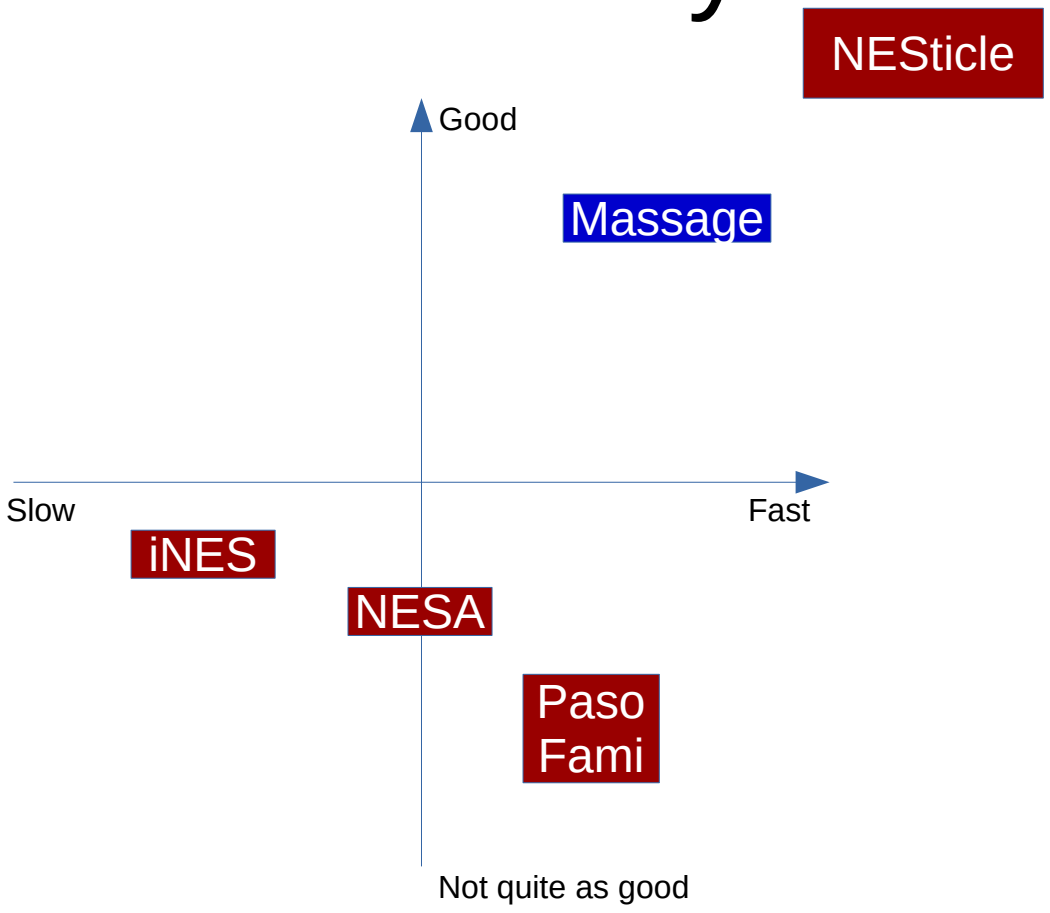
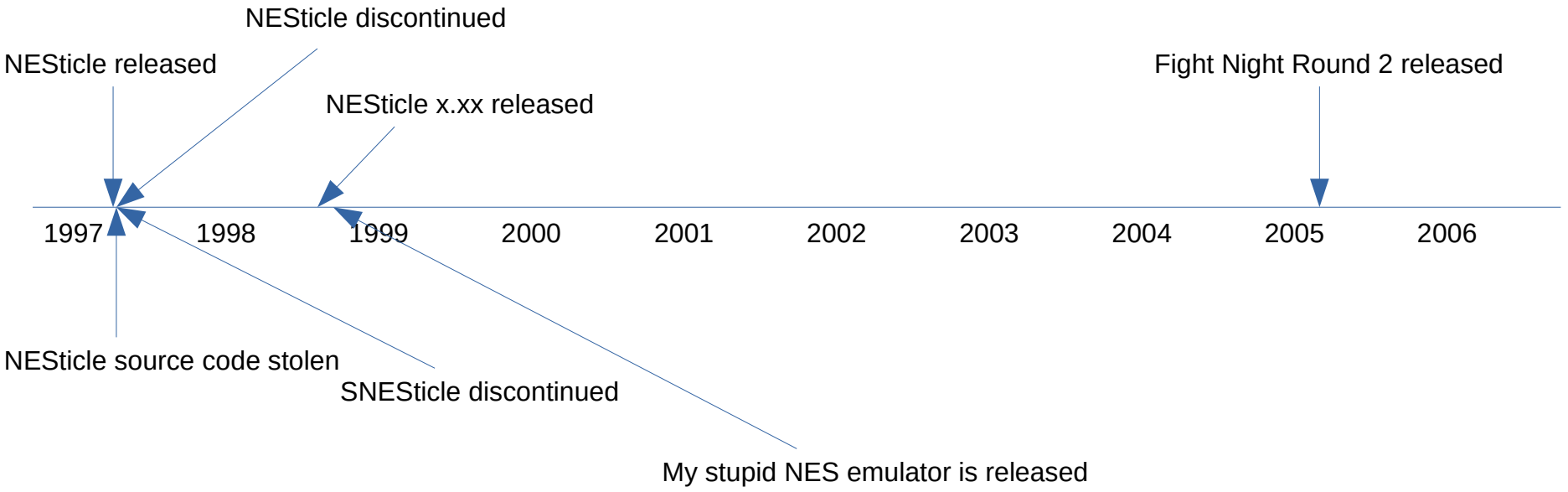
The SNESticle Liberation Project

Johannes Holmberg, josk@dfupdate.se

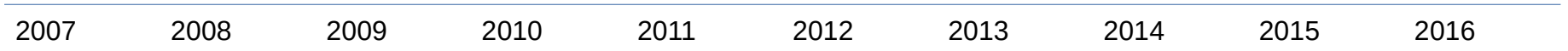
Emulators of early 1997



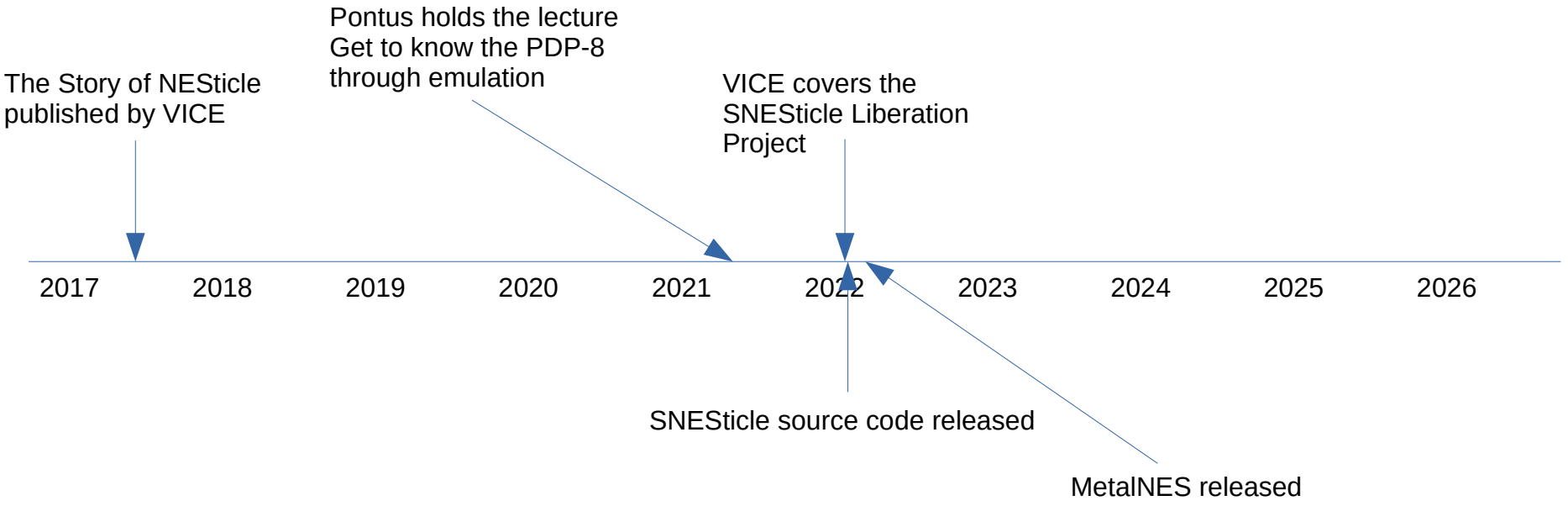
Important world events



Important world events



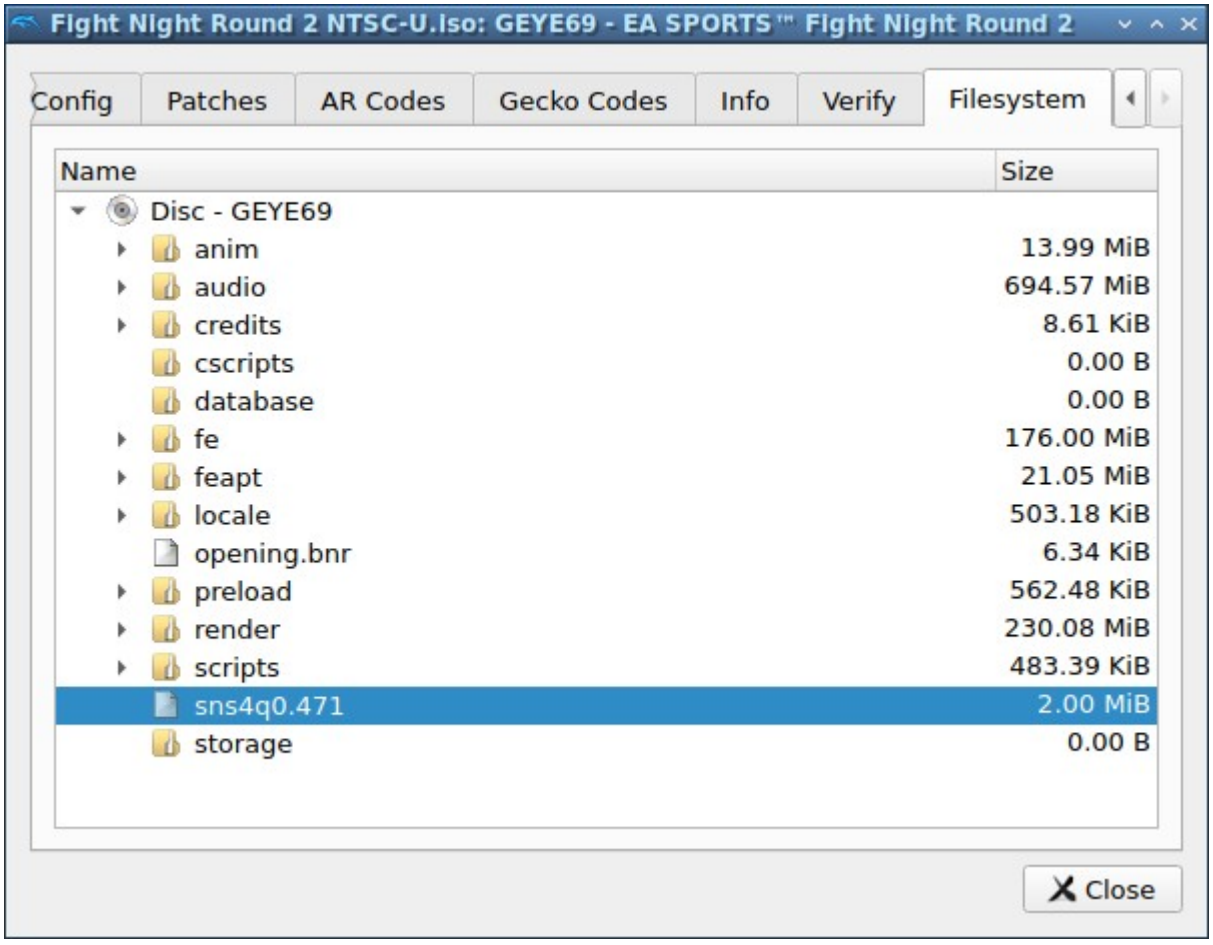
Important world events



Tools

- Dolphin (Gamecube emulator)
- Ghidra (RE tool)
- Hexcurse (hex editor)
- Python

fn22snesticle.py demo


Fight Night Round 2 NTSC-U.iso: GEYE69 - EA SPORTS™ Fight Night Round 2
Config
Patches
AR Codes
Gecko Codes
Info
Verify
Filesystem
Name
Size
Disc - GEYE69
anim 13.99 MiB
audio 694.57 MiB
credits 8.61 KiB
cscripts 0.00 B
database 0.00 B
fe 176.00 MiB
feapt 21.05 MiB
locale 503.18 KiB
opening.bnr 6.34 KiB
preload 562.48 KiB
render 230.08 MiB
scripts 483.39 KiB
sns4q0.471 2.00 MiB
storage 0.00 B
Close

PPC assembly crash course

- All instructions are 32 bits
- Operand order is destination, source
- Immediate values are typically 16 bits
- 32 general purpose registers (r0 – r31)
- Function arguments go in r3 - r10
- Return value is in r3
- Examples:
  - `addi r1, r2, 5 ; r1 = r2 + 5`
  - `ori r0, r0, 0 ; NOP (0x60000000)`
  - `stw r0, 4(r1) ; Store r0 in (r1 + 4)`

```
800ecadc 94 21 ff f8     stwu        r1,local_8(r1)          b 0x801a0254 ; jump to snesticle
800ecae0 7c 08 02 a6     mfspr       r0,LR
800ecae4 90 01 00 0c     stw         r0,local_res4(r1)
800ecae8 48 00 9d 39     bl          FUN_800f6820                                undefined FUN_800f6820(undefined...
800ecaec 38 60 00 00     li          param_9,0x0
800ecaf0 48 1b c4 f9     bl          FUN_802a8fe8                                undefined FUN_802a8fe8(int param...
800ecaf4 48 00 00 55     bl          FUN_800ecb48                                undefined FUN_800ecb48(void)
800ecaf8 4b ff fc 3d     bl          FUN_800ec734                                undefined FUN_800ec734(undefined...
800ecafc 3d 20 80 4c     lis         param_15=>PTR_s_Ref_pushed_boxer_1_804c0000,-0... = 8046b054
800ecb00 80 09 70 50     lwz         r0,offset DAT_804c7050(param_15)
800ecb04 2c 00 00 00     cmpwi       r0,0x0
800ecb08 41 82 00 24     beq         LAB_800ecb2c
800ecb0c 3d 20 80 4c     lis         param_15=>PTR_s_Ref_pushed_boxer_1_804c0000,-0... = 8046b054
800ecb10 38 00 00 01     li          r0,0x1
800ecb14 3c 60 80 0f     lis         param_9,-0x7ff1
800ecb18 90 09 70 a0     stw         r0,offset DAT_804c70a0(param_15)
800ecb1c 38 63 cb 7c     subi        param_9=>FUN_800ecb7c,param_9,0x3484
800ecb20 38 80 00 00     li          param_10,0x0
800ecb24 38 a0 00 00     li          param_11,0x0
800ecb28 48 2d cb c1     bl          FUN_803c96e8                                undefined FUN_803c96e8(int param...

                     LAB_800ecb2c                                    XREF[1]:     800ecb08(j)
800ecb2c 38 60 00 00     li          param_9,0x0
800ecb30 38 80 00 00     li          param_10,0x0
800ecb34 48 00 00 49     bl          FUN_800ecb7c                                undefined4 FUN_800ecb7c(undefine...
800ecb38 80 01 00 0c     lwz         r0,local_res4(r1)
800ecb3c 7c 08 03 a6     mtspr       LR,r0
800ecb40 38 21 00 08     addi        r1,r1,0x8
800ecb44 4e 80 00 20     blr
```

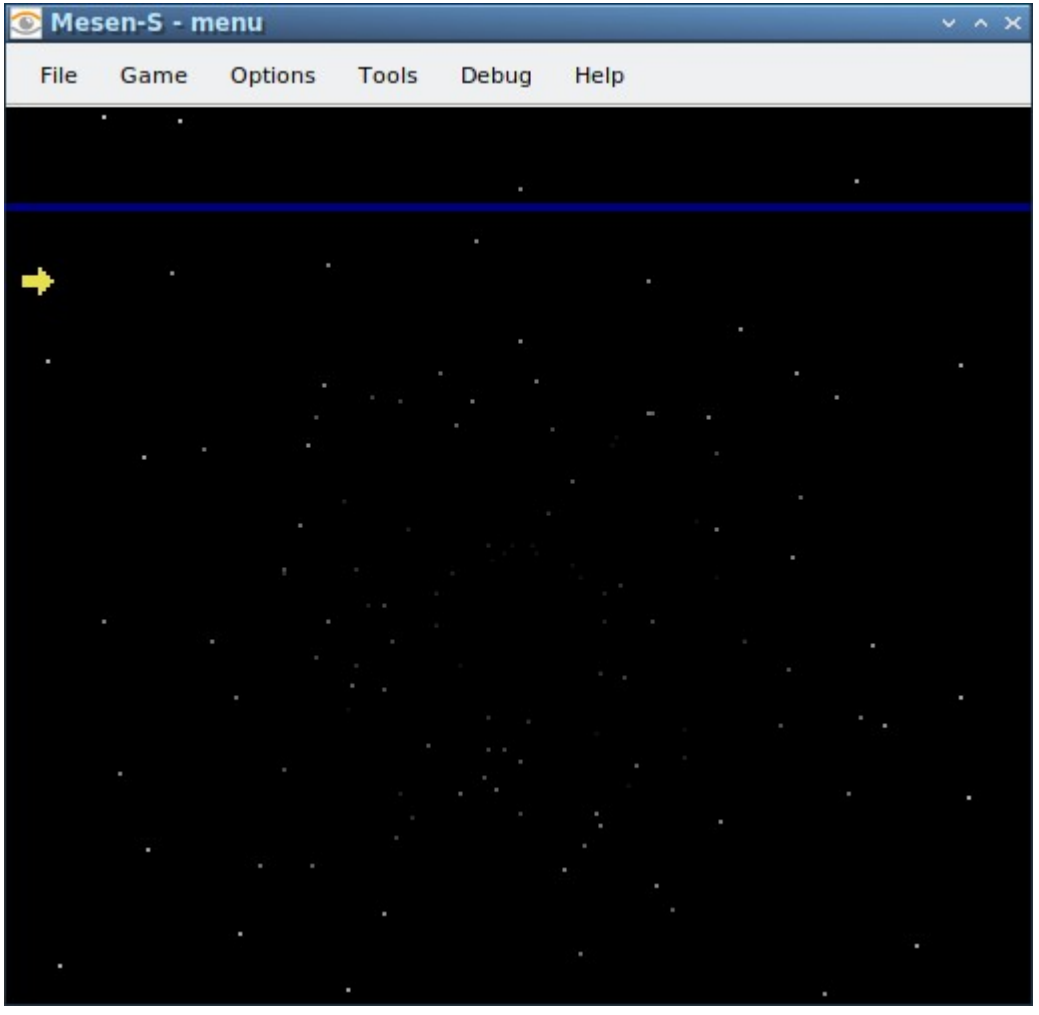
How to slap a menu onto this?

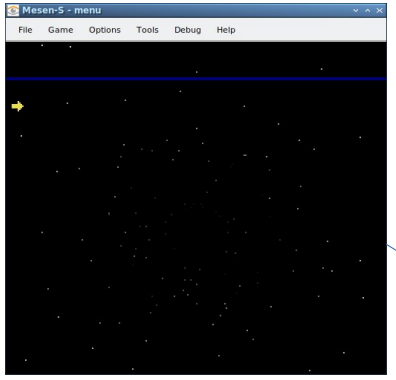
- Gamecube is inscrutable modern hardware
- Don’t want to setup a dev environment
- Difficult to know which code is safe to overwrite
- If only there was a friendlier environment

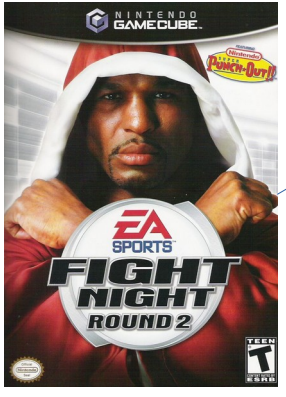
Need more tools!

- Mesen-SX (SNES emulator)
- cc65/ca65 (65816 assembler)
- More python

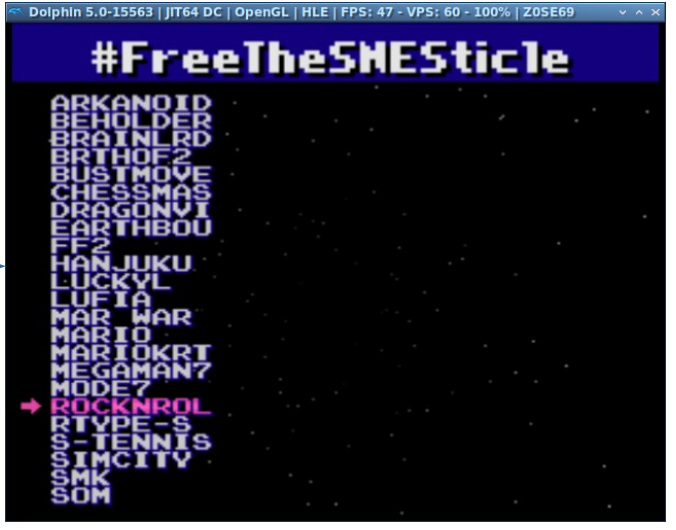

Mesen-S - menu
File
Game
Options
Tools
Debug
Help
#FreeTheSNESticle
ARKANOID
BEHOLDER
BRAINLRD
BRTHOF2
BUSTMOVE
CHESSMAS
DRAGONVI
EARTHBOU
FF2
HANJUKU
LUCKYL
LUFIA
MAR WAR
MARIO
MARIOKRT
MEGAMAN7
MODE7
ROCKNROL
RTYPE-S
S-TENNIS
SIMCITY
SMK
SOM


Mesen-S - menu
File
Game
Options
Tools
Debug
Help





fn22snesticle.py



ISO file system

Old iso file system contents:

sns4q0.471 (smw or something)
opening.bnr

New iso file system contents:

sns4q0.471 (menu.sfc)
opening.bnr
01 (Super Punch Out!!)
02 (smw.sfc)
03 (zelda3.sfc)
…

(The GC binary “main.dol” is not part of the file system)

ISO file system

New iso file system contents:

sns4q0.471 (menu.sfc)
opening.bnr
01 (Super Punch Out!!)
02 (smw.sfc)
03 (zelda3.sfc)
…

SNES ROM contents:

SMW (“02”)
SUPER PUNCH OUT!! (“01”)
ZELDA3 (“03”)
...

Jump destination

Delicious code real-estate

```
801a0250 90 09 cc 20     stw        r0,-0x33e0(param_15)=>DAT_804ccc20              = 00000001h
801a0254 4b fd 18 21     bl         FUN_80171a74                                    undefined4 * FUN_80171a74(undefi...
801a0258 4b fd 33 91     bl         FUN_801735e8                                    undefined FUN_801735e8(undefined...
801a025c 48 0e da e1     bl         snesticle_FUN_8028dd3c                          undefined snesticle_FUN_8028dd3c...
801a0260 48 00 00 f0     b          LAB_801a0350

                     LAB_801a0264                                        XREF[1]:     801a0240(j)
801a0264 4b e6 46 b5     bl         FUN_80004918                                    int * FUN_80004918(undefined8 pa...
801a0268 3b c0 00 00     li         r30,0x0
801a026c 38 80 00 00     li         param_10,0x0
801a0270 38 a0 00 05     li         param_11,0x5
801a0274 4b e6 55 c5     bl         FUN_80005838                                    undefined FUN_80005838(int param...
801a0278 3b a0 00 01     li         r29,0x1
801a027c 4b e6 46 9d     bl         FUN_80004918                                    int * FUN_80004918(undefined8 pa...
801a0280 3b e0 00 00     li         r31,0x0
801a0284 38 a0 00 04     li         param_11,0x4
801a0288 38 80 00 01     li         param_10,0x1
801a028c 4b e6 55 ad     bl         FUN_80005838                                    undefined FUN_80005838(int param...
801a0290 4b f3 de 95     bl         FUN_800de124                                    undefined * FUN_800de124(undefin...
801a0294 38 80 00 01     li         param_10,0x1
801a0298 4b f3 e0 85     bl         FUN_800de31c                                    undefined FUN_800de31c(undefined...
801a029c 4b f7 4c dd     bl         FUN_80114f78                                    undefined FUN_80114f78(void)
801a02a0 48 08 b0 6d     bl         FUN_8022b30c                                    undefined * FUN_8022b30c(undefin...
801a02a4 48 08 a4 61     bl         FUN_8022a704                                    undefined FUN_8022a704(undefined...
801a02a8 4b f4 da a5     bl         FUN_800edd4c                                    undefined FUN_800edd4c(undefined...
801a02ac 93 dc 01 44     stw        r30,0x144(r28)
801a02b0 4b f6 b0 89     bl         FUN_8010b338                                    undefined * FUN_8010b338(undefin...
801a02b4 93 a3 00 0c     stw        r29,0xc(param_9)
801a02b8 4b f4 da 15     bl         FUN_800edccc                                    undefined FUN_800edccc(undefined...
801a02bc 4b f4 c9 9d     bl         finish_loading_FUN_800ecc58                     undefined finish_loading_FUN_800...
```

Jump destination

```
801a0250 90 09 cc 20     stw        r0,-0x33e0(param_15)=>DAT_804ccc20        = 00000001h
801a0254 4b fd 18 21     bl         FUN_80171a74                              undefined4 * FUN_80171a74(undefi...
801a0258 4b fd 33 91     bl         FUN_801735e8                              undefined FUN_801735e8(undefined...
801a025c 48 0e da e1     bl         snesticle_FUN_8028dd3c                    undefined snesticle_FUN_8028dd3c...
```

```
lis  r3, 0x8063
addi r3, r3, -0x5574  ; SNES memory pointer (0x8062aa8c)
lwz  r3, 0x24(r3)     ; Read game file name
lis  r4, 0x8049
addi r4, r4, 0x63ac   ; ROM filename pointer (0x804963ac (=SNS4Q...))
stw  r3, 0(r4)        ; Store game file name
lis  r3, 0x8049
addi r3, r3, -0x19e8  ; Z check instruction (0x8028e618)
lis  r4, 0x6000       ; r4 = NOP
stw  r4, 0(r3)        ; Never exit snesticle
b    0x801a025c
```

Jump destination

```
801a0250 90 09 cc 20     stw        r0,-0x33e0(param_15)=>DAT_804ccc20        = 00000001h
801a0254 4b fd 18 21     bl         FUN_80171a74                              undefined4 * FUN_80171a74(undefi...
801a0258 4b fd 33 91     bl         FUN_801735e8                              undefined FUN_801735e8(undefined...
801a025c 48 0e da e1     bl         snesticle_FUN_8028dd3c                    undefined snesticle_FUN_8028dd3c...
```

```
lis  r3, 0x8063
addi r3, r3, -0x5574  ; SNES memory pointer (0x8062aa8c)
lwz  r3, 0x24(r3)     ; Read game file name
lis  r4, 0x8049
addi r4, r4, 0x63ac   ; ROM filename pointer (0x804963ac (=SNS4Q...))
stw  r3, 0(r4)        ; Store game file name
lis  r3, 0x8049
addi r3, r3, -0x19e8  ; Z check instruction (0x8028e618)
lis  r4, 0x6000       ; r4 = NOP
stw  r4, 0(r3)        ; Never exit snesticle
addi r4, 0, 0x100
bl   ICInvalidateRange
b    0x801a025c
```

fn22snesticle.py demo 2

main 1 branch 0 tags

Go to file Code

Icer SNESticle source code (circa ~2004) `9590ebf` on Jan 13 **2** commits

Gep	SNESticle source code (circa ~2004)	3 months ago
SNESticle	SNESticle source code (circa ~2004)	3 months ago
LICENSE	Initial commit	3 months ago
README.md	SNESticle source code (circa ~2004)	3 months ago

README.md

SNESticle

SNESticle source code (circa ~2004) May build on a ps2 or dreamcast homebrew dev environment, or maybe on windows.

You guys have way too much free time.

About

SNESticle source code (circa ~2004)

Readme

MIT License

314 stars

15 watching

33 forks

Releases

No releases published

Packages

No packages published

Languages

C 53.1% **C++** 24.4%

SourcePawn 14.2% **Makefile** 3.8%

Assembly 2.4% **JavaScript** 1.2%

Other 0.9%

breakthetargets @breakthetargets · Jan 18
github.com/iaddis/SNEStic...

SNESticle's source code has been released by it's author!

4 18 82

Villodre
@AVillodre

Replying to @breakthetargets and @Denymetanol

Just after a day of so of this initiative:
dataswamp.org/~josk/snesticl...

It's a great gesture by Iaddis

8:24 AM · Jan 18, 2022 · Twitter Web App

calima

Posts: 1429
Joined: Tue Oct 06, 2015 10:16 am

Re: SNESTicle released, with article.
by **calima** » Tue Jan 18, 2022 9:25 am

Ha, excellent trolling. Two days after someone spends months REing the GC binary, release source.

Hayama Akito @TheBurpMan · Jan 19

Tuvieron que pasar 25 años... y ocurrió: señoras y señores, SNESticle

github.com

GitHub - iaddis/SNESticle: SNESticle source code (circa ~2004)

SNESticle source code (circa ~2004). Contribute to iaddis/SNESticle development by creating an account on GitHub.

6 4 17

pixel_meow

@aran_sam_us

Replying to @TheBurpMan

Y nisiquiera fue porque "ahh voy a tirar el código fuente como preservación histórica", sino que porque un weon aburrido, con ingeniería inversa, cachó que el emulador entero estaba metido dentro del Fight Night Round 2 de Gamecube jaja.

Translated from Spanish by Google

And it wasn't even because "ahh I'm going to throw away the source code as historical preservation", but because some boring, reverse-engineered guy figured out that the entire emulator was stuffed into Gamecube's Fight Night Round 2 haha.

2:03 AM · Jan 20, 2022 · Twitter for Android

Thanks for coming

https://dataswamp.org/~josk/snesticle

https://github.com/jolmberg/fn22snesticle

https://twitter.com/jolmberg

josk@dfupdate.se