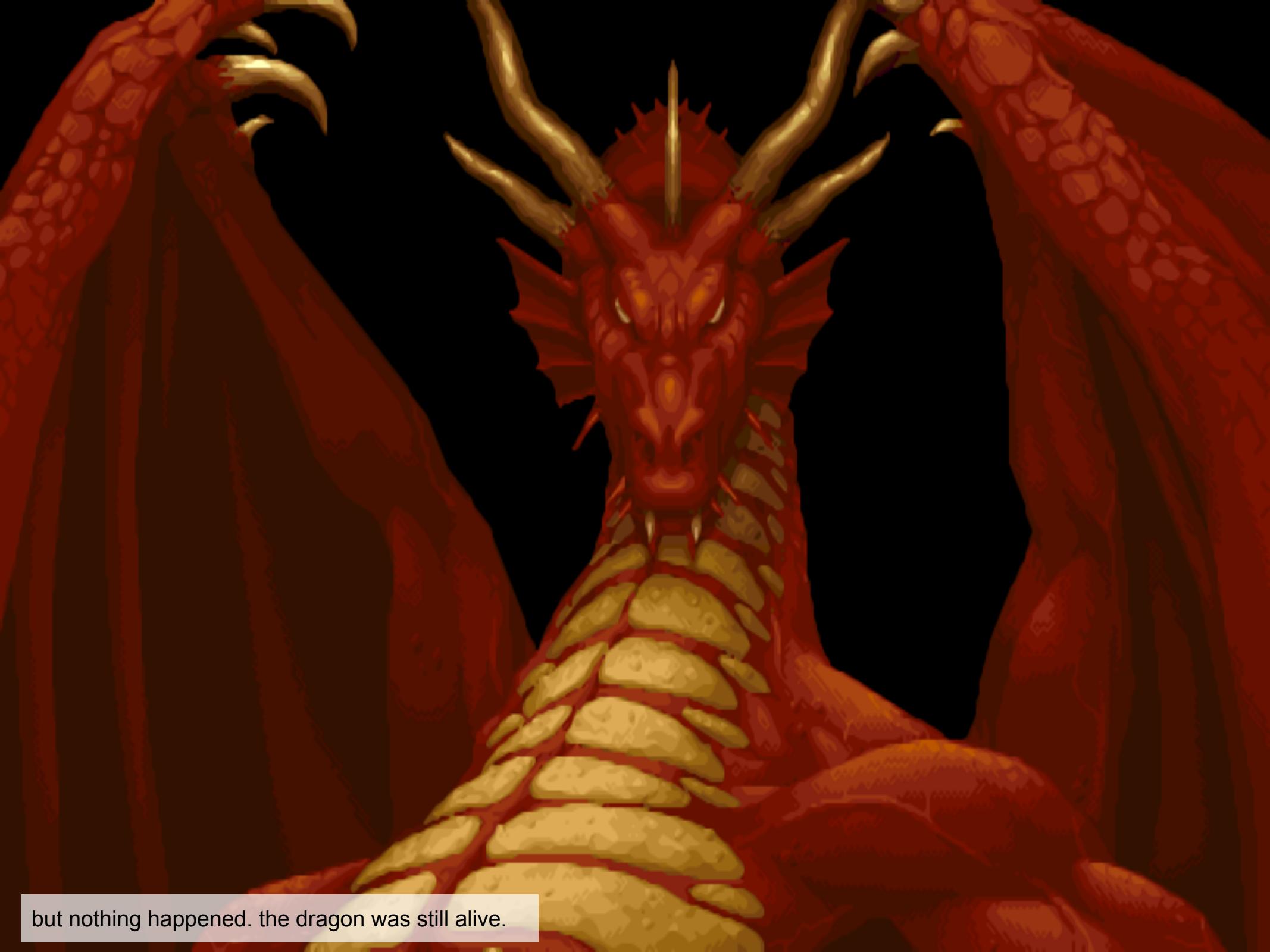
C P S C H A N G E R

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



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





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)

---ILLEGAL INSTRUCTION---

ADDRESS : 7A0A0000

AC ADRS :

R W :

MODE :

FC :

D0 : FFFF4A44 D4 : 00A80158 A0 : 6FC42E65 A4 : 00FFB380
D1 : 00000004 D5 : 0000FFF A1 : 00FF081C A5 : 00000000
D2 : 00080000 D6 : 00000000 A2 : 007082F0 A6 : FFFFAD80
D3 : 00000008 D7 : 00000000 A3 : 00FFB19A A7 : 0000000A
SSP : 00FF081C
SR : 4A44

	+0	+2	+4	+6	+8	+A	+C	+E
00FF8000	0010	0000	0002	0000	0002	0071	0000	0000
00FF8010	0000	0000	0000	0000	5680	0000	0000	9000
00FF8020	92C0	90C0	9100	9160	9140	0000	0000	01DA
00FF8030	000C	01B5	0006	000C	000F	12C2	0000	0000
00FF8040	0000	0000	003F	7000	807D	1234	0040	0010
00FF8050	0000	0000	0000	0000	0000	0000	0000	0000
00FF8060	E021	0FOC	0000	0000	0100	FFFF	FFFF	FFFF
00FF8070	FFFF							

In November 1999, Razoola re-enabled SFZ's internal debugger (first working CPS2 patch !)
→ not blind anymore !



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
Register Direct Addressing Data Register Direct Address Register Direct	EA=Dn EA=An	Dn An
Absolute Data Addressing Absolute Short Absolute Long	EA = (Next Word) EA = (Next Two Words)	(xxx).W (xxx).L
Program Counter Relative Addressing Relative with Offset Relative with Index and Offset	EA = (PC)+d16 EA = (PC)+d8	(d16,PC) (d8,PC,Xn)
Register Indirect Addressing Register Indirect Postincrement Register Indirect Predecrement Register Indirect Register Indirect with Offset Indexed Register Indirect with Offset	EA = (An) EA = (An), An \leftarrow An+N An \leftarrow An-N, EA=(An) EA = (An)+d16 EA = (An)+(Xn)+d8	(An) (An)+ (An) (d16,An) (d8,An,Xn)
Immediate Data Addressing Immediate Quick Immediate	DATA = Next Word(s) Inherent Data	#<data>
when reading relatively to code (PC), memory fetches are actually decrypted ! Sega prevented that, but Capcom failed. → first CPS2 decryption, word by word	EA = SR, USP, SSP, PC, VBR, SFC, DFC	SR,USP,SSP,PC, VBR, SFC,DFC

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

nop

nop

nop

nop

nop

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)	move.l (A0)+, (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,D1

NON BRUTEFORCING

Address : 00000176	Address : 00000176
Encrypted : 363A	Encrypted : E
Nonencrypted : 0080	Nonencrypted : 40

GRAVIS
PC GamePad

Please wait, this will take some time.

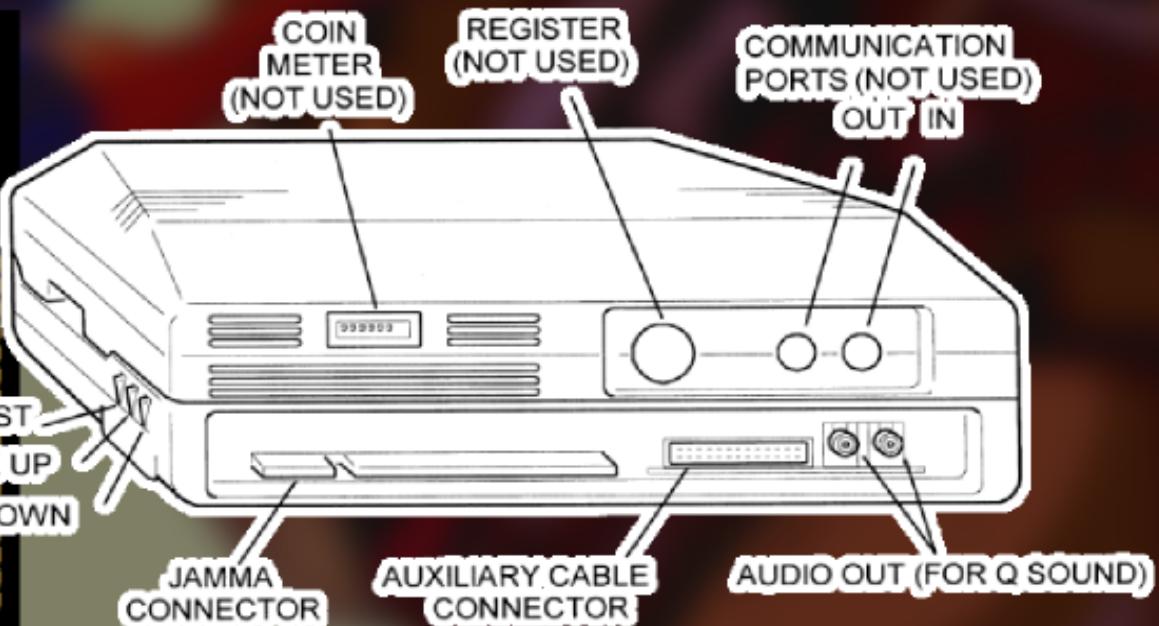
we dumped by connecting the CPS2 to the joystick port of the PC.
ugly, clumsy, slow, but worked !

--- CPS-2 Hacker ---

Use the 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	0000
00FF8010	0000	0000	0000	0000	0000	0000	0000	0000
00FF8020	0080	0000	0100	0160	0140	0000	0000	0000
00FF8030	0000	0002	0000	0000	003F	00C2	0000	0000
00FF8040	0000	7FFF	003F	0000	0000	0000	0000	0000
00FF8050	0000	0000	0000	0000	0000	0000	0000	0000
00FF8060	0000	000C	0000	00FF	0000	0000	0000	0000
00FF8070	0000	0000	0000	0000	0000	0000	0000	0000
00FF8080	0000	0000	0000	0000	0000	0000	0000	0000
00FF8090	0000	0000	0000	0000	0000	0000	0000	0000
00FF80A0	0000	0000	0000	0000	0000	0000	0000	0000
00FF80B0	0000	0000	0000	0000	0000	0000	0000	0000
00FF80C0	0000	0000	0000	0000	0000	0000	0000	0000
00FF80D0	0000	0000	0000	0000	0000	0000	0000	0000
00FF80E0	0000	0000	0000	0000	0000	0000	0000	0000
00FF80F0	0000	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 Register®

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.

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



game over for CPS2 ?

not fully. encryption still unknown, no possible restoration yet.

TOTAL

65200

1P

COM INSERT COIN

45

ROCK HOWARD

MOTARU FUTABA

CREDIT 00

recent NeoGeo games also featured better protection

NEOGEO HACKER by Razoola

Use Joystick and button 1.

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

DO NOT DISTRIBUTE THIS SOFTWARE.

NEOGEO HACKER by Razoola

Start PO 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.

XXXXXX+-----]

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

Use the joystick to scroll and the following buttons for extras:

Button 1 = Speed scroll.
 Button 2 = Jump to bank region.
 Button 3 = To99ie selected bank.
 Button 4 = QUIT.

OFFSET	+0	+2	+4	+6	BANK=0
00000000	0010	F300	0000	0402	.
00000008	00C0	0408	0000	040E	.
00000010	0000	0414	0000	0426	.
00000018	00C0	0426	0000	042E	.
00000020	0000	041A	0000	0420	.
00000028	00C0	0426	0000	042E	.
00000030	0000	0426	0000	0426	.
00000038	0000	0426	0000	0420	.
00000040	00C0	0426	0000	042E	.
00000048	0000	0426	0000	0426	.
00000050	00C0	0426	0000	042E	.
00000058	0000	0426	0000	0426	.
00000060	00C0	0432	0000	0436	.
00000068	0000	2580	0000	042E	.
00000070	0000	0426	0000	0426	.
00000078	00C0	0426	0000	042E	.

NEOGEO HACKER by Razoola

NEOGEO HACKER by Razoola

Use PO 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

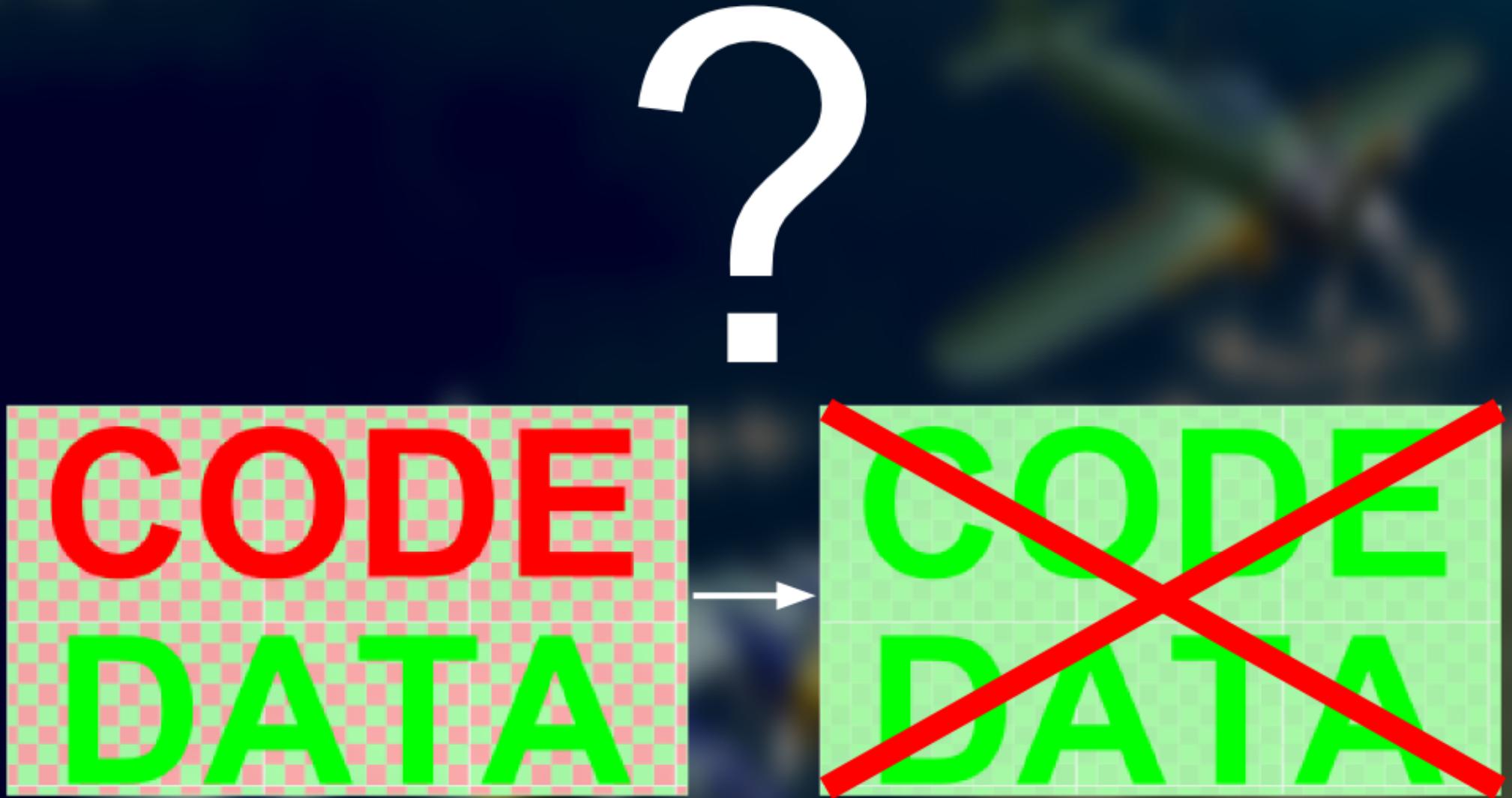
DO NOT DISTRIBUTE THIS SOFTWARE.



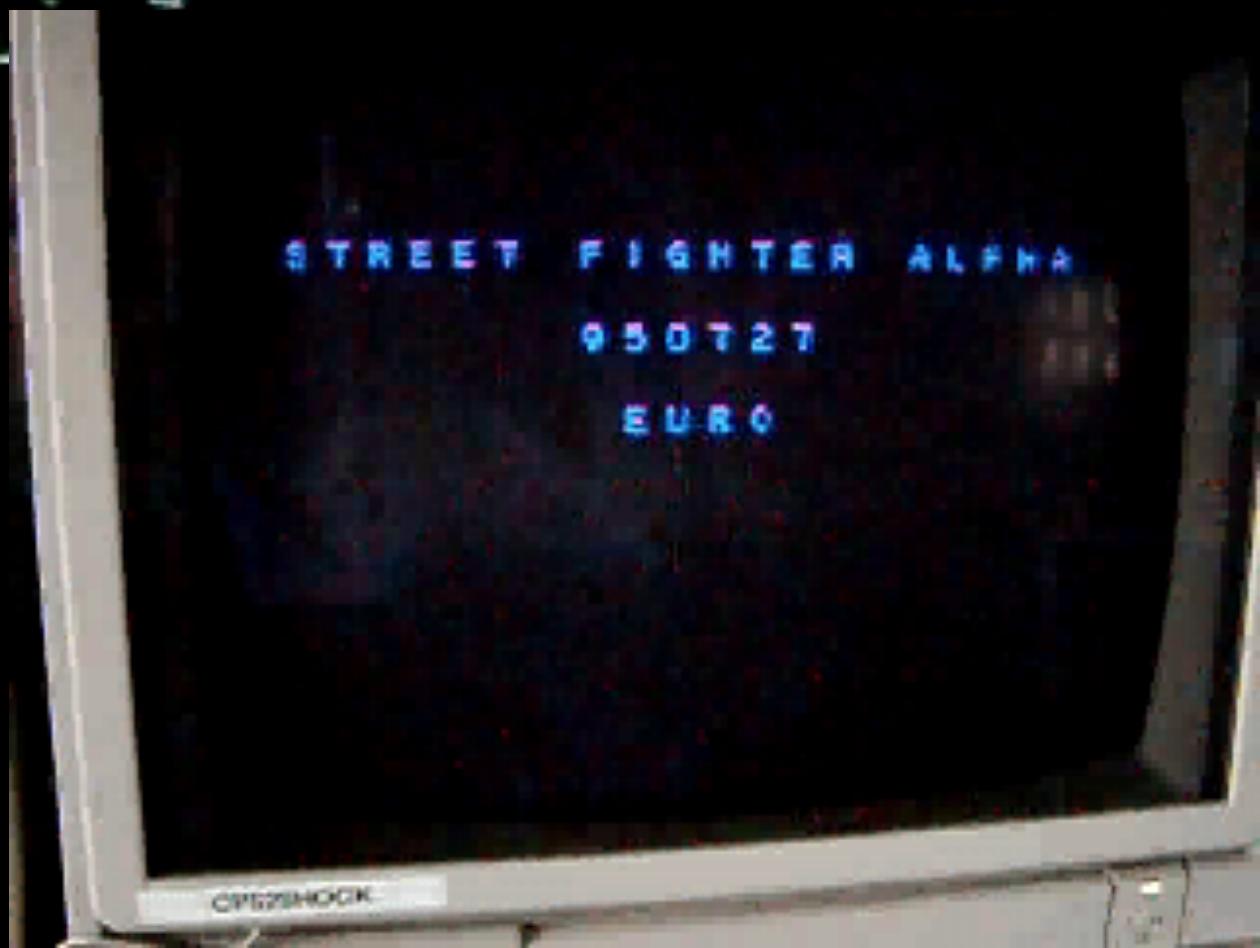
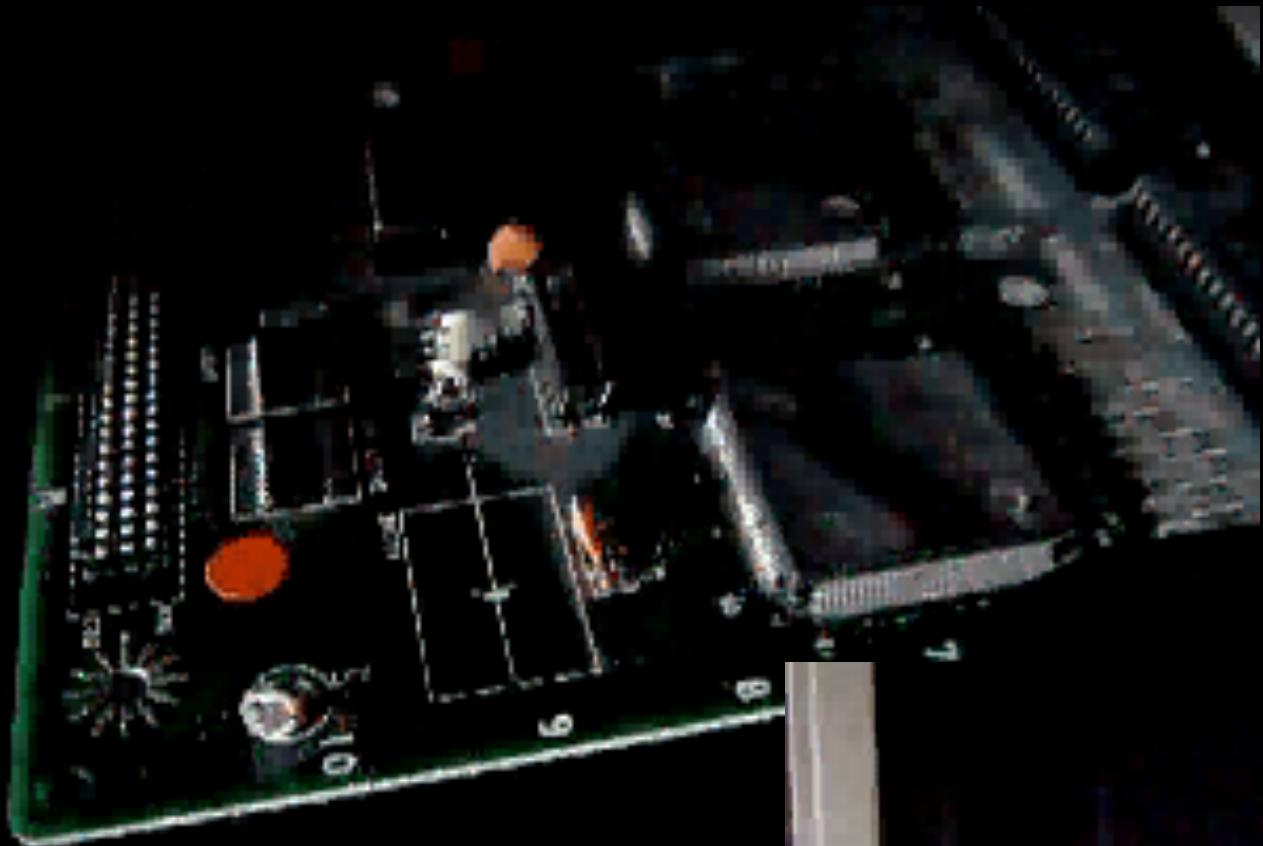
what about dead CPS2 boards ?

CREDIT

0



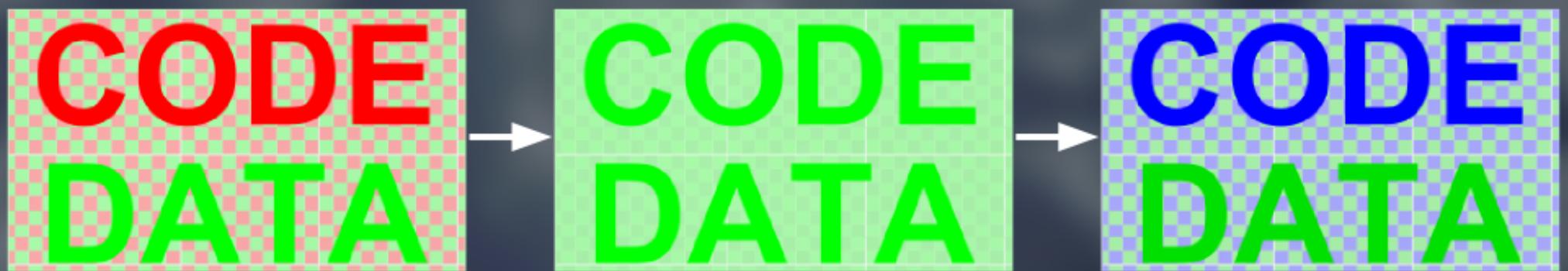
if you put back decrypted code on a dead CPS2,
it still doesn't work.



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

move.w #\\$7000, \$400000.1	move.w #\\$7000, \$fffff0.1
move.w #\\$0, \$8040a0.1	move.w #\\$0, \$8040a0.1
move.w #\\$807d, \$400002.1	move.w #\\$807d, \$fffff2.1
move.w #\\$1234, \$400004.1	move.w #\\$1234, \$fffff4.1
move.w #\\$0, \$400006.1	move.w #\\$0, \$fffff6.1
move.w #\\$40, \$400008.1	move.w #\\$40, \$fffff8.1
move.w #\\$10, \$40000a.1	move.w #\\$10, \$fffffa.1
move.w #\\$f00, \$804040.1	move.w #\\$f00, \$804040.1
cmpi.l #\\$5642194, D0	cmpi.l #\\$5642194, D0
lea (\$6, PC), A4; (\$9d6)	lea (\$6, PC), A4; (\$9d6)
bra \$e82	bra \$e82
move.w #\\$ffc0, \$80010c.1	move.w #\\$ffc0, \$80010c.1
move.w #\\$0, \$80010e.1	move.w #\\$0, \$80010e.1
move.w #\\$9000, \$800100.1	move.w #\\$9000, \$800100.1
move.w #\\$9080, \$800102.1	move.w #\\$9080, \$800102.1
move.w #\\$90c0, \$800104.1	move.w #\\$90c0, \$800104.1

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

Q SOUND RAM = GOOD

ERRORS FOUND ON GAME BOARD

(C) RAZOOLA, WWW.CPS2SHOCK.COM

CAPCOM PHOENIX EDITION

> REGION SETUP <

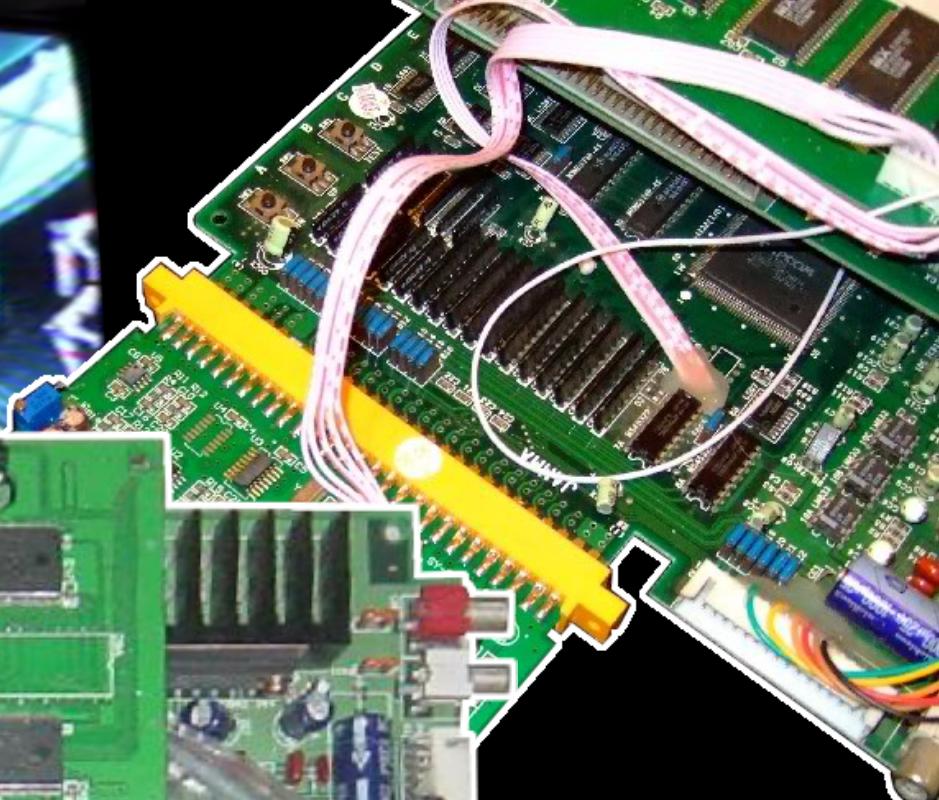
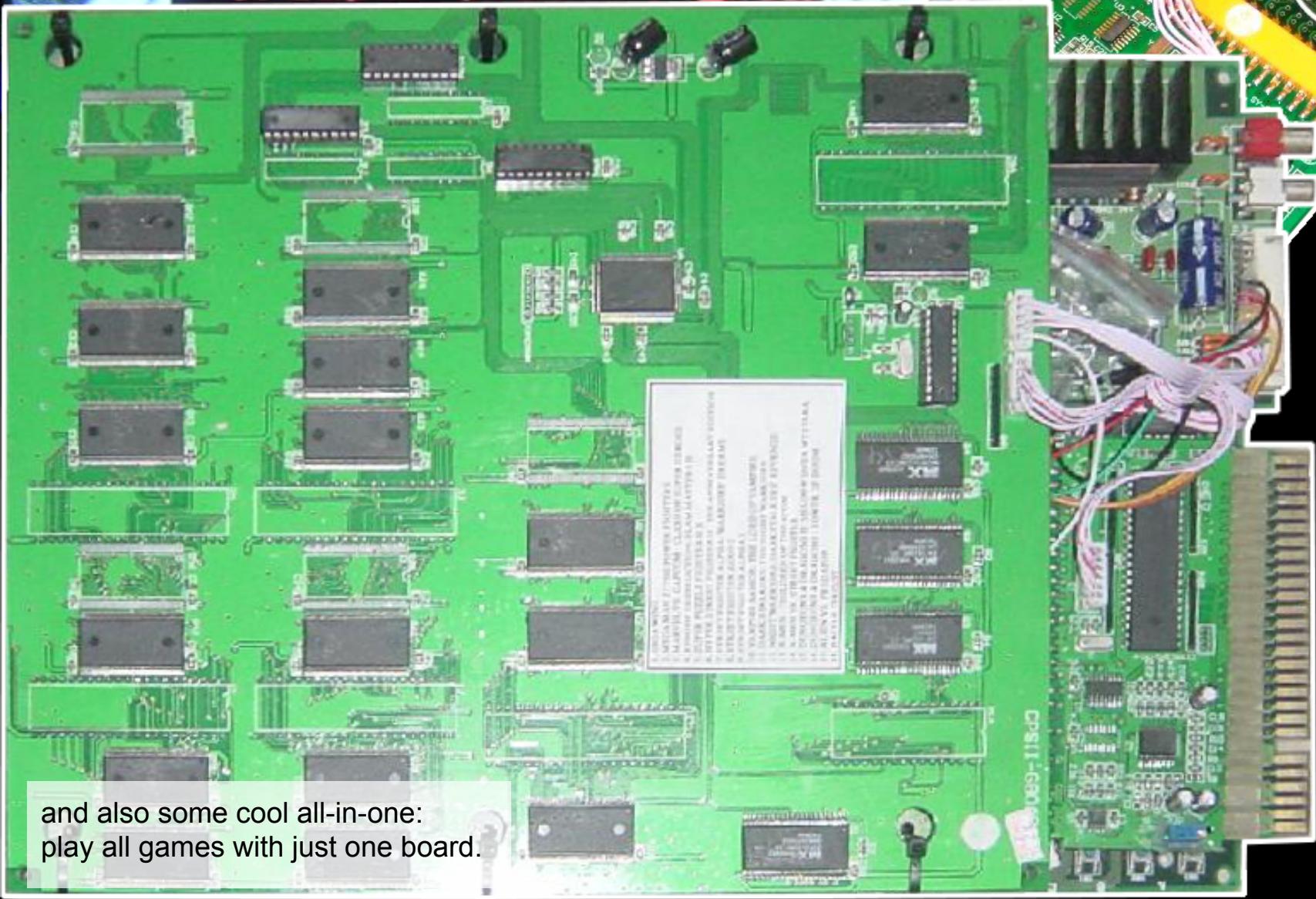
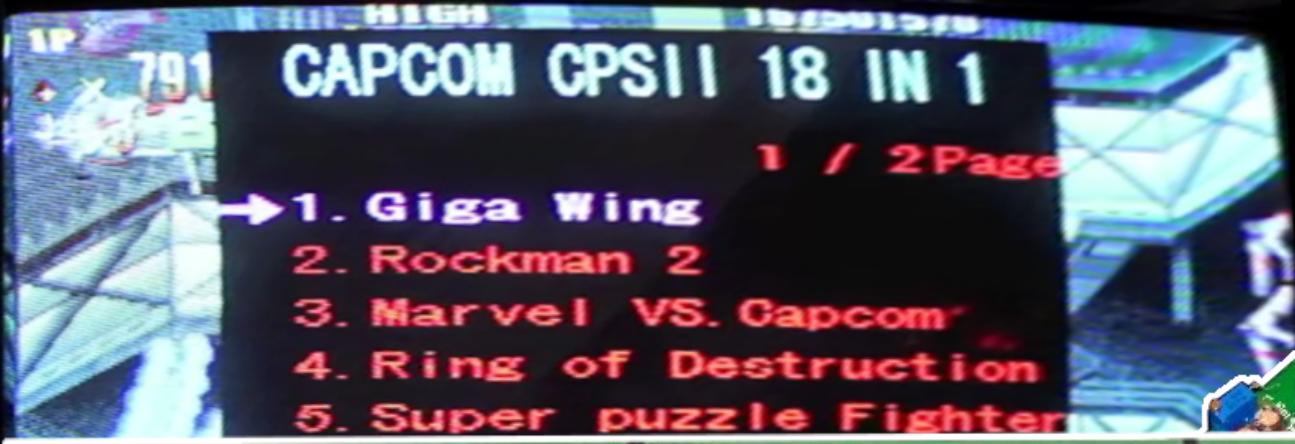
JUKEBOX PLAYER

START GAME

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



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



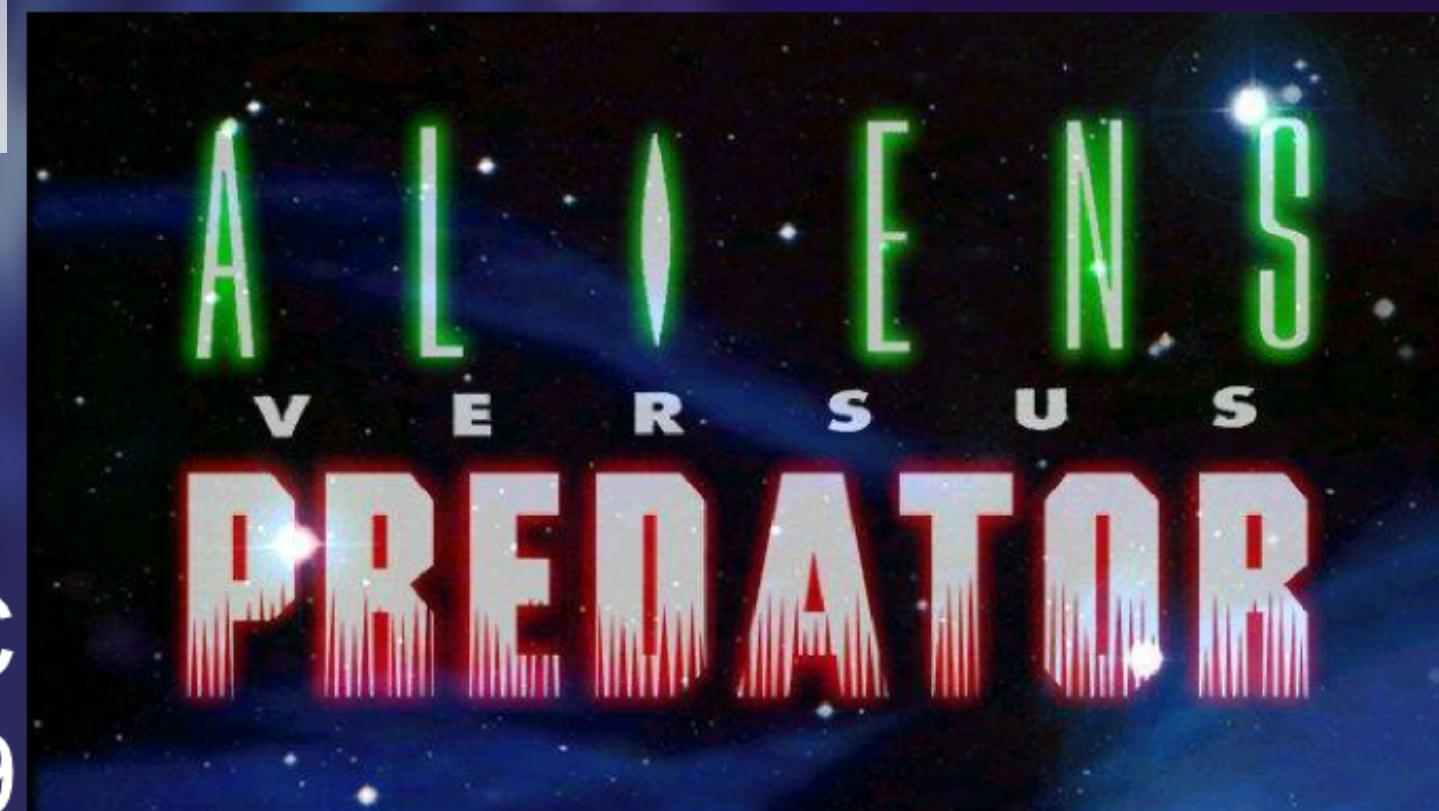
PC, 1999

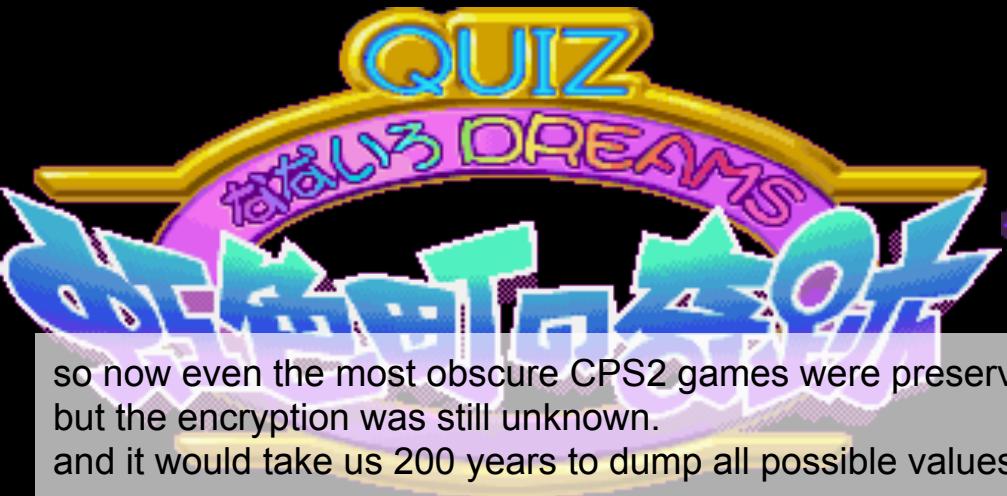
CPS2
1994



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





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

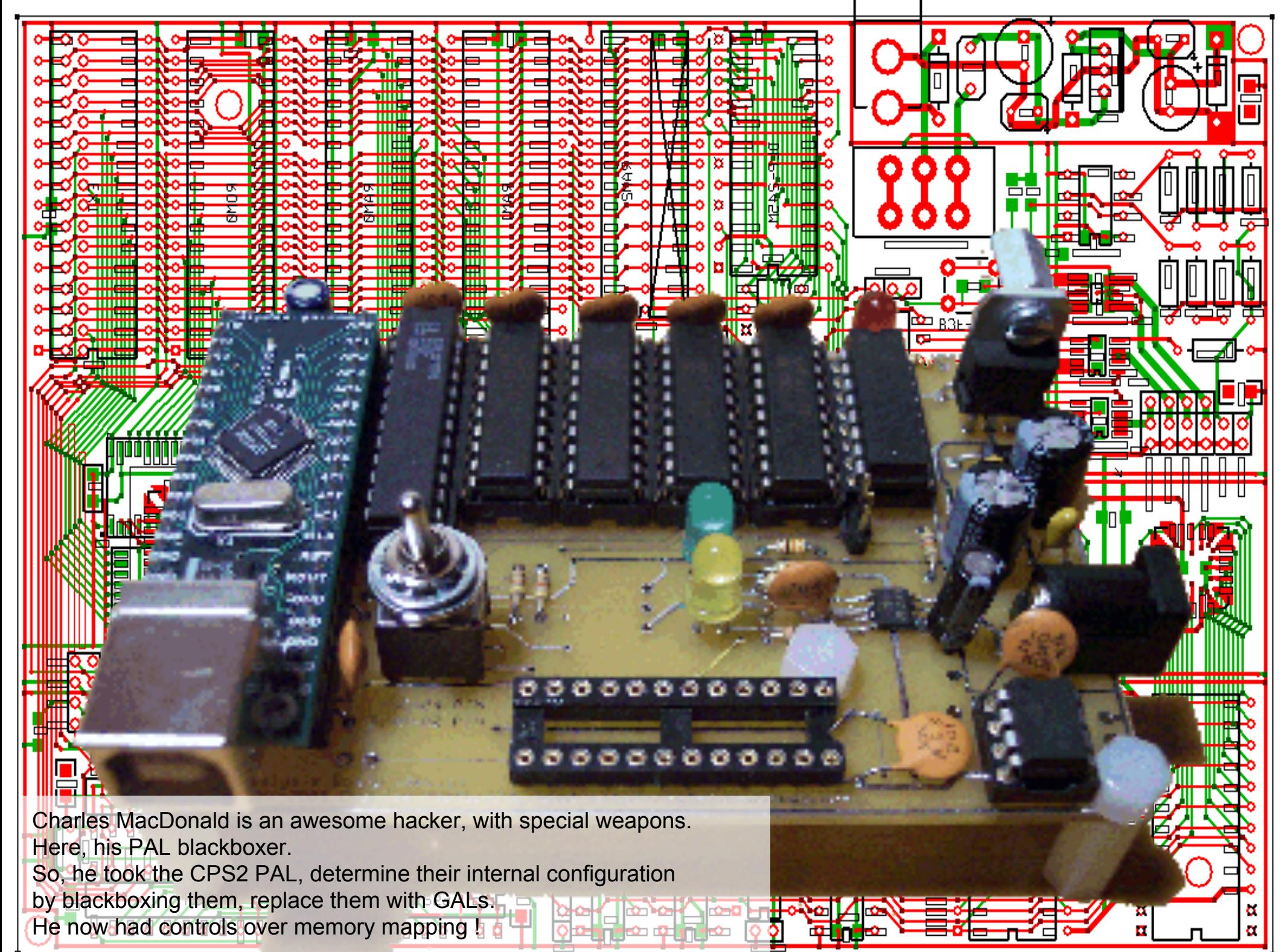
51

Special

Special



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

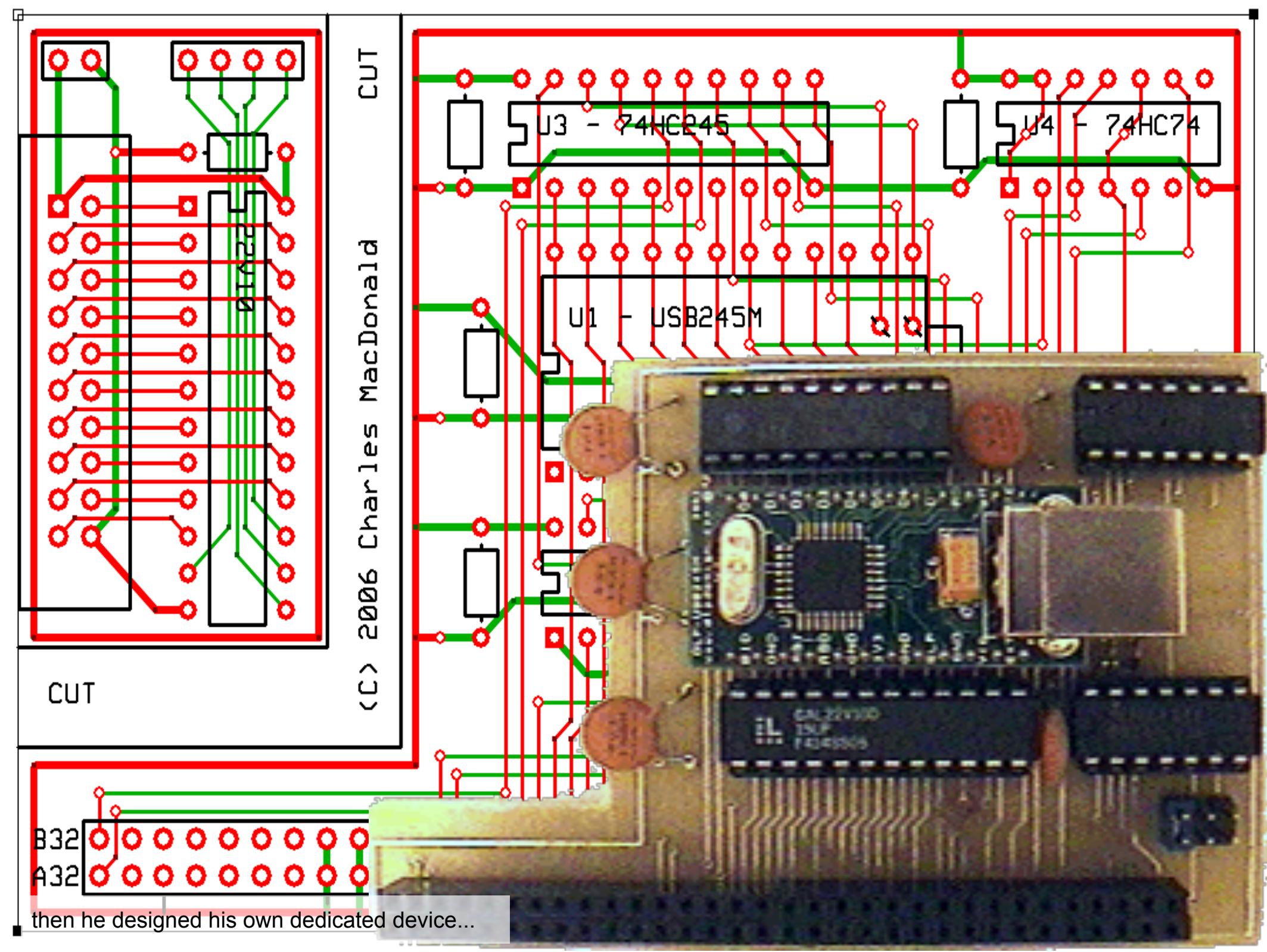


Charles MacDonald is an awesome hacker, with special weapons.

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 !



CPS-2 USB Loader
CPS 2000-2005 Charles MacDonald
URL: [HTTP://csm128.mmunews.com](http://csm128.mmunews.com)
ID: 00FF0000
SP: 00001684



to dump CPS2 directly via its expansion port, to USB !!!

He could dump the 8 Gb set in 17h.

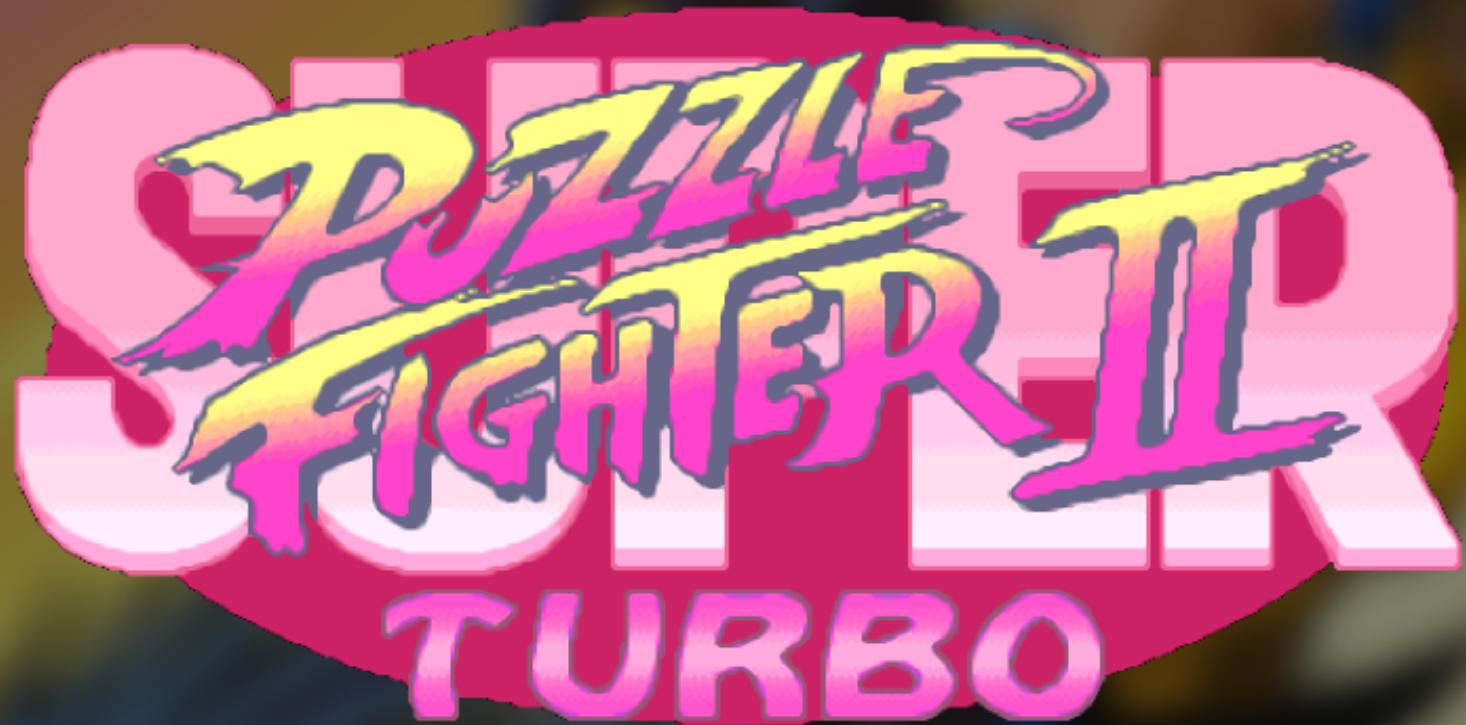
He did that for several games. but that wasn't enough to understand the algorithm.....

CONTINUE?
04

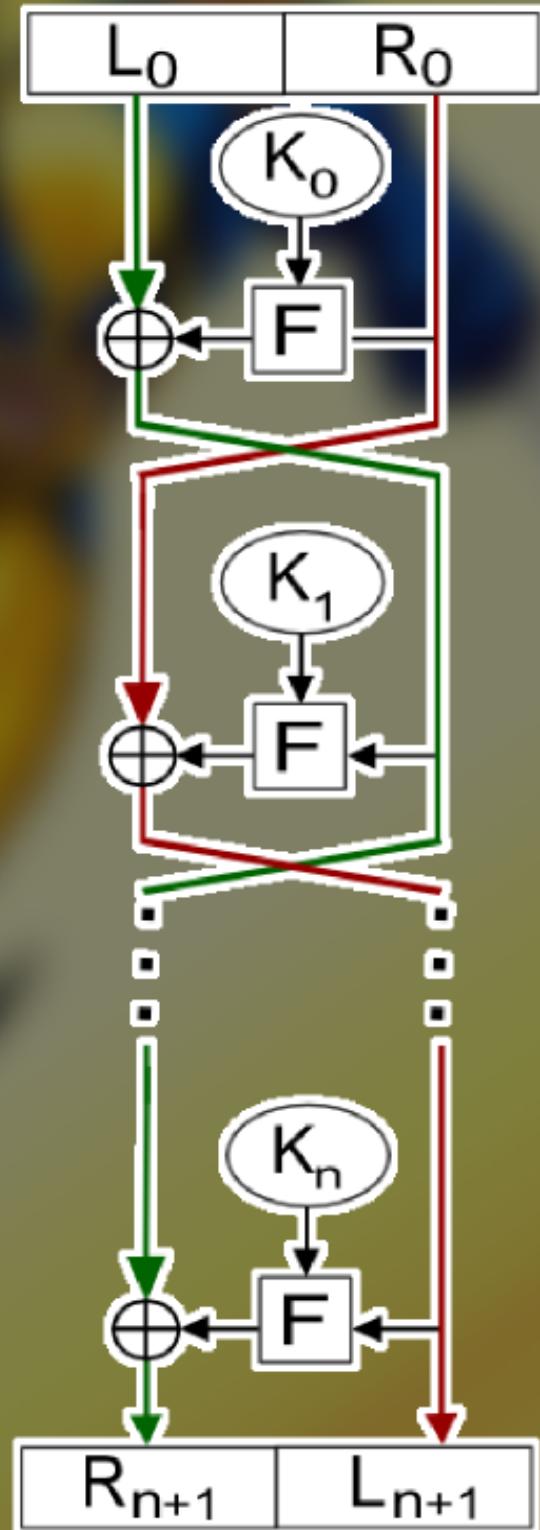
CONTINUE?
04



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



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
Q SOUND	RAM OK

3. SOUND & VOICE TEST

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. SOUND & VOICE TEST

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

30

MIN ++++++ MAX

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 !

EXIT = 1P & 2P START

~Epilogue~

UNENCRYPTED VERSION

DEBUGGER

UNENCRYPTED RANGE

ADDRESSING MODE

KEY LEAK

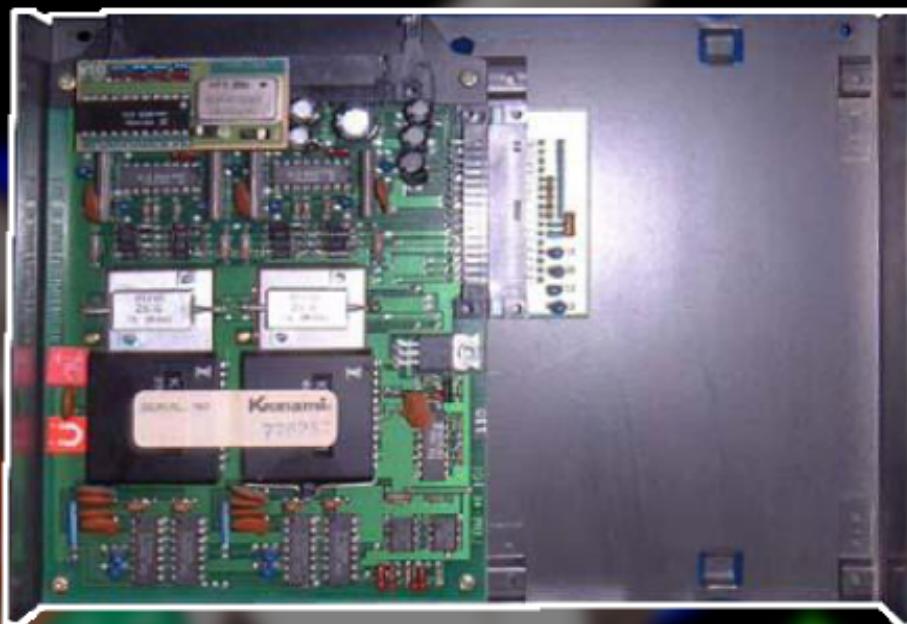
CLUMSY HACKS
JOINT EFFORT
MANY CONTRIBUTIONS

SUCCESS



AWESOME VICTORY

and overall, an awesome victory !



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

WARMING UP NOW



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®

© SEGA 1989

SCORE**LIFE**

800

SCORE**LIFE**

400



it's one of the first split-screen multiplayer FPS

**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

Charles MacDonald

<http://cgfm2.emuvie.ws.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

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

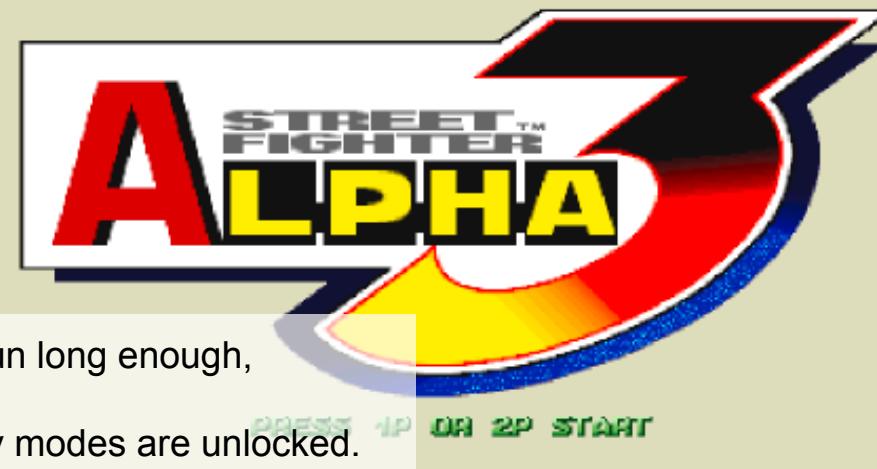
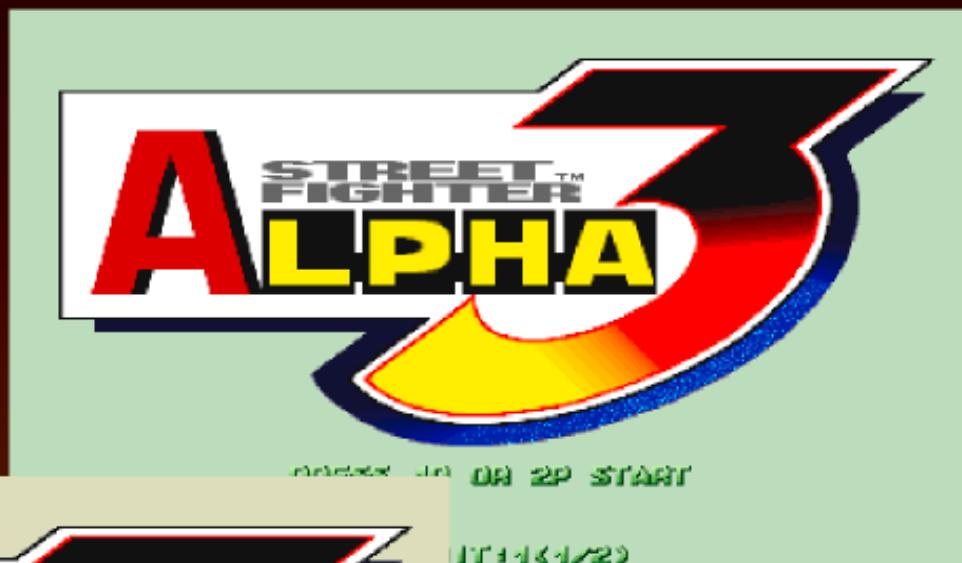
06800

Ryu

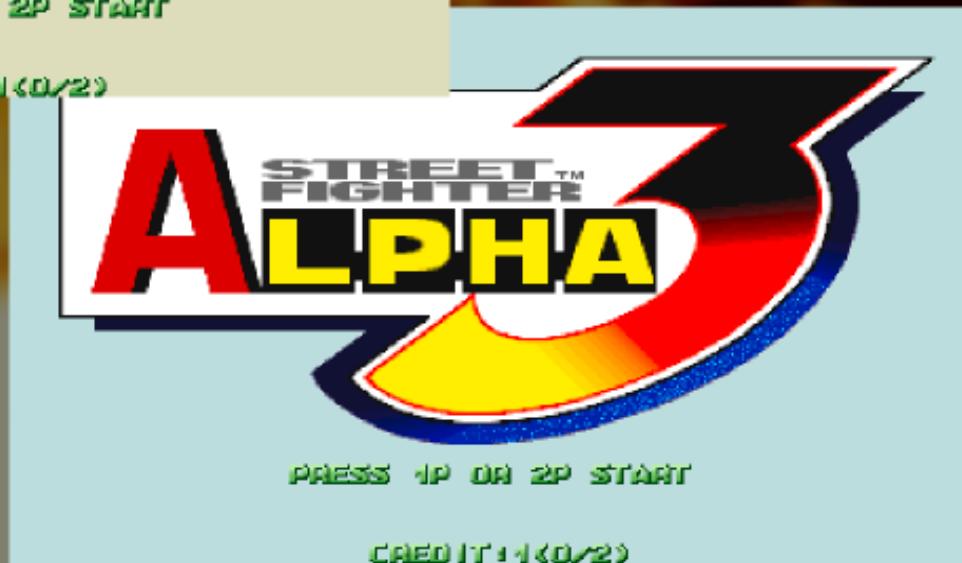
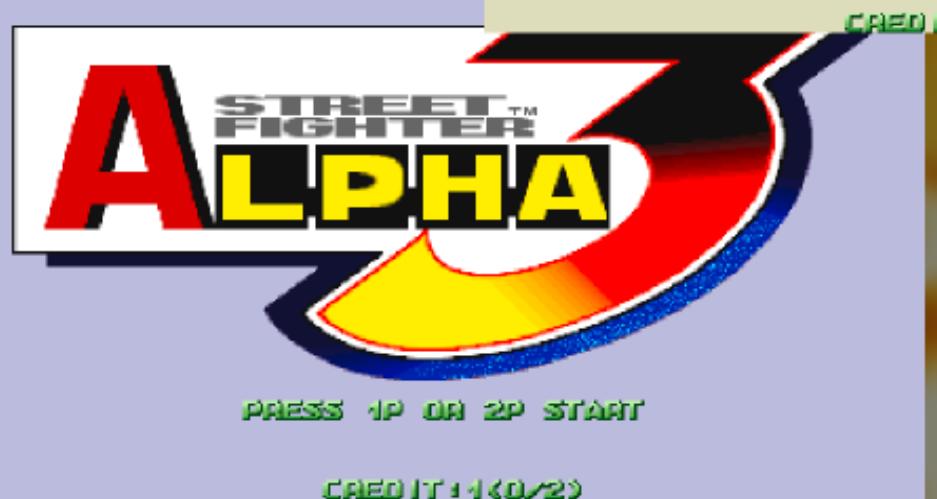
25



some bonus ?

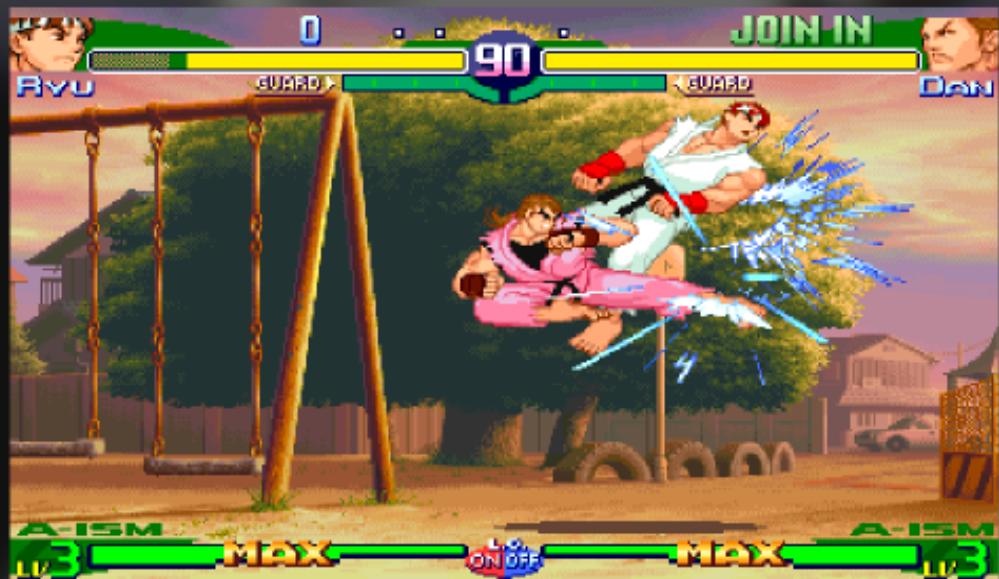


SFA3 has a time lock: if you let it run long enough,
some special modes are unlocked.
the title background tells how many modes are unlocked.





extra characters, extra playing modes



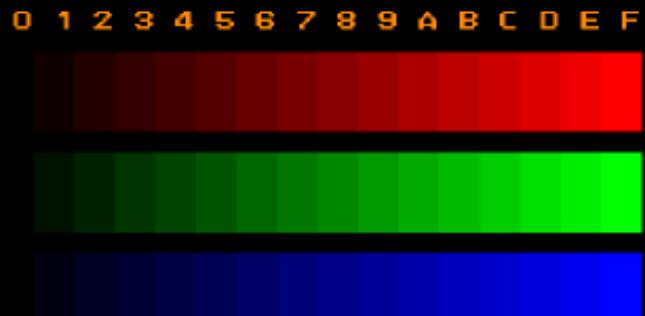
1 . I N P U T T E S T

SERVICE TEST	0	0
COIN START	1P 0	2P 0
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



P1: LK MP U (S+LP)

P2: HK MP

TRADITIONAL FIGHT BEGINS

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

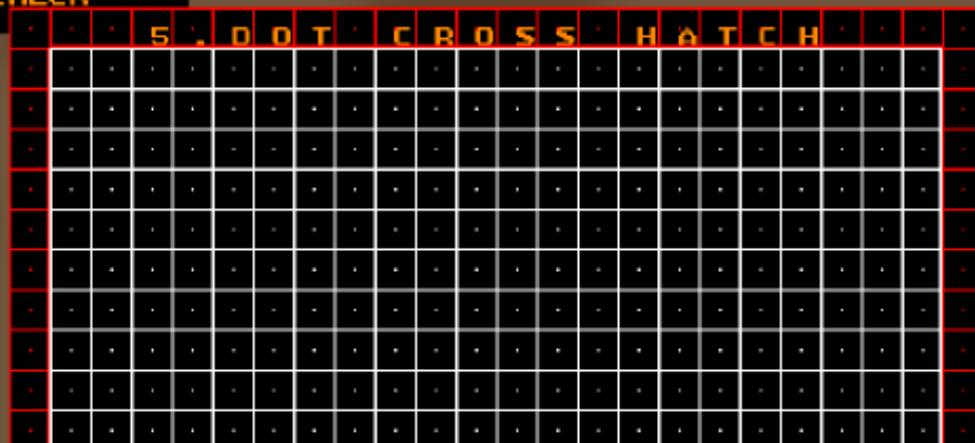
COIN	COUNTER	000036
SERVICE	COUNTER	000000
FREEPLAY	COUNTER	000000

P1: L R D U (S+LP)

P2: R D HK LP

ENJOY NEW FIGHTING STYLE

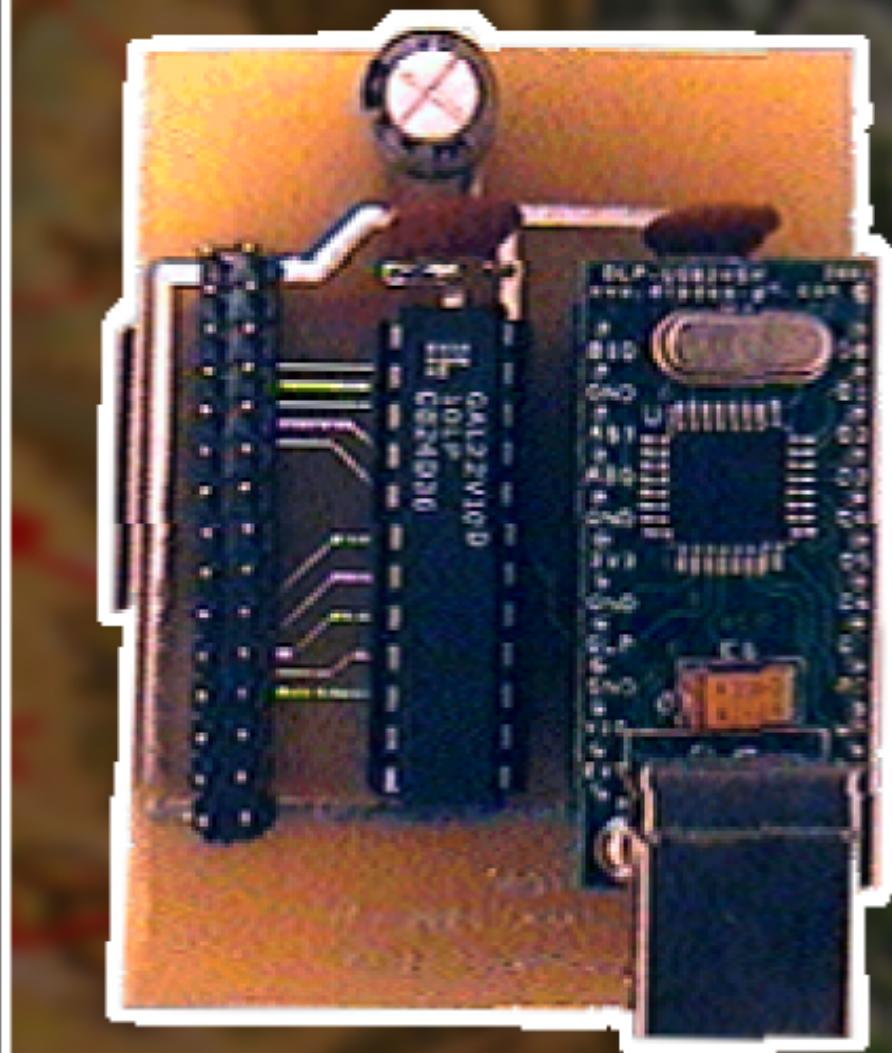
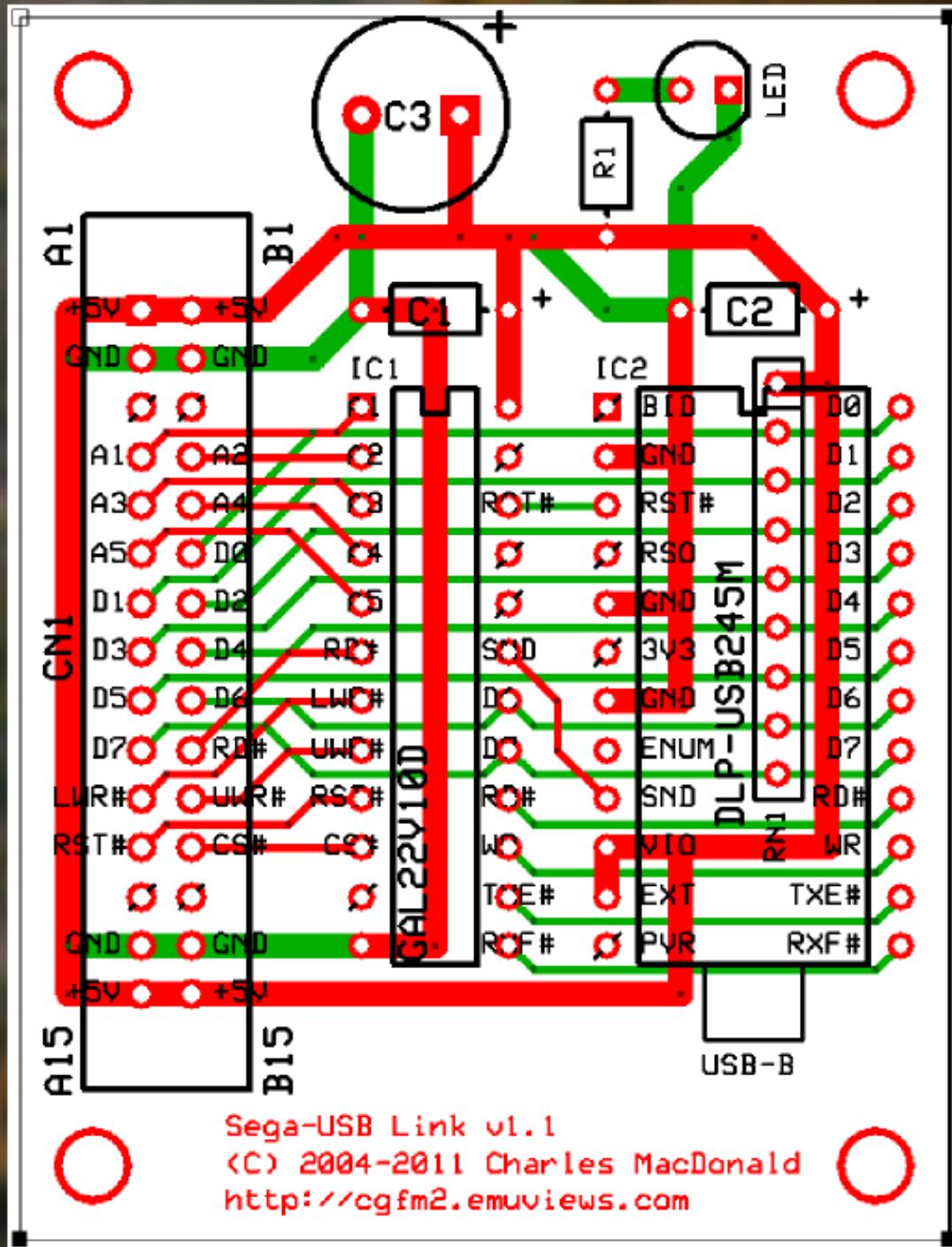
5 . D O T C R O S S H A T C H



P1: MK D D L MP U D LK (S+LP)

P2: D R R HP L R MK

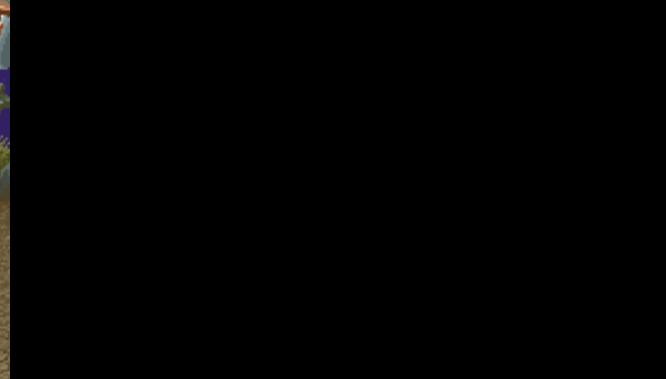
THANK YOU SO MUCH FOR LONG PLAYING



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



Dumping from a Sega System24's FD1094 to USB

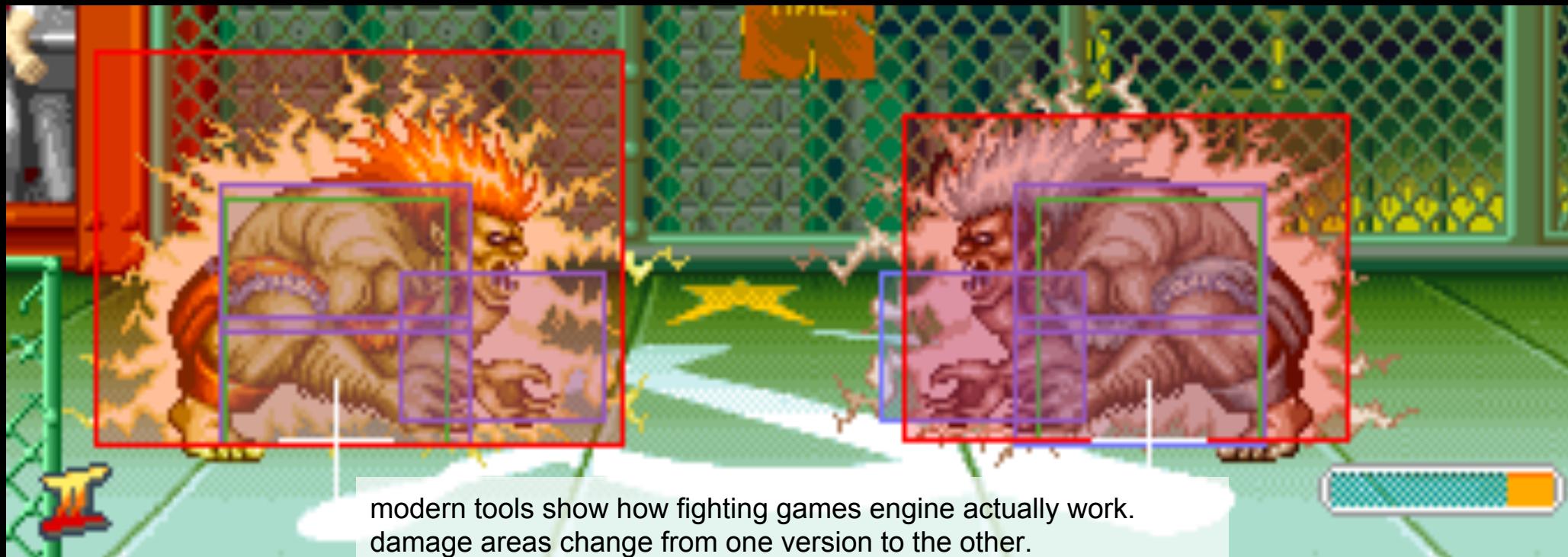


to preserve games from
System 16, 24 & System X

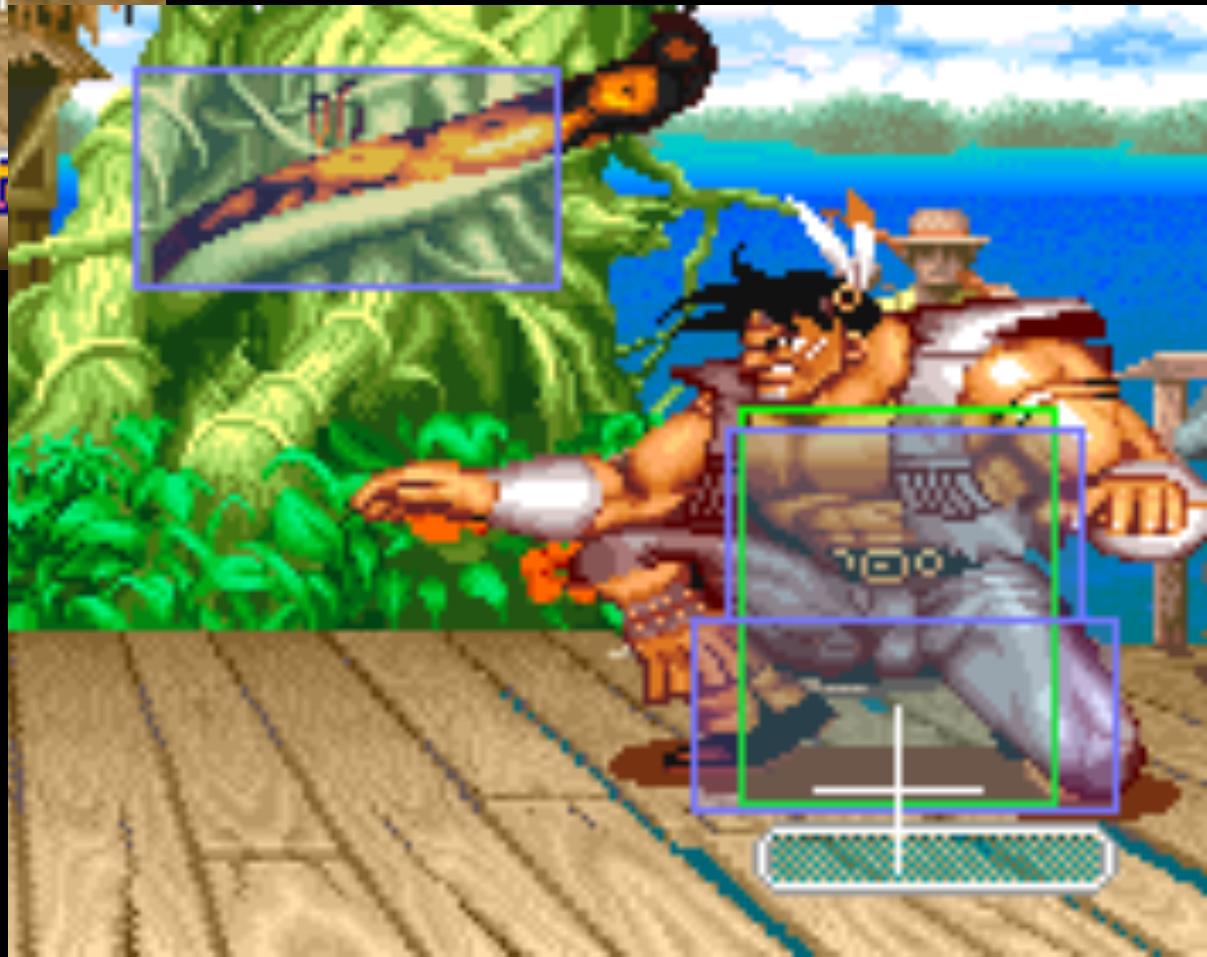
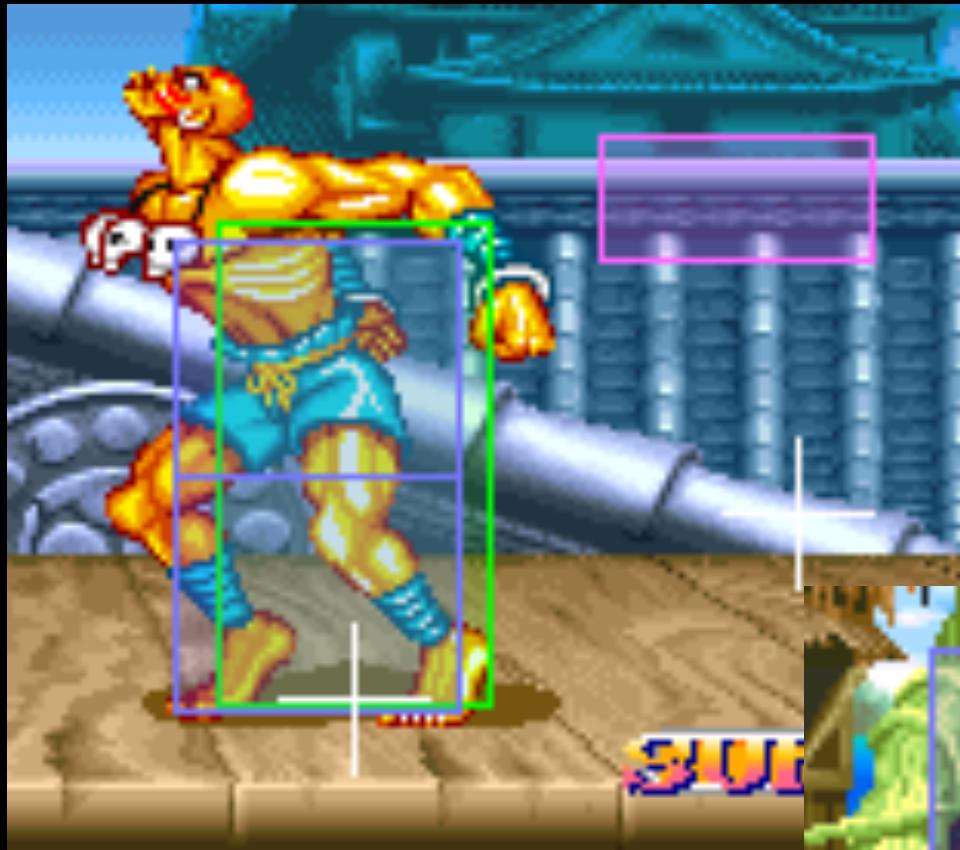




BLANKA HYPER VS BLANKA



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 ...?