



\$5 Cyberweapons & how to use them

Introduction to Offensive Hacking with Microcontrollers

Introduction

- I'm Kody Kinzie, Security researcher at Varonis
- I host hacking shows on YouTube
- Live in the Treasure State, AKA Big Sky Country
- Null Byte, Hak5, SecurityFWD
- Livestream 2x per week on Hak5 and SecurityFwd
- Specialize in Wi-Fi hacking, OSINT, and microcontrollers



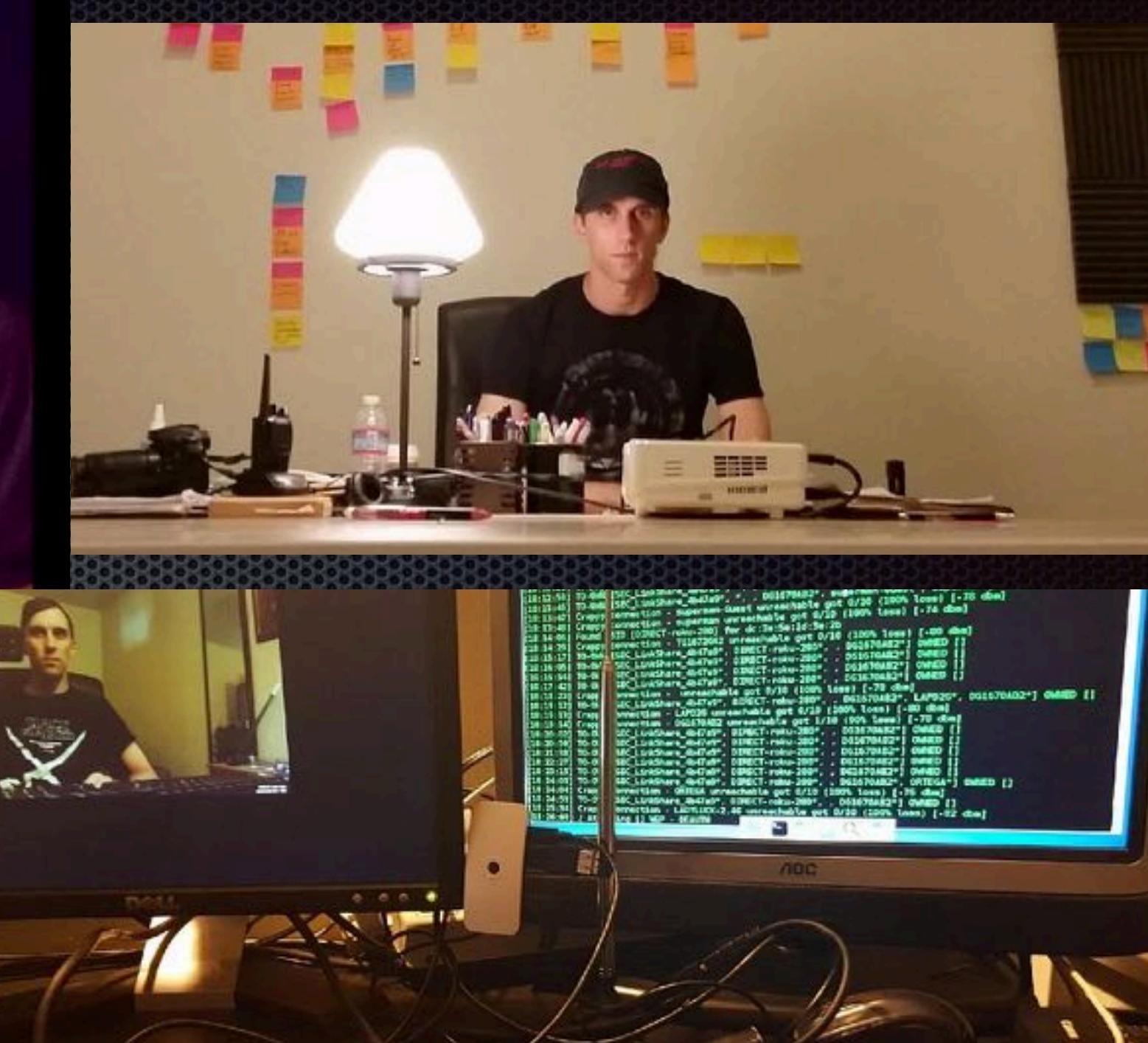
Introduction

- Outside of work, I like urban exploration, photography, & street art
- I've been mapping and documenting art in the LA storm drains since 2015



Path to here

- Started as a photographer
- Became a bouncer for The Echoplex in Los Angeles
- Worked at Korean a logistics tech startup
- Started making hacking tutorials & videos
- Went to Pasadena City College (AKA School of Worf) for programming & electrical engineering
- Started working as a security researcher & content creator at Varonis



Current Project

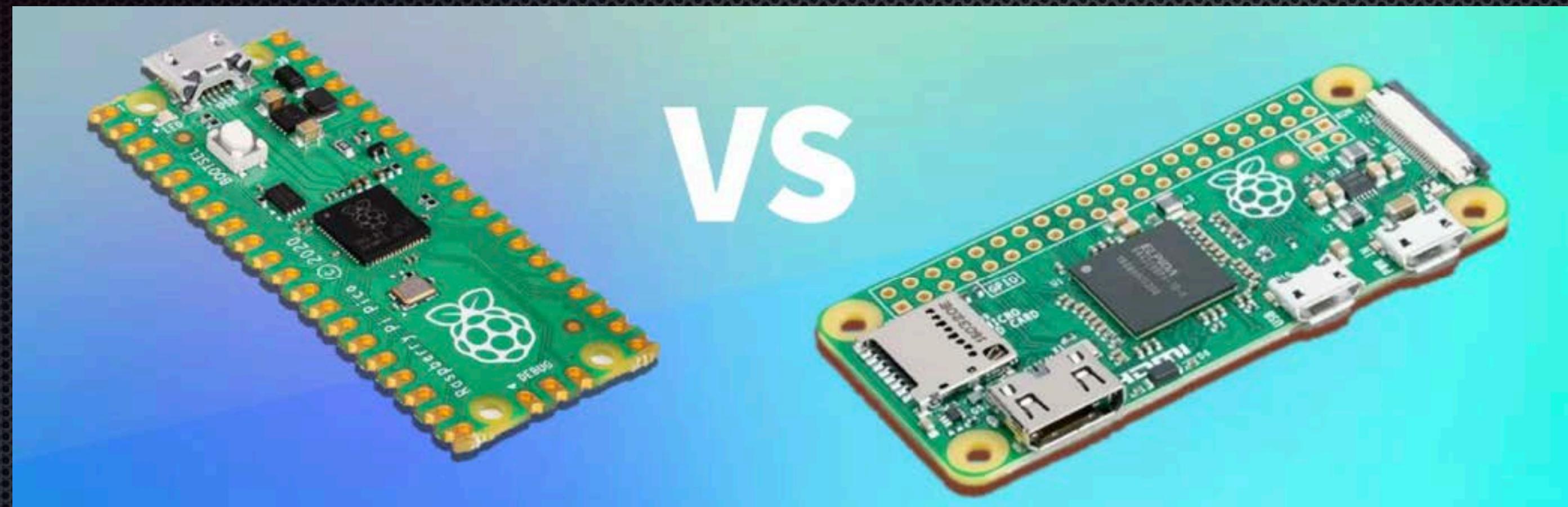
- Work with Alex Lynd on a cat-shaped USB attack tool
- Based on microcontrollers we're covering today
- If you want to support us, buy one at hakcat.com
- We work hard to make videos & docs to add value
- Prefer giving something cute & useful to Patreon
- Feel free to make your own (if you've got extra time & braincells)



Attacks We'll Cover Today

- Disconnect (deauthenticate) Wi-Fi
- Phishing Wi-Fi passwords
- Identifying networks stored in Wi-Fi devices
- Keystroke injection
- Mouse jigglers
- Wi-Fi handshake extraction
- aGPS spoofing
- Wi-Fi surveillance / presence detection
- Wi-Fi wardriving / warflying
- Wi-Fi routing
- Network honeypots
- And more!

Raspberry Pi Pico vs Pi Zero

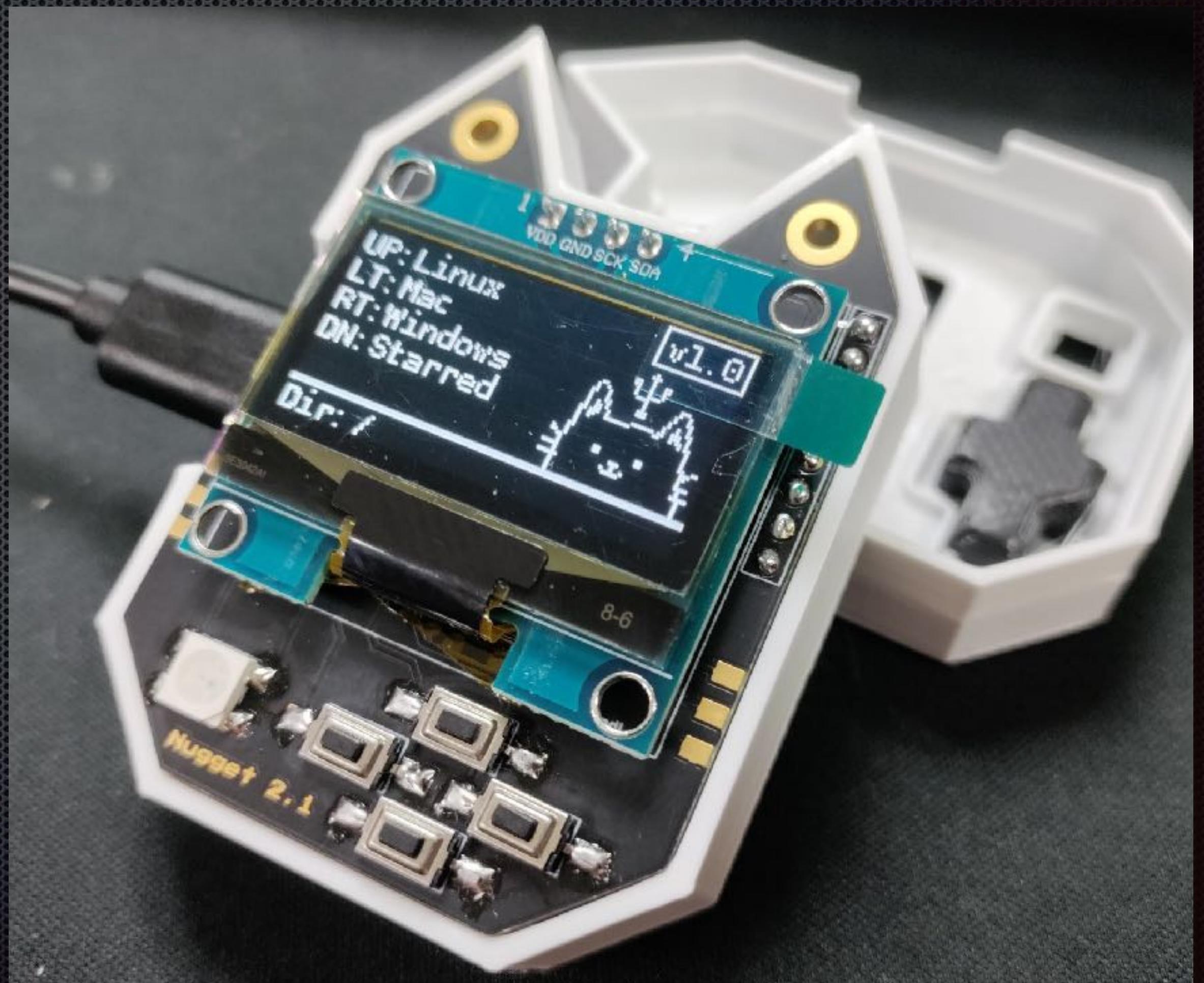


Source: @AshPuckettB2B howchoo.com

- Microcontroller
- For simple tasks and hardware control
- Programmed with CircuitPython / Arduino
- Includes 1 USB port & 20 GPIO pins
- Costs \$4
- Single-board computer (SBC)
- For running a Linux desktop environment
- Runs Raspberry Pi OS & more
- Includes HDMI, USB, & microSD card
- Costs \$200 (on Ebay)

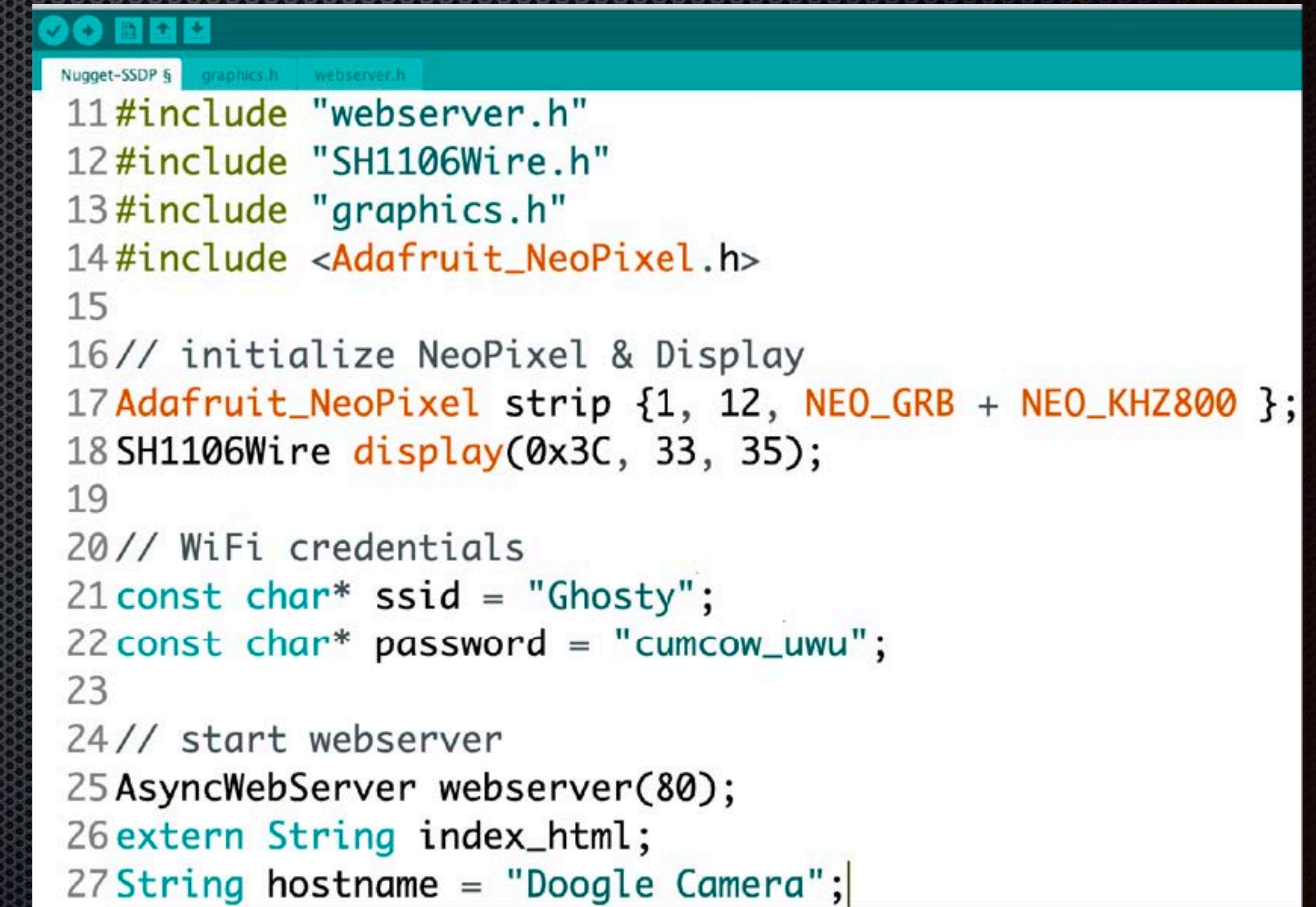
Skills required for hacking

- Flashing community projects via a web browser
- Installing Arduino IDE
- Adding boards to Arduino IDE
- Compiling & flashing source code
- Flashing CircuitPython via web browser



Skills required for Developing

- Experience in C++, Arduino, or Python
- Python command line utilities
- Mu editor, Arduino IDE
- Basic knowledge of serial ports and running Python programs
- Good research skills

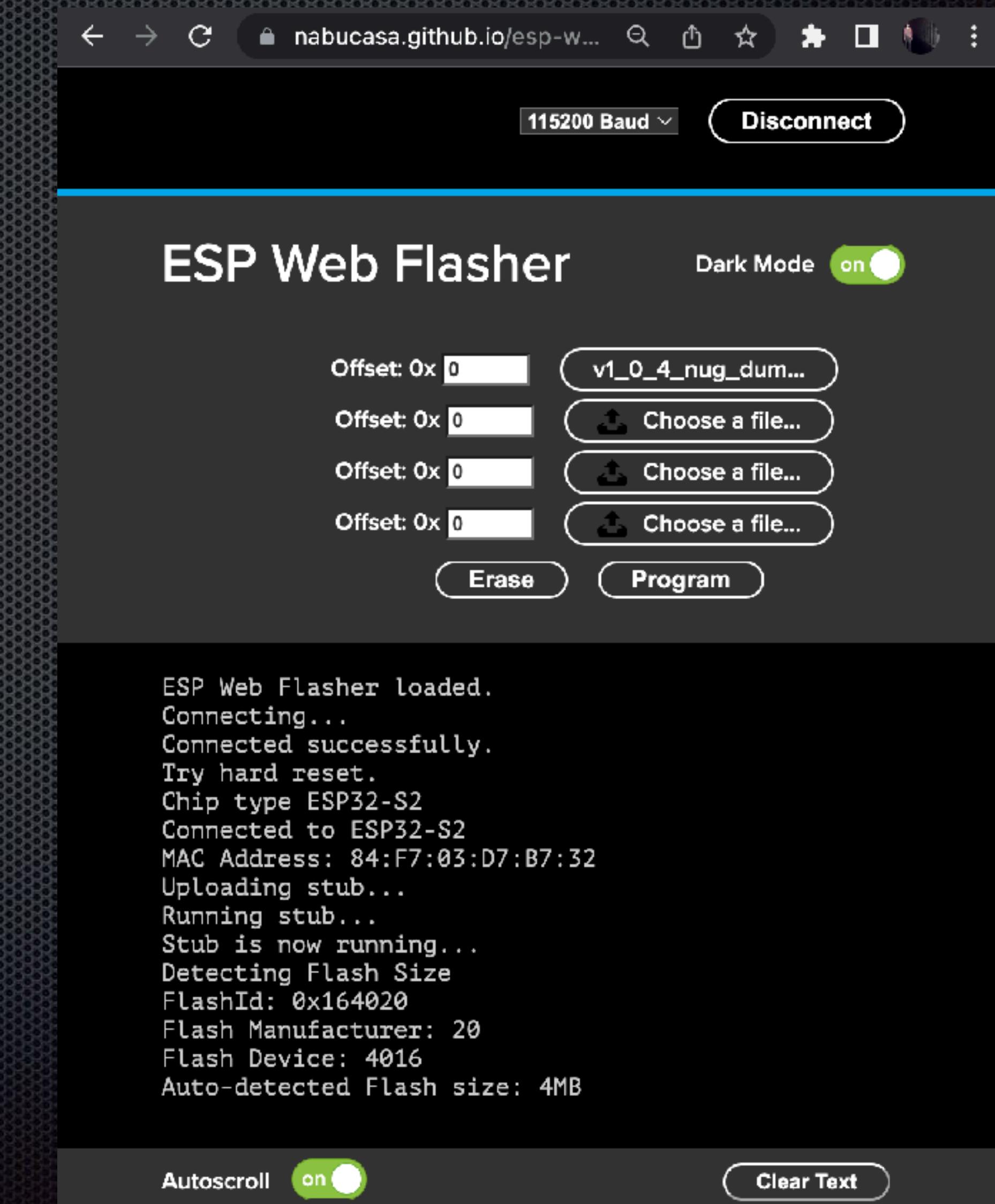


The screenshot shows a code editor window with a teal header bar. The tabs at the top are labeled "Nugget-SSDP", "graphics.h", and "webserver.h". The main text area contains the following C++ code:

```
11#include "webserver.h"
12#include "SH1106Wire.h"
13#include "graphics.h"
14#include <Adafruit_NeoPixel.h>
15
16// initialize NeoPixel & Display
17Adafruit_NeoPixel strip {1, 12, NEO_GRB + NEO_KHZ800 };
18SH1106Wire display(0x3C, 33, 35);
19
20// WiFi credentials
21const char* ssid = "Ghosty";
22const char* password = "cumcow_uwu";
23
24// start webserver
25AsyncWebServer webserver(80);
26extern String index_html;
27String hostname = "Doogle Camera";|
```

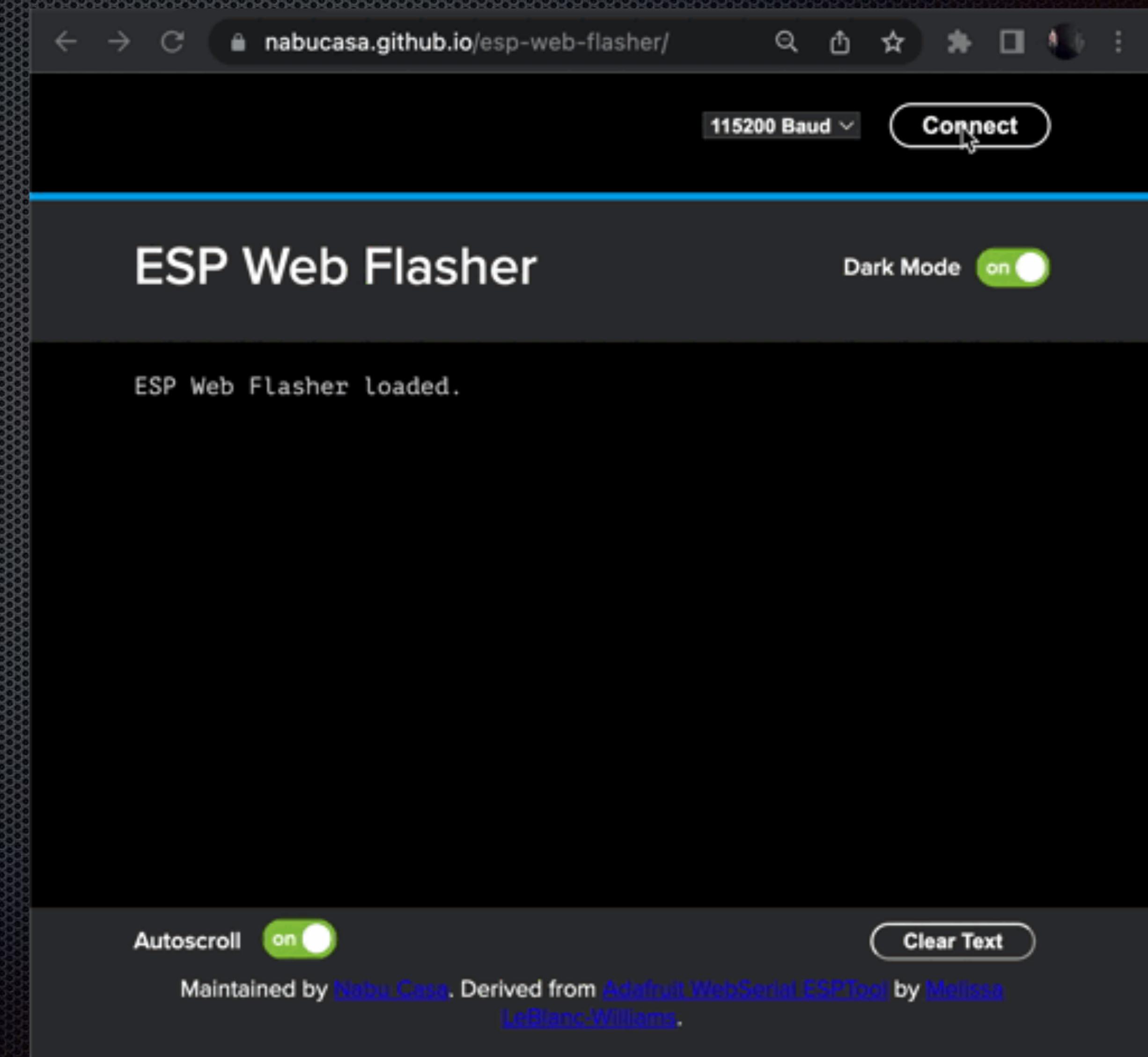
3 ways to program a microcontroller

- Flash a binary file via browser
- Flash CircuitPython, write Python code
- Program in Arduino IDE, flash the compiled binary file



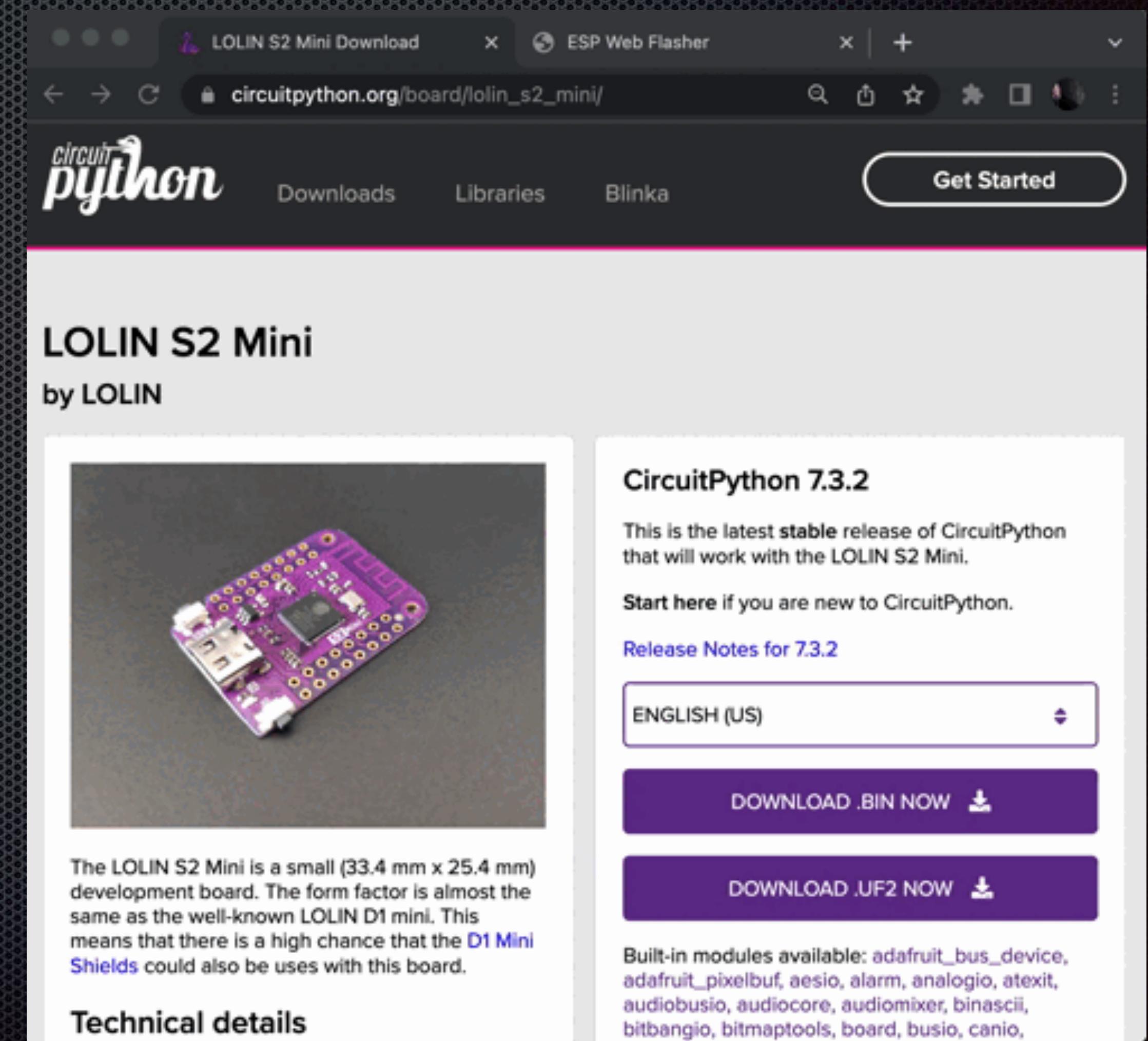
Flashing a Project via Chrome

- Download a .BIN file to flash
- Hold the programming button & plug in your device
- Select your device in the browser & click erase
- Select your .BIN file & click flash when erasing is complete



Flashing CircuitPython & Programming

- Download the CircuitPython binary
- Connect to your board via browser
- Erase the flash memory
- Flash the CircuitPython binary
- The device appears as a USB drive, complete with a code.py file!



Programming & Flashing via Arduino

- Add device URL to the board manager
- Install the board in the board manager
- Plug in your device & select serial port
- Write your code & hit compile
- Reset your board to run code

The screenshot shows the Arduino IDE interface. The code editor window displays the following sketch:

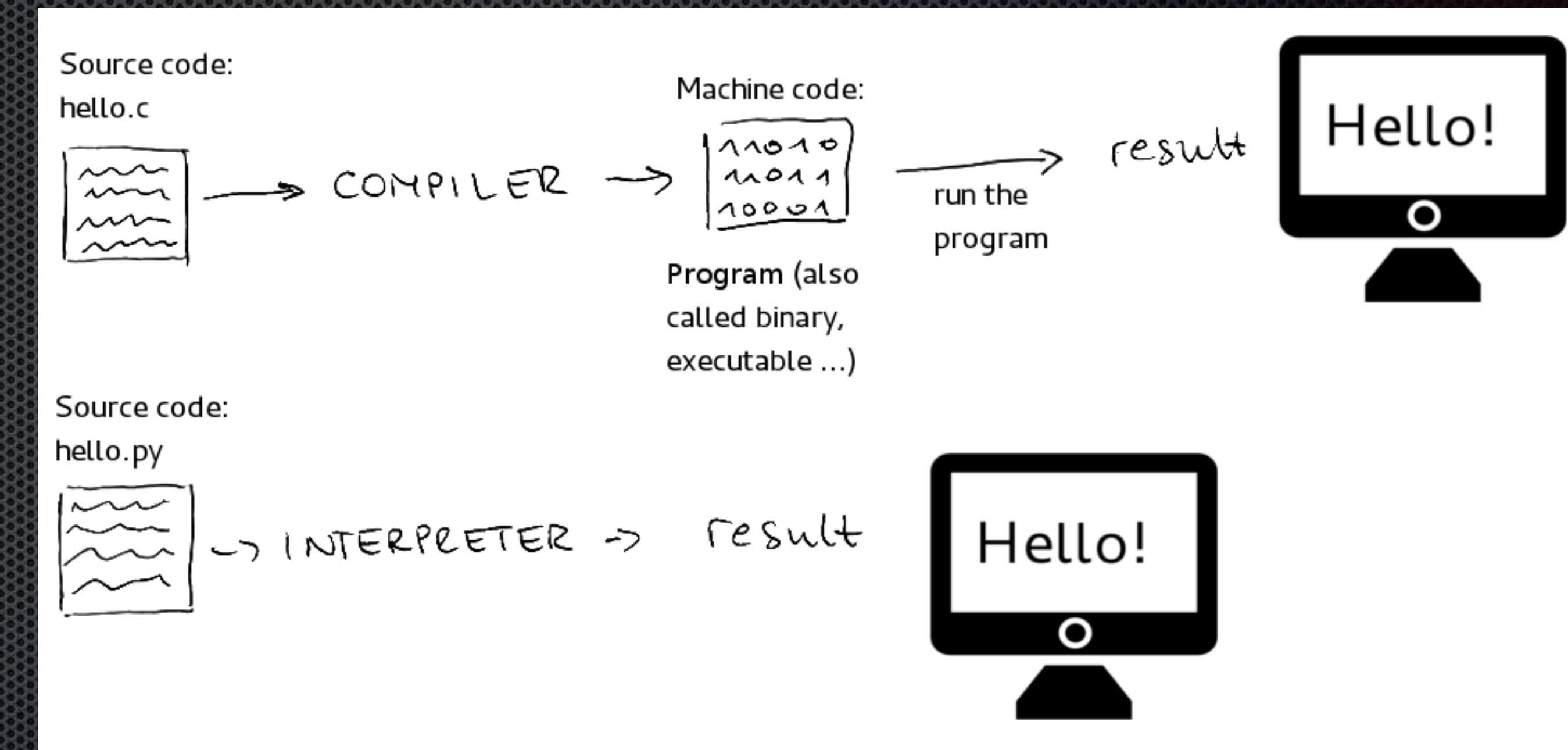
```
11#include "webserver.h"
12#include "SH1106Wire.h"
13#include "graphics.h"
14#include <Adafruit_NeoPixel.h>
15
16// initialize NeoPixel & Display
17Adafruit_NeoPixel strip {1, 12, NEO_GRB + NEO_KHZ800 };
18SH1106Wire display(0x3C, 33, 35);
19
20// WiFi credentials
21const char* ssid = "NewHope-Secure";
22const char* password = "hope2022";
23
```

An error occurred while uploading the sketch

```
Writing at 0x000b9380... (99 %)
Writing at 0x000b9fdd... (100 %)
Wrote 696800 bytes (444770 compressed) at 0x00010000 in 7.8 seconds
Hash of data verified.
Compressed 3072 bytes to 128...
Writing at 0x00008000... (100 %)
Wrote 3072 bytes (128 compressed) at 0x00008000 in 0.0 seconds
Hash of data verified.
```

Programming languages

- Virtually all of the microcontrollers we're talking about today can be programmed with Arduino IDE
- Many of them can be programmed with MicroPython
- Only those with USB support can be programmed with CircuitPython



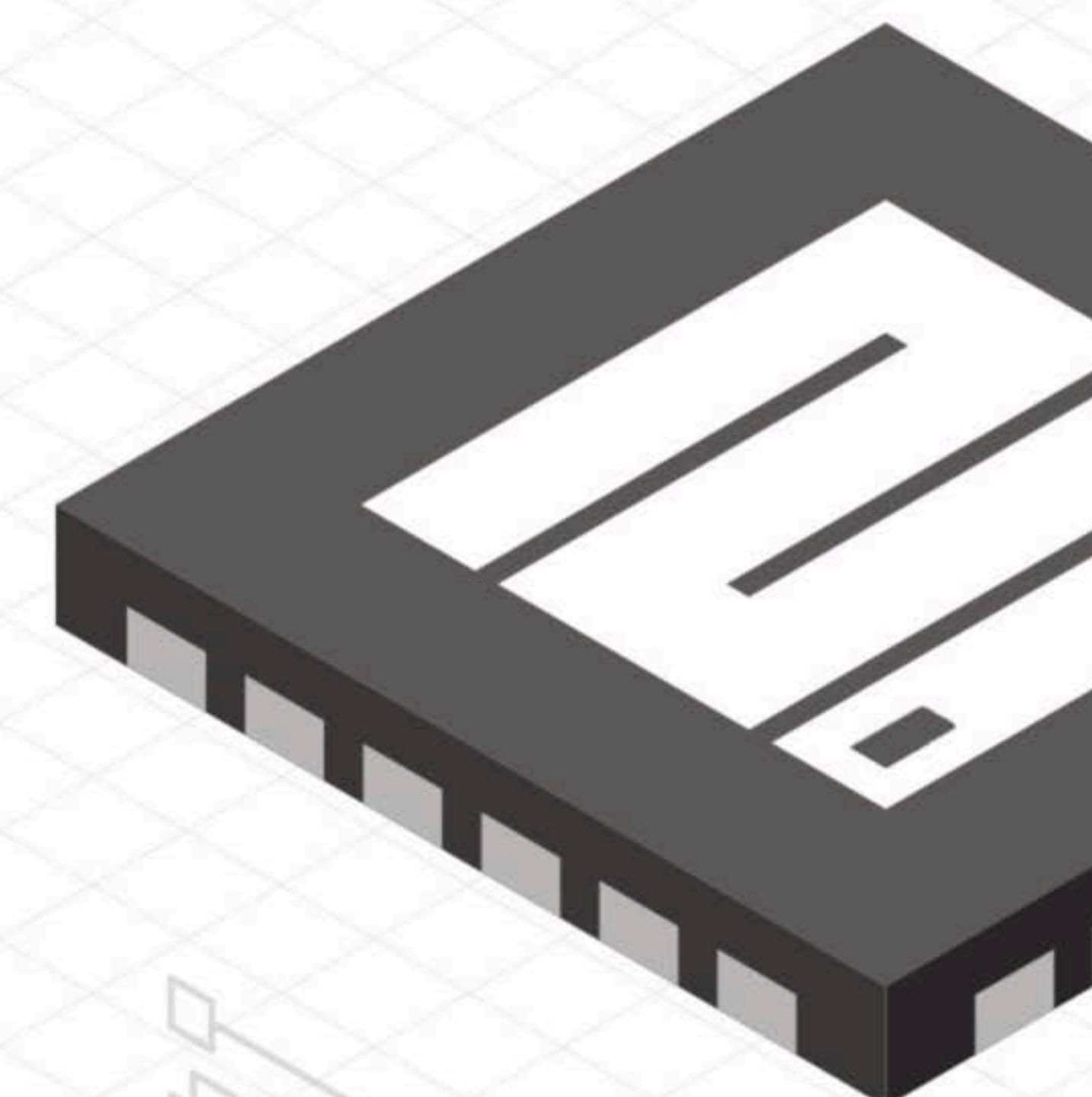
CircuitPython

- CircuitPython is an interpreted language supported by Adafruit
- It's beginner-friendly and based on Python
- CircuitPython devices support USB for drag and drop coding!
- Adding libraries is just as easy



MicroPython

- Community maintained Python implementation for Microcontrollers
- Works on microcontrollers that CircuitPy does not
- Doesn't support USB - get ready for adventures in serial connections!



MicroPython

MicroPython is a lean and efficient implementation of the [Python 3](#) programming language that includes a small subset of the Python standard library and is optimised to run on microcontrollers and in constrained environments.

The MicroPython [pyboard](#) is a compact electronic circuit board that runs MicroPython on the bare metal, giving you a low-level Python operating system that can be used to control all kinds of electronic projects.

MicroPython is packed full of advanced features such as an interactive prompt, arbitrary precision integers, closures, list comprehension, generators, exception handling and more. Yet it is compact enough to fit and run within just 256k of code space and 16k of RAM.

MicroPython aims to be as compatible with normal Python as possible to allow you to transfer code with ease from the desktop to a microcontroller or embedded system.

[TEST DRIVE A PYBOARD](#) [BUY A PYBOARD](#) [USE MICROPYTHON ONLINE](#)

Why CircuitPython over MicroPython

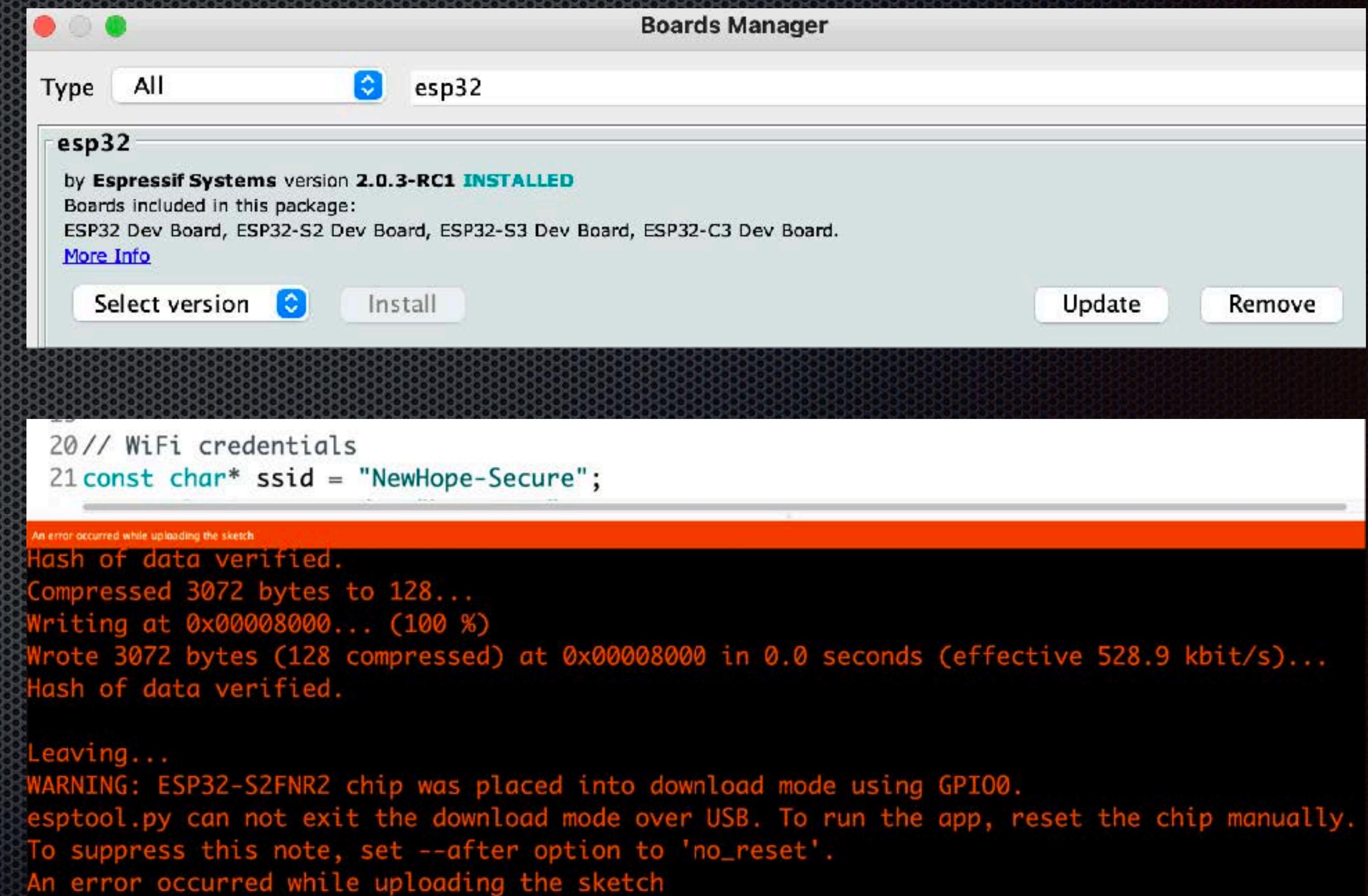
- USB Support
- WebSerial
- No command line needed
- Adafruit has great documentation

CircuitPython vs MicroPython



Arduino

- Compiled language based on C++
- Low level control of hardware
- More challenging to write & run
- Many hardware libraries available
- Compiler errors are discouraging



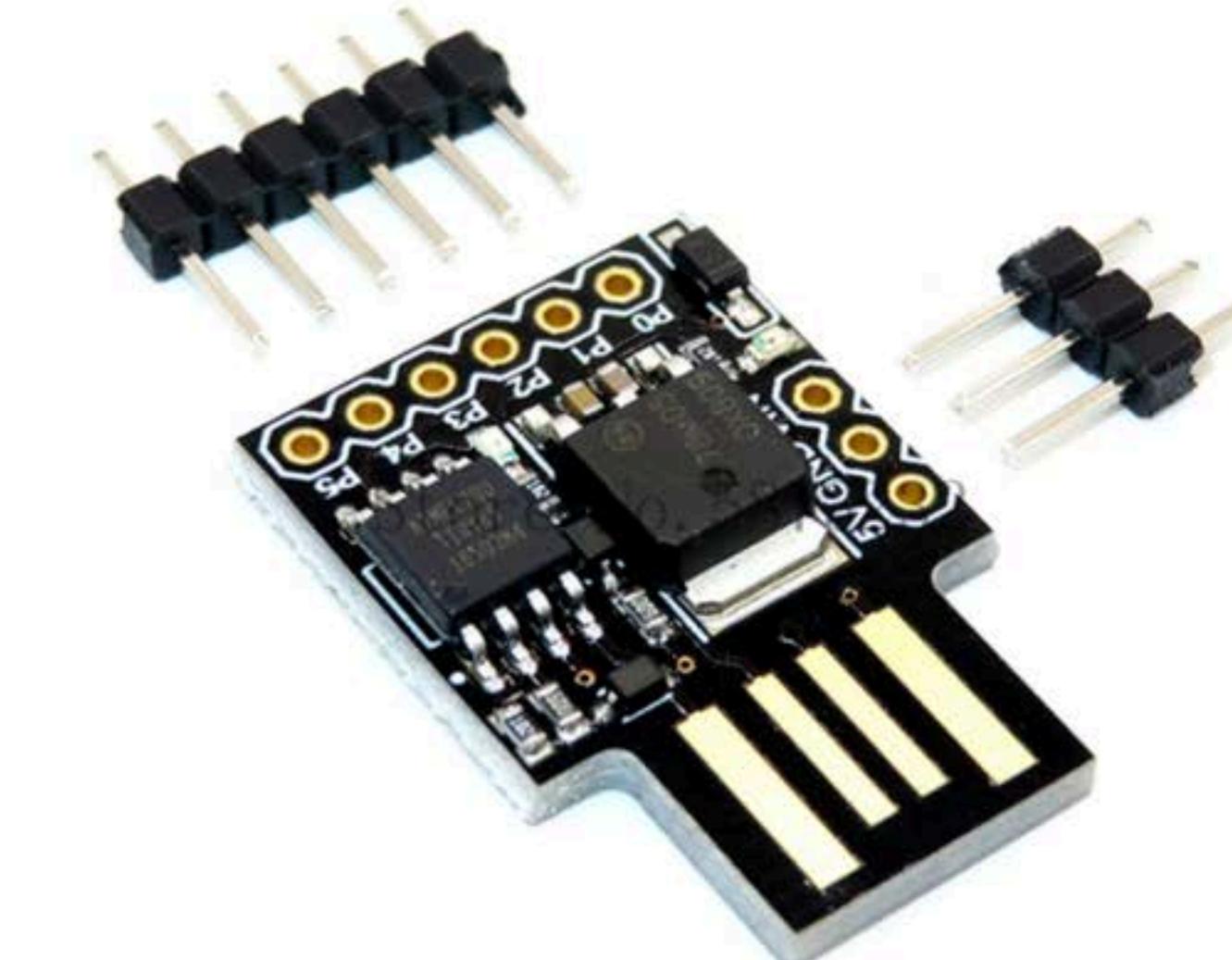
Price ranges

- Microcontrollers we'll cover today start at .80 cents up to \$5
- On the low end, the Attiny85 starts at .80 cents
- On the high end, the ATmega34u costs \$5.55

Attiny85

- Tiny, low power microcontroller
- Digispark module is the most useful form factor
- Can be bought alone for .80 cents
- Traces don't line up with all USB ports!

FDKJGEF®



ATTINY85

Digispark kickstarter development board ATTINY85 module for Arduino USB

★★★★★ 4.7 ▾ 26 Reviews 54 orders

US \$2.50

Color: ATTINY85



Quantity:

1 + 1% off (5 Pieces or more)
988 Pieces available

Ships to [United States](#)

Shipping: \$2.18

Estimated delivery on Sep 15
From China to United States via Cainiao Super Economy Global

[More opt](#)

Buy Now **Add to Cart**

 **75-Day Buyer Protection**
Money back guarantee



Attiny85 BadUSB

- Run a DuckyScript Payload!
- Flashes via Arduino IDE
- Very tricky to flash sometimes
- Only takes one payload
- Payloads must be converted to Arduino
- Hate these little shits

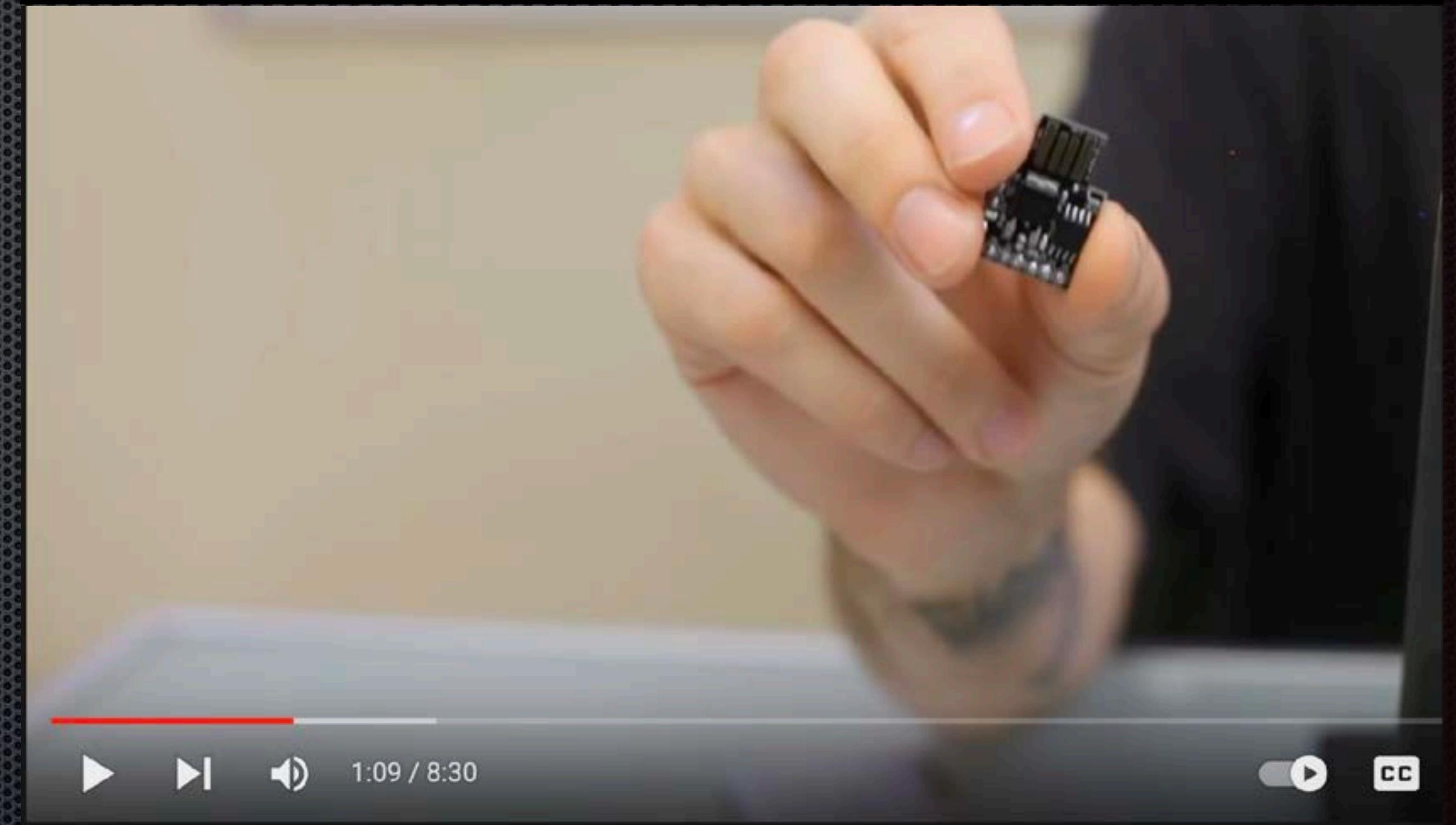
HOW TO

Run USB Rubber Ducky Scripts on a Super Inexpensive Digispark Board

BY KODY · ① 11/22/2019 4:43 PM · C 12/13/2019 1:28 PM · CYBER WEAPONS LAB · DIGISPARK · USB RUBBER DUCKY

The [USB Rubber Ducky](#) is a famous attack tool that looks like a USB flash drive but acts like a keyboard when plugged into any unlocked device. The Ducky Script language used to control it is simple and powerful, and it works with Arduino and can run on boards like the [ultra-cheap Digispark board](#).

<https://null-byte.wonderhowto.com/how-to/run-usb-rubber-dukey-scripts-super-inexpensive-digispark-board-0198484/>



Use USB Rubber Ducky Scripts & Payloads on an Inexpensive Digispark Board [Tutorial]

96,737 views · Nov 22, 2019

2.5K

DISLIKE

SHARE

<https://youtu.be/A3cB9BDE6XM>

Attiny85 Mouse Jiggler

- Moves the mouse to prevent computer from locking
- Flashes via Arduino IDE
- Can also click
- Makes a good auto-clicker
- Actually works pretty well

HOW TO

Create a USB Mouse Jiggler to Keep a Target Computer from Falling Asleep (& Prank Friends Too)

BY RETIA · 01/29/2021 5:06 PM · C 02/01/2021 11:50 AM · CYBER WEAPONS LAB · DIGISPARK

While obvious, it's a lot more difficult to hack into a locked computer than an unlocked computer. As a white-hat hacker, pentester, cybersecurity specialist, or someone working in digital forensics, there's an easy solution — make it so that the computer won't fall asleep and lock automatically in the first place.

<https://null-byte.wonderhowto.com/how-to/create-usb-mouse-jiggler-keep-target-computer-from-falling-asleep-prank-friends-too-0236798/>



Create Your Own Mouse Jiggler with a Digispark & Arduino [Tutorial]

25,799 views · Jan 29, 2021

786 DISLIKE SHARE CLIP SAVE

<https://youtu.be/x4Ap-ypWdFo>

Atmega32u4

- Faster than the ATTiny
- Similar capabilities but less frustrating to work with
- Must be pre-flashed with payloads
- Only works as USB device, doesn't mount as USB storage
- No wireless anything, we'll come back to this

FEIYANG

Pro Micro ATmega32U4 5V 16MHz Replace ATmega328 For arduino Pro Mini With 2 Row Pin Header For Leonardo Mini Usb Interface

★★★★★ 4.9 ⚡ 52 Reviews 286 orders

US \$4.96

US \$88.00 Off Store Coupon Get coupons

Quantity: 1 + 1% off (3 Pieces or more)
40174 Pieces available

Ships to United States

Shipping: \$2.63

From China to United States via AliExpress Standard Shipping
Estimated delivery on Aug 13

More options ▾

Buy Now Add to Cart

75-Day Buyer Protection Money back guarantee

Black/white mini Beetle Leonardo USB ATMEGA32U4 Mini development board

★★★★★ 5.0 ⚡ 5 Reviews 28 orders

US \$5.55

Color: white

M- M-

Quantity: 1 + 88812 Pieces available

Ships to United States

Shipping: \$3.11

From China to United States via AliExpress Standard Shipping
Estimated delivery on Aug 14

More options ▾

Buy Now Add to Cart

75-Day Buyer Protection Money back guarantee

Free Return
Return for any reason within 15 days

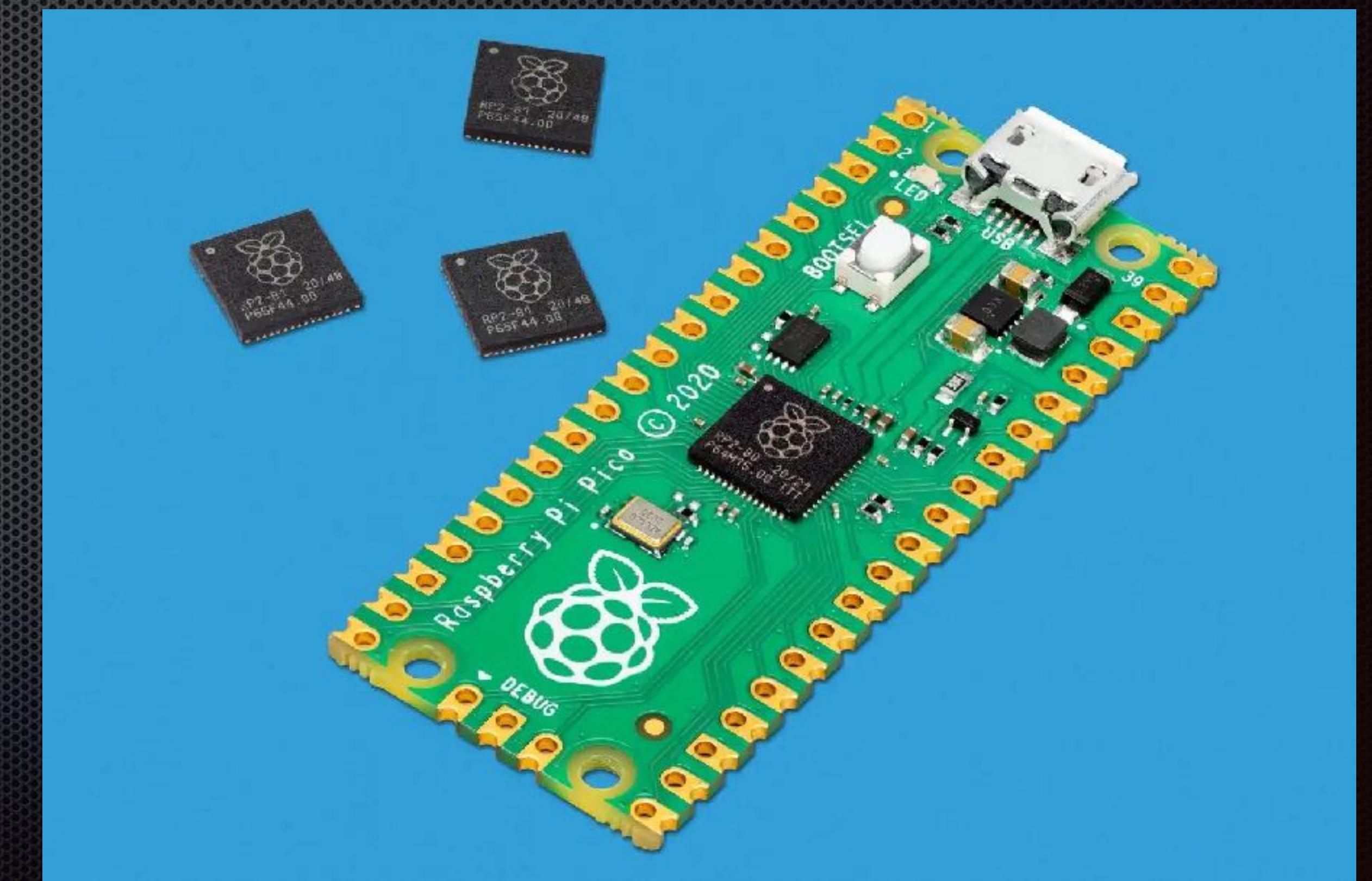
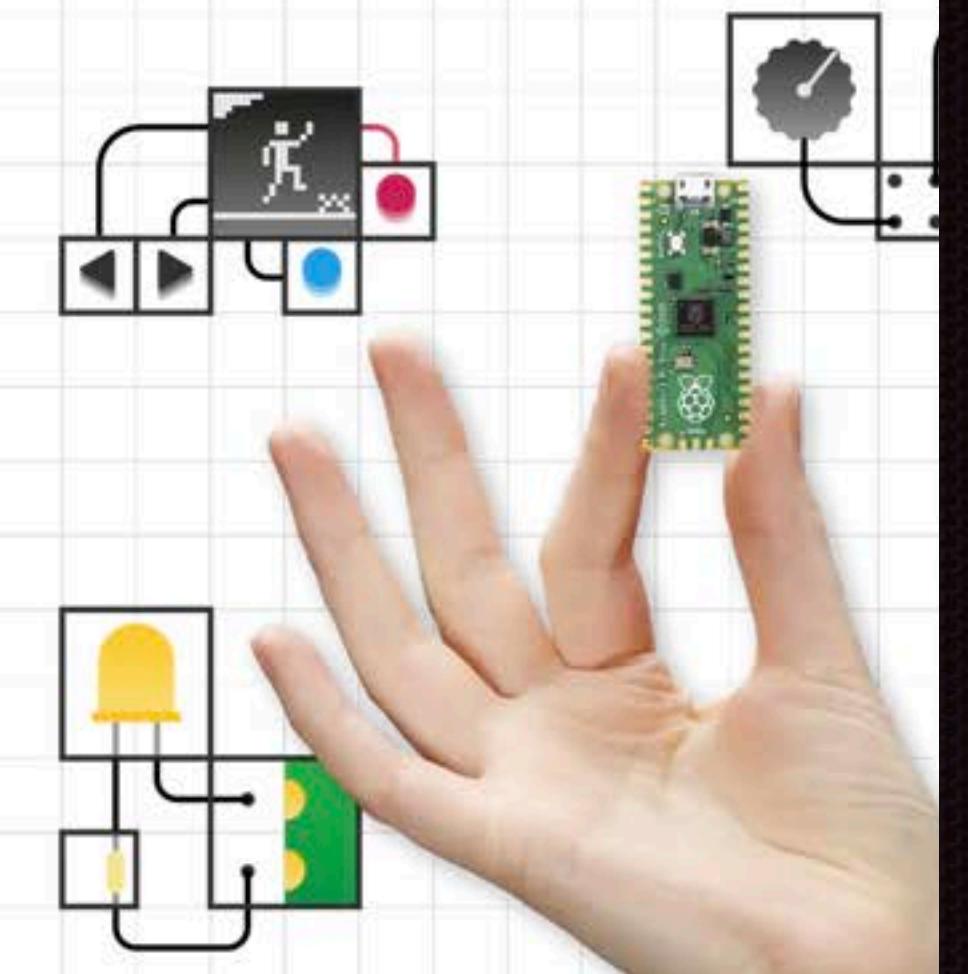
Raspberry Pi Pico

- Based on RP2040
- Native USB!
- Supports CircuitPython
- Supports Arduino IDE
- Mounts as USB drive
- No Wireless

Raspberry Pi Pico

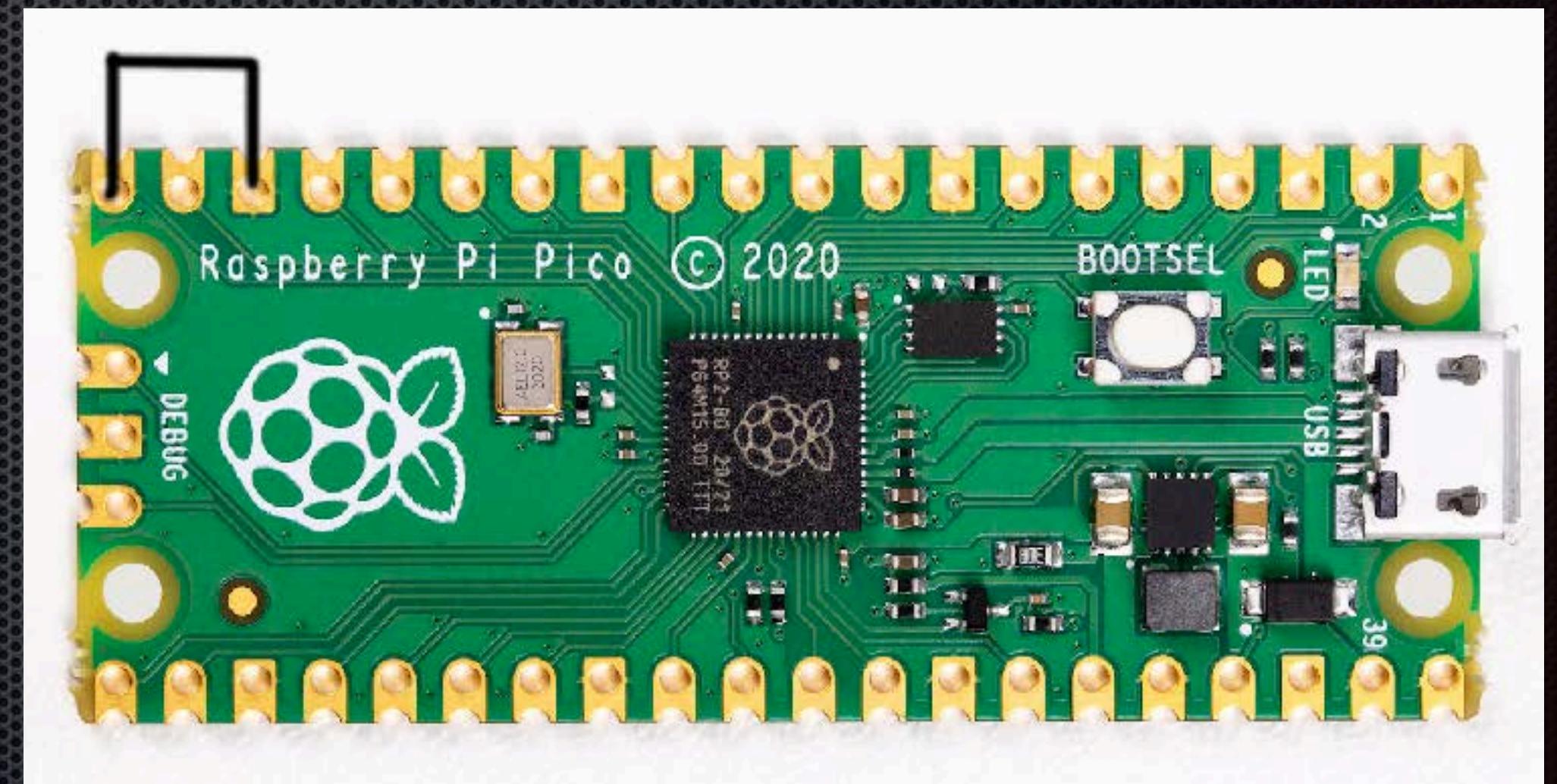
The powerful, flexible microcontroller board,
available from \$4

Raspberry Pi Pico is a tiny, fast, and versatile board
built using RP2040, the flagship microcontroller chip
designed by Raspberry Pi in the UK



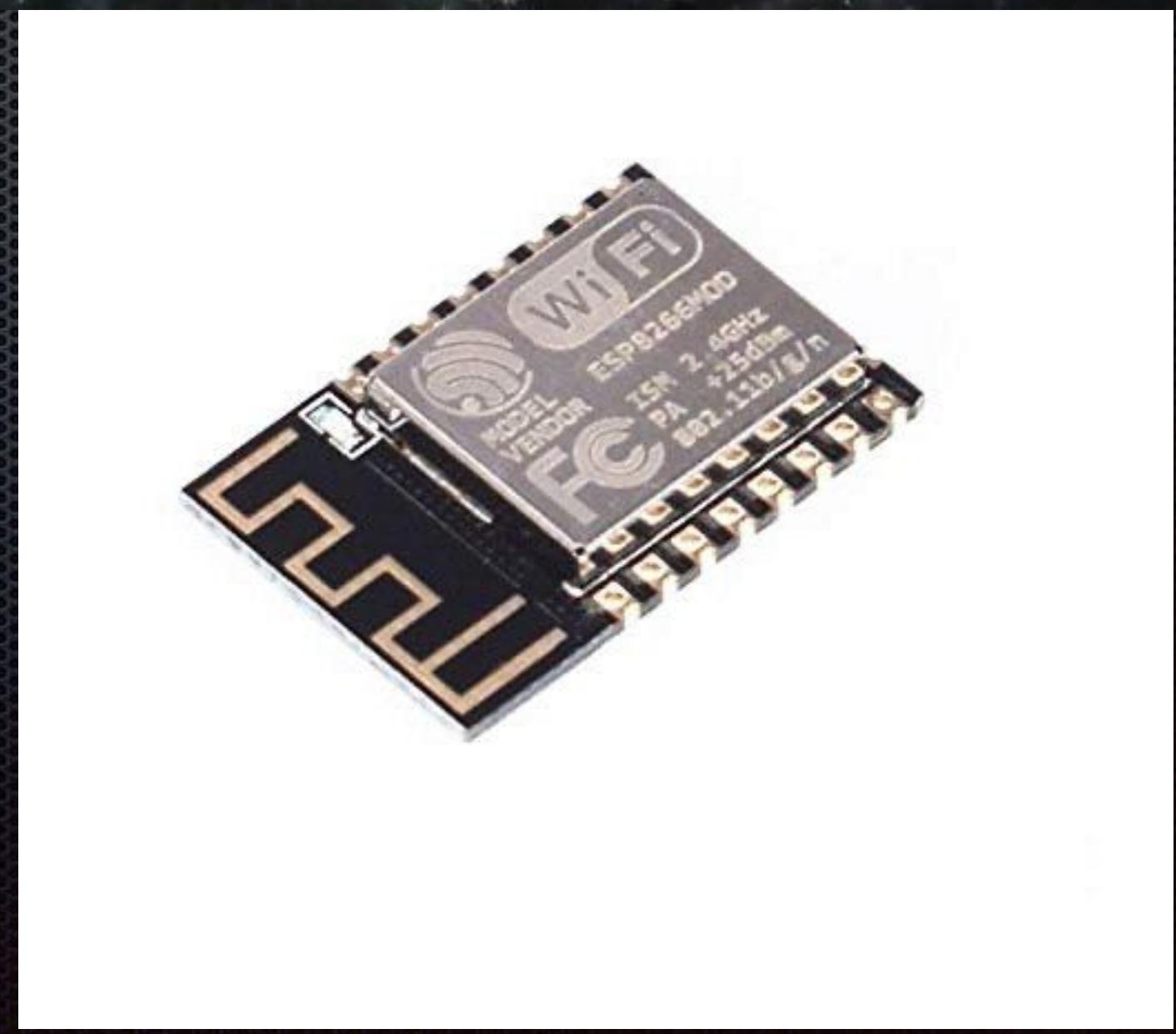
PicoDucky

- Awesome CircuitPython project to parse DuckyScript & deliver payloads
- Created by Dave Bailey
- Mounts as USB drive to drag & drop payloads
- Supports multiple keyboards
- No screen or buttons to interface with
- Requires you to jump connections to switch between program & attack mode



Esp8266

- Star of Wi-Fi hacking microcontrollers
- \$1.73 for ESP8266 modules
- Capable of Wi-Fi packet injection
- Can host web servers
- Modules have USB serial chips



Esp8266 Modules

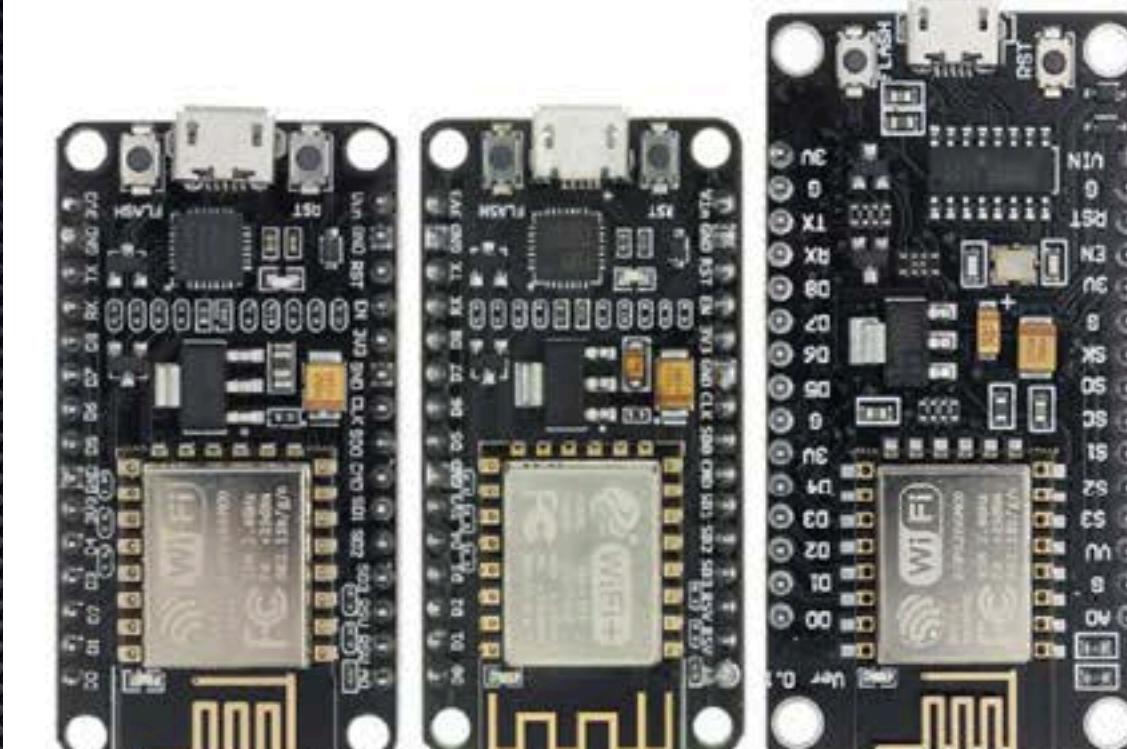
- The NodeMCU is a beefy module with 3 versions
- V3 is TERRIBLE
- D1 Mini has 3 versions
- All versions are okay
- “Pro” version allows for external antennas to be added

Wireless module CH340/CP2102 NodeMcu V3 V2 Lua WiFi Internet of Things development board based ESP8266 ESP-12E with pcb Antenna

★★★★★ 4.9 ✓ 546 Reviews 1394 orders

US \$2.85 US \$3.56 -20%

Color: NodeMcu V2 CP2102



Quantity:

- 1 + Additional 1% off (10 Pieces or more)
9134 Pieces available

Ships to United States

Shipping: \$1.75
Estimated delivery on Sep 15
From China to United States via Cainiao Super Economy Global

More options ▾

[Buy Now](#) [Add to Cart](#) [Heart 1680](#)

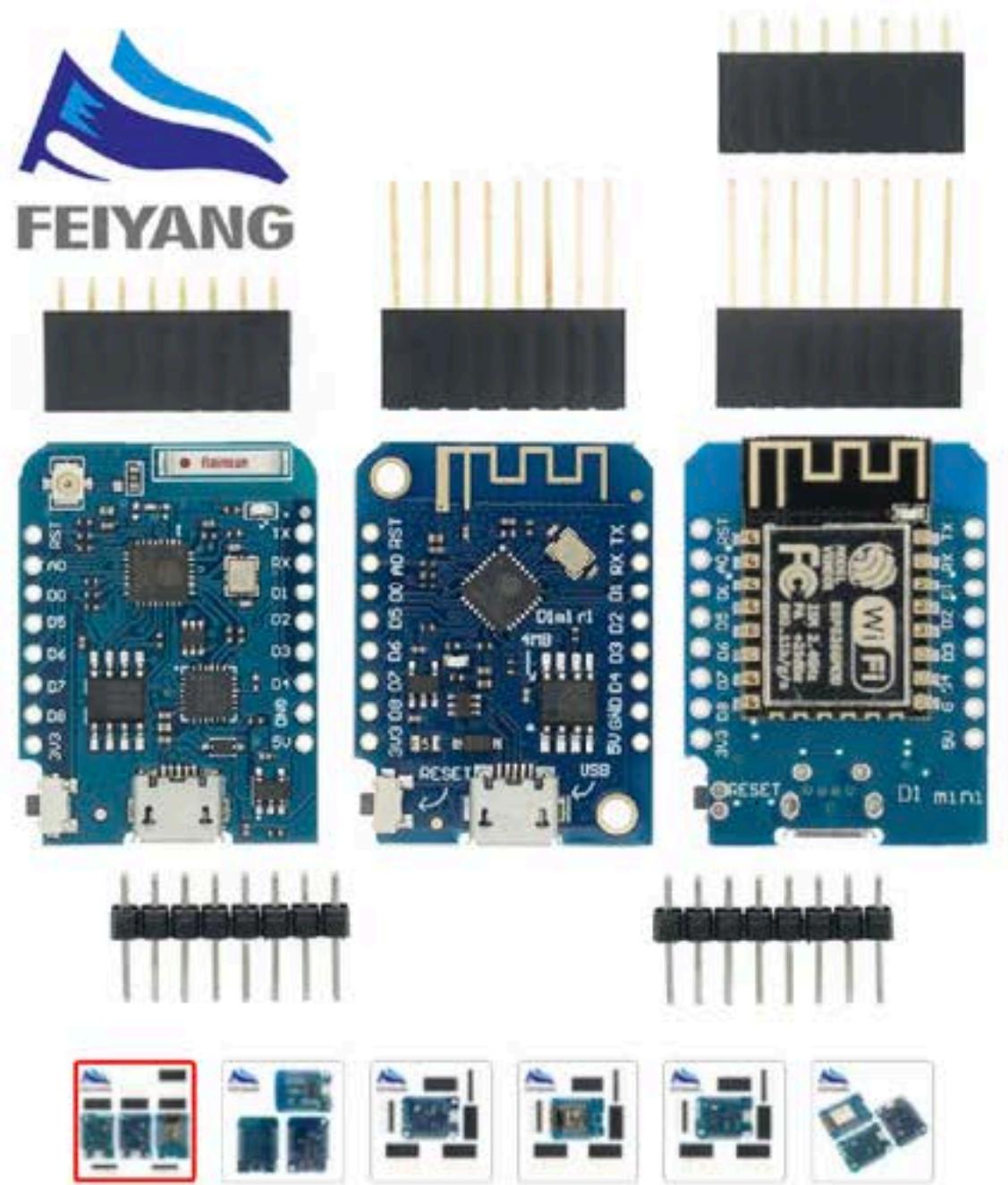
WeMos D1 Mini Pro V3.0 NodeMcu 4MB/16MB bytes Lua WiFi Internet of Things Development board based ESP8266 CH340G Nodemcu V2

★★★★★ 4.9 ✓ 1129 Reviews 3219 orders

US \$1.73

US \$88.00 Off Store Coupon [Get coupons](#)

Color: D1 MINI CH340



Quantity:

- 1 + 2% off (3 Pieces or more)
7359 Pieces available

Ships to United States

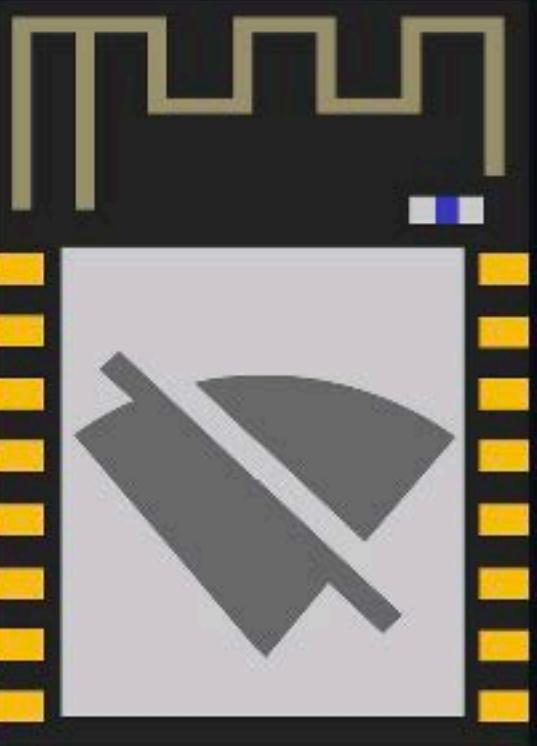
Shipping: \$2.53
From China to United States via AliExpress Standard Shipping
Estimated delivery on Aug 13

More options ▾

[Buy Now](#) [Add to Cart](#) [Heart 4865](#)

ESP8266 Deauther

- Runs on the ESP8266
- Flash via binary file or Arduino IDE
- Offers a web & serial interface
- Scan for Wi-Fi Access Points
- Scan for Wi-Fi Clients
- Jam Wi-Fi Clients (protocol based jammer)
- Create fake AP's (Trick clients into trying to join)
- Create fake probe frames (Wi-Fi Pineapple detector)



Scan for WiFi devices, block selected connections, create dozens of networks and confuse WiFi scanners!

<https://null-byte.wonderhowto.com/how-to/create-usb-mouse-jiggler-keep-target-computer-from-falling-asleep-prank-friends-too-0236798/>

Feature	Version 2	Version 3
Web Interface	✓	
Display support	✓	
Serial Command Line	✓	✓
Scanner	✓	✓
Deauth attack	✓	✓
Beacon attack	✓	✓
Probe attack	✓	✓
Huhnitor support		✓
Signal strength scanner		✓
Authentication scanner		✓
Rogue AP		✓

ESP8266 Deauther Web Interface

Access Points: 6

SSID	Name	Ch	RSSI	Enc	MAC	Vendor
0 Don't	-SpaceRouter!--	6	-57	WPA2	f4:6b:de:da:8d:95	Spacehuhn
1 call		1	-80	-	cc:cf:1e:d5:5b:2b	SpaceLtd
2 it		6	-81	WPA*	5c:37:3b:f7:67:be	SpaceBox
3 a		8	-82	WPA2	cd:ce:1e:0a:4e:9e	SpacEEE
4 jammer		8	-83	WPA2	c7:0e:14:95:a1:3b	Chicken!
5 Don't call it a Jammer! DON'T !!		8	-90	WPA2	c8:0e:14:95:a1:3b	Huhn

SELECT ALL **Deselect All**

Scan SSIDs Attacks Settings Info

SSIDs

SSID:
WPA2
Number:
Overwrite:

ADD **CLONE SELECTED APS**

INFO:
- This SSID list is used for the beacon and probe attack.
- Each SSID can be up to 32 characters.
- Don't forget to click save when you edited a SSID.
- You have to click Reload after cloning SSIDs.
In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

Time Interval: 10 s

ENABLE RANDOM MODE

- This SSID list is used for the beacon and probe attack.
- Each SSID can be up to 32 characters.
- Don't forget to click save when you edited a SSID.
- You have to click Reload after cloning SSIDs.
In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

Time Interval: 10 s

ENABLE RANDOM MODE

Enable the random mode to generate a random SSID list in a given interval.

0: test1231231231231231231231231	<input checked="" type="checkbox"/>	SAVE	<input type="button" value="X"/>
1: test1	<input type="checkbox"/>	SAVE	<input type="button" value="X"/>
2: test2	<input type="checkbox"/>	SAVE	<input type="button" value="X"/>
3: test3	<input checked="" type="checkbox"/>	SAVE	<input type="button" value="X"/>
4: test4	<input type="checkbox"/>	SAVE	<input type="button" value="X"/>

Scan SSIDs Attacks Settings Info

Attacks

INFO:
- You might lose connection when starting an attack!
- You need to select a target for the deauth attack.
- You need a saved SSID for the beacon and probe attack.
- Click reload to refresh the packet rate.
In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

1 **RELOAD**

Attacks	Targets	Pkts/s	START / STOP
Deauth	0	0/0	START
Beacon	0	0/0	START
Probe	0	0/0	START

ESP8266 Deauther V3

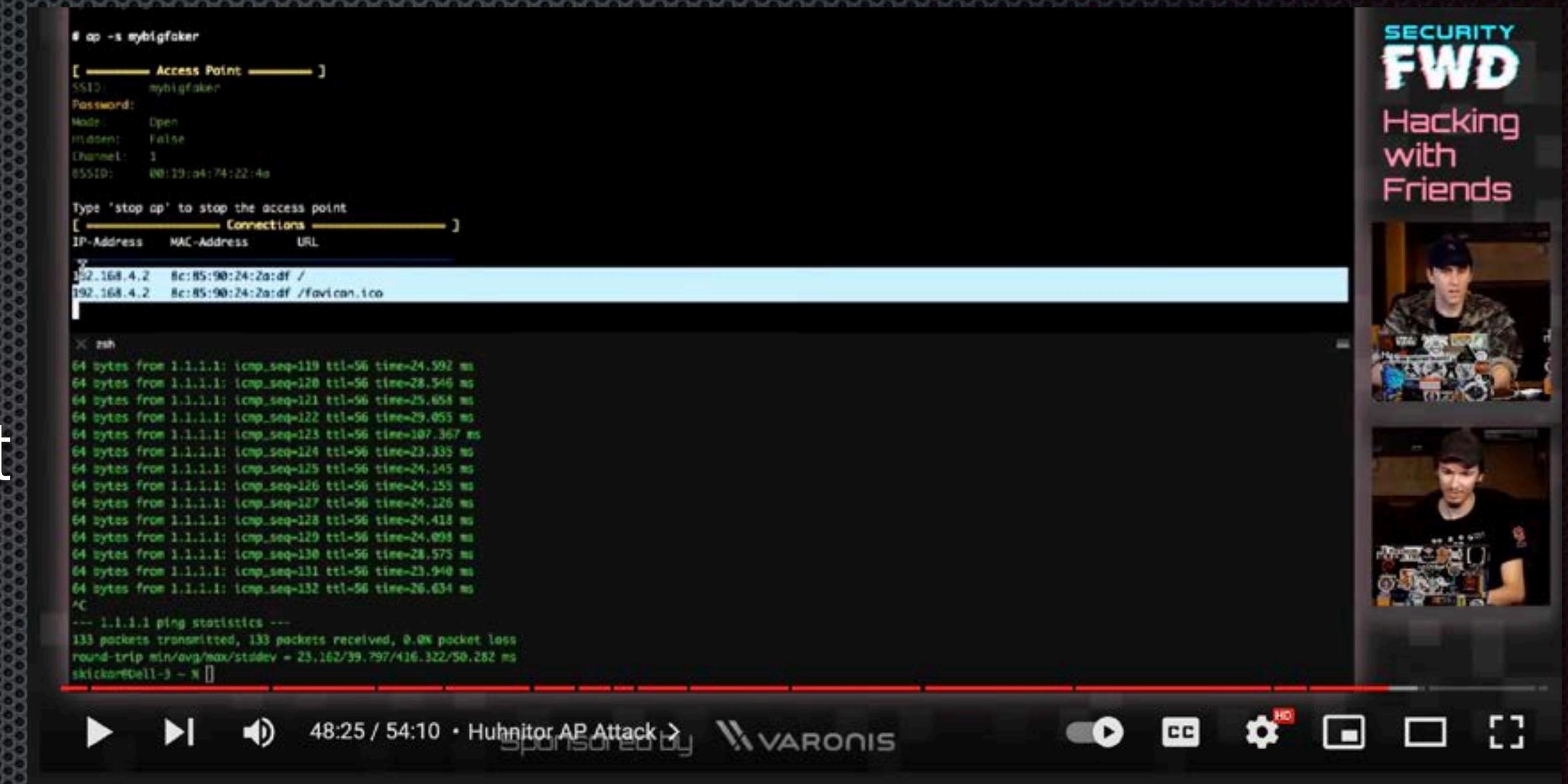
- Serial-only version of the Wi-Fi Deauther
- Execute advanced attacks with the radio free
- Supports Wi-Fi Phishing!
- Supports Rogue AP creation (no data)
- Supports beacon swarm attack

Feature	Version 2	Version 3
Web Interface	✓	
Display support	✓	
Serial Command Line	✓	✓
Scanner	✓	✓
Deauth attack	✓	✓
Beacon attack	✓	✓
Probe attack	✓	✓
Huhnitor support		✓
Signal strength scanner		✓
Authentication scanner		✓
Rogue AP		✓

https://github.com/SpacehuhnTech/esp8266_deauther/tree/v3

ESP8266 Wi-Fi Phishing

- Instead of an interface, we use Wi-Fi to make a phishing page
- First we scan & find a target AP with a client
- Deauthenticate client & create an open network with the same name
- Victim client connects to open network & see a fake router update page
- If they provide the password, deauthentication stops



Wi-Fi Phishing for Passwords with Cheap Microcontrollers

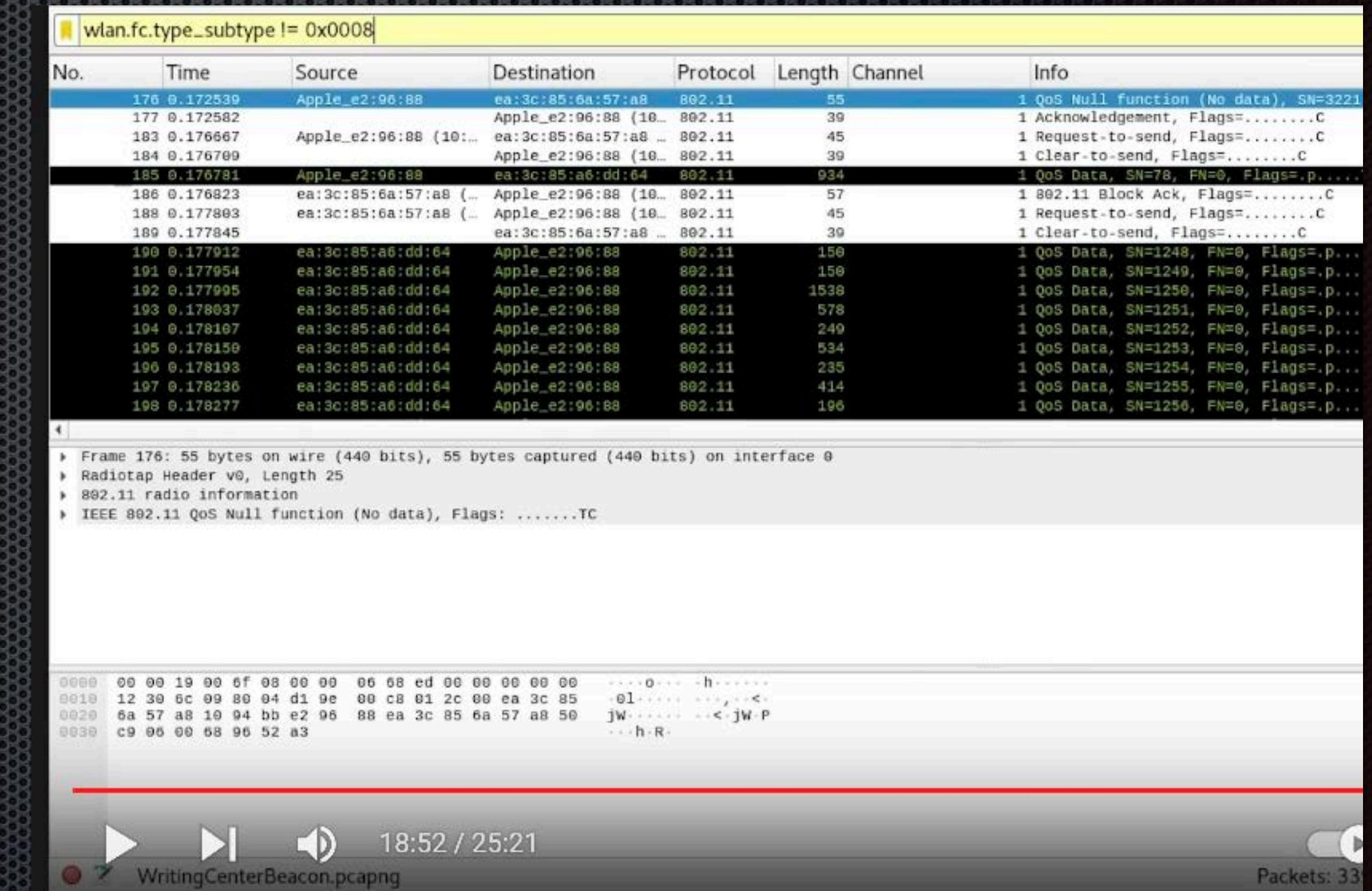
3,791 views • Streamed live on Oct 20, 2020

104 DISLIKE SHARE CLIP SAVE

<https://youtu.be/OIYyLHkTS7o>

ESP8266 Beacon Swarm

- By creating hundreds of fake networks, we can detect when nearby devices try to join
- I made lists of common open Wi-Fi networks & broadcasted them
- Nearby devices recognize networks they've connected to before
- Victim devices auto-join open networks they've seen in the past!
- We can detect if victims have joined networks with a password, but not force them to join



Track & Connect to Smartphones with a Beacon Swarm [Tutorial]

1,025,105 views • Oct 5, 2018

23K DISLIKE

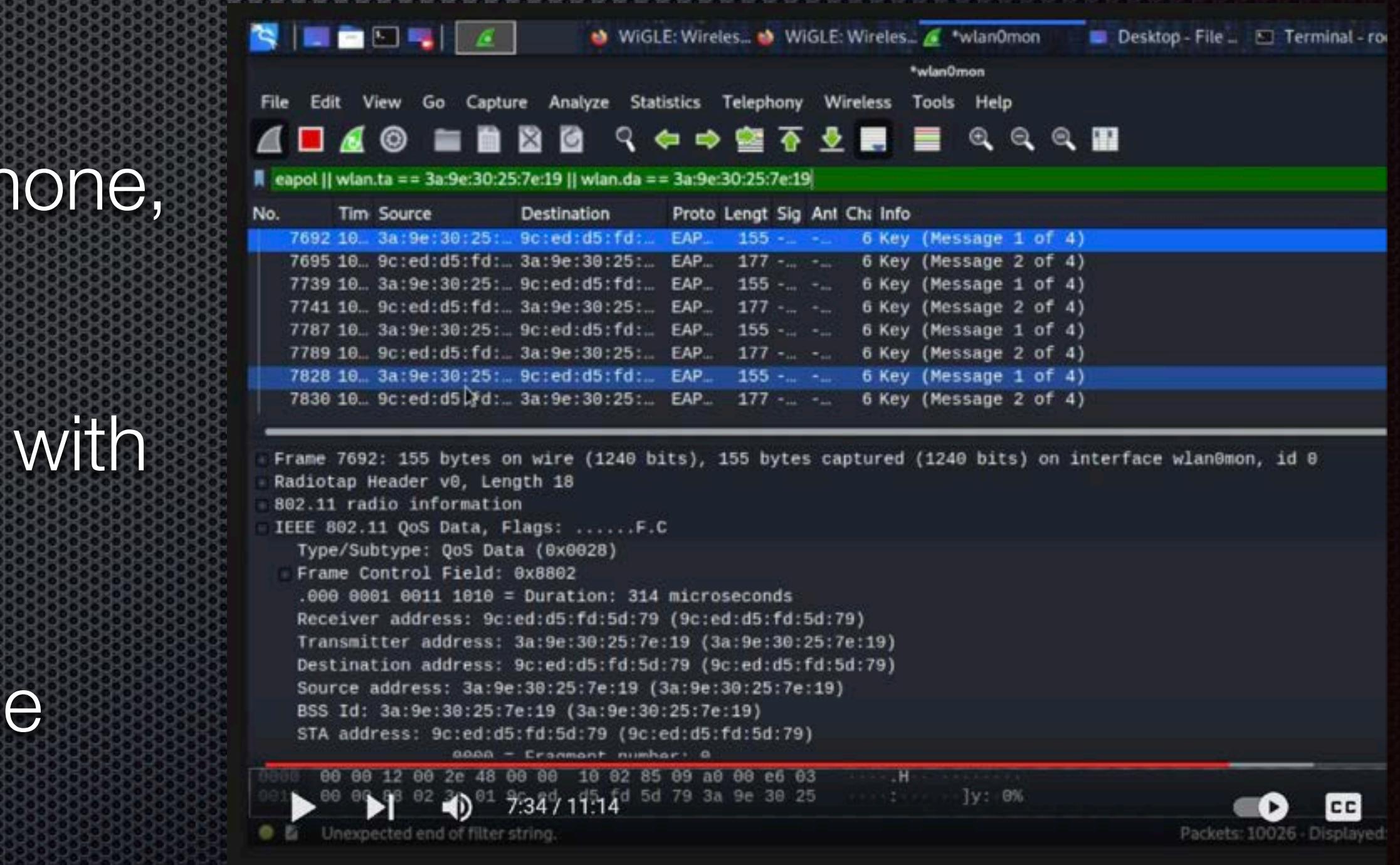
<https://null-byte.wonderhowto.com/how-to/use-esp8266-beacon-spammer-track-smartphone-users-0187599/>

https://youtu.be/o95Or-Z_Ybk

ESP8266 Beacon Half-Handshake

- After running a beacon swarm, I know which networks your phone has connected to
- If I want to crack a password stored in your phone, I can!
- Create a fake AP matching one in your phone with a random password
- When your device connects, I can intercept the hash in Wireshark* & crack it!
- Now I know your home/office Wi-Fi password

*Computer required for this step



HakByte: Capture Wi-Fi Passwords From Smartphones with a Half-Handshake Attack

327,244 views • Aug 5, 2021

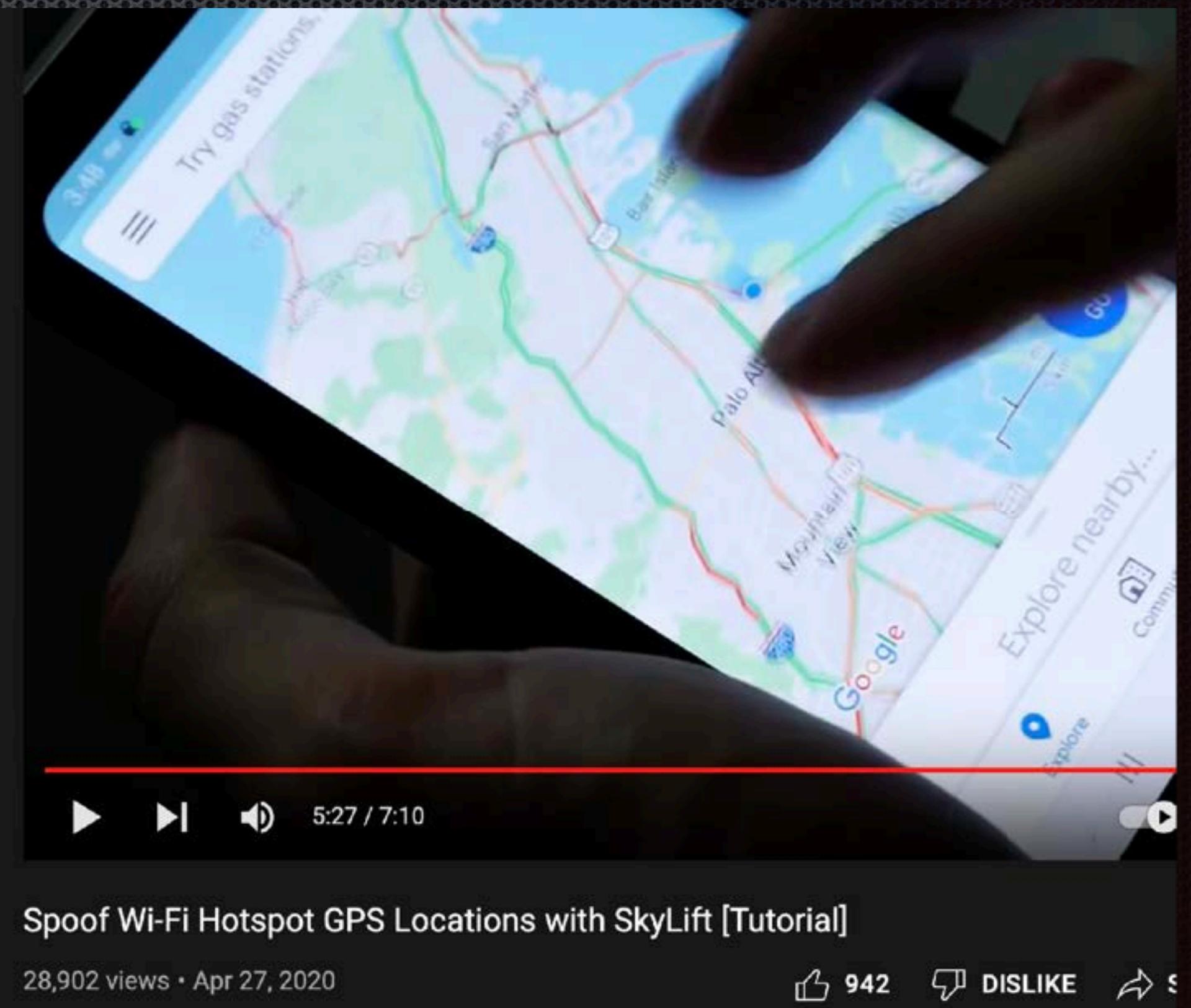
10K DISLIKE SHARE

<https://youtu.be/5guDKTc6Hak>

aGPS Spoofing with Skylift

- Most phones get GPS coordinates faster by using Wi-Fi to find their location
- This project spoofs the Wi-Fi network near Zuck's pool
- Devices with poor GPS reception will fall back to a location calculated by nearby Wi-Fi networks
- Successfully spoofed Zuck's pool location at a mall parking garage

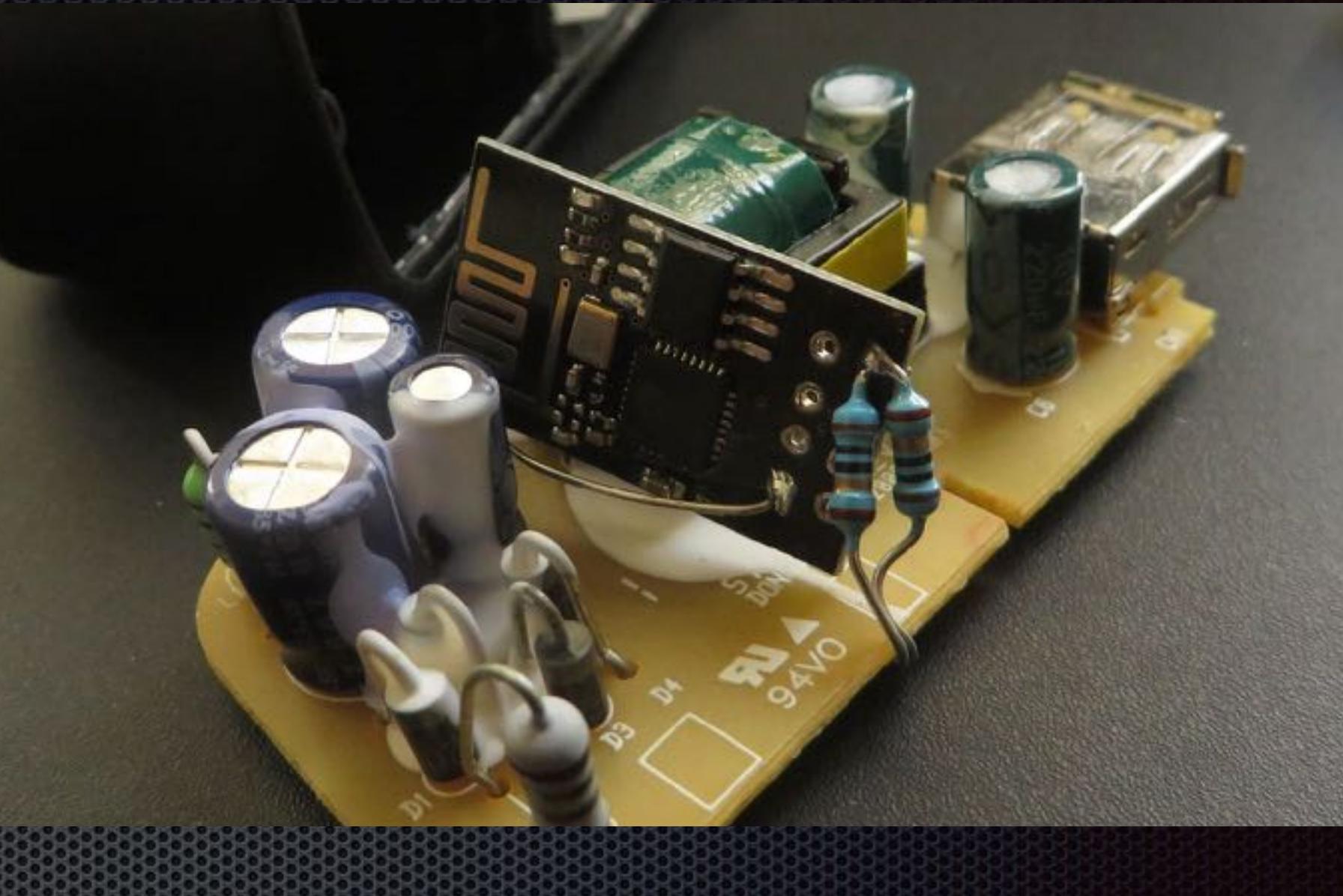
<https://nulb.app/x4q82>



<https://youtu.be/X-ml7bLYWpk>

ESP-Bug Wi-Fi Spying

- The ESP-Bug connects to a Wi-Fi network & monitors the signal strength of nearby Wi-Fi devices
- It reports the signal strength of nearby devices to a web server
- A hacker can tell who is in the room remotely by watching the server interface
- Designed to be hidden in electronics



Known Devices					
Clients					
Name	BSSID	Manufacturer	Channel	RSSI	Associated
	78:0C:B8:EF:6A:05	Intel Corporate	0	-59	bcdde2b2bf58
	98:1E:19:51:1E:26	unknown	0	-60	5460090b135c
	98:1E:19:51:1E:22	unknown	0	-60	5460090b135c
	B4:E3:42:67:A3:73	unknown	0	-86	981e19511e26
	6E:89:04:92:89:E4	unknown	0	-74	981e19511e26
	BE:49:62:C1:E8:60	unknown	1	-82	ffffffffffff
	A8:9A:93:C7:74:E6	unknown	0	-93	da2a4ce376cb
	38:F9:D3:8C:95:7C	unknown	0	-83	7cdb98d63457

<https://youtu.be/1uSg9JoDGeU>

<https://github.com/AlexLynd/ESP-Bug>

Wardriving (or Warflying)

- Connect a \$2 GPS, \$1 SD card module & a \$1.80 ESP8266
- Now we can wardrive!
- Stores seen networks, signal strength, & GPS location to SD card
- We mounted ours on a DJI mini 2
- Located a target smartphone by air!

<https://github.com/AlexLynd/ESP8266-Wardriving>

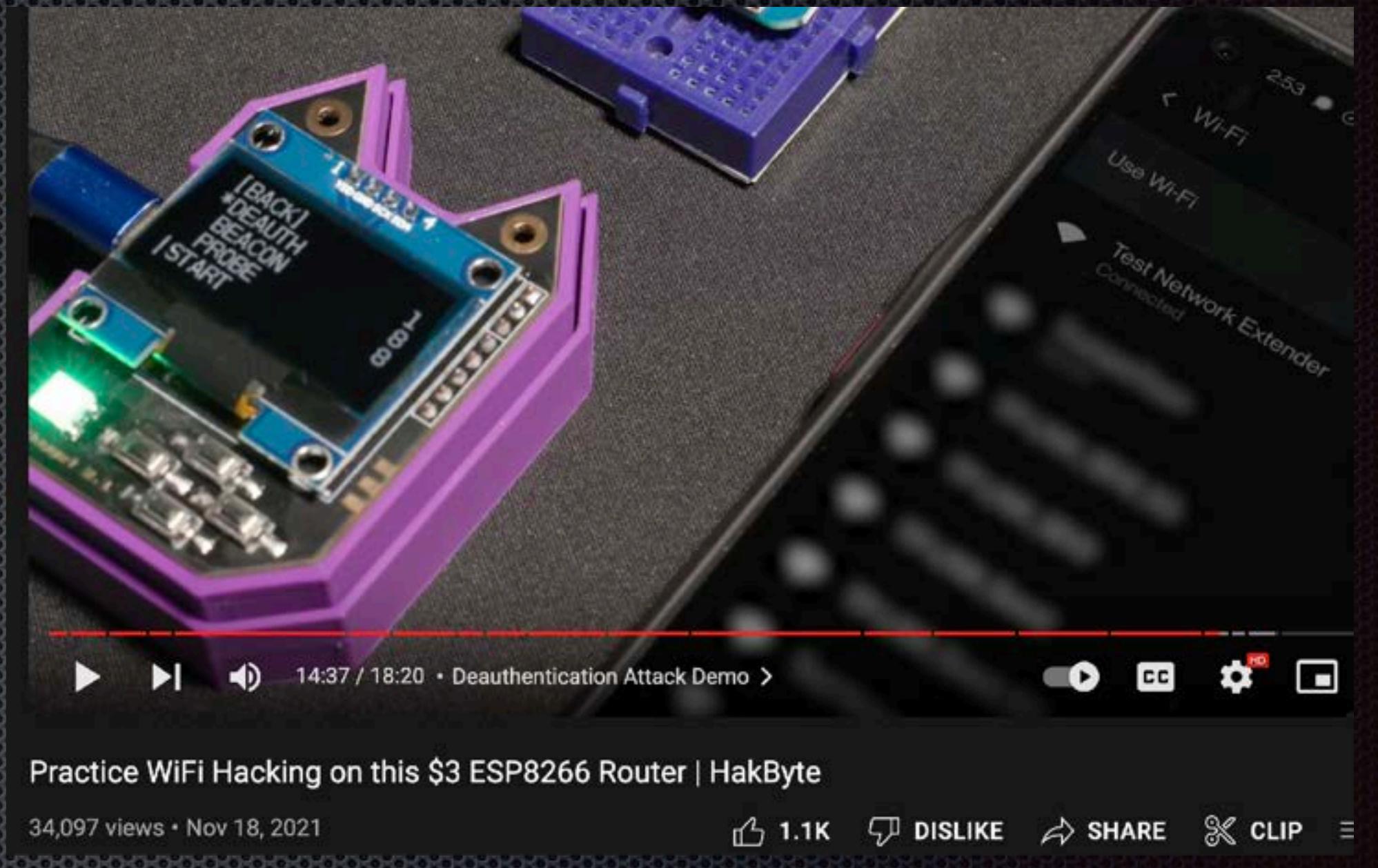


<https://youtu.be/oWNIWHT8q1A>



ESP8266 NAT Router

- The ESP8266 can route internet like a network extender
- The connection is slow but works
- Use it to practice hacking routers
- Use it to isolate IoT devices from your network



<https://youtu.be/hMyH-omBjY4>

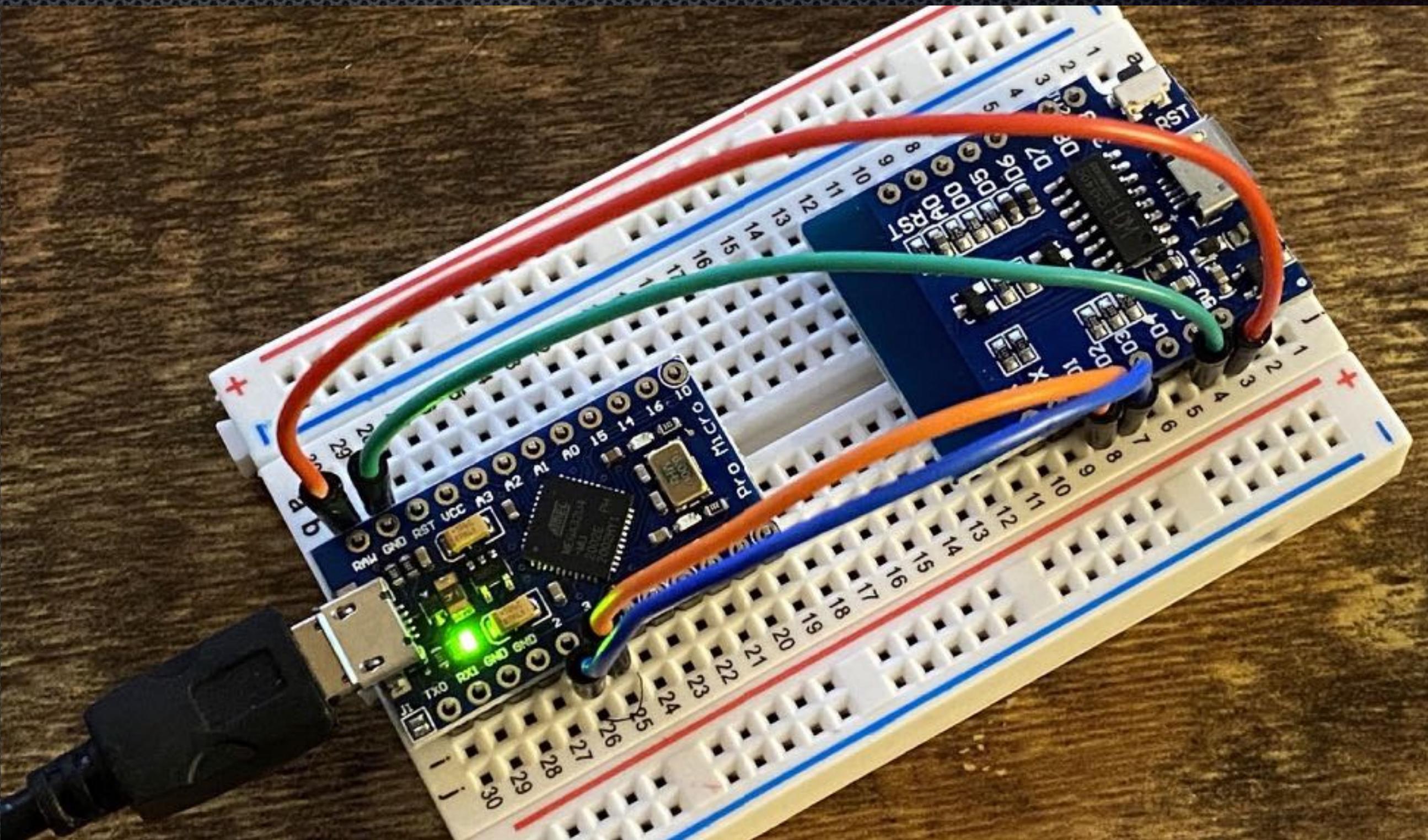
https://github.com/martin-ger/esp_wifi_repeater

Limitations

- ESP8266 cannot see anything but Wi-Fi packet headers
- Not very powerful
- No handshakes, just metadata
- No 5GHz Wi-Fi
- Sucks as a NAT router
- No native USB support

Esp8266 + atmega32u4

- Stick a microcontroller that supports Wi-Fi to one that supports USB
- This gives you a bad USB devices with Wi-Fi
- Close to our budget but worth mentioning
- There are chips that do both in 1



Wi-Fi Duck

- Open source project by @Spacehuhn
- Requires you to flash each chip
- ESP8266 handles Wi-Fi web interface
- ATmega34u handles USB functions
- Connected over i2c
- Run, edit, and save payloads
- Auto-run payloads on insertion
- Access menu via any Wi-Fi device



HOW TO

Hack Computers Over Wi-Fi with the WiFi Duck Payload Deliverer

BY RETIA © 11/12/2020 9:07 PM CYBER WEAPONS LAB ESP8266 MCUS

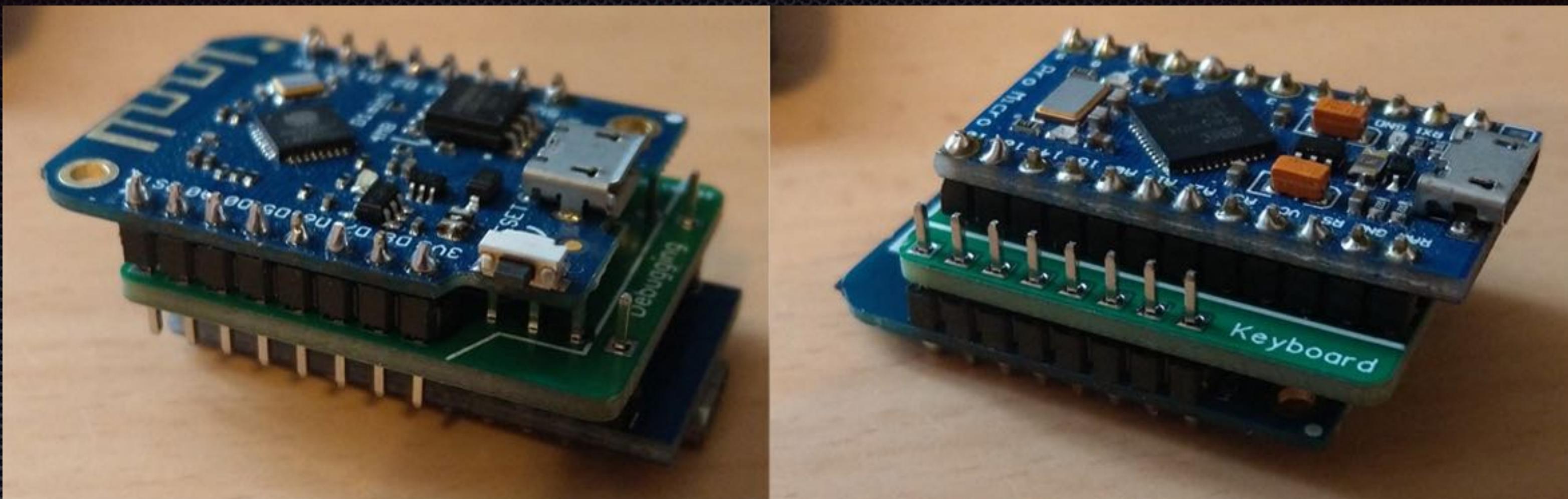
The [USB Rubber Ducky](#) is a well-known hacking device in the cybersecurity industry, but it needs to be preprogrammed before it can be used. That means it's not easy to issue commands to a target computer since you can't interact with it from afar after plugging it in. And if you don't know what the target computer is, you might come up empty. That's where the WiFi Duck comes in handy.

<https://null-byte.wonderhowto.com/how-to/hack-computers-over-wi-fi-with-wifi-duck-payload-deliverer-0296285/>



<https://vimeo.com/381208724>

Wi-Fi Duck



<https://github.com/spacehuhntech/wifiduck>

The WiFi Duck software interface is displayed in two panels. The left panel, titled "Status", shows a green "Connected" bar at the top. Below it, there's a "Storage: 502 byte used (99% free)" message and three buttons: "FORMAT" (red), "STOP" (yellow), and "RECONNECT". The right panel, titled "Scripts", has a "File" column with "/test", a "Byte" column with "20", and an "Actions" column with "EDIT" and "RUN" buttons. A "CREATE" button is at the bottom. The status bar at the bottom of the right panel shows "Output: saved".

WiFi Duck Settings Terminal

Connected

About

Status

Storage: 502 byte used (99% free)

FORMAT STOP RECONNECT

Scripts

File Byte Actions

/test 20 EDIT RUN

CREATE

Editor

/test DELETE DOWNLOAD ENABLE AUTORUN

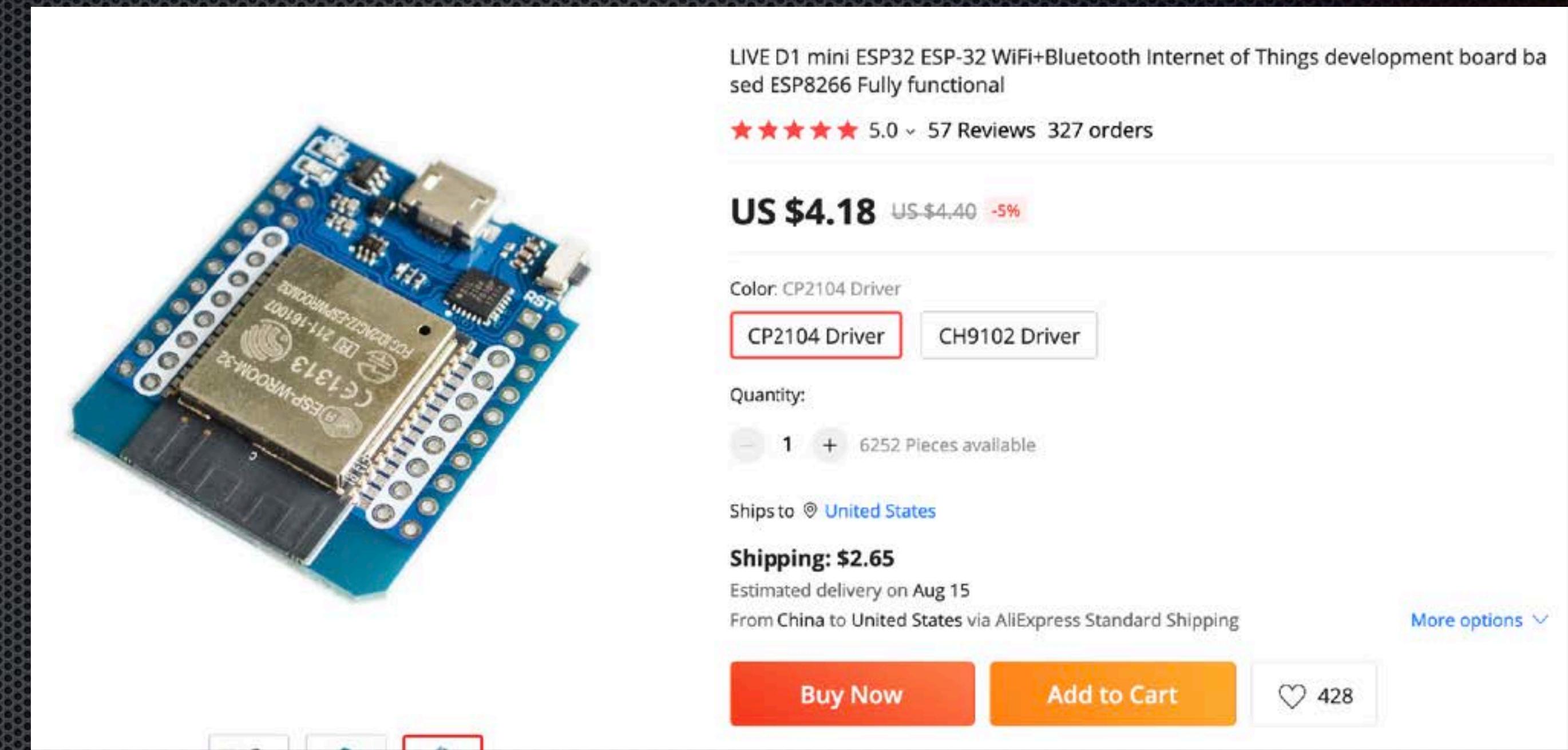
GUI r
STRING Hi

Output: saved

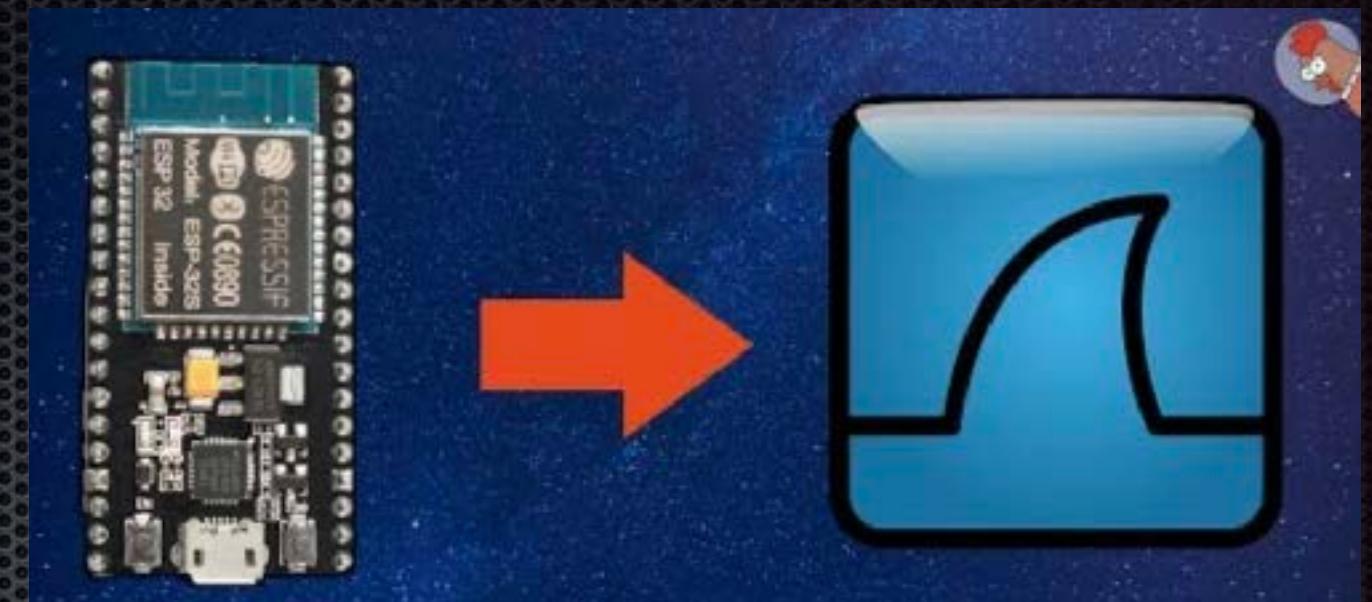
SAVE RUN STOP

Esp32

- More powerful than the ESP8266
- Supports Arduino, MicroPython
- Does not support Wi-Fi attacks
- Does not support native USB
- Useful for applications like video & basic routing

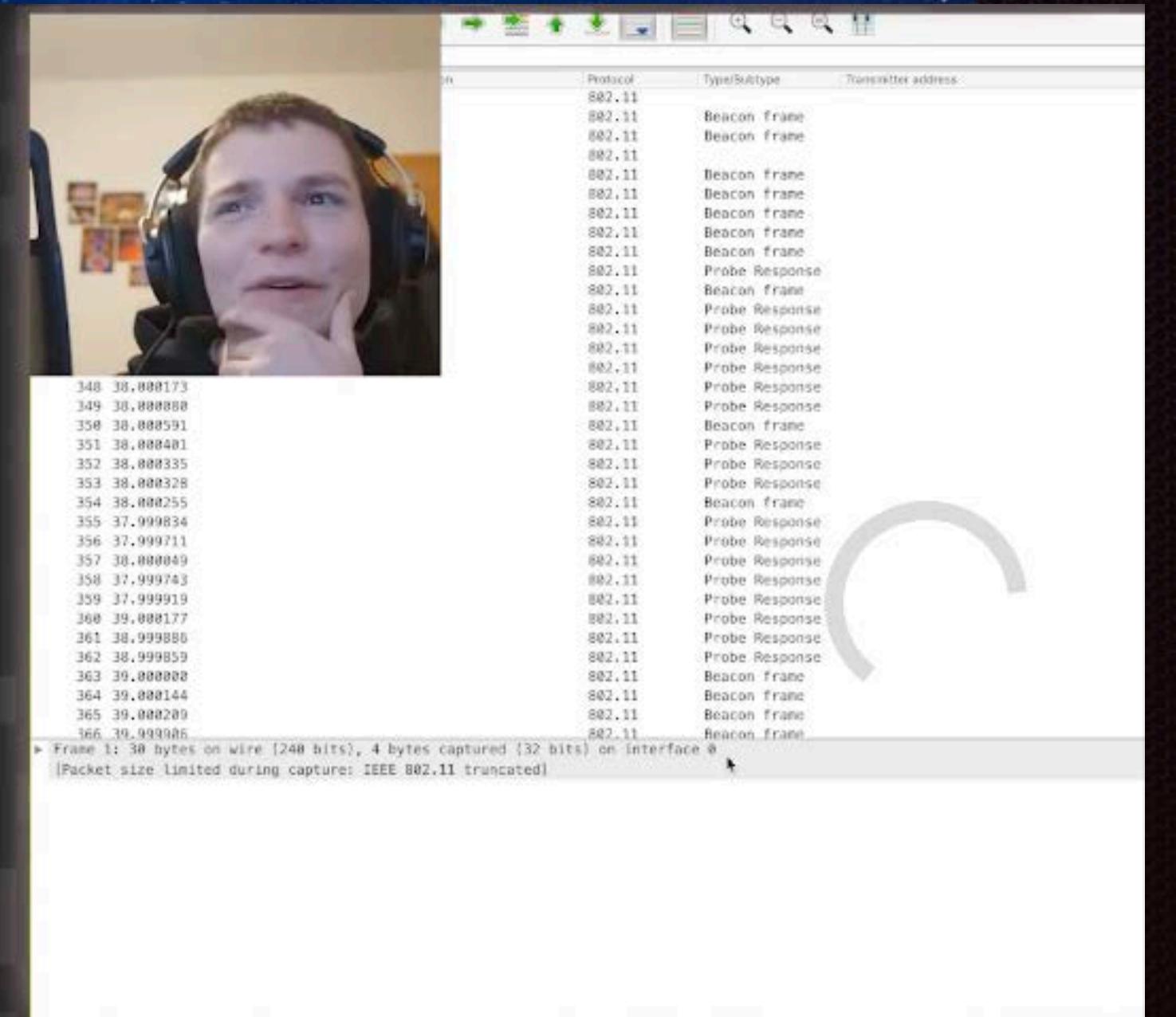


ESP32 Packet Capture



Connect ESP32 to Wireshark

- Unlike the esp8266, the ESP32 can capture full packets
- @Spacehuhn wrote a library to convert to .PCAP files
- Runs on SD card or over Serial
- I have never succeeded at capturing a handshake
- Also haven't tried more than 2x



SECURITY
FWD Hacking
with Friends

Using the ESP32 Microcontroller for Packet Sniffing

2,625 views

47

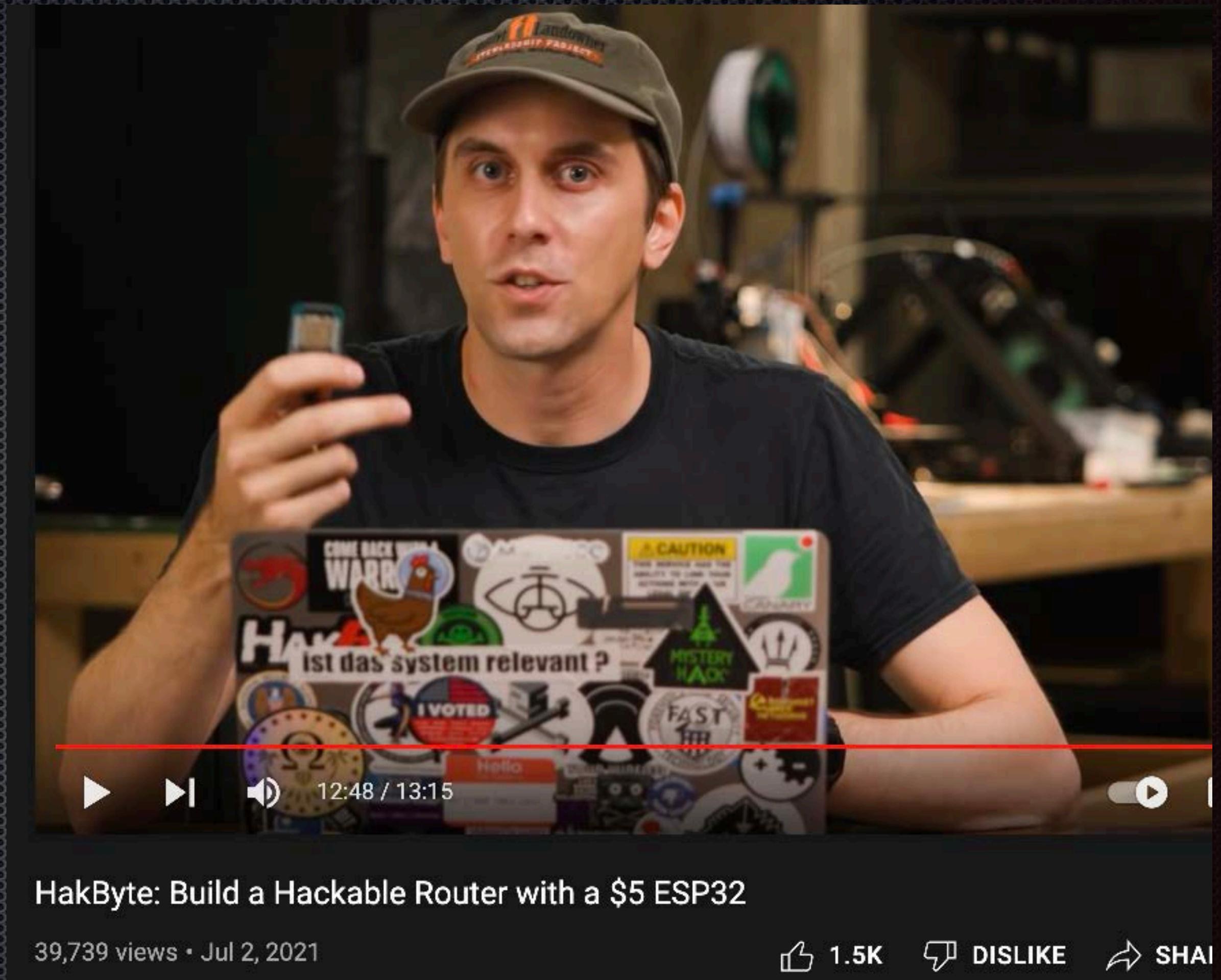
DISLIKE

<https://github.com/spacehuhn/ArduinoPcap>

<https://youtu.be/4Hs6x1tMzf4>

ESP32 NAT Router

- The ESP32 can also route internet like a network extender
- The connection is faster & more reliable than esp8266 version
- Use it for the same testing, IoT, or phishing purposes



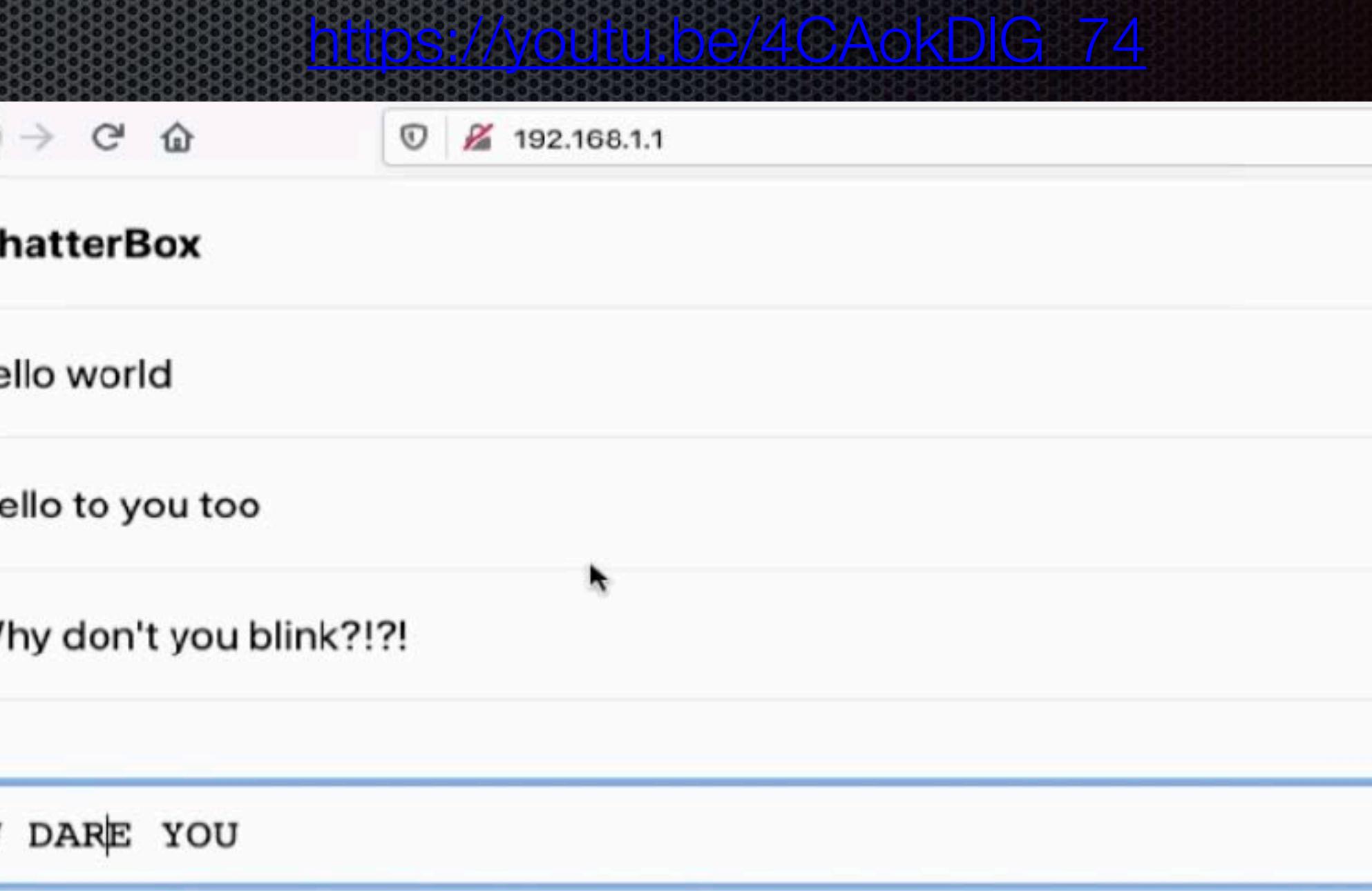
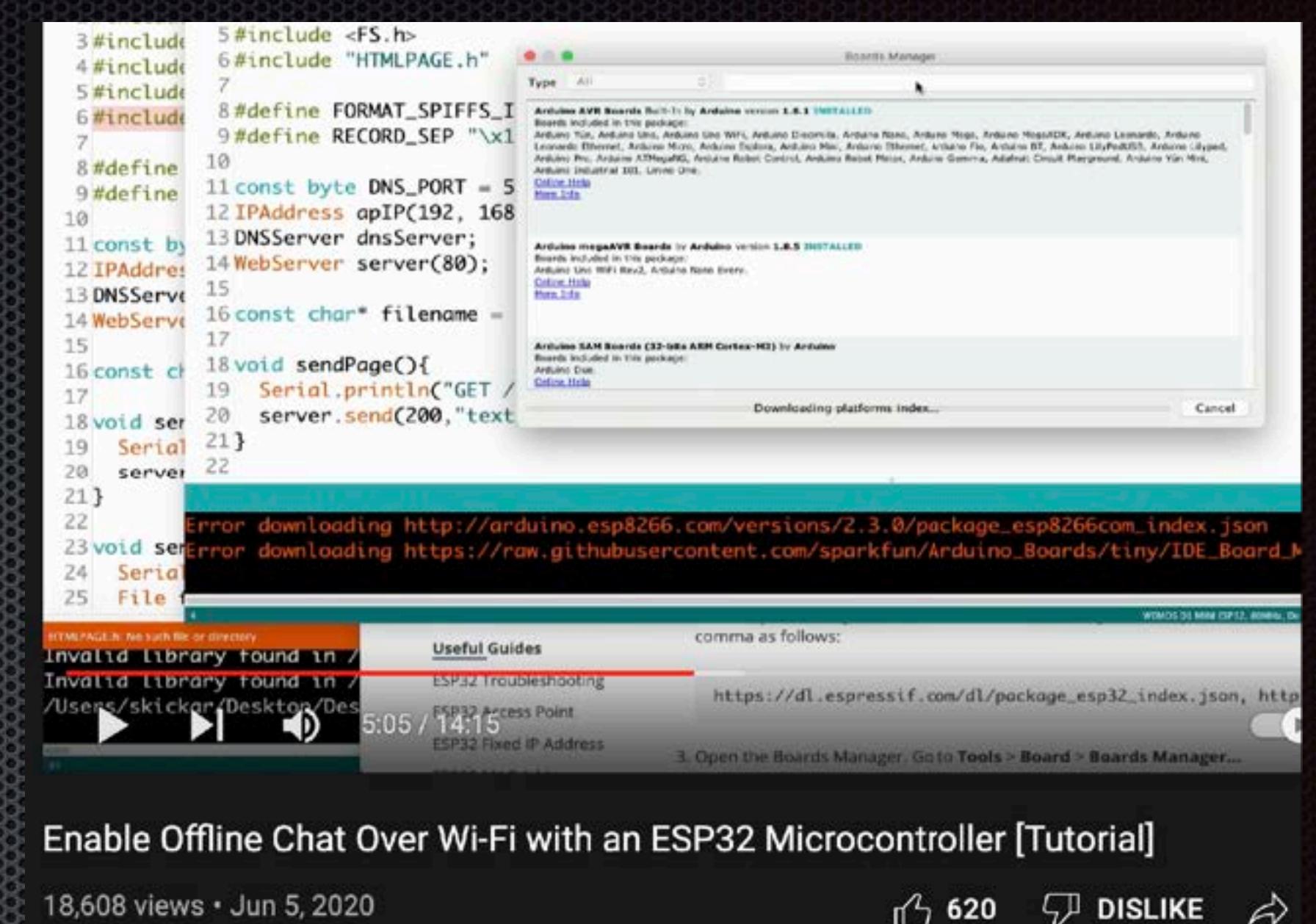
<https://youtu.be/41Lymi6rXA8>

https://github.com/martin-ger/esp32_nat_router

ESP32 Offline Chat

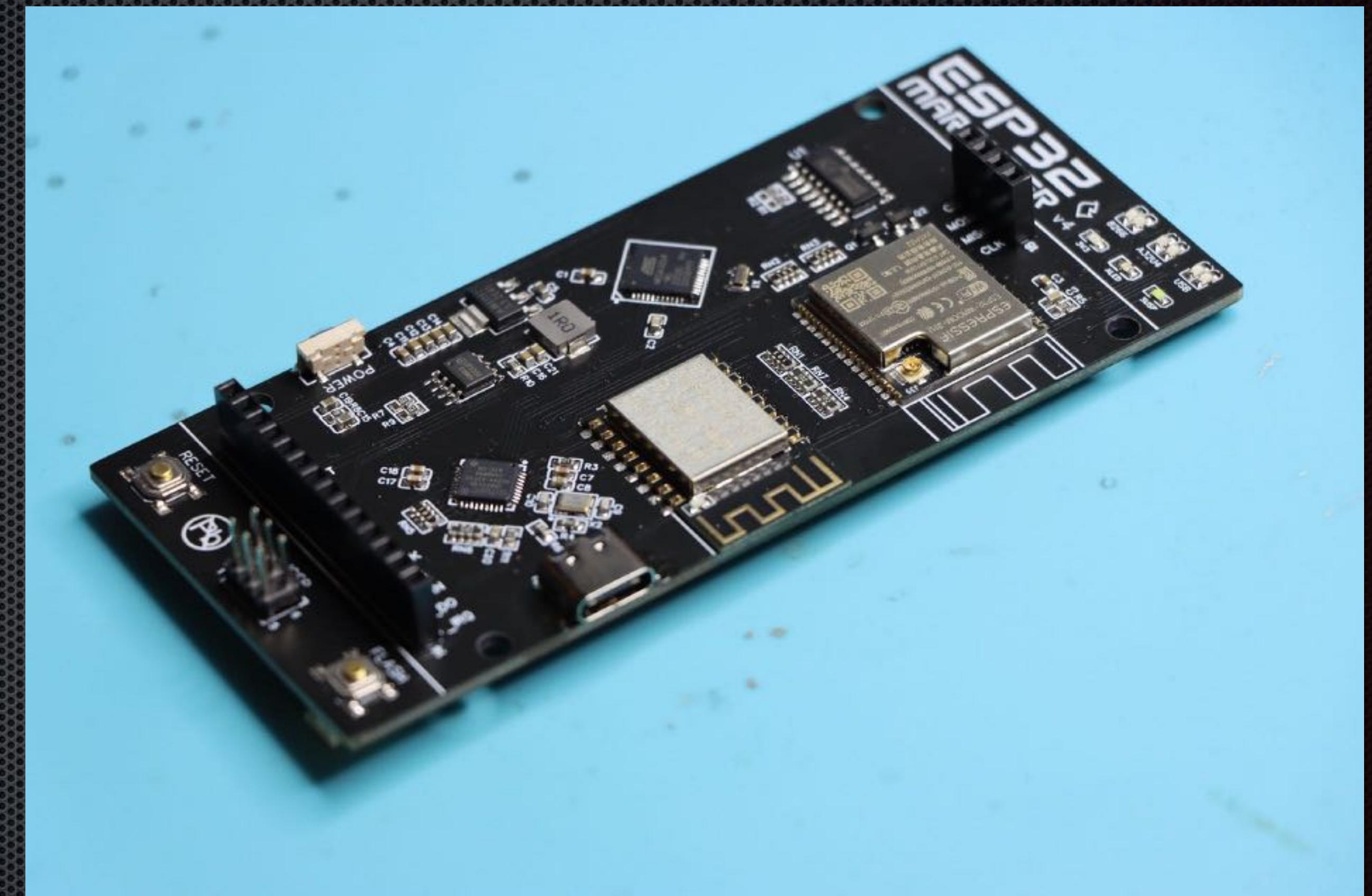
- The ESP32 can act as a webserver to host a chat or clandestine conversation
- Any device in Wi-Fi range can join & chat
- Offline data exchange useful for private chat or message board
- Anonymous messages or CTF

<https://nulb.app/z6vu2>



Esp8266 + ESP32

- By combining the ESP32 and ESP8266, we can get the advantages of both
- The ESP Marauder links these microcontrollers together
- Features deauthentication and handshake capture
- Ends up being kind of a multi tool without a specific focus
- Over our budget



<https://github.com/justcallmekoko/ESP32Marauder>

Esp32cam

- Integrated camera with ESP32
- Easy to hide Wi-Fi enabled webcam
- Supports facial recognition
- No USB port (good luck)



KKCHIP ESP32CAM OV2640 WiFi+Bluetooth ESP32-CAM Module Serial to WiFi ESP32 CAM Development Board

★★★★★ 5.0 ▾ 4 Reviews 27 orders

US \$4.89

Quantity:

- 1 + 591 Pieces available

Ships to [United States](#)

Shipping: \$3.43

From China to United States via AliExpress Standard Shipping
Estimated delivery on Aug 13

[More options ▾](#)

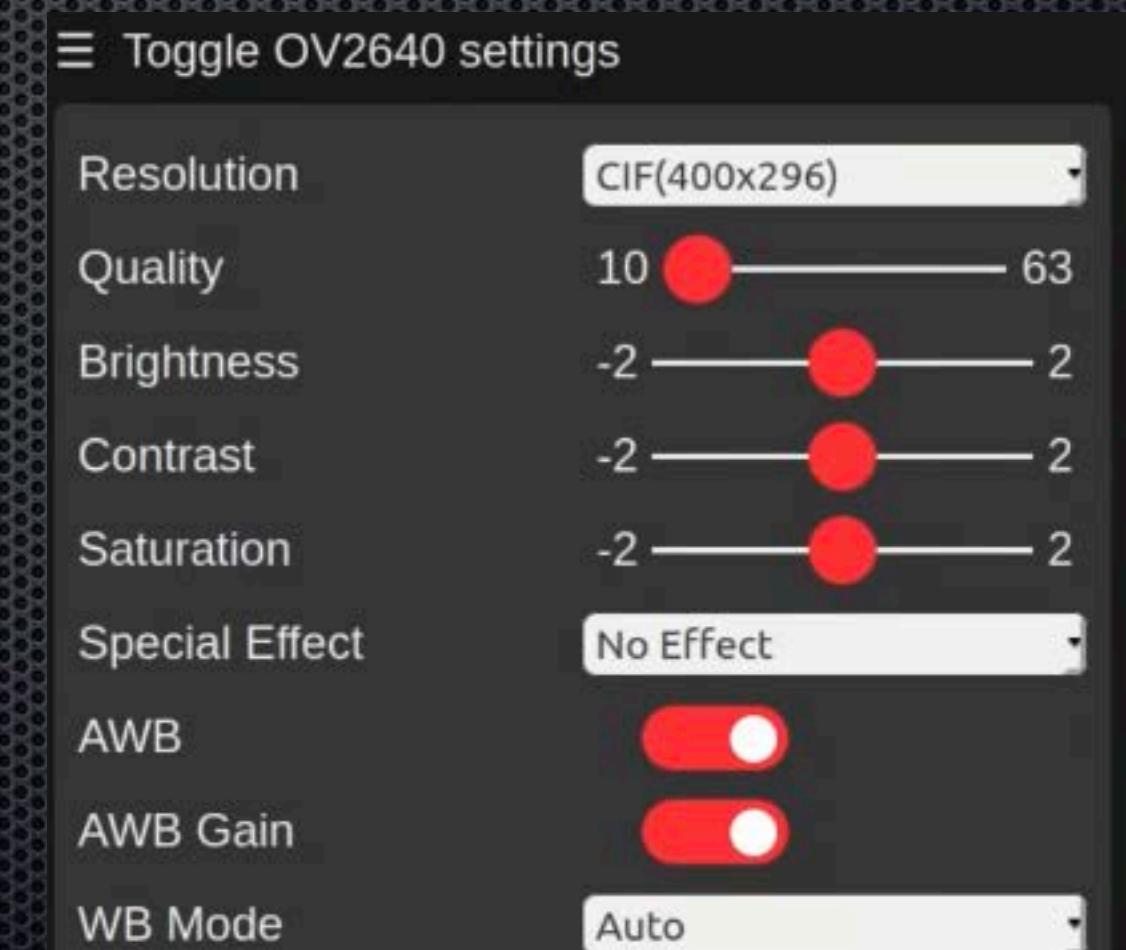
[Buy Now](#) [Add to Cart](#) 24

 **75-Day Buyer Protection**
Money back guarantee

Esp32cam Spy Camera

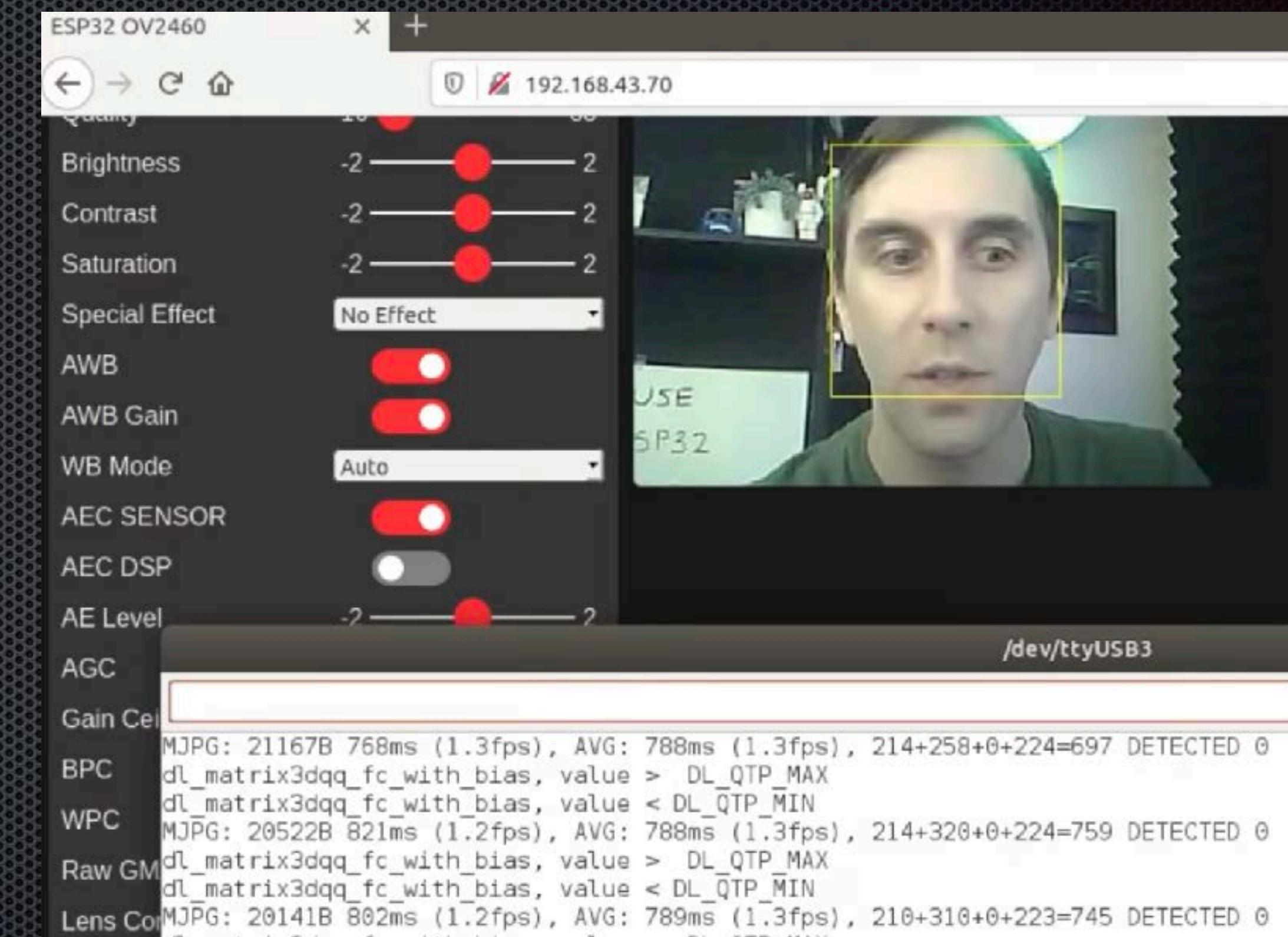
- With a LiPo battery & serial connector, we have a Wi-Fi spy camera!
- Connects to Wi-Fi & streams video
- Adjustable resolution
- Easy to record stream from another device

<https://nulb.app/x5qaf>



Esp32cam Facial Recognition

- The ESP32cam supports basic facial detection & recognition
- No depth - easy to fool with a picture
- Can alert on known or unknown faces
- Run a program when a face is detected



<https://youtu.be/L0qVle9cnW8>

<https://nulb.app/x6ur7>

Esp32s2

- Supports Wi-Fi
- Supports native USB
- Comes in module that is pin-compatible with ESP8266 D1 Mini
- Does everything the Wi-Fi Duck can do in one chip!

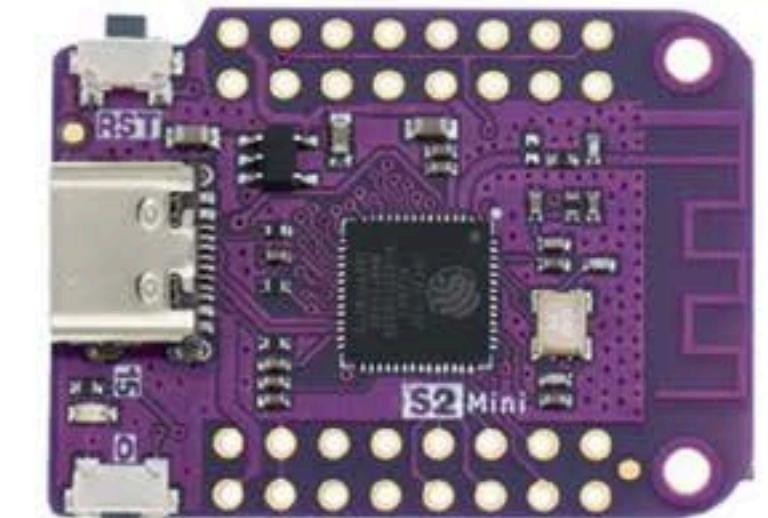
ESP32 S2 Mini WIFI Board Based ESP32-S2FN4R2 ESP32-S2 4MB FLASH 2MB PSRAM MicroPython For Arduino Compatible D1 mini upgrade

★★★★★ 4.2 ▾ 5 Reviews 119 orders

US \$2.94 US \$3.34 -12%

US \$10.00 Off Store Coupon Get coupons

Color: S2 Mini



Quantity:

- 1 + Additional 1% off (100 Pieces or more)
151842 Pieces available

Ships to United States

Shipping: \$1.75

Estimated delivery on Sep 15
From China to United States via Cainiao Super Economy Global

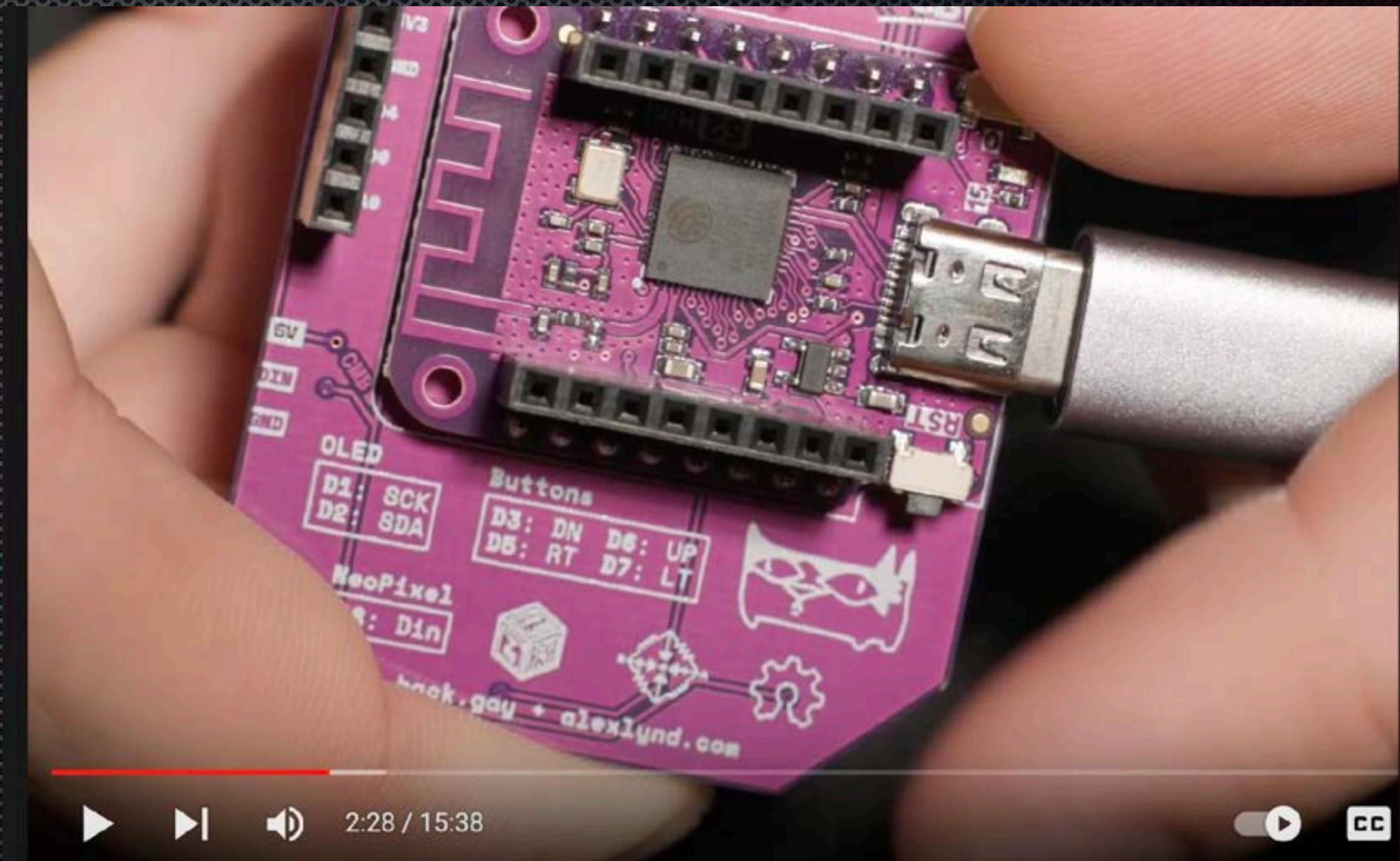
More options ▾

Buy Now **Add to Cart** 42

Mouse Control with CircuitPython

- Because the ESP32s2 supports native USB & CircuitPython, we can easily control the mouse
- Simple mouse jiggler shows a very simple way to use Python to jiggle or click the mouse

[https://github.com/HakCat-Tech/S2-Nugget/blob/main/
Mouse_Jiggler_Example.zip](https://github.com/HakCat-Tech/S2-Nugget/blob/main/Mouse_Jiggler_Example.zip)



Keep Computers From Locking with a CircuitPython Mouse Jiggler | HakByte

14,021 views • Dec 9, 2021

504

DISLIKE

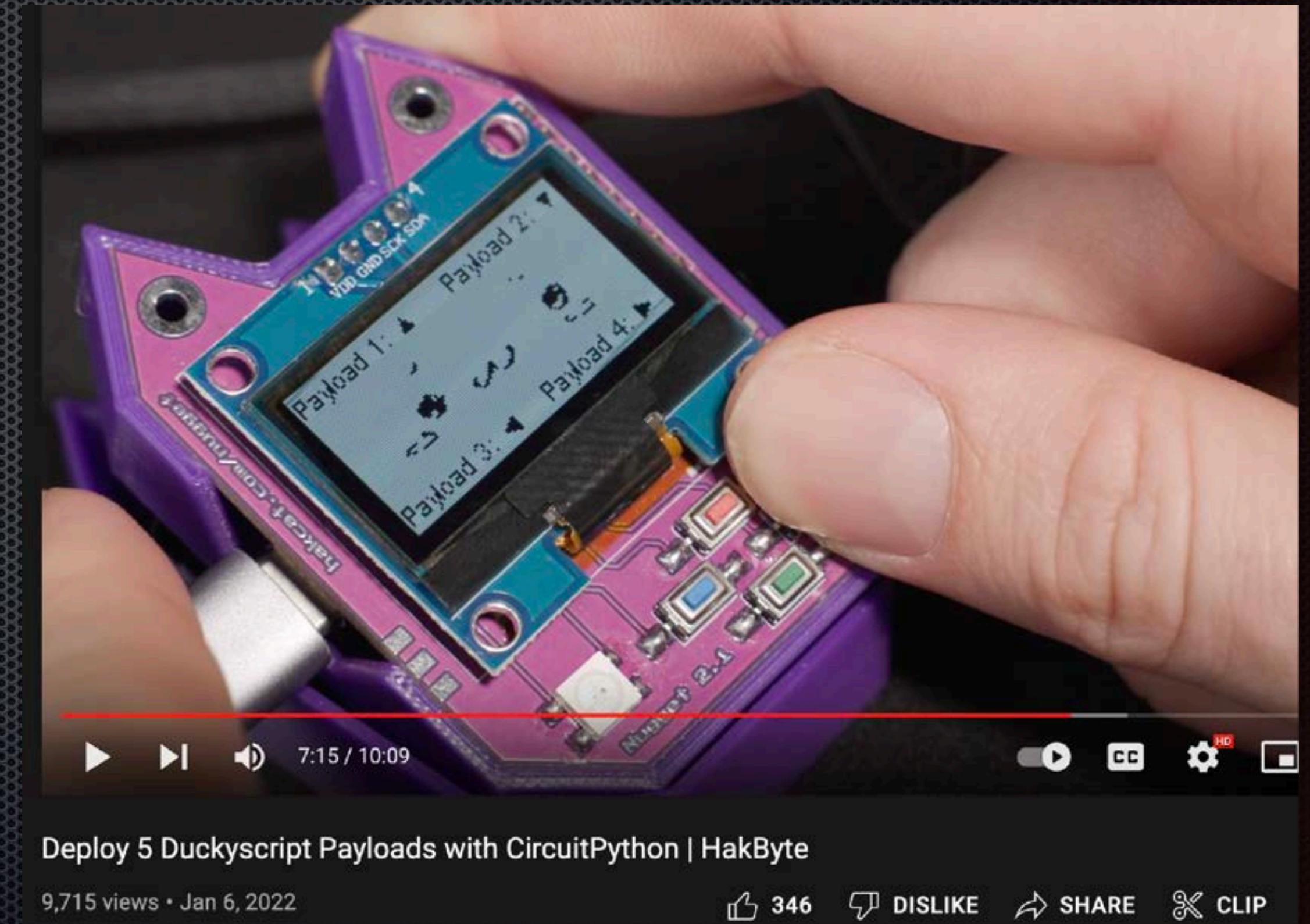
SHARE

<https://youtu.be/aZ8u56I3J3I>

Rubber Nugget

- CircuitPython Project supporting basic DuckyScript injection
- Ported from the PicoDucky project for the Pi Pico
- Button operated with a basic Wi-Fi interface
- I wrote this trash fire

<https://github.com/HakCat-Tech/RubberNugget-CircuitPython>



https://youtu.be/XqwR0bGrc_Y

USB Nugget

- Advanced HID attack device written in Arduino by Alex Lynd
- Supports 36 payloads organized into folders
- Web interface to edit, save, or run saved payloads
- USB interface for easy editing of payloads

<https://github.com/HakCat-Tech/RubberNugget>



How Hackers Use PwnKit to Get Root Access in Seconds

34,623 views • Feb 10, 2022

1.2K DISL

https://youtu.be/hiRh_2IL7RY



RubberNugget v1.0

- Built in Flash Drive for data exfiltration
- DuckyScript™ Compatible USB attack payloads
- Web Interface for remote payload deployment

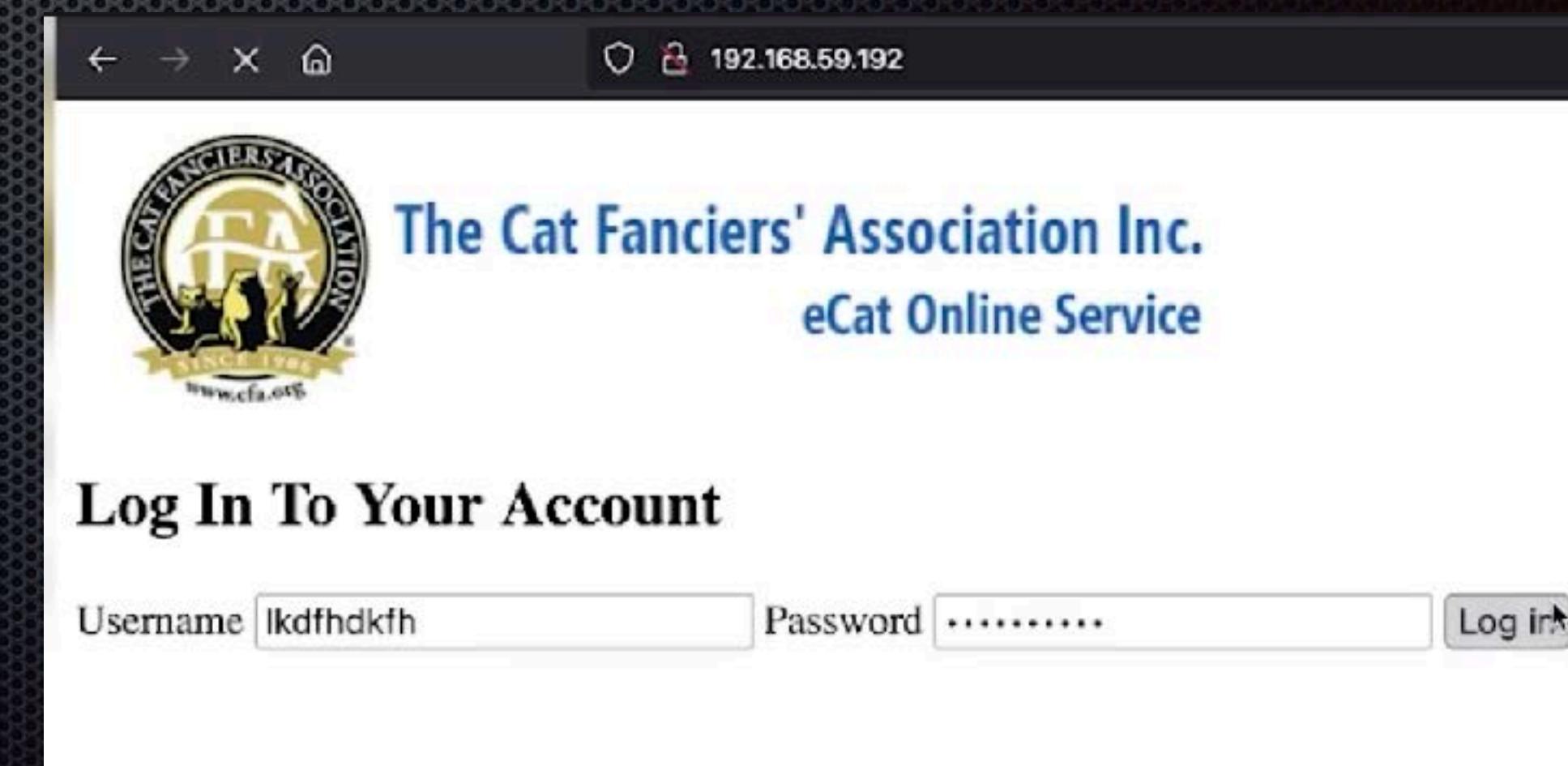
Learn more at: wifinugget.com

<https://docs.hak5.org/rubber-nugget/>

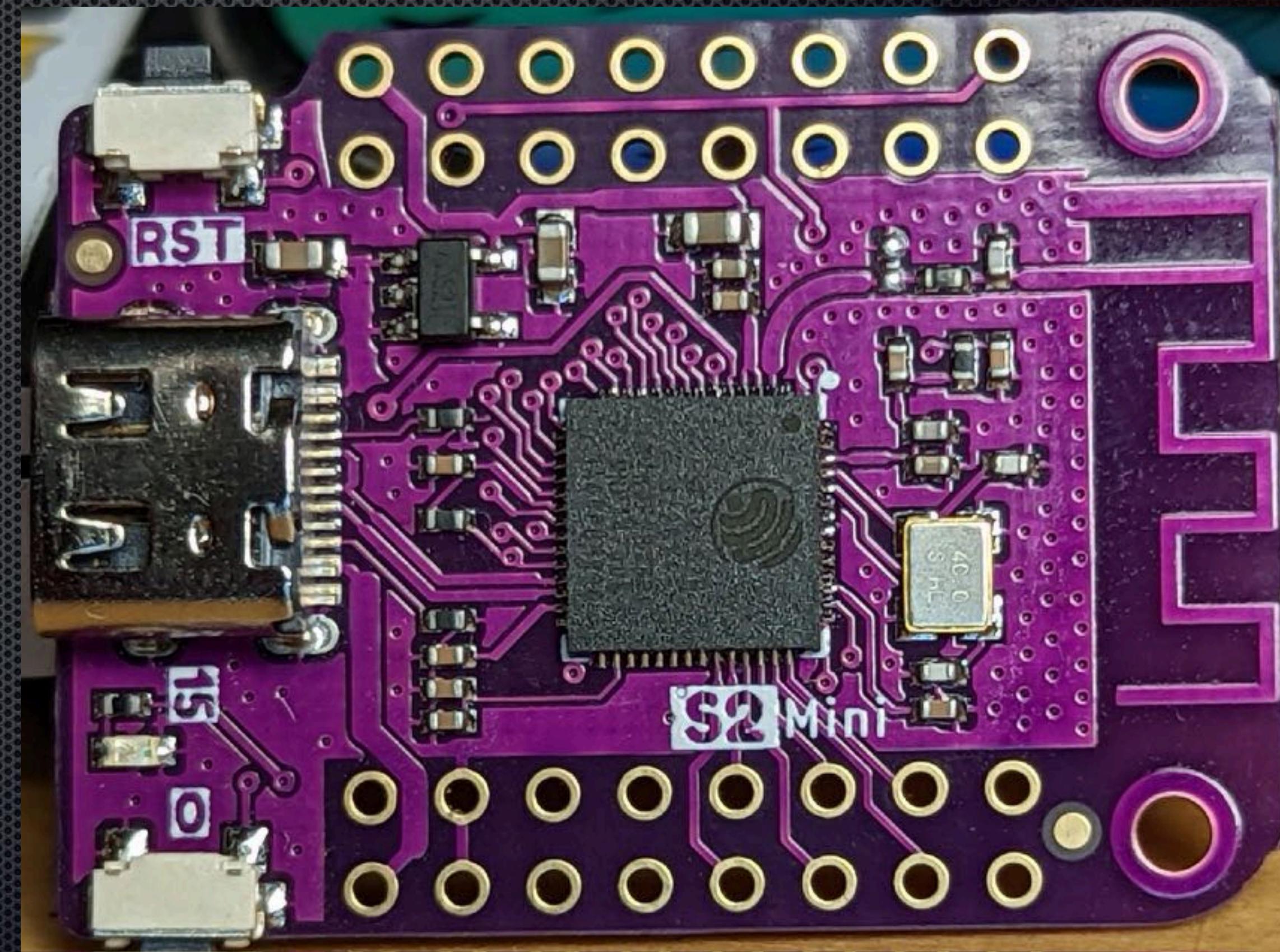
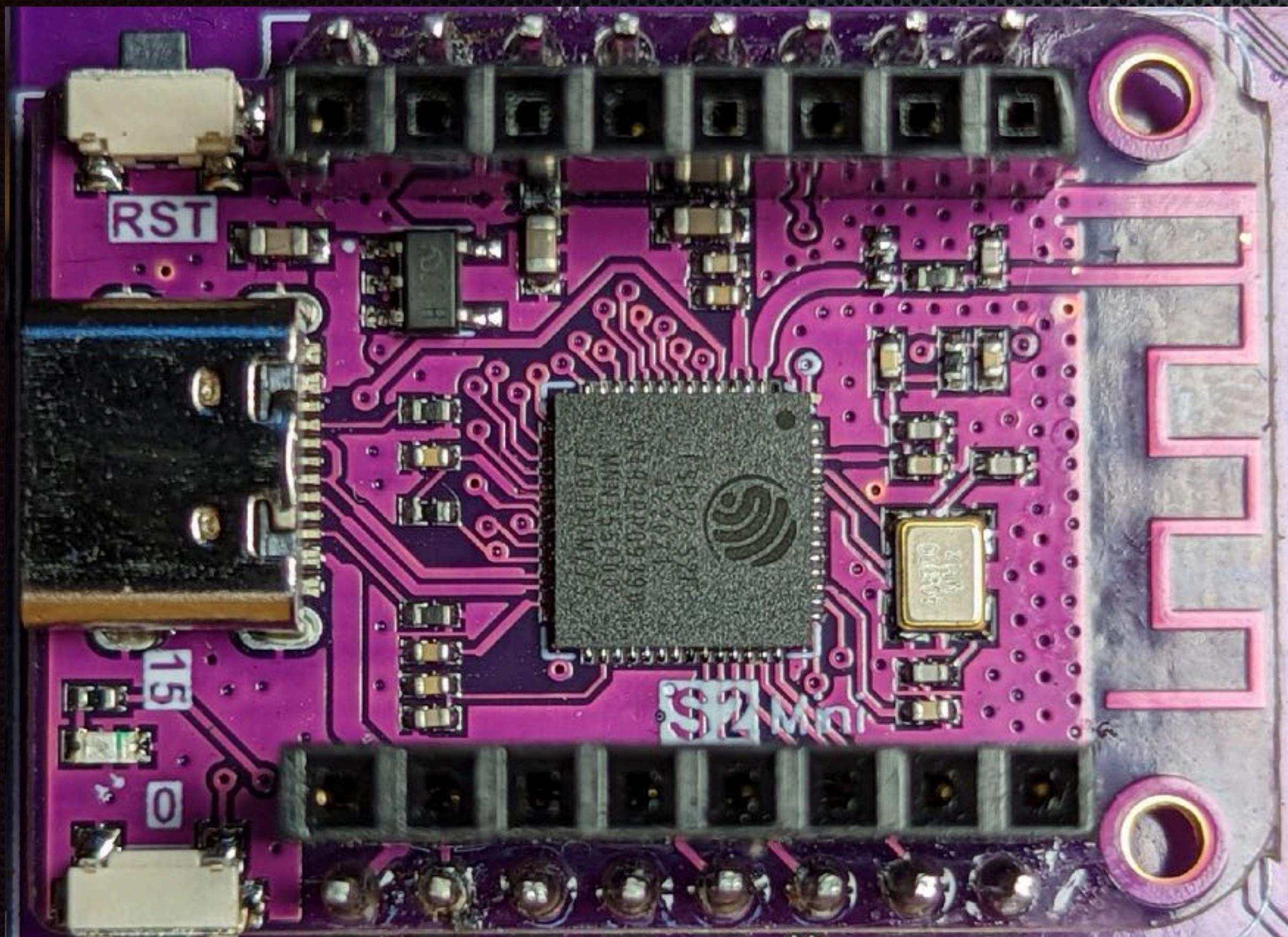
Damn Vulnerable Nugget

- The Damn Vulnerable Nugget is a simple vulnerable web app written in CircuitPython
- Users can attack it using OWASP Zap or Burpsuite to practice authentication attacks
- It picks a new password each time you run it
- Wet anime eyes to celebrate a win
- I wrote this!

<https://github.com/HakCat-Tech/DamnVulnerableNug>

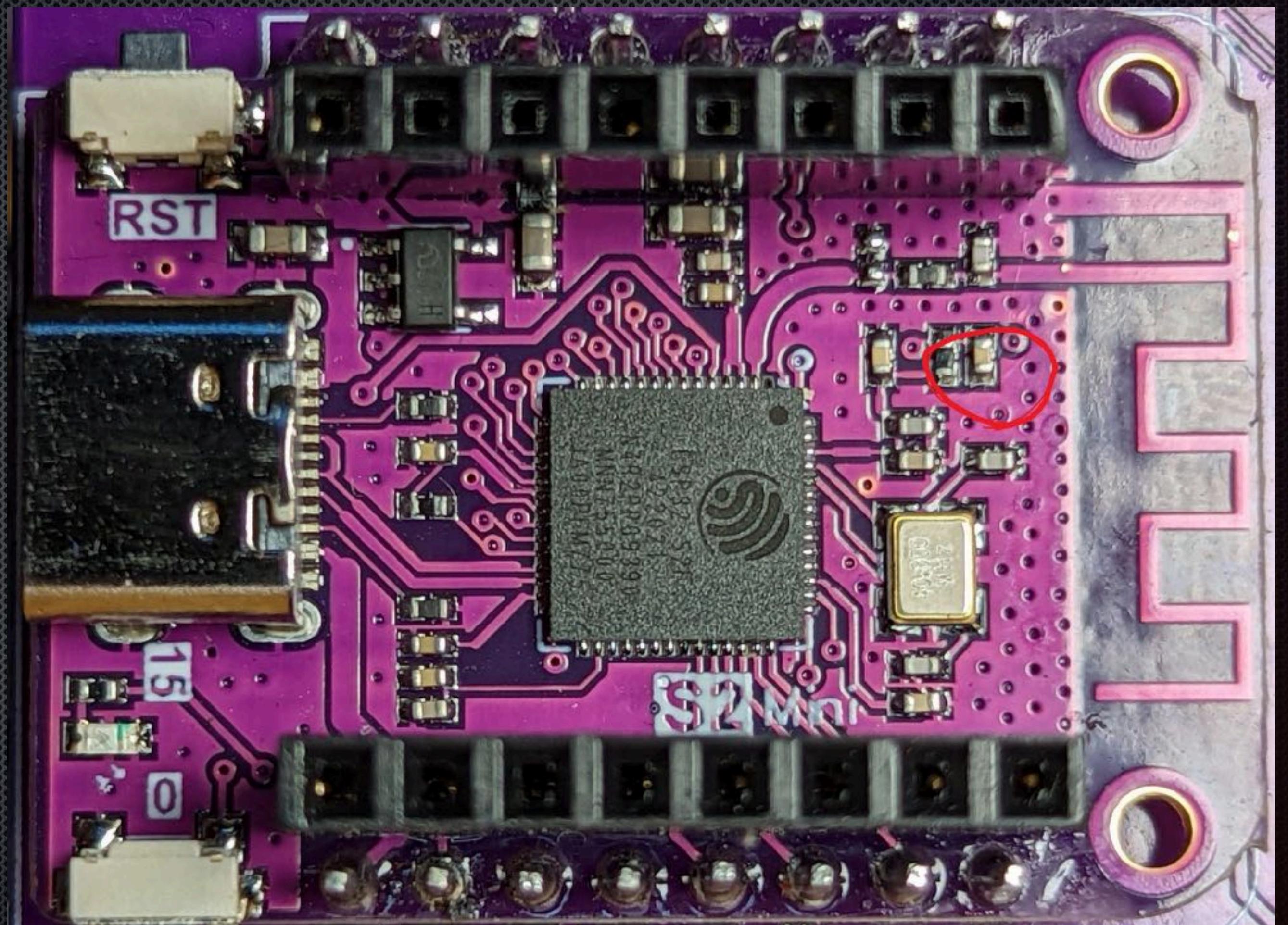


Comparing 2 S2 Mini Modules



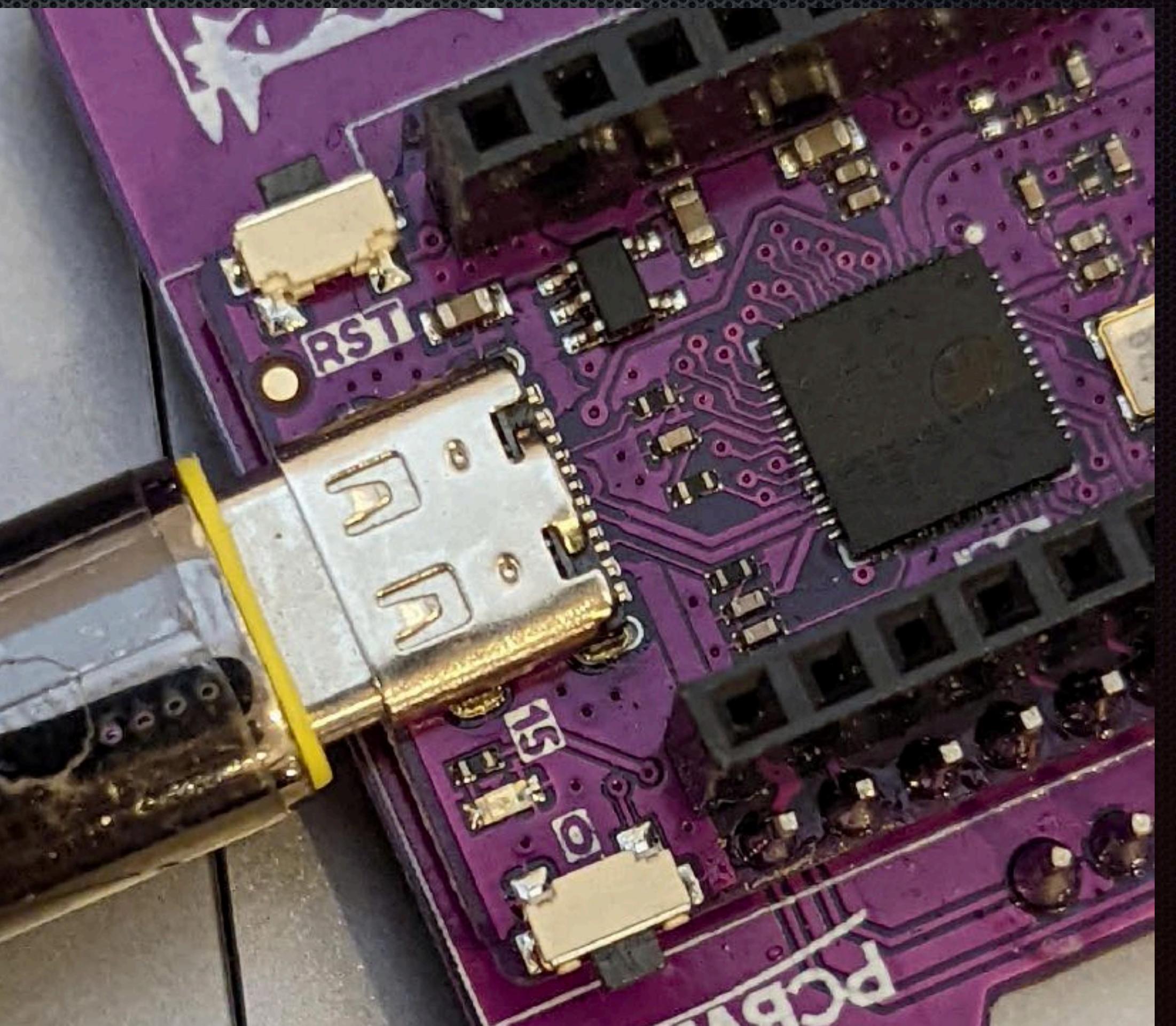
A bad S2 Mini Module

- This module has a single floating connection
- Causes power instability
- Cursed but fix is easy
- Adding solder blob to ground plane fixed it



ESP32s2 Limitations

- No Bluetooth
- No Wi-Fi Attacks (SDK too new)
- No 5GHz Wi-Fi



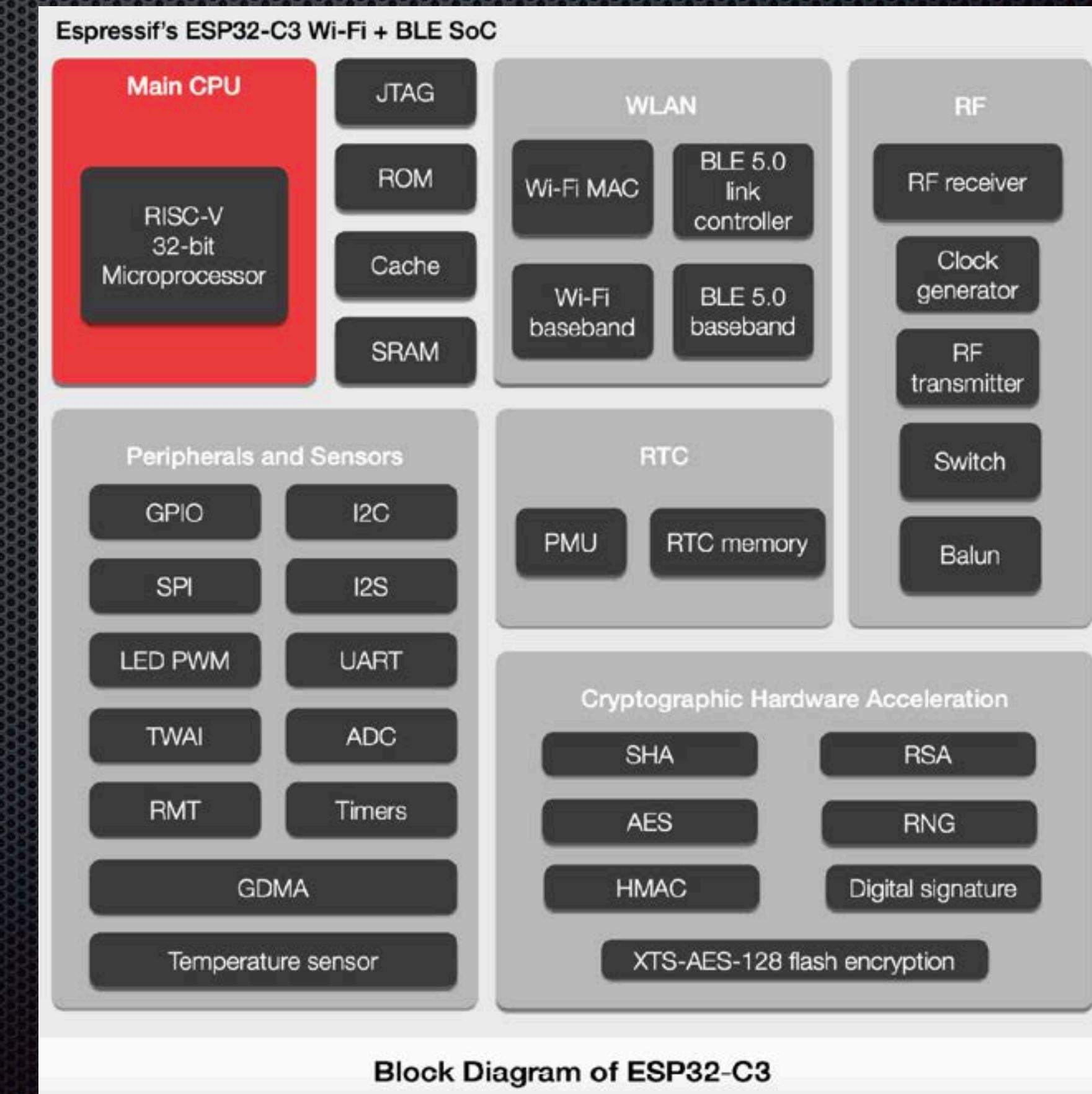
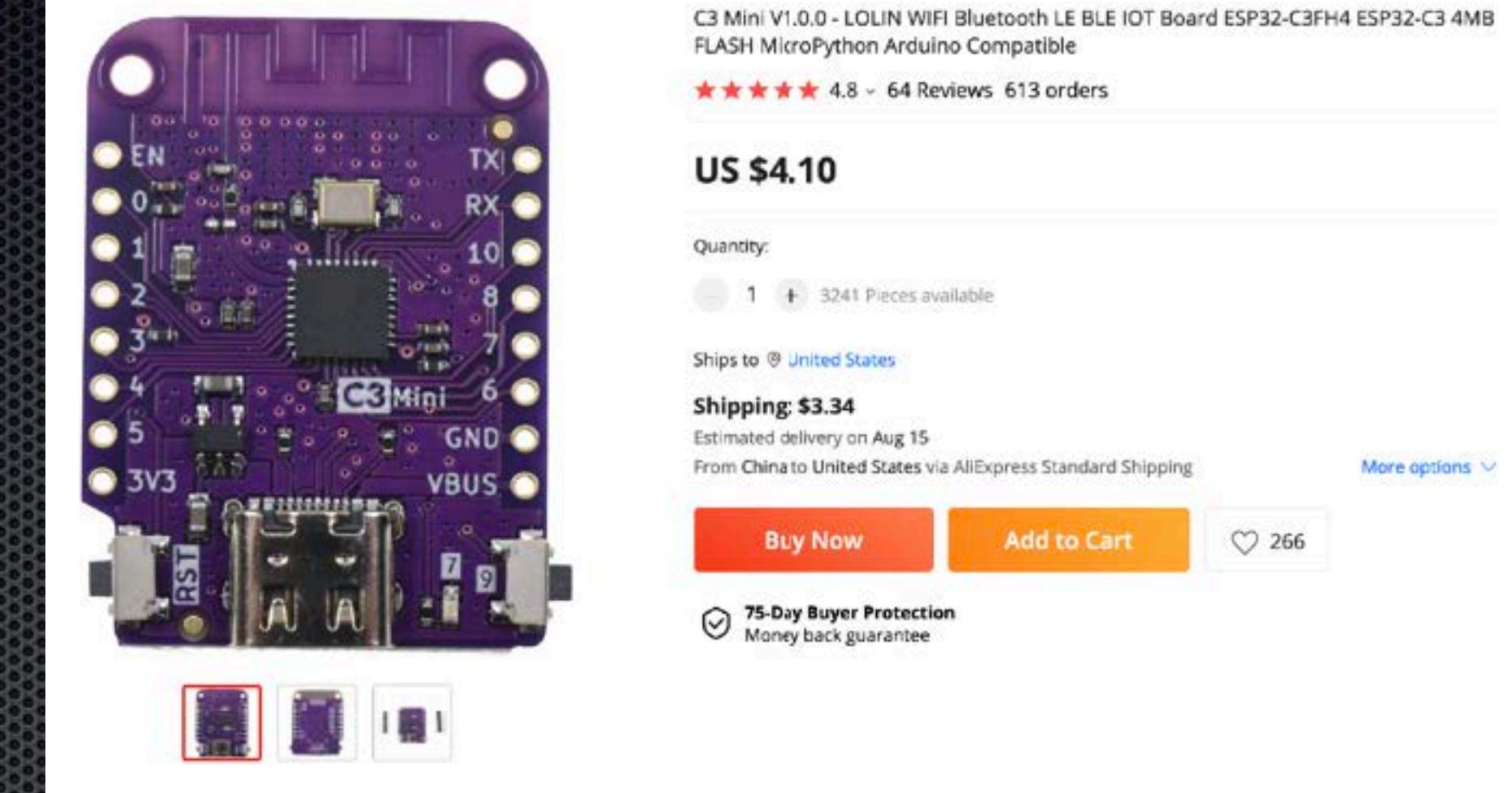


Future boards for hacking

Microcontrollers to pay attention to

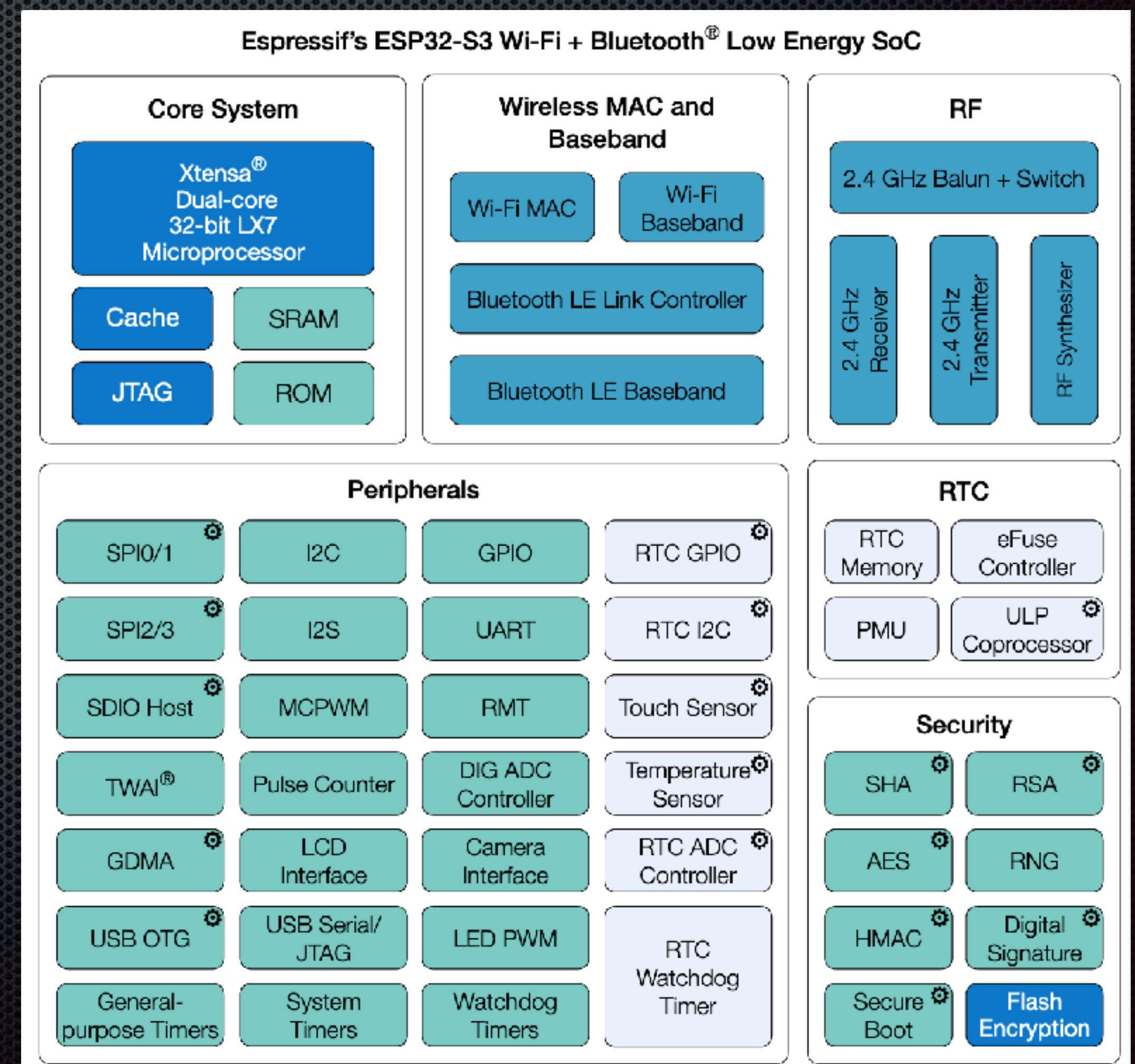
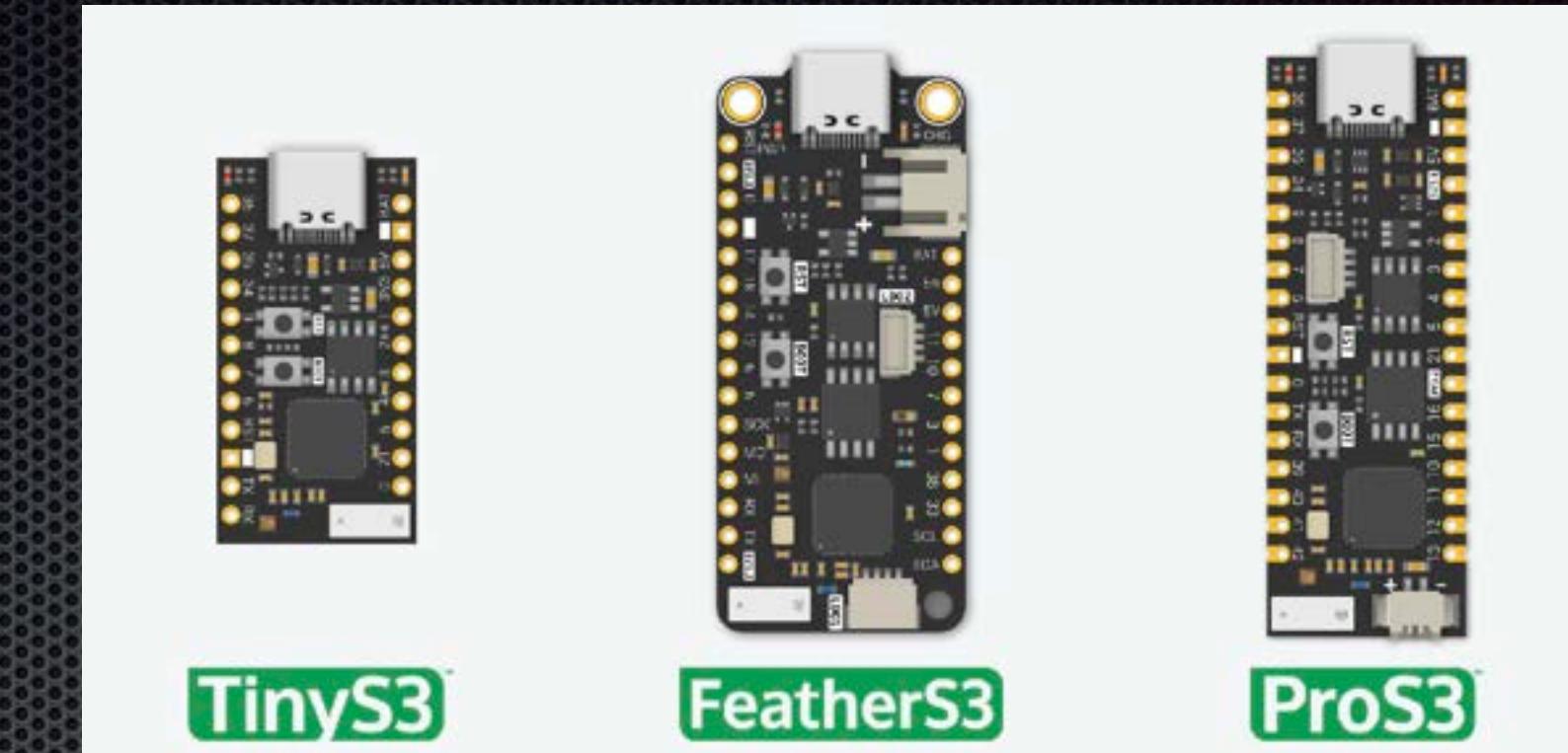
Esp32c3

- Supports 2.4 GHz Wi-Fi
- Supports Bluetooth 5 (LE)
- No native USB



Esp32s3

- New flagship model!
- Supports Bluetooth LE
- Supports 2.4 GHz Wi-Fi
- Supports native USB
- Supports the kitchen sink
- You can buy these now!



Esp32c5



ESP32-C5

2.4 and 5 GHz Dual-band Wi-Fi 6 SoC



2.4&5 GHz



Bluetooth 5

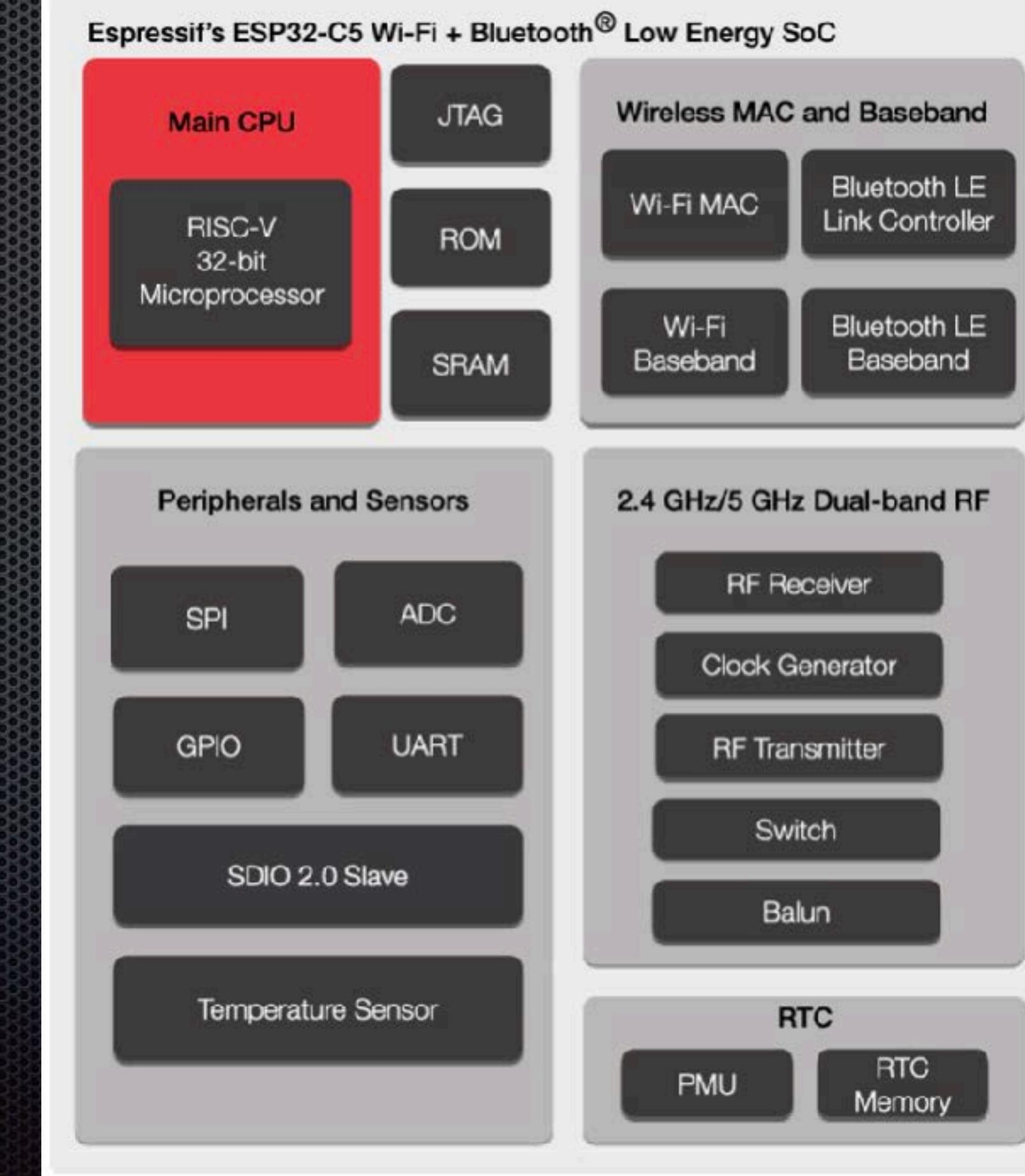


(LE)



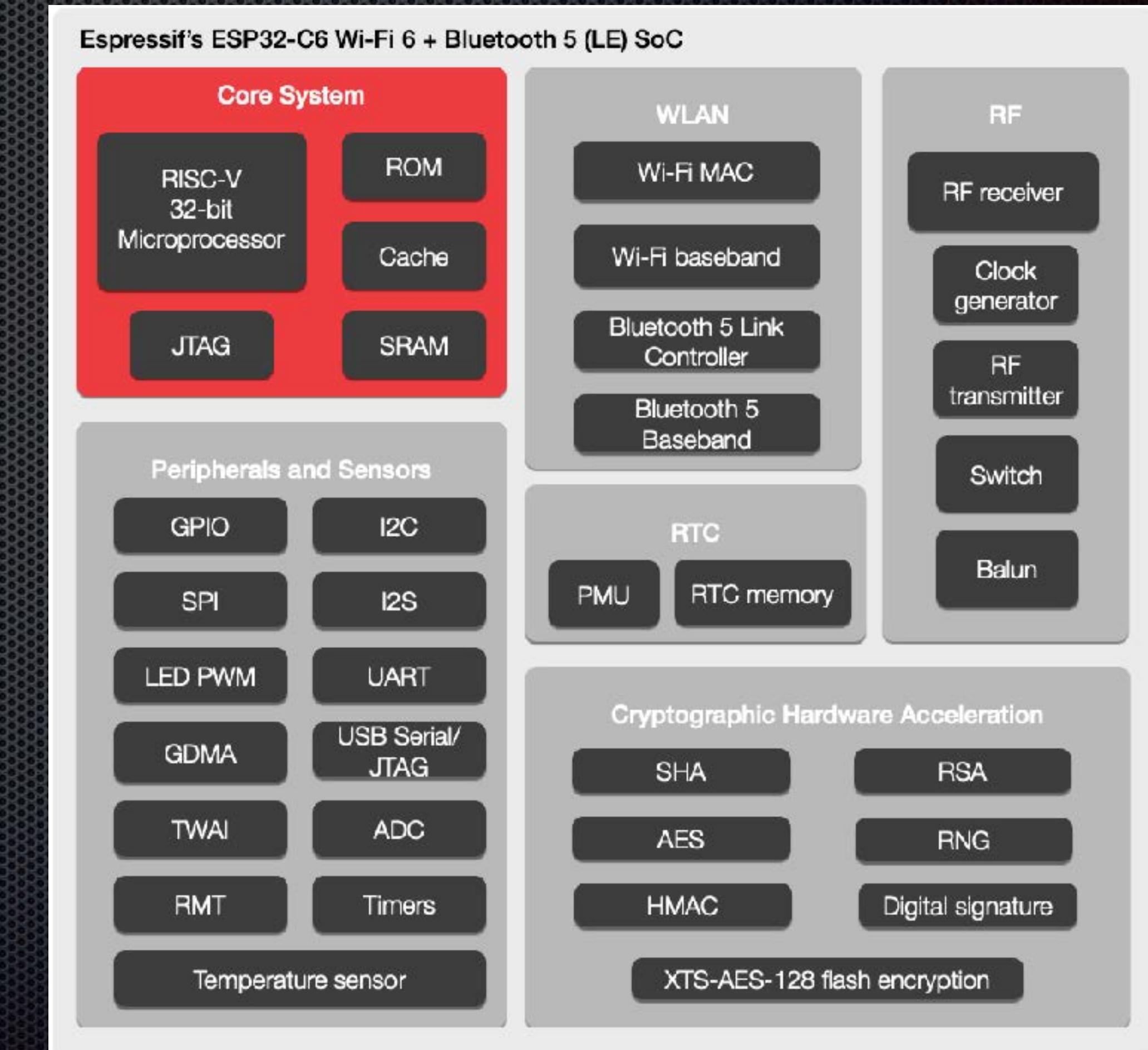
ESP32-C5

- First Espressif 5GHz microcontroller
- No native USB
- Supports Bluetooth LE



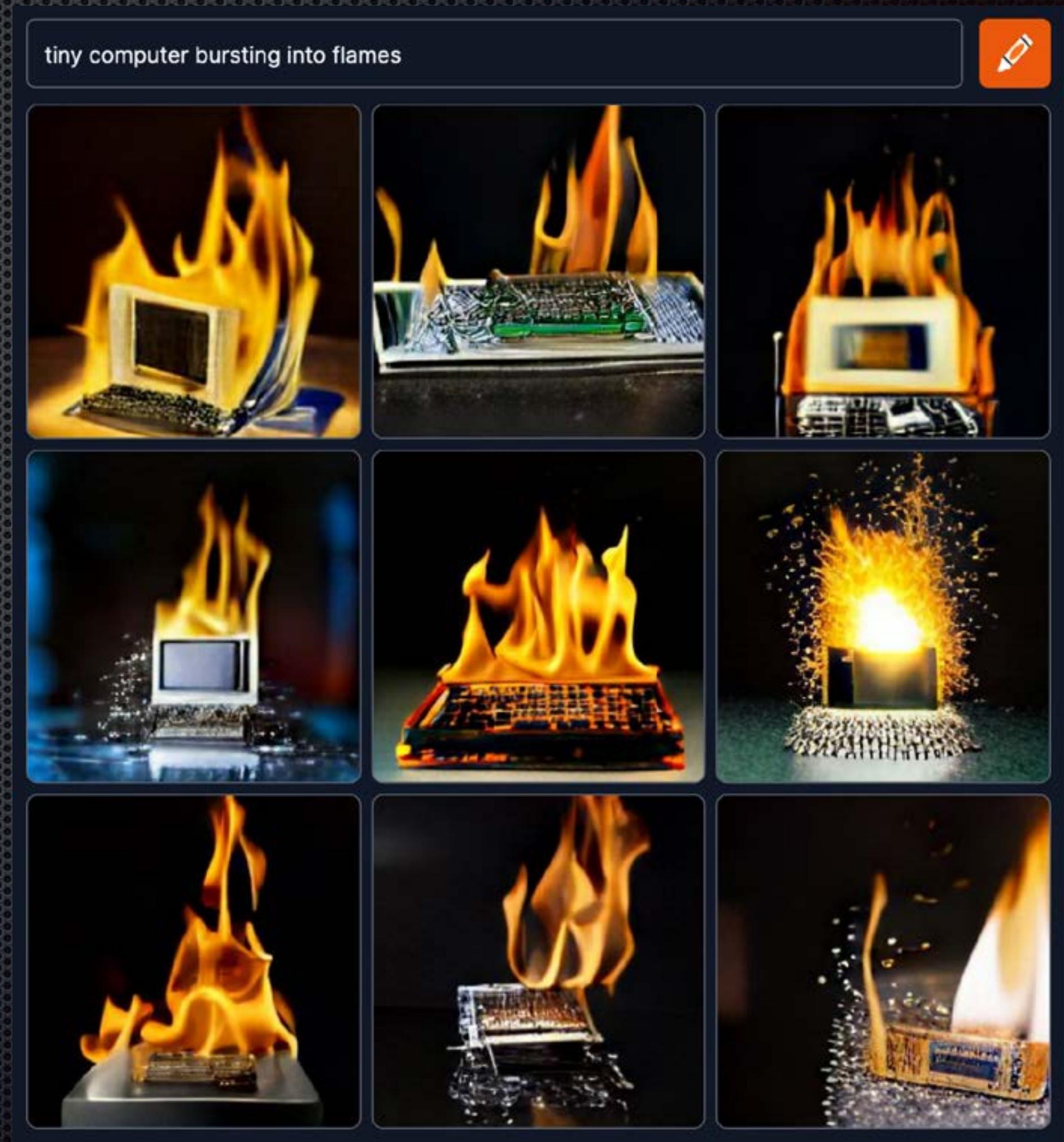
Esp32c6

- 2.4 GHz Wi-Fi 6 (802.11ax) radio also supports the 802.11b/g/n standard for backward compatibility
- Supports Bluetooth
- RISC-V 32 bit microprocessor
- Supports USB serial*



Takeaways

- I learned all this in 3 years
- Microcontrollers are more fun to use, abuse, & destroy than a Raspberry Pi
- You don't need to be a computer scientists to try these projects
- You can learn meaningful attacks for less than \$5
- There is a place for every level of skill in hardware hacking



Thanks for coming!

Find more of my content at hack.gay
or follow me on Twitter @KodyKinzie

Support our team - Buy a USB Nugget at [HakCat.com!](https://HakCat.com)

