PROJECT

BSIDES SLC 2020 BADGE

DESIGNER

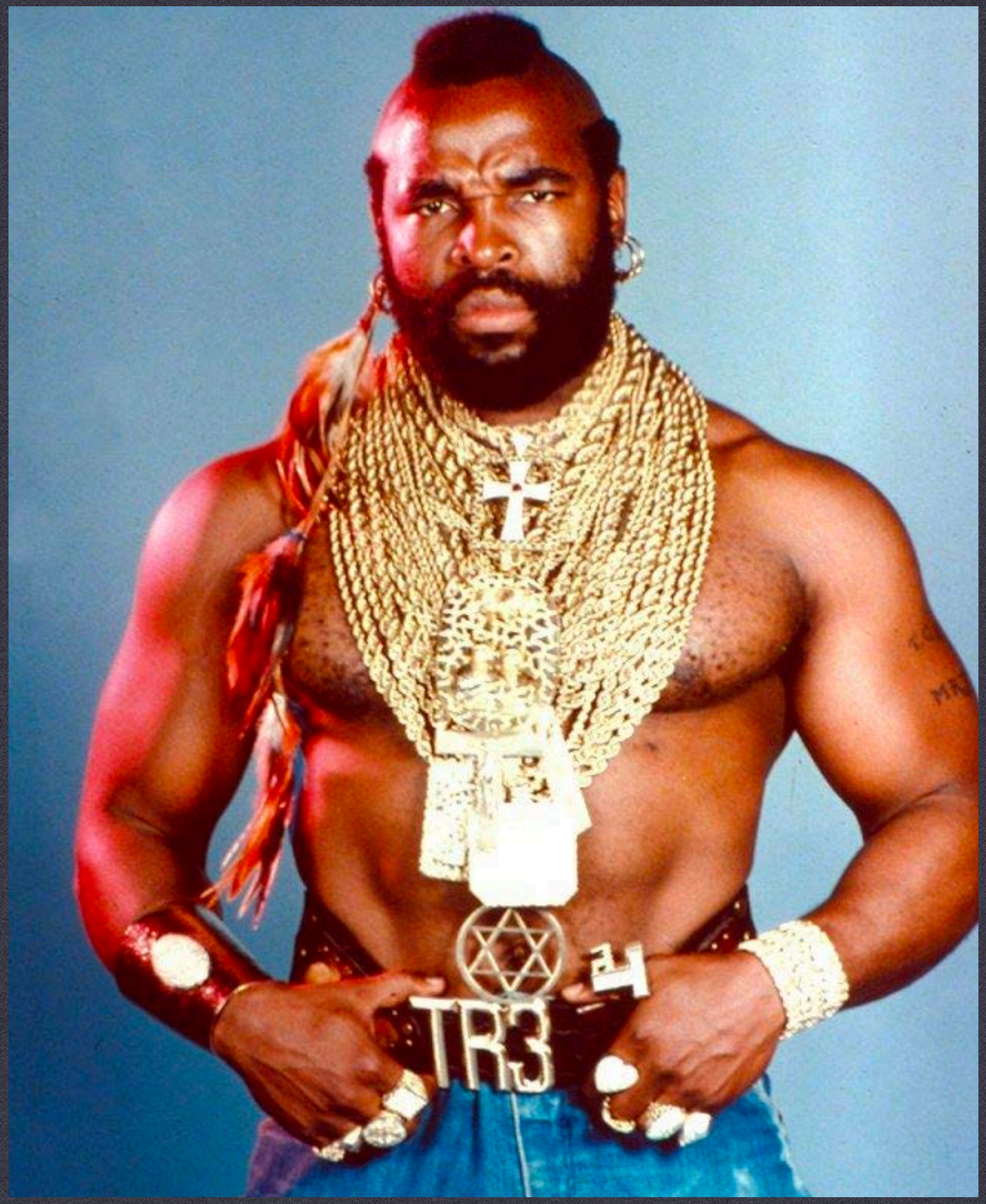
WAYLON GRANGE

DATE

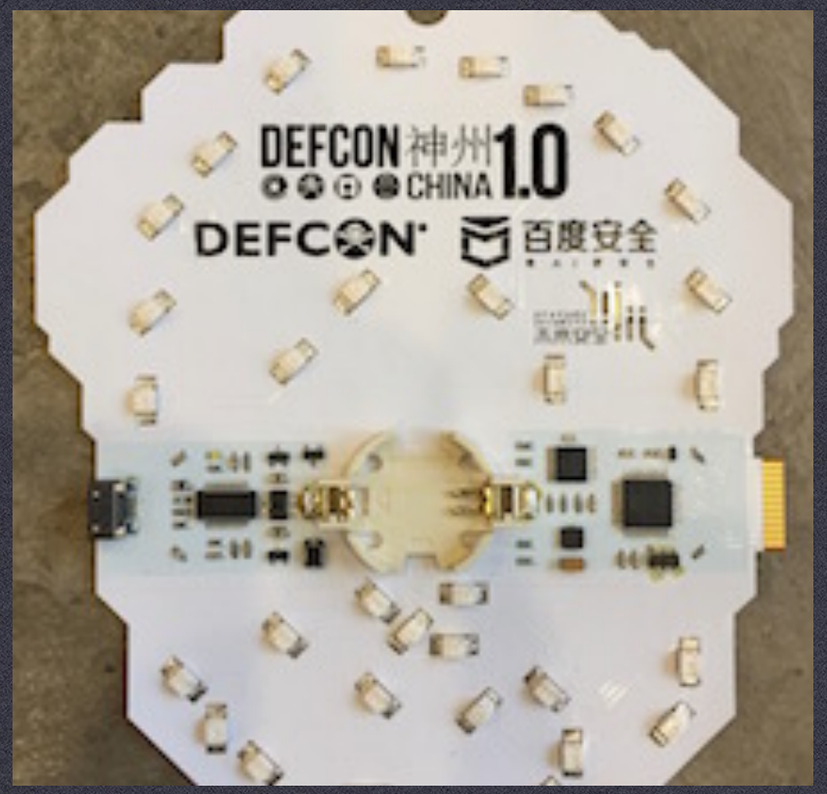
3/20/2020

TWITTER

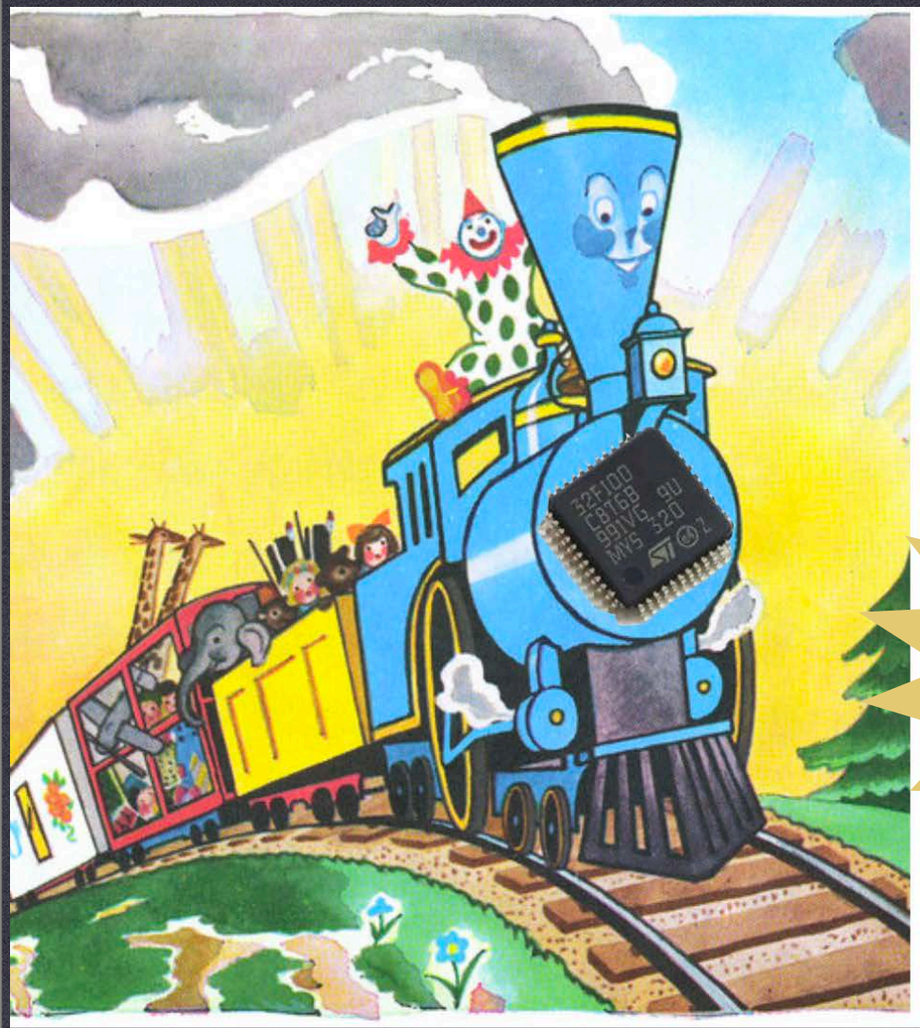
@PROFESSOR__PLUM



INSPIRATION — DEFCON / MR. T



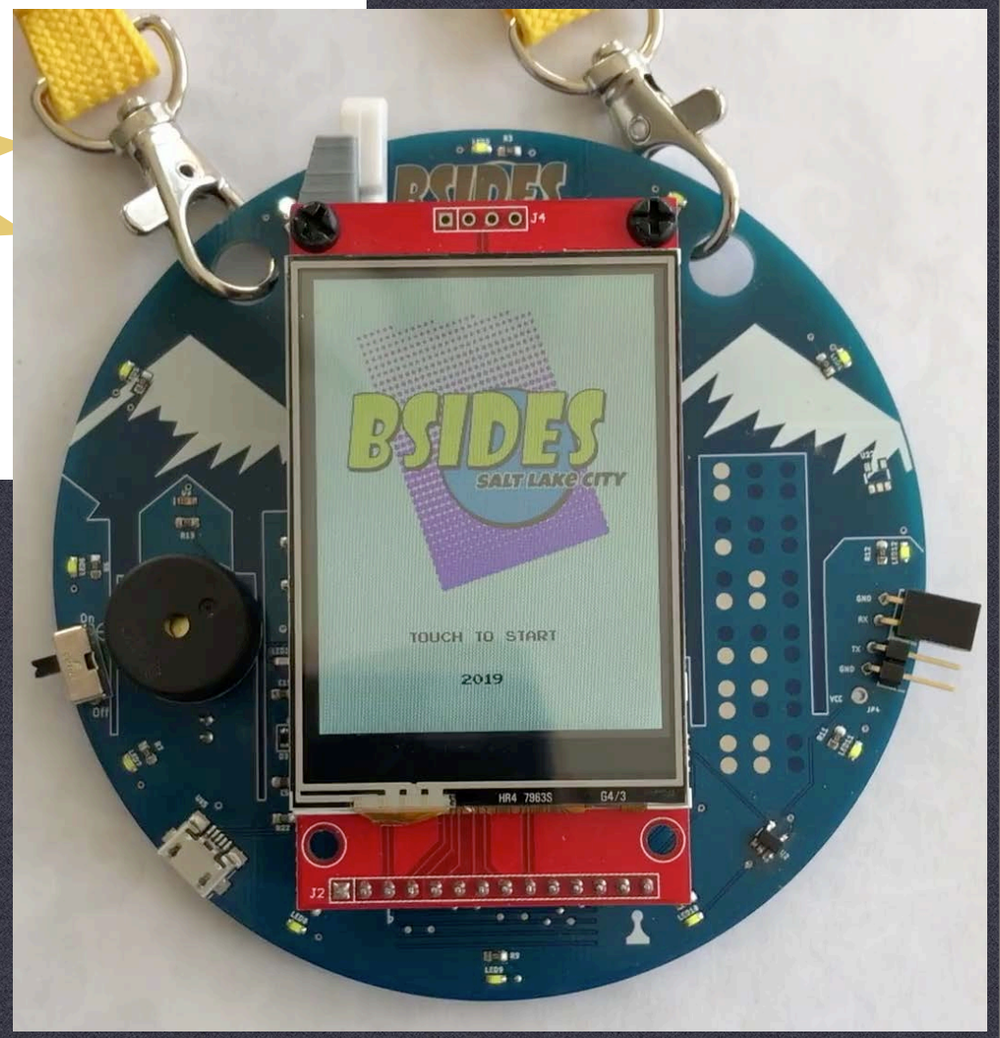
INSPIRATION — DEFCON CHINA BADGE



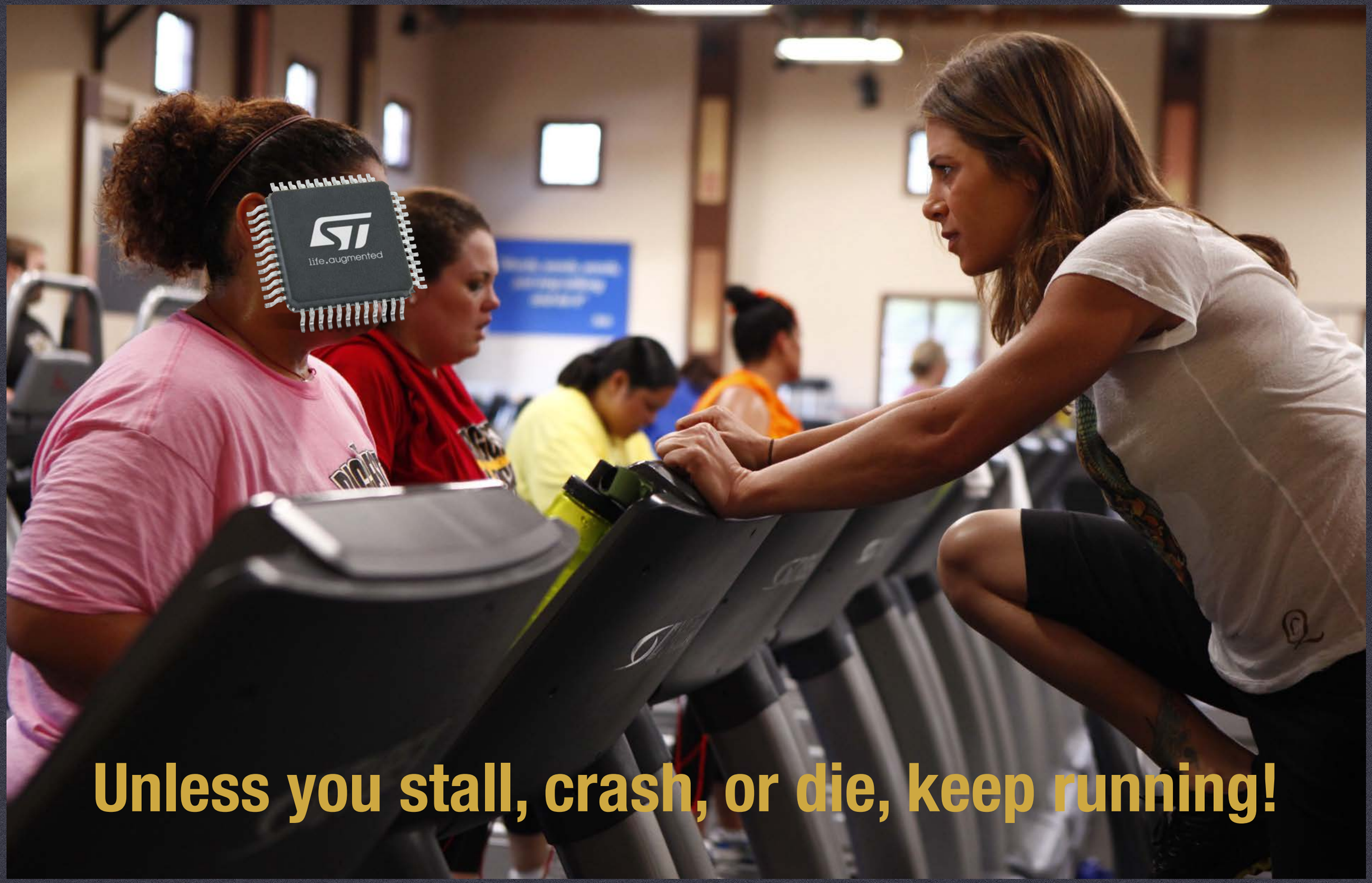
THE LITTLE MCU THAT COULD

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

Now with 66% less processing power!

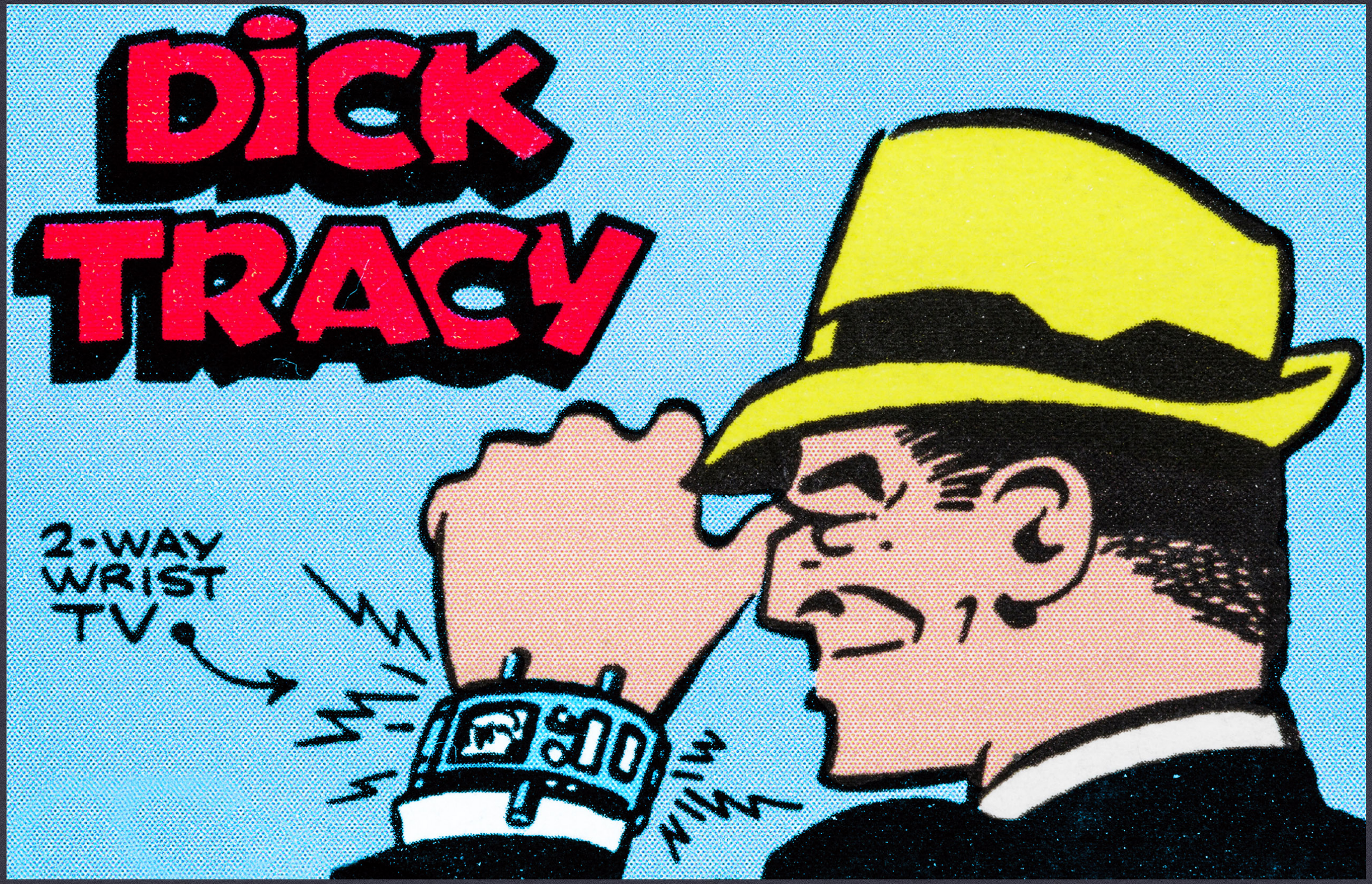


INSPIRATION — BSIDES 2019



INSPIRATION — BIGGEST LOSER

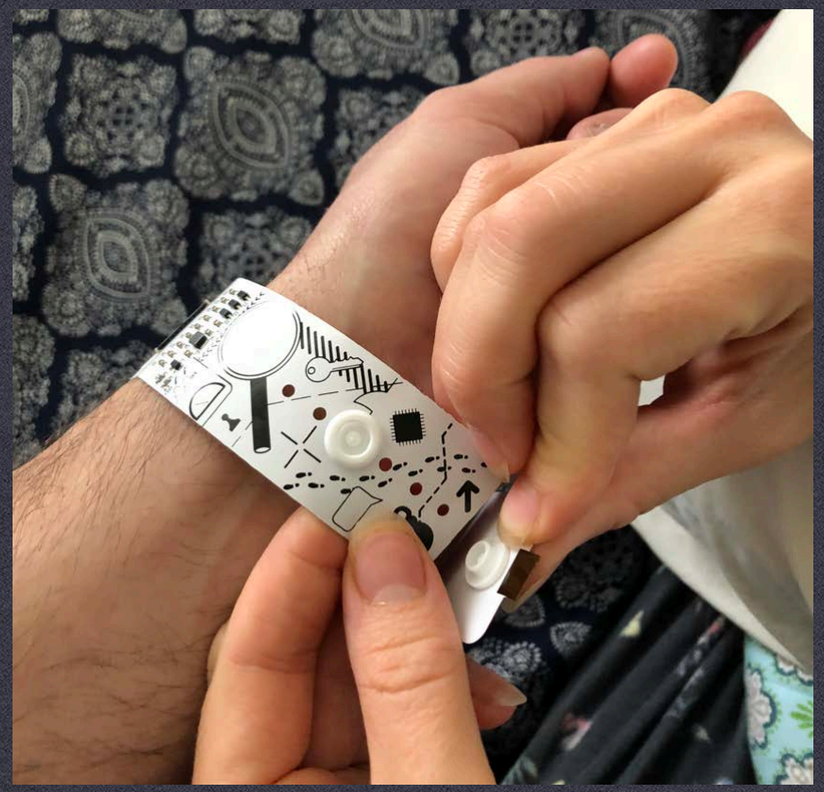
MICROPROCESSOR EDITION



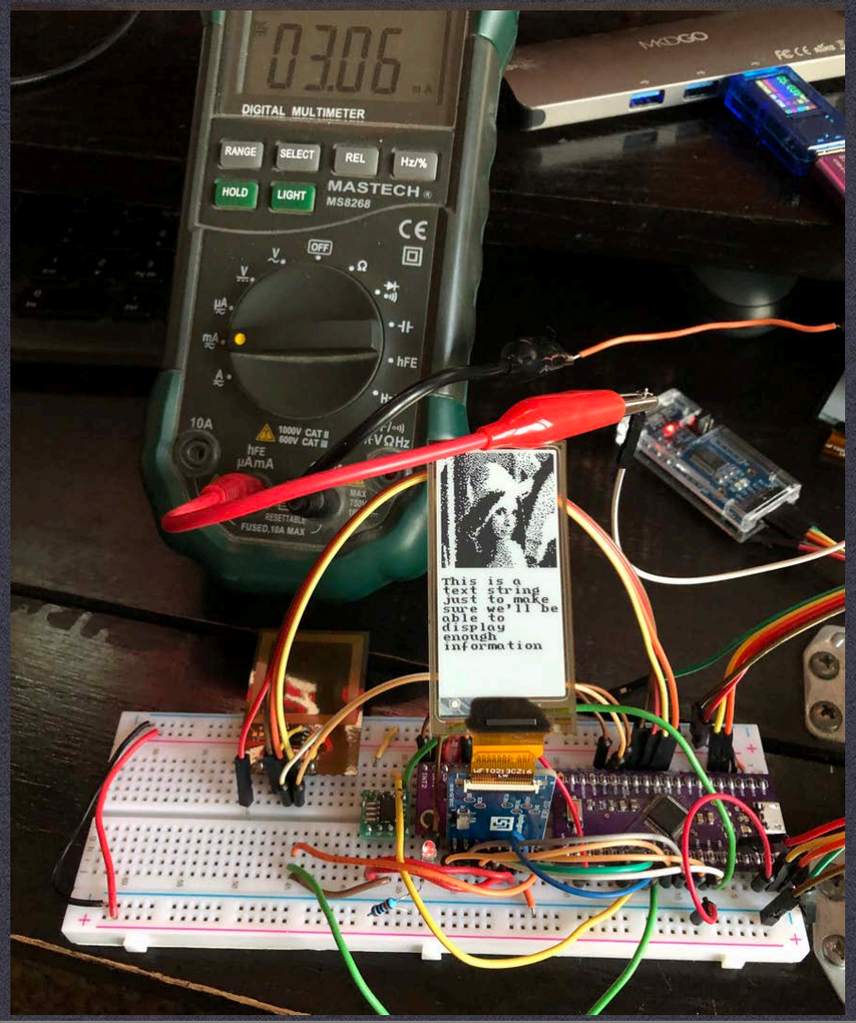
INSPIRATION — DICK TRACY

BADGE OVERVIEW

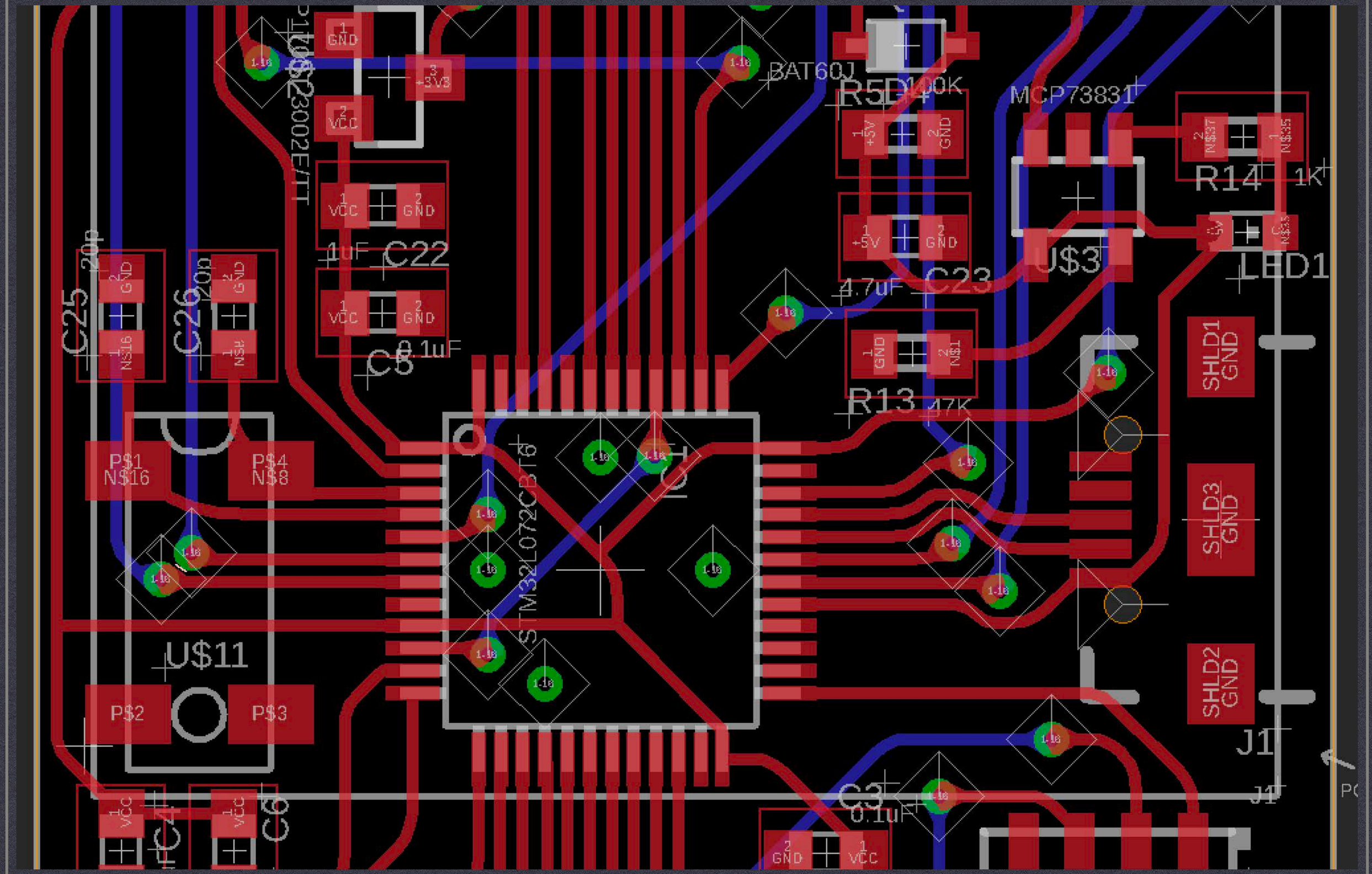
- FUNCTIONAL WATCH
- TEXT BASED ADVENTURE GAME
- E-PAPER DISPLAY
- 3D PRINTED CASE
- SIZABLE BUTTON SNAP
- MASS STORAGE DRIVE (USB)
- CDC SERIAL DEVICE
- AND MORE…



SNAP IT

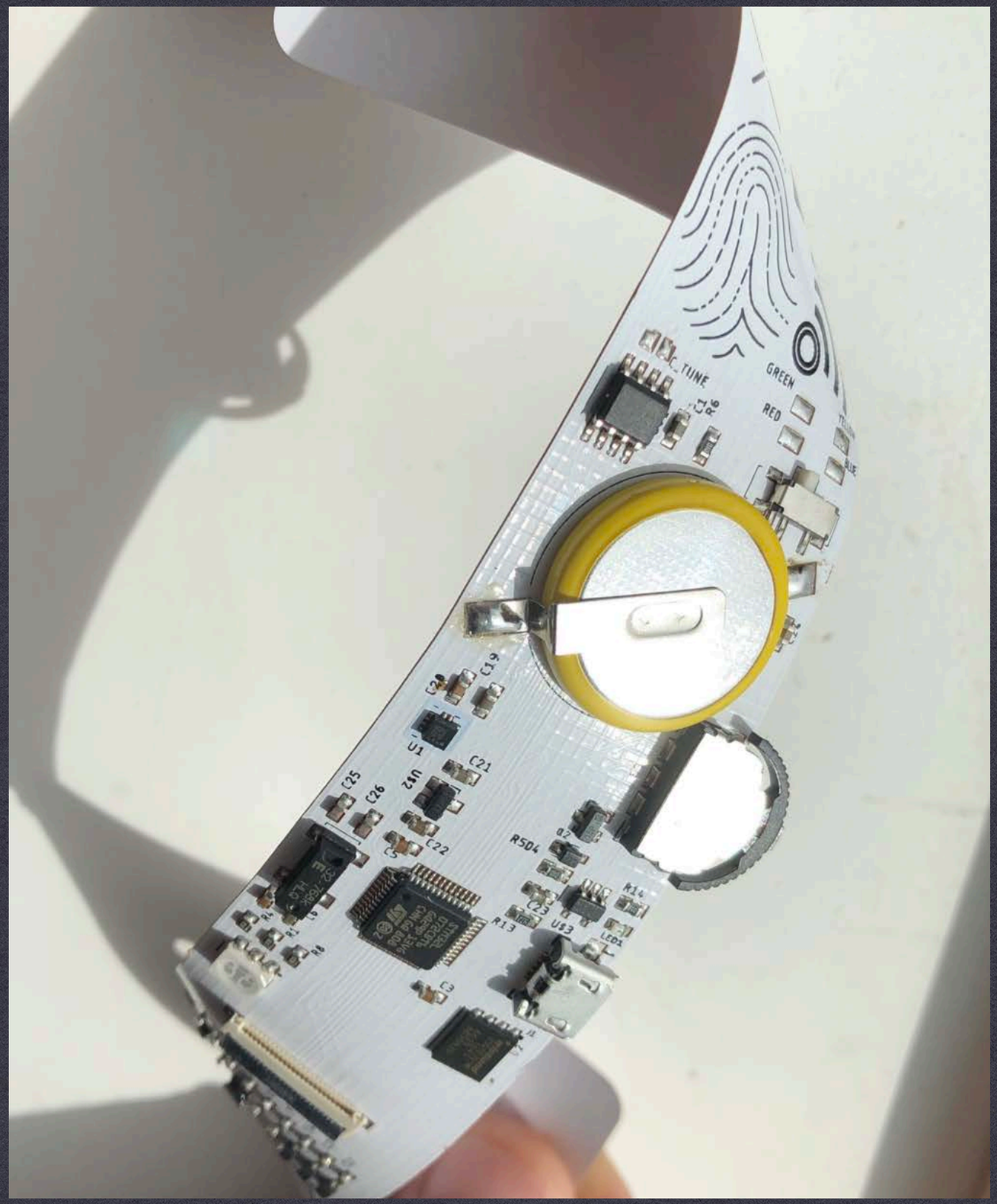


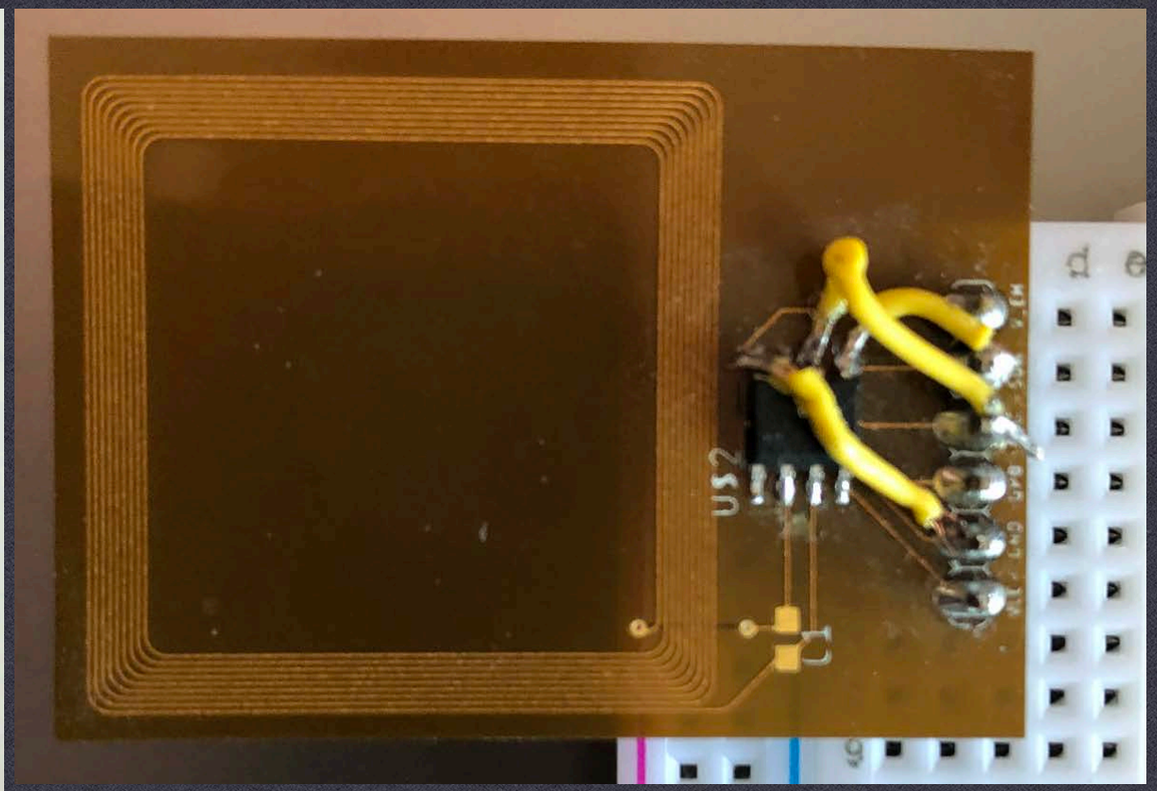
FROM PROTOTYPE TO FINAL DESIGN



HARDWARE

FLEX PCB, 32BIT ARM, FLEXIBLE E-PAPER DISPLAY, LIPO BATTERY, NFC, ACCELEROMETER, 2MB FLASH STORAGE, RTC





FLEXIBLE PRINTED CIRCUIT BOARDS

REALLY COOL … KIND OF

	2019 Badge	2020 Badge
Battery capacity	750 mAH	40 mAH
Screen refresh	110 mA	11 mA
Idle	40 mA	5 mA
Sleep	11 mA	3 mA
Standby	NA	25 µA

LESS POWER THAN A SINGLE LED

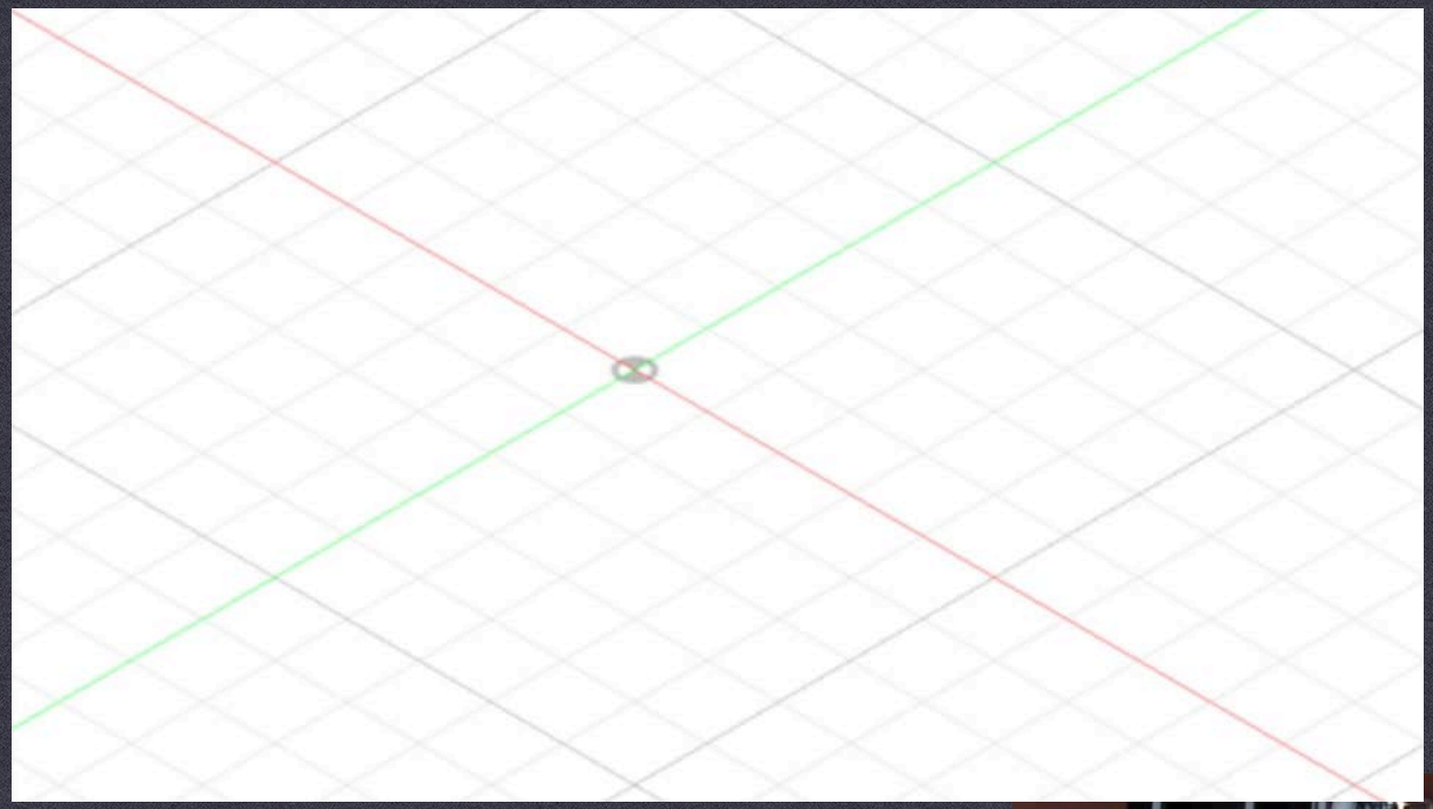
FLEXIBLE E-PAPER DISPLAY

NOT SO FLEXIBLE E-PAPER DISPLAYS

PILE OF BROKEN DISPLAYS

THE SCREENS ARE EXTREMELY FRAGILE

DON’T PUSH ON THE SCREEN, IT WILL BREAK



3D PRINTED CASE

DESIGNED IN FUSION 360, PRINT VIA 3D HUBS

FIRMWARE

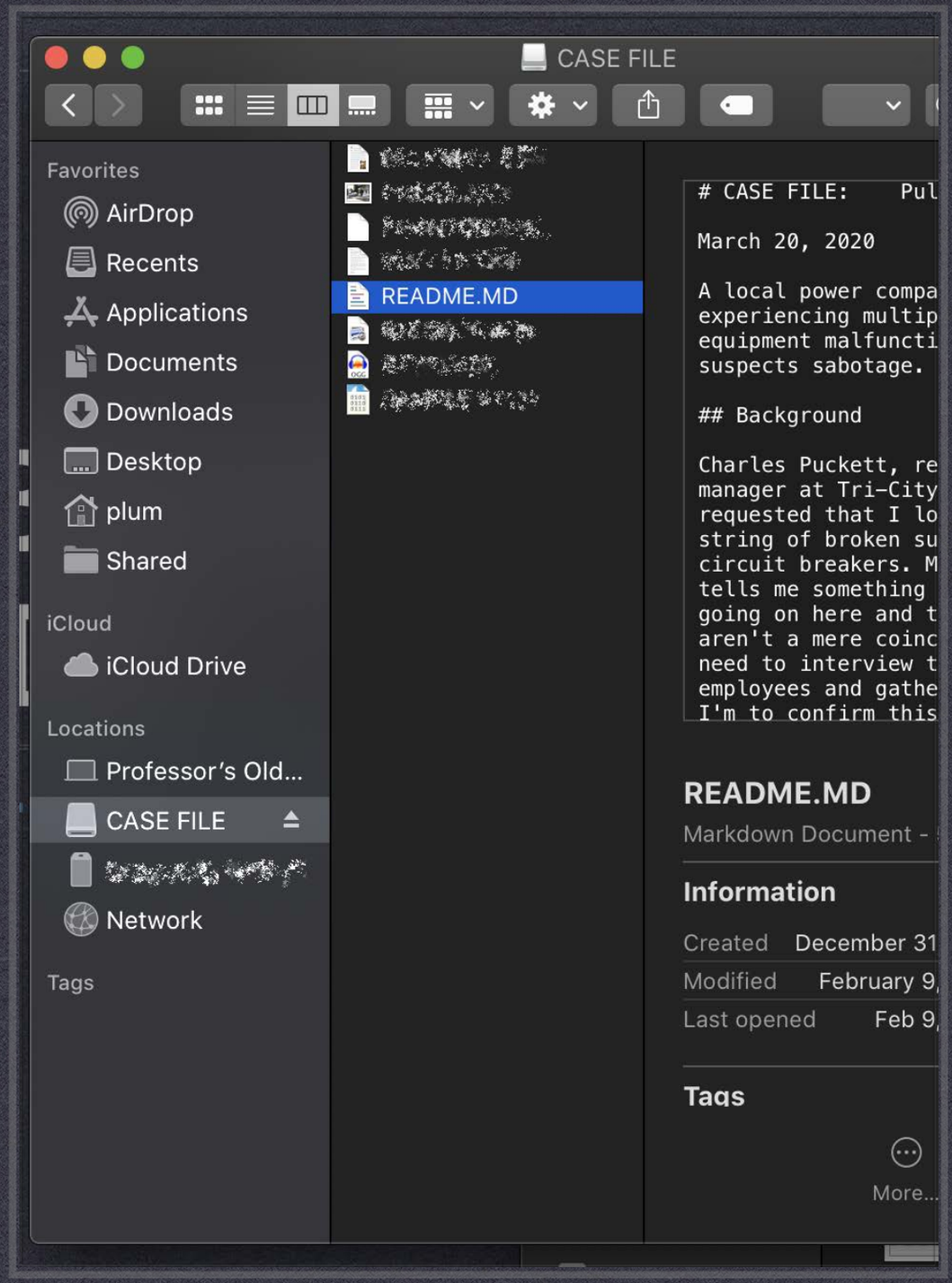
~3500 LINES OF CODE, EVERYTHING IMPLEMENTED IN INTERRUPTS, GAME STATE SAVED TO EPROM & 1 RTC REGISTER

I'M LATE, I'M LATE!

- AFTER 1 WEEK THE BADGE WOULD LOOSE ~4 MINUTES
- DURING DEBUGGING TIME IS VERY PRECISE
- HOW DO YOU DEBUG A PROCESSOR THAT IS POWERED OFF?
- DURING BOOT BADGE WOULD RE-INIT RTC WHICH RESULTED IN 20MS LOST
- 20MS * 60 * 24 * 7 = 3.36 MINUTES

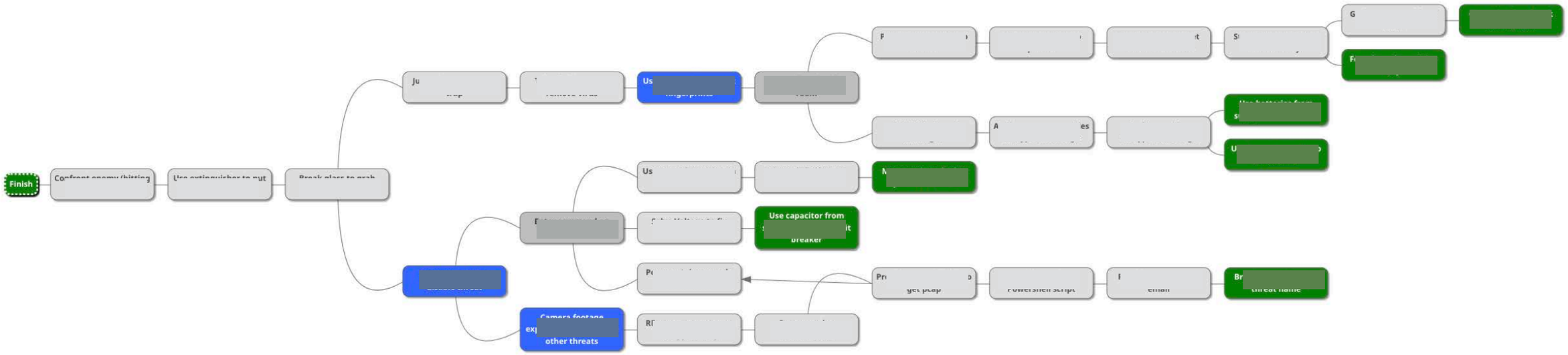
WHERE DO I STORE FILES?

- FLASH SPACE USED FOR USB MASS STORAGE DEVICE
- HOW DO I ONLY SHOW FILES ONCE DISCOVERED IN GAME?
- NO ROOM TO STORE THEM ELSEWHERE
- USB MSC USES SCSI COMMANDS
  - NO EASY FILE LISTING TO EDIT, JUST SECTOR READS
- SOLUTION… A ROOTKIT!
  - INTERCEPT SECTOR READS FOR FILE ALLOCATION TABLE



DIGITAL FORENSICS / INCIDENT RESPONSE THEMED

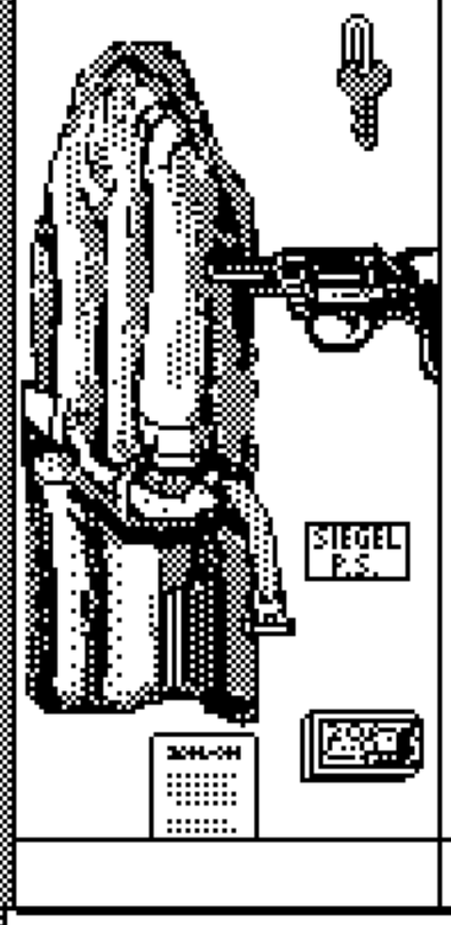
- DISCOVERED CLUES ARE PRESENTED ON USB STORAGE DRIVE
- PUZZLES INCLUDE
  - PACKET CARVING
  - REVERSE ENGINEERING
  - MALWARE ANALYSIS
  - DISK IMAGING
  - STEGANOGRAPHY
  - AND MORE
- THE BADGE BLINKS 4 TIME SIGNIFYING GAME PROGRESSION
- RED→WHITE→GREEN→CYAN→BLUE



GAME PROGRESS LOGIC

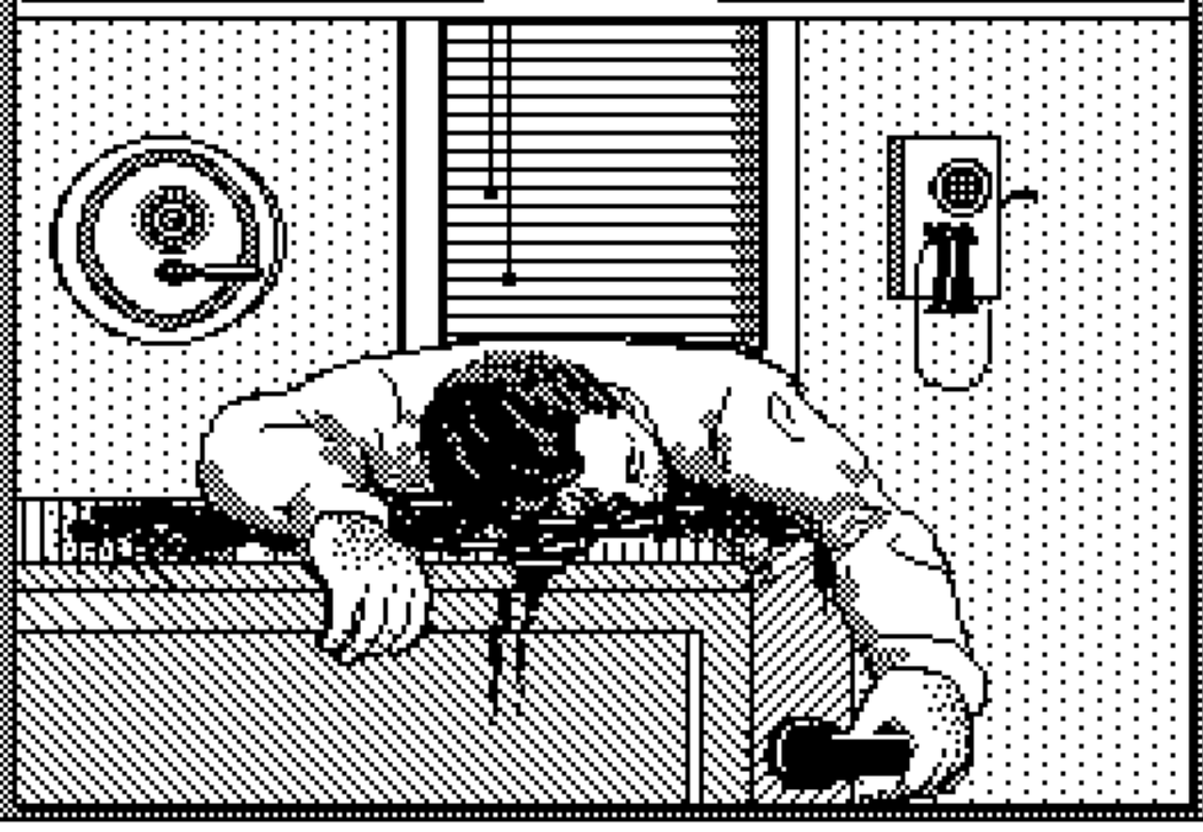
File Edit Special Font FontSize 12:23 PM

invent



Examine | Open | Close | Speak
Operate | Go | Hit | Consume

Office



SELF

System 7.5.3

Exits

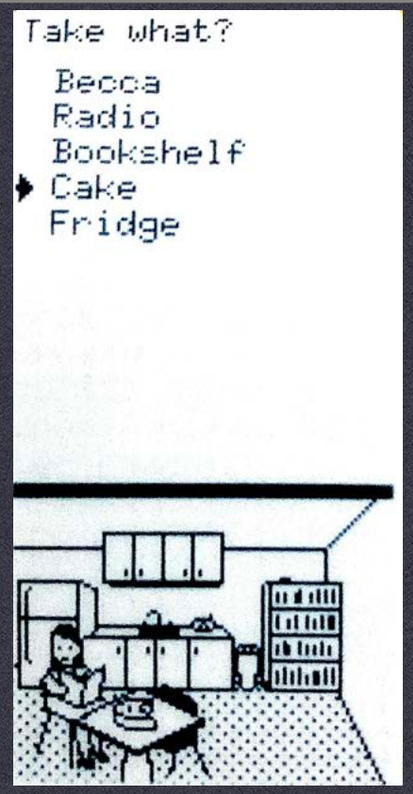
Untitled

You're in an office. There is a dead body slumped over the desk. His left hand still grips the phone receiver. In the background there is a wall safe, a window, and a telephone.

DÉJÀ VU — MACINTOSH


Select your avatar


Select topic
their position
damage
suspects
goodbye


Take what?
Becca
Radio
Bookshelf
Cake
Fridge


You stand at the entrance to some service tunnel which apparently runs under the whole city. It's a dark dingy place, maybe a slight step up from the sewers.


Take what?
Dresden
Meeting Table
Chairs
Blueprints
Crumpled note


Oh yes, I got an email from them. They offered free movies but it was fake, nothing happened when I opened the file. I'll forward you the email. (PH4N70M.EML added to CASE FILE)

Thanks for arriving so quickly detective. As you've probably heard, we've had a number of large circuit breakers fail. Some here suspect fowl play.

You're standing in the head office of the Tri-city Power Corp east side branch. The room is pretty bland and the walls look bare. The desk in the center is the only focal point.

A typical office break room. Complete with community fridge, microwave, and table. The young women sitting there glances up from her magazine to shoot you a polite gesture then returns to her reading.

Well, there goes my weekend. Can you find out if the malware called out to anywhere? If you know the IP address I could probably pull the traffic capture, assuming it hasn't rolled off yet.

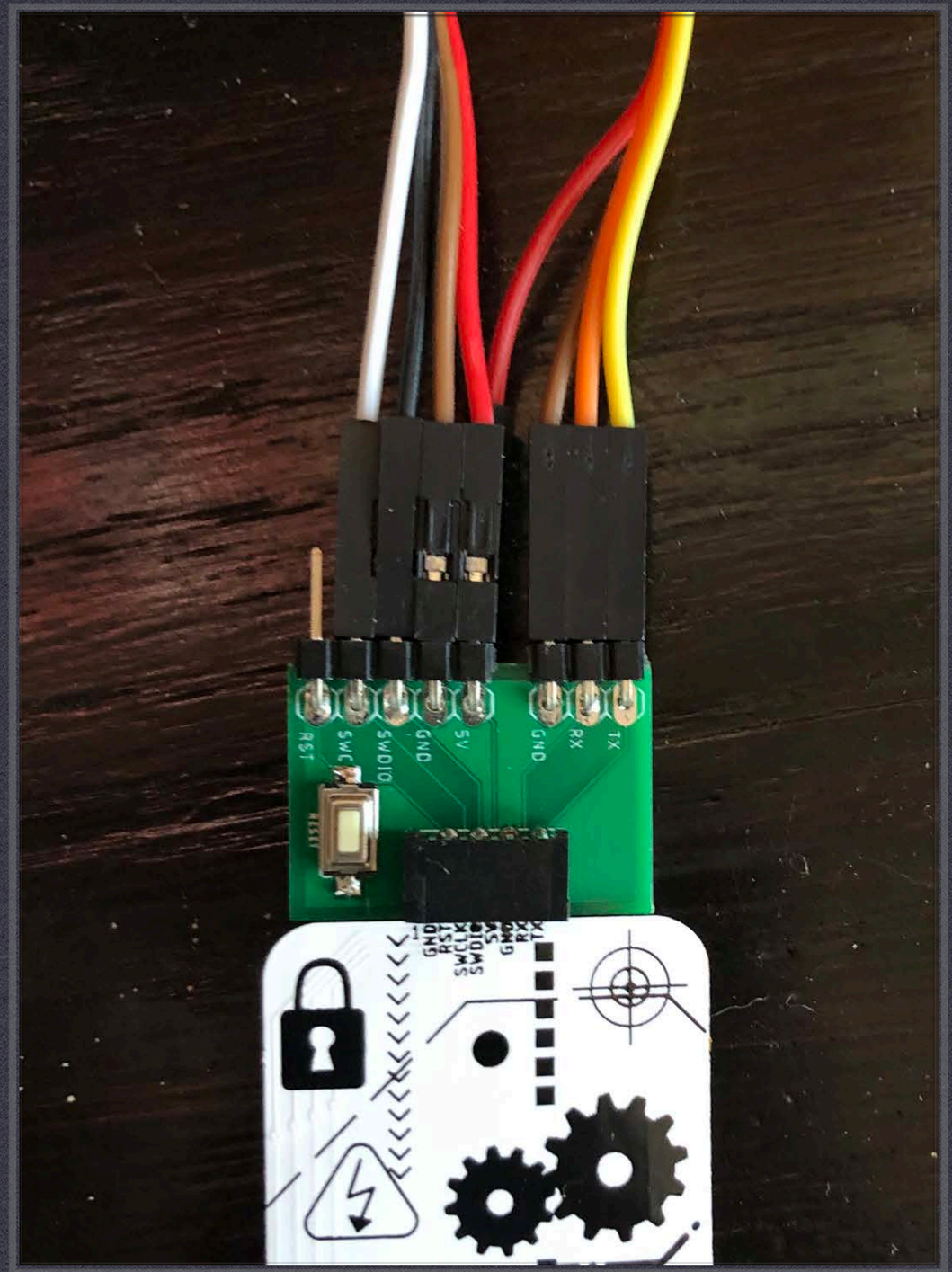
Inspect what?
Computer
Desk
Papers
Key card
Packing Tape

You stand at the entrance to some service tunnel which apparently runs under the whole city. It's a dark dingy place, maybe a slight step up from the sewers.

GAME PLAY

ADMINISTRATIVE

- ALL RESOURCES WILL BE RELEASED AT LINK BELOW
- SOME PROGRAMMING BOARDS AVAILABLE
- SET TIME VIA TEXT TAG
  - Date: 03/20/20 15:00:00
- SPECIAL THANKS TO:
  - BSIDES STAFF
  - COMPUKIDMIKE



https://github.com/Professor-plum/BSides-SLC-Badge-2020

THANK YOU

@professor__plum

STAGE 2
SECURITY