The amazing life & achievements of...

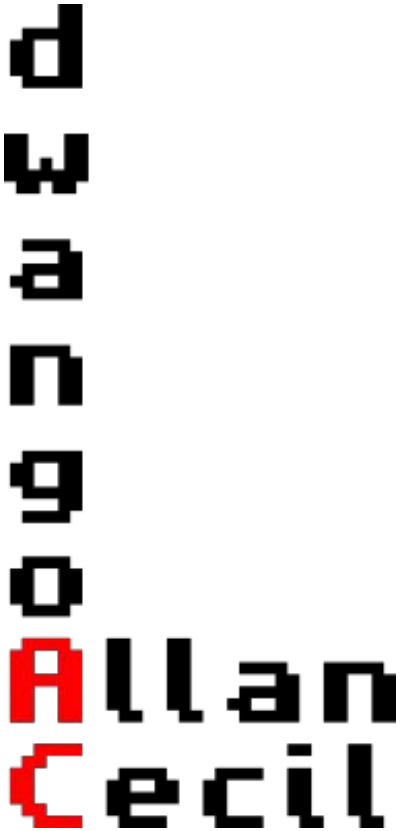
TASBot

THE PERFECTIONIST

Twitch.tv/dwangoAC @MrTASBot

dwangoAC DEFCON

Presented and written by...



http://acbit.net

Presented and written by...

dwanggo Allan Cecil

President of the North Bay Linux Users' Group

http://nblug.org

http://acbit.net

Presented and written by...

dwaango

Allan Cecil

http://acbit.net

President of the North Bay Linux Users' Group

Senior Engineer at ~~Cyan~~ Ciena

http://nblug.org

http://www.ciena.com/

Presented and written by...

Dwango

Allan Cecil

http://acbit.net

President of the North Bay Linux Users' Group

Senior Engineer at ~~Cyan~~ Ciena

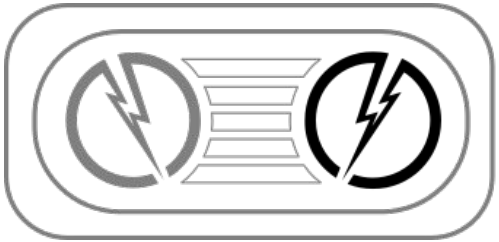
NBLUG North Bay Linux Users' Group

http://nblug.org

ciena

http://www.ciena.com/

http://tasvideos.org/DwangoAC.html



TASER

http://tasbot.net


TASVideos
SELECT START
B
A

Speedrunning

Human limits

http://speeddemosarchive.com/

Playing games fast

http://speeddemosarchive.com/

Playing games fast

- Inspiration: in-game completion timers

Playing games fast

- Inspiration: in-game completion timers
- Many categories, ranging from "any%" to "low% no major glitches"
- SPEED DEMOS ARCHIVE and others track fastest completion times
- Strict rules + peer review: no cheats, no macros
- Typically highly entertaining

Games Done Quick

Games Done Quick

Speedrunning marathons for charity streamed live on twitch

Classic **GDQ** (2010), **A**wesome **GDQ** (2011-), **S**ummer **GDQ** (2011-)

prevent cancer FOUNDATION

MEDECINS SANS FRONTIERES
DOCTORS WITHOUT BORDERS

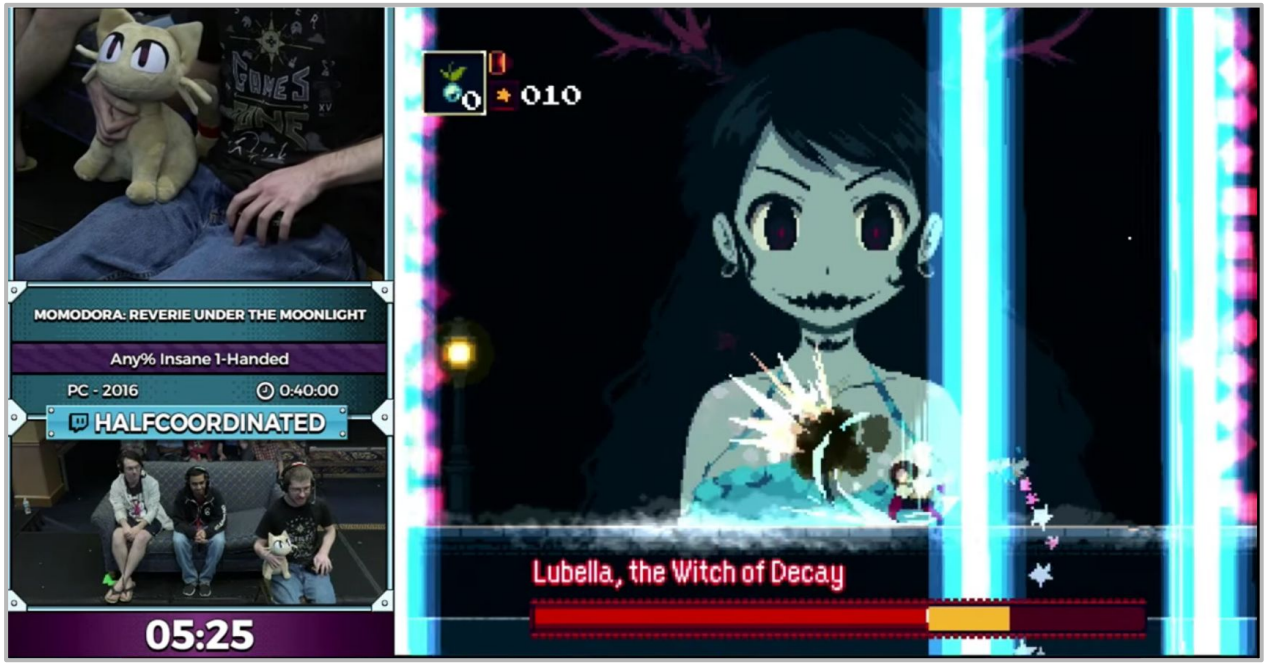
https://youtu.be/kIIzE_H7D2g?t=5m27s AGDQ 2014

Abusing games

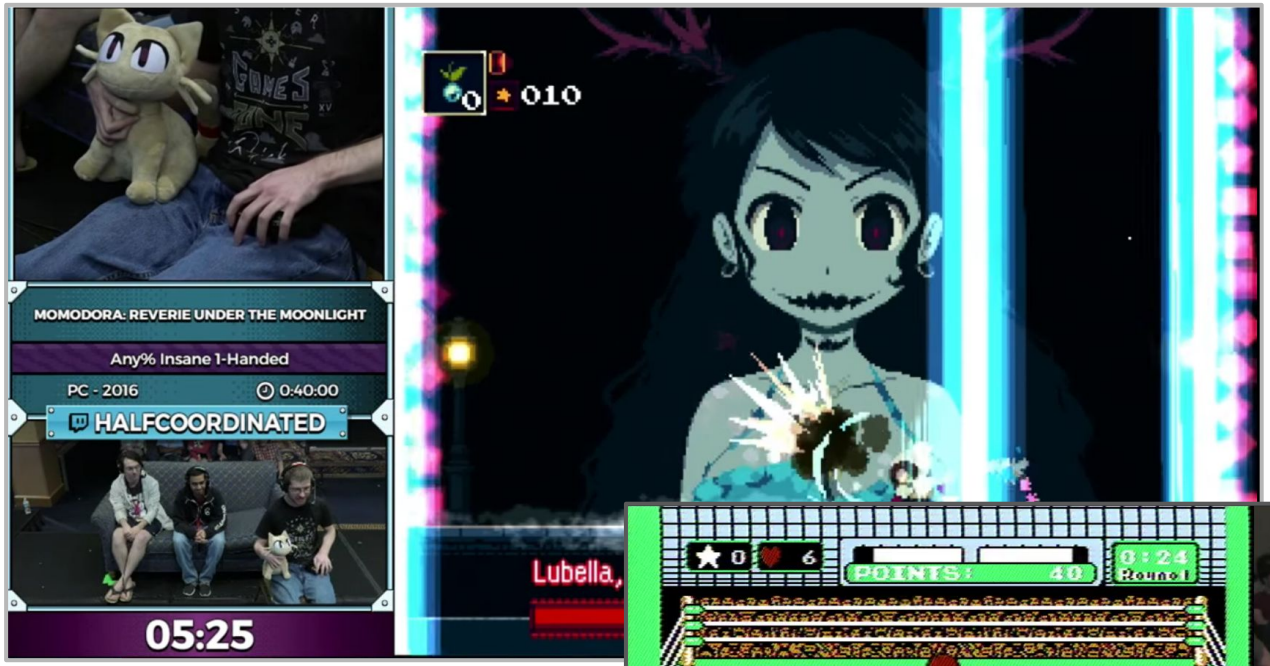
https://youtu.be/kIIzE_H7D2g?t=5m27s AGDQ 2014

Abusing games

Metroid 15:43 World Record https://www.youtube.com/watch?v=67kQ3l-1qMs

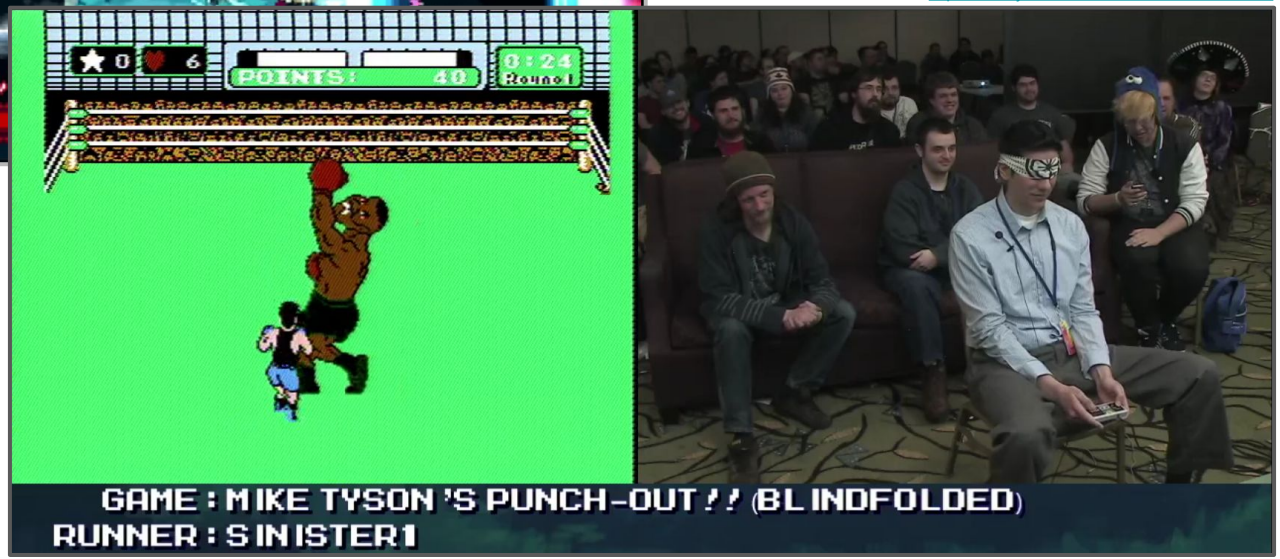


https://www.youtube.com/watch?v=JXtUwIW7cL8
Momodora by Halfcoordinated - SGDQ 2016

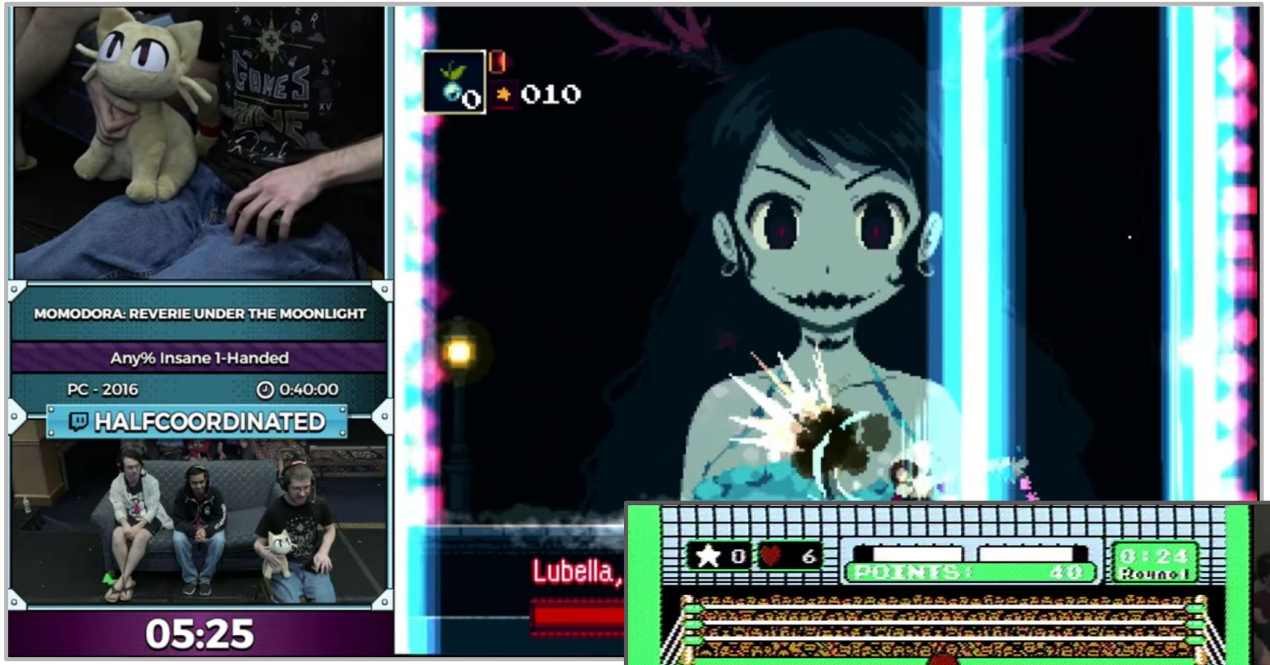


https://www.youtube.com/watch?v=JXtUwIW7cL8
Momodora by Halfcoordinated - SGDQ 2016

Punch-Out blindfolded by Sinister1 - AGDQ 2014
https://www.youtube.com/watch?v=CvzIb53Lcno

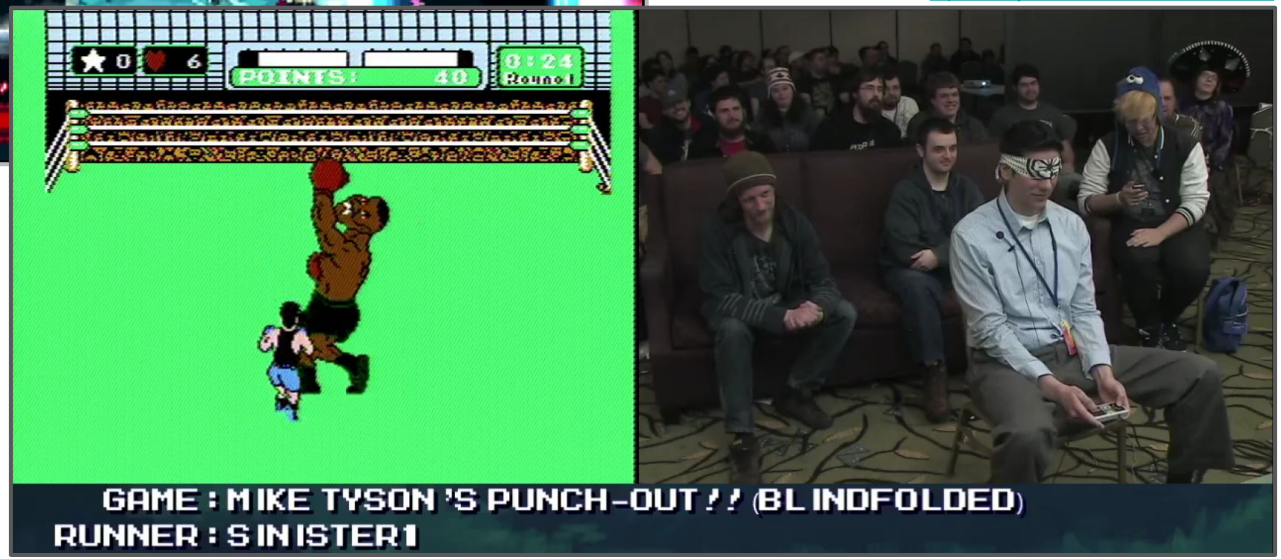


Beyond standard limits!



https://www.youtube.com/watch?v=JXtUwIW7cL8
Momodora by Halfcoordinated - SGDQ 2016

Punch-Out blindfolded by Sinister1 - AGDQ 2014
https://www.youtube.com/watch?v=CvzIb53Lcno



Even 1-handed, blindfolded...


TRS VIDEOS

Tool-**A**ssisted **S**uperplays

Speedruns

From human limits

To hardware limits

Tool-**A**ssisted **S**uperplays

Speedruns

From human limits
To hardware limits

TAS *verb / noun* ~ **TASer** *noun*

"I'm a TASer working on Tetris." / "I'm TASing Tetris."
"I TAS'ed Tetris." / "They made a TAS of Tetris."

Harder Faster Better Stronger

Harder Faster Better Stronger

- Early PC game TAS’s: Savestates, slow motion, and recording tools

Harder Faster Better Stronger

- Early PC game TAS’s: Savestates, slow motion, and recording tools
- ~1999: Doom Done Quick in 19:41

2003 SUPER MARIO BROS. 3

https://www.youtube.com/watch?v=BEcrJLM4GgU
http://web.archive.org/web/20031203222907/http://soramimi.egoism.jp/emu.htm

2003 SUPER MARIO BROS. 3

CONTROVERSIAL

https://www.youtube.com/watch?v=BEcrJLM4GgU
http://web.archive.org/web/20031203222907/http://soramimi.egoism.jp/emu.htm

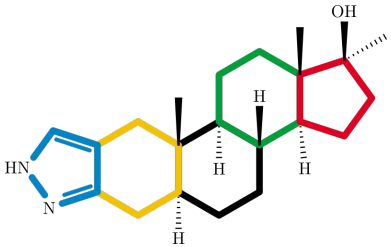
Inhuman skill on display

- Tools meant hardware limits became the **only** limits

http://tasvideos.org/WelcomeToTASVideos.html
https://web.archive.org/web/20060511210906/http://bisqwit.iki.fi/nesvideos/

Inhuman skill on display

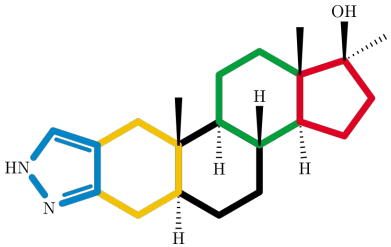
- Tools meant hardware limits became the **only** limits
- TASing looked like the Doped Olympics
  - Competitors should admit to doping
  - Videos made with TAS tools should be labeled



http://tasvideos.org/WelcomeToTASVideos.html
https://web.archive.org/web/20060511210906/http://bisqwit.iki.fi/nesvideos/

Inhuman skill on display

- Tools meant hardware limits became the **only** limits
- TASing looked like the Doped Olympics
  - Competitors should admit to doping
  - Videos made with TAS tools should be labeled

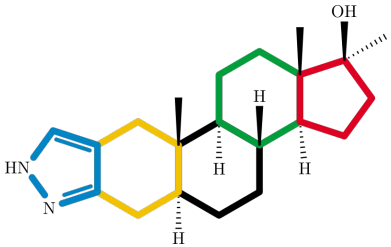


- NESVideos created by Bisqwit in 2004

http://tasvideos.org/WelcomeToTASVideos.html
https://web.archive.org/web/20060511210906/http://bisqwit.iki.fi/nesvideos/

Inhuman skill on display

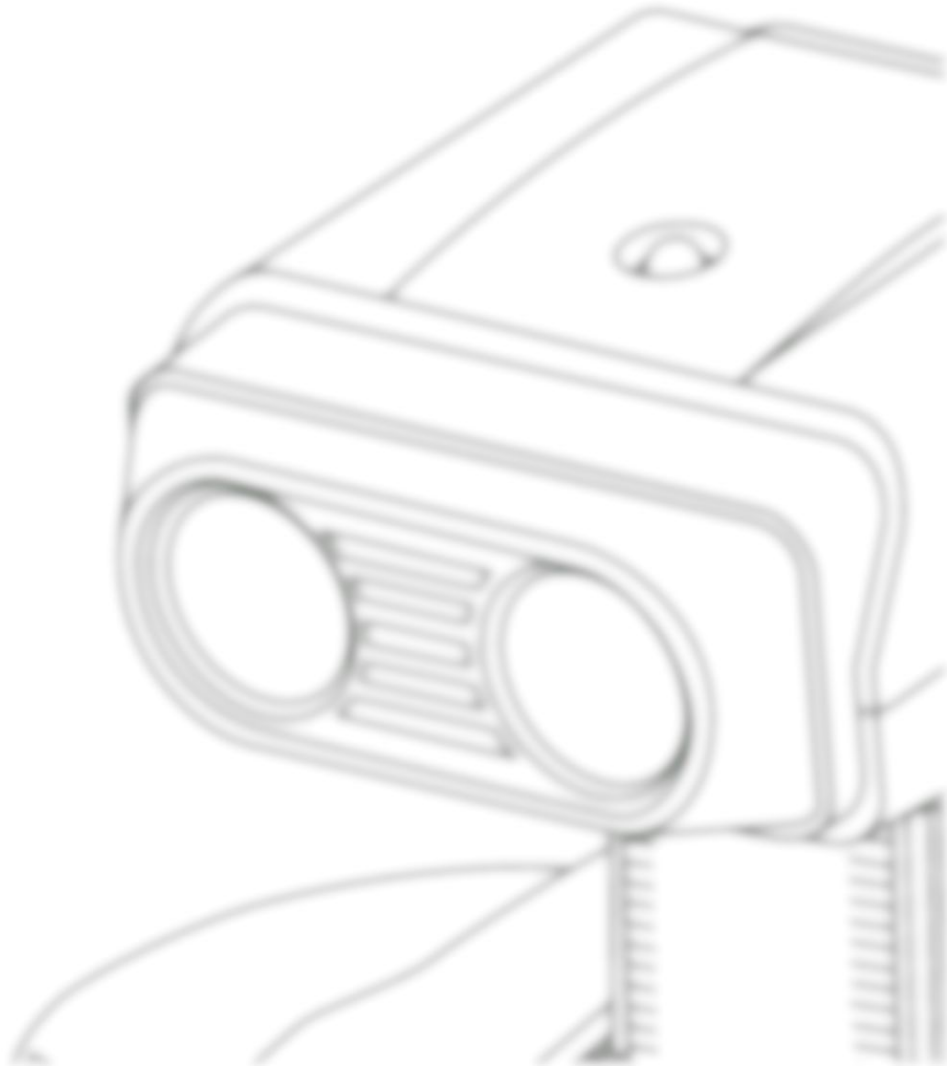
- Tools meant hardware limits became the **only** limits
- TASing looked like the Doped Olympics
  - Competitors should admit to doping
  - Videos made with TAS tools should be labeled



- NESVideos created by Bisqwit in 2004
  - Now at TASVideos.org with runs for many platforms

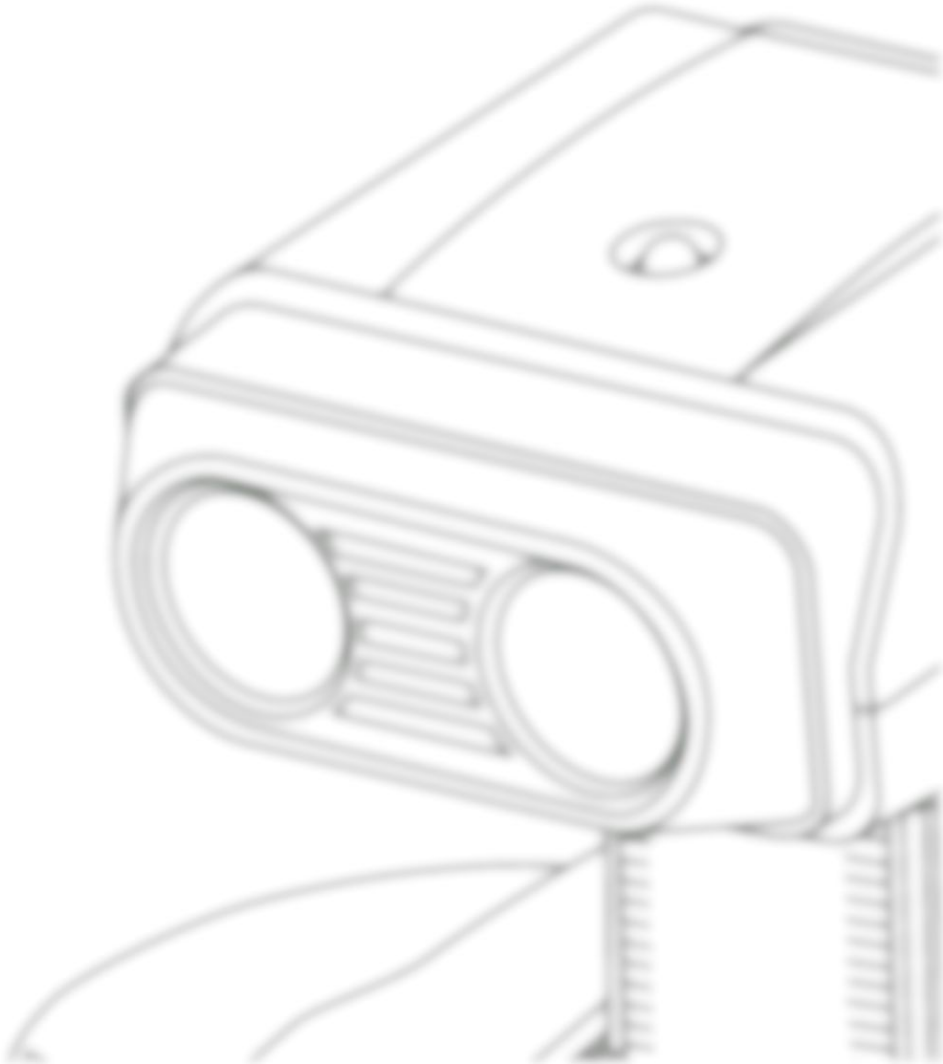
Nesvideos
Tool-assisted speedruns

http://tasvideos.org/WelcomeToTASVideos.html
https://web.archive.org/web/20060511210906/http://bisqwit.iki.fi/nesvideos/



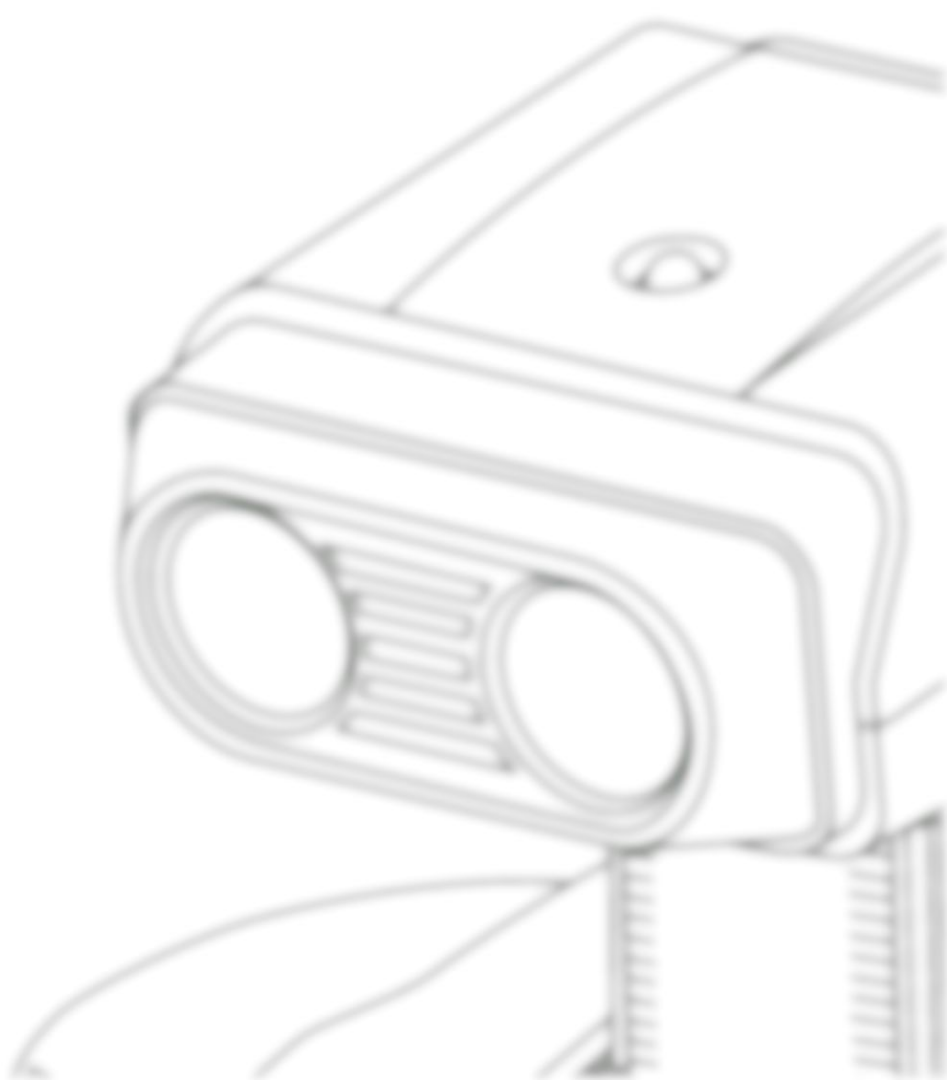
Console verified

Pushing hardware limits



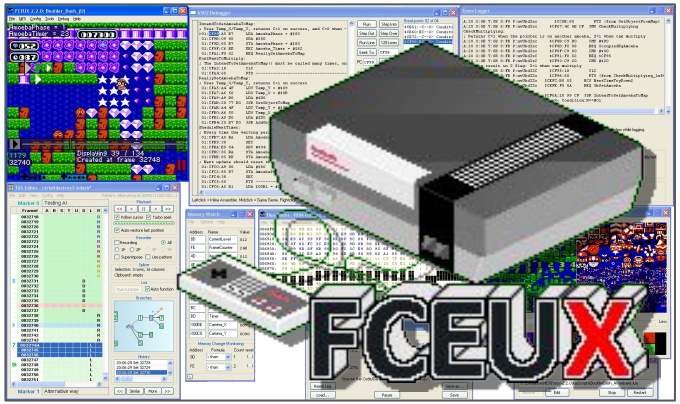
Console verified

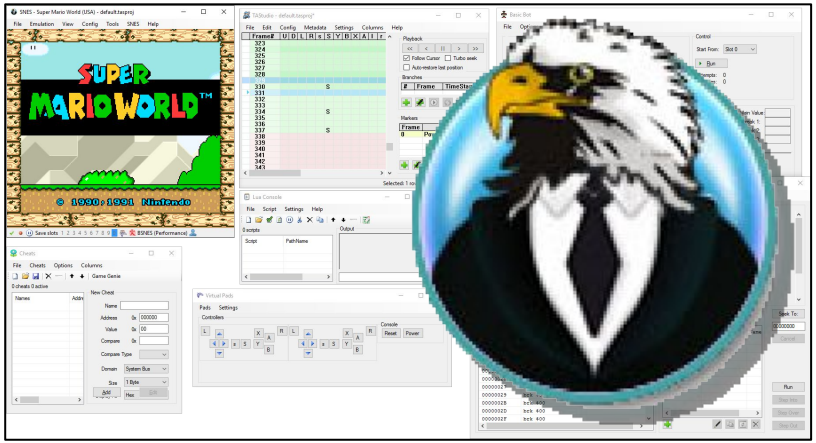
Pushing hardware limits



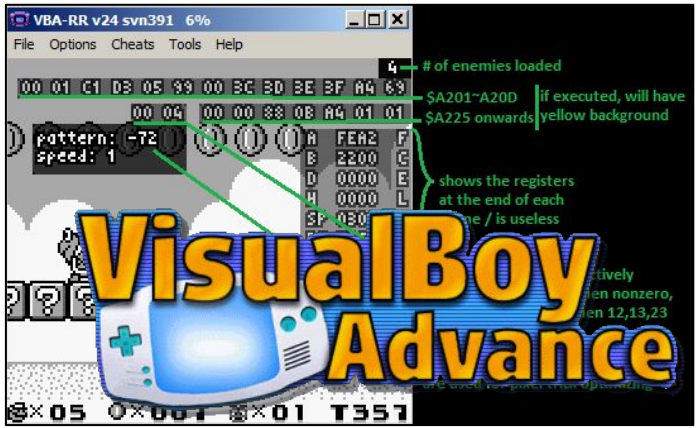
Console emulators

http://tasvideos.org/Lsnes.html Lsnes



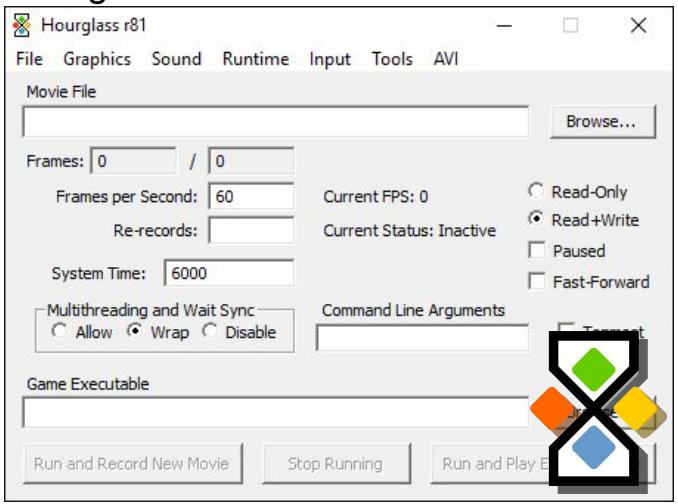


BizHawk http://tasvideos.org/BizHawk.html



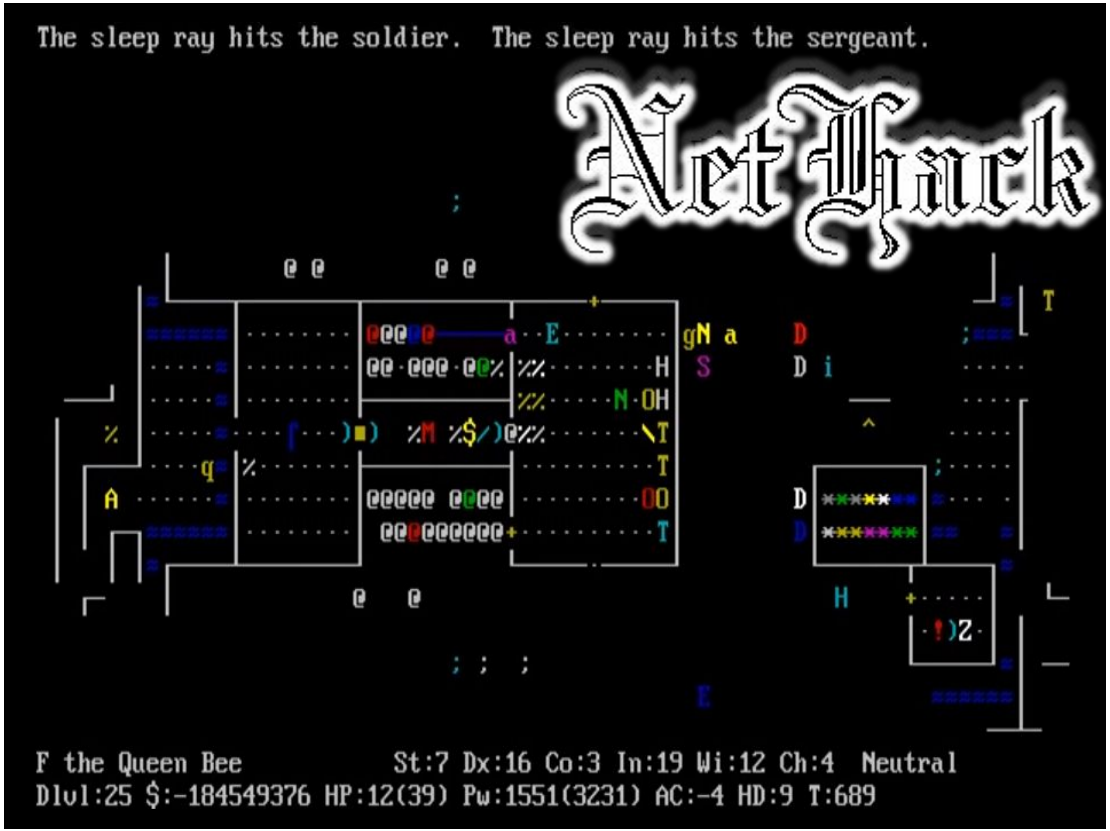
Rerecording frameworks

Hourglass



http://tasvideos.org/EmulatorResources/Hourglass.html

NetHack specific tools



http://tasvideos.org/GameResources/DOS/Nethack.html

Emulation accuracy evolution

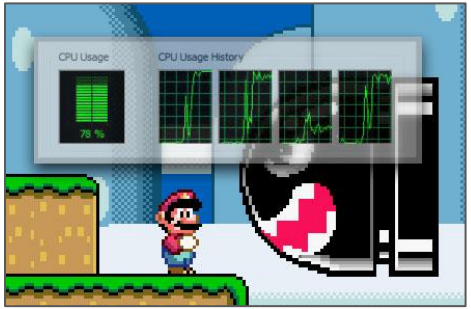
Emulation accuracy evolution

- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals

http://arstechnica.com/gaming/2011/08/accuracy-takes-power-one-mans-3ghz-quest-to-build-a-perfect-snes-emulator/
https://web.archive.org/web/20120915125144/http://byuu.org/bsnes/accuracy

Emulation accuracy evolution

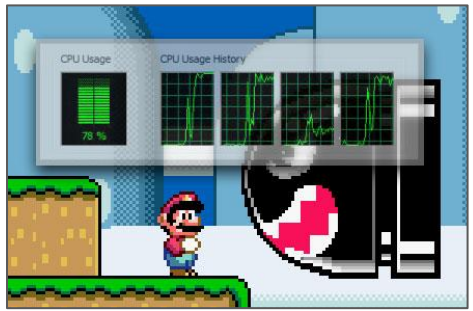
- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
- *bsnes*: extreme accuracy, poor usability



http://arstechnica.com/gaming/2011/08/accuracy-takes-power-one-mans-3ghz-quest-to-build-a-perfect-snes-emulator/
https://web.archive.org/web/20120915125144/http://byuu.org/bsnes/accuracy

Emulation accuracy evolution

- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
- *higan*: extreme accuracy, poor usability



higan

http://byuu.org/emulation/higan/

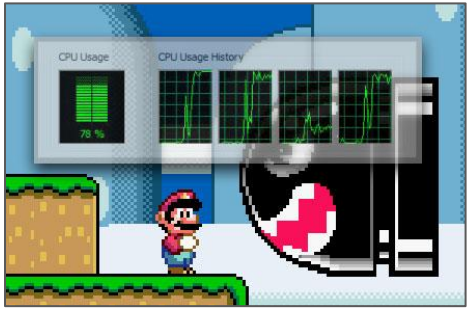
http://arstechnica.com/gaming/2011/08/accuracy-takes-power-one-mans-3ghz-quest-to-build-a-perfect-snes-emulator/
https://web.archive.org/web/20120915125144/http://byuu.org/bsnes/accuracy

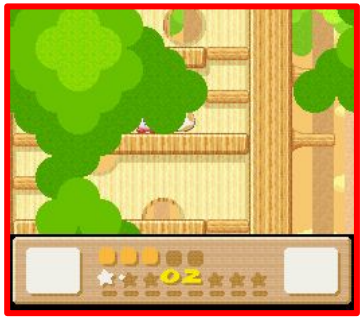
Emulation accuracy evolution

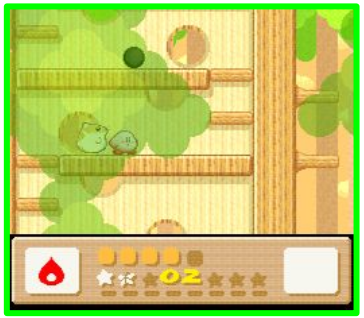
- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
- *higan*: extreme accuracy, poor usability

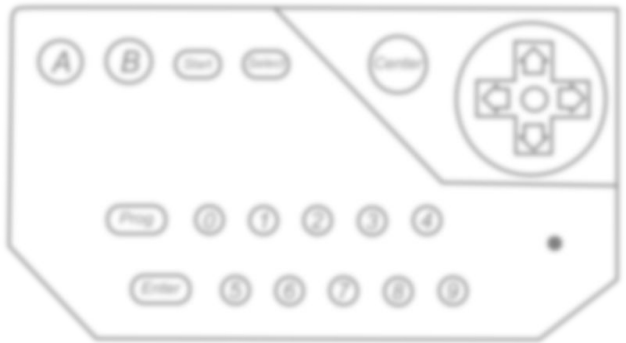
http://byuu.org/emulation/higan/

⇒ match actual hardware, frame for frame



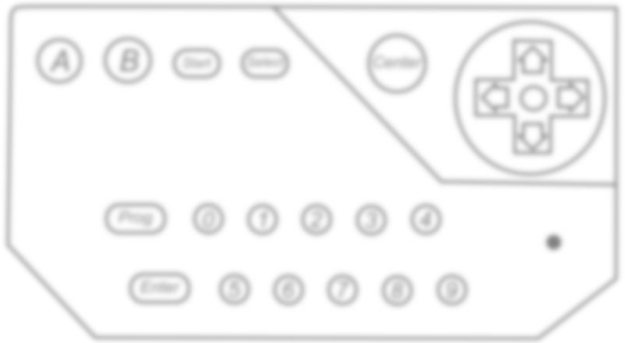





A
B
Start
Select
Combo
Prog
0
1
2
3
4
Enter
5
6
7
8
9

Memory searching, Lua scripting, disassembly

https://www.lua.org/

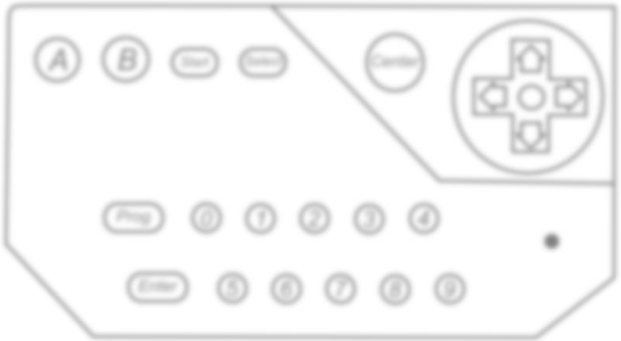


Memory searching, Lua scripting, disassembly

- More than just frame advance and savestates

https://www.lua.org/

https://www.youtube.com/watch?v=RtaS4KEl4Qc

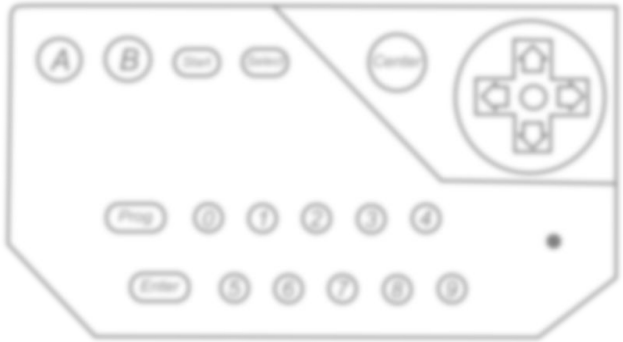


Memory searching, Lua scripting, disassembly

https://www.lua.org/

- More than just frame advance and savestates
- Find a specific value: save, reset memory search, run
  - Search based on conditions, repeat

https://www.youtube.com/watch?v=RtaS4KEl4Qc

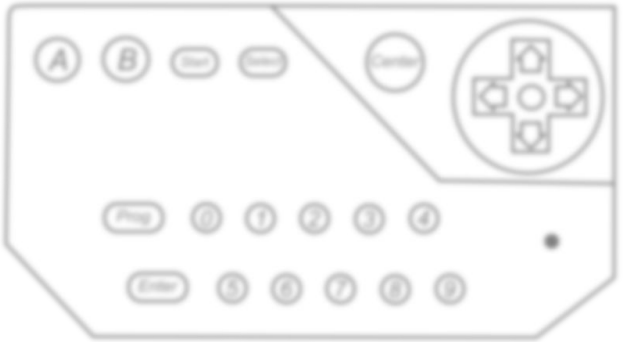


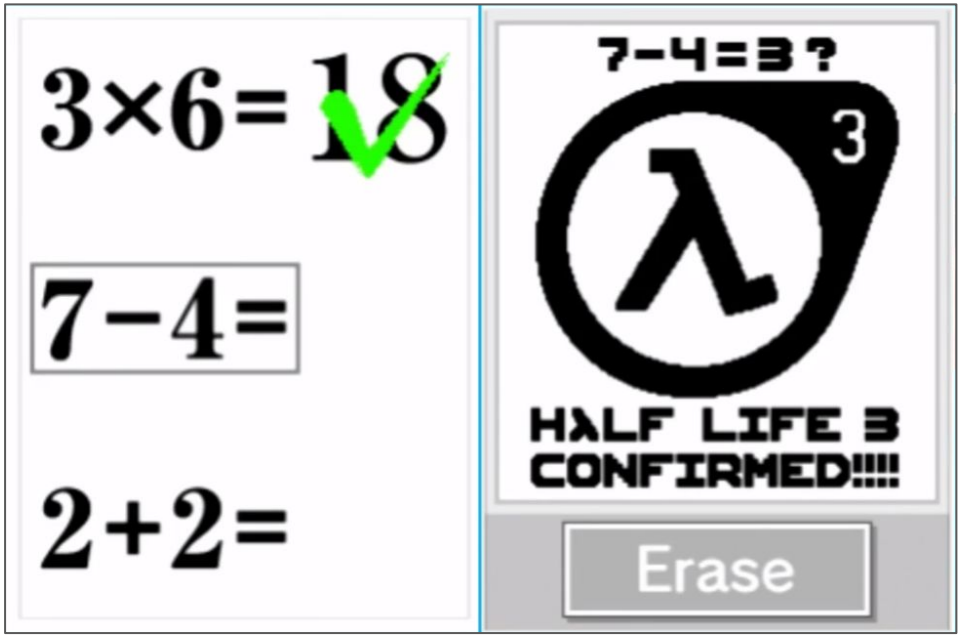
Memory searching, Lua scripting, disassembly

https://www.lua.org/

- More than just frame advance and savestates
- Find a specific value: save, reset memory search, run
  - Search based on conditions, repeat
- Disassembly of RAM or ROM for complete understanding

https://www.youtube.com/watch?v=RtaS4KEl4Qc

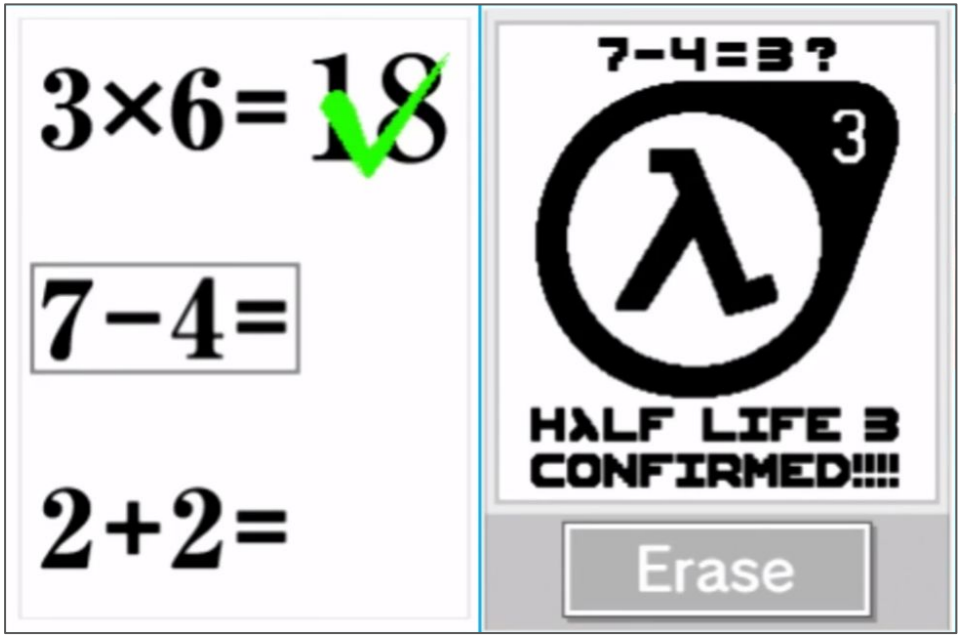




Abusing handwriting recognition

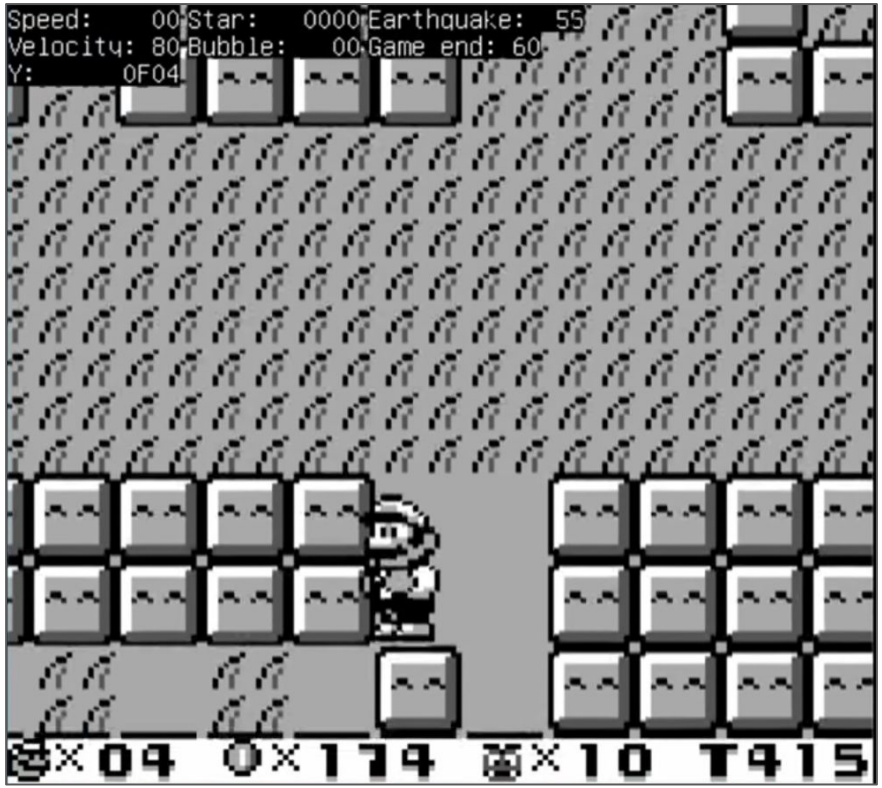
https://youtu.be/mSFHKAvTGNk?t=29m53s AGDQ 2016

Abusing handwriting recognition



https://youtu.be/mSFHKAvTGNk?t=29m53s AGDQ 2016

SGDQ 2016 https://youtu.be/EHfw-BEuRO8?t=12m28s



Editing memory live directly in the game


POWER GLOVE

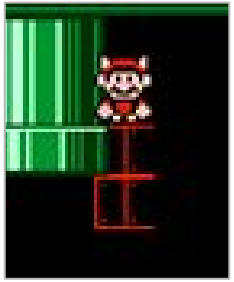
TAS ⇔ Infosec equivalents

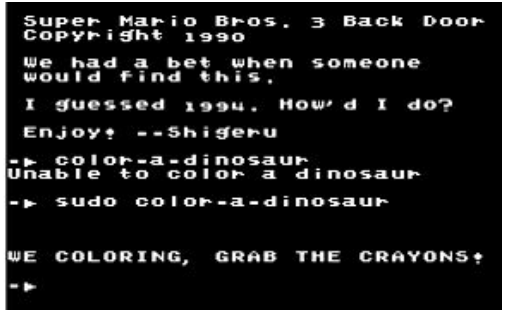
- Savestate = VM snapshot
- Frame advance = VM CPU step / tick
- Glitch = Vulnerability
- Arbitrary Code Execution = Exploit
- Console verification = Evil maid attack

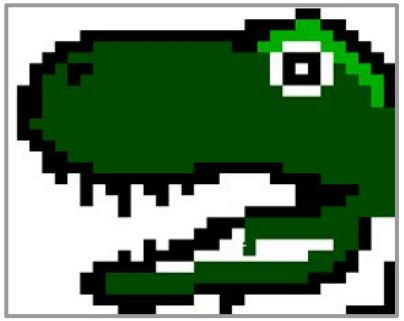
⇒ TAS = fun, technical, educational

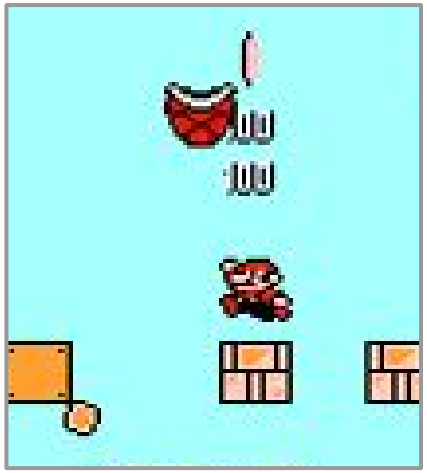
AGDQ 2016 https://youtu.be/pj7RE2DcRgc?t=50m23s

SMB3 Total Control Glitchfest by Lord Tom









TASBot

TASBot

plays

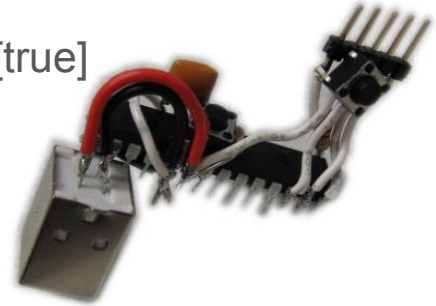
TASBot

plays

Early console verification devices

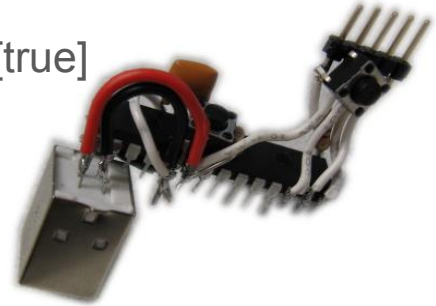
Early console verification devices

- **2009**
  - a PIC to press NES buttons [true]



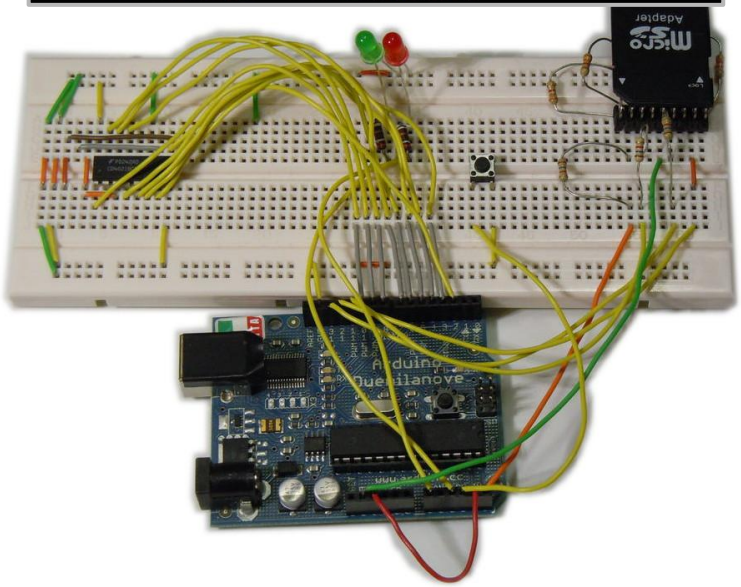
Early console verification devices

- **2009**
  - a PIC to press NES buttons [true]



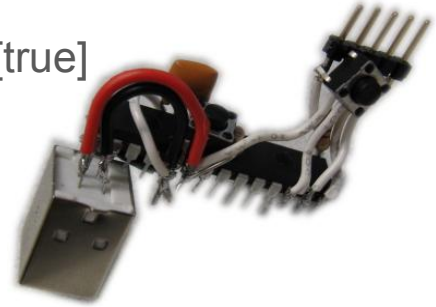
- **2011**
  - NESBot [micro500]: first replay of SMB1
    - Used at SGDQ 2011 on SMB2 and W&W 3

https://www.youtube.com/watch?v=KQXVgMKJEDY



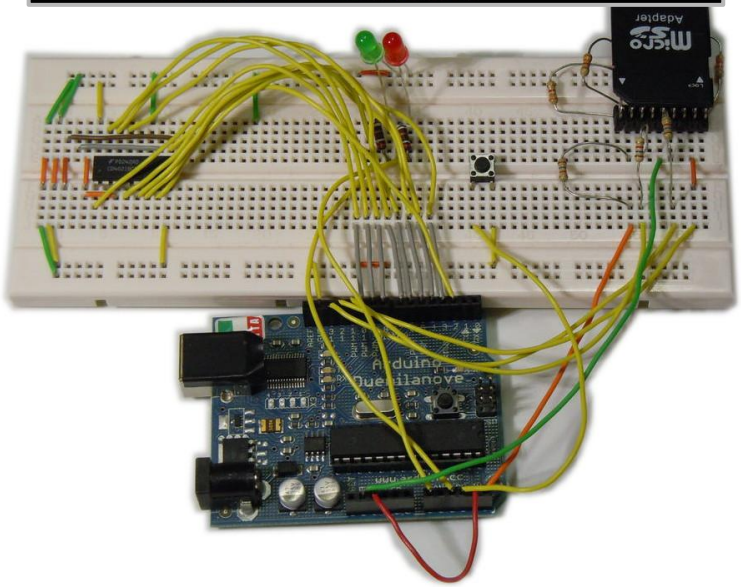
Early console verification devices

- **2009**
  - a PIC to press NES buttons [true]



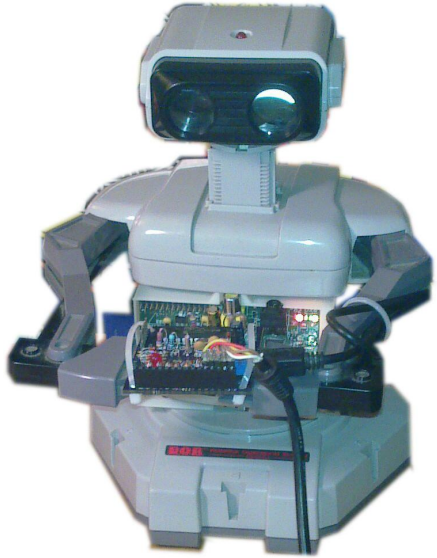
- **2011**
  - NESBot [micro500]: first replay of SMB1
    - Used at SGDQ 2011 on SMB2 and W&W 3
  - Droid64 [SoulCal]
- **2012**
  - N64 [micro500]

https://www.youtube.com/watch?v=KQXVgMKJEDY



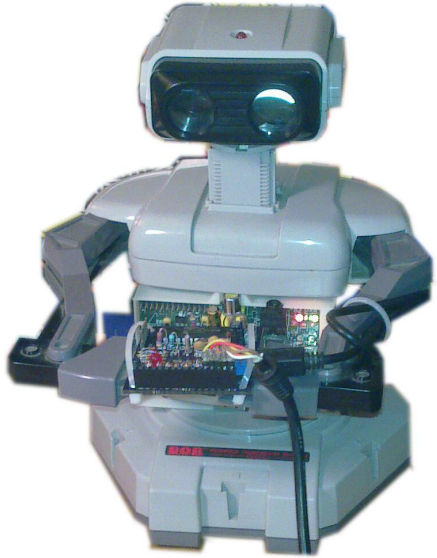
- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates

The birth of TASBot



- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
- 2014
  - Nintendo R.O.B + board + legos: "TASBot"

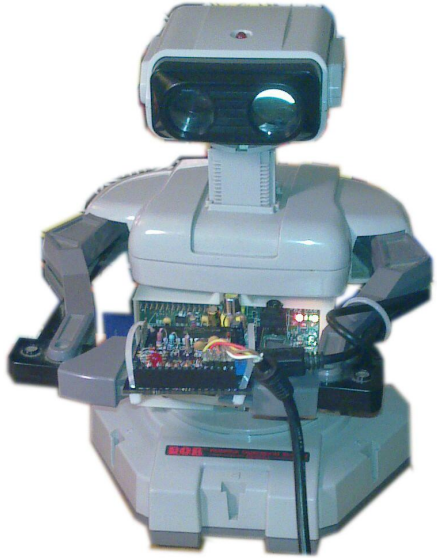
The birth of TASBot



- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
- 2014
  - Nintendo R.O.B + board + legos: "TASBot"
- 2015
  - Multireplay device [true]: self-contained ⇒ faster datarates

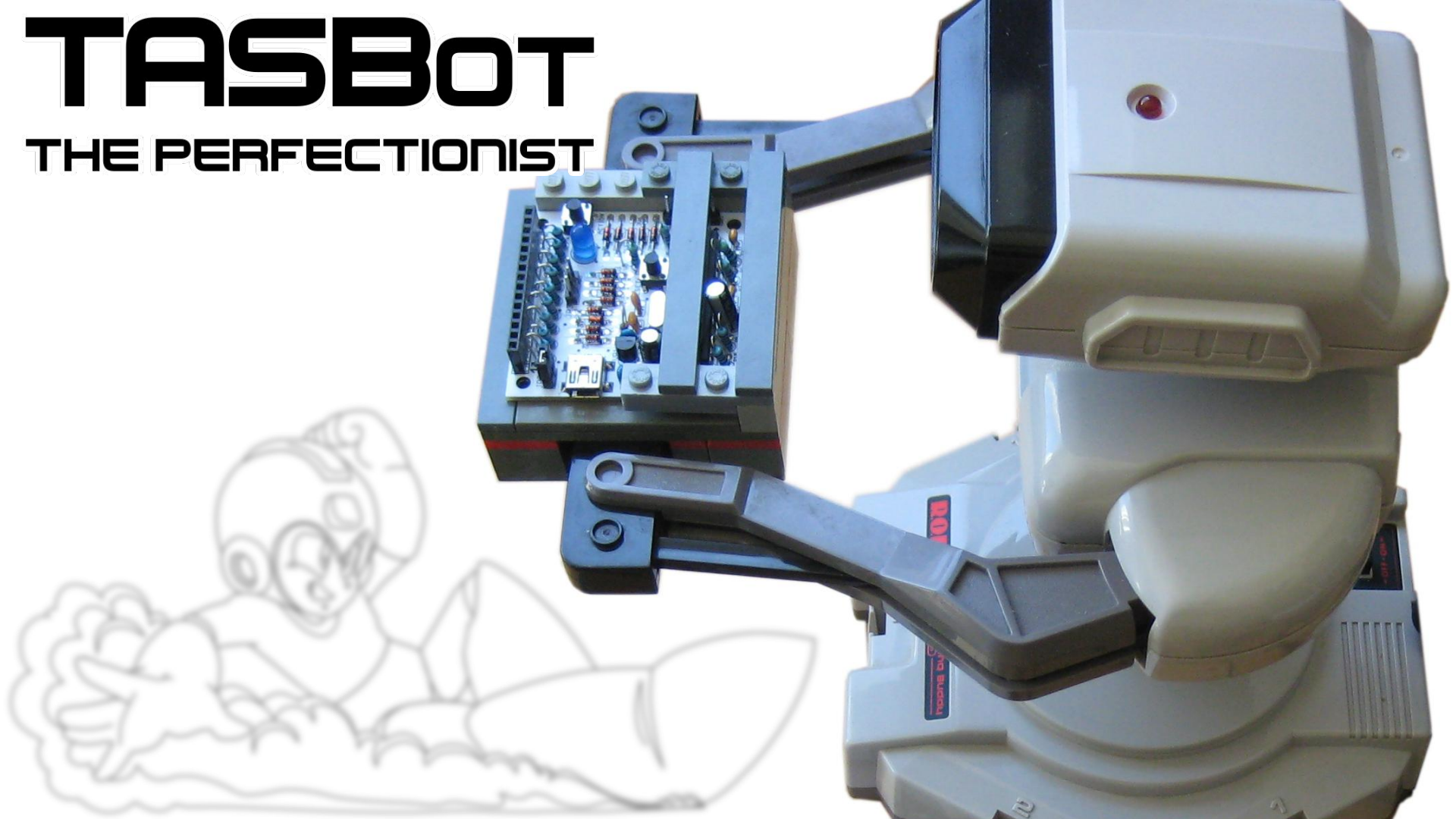
The birth of TASBot

- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
- 2014
  - Nintendo R.O.B + board + legos: "TASBot"
- 2015
  - Multireplay device [true]: self-contained ⇒ faster datarates
  - Game Boy Player Player [endrift] (GBA on GameCube)



TASBot

THE PERFECTIONIST



TASBot

TASBot

plays

TASBot

plays

TASBot

plays

in

TASBot

plays

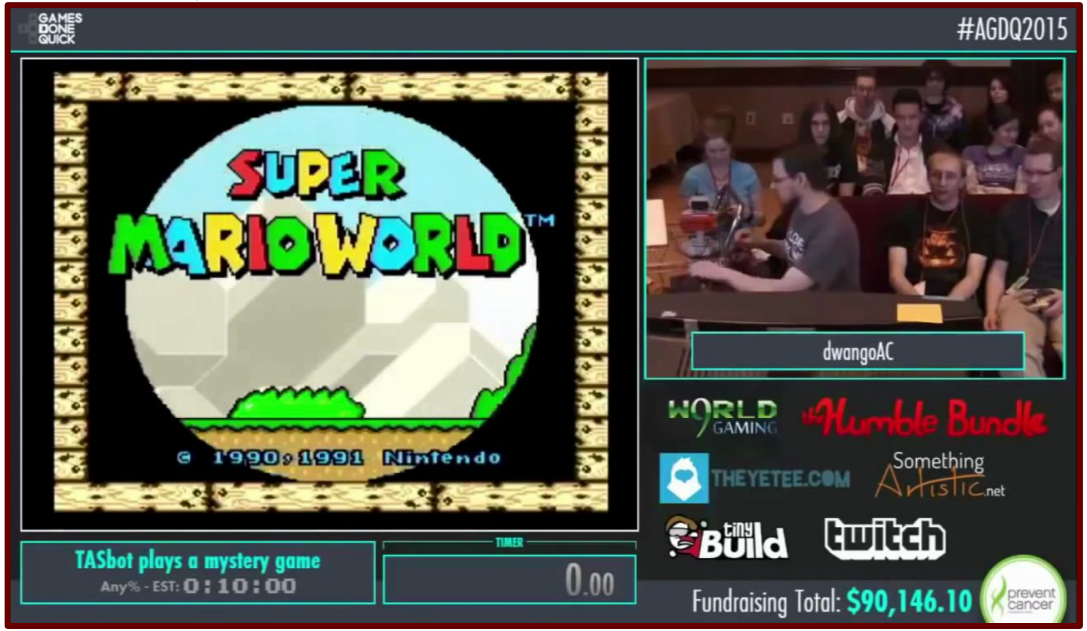
in

SMB in SMW by p4plus2 and Masterjun

TASBot plays the SNES classic...

http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/
https://www.youtube.com/watch?v=YHyaTCuZRzM

credits: p4plus2, Masterjun



TASBot plays the SNES classic...

http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/
https://www.youtube.com/watch?v=YHyaTCuZRzM

credits: p4plus2, Masterjun

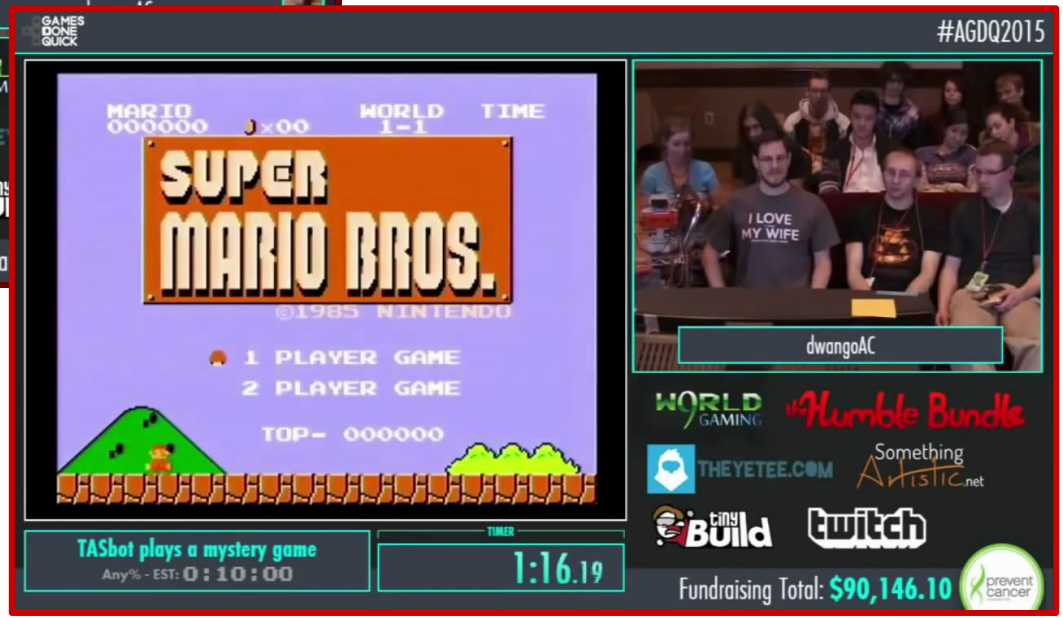
Exploits it via input...

TASBot plays the SNES classic...

http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/
https://www.youtube.com/watch?v=YHyaTCuZRzM

credits: p4plus2, Masterjun

Exploits it via input...



A homemade port of the NES classic is sent as payload...

TASBot plays the SNES classic...

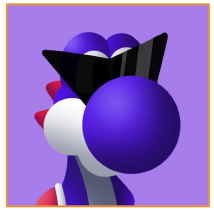
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/
https://www.youtube.com/watch?v=YHyaTCuZRzM

credits: p4plus2, Masterjun

A 8-bit game, on a 16-bit system!

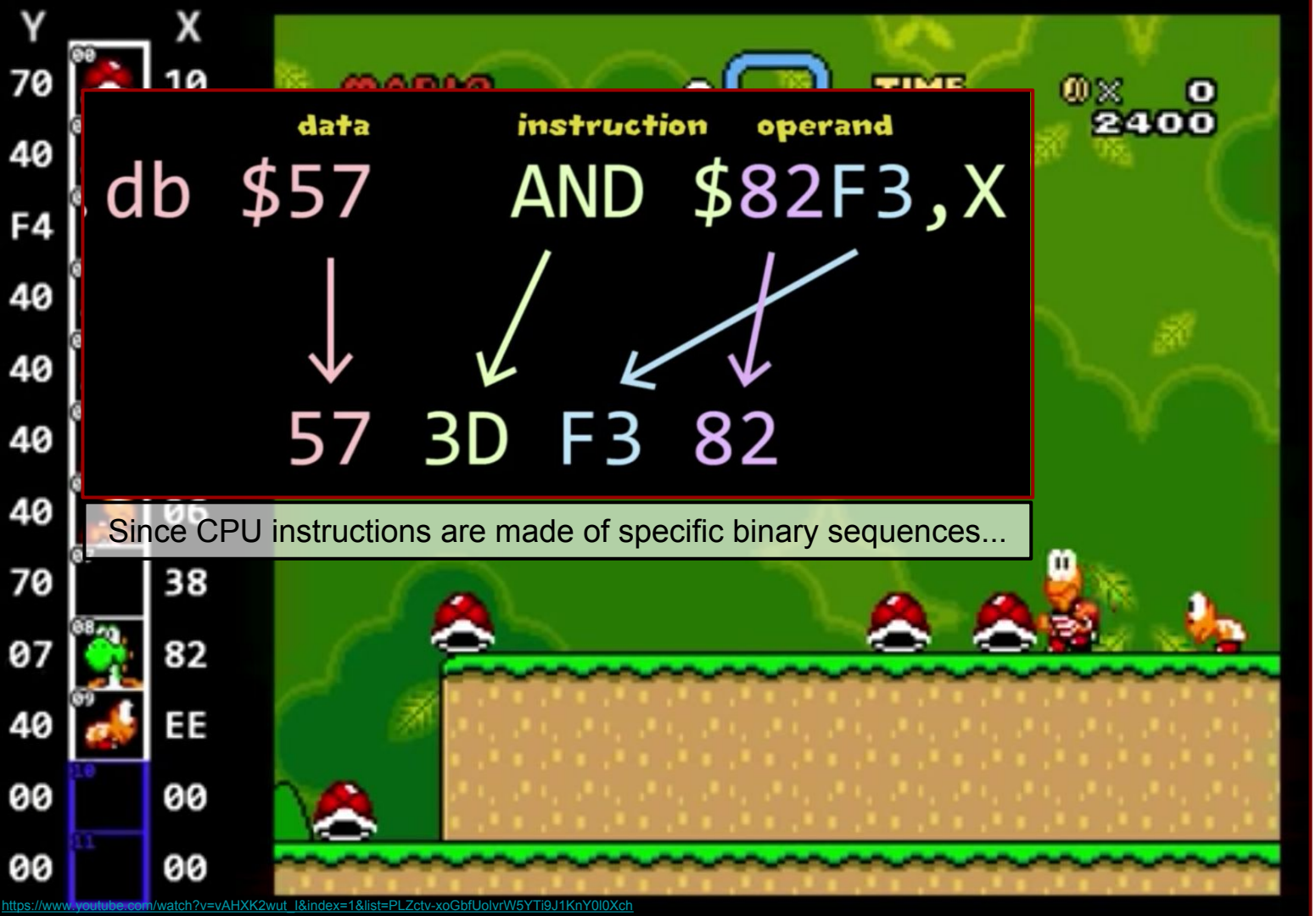
Exploits it via input...

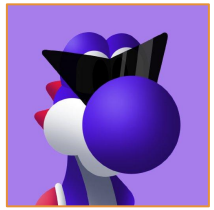
A homemade port of the NES classic is sent as payload...



dotsarecool

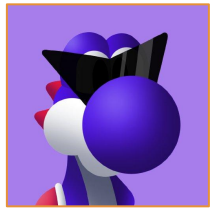
https://www.youtube.com/watch?v=vAHXK2wut_I&index=1&list=PLZctv-xoGbfUolvrW5YTi9J1KnY0l0Xch



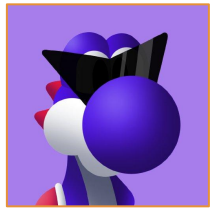


dotsarecool

https://www.youtube.com/watch?v=vAHXK2wut_I&index=1&list=PLZctv-xoGbfUolvrW5YTi9J1KnY0l0Xch



dotsarecool



dotsarecool


dotsarecool
data
instruction
operand
Main Memory
PC = 0100E0
17
4A
CC
F3
Stack
X = 09
...we can
So, just via input...
...you can directly trigger the credits sequence!
MARIO
TIME
249
2400
https://www.youtube.com/watch?v=vAHXK2wut_I&index=1&list=PLZctv-xoGbfUolvrW5YTi9J1KnY0l0Xch

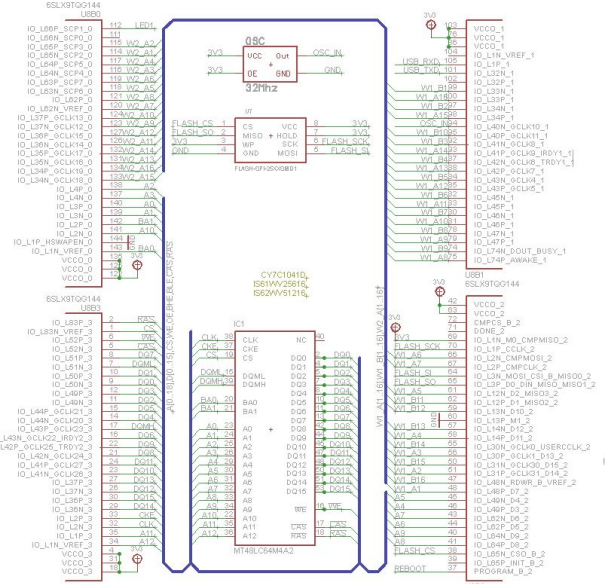
TASLink

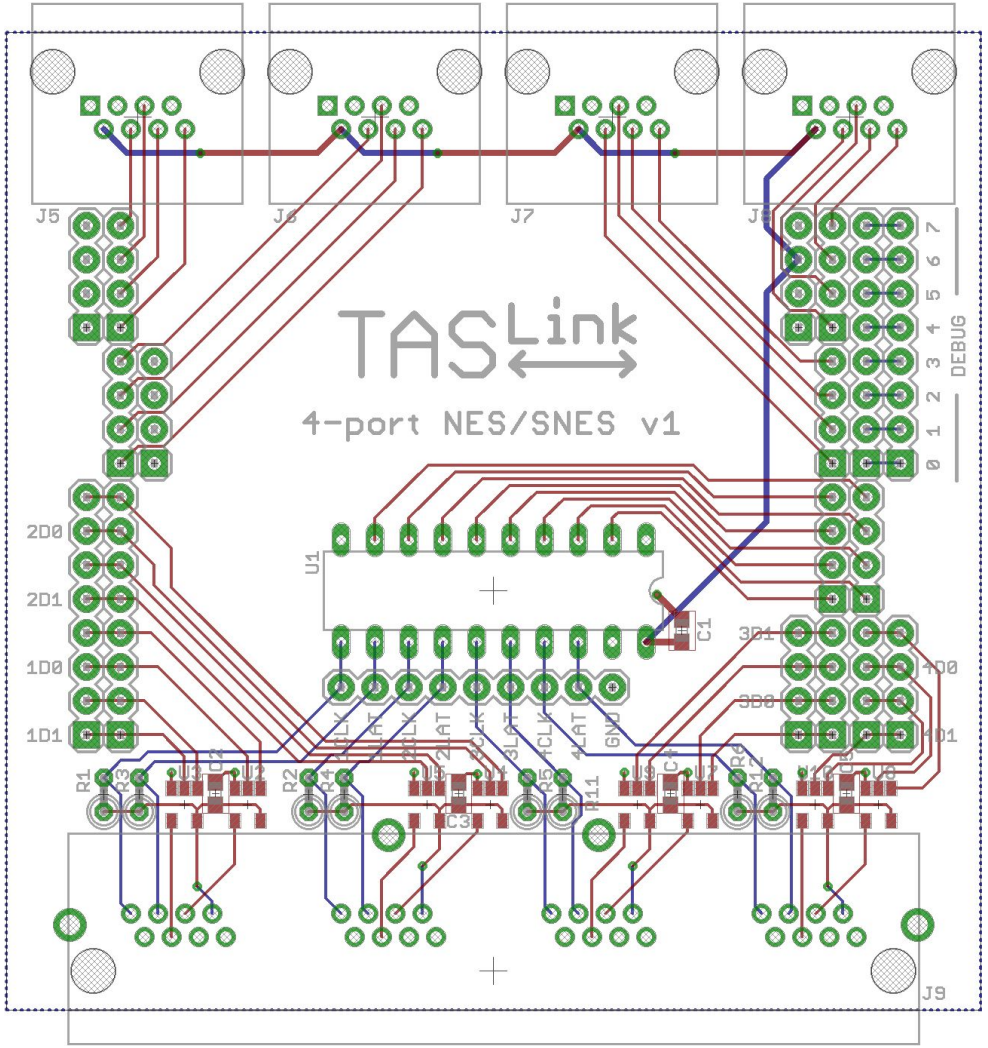
~184 Kbps
was ***too*** limiting

32Mhz FPGA

Papilio Pro's Spartan 6 LX

max poll rate of the serial port (2Mb/s)





http://papilio.gadgetfactory.net/index.php?n=Papilio.PapilioPro

SMB1+2+3+Lost Levels played simultaneously during SGDQ 2016

https://youtu.be/EHfw-BEuRO8?t=58m29s

Anatomy of an Arbitrary Code Execution

Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit

Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
2. Take over
   the Super GameBoy

Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
2. Take over
   the Super GameBoy
3. Gain full access to
   the Super Nintendo

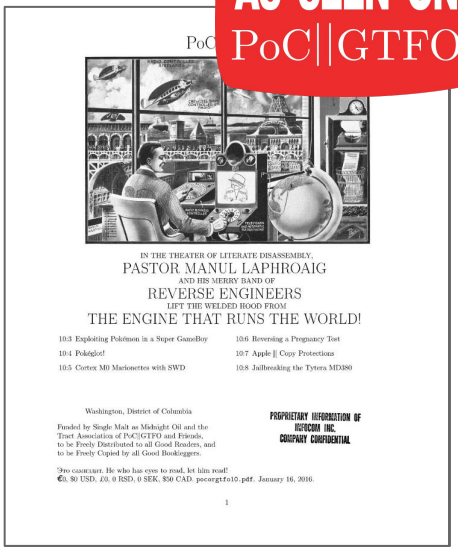
Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
2. Take over
   the Super GameBoy
3. Gain full access to
   the Super Nintendo
4. Anything is possible


that the team put into it.
Pokemon Plays Twitch Credits:
dwangoAC: Main project organizer
and presenter, primary tester,
Stage 0/1 movie files, PR
Ilari: Emulator coder (lsnes),
Stages 3-5 developer, payload
tester, game mechanic researcher
p4plus2: Primary payload author,
encoding scheme creator, SNES
expert, general stage 3-x help
Masterjun: Stage 0/1 original
idea and research, SNES advice
micro500: Wiring harness build,
Python IRC to bot streaming,
poll speed firmware modification
true: Creator of NES/SNES Replay
device, reset handling updates
TheAxeMan: Python script support
ais523: Data encoding assistance
Nach: SGB docs, site defacement
Tompa: On-site hardware support
padz: Pokemon Red research
Vulaj in: Camera serial interface
twms: Initial IRC Python script
Full article in next PoC||GTFO!
Chat
2015
RUNNER
TAS Bot
GAME BOY

TASVIDEOS



PoC

IN THE THEATER OF LITERATE DISASSEMBLY,

PASTOR MANUL LAPHROAIG

AND HIS MERRY BAND OF

REVERSE ENGINEERS

LIFT THE WELDED HOOD FROM

THE ENGINE THAT RUNS THE WORLD!

10:3 Exploiting Pokémon in a Super GameBoy

10:4 Pokéglot!

10:5 Cortex M0 Marionettes with SWD

10:6 Reversing a Pregnancy Test

10:7 Apple][Copy Protections

10:8 Jailbreaking the Tytera MD380

Washington, District of Columbia

Funded by Single Malt as Midnight Oil and the Tract Association of PoC||GTFO and Friends, to be Freely Distributed to all Good Readers, and to be Freely Copied by all Good Bootleggers.

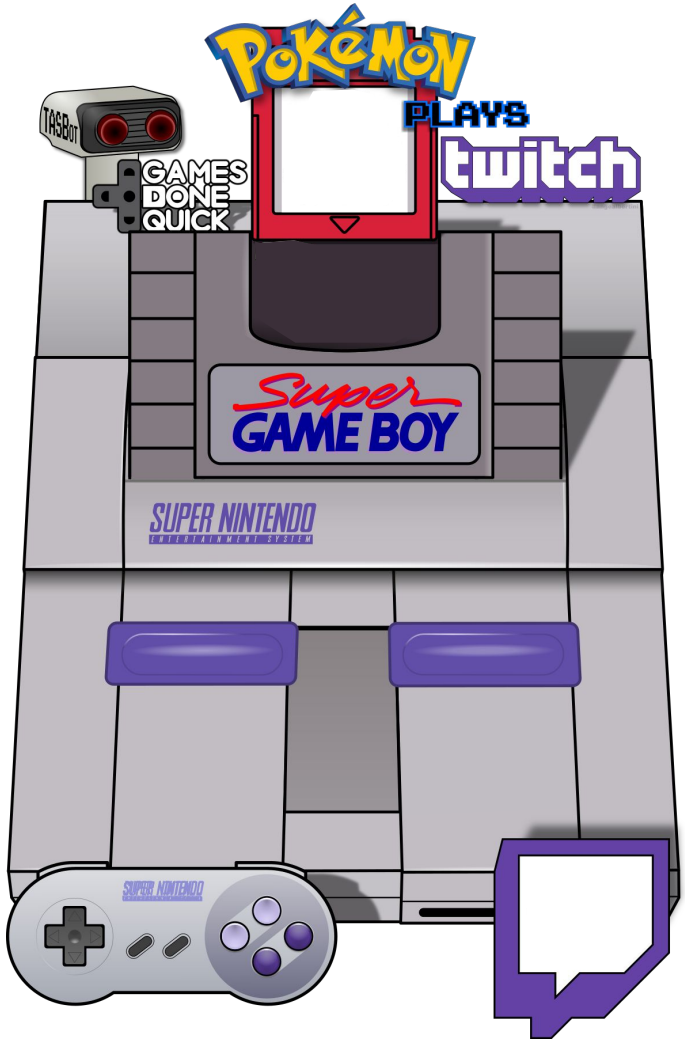
PROPRIETARY INFORMATION OF
INTECOM INC.
COMPANY CONFIDENTIAL

Pro casanare. He who has eyes to read, let him read!

€0, $0 USD, £0, 0 RSD, 0 SEK, $50 CAD. pocorgtfo10.pdf. January 16, 2016.

AS SEEN ON
PoC||GTFO

TASVIDEOS

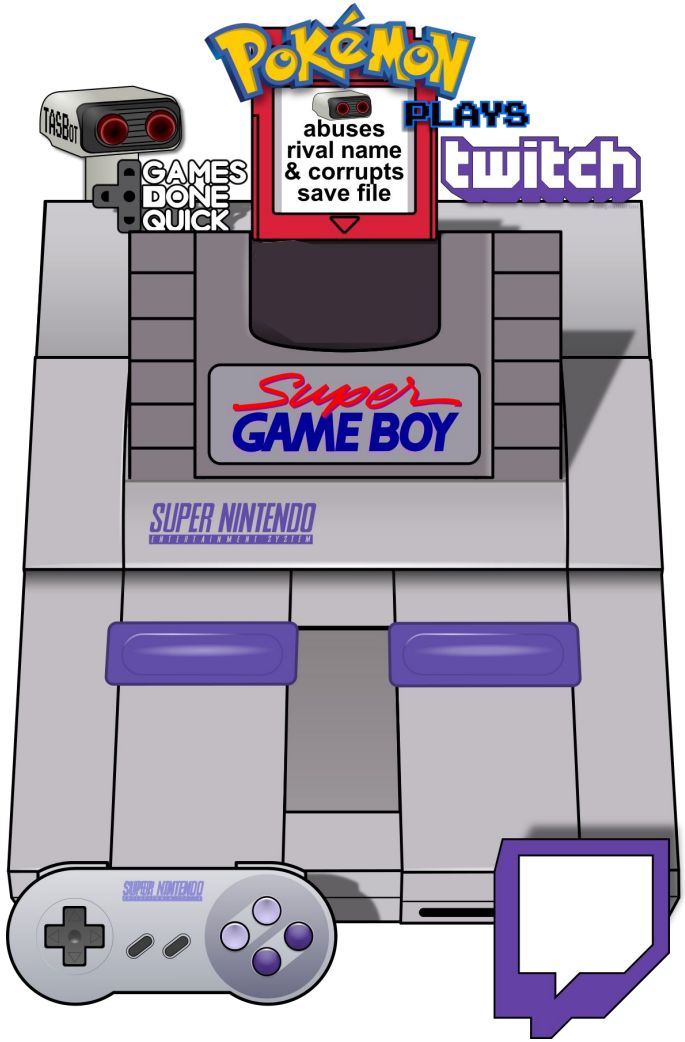


https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

credits: micro500, llari, p4plus2

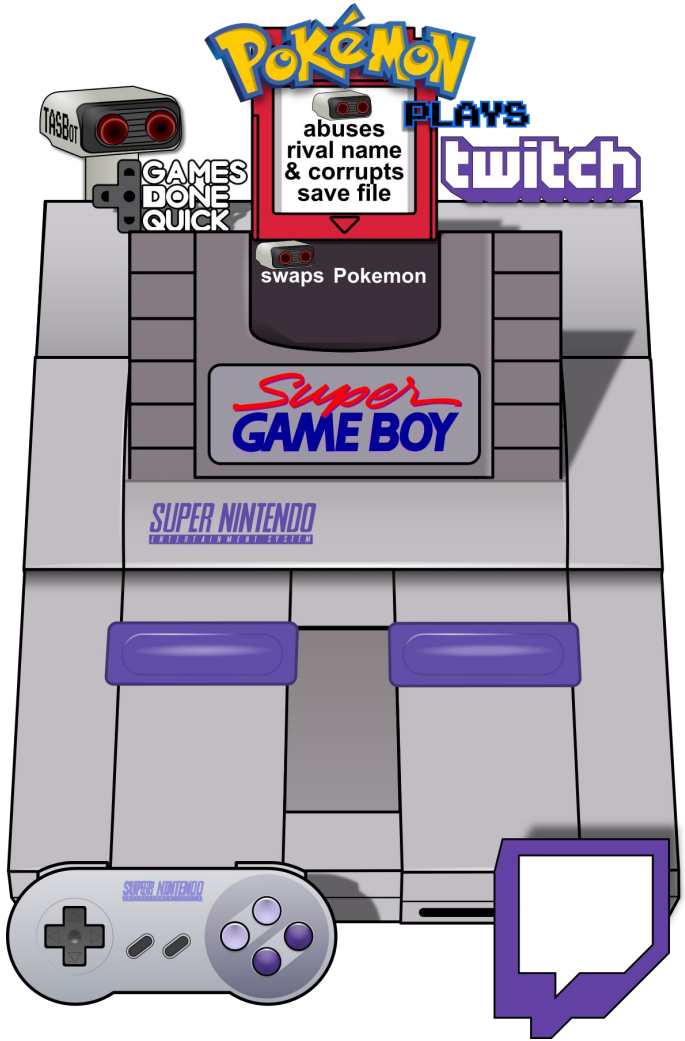
https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

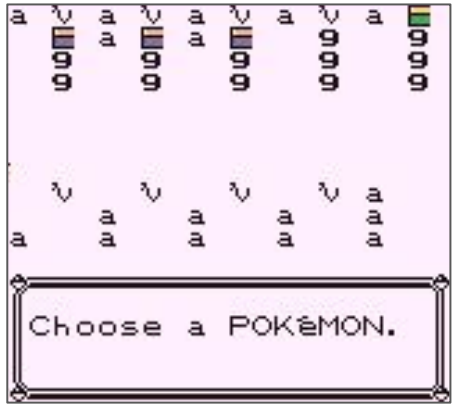
credits: micro500, llari, p4plus2



https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

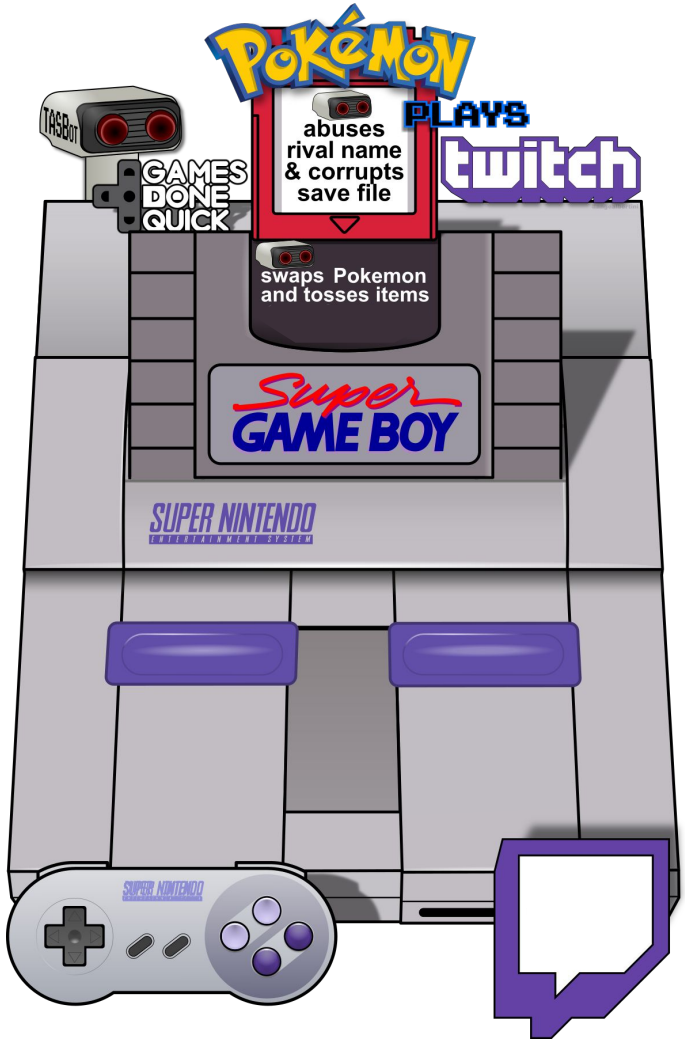
credits: micro500, llari, p4plus2

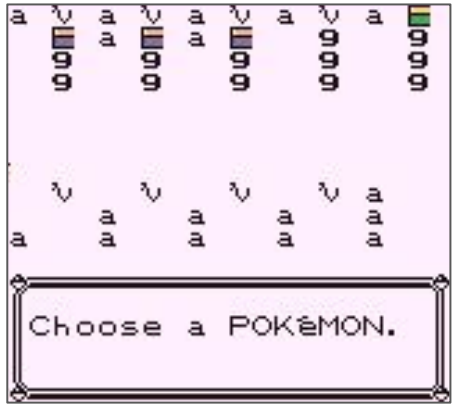




https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

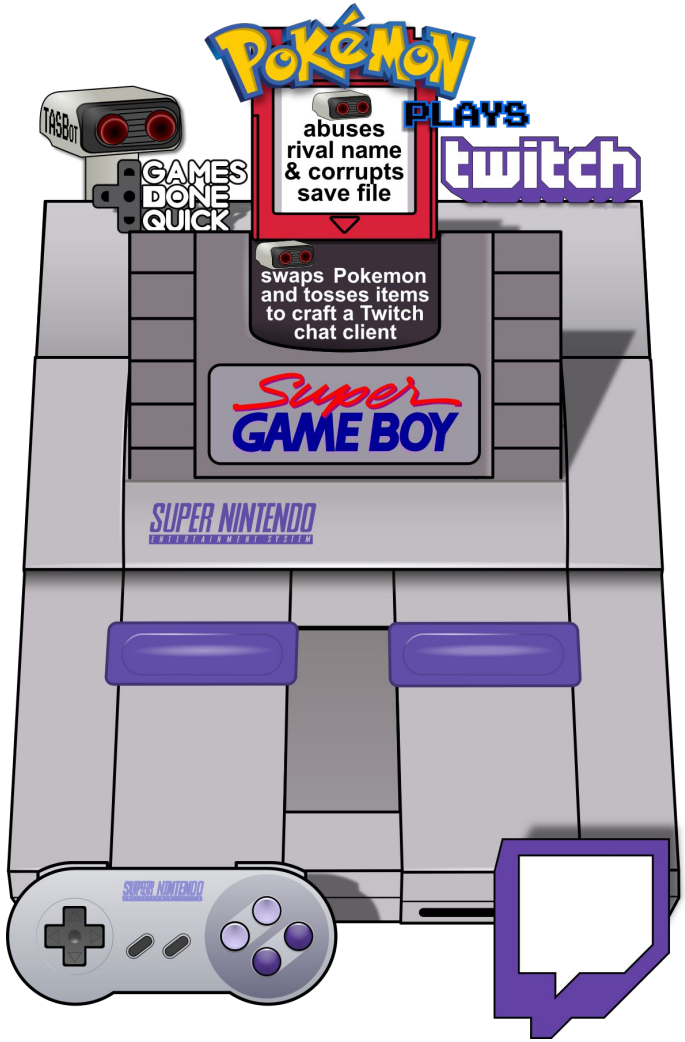
credits: micro500, llari, p4plus2

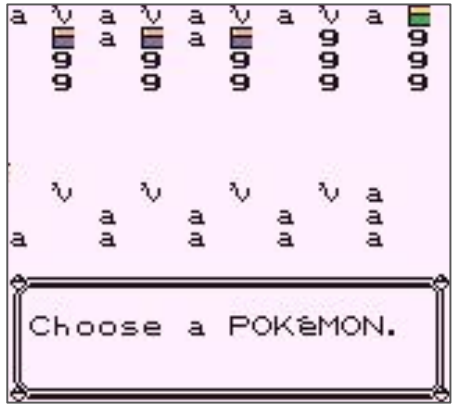




https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

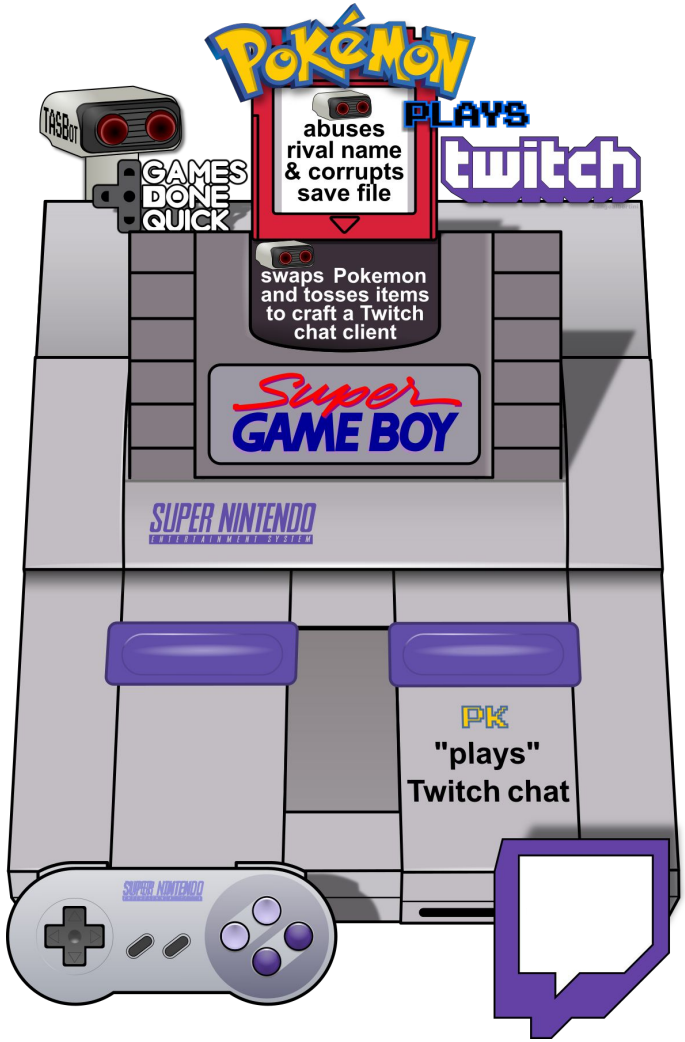
credits: micro500, llari, p4plus2

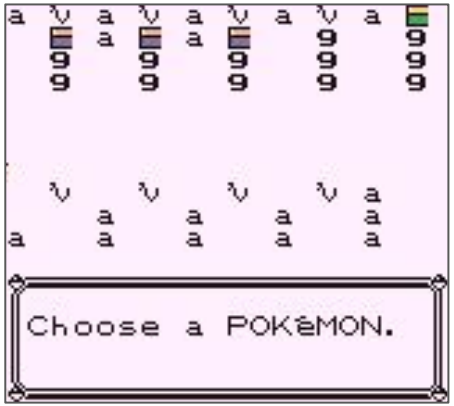




https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

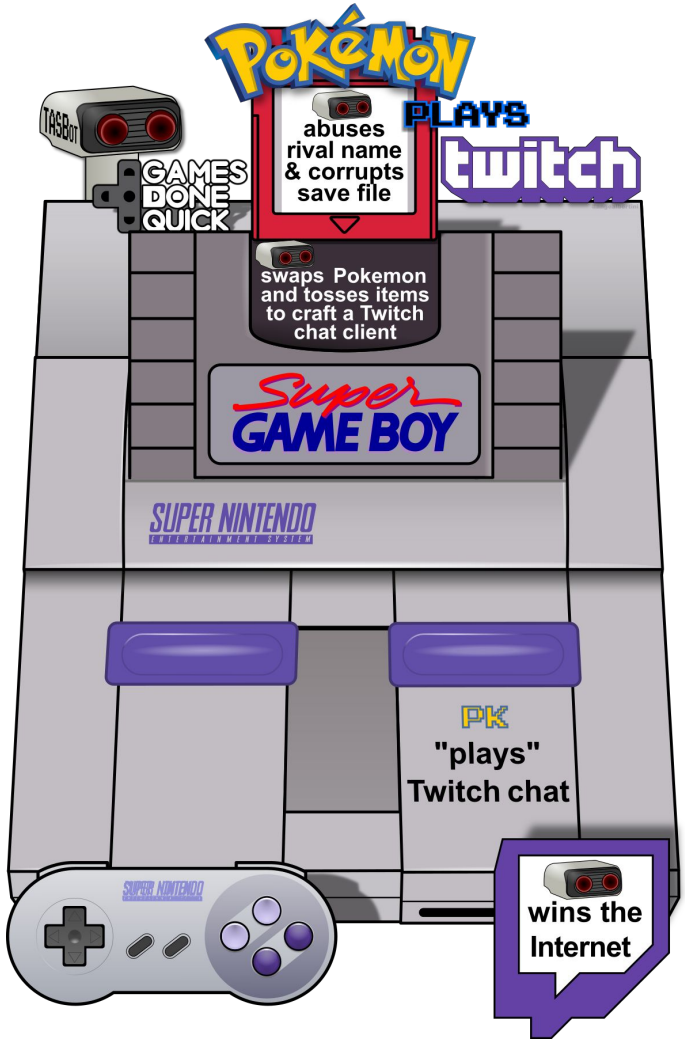
credits: micro500, llari, p4plus2

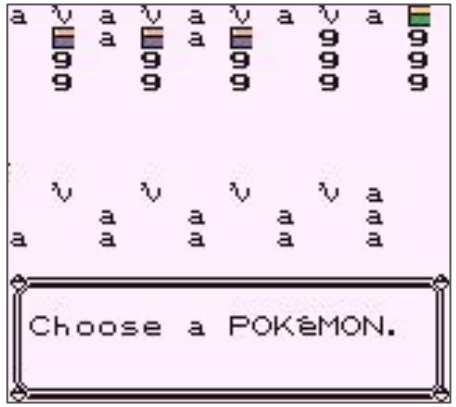


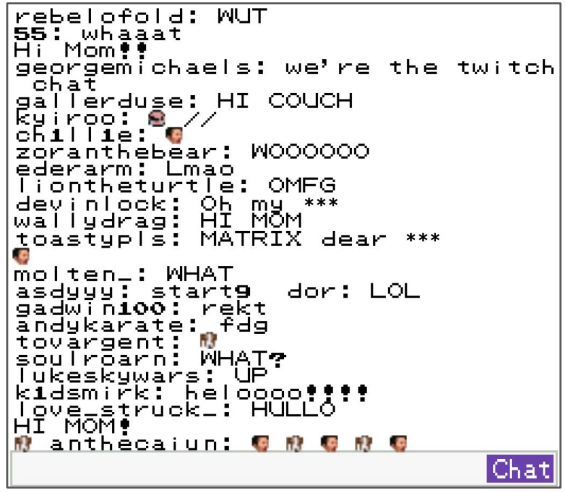


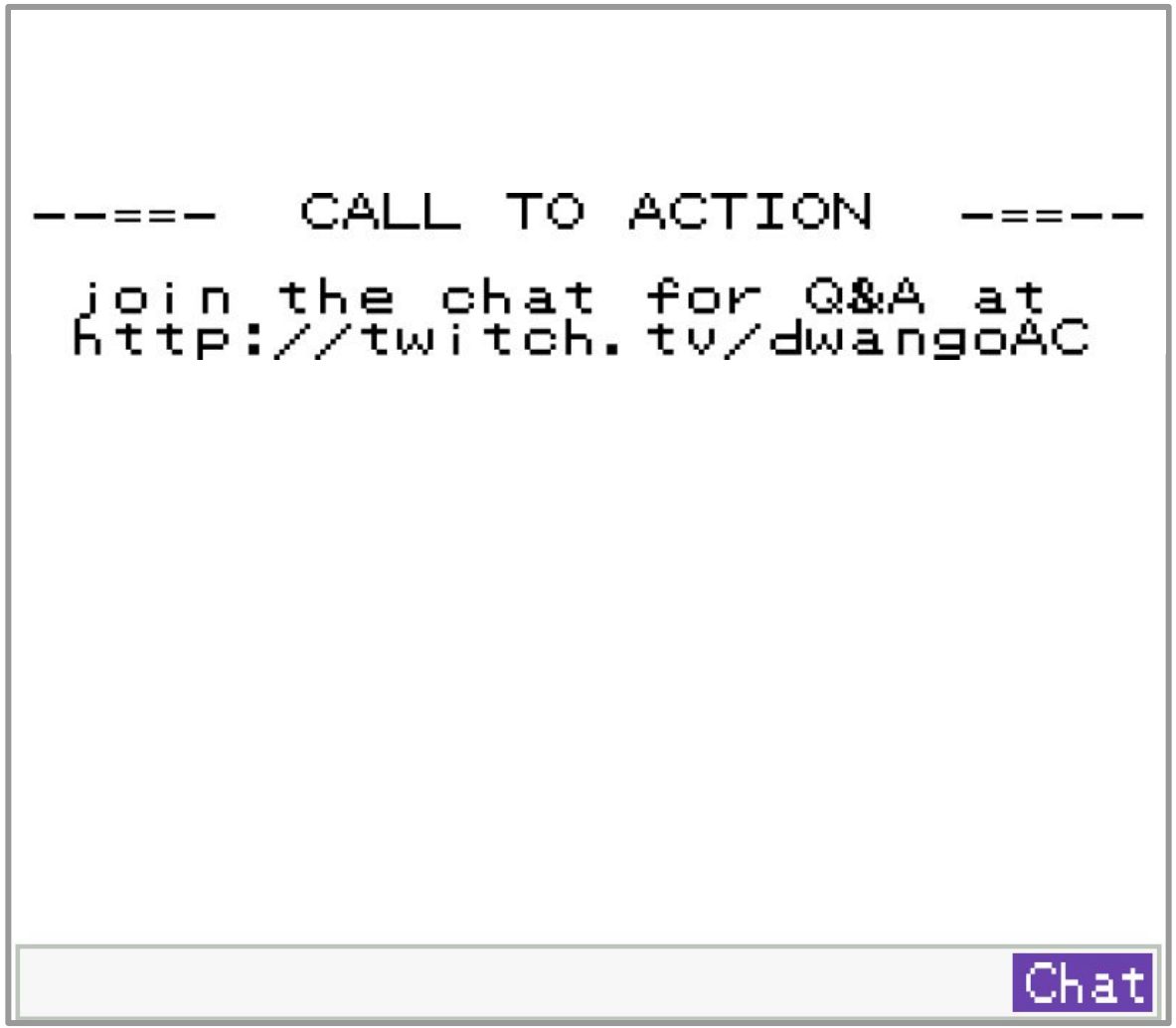
https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
http://arstechnica.com/gaming/2015/01/pokemon-plays-twitch-how-a-robot-got-irc-running-on-an-unmodified-snes/

credits: micro500, llari, p4plus2





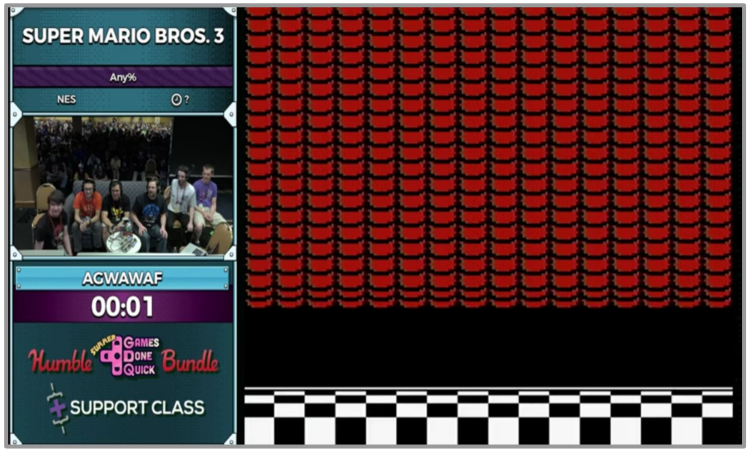



----- CALL TO ACTION -----
join the chat for Q&A at
http://twitch.tv/dwangoAC
Chat

https://youtu.be/EHfw-BEuRO8?t=1h13m50s

From boot...

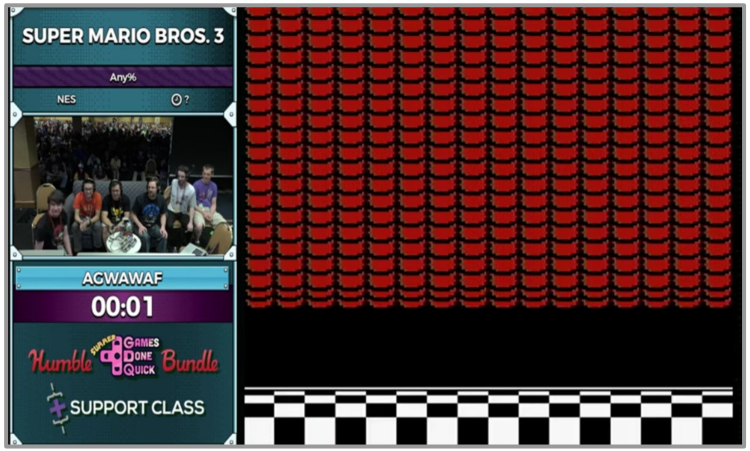
credits: total_ ais523



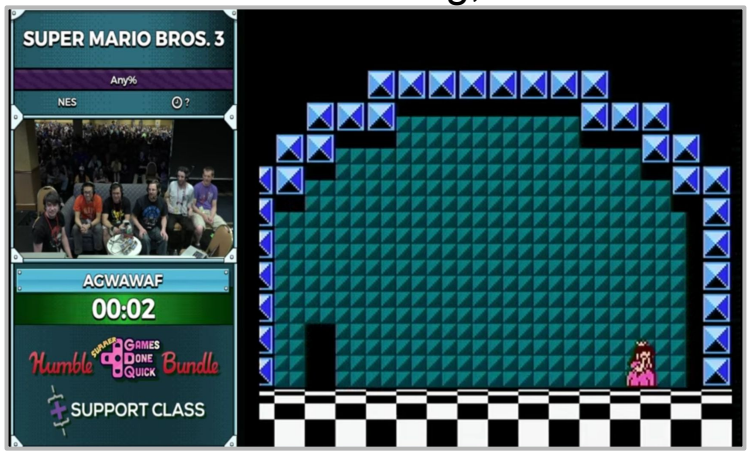
https://youtu.be/EHfw-BEuRO8?t=1h13m50s

From boot...

credits: total_ ais523



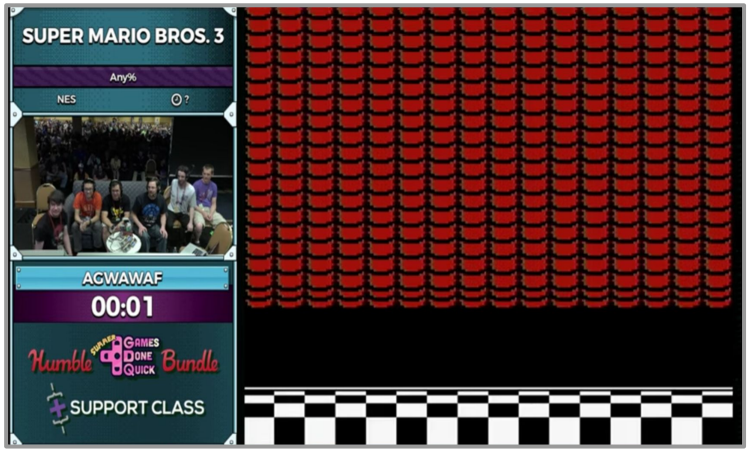
...to ending, in 16 frames!



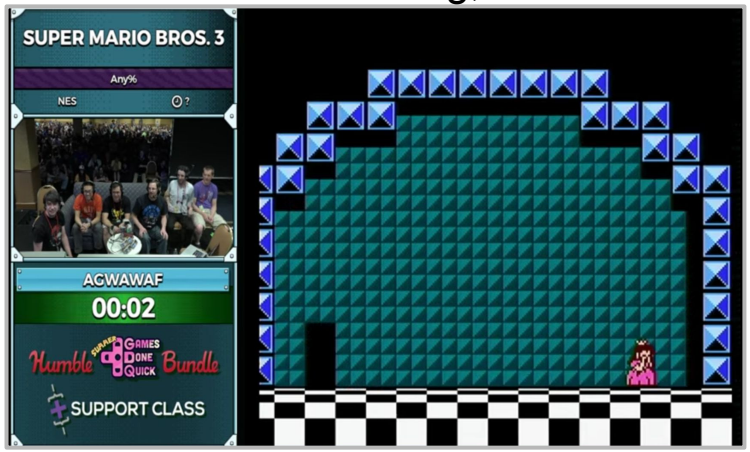
https://youtu.be/EHfw-BEuRO8?t=1h13m50s

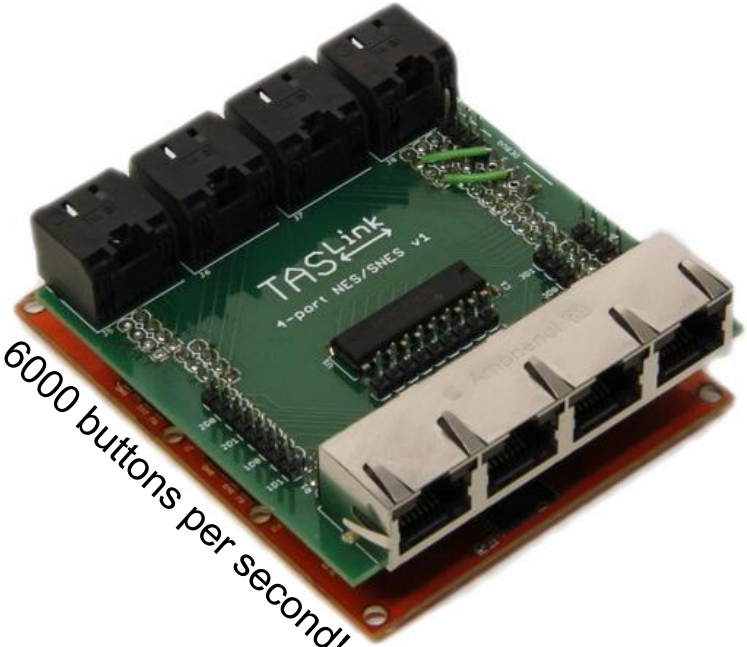
From boot...

credits: total_ ais523



...to ending, in 16 frames!

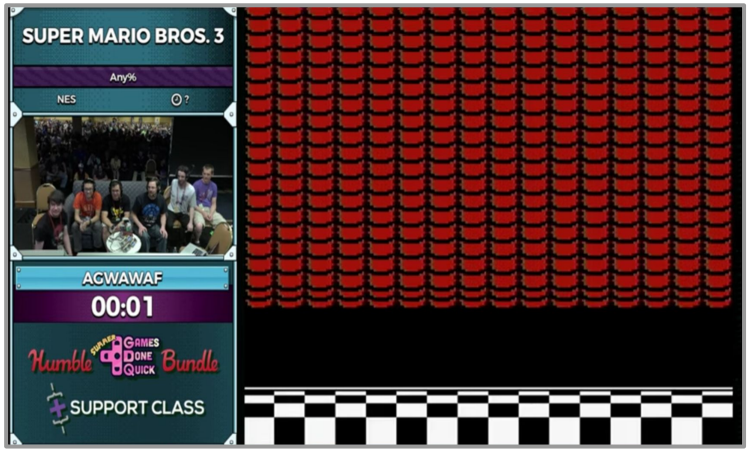




6000 buttons per second!

https://youtu.be/EHfw-BEuRO8?t=1h13m50s

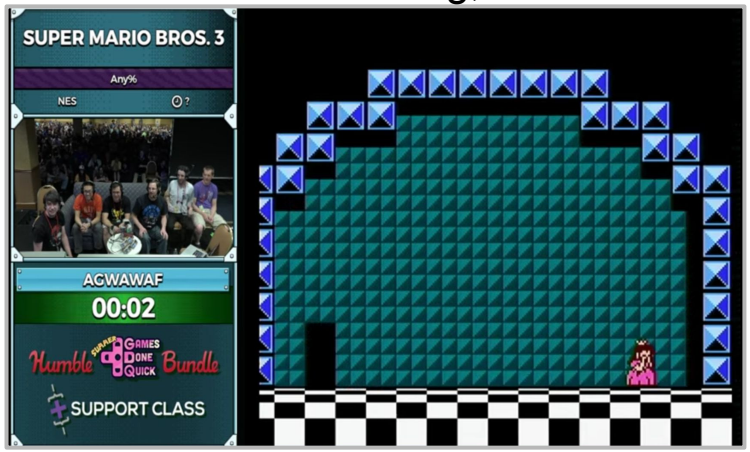
From boot...

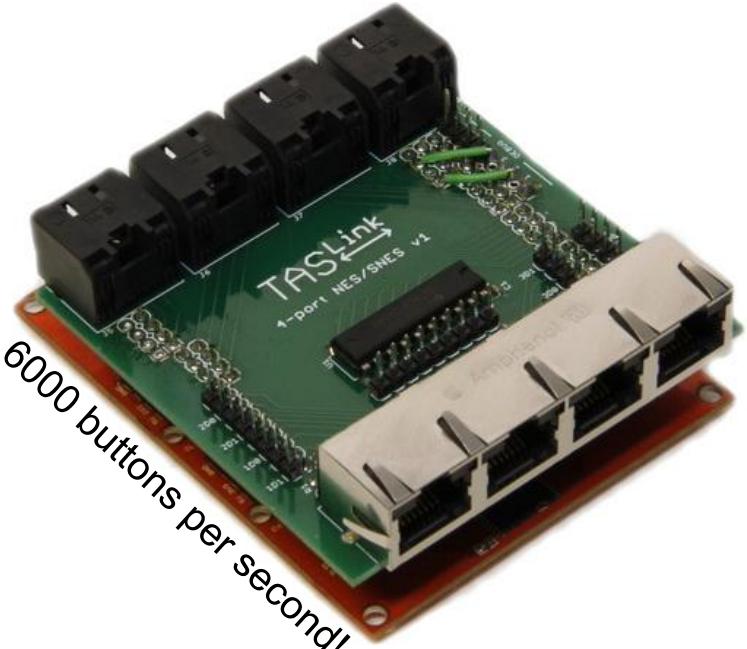


credits: total_ ais523

Some glitches are expected!

...to ending, in 16 frames!





6000 buttons per second!

DPCM memory

conflict

↓

game controller

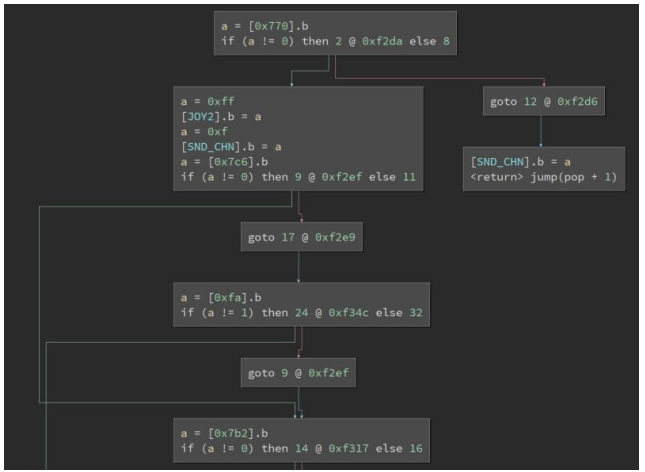
Flood weak controller code
to abuse raster interrupt
and take over execution

http://www.qmtpro.com/~nes/chipimages/#rp2a03
http://arstechnica.com/gaming/2016/07/how-to-beat-super-mario-bros-3-in-less-than-a-second/

TAS'ers lethal weapon

- More flexible than IDA
- Graph view, low level IL and annotation support
- Python scripting
- NES support: ability to add new mappers

BINARYNINJA



♫♪ Am I...

♫♪ Am I...

cheating?

♫♪ Am I...

cheating?

♫ No

♫♪ Am I...

cheating?

♫ No, I'm just looking for...

technical challenge & visual entertainment!

♫♪ Am I...

cheating?

♫ No, I'm just looking for...

technical challenge & visual entertainment!

♩ And I'm not the only one... ;)

♫ But more importantly....

♫ But more importantly....

over $200k USD

Raised for charity!

http://tasvideos.org/forum/viewtopic.php?p=437688#437688

Thanks to:

micro500 llari

Thanks to:

micro500 llari

p4plus2 Masterjun true

total_ psifertex rusty

Thanks to:

micro500 llari

p4plus2 Masterjun true

total_ psifertex rusty

TheAxeMan ange_ greenfly

ais523 and many, many others

Twitch.tv/dwangoAC

@MrTASBot

IN COLLABORATION
WITH ANGE ALBERTINI