Bet You Never Played an NES Game Like This

Innovating Under Limitations

12 Apr 2019 - CypherCon 4.0 - Milwaukee, WI

Presented By

Vi Grey
Technology Researcher
Software Engineer

vigrey.com

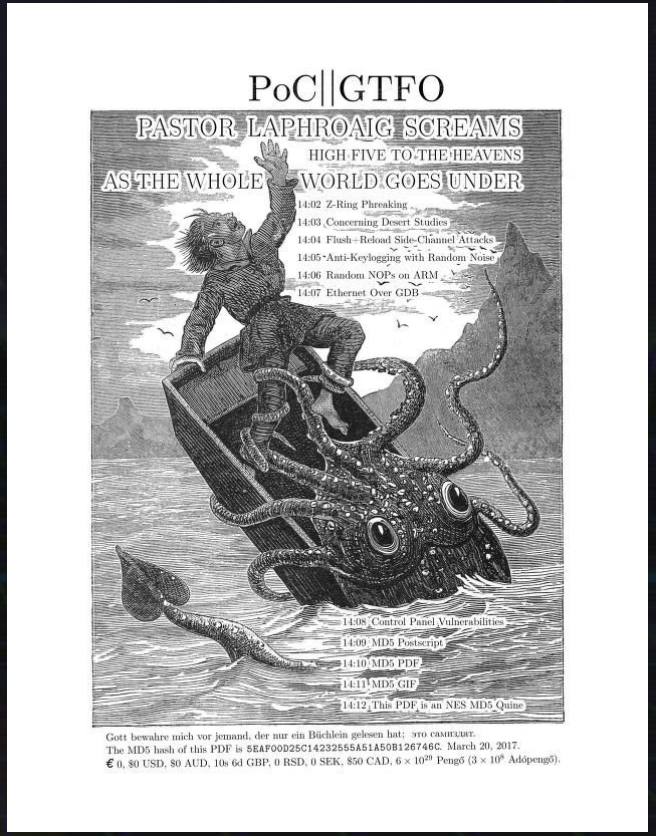
Who am I?

- Background in Software Development and Technology Research
- Affinity for Information Theory
- Run an interactive technology studio
- Accidental NES game developer
- "Retro" category winner of the DEFCON 26 Badge Life contest

This Talk Relates to the NES

But Why? (Origin Story)

- Issue 0x14 of Proof of Concept or GTFO
- "This PDF is an NES ROM that prints its own MD5 hash!"
- PDF of that issue was also an NES ROM
- Why not have my resume be a copy of Super Mario Bros?
- I failed...



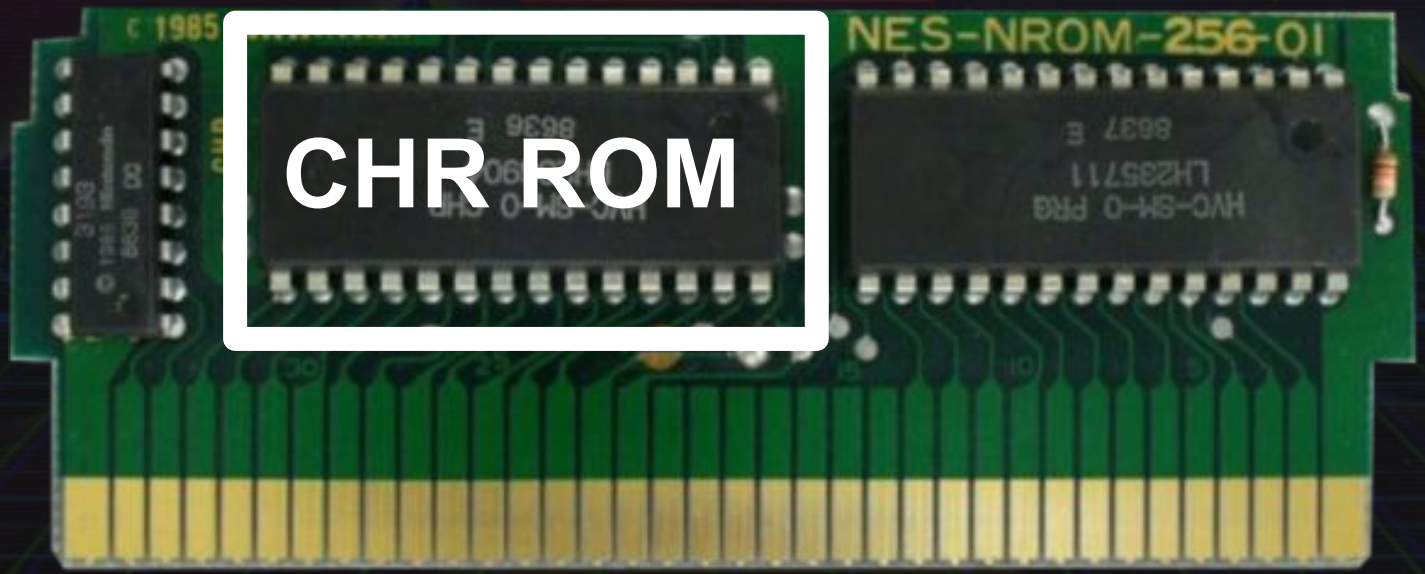
So... I learned to program for the NES

Limitation Note

We'll limit ourselves cartridge wise to what was possible back in 1985 for Super Mario Bros.

The NROM-256 Board

The NROM-256 Board



CHR ROM

8 KiB of Graphical Data

Sprites and Background Tiles

CHR ROM
8 KiB

The NROM-256 Board

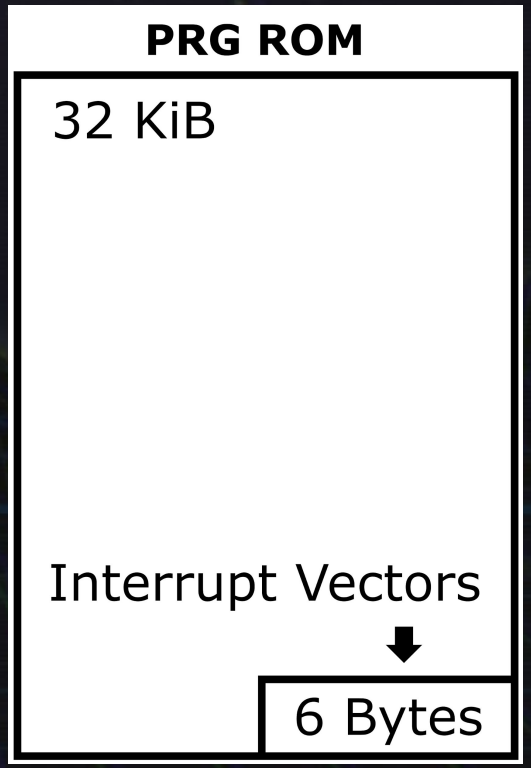
PRG ROM

32 KiB of Program Data

6502 Machine Code

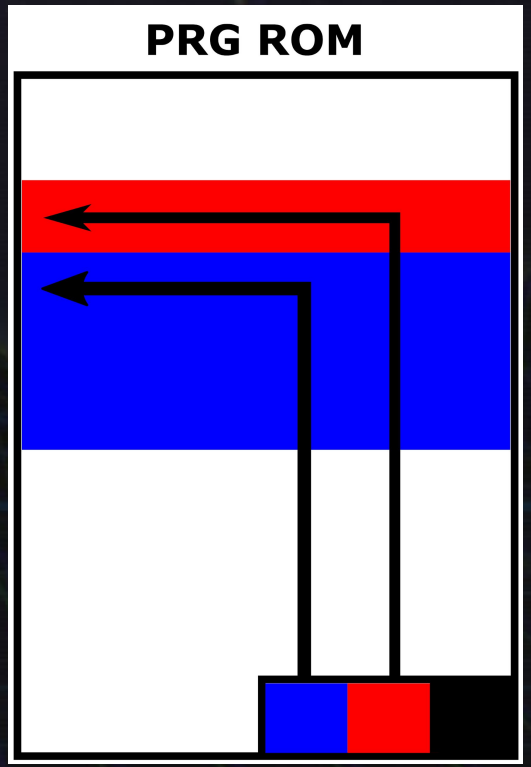
Last 6 Bytes are 6502 CPU Interrupts

- Address of code that runs at frame start
- Address of code that runs on Reset
- IRQ (Interrupt Request)



PRG Interrupts

- First 2 bytes Frame Start Code Address
- Second 2 bytes Reset Vector Code Address
- YOU define where code starts
- Empty spaces abound!



We Can Do
Something with The
Empty PRG Space

Polyglot Files

- Polyglot (n): a person who knows and is able to use several languages
- Polyglot File: a file that simultaneously works as several types of files
- Imagine downloading a .jpg image that works as a .zip file

What Makes a File a File?

- Download a random .jpg file. Change the extension to .mp3. Will it work in a music app?
- It fails to open the data as a song, but why?
- The file extension doesn't make the file, the file data does

File Formats

- Not every file format looks the same
- File formats determine if the file data is correct
- File Formats are often determined by "Magic Strings" and Header Data

Header Data

- Often times at the beginning of a file (but not always)
- Tells programs what type of file is running
- May contain metadata

Metadata

- Extra data given about a file
- May contain:
  - Comment
  - Creation or Last Saved Date and Time
  - GPS Coordinates/Location
  - Etc…
- NOT the file data

Magic Strings

- NES ROM - NES<1A>
- JPEG Image - <FF><D8><FF>
- PDF - %PDF-
- ZIP - PK

Making a Polyglot File Work

Imagine a plot of land

- Barn - The land is a farm
- Jungle Gym - The land is a park
- Telescope - The land is an observatory

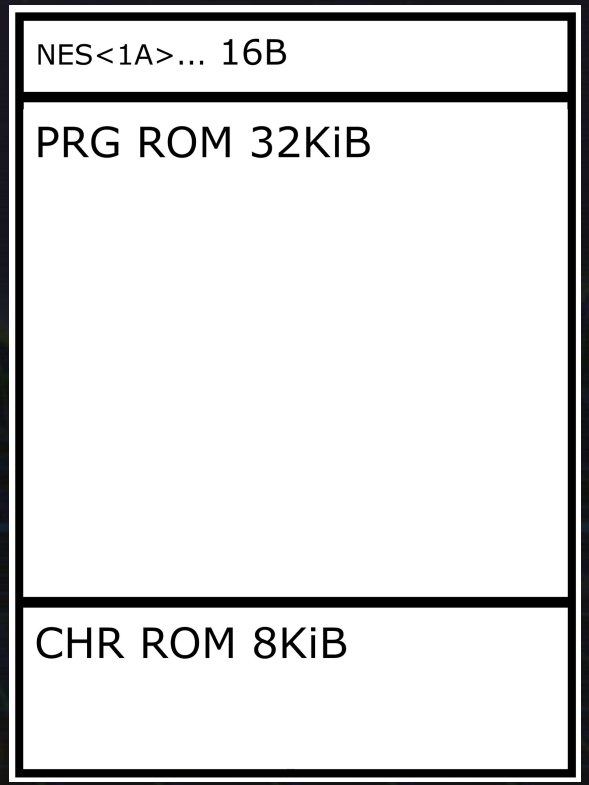
All three can be true at the same time

Looking for "Headers" in Different Locations

- Some files start with the header (NES, JPEG)
- Some files are a bit flexible (PDF, HTML)
- Some files expect the "header" to be near the end (ZIP, 7z, RAR)

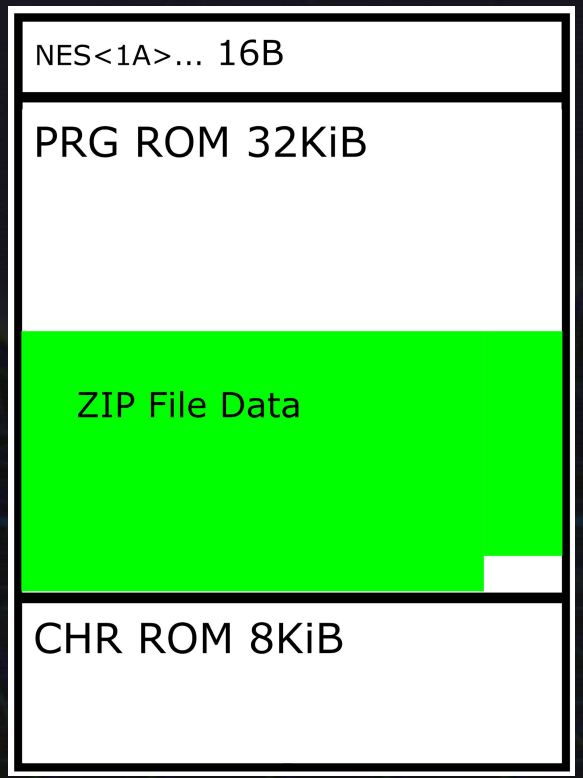
NROM-256 ROM for Emulators

- 16 Byte Header at start
- 32KiB PRG ROM data
- 8KiB CHR ROM data

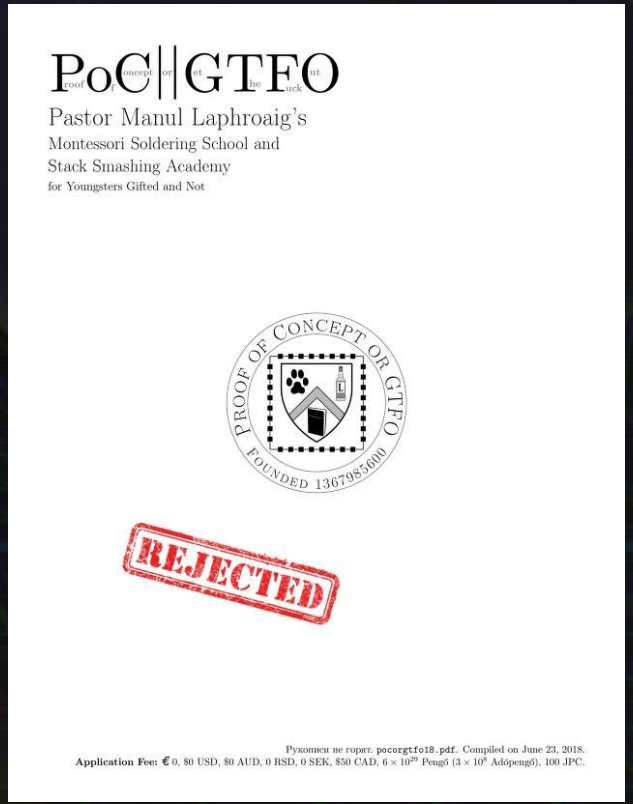


Making an NES ROM That Is Also a ZIP File

- NES ROM (iNES) Header must be at beginning
- ZIP file "header" must be near the end



A Game That Is Also ZIP File That Is A Copy of Its Source Code



ROM Chips

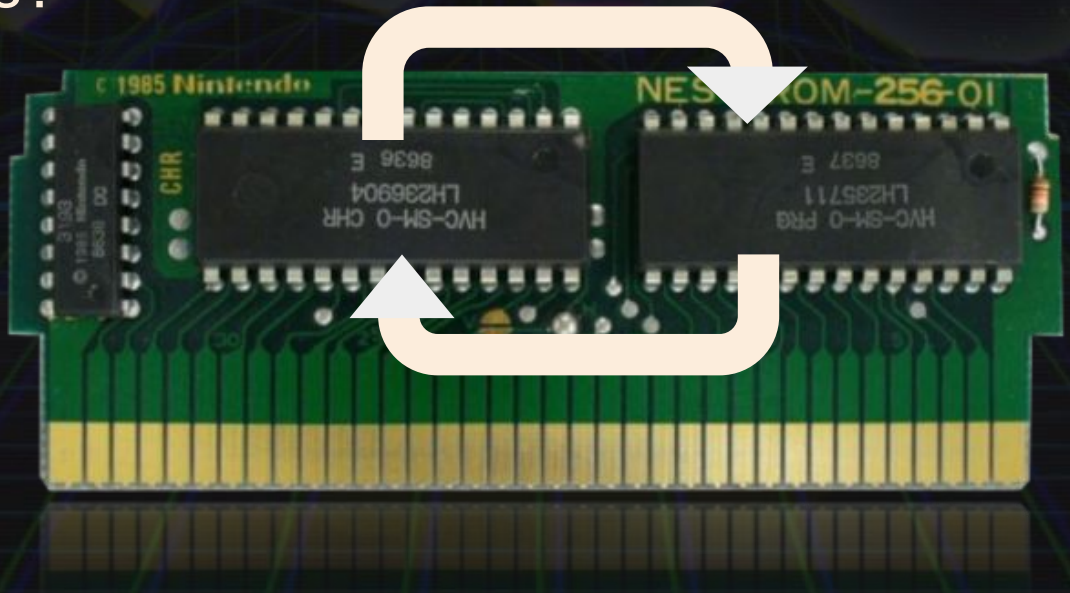
PRG ROM burned onto 27C256 EPROM

Erasable **P**rogrammable **R**ead **O**nly **M**emory

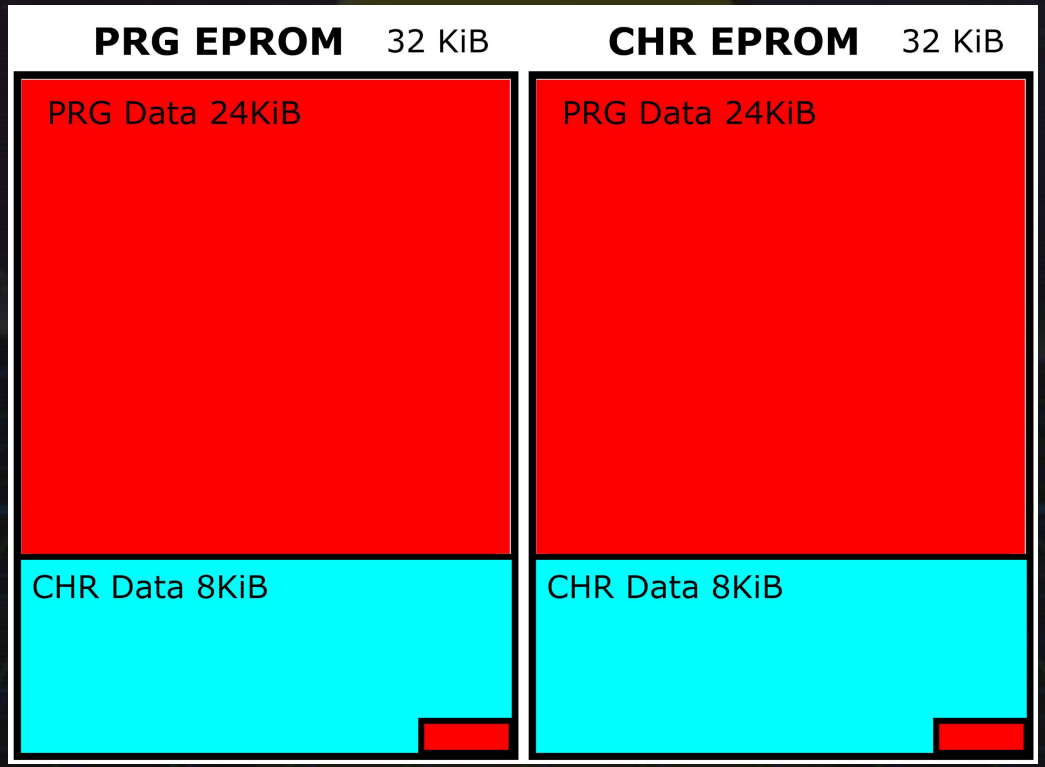
8KiB CHR ROM data can also be burned onto 27C256 EPROM (Last 8KiB read)

CHR vs PRG

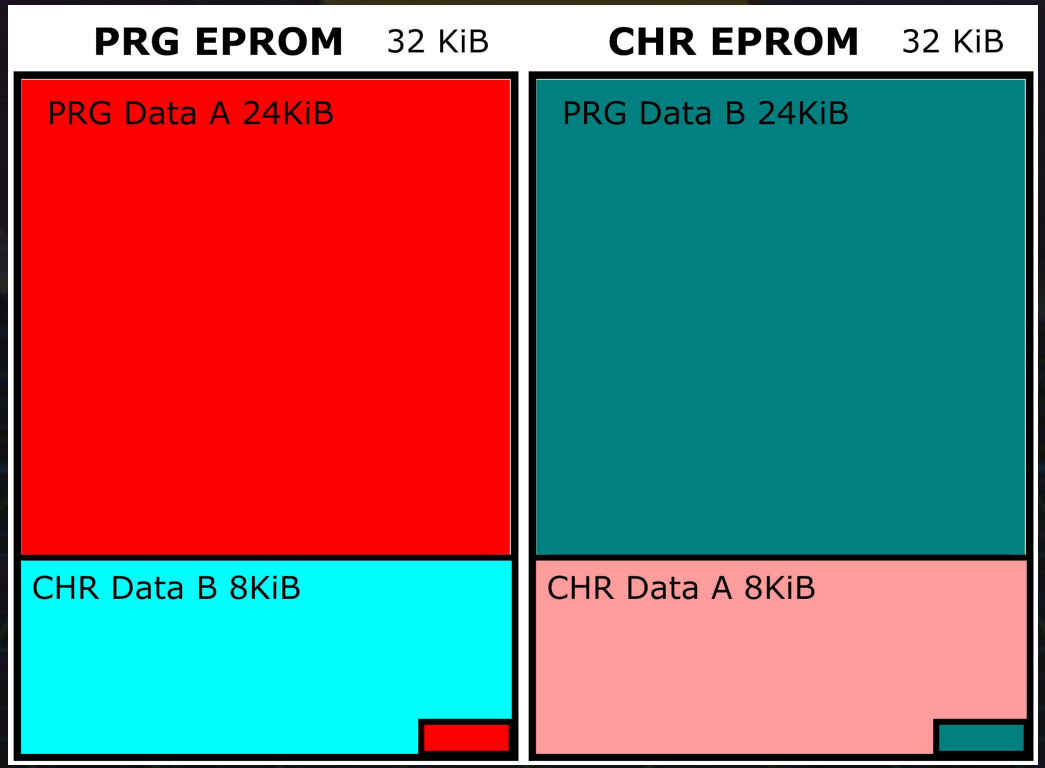
- CHR does not contain Programming data
- PRG does not contain Graphic data
- But what if they did? What if we could swap the EPROMs?



Gemini - Swapping the CHR and PRG Results in the Same Game



Gemini A/B - Swapping the CHR and PRG Results in a Different Game



The NROM-256 Board

10NES CIC Chip

Region Lockout Chip

Lock/Key System

- Console is the Lock
- Cartridge is the Key

Anti-Piracy System

Famicom and NES Top Loader (NES-101) did NOT include 10NES CIC Chip

Cartridge Swapping

- Console Region lock chip prevents cartridge swapping
- Disable the console region lock chip and you CAN cartridge swap
- While power is on, RAM state is kept for a few seconds during a cartridge swap
- This means you can utilize active RAM data from another game

MARIO
WORLD
1-1

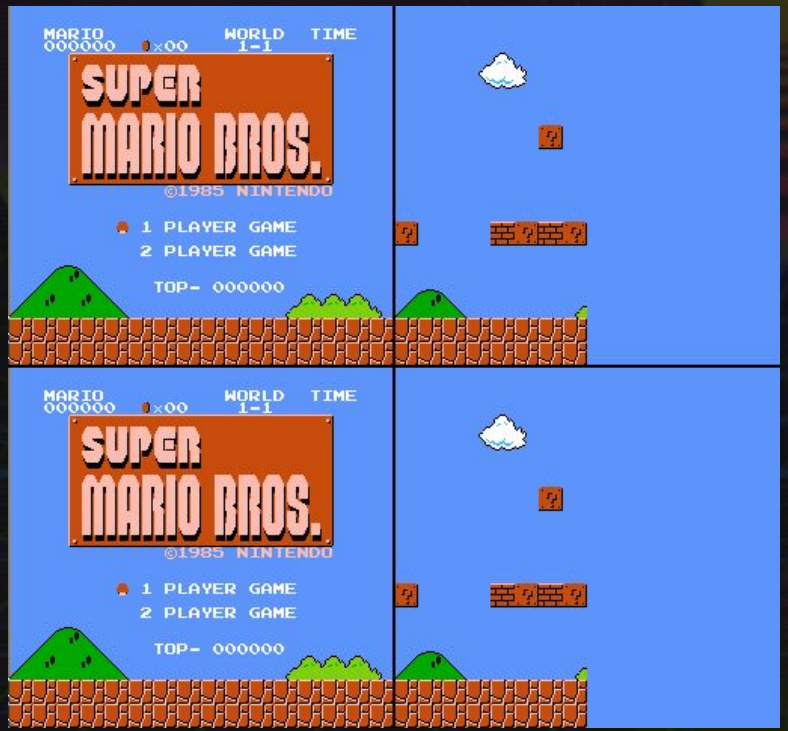
The NROM-256 Board

Drawing Graphics on the Screen

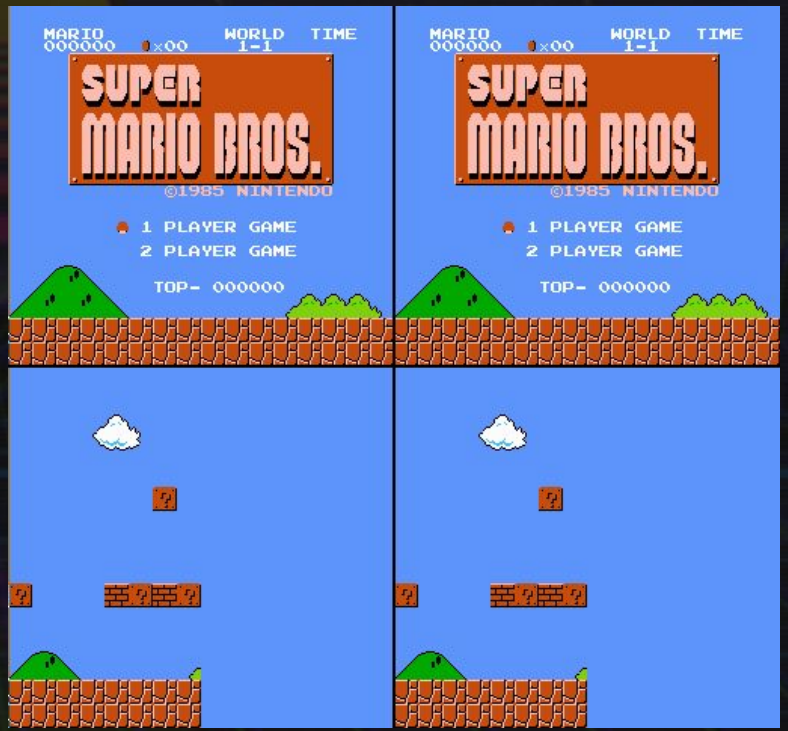
- Program data tells the NES what graphics to draw on the screen
- Screen "Camera" is 256px * 240px
- Screen "Canvas" is 2 screens by 2 screens
- Ability to be vertically or horizontally mirrored

Mirroring

Vertical



Horizontal

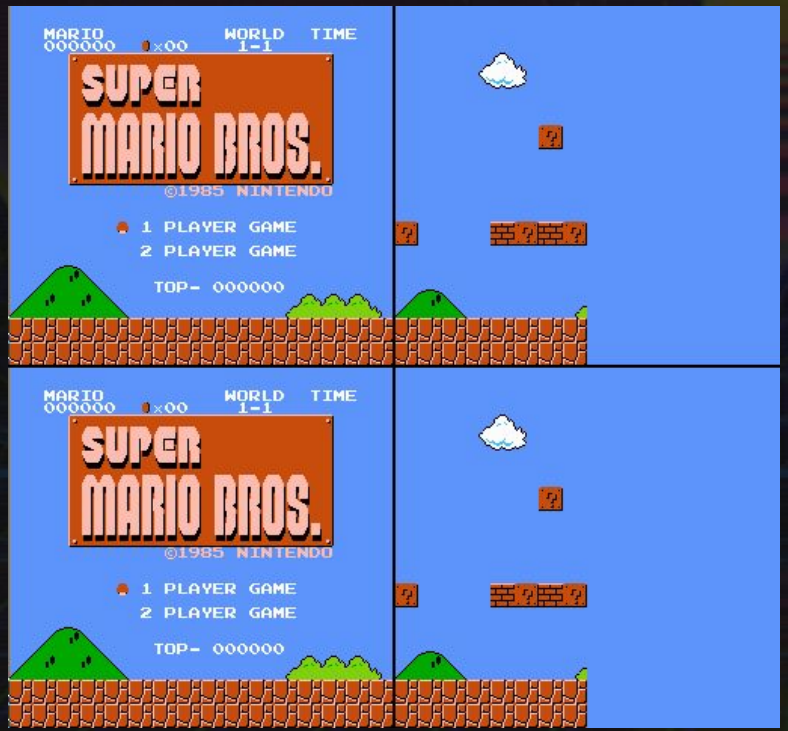


Determining Mirroring

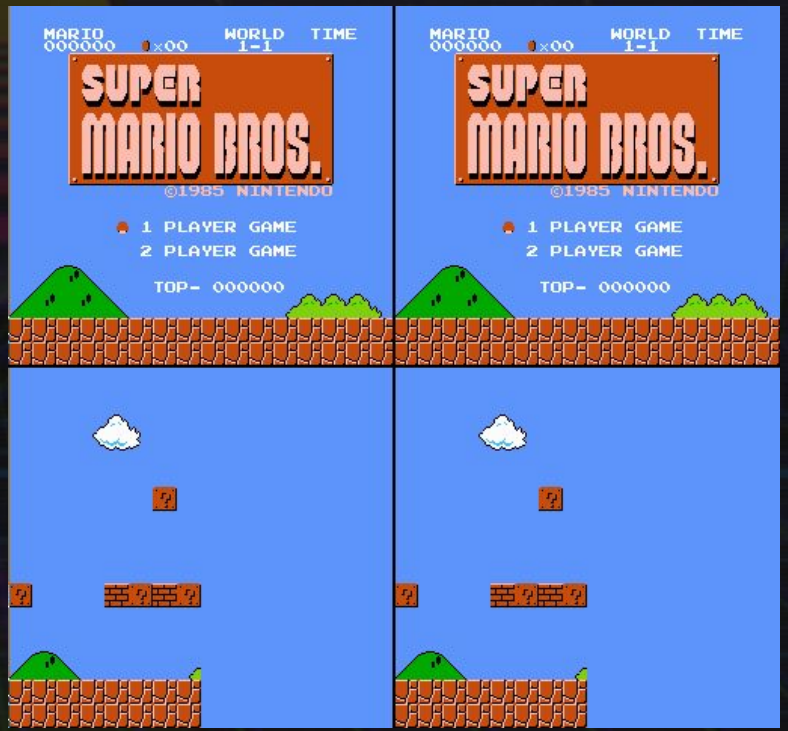
- Draw a tile on the screen
- Check if tile is the same on horizontal adjacent screen
  - If so, game is horizontally mirrored
- Check if tile is the same on vertically adjacent screen
  - If so, game is vertically mirrored

Determining Mirroring

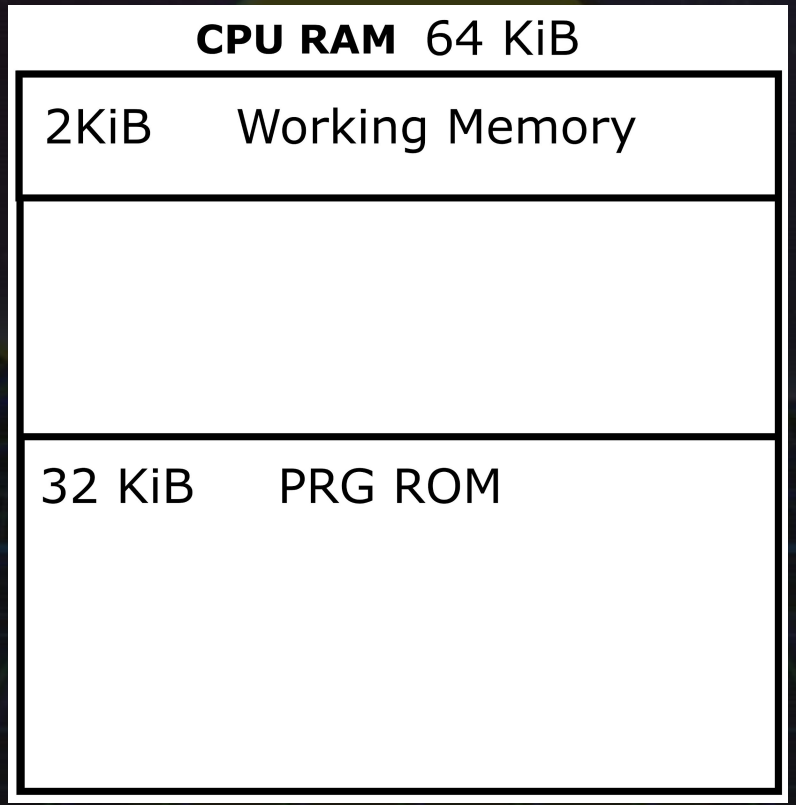
Vertical



Horizontal



NES CPU Memory



NES CPU Memory

Only 2KiB of Working Memory ($0000 - $0FFF)

256 Bytes ($0100 - $01FF) used for the stack

256 Bytes ($0200 - $02FF) used for sprite data

2 KiB CPU Working Memory

$0000 - $00FF	Free Working Memory
$0100 - $01FF	Stack (Be careful about modifying this)
$0200 - $02FF	Sprite Data (May not matter)
$0300 - $07FF	Free Working Memory

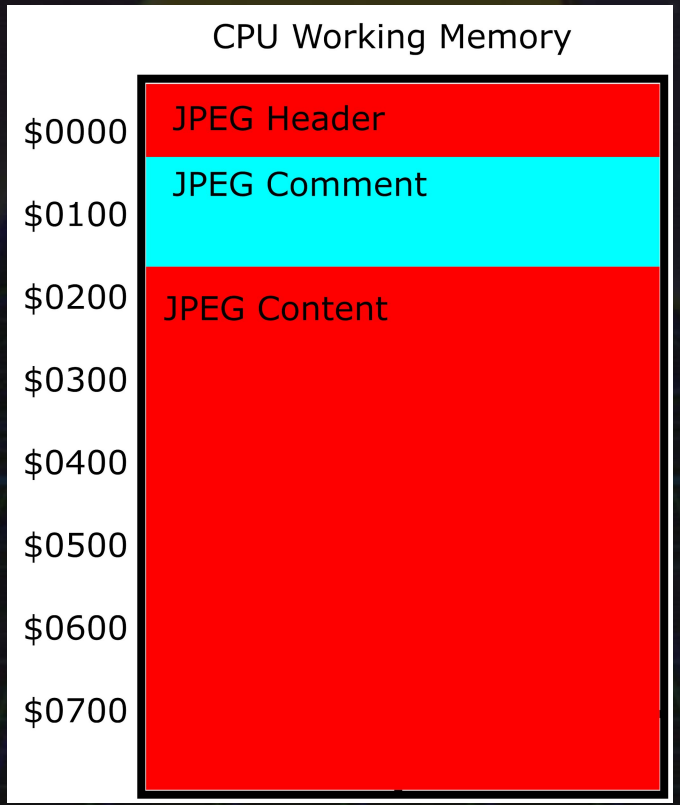
What Can We Do With 2 KiB of Working Memory?

- 2 KiB (more like 1.75KiB) doesn't really seem like a lot…
- Maybe we can fit a low quality JPEG image in there!
- But what about the memory that actually needs to be manipulated? What about the stack?

An NES Game Whose Memory Dump is a JPEG Image

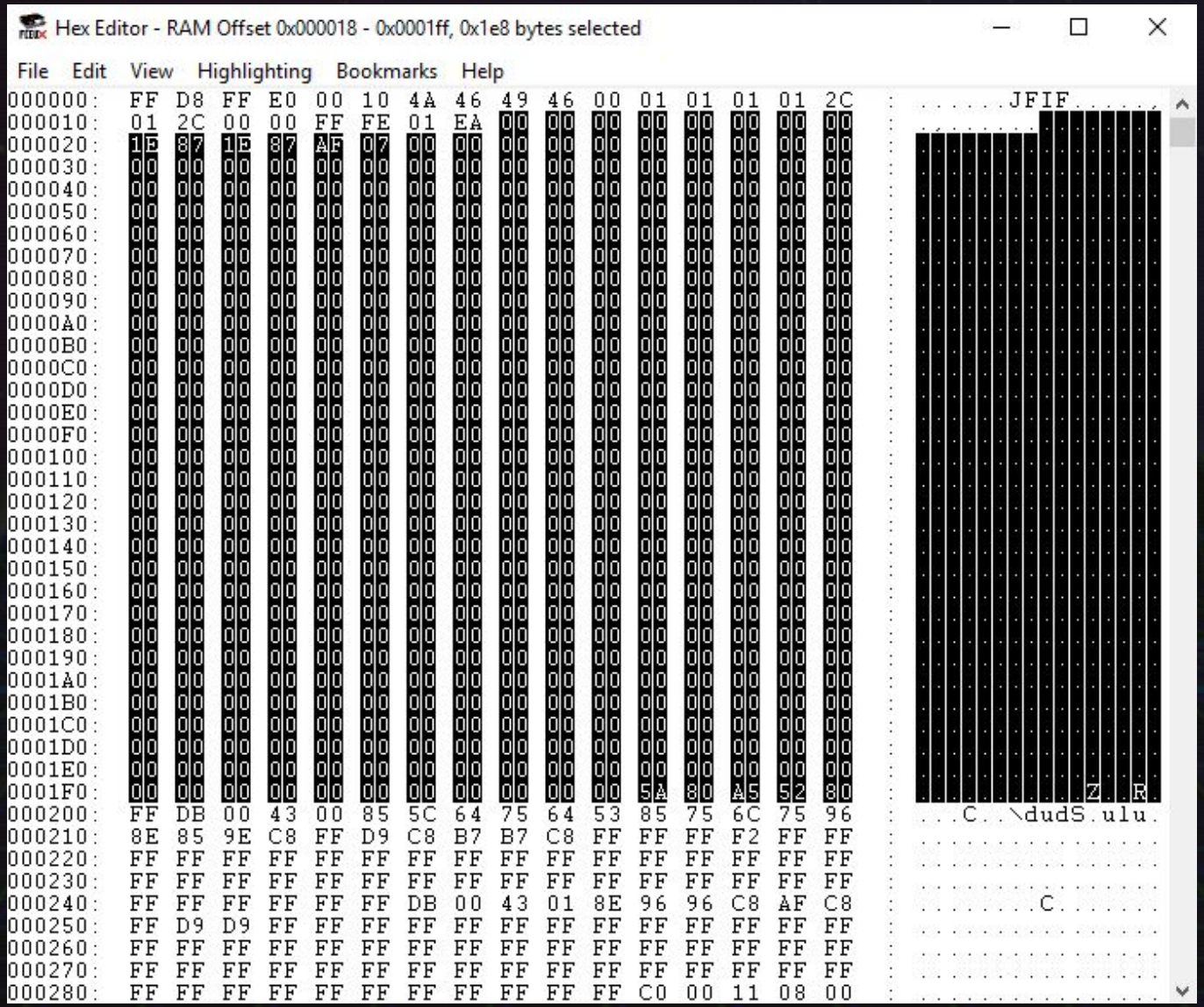
- JPEG file comments to the rescue!
  - Data in comments aren't important anyways
- Make a comment that ends at $0200 (or $0300 if you want sprites)

An NES Game Whose Memory Dump is a JPEG Image



THE MEMORY DUMP OF THIS GAME IS ALSO A JPEG IMAGE OF LENNA

VI GREY 2019


Hex Editor - RAM Offset 0x000018 - 0x0001ff, 0x1e8 bytes selected
File Edit View Highlighting Bookmarks Help
000000: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 01 2C : ......JFIF.....,
000010: 01 2C 00 00 FF FE 01 EA 00 00 00 00 00 00 00 00 : .,..............
000020: 1E 87 1E 87 AF 07 00 00 00 00 00 00 00 00 00 00 : ....
000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0000D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0000E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0000F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0001A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0001C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0001D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0001E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : ....
0001F0: 00 00 00 00 00 00 00 00 00 00 00 00 5A 80 A5 52 80 : ............Z..R.
000200: FF DB 00 43 00 85 5C 64 75 64 53 85 75 6C 75 96 : ...C..\dudS.ulu.
000210: 8E 85 9E C8 FF D9 C8 B7 B7 C8 FF FF FF F2 FF FF : ....
000220: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF : ....
000230: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF : ....
000240: FF FF FF FF FF FF DB 00 43 01 8E 96 96 C8 AF C8 : ....C.......
000250: FF D9 D9 FF FF FF FF FF FF FF FF FF FF FF FF FF : ....
000260: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF : ....
000270: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF : ....
000280: FF FF FF FF FF FF FF FF FF FF FF FF C0 00 11 08 00 : ....

Full Circle

- I failed to reproduce the PDF/NES polyglot file Proof of Concept
- I thought I failed because I didn't know enough about how NES ROMs work
- Funny story… turns out I didn't know enough about how PDF files worked… Oops
- Hey, this presentation is a PDF file!

Change the file extension from .pdf to .nes

Source Code and Files

https://github.com/ViGrey/CypherCon4

https://vigrey.com/CypherCon4

Special Thanks / Inspirations

CypherCon

Tymkrs & The Rabbit Hole

Johnny Xmas

Jaku & Warp World

Ange Albertini

Evan Sultanik & Evan Teran

NESDev Forums & Wiki

The Machine Shed LLC