BADGE TALK

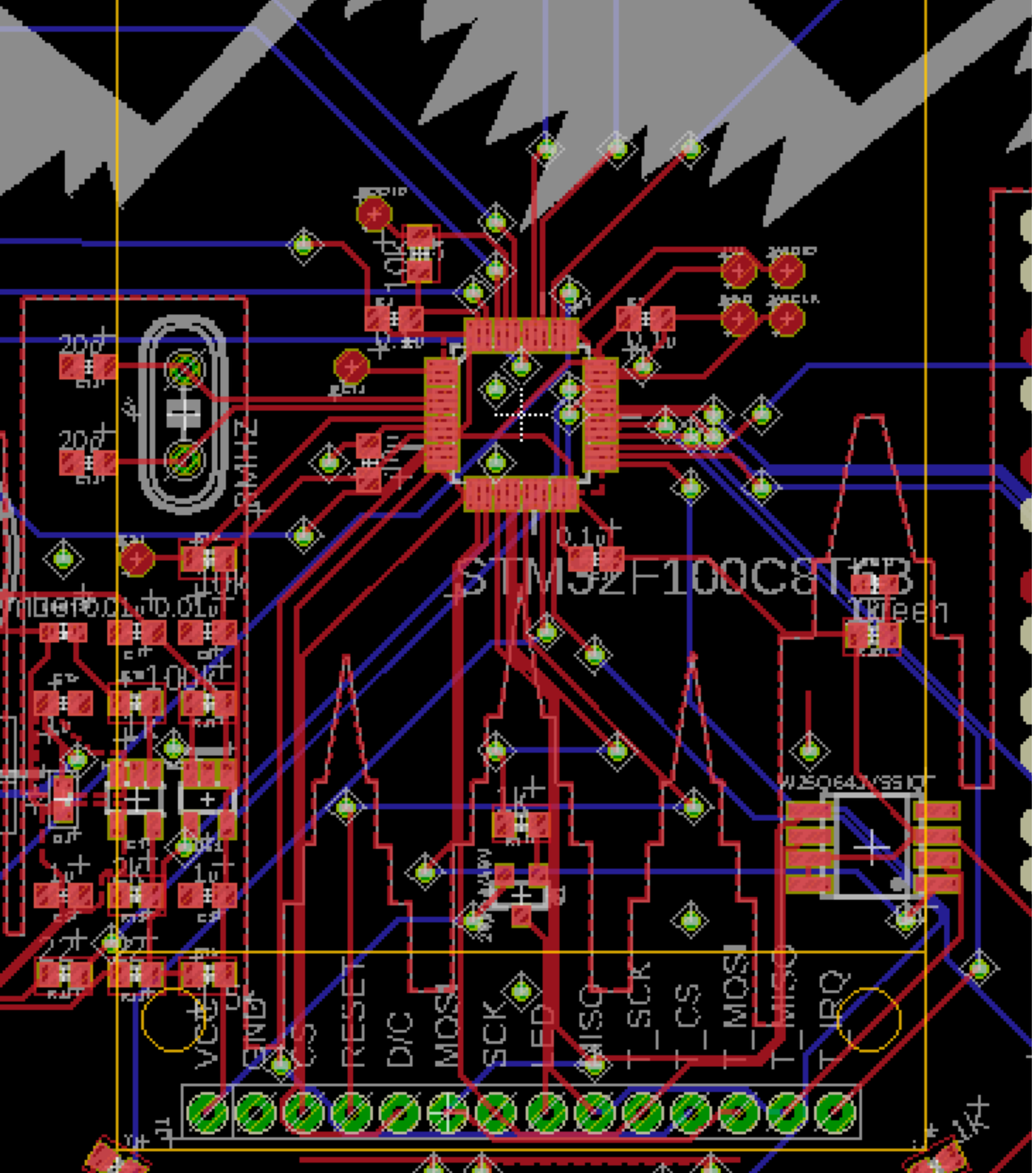
@professor__plum

BADGE TALK

@professor__plum

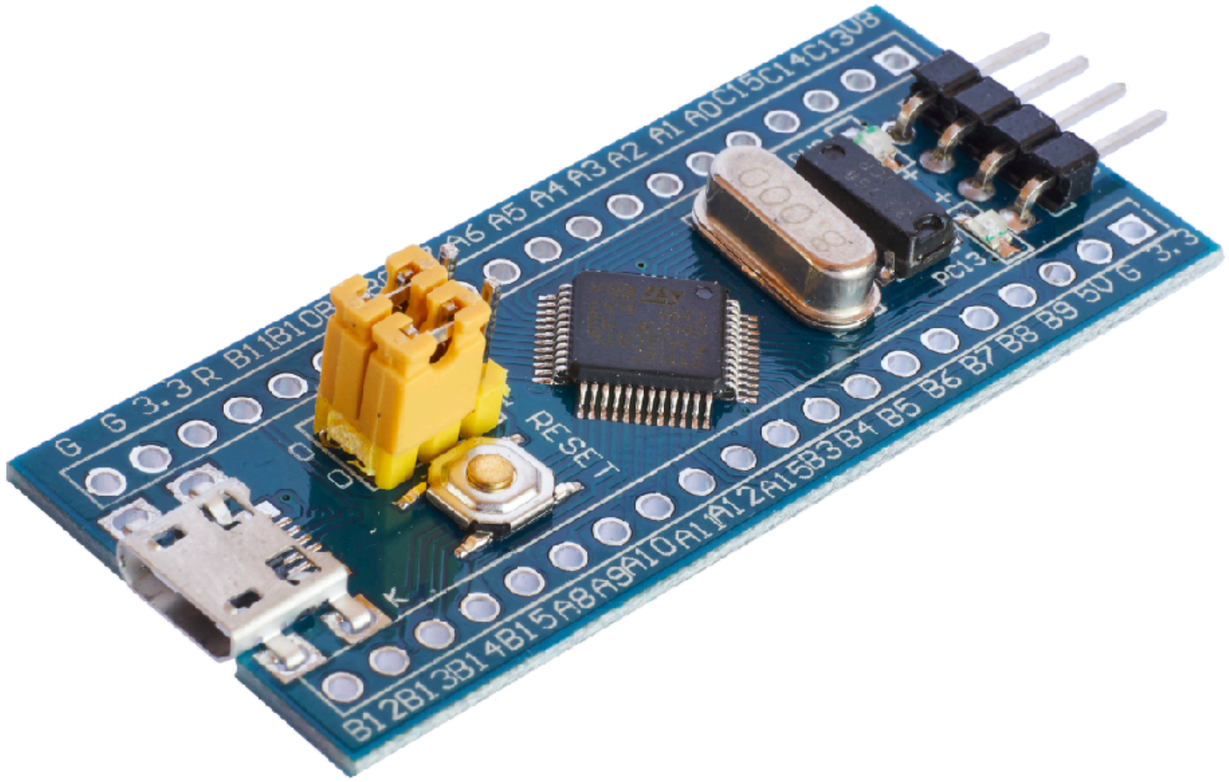
BADGE BASICS

- 12 challenges (crypto, RE, soldering, trivia, ciphers, password cracking, …)
- Dev boards given to everyone (first 100) who complete all challenges
- Teamwork is encouraged (no prize for first place)



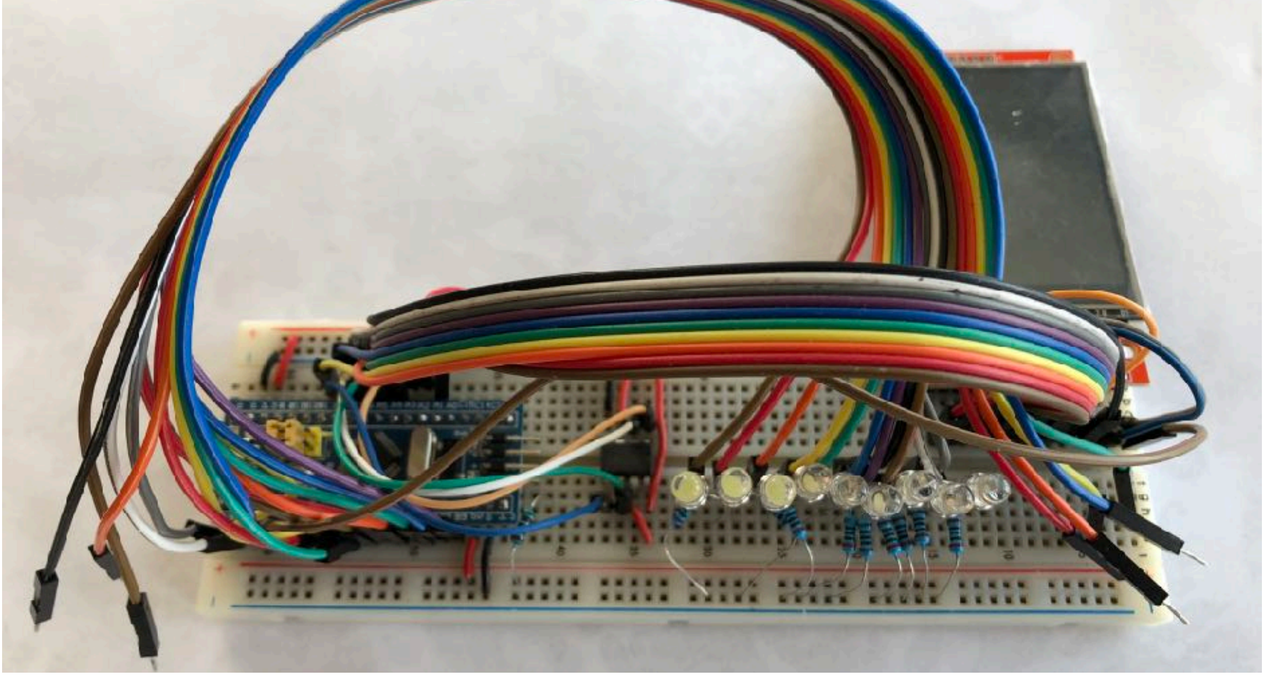
HARDWARE

- ARM 32bit processor
- 320x240 pixel 16bit LCD
- Resistive touch screen
- Piezo buzzer
- 64Mb SPI Flash Storage
- Light sensor
- Designed in Eagle



BLUE PILL

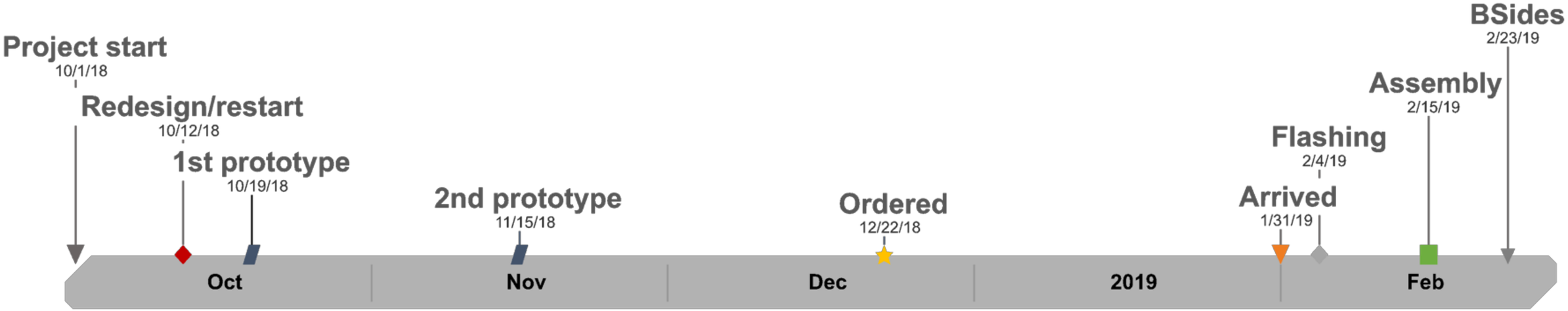
- Arduino compatible
- 72Mhz ARM cortex-M3
- Programmable via USB
- 7 channel DMA
- 7 Timers
- JTAG debugging
- I2C/USART/SPI/CAN/USB
- Cheap! Less than $2
- http://wiki.stm32duino.com/index.php?title=Blue_Pill

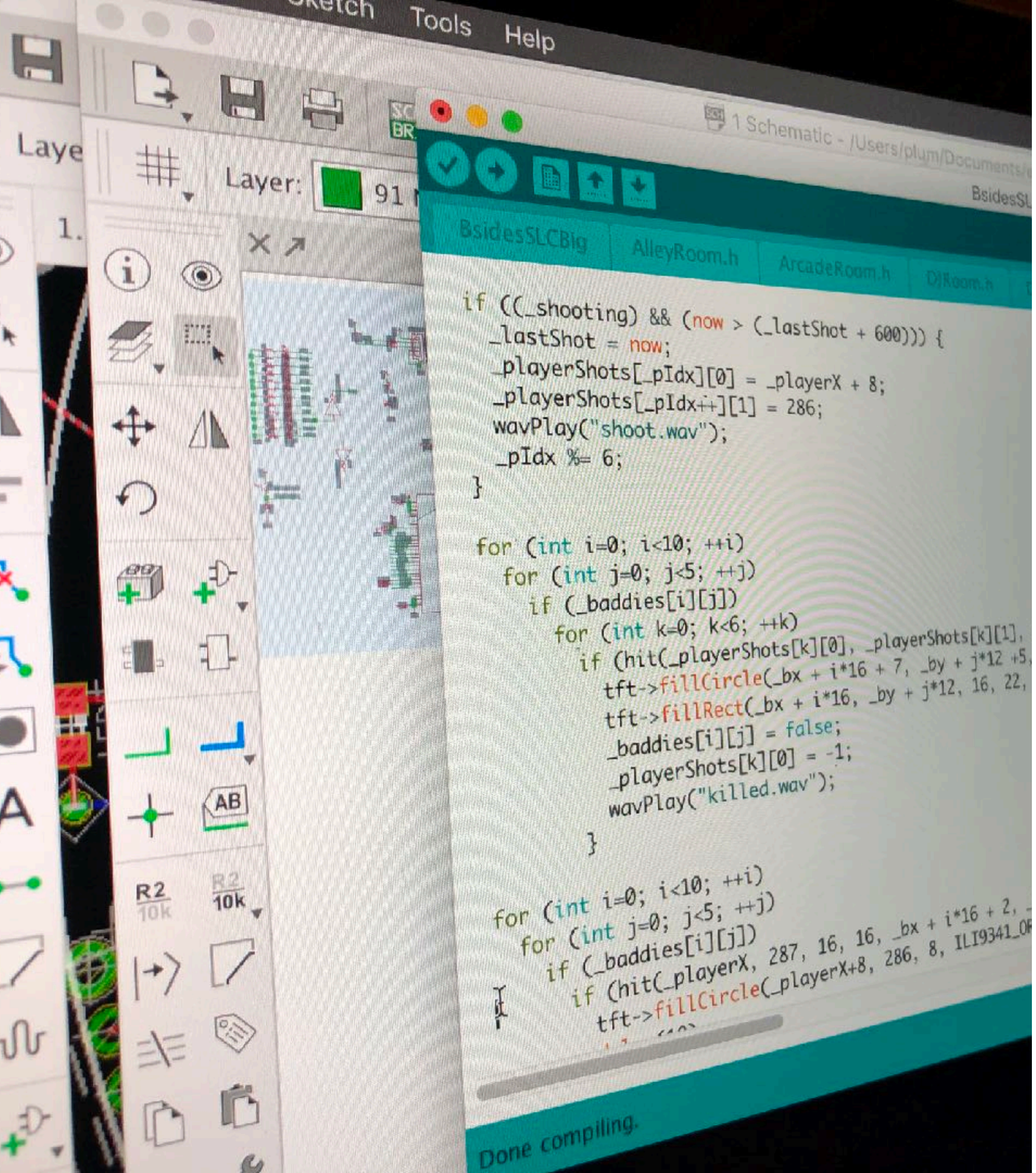


BSides SLC
Logo Here
HACK THE PLANET

BSIDES

TIMELINE


Project start
10/1/18
Redesign/restart
10/12/18
1st prototype
10/19/18
2nd prototype
11/15/18
Ordered
12/22/18
Arrived
1/31/19
Flashing
2/4/19
Assembly
2/15/19
BSides
2/23/19
Oct
Nov
Dec
2019
Feb

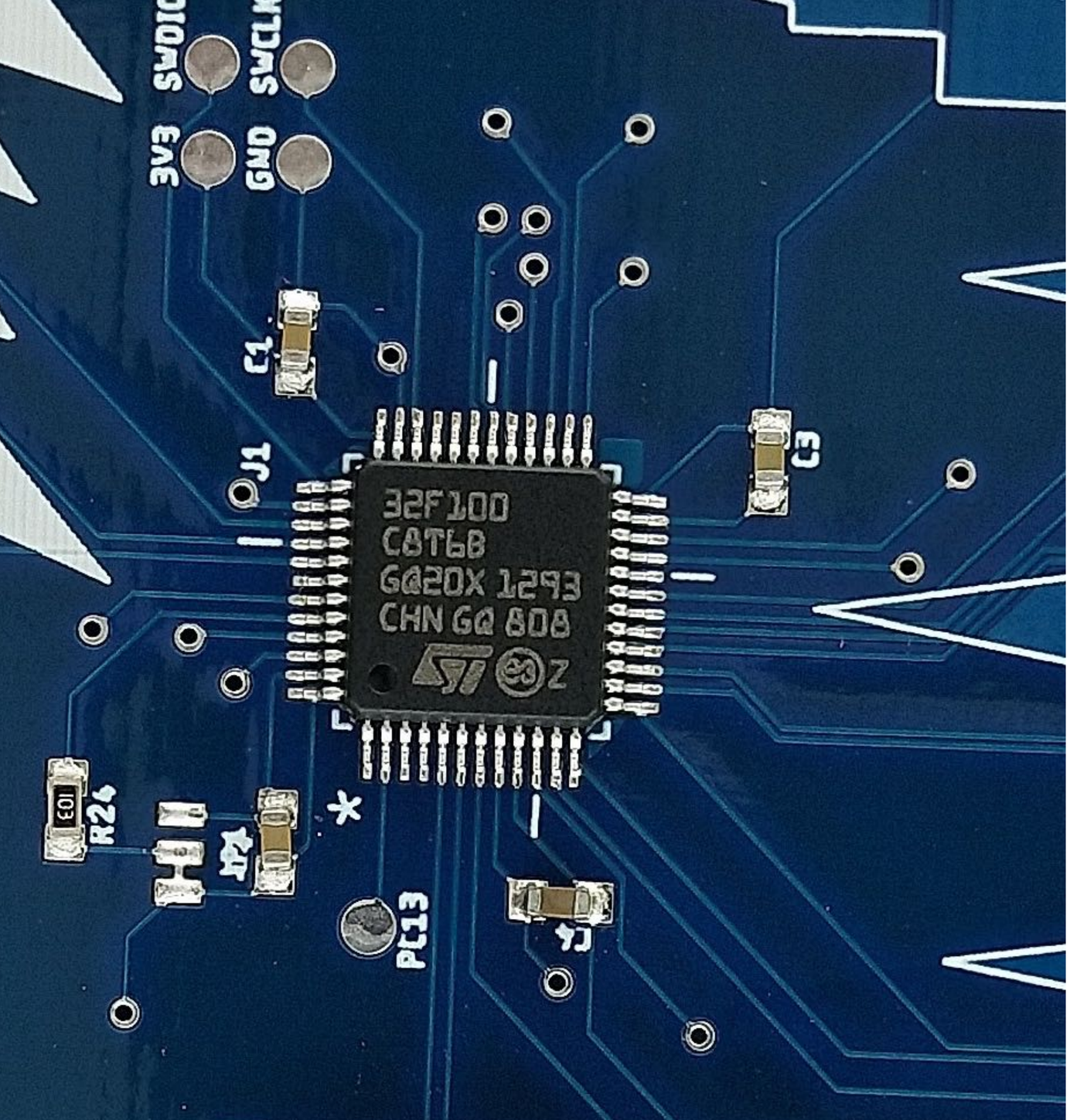


SOFTWARE

- Written using Arduino IDE (C++)
- ~3000 lines of code
- Flash, LCD, ~~LEDs~~ and audio all communicate over DMA
- The MCU shutdowns external components when idle to save power
  - From 110ma to 11ma
- Programmed via clamp & serial
- No EEPROM so part of flash is being used to store status

ARTWORK

- Bids for artwork out of budget
  - left to my own devises
- Never done pixel art before
  - (or any art really)
- 16 animated scenes
  - Totals ~1.7 Million pixels
- Took an online pixel art course
  - https://www.udemy.com/pixel-art-master-course/
  - I now know enough to know I'm doing it wrong
- Arguably the hardest part (for me)



BIG TROUBLE IN LITTLE CHINA

- 500 boards arrived, 100% non-functional
  - USB interface dead
  - Couldn’t flash or program chip
- I approved the wrong component
  - Not just any component, the MCU
  - STM32F100C8 not STM32F103C8
- $10000 worth of coffee coasters?

YEAR OF THE PIG

Chinese New Year 2019!

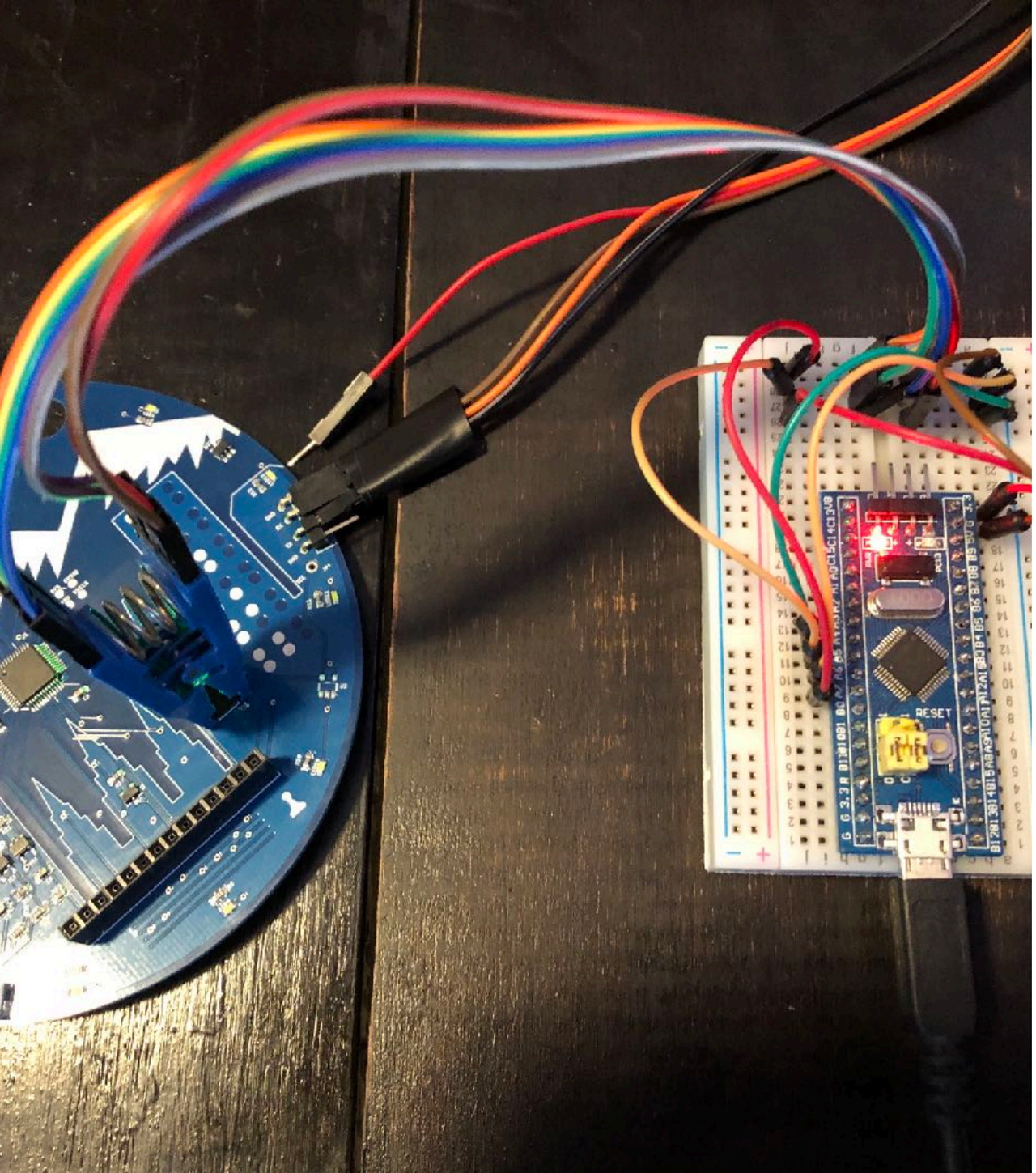
NOTICE:

With the coming of the Chinese New Year we will be close from Jan. 30th to Feb. 11th. Kindly take note there will be a production delay during these days.

SIDE BY SIDE

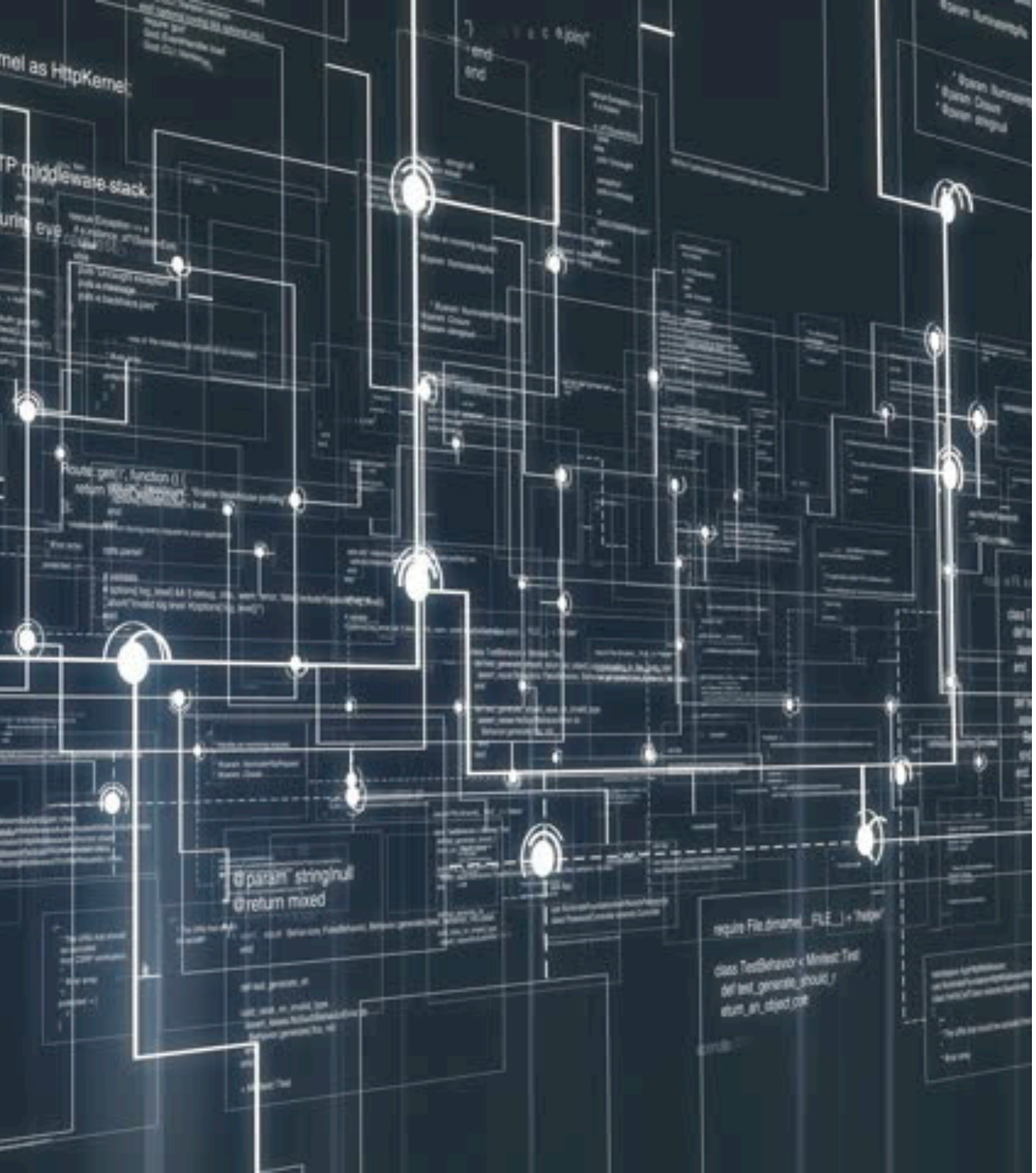
STM32F103C8	STM32F108C8
ARM Cortex-M3	ARM Cortex-M
72 Mhz	24 Mhz
20k RAM	8k RAM
64k Flash	64k Flash
SPI, I2C, USART	SPI, I2C, USART
USB, CAN, SDIO	Nope
48Mhz max SPI	12Mhz max SPI

Now with 66% less processing power!



IT'S ALIVE!

- Chip not ported to Arduino (yet)
- Day 1: lights blink, I may survive
- Remove all USB references
- Not enough RAM for current code
- ~70% of the code was salvageable but parts run really really slow
- What about programming the SPI Flash?
  - 1st attempt to flash via serial port took 3 hours…



OPTIMIZE! OPTIMIZE! OPTIMIZE!

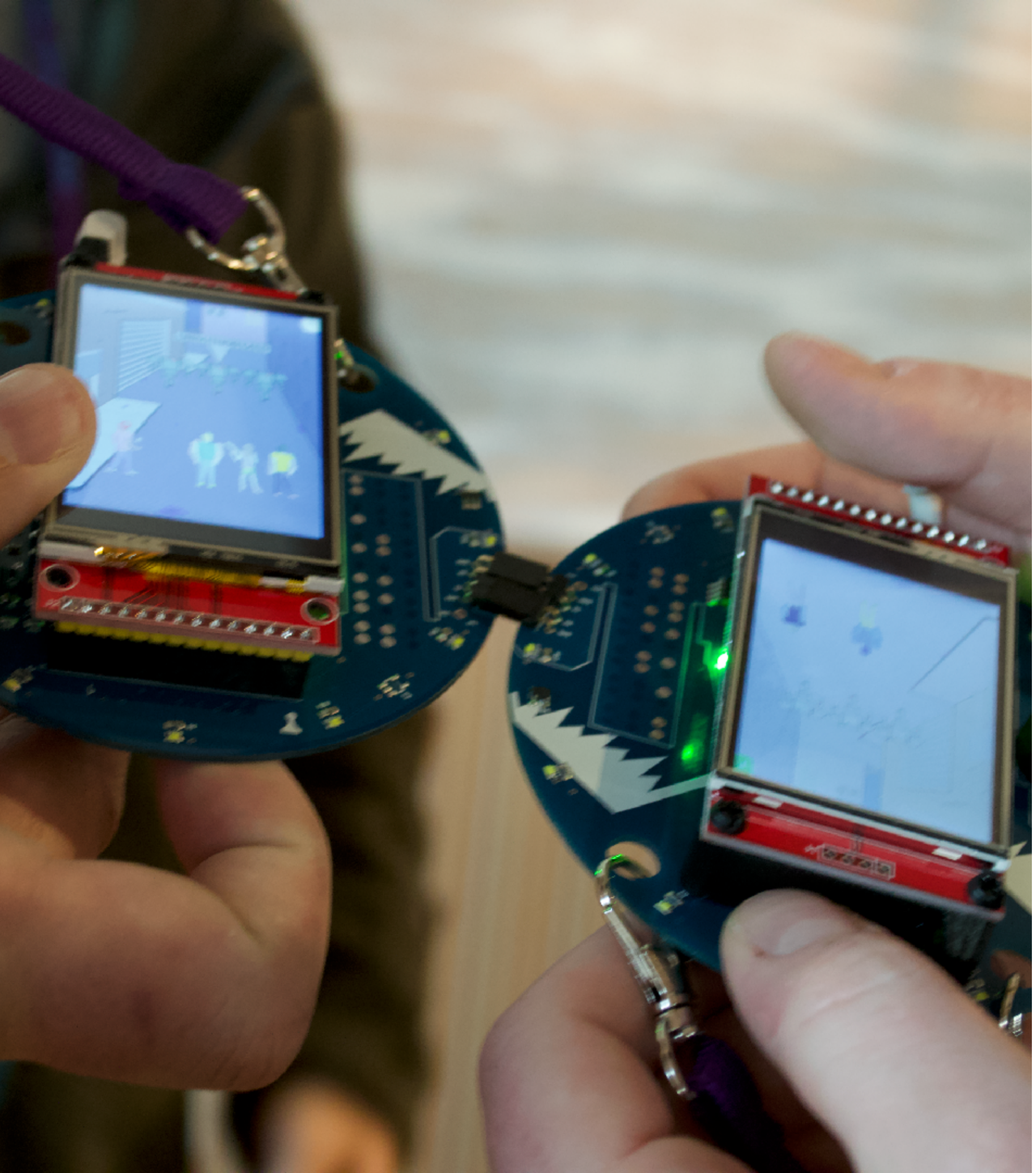
- Optimize variable storage
  - Does the speaker really need a 4k buffer?
  - Only keep one room in memory at a time
  - Int vs char
- DMA all the things!
- Only redraw what’s absolutely necessary
- Look for early outs
- Loop hoisting

THE LITTLE MCU THAT COULD

- 33 of 36 GPIO pins used (92%)
- 6k+2k of 8k RAM used (99%)
- 78k of 64k Flash used (119%)

THANKS

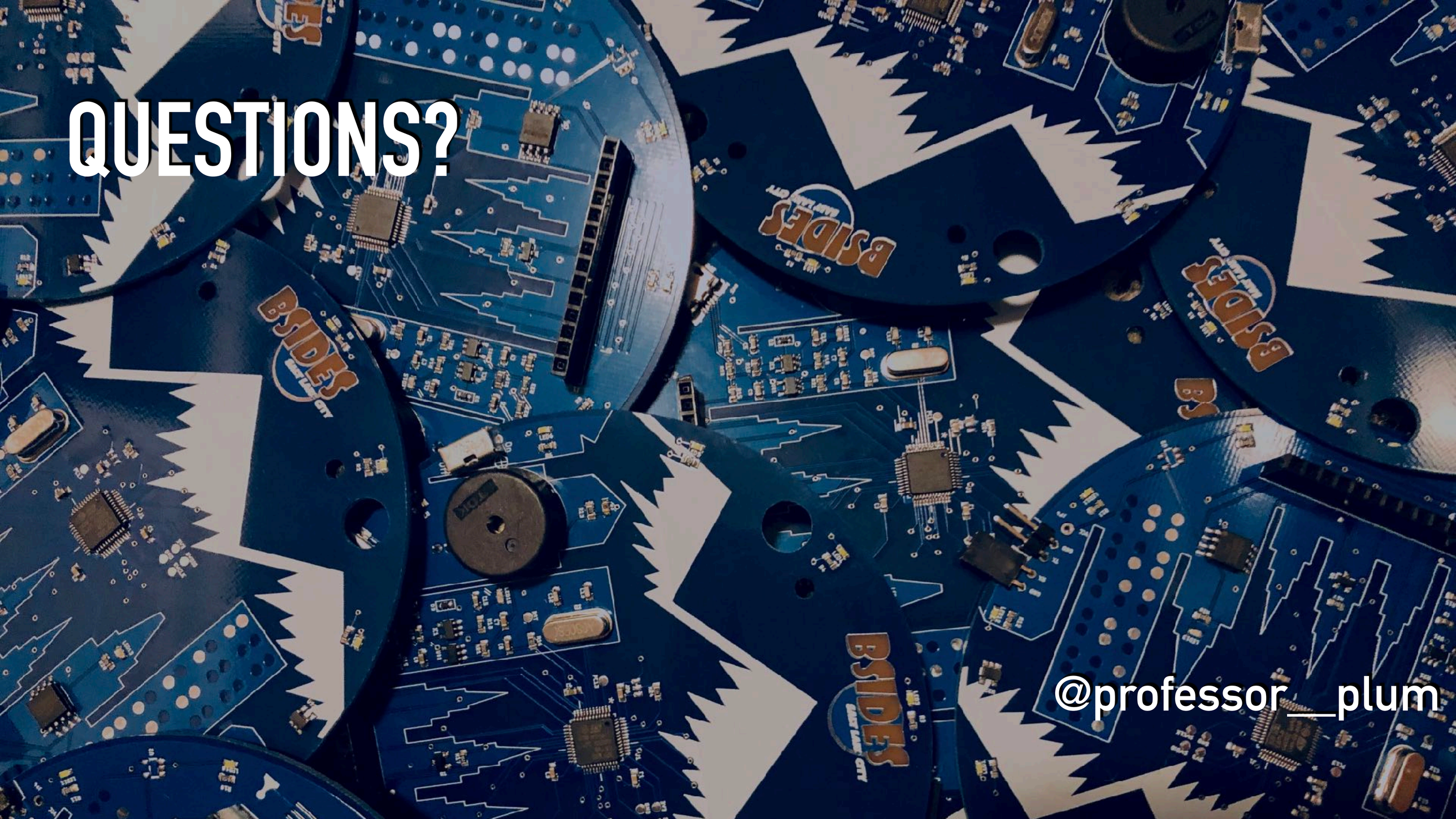
- @Sirged for designing and printing the stylus holder
- Adobe for kitting the badges
- @Compukidmike for being my sounding board
- Bryce for being patent when I shot myself in the foot



ADMINISTRATIVE

- You can completely reset the device by holding down on splash for 6 seconds
  - You will loose all pairing
- The QR message was missing the following info
  - "NTSC-M with echo canceling, medium gain, and HIGH bitrate”
- The schematics, source code and artwork will be at https://github.com/Professor-plum/BSides-SLC-Badge-2019
  - Spoilers in source (duh)

QUESTIONS?

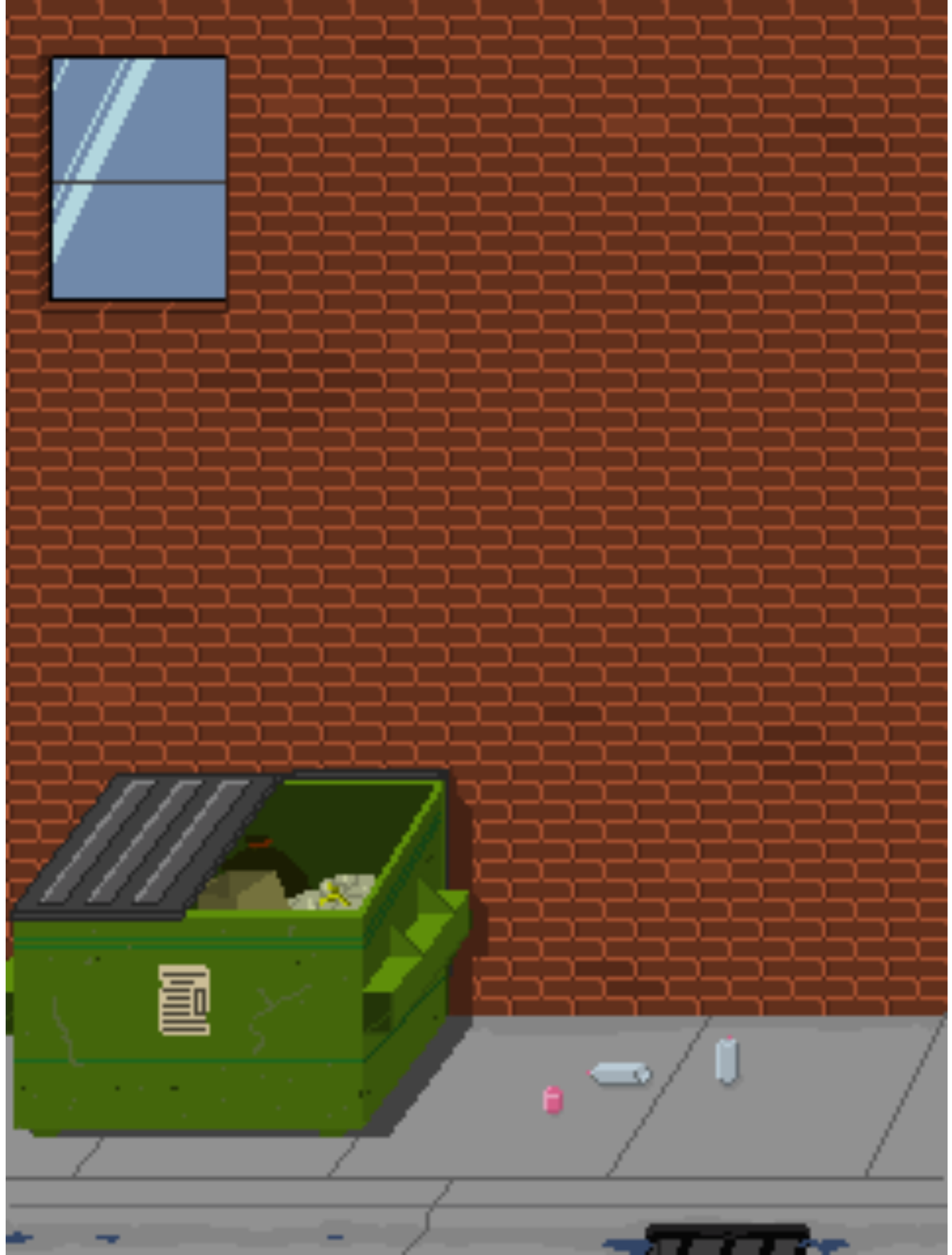


@professor__plum

WARNING
SPOILER
ALERT

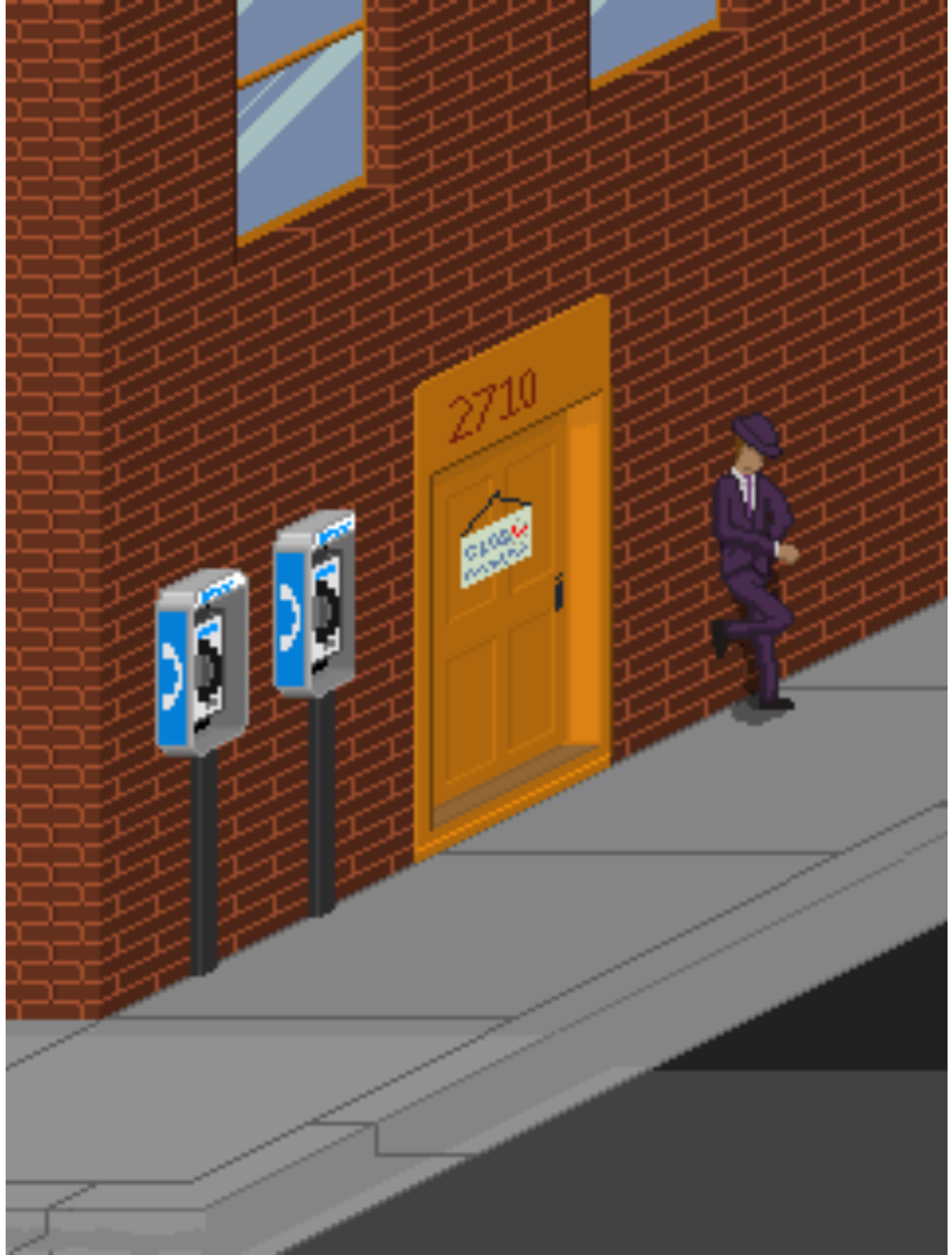
TV SCENE

- The antenna can be moved
- The clock is a hint
- “U2 missing” is a hint regarding the soldering challenge
- There’s a hint behind the poster regard badge pairing



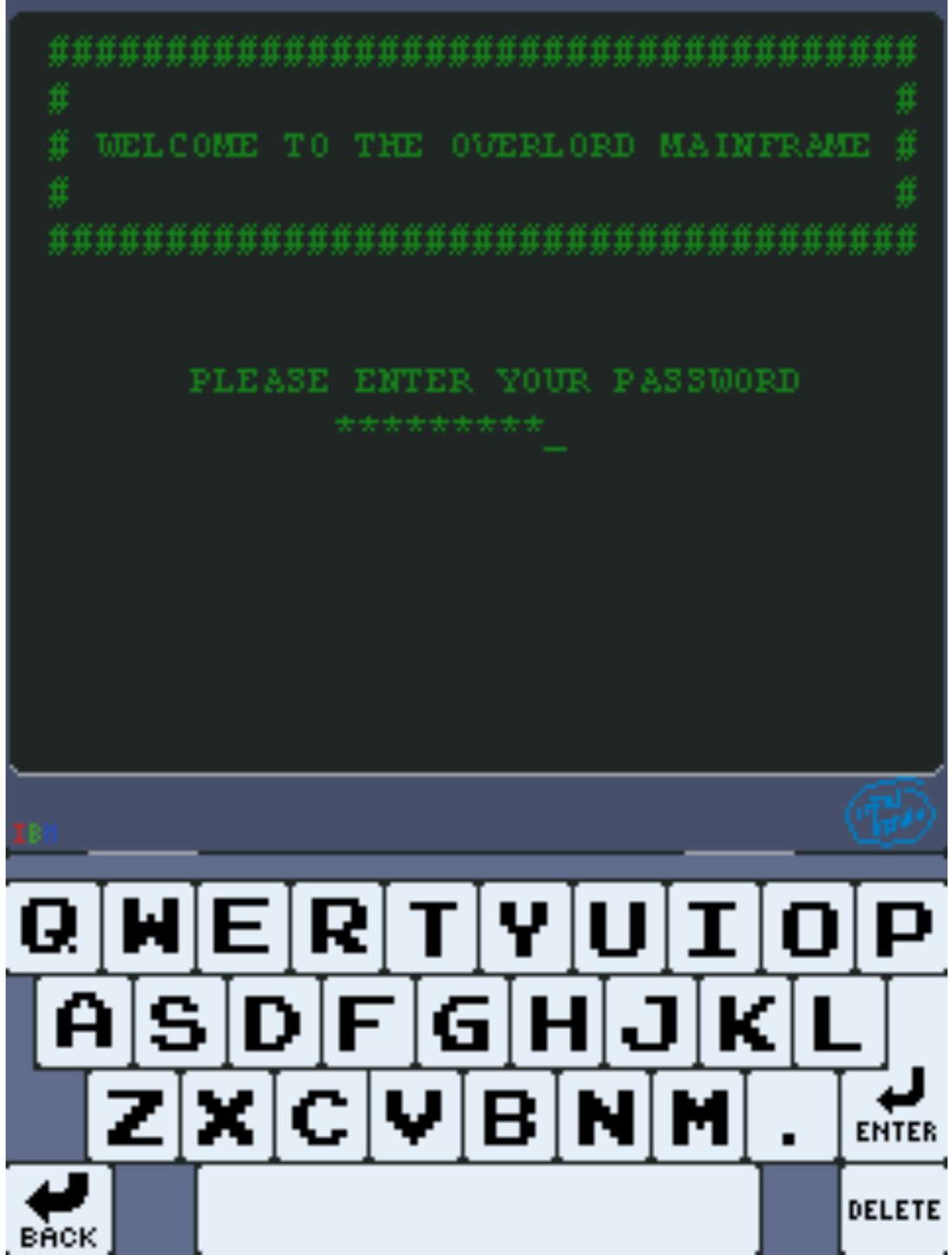
ALLEY SCENE

- More of a play area
- Contains a randomly shown hint about the RE challenge
- Dumpster dive



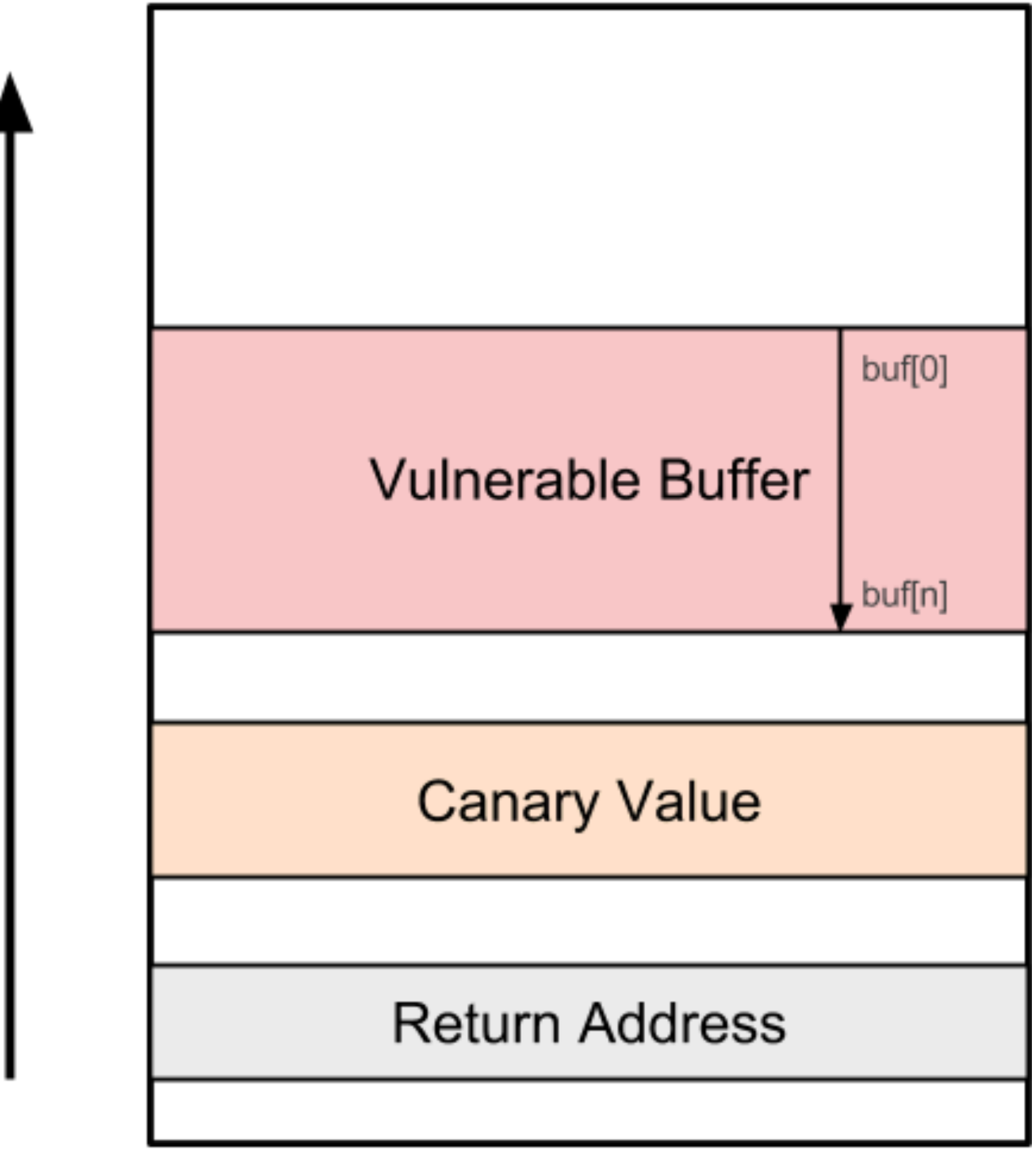
APARTMENT FRONT SCENE

- Phone booths
- The figure gives you a hint regard what number to call
- It is a 10 digit “text” number
  - Thus, the answer is a 10 letter word



MAINFRAME SCENE

- Requires a password to access
- Need to find a “hash in the trash”



MAINFRAME (PART2)

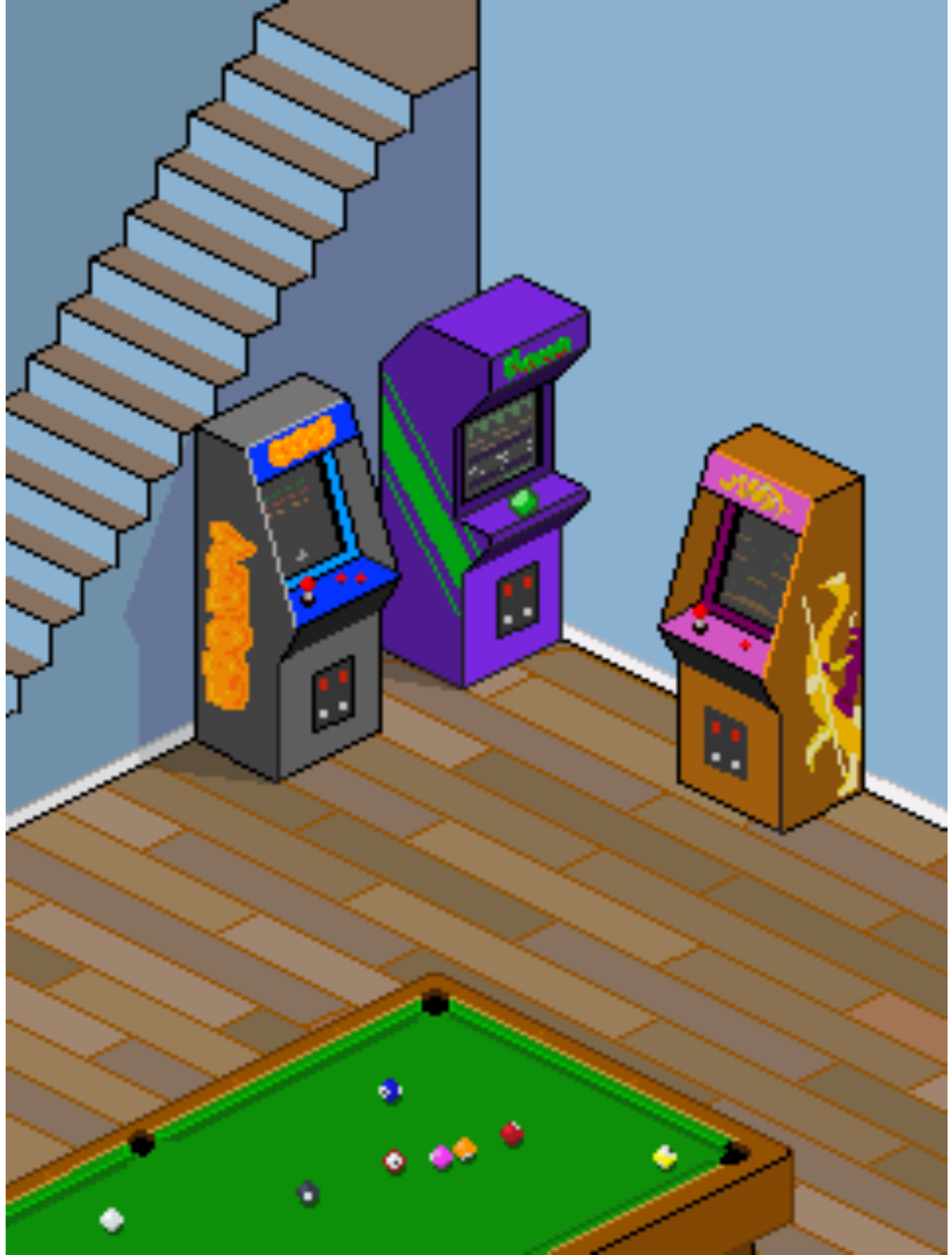
- Exploiting requires understanding stack canaries
- After completing the puzzles the core dump contains a hint regard badge pairing secrets

NIGHTCLUB SCENE

- Hardware puzzle
- Hint in the window

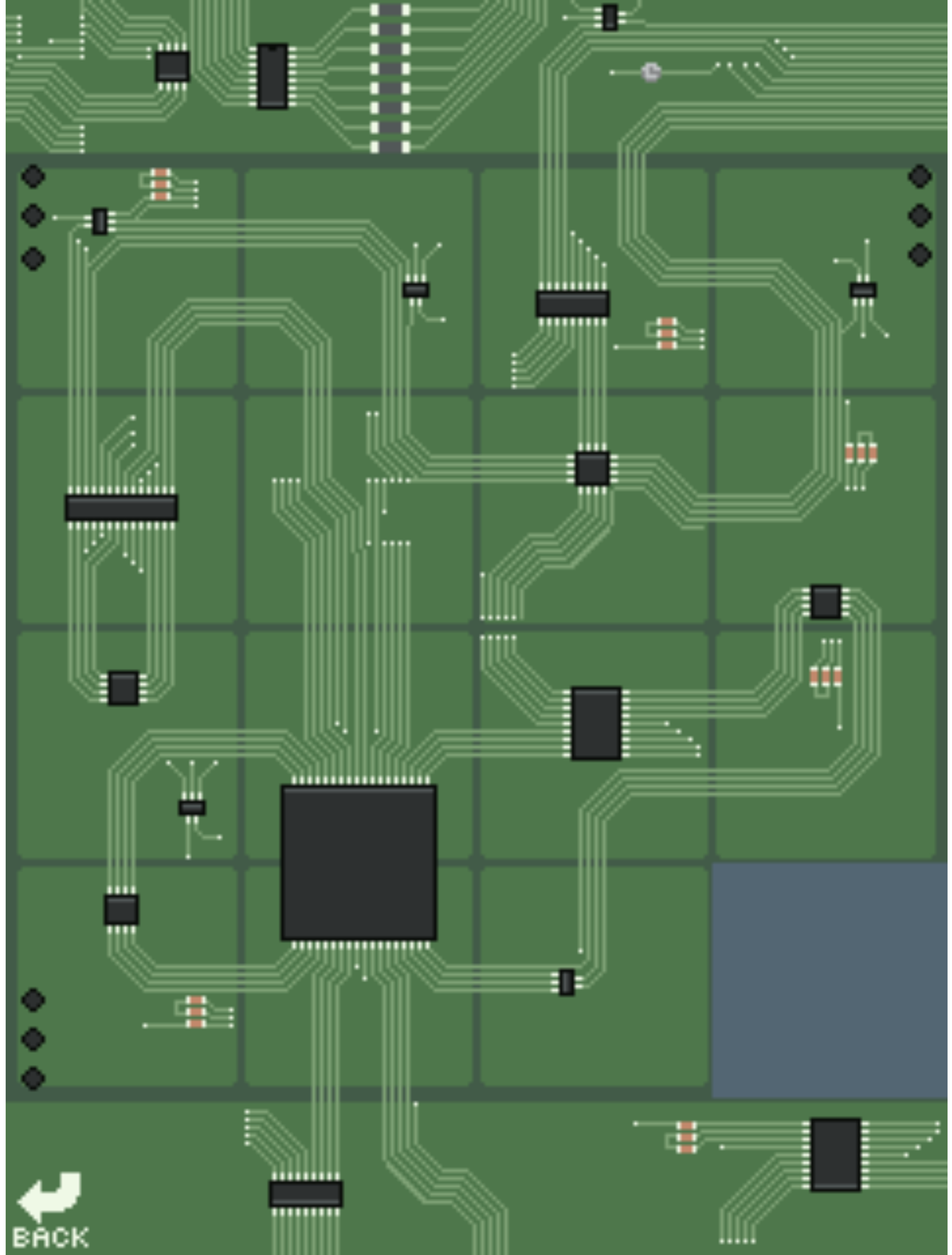
DJ SCENE

- Drop the bass!
- Hint on the wall regarding the keypad/ badge cipher challenge



ARCADE SCENE

- Play some (a) game
- Circuit panel can appear on the wall

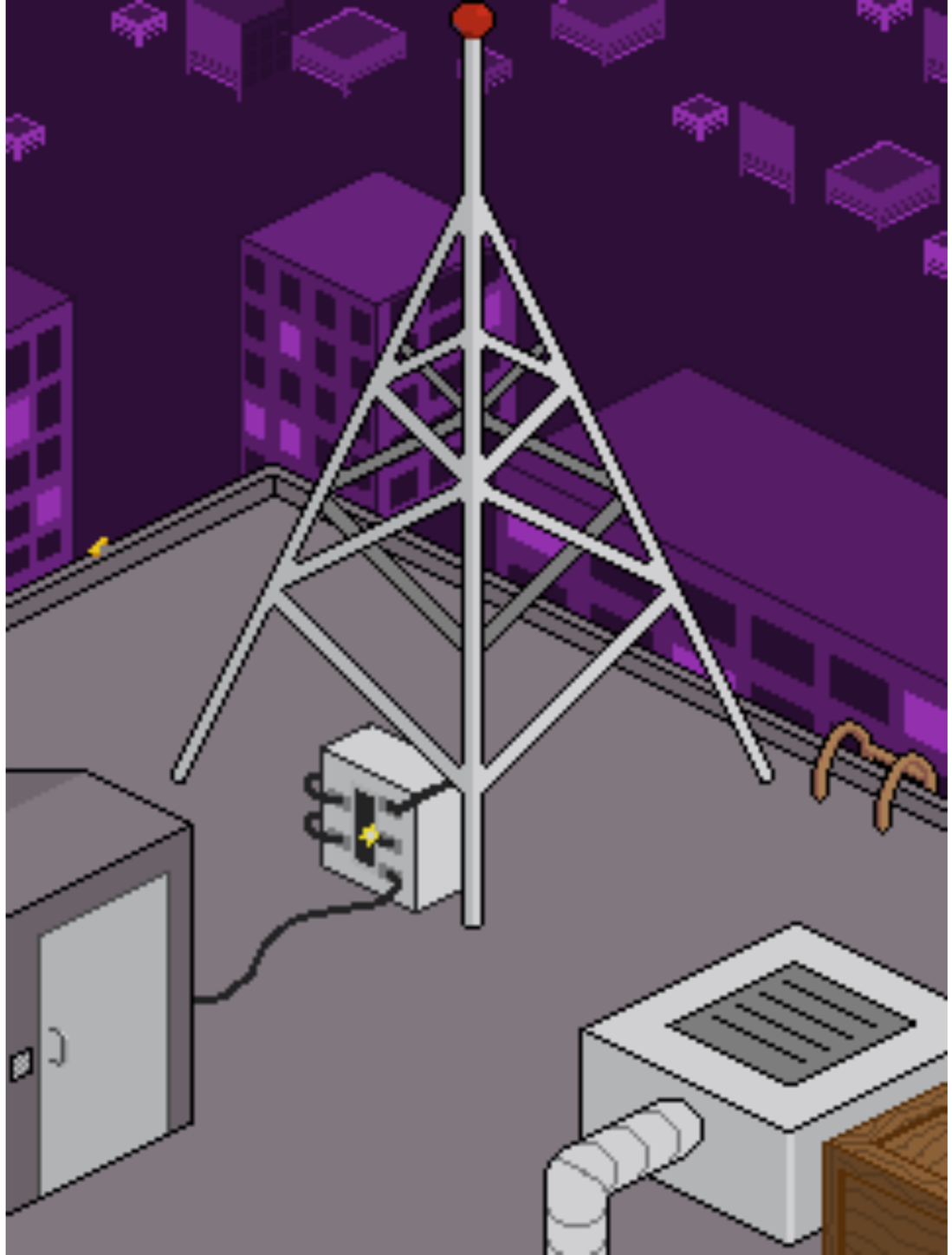


CIRCUIT PUZZLE SCENE

- Please don’t hate me
- (take a picture of the solution)
- After solving lights at the top provide a hint to the crypto puzzle (not necessary)
- Bug: if you drag from below the puzzle up to the empty square odd things happen

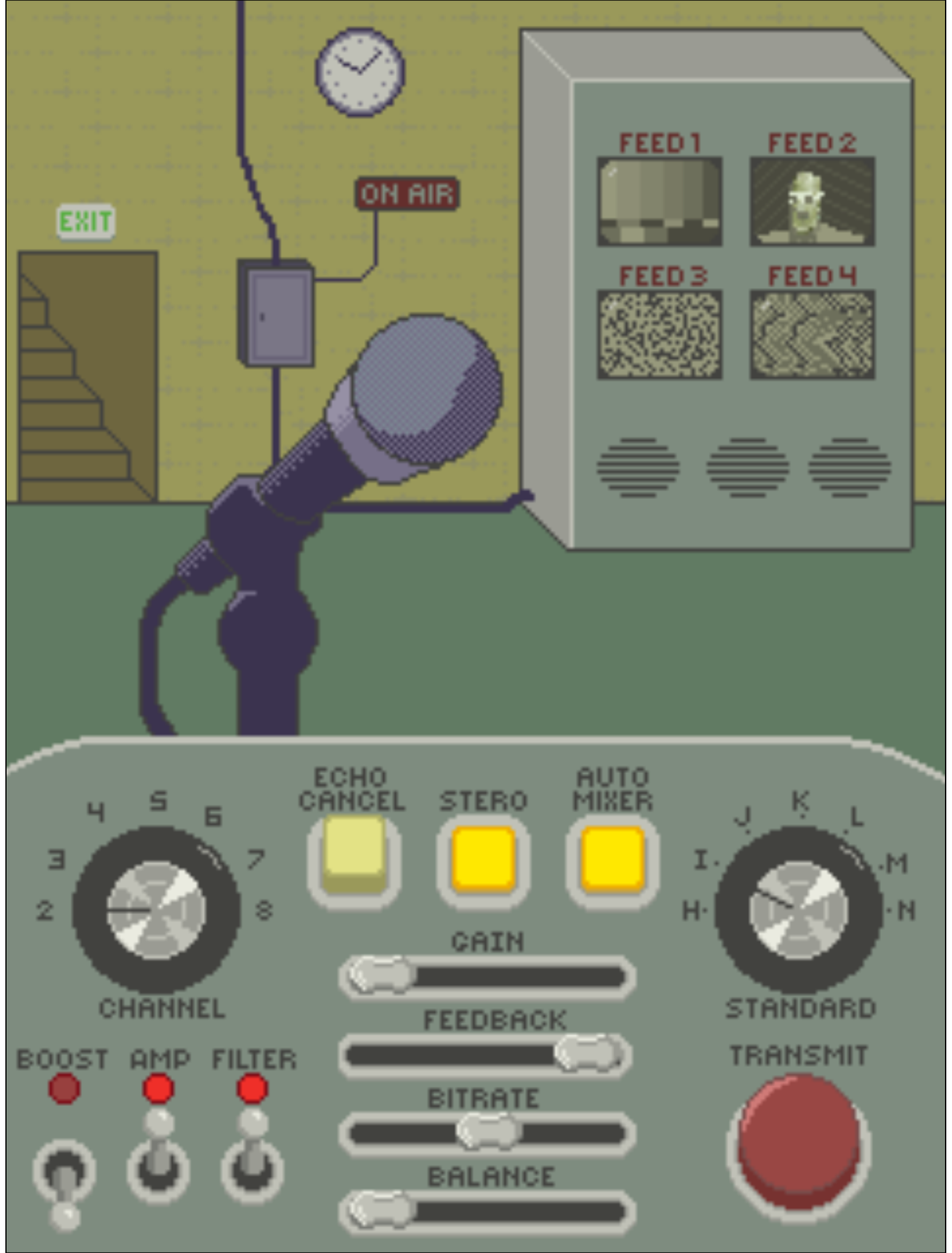
STREET SCENE

- Requires pairing with 5 different types of badges
- Service panel contains hint regarding soldering challenge



TOWER SCENE

- Requires solving the soldering challenge
- You can access a key pad by clicking the very small box by the door
- Hint for the phone booth behind the crate
- The “canary” is a small hint regarding the RE puzzle



BROADCAST ROOM SCENE

- Requires solving the crypto puzzle
- If you have completed all other challenges before completing this one you make it to the ending scene