There's a ZIP File in My NES Cartridge

16 Feb 2018 - DEFCON 201 Technical Meeting - Hoboken, NJ

Presented By

Vi Grey
Technology Researcher
Software Engineer

vigrey.com

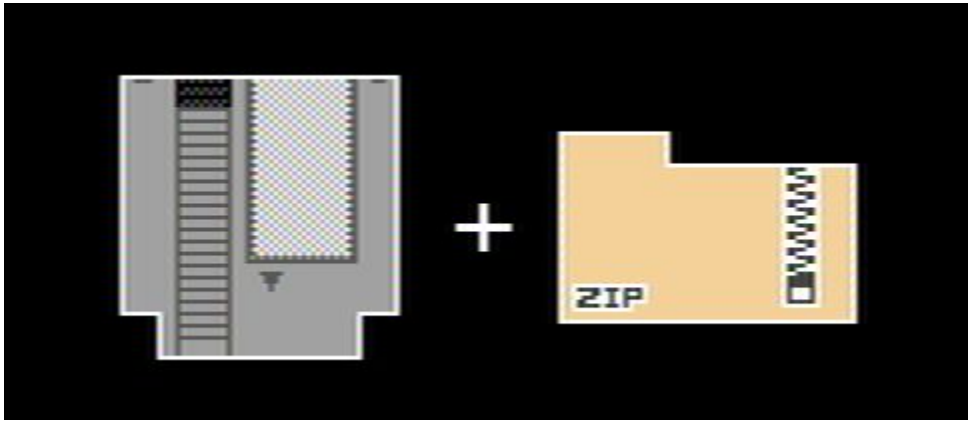
Who Am I?

- Technology Researcher
- Software Engineer
- Web Developer

[Frequently Spotted Solving Rubik's Cubes]

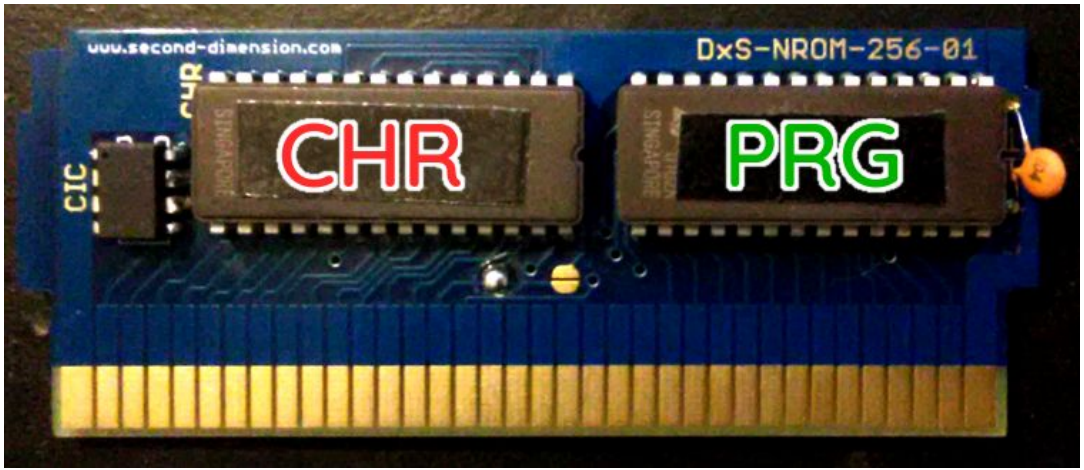
We're Creating a Polyglot File

- A file that is 2 or more different files at the same time
- In this case, NES ROM + ZIP



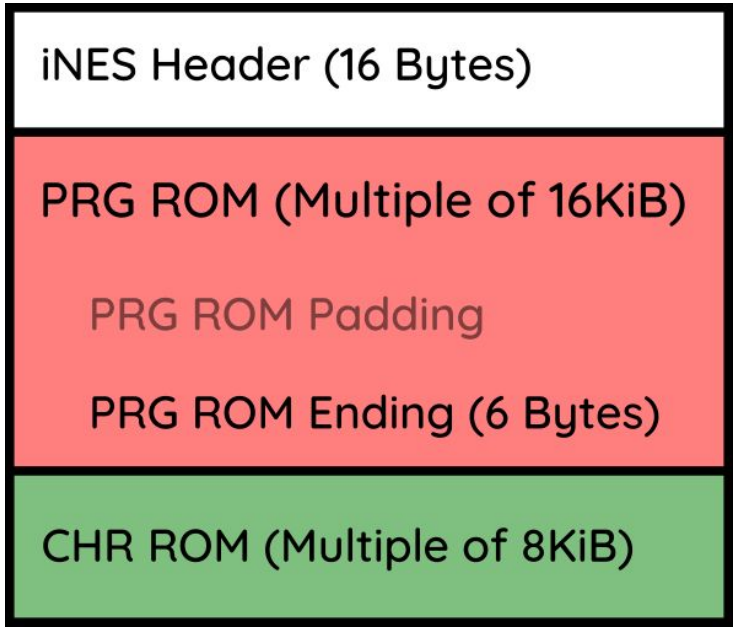
A Look Inside an NES Cartridge

- CHR ROM stores graphic tile data
- PRG ROM stores program data



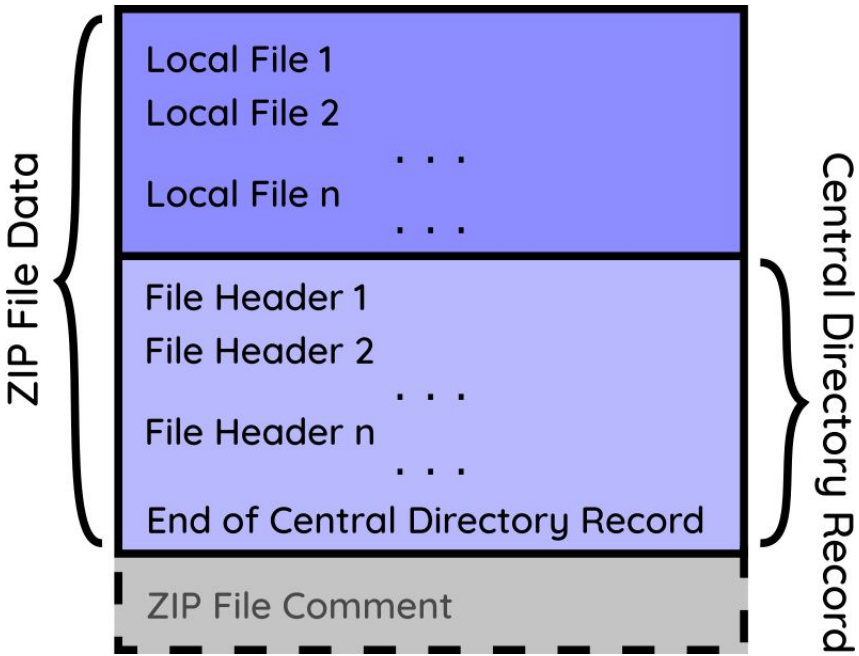
NES ROM File Format *(NROM)*

- Beginning of file is 16 Byte iNES Header
- PRG ROM Data
  - Padding is unused space
  - Last 6 Bytes are important
- CHR ROM Data



ZIP File Format

- No header at beginning of ZIP File
- ZIP File Data
  - Local Files
  - Central Directory Record
- Optional ZIP File Comment

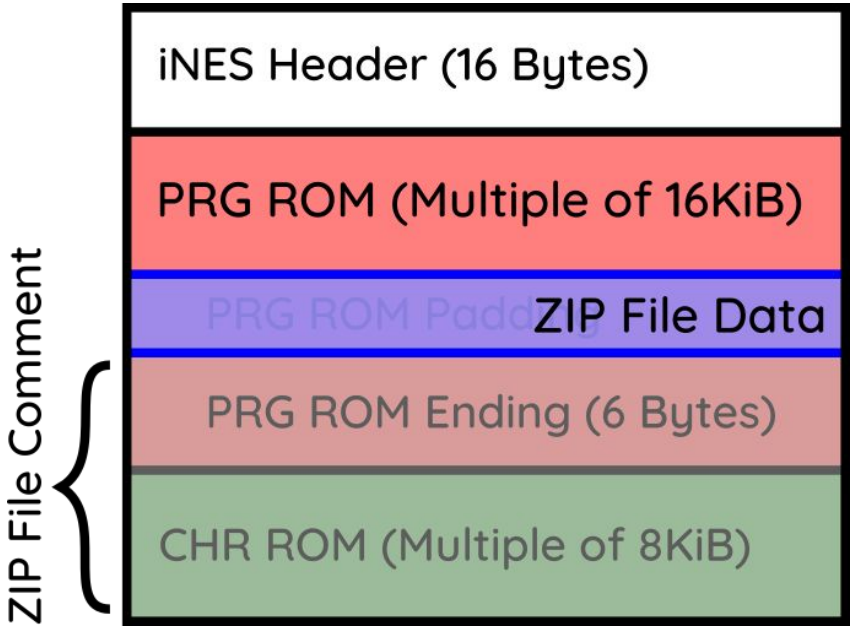


How ZIP File Works

- End of Central Directory Record (EOCDR)
  - File scanned from the end to find EOCDR Signature
  - Specifies Central Directory Record start offset
  - Sets length of ZIP File Comment
- Central Directory Record - File Headers
  - File Headers start with a Signature
  - Specifies start offsets of Local Files

NES ROM + ZIP Polyglot File

- Replace some PRG ROM Padding with the ZIP File Data
- Set everything after ZIP File Data as a ZIP File Comment
- Update ZIP File Data Offsets



Working NES ROM + ZIP Polyglot File

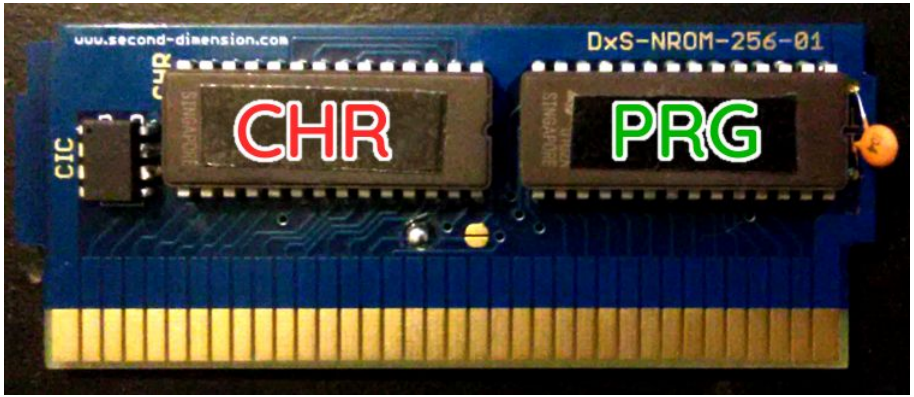
- NES ROM File is to standard
  - First 16 Bytes of file are iNES header
  - Required PRG ROM Data stays intact
  - CHR ROM Data stays intact
- ZIP File is to standard

How to Unzip File

- Rename the ROM **dc201-neszip.nes** to **dc201-neszip.zip**
- Extract with whatever ZIP File extractor you want

Burn Data onto NES Cartridge

- CHR ROM data is unchanged
- PRG ROM data is the same size as before
- ZIP File is embedded in unused PRG ROM data



Special DEFCON 201
NES ROM + ZIP Polyglot File!

GitHub.com/Defcon201/dc201-neszip

Thank You

Website: vigrey.com
Email: vi@vigrey.com

Twitter: @ViGreyTech
GitHub: ViGrey

Project Code: GitHub.com/Defcon201/dc201-neszip

Slides: vigrey.com/presentations/2018-02-16-defcon-201.pdf

Other Presentations: vigrey.com/presentations