
Due to local laws,
we are temporarily
restricting access to
this content until
DEF CON can
estimate your age

*Joke

West of the DEF CON Creator stages

You are standing in the midst of the bustling DEF CON crowds. There's a mysterious flyer on the ground here.

> pick up flyer

You grab the flyer and read it.

(taken)

"WELCOME TO 'THE POWER(POINT) GLOVE'!

This is a talk of adventure, failures and low cunning. In it you will explore usage of weird presentation props. No hacker should be without one!"

> go east

Creator stages.

You are here!

Credit: Start of the adventure game, Zork! by Infocom

The Power(Point) Glove

Parsia ~~Hakimian~~ Hackerman

DEF CON 33 (8-10 Aug 2025)
Hardware Hacking and Soldering Skills Village

Friendship ended with Clicker

Now

PowerPoint

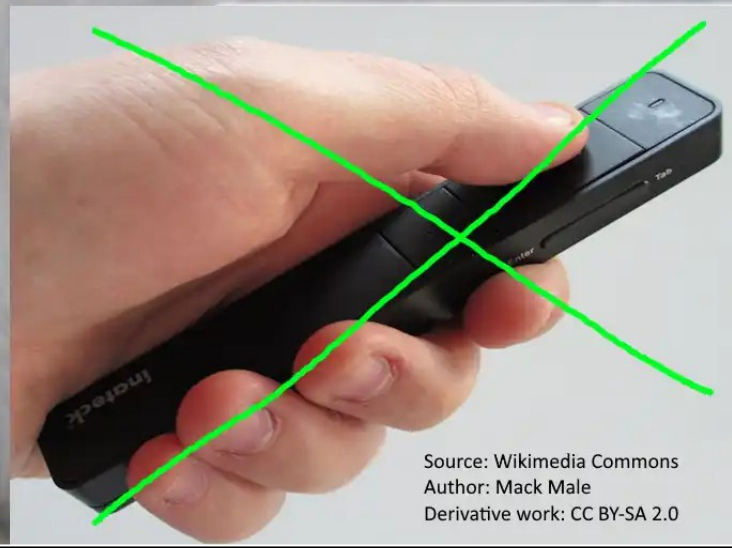
Glove

is my

best friend

Source: Wikimedia Commons - public domain

Souce:
Wikimedia Commons - public domain



Source: Wikimedia Commons
Author: Mack Male
Derivative work: CC BY-SA 2.0

Agenda

- Intro
- Motivation
- Power Glove History
- How it Works
- Literature Review
- Development Boards
- ESP32 Development
- Controller Button Presses
- ESP32 as HID
- Demo

~~Humble Brag~~ about.md

- Security @ MSFT
- DEF CON 26/28/33
- No 1337 name
- LARPs as a hacker

Incoming Transmission from the Big Giant Head

- Independent "research"
- Not affiliated with:
  - My employer
  - Your employer
  - Any employer
  - Your uncle at Nintendo

Contertainment!

- A talk about (info-sec) talks
  - Haroon Meer
  - 44CON 2013 Keynote

- Entertainment fills the seats
- No one remembers how many bugs you found!

Learning the Wrong Lessons from Haroon

1. Magic
    - "Any sufficiently advanced technology is indistinguishable from magic."
      - Arthur C. Clarke
2. Charisma
    - Have rizz, will travel.

3. Pizzaz
    - Make it pop!

Barnaby Jack – Black Hat US 2010, photo by Dan Tentler (Viss)

History

- NES accessory
- 1989 @ $75~100
  - $200~250
- Not created by Nintendo.
  - Abrams/Gentile Entertainment
- Production:
  - Pax (Japan)
  - Mattel (US)

What even is a Power Glove?

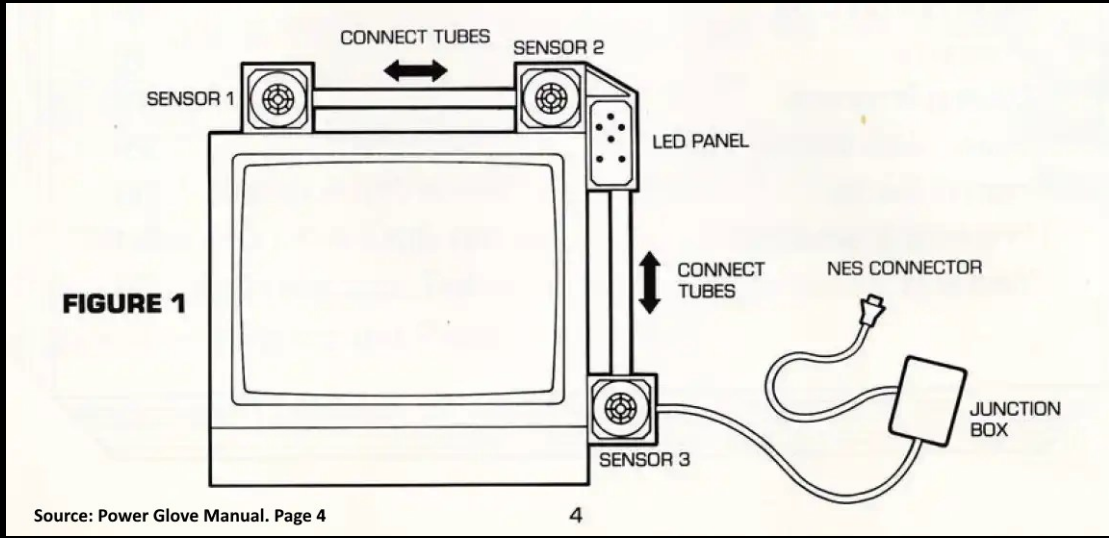
The Beauty and the Beast

The Wizard

The Wizard

The Wizard

The Sensor Array



Source: Power Glove Manual. Page 4

The Junction Box

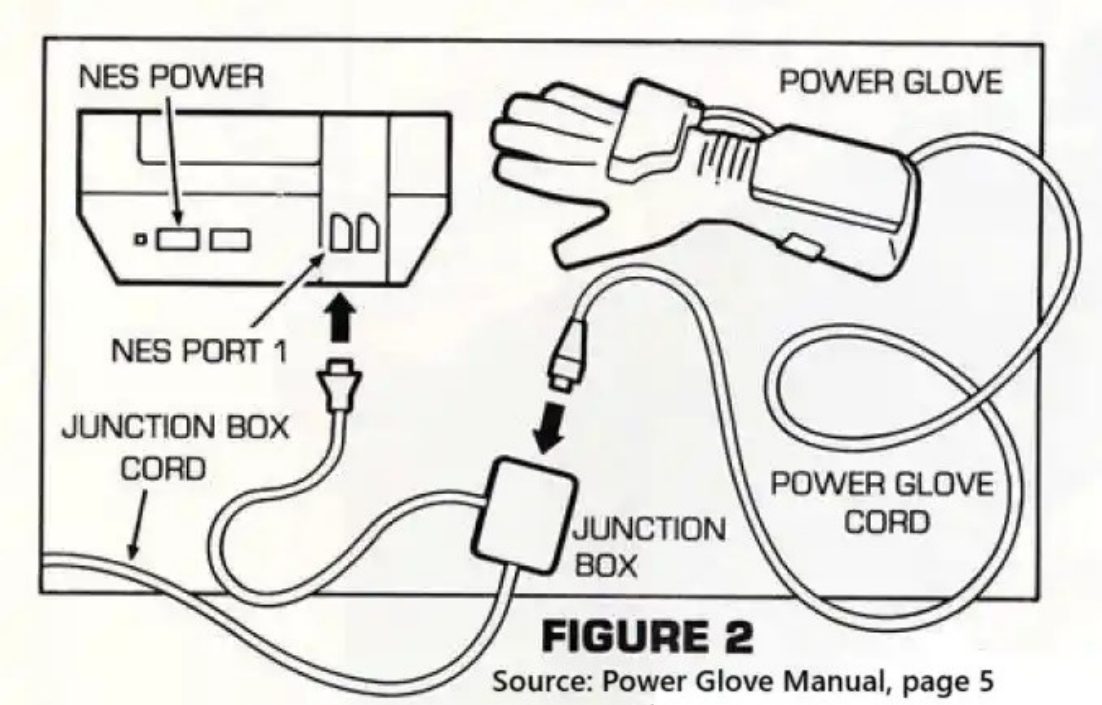
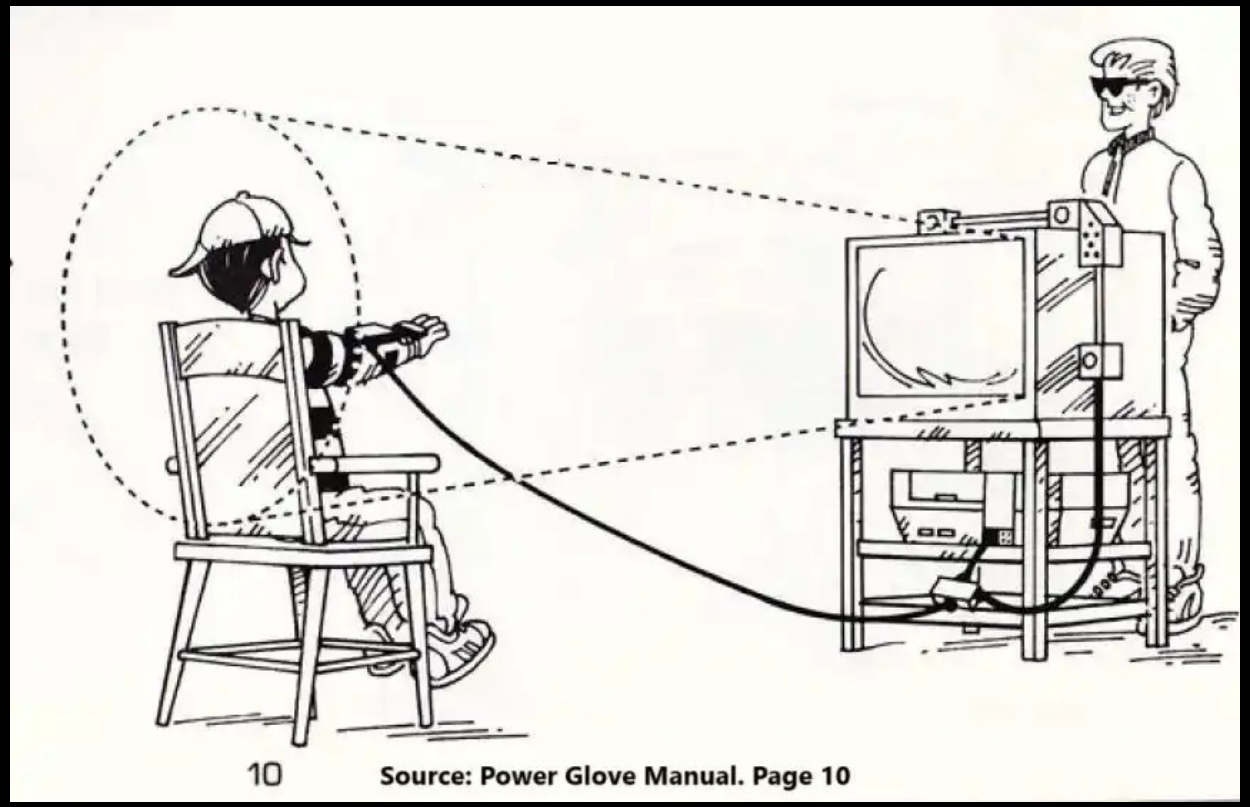


FIGURE 2

Source: Power Glove Manual, page 5

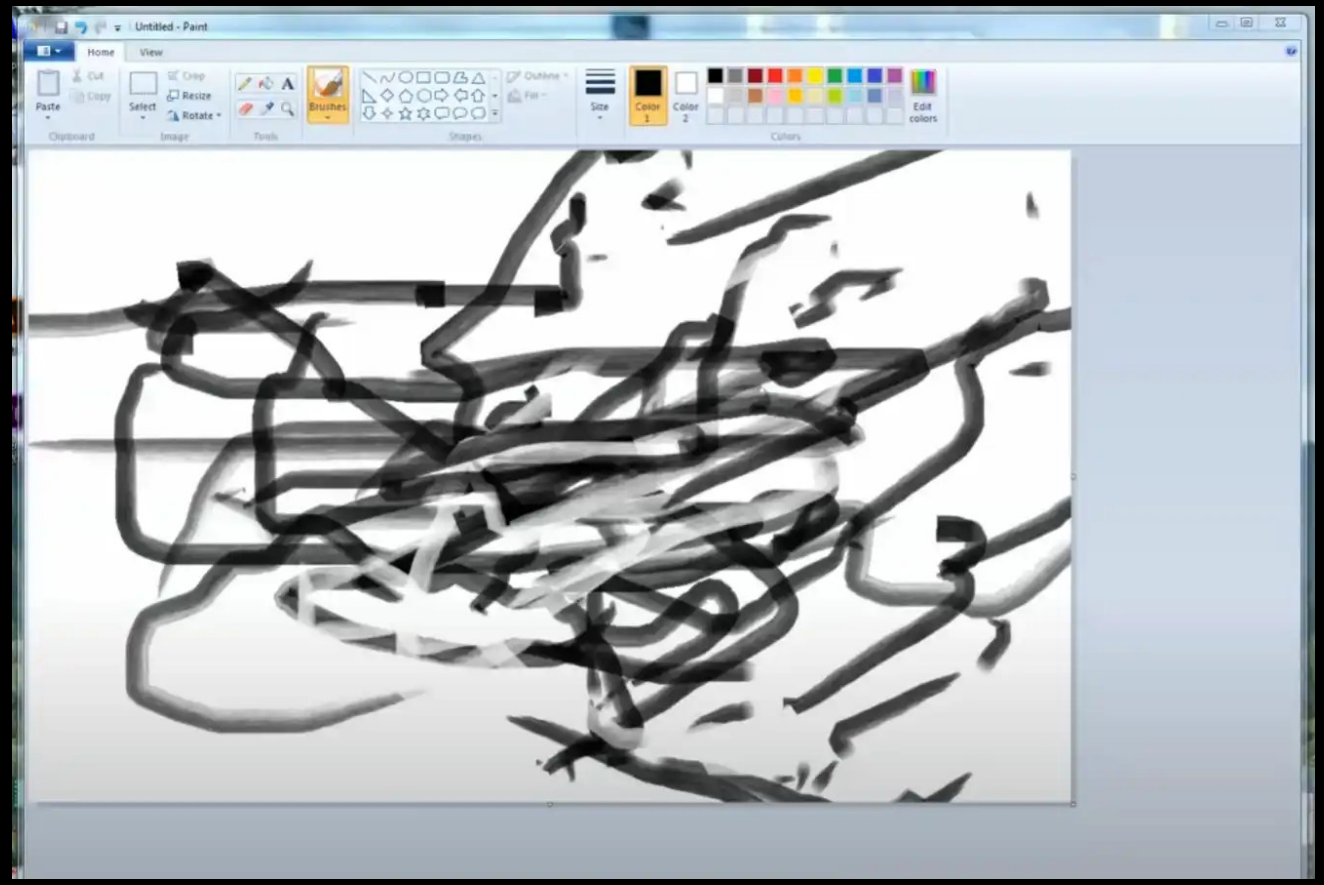
~~I am Batman~~ So it’s like a bat (without the echo)



Literature Review – Flipper Zero (2023)

Source: Twitter user @lamp_sec @ DEF CON 31 (2023)

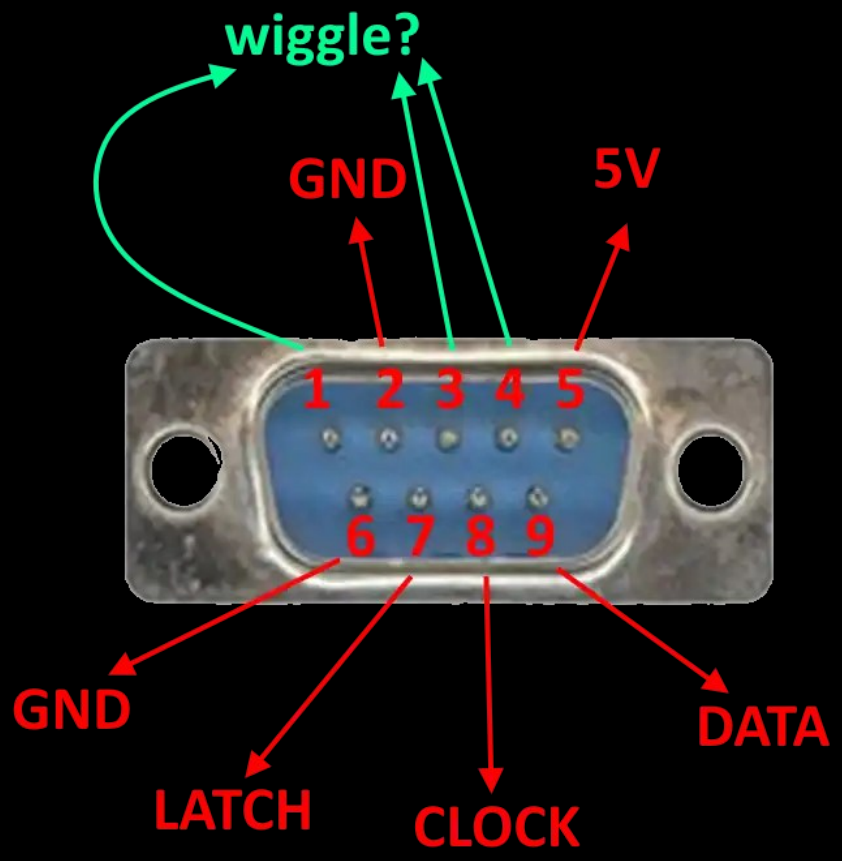
Literature Review



Ben Heck's Power Glove Teardown (2016)
https://www.youtube.com/watch?v=KAUp1c3_8wg

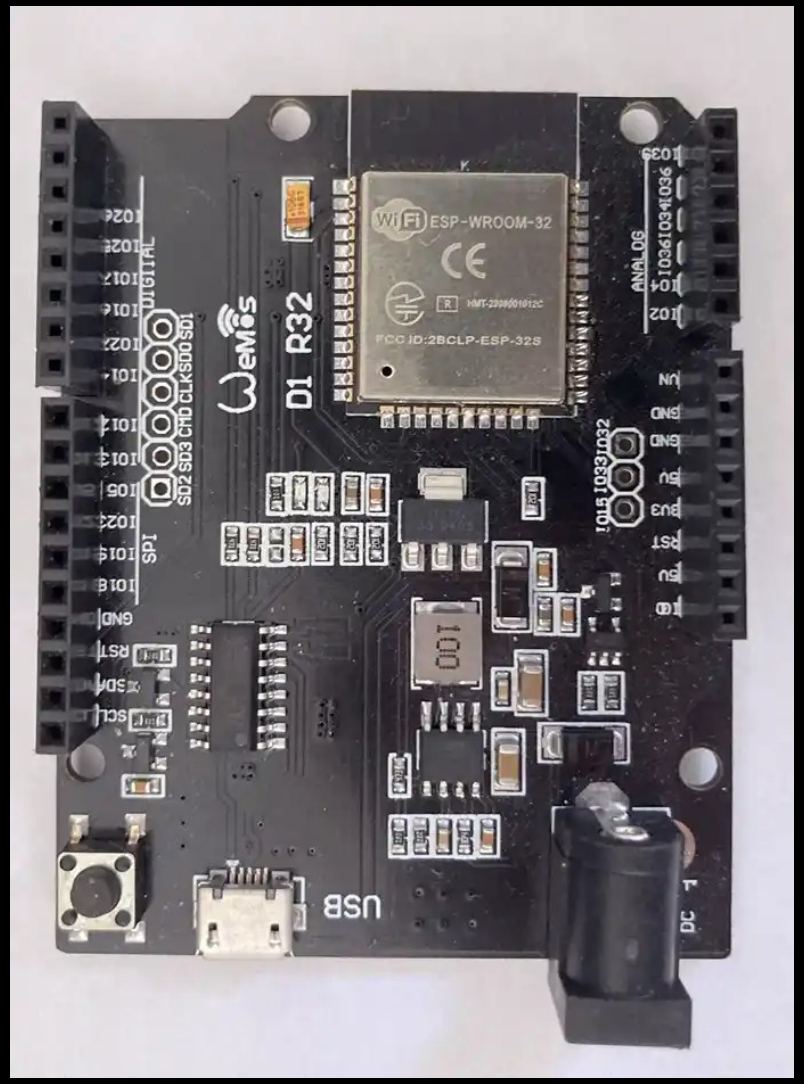
Dr. Benjamin Blundell (2018)
Blog: https://benjamin.computer/posts/2018-10-15-powerglove.html
Code: https://github.com/OniDaito/PowerGlove

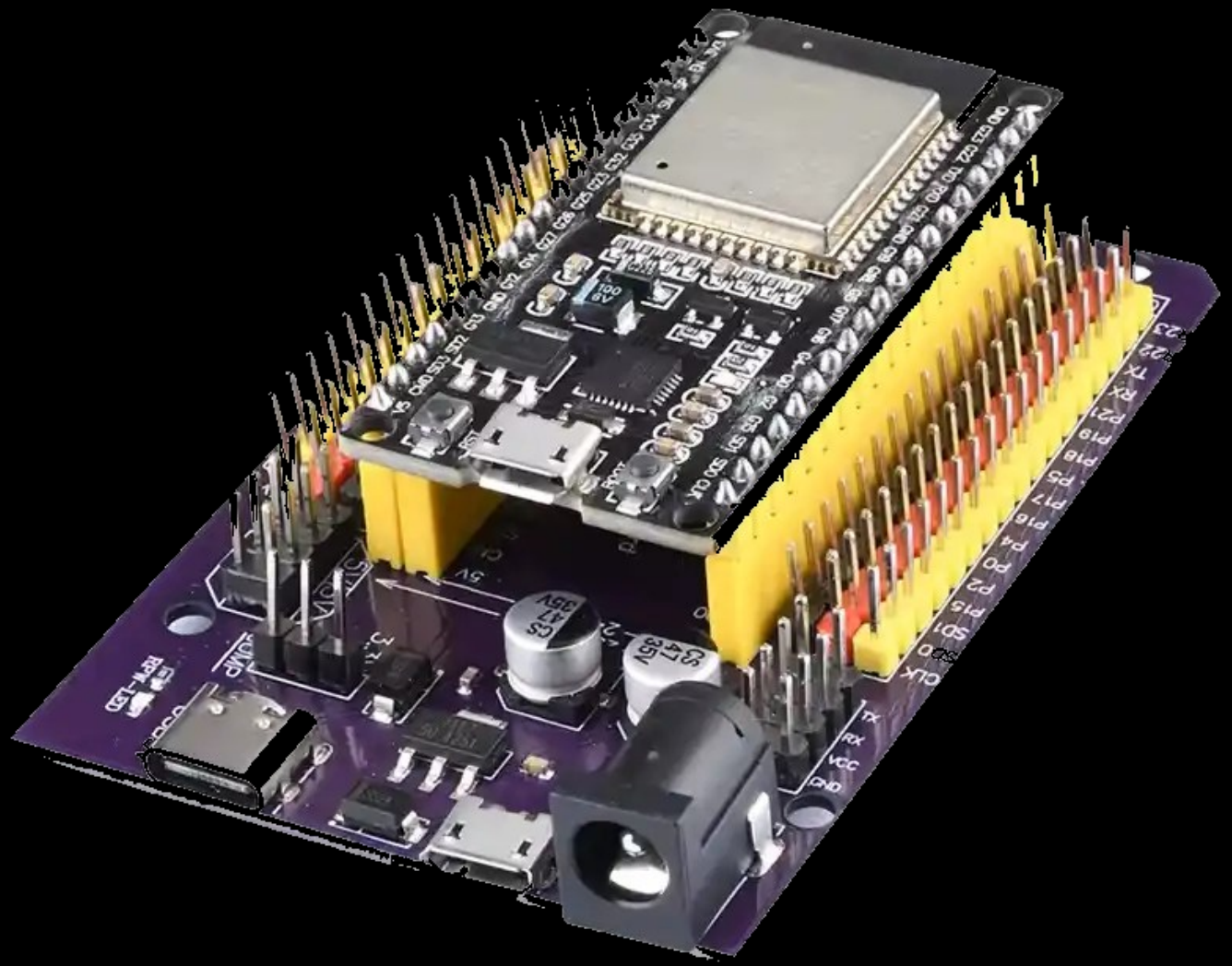
DB9/DE9 Diagram



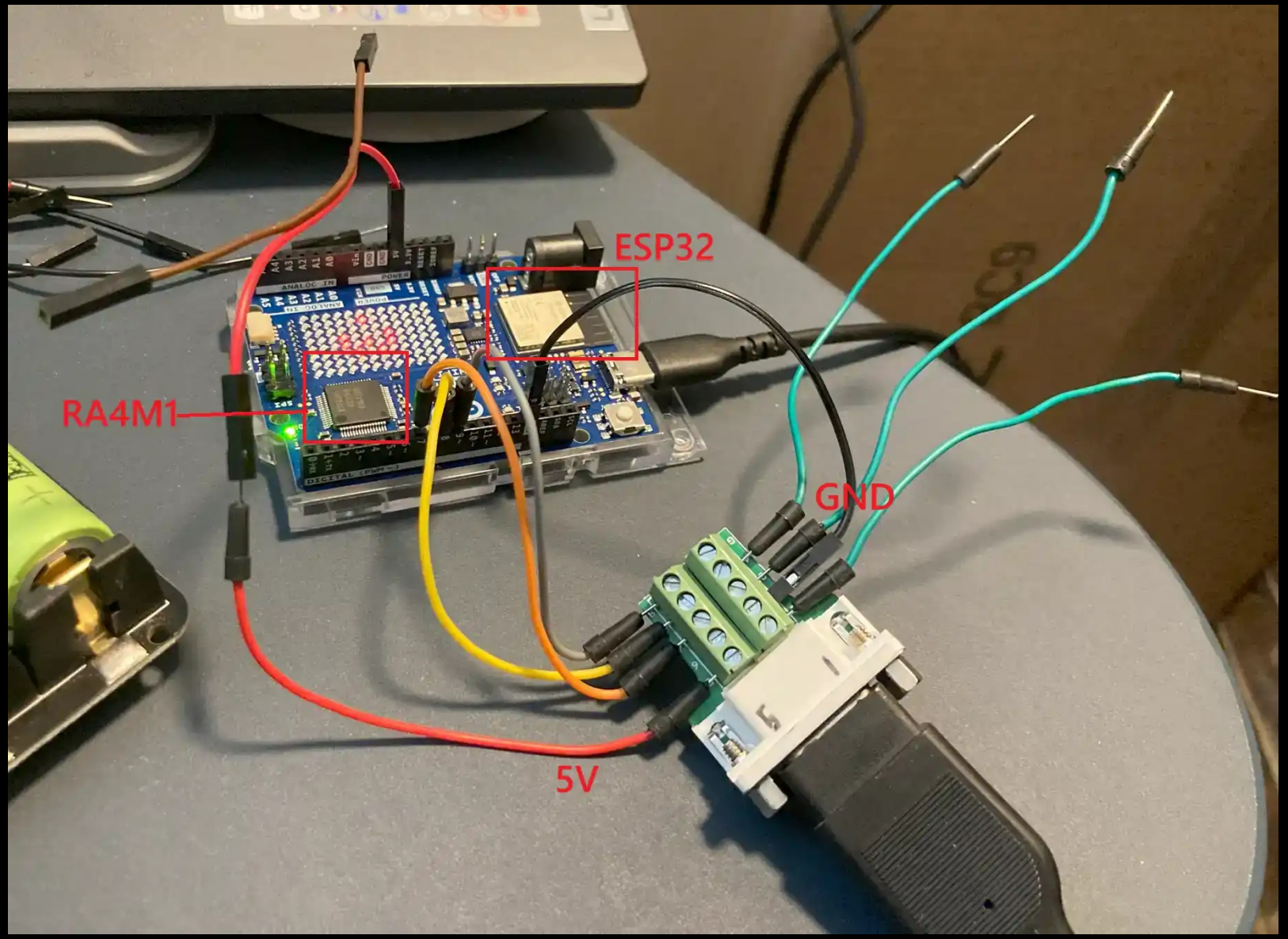
https://www.retrousb.com/product/nes-retroport/24

ESP32

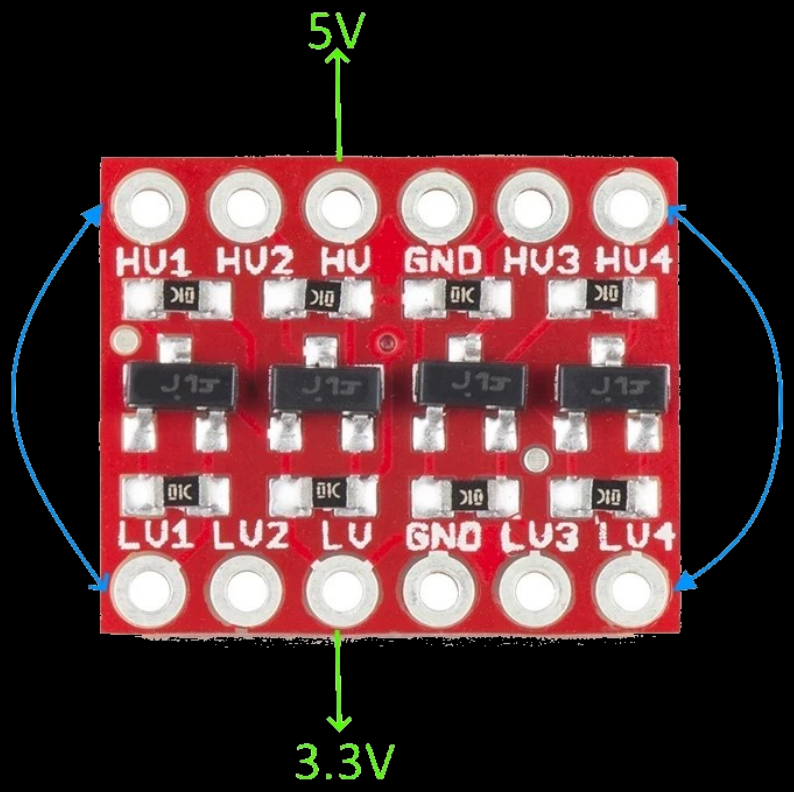


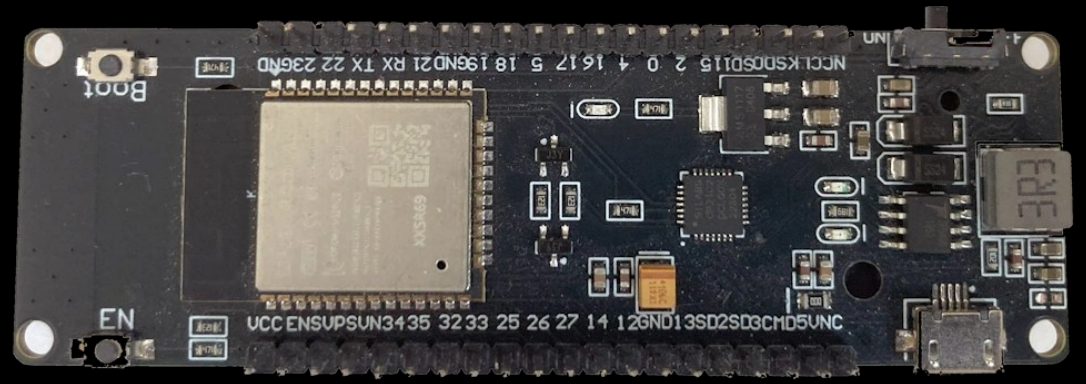


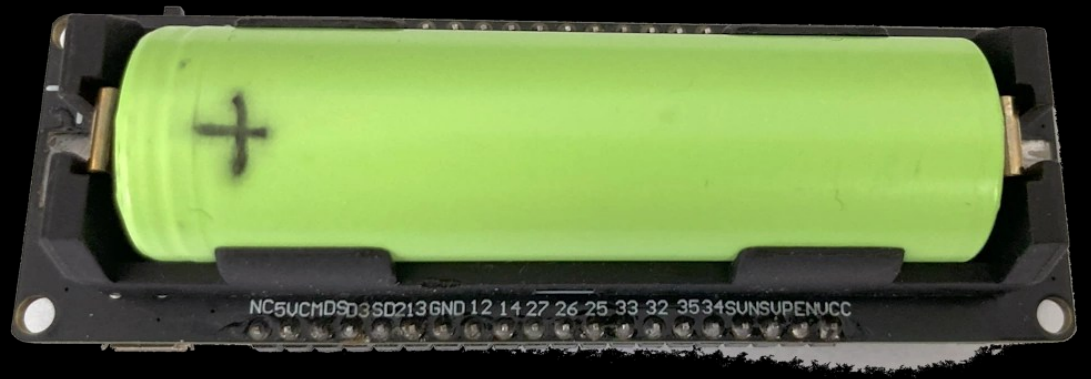
He was a 5V boy, She was a 3.3V girl!



https://store.arduino.cc/products/uno-r4-wifi







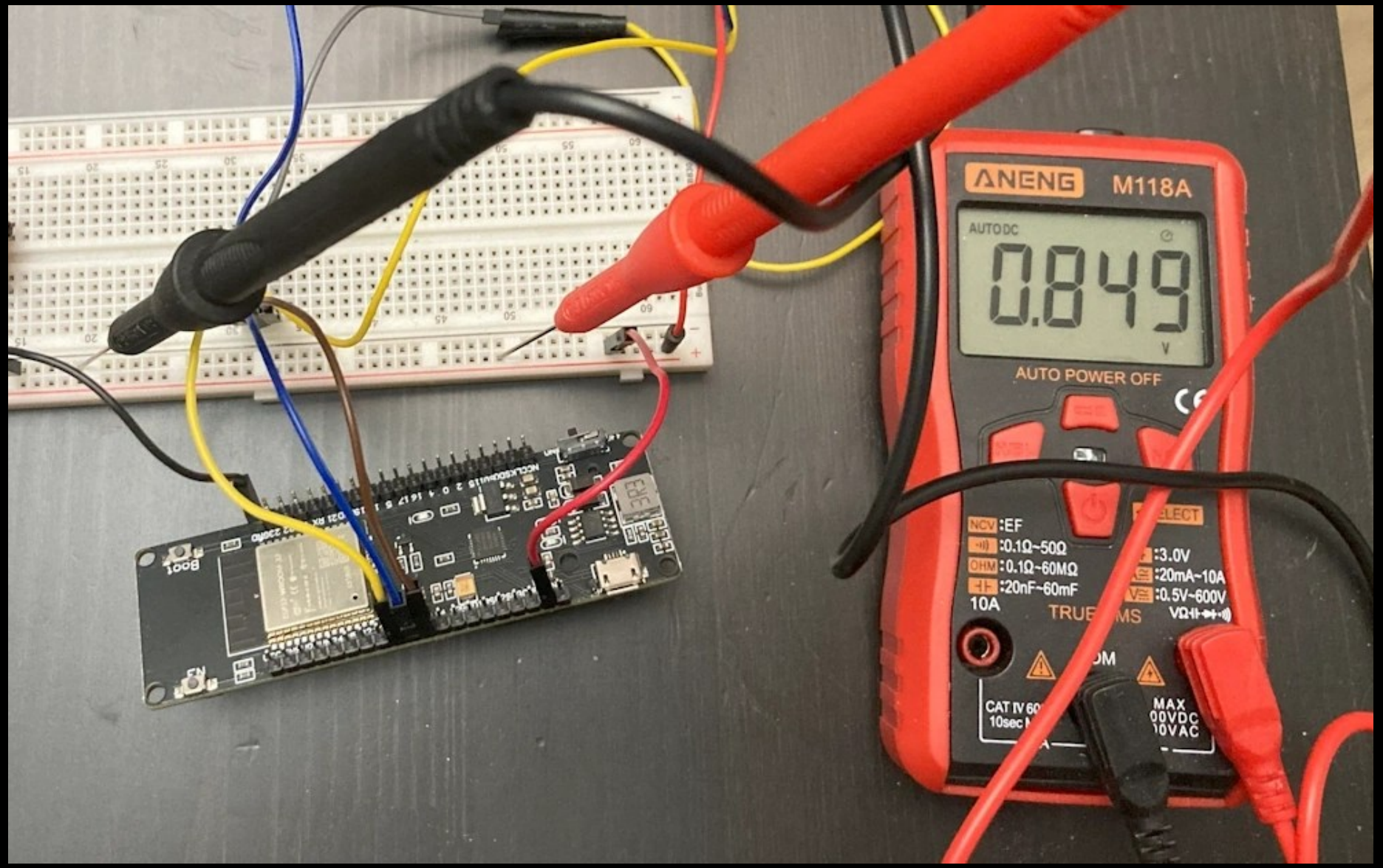
https://www.sparkfun.com/sparkfun-logic-level-converter-bi-directional.html

https://www.taydaelectronics.com/wifi-and-bluetooth-battery-esp-wroom-32-with-18650-battery-socket.html

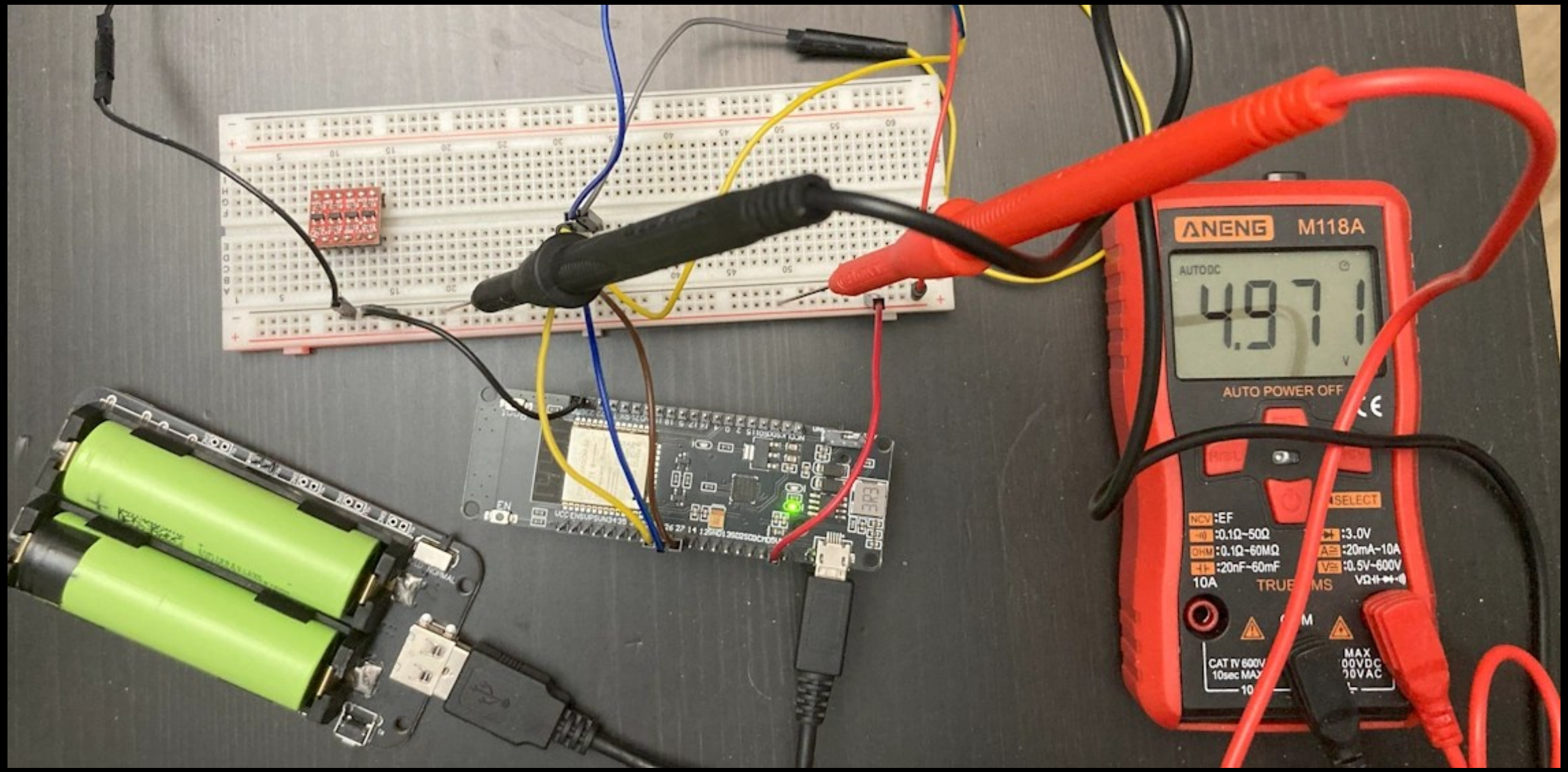
18650

- Over discharge --> battery dies!
- Over charge --> bad!
- TP4056

Festival of Failures!



5V 5V Whatcha Gonna Do?



Development Environment

- Arduino IDE
  - Better on Windows (for me)
  - Has ESP32 support
  - Didn’t put the board in download mode – hold boot
- ESP-IDF
  - Better on WSL (for me)
  - No hands downloading
- Unlicensed code samples from Espressif are a life saver (some Apache V2).
  - https://github.com/espressif/esp-idf/blob/master/examples/

Setup in WSL

- On Windows:
  - winget install usbipd
  - usbipd list
  - usbipd --bind --b 1-13 (admin cmd)
  - usbipd attach --wsl --busid 1-13
    - After restart
- In WSL:
  - sudo modprobe vhci_hcd

```
PS C:\Users\Parsia> usbipd list
Connected:
BUSID  VID:PID    DEVICE                                                        STATE
1-6    048d:c988  USB Input Device                                              Not shared
1-9    0639:7213  Billboard                                                     Not shared
1-11   30c9:00ac  Integrated Camera, APP Mode, Tobii Experience                 Not shared
1-13   10c4:ea60  Silicon Labs CP210x USB to UART Bridge (COM5)                  Not shared
1-14   8087:0033  Intel(R) Wireless Bluetooth(R)                                Not shared
7-1    1532:0037  USB Input Device                                              Not shared
7-3    17ef:30e1  Billboard Device, Vendor Interface                            Not shared
7-4    1038:2253  SteelSeries Arctis Nova 5X, USB Input Device, SteelSeries...  Not shared
8-4    046d:c338  G610, USB Input Device, Virtual HID Framework (VHF) HID d...  Not shared

Persisted:
GUID                                  DEVICE
813f5128-ed64-401c-b277-f5065f62d27c  USB-Enhanced-SERIAL CH9102 (COM5)
a67f9604-8456-405a-a4bf-6d782f4c0f55  USB Input Device, USB Serial Device (COM8)
d0328100-93a2-4036-ae85-2d6590c601a4  USB Serial Device (COM9), USB JTAG/serial debug unit

PS C:\Users\Parsia>
```

Read NES Controller

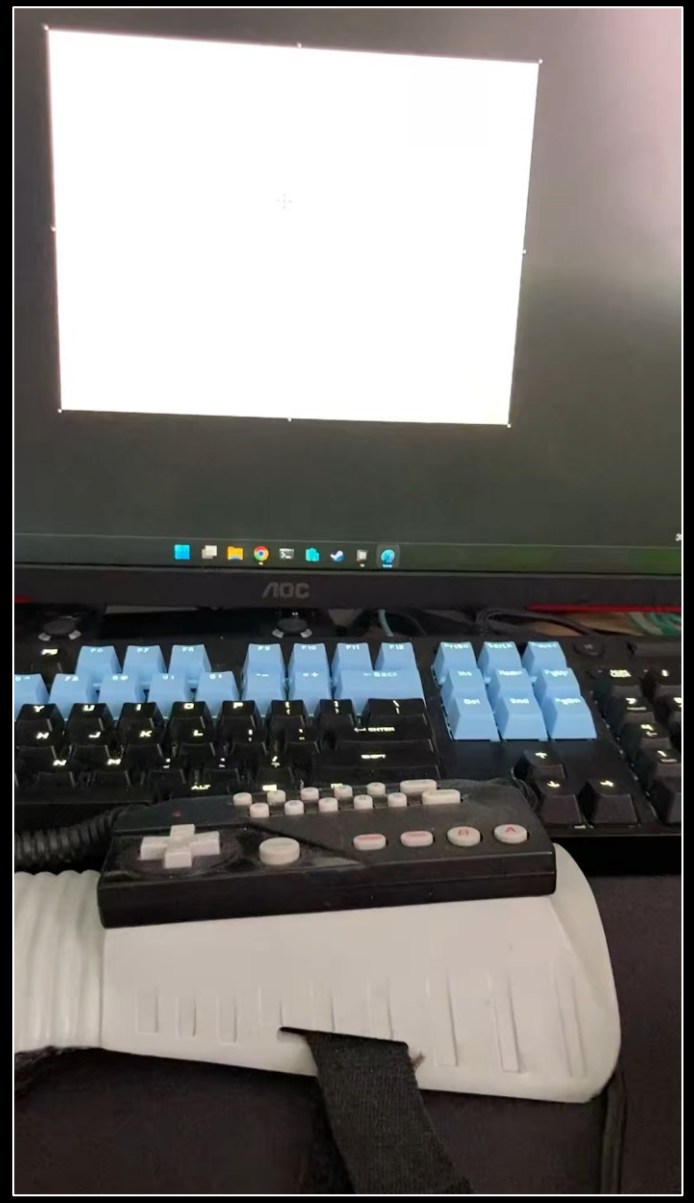
```
uint8_t readController() {
  uint8_t tempData = 255;  // Preload a variable with all 1s. This means nothing is pressed.

  digitalWrite(LATCH, LOW);
  digitalWrite(CLOCK, LOW);
  delayMicroseconds(12);

  digitalWrite(LATCH, HIGH); // Pulse the LATCH
  delayMicroseconds(12);

  // After latching, we can read the first bit (A_BUTTON).
  if (digitalRead(DATA) == LOW) bitClear(tempData, 0);

  digitalWrite(LATCH, LOW);
  delayMicroseconds(6);
  // We have to read 7 more bits. So PULSE the clock and read the bits.
  for (int i = 1; i < 8; i ++) {
    digitalWrite(CLOCK, HIGH);
    delayMicroseconds(6);
    if (digitalRead(DATA) == LOW) {
      bitClear(tempData, i);
    }
    digitalWrite(CLOCK, LOW);
    delayMicroseconds(6);
  }
  return tempData;
}
```

Bluetooth Mouse

```
uint8_t buttons = 0;
char dx = 0;
char dy = 0;

// Up
if (!(incomingData & BUTTON_UP)) dy = -1;
// Down
if (!(incomingData & BUTTON_DOWN)) dy = 1;
if (!(incomingData & BUTTON_LEFT)) dx = -1;
// Right
if (!(incomingData & BUTTON_RIGHT)) dx = 1;

// A was pressed. Left-click, set the first bit to 1.
if (!(incomingData & BUTTON_A)) buttons = 1;

// B was pressed. Right-click, set the 2nd bit to 1.
if (!(incomingData & BUTTON_B)) buttons = 2;

// Optional: Do stuff with `Start` and `Select`.
// if (!(incomingData & BUTTON_SELECT)) actionC(); // Select
    // if (!(incomingData & BUTTON_START)) actionD(); // Start

// 4th item is wheel which is zero here.
send_mouse(buttons, dx*STEP, dy*STEP, 0);
```

esp-idf/esp_hid_device example

World’s Clunkiest Etch A Sketch



Keyboard Report #1

```
// Check if lower or upper case
if(ch >= 'a' && ch <= 'z')
{
    buffer[0] = 0;
    // convert ch to HID letter, starting at a = 4
    buffer[2] = (uint8_t)(4 + (ch - 'a'));
}
else if(ch >= 'A' && ch <= 'Z')
{
    // Add left shift
    buffer[0] = USB_HID_MODIFIER_LEFT_SHIFT;
    // convert ch to lower case
    ch = ch - ('A'-'a');
    // convert ch to HID letter, starting at a = 4
    buffer[2] = (uint8_t)(4 + (ch - 'a'));
}
```

Bluetooth Keyboard Mappings

```
ButtonMapping arrowMappings[] = {
  {BUTTON_RIGHT, KEY_RIGHT_ARROW},
  {BUTTON_LEFT,  KEY_LEFT_ARROW},
  {BUTTON_UP,    KEY_UP_ARROW},
  {BUTTON_DOWN,  KEY_DOWN_ARROW},
};

MediaButtonMapping mediaMappings[] = {
  // KEY_MEDIA_WWW_SEARCH
  {BUTTON_A, {0, 8}},
  // KEY_MEDIA_LOCAL_MACHINE_BROWSER
  // My computer on Windows
  {BUTTON_B, {0, 1}},
  // KEY_MEDIA_CALCULATOR
  {BUTTON_SELECT, {0, 2}},
  // KEY_MEDIA_WWW_BOOKMARKS
  // Doesn't work on Windows :(
  {BUTTON_START, {0, 4}},
};
```

The Loop

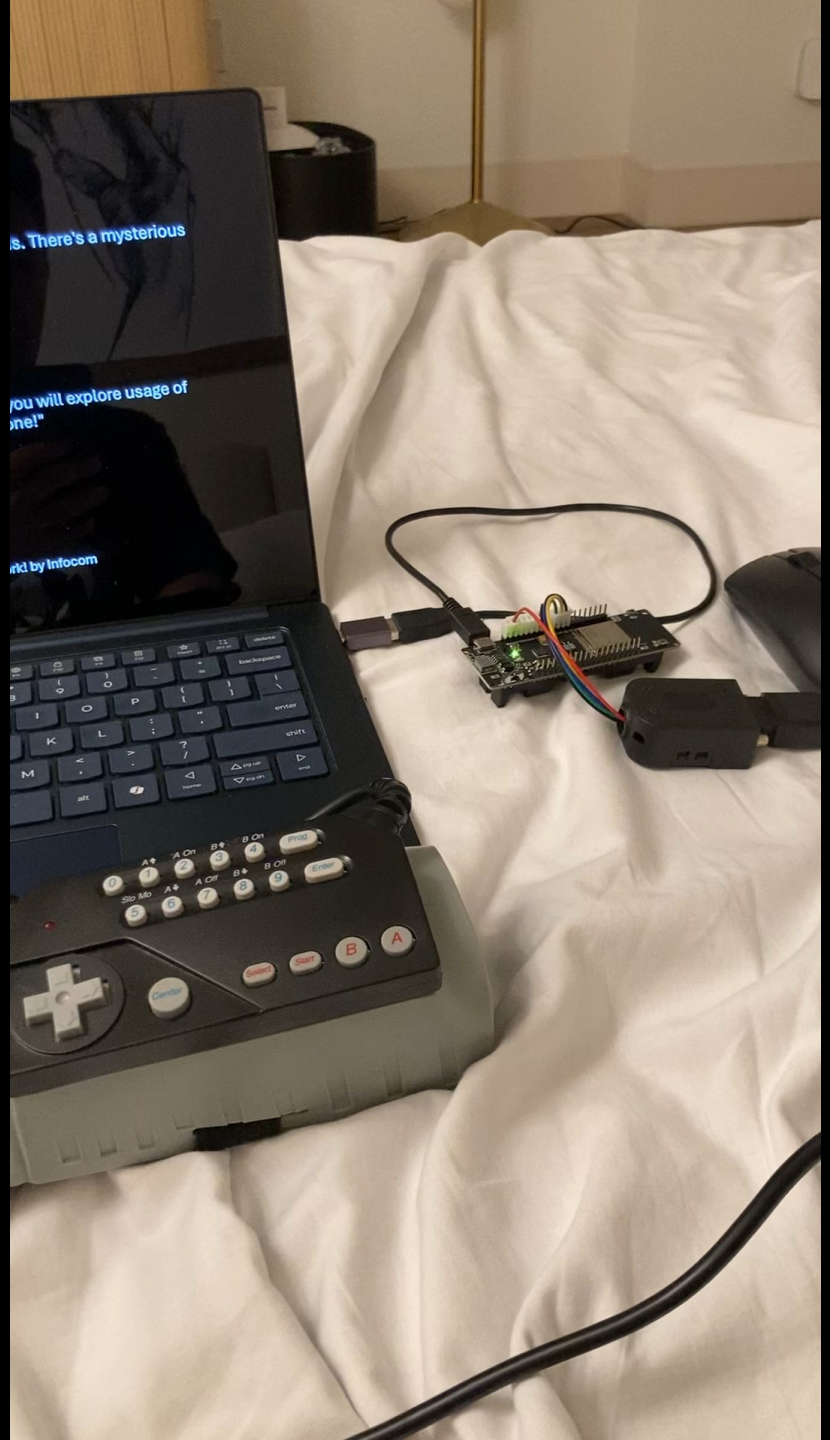
```
void loop() {

  if(bleKeyboard.isConnected()) {

    uint8_t incomingData = readController();

    if ((incomingData == 0x00) || (incomingData == 0xFF) ) {
      delay(DELAY);
      return;
    }

    for (int i = 0; i < sizeof(arrowMappings) / sizeof(arrowMappings[0]); i++) {
      if (!(incomingData & arrowMappings[i].buttonMask)) {
        bleKeyboard.write(arrowMappings[i].keyboardEvent);
      }
    }

    for (int i = 0; i < sizeof(mediaMappings) / sizeof(mediaMappings[0]); i++) {
      if (!(incomingData & mediaMappings[i].buttonMask)) {
        bleKeyboard.write(mediaMappings[i].keyboardEvent);
      }
    }
    // Avoid multiple actions with one press.
    delay(300);
  }
}
```

Library used: https://github.com/TriDEntApollO/ESP32-BLE-Keyboard-V2

Demo?


POWER GLOVE
I am
the demo
OK, fine!
Source: 'School of Athens' by Raffaello Sanzio (1483-1520)

Demo!


s. There's a mysterious
you will explore usage of
one!"
rkl by Infocom

I Better See Some Weird Presentation Props Next Year

- Code: https://github.com/parsiya/PowerPointGlove
- Slides: https://github.com/parsiya/presentations
- Suggestions/feedback/jokes (after Aug 15th please):
  - https://parsiya.net
  - https://twitter.com/CryptoGangsta
  - “parsiya” in pretty much every place.