$5 Cyberweapons & how to use them

Introduction to Offensive Hacking with Microcontrollers

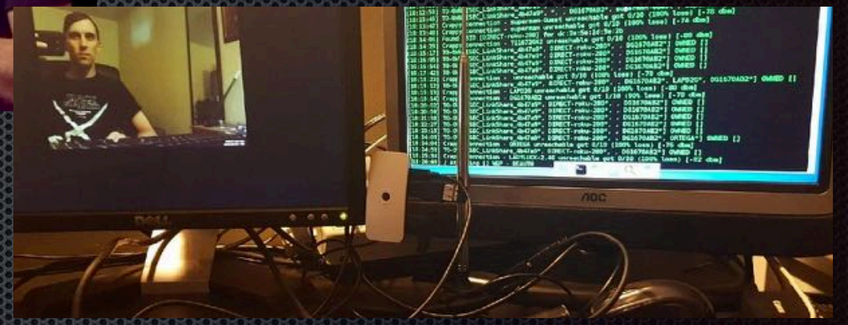
Introduction

- 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

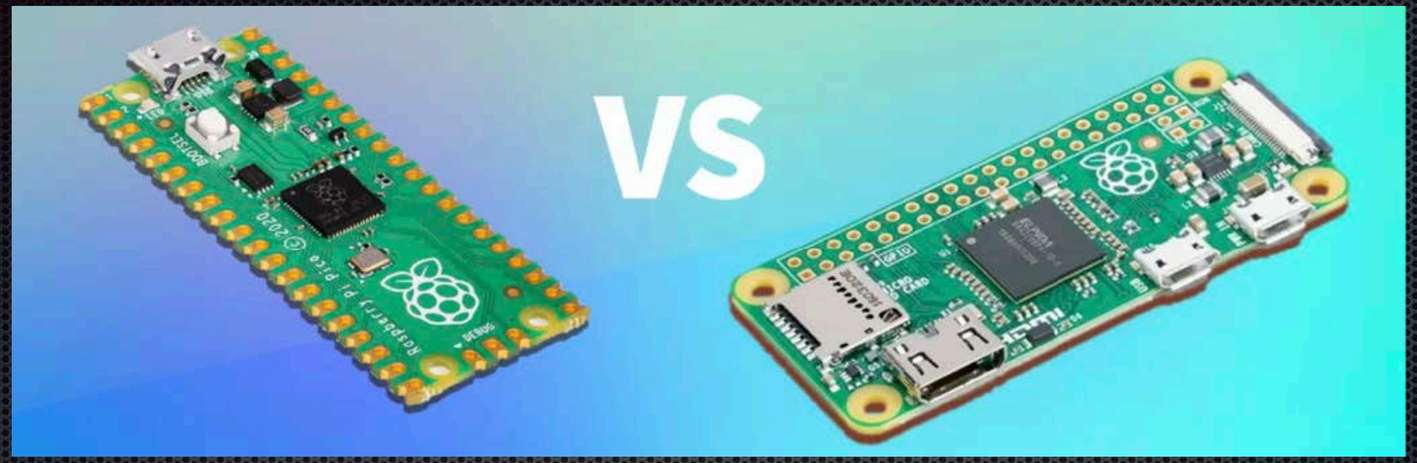
Current Project

- 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**



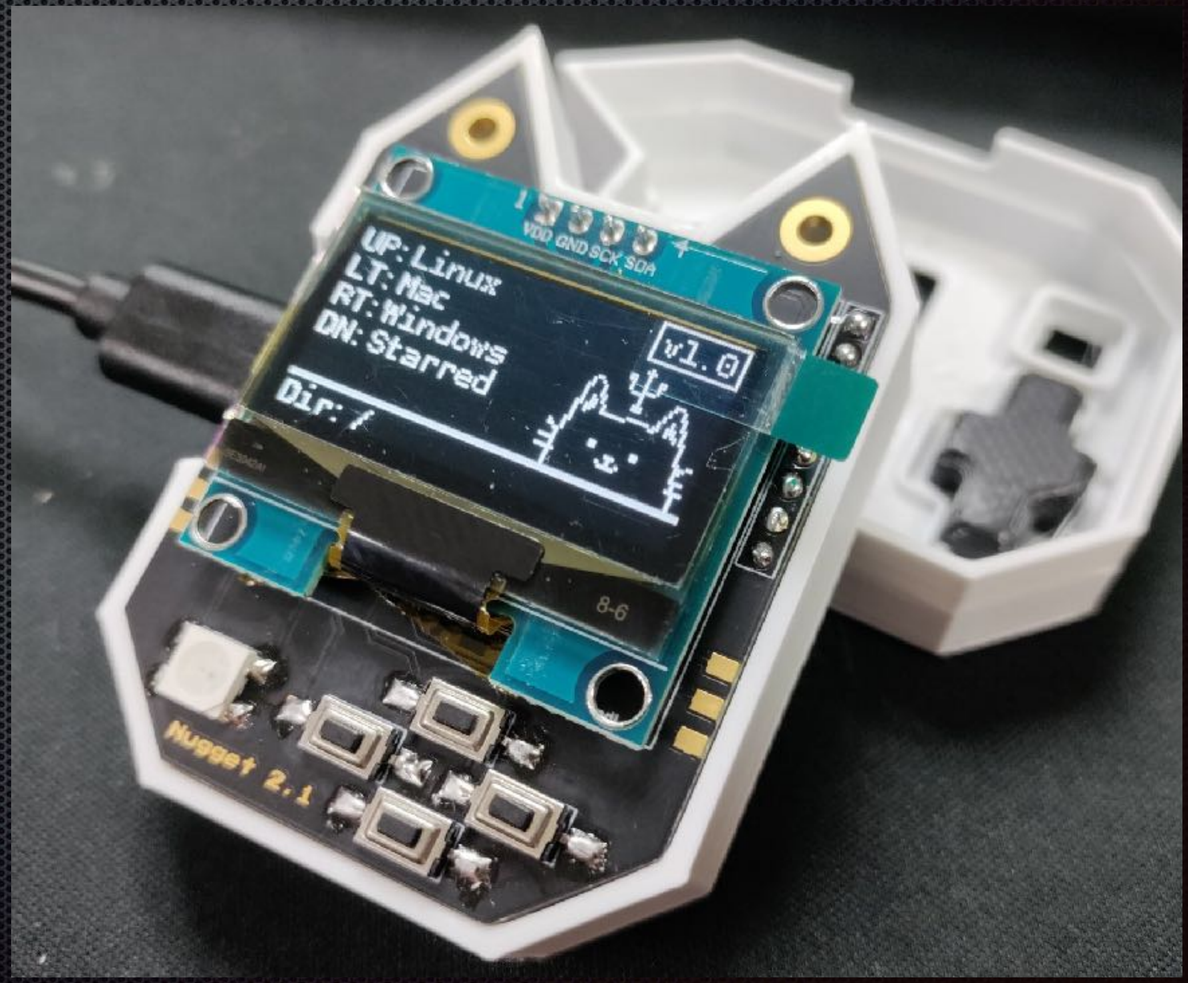
Source: @AshPuckettB2B howchoo.com

- 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 Rasperry Pi OS & more
- Includes HDMI, USB, & microSD card
- Costs $200 (on Ebay)

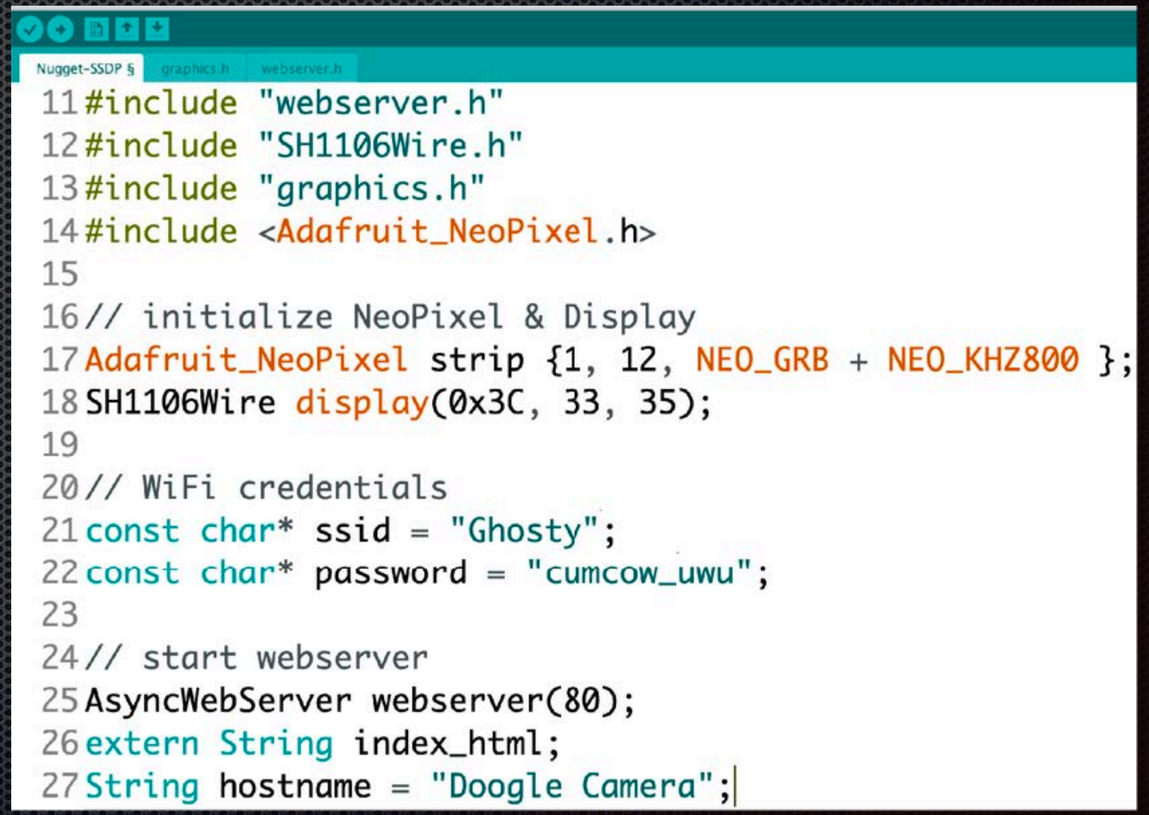
Skills required for hacking

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



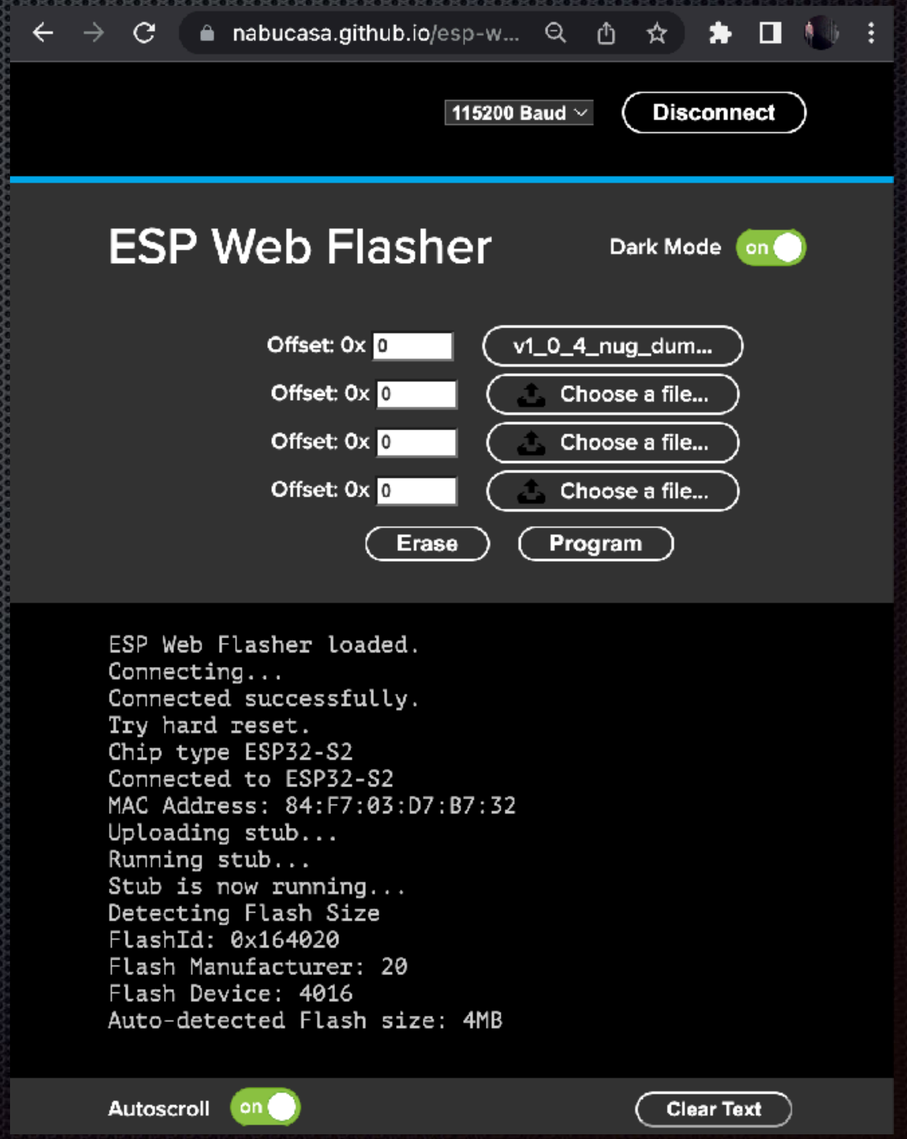
Skills required for Developing

- 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



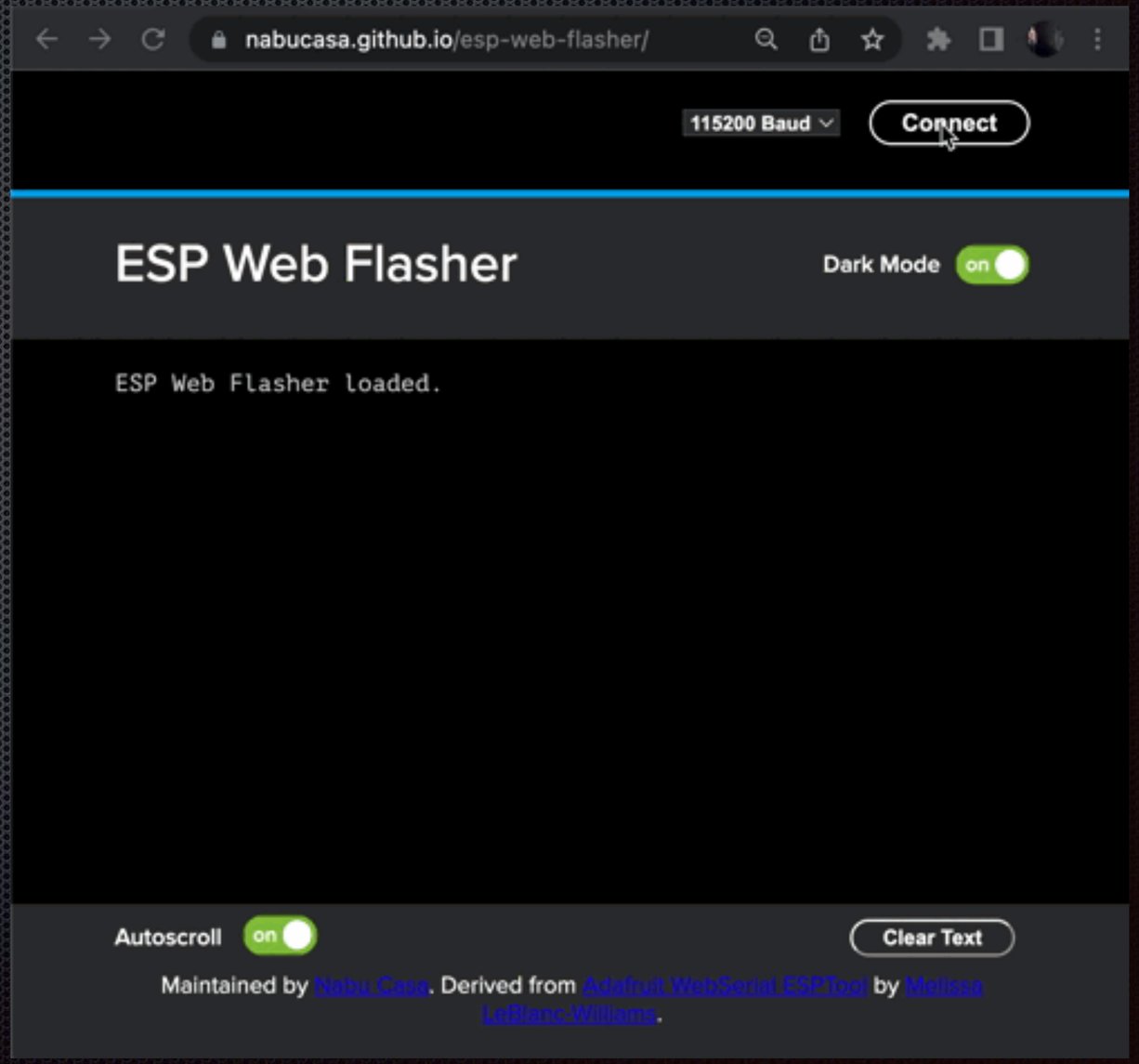
3 ways to program a microcontroller

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



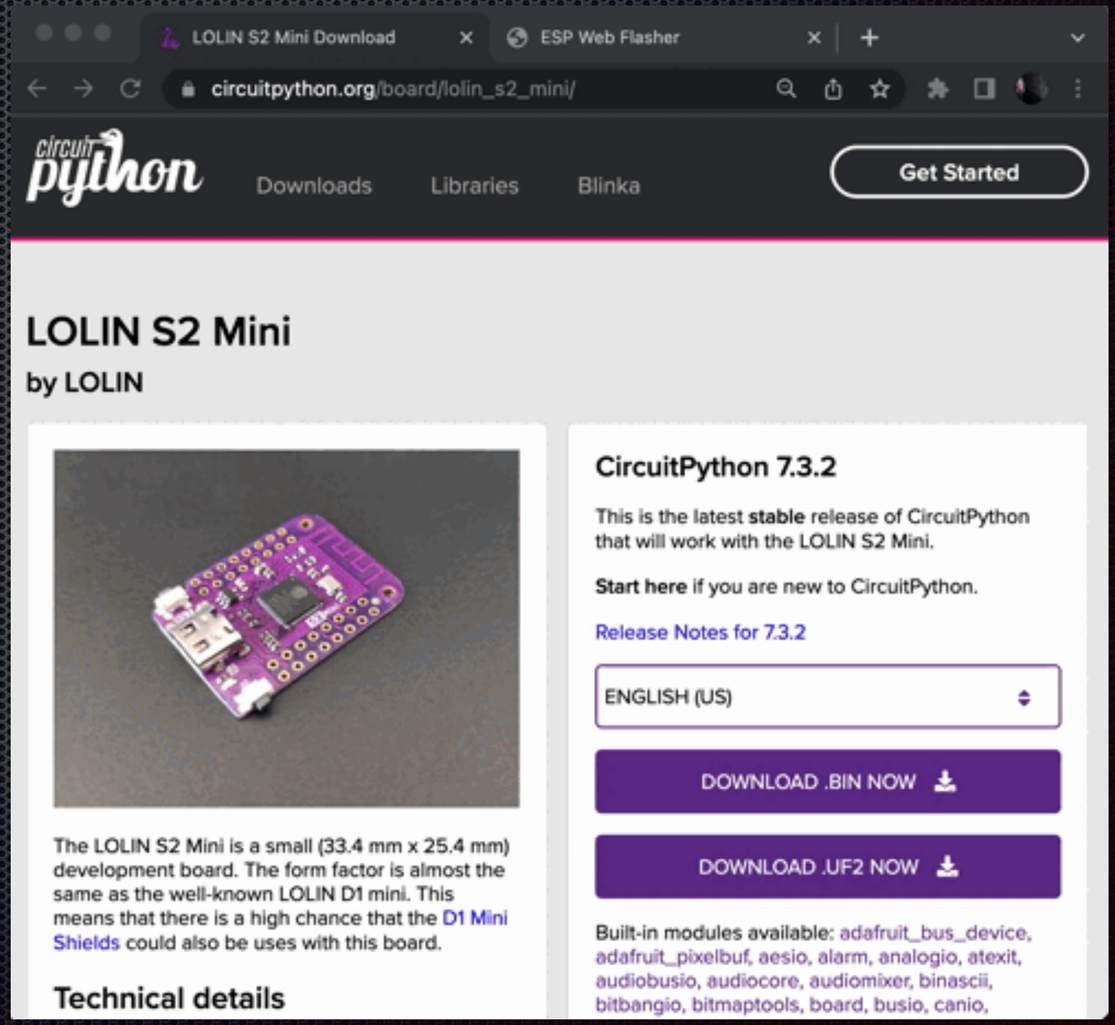
Flashing a Project via Chrome

- 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



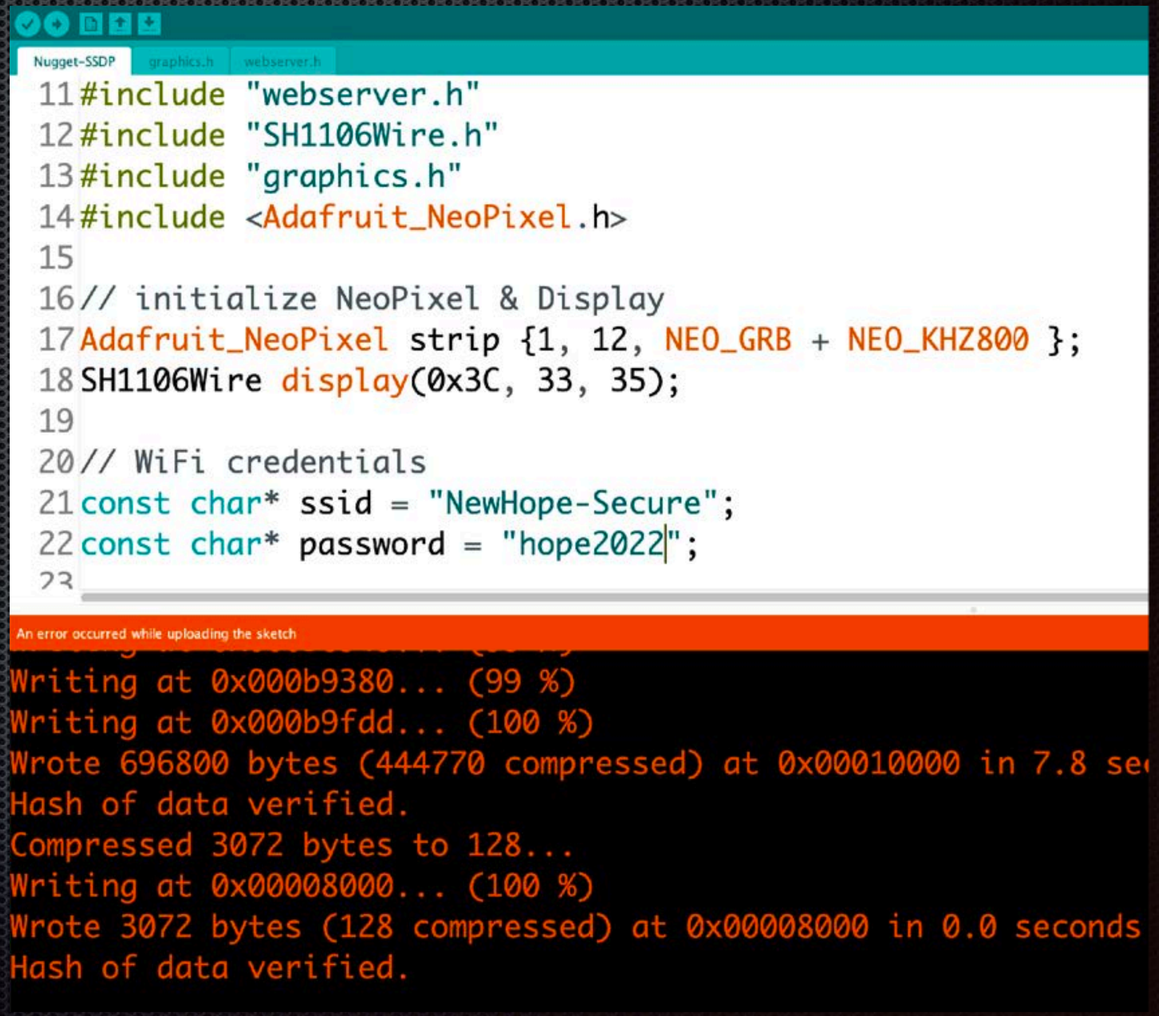
Flashing CircuitPython & Programming

- 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!



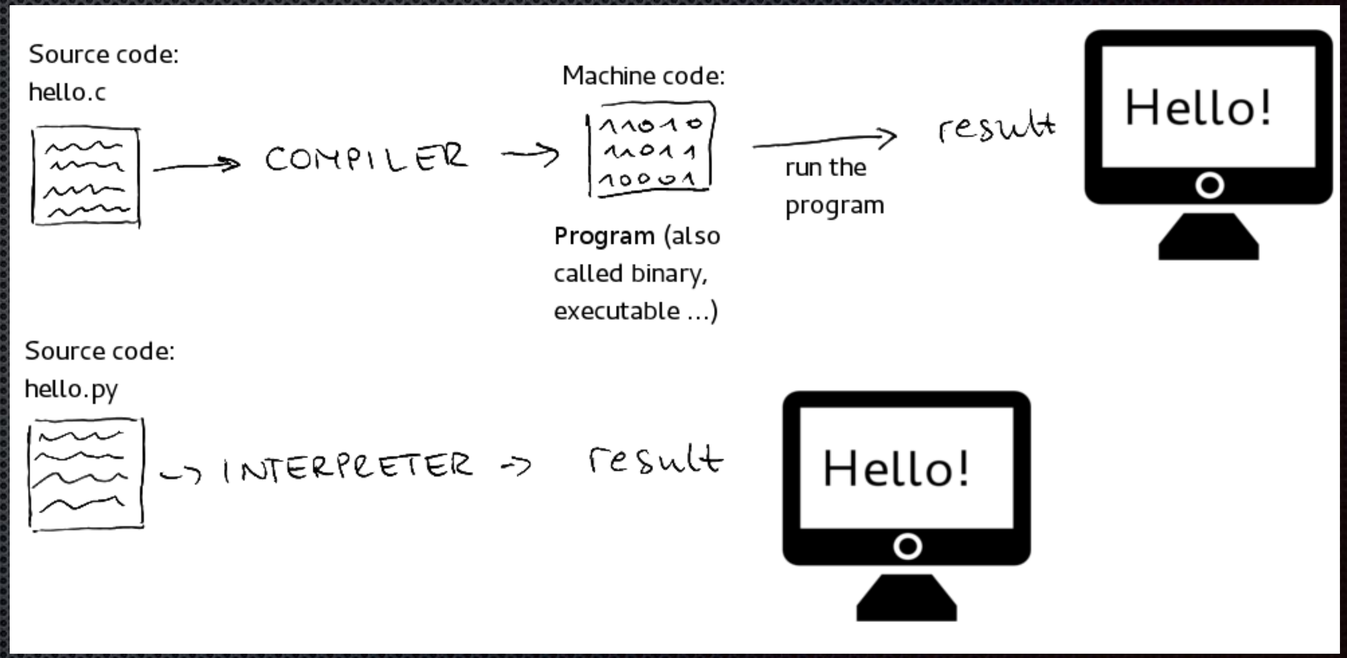
Programming & Flashing via Arduino

- 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



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

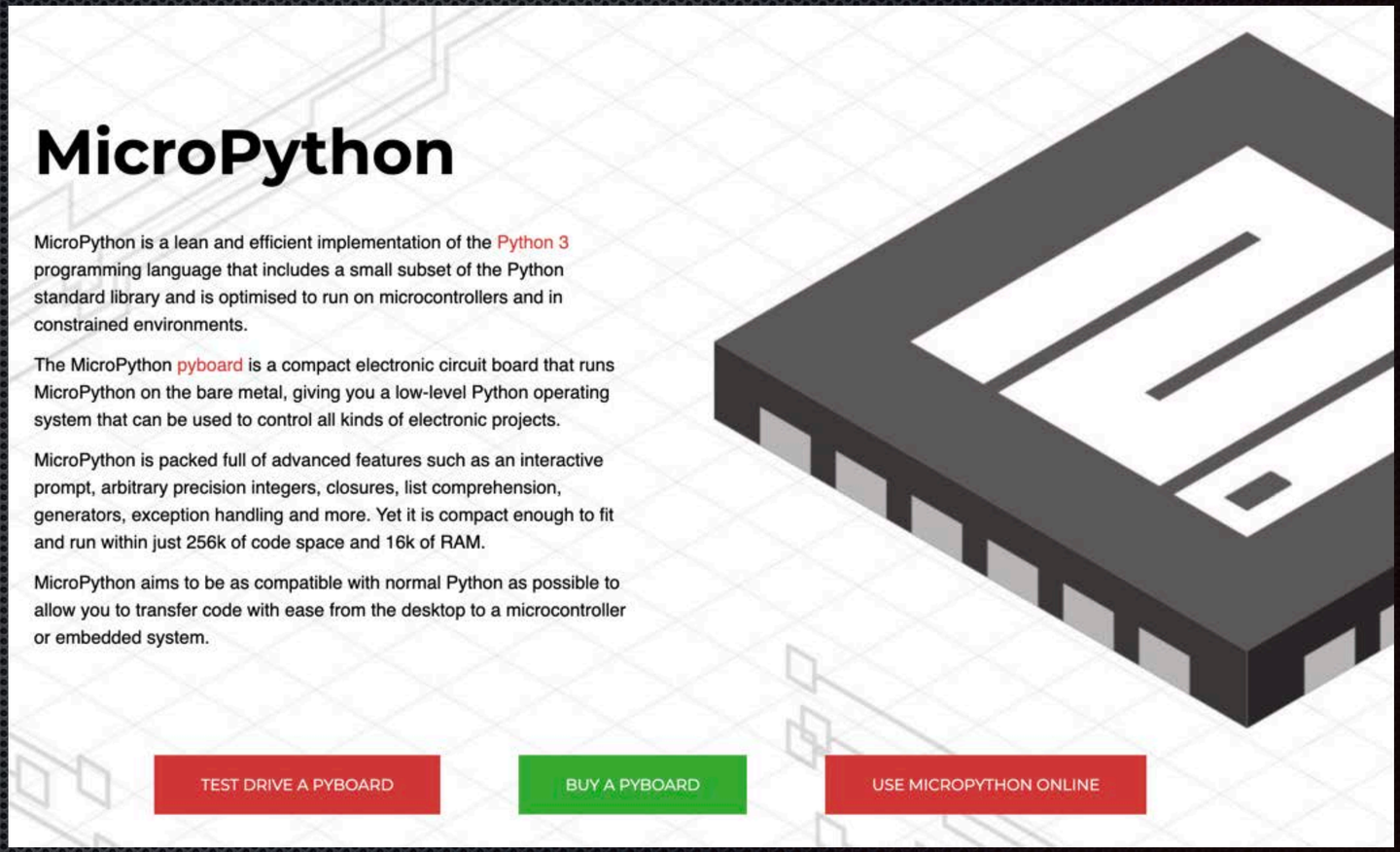


CircuitPython

- 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

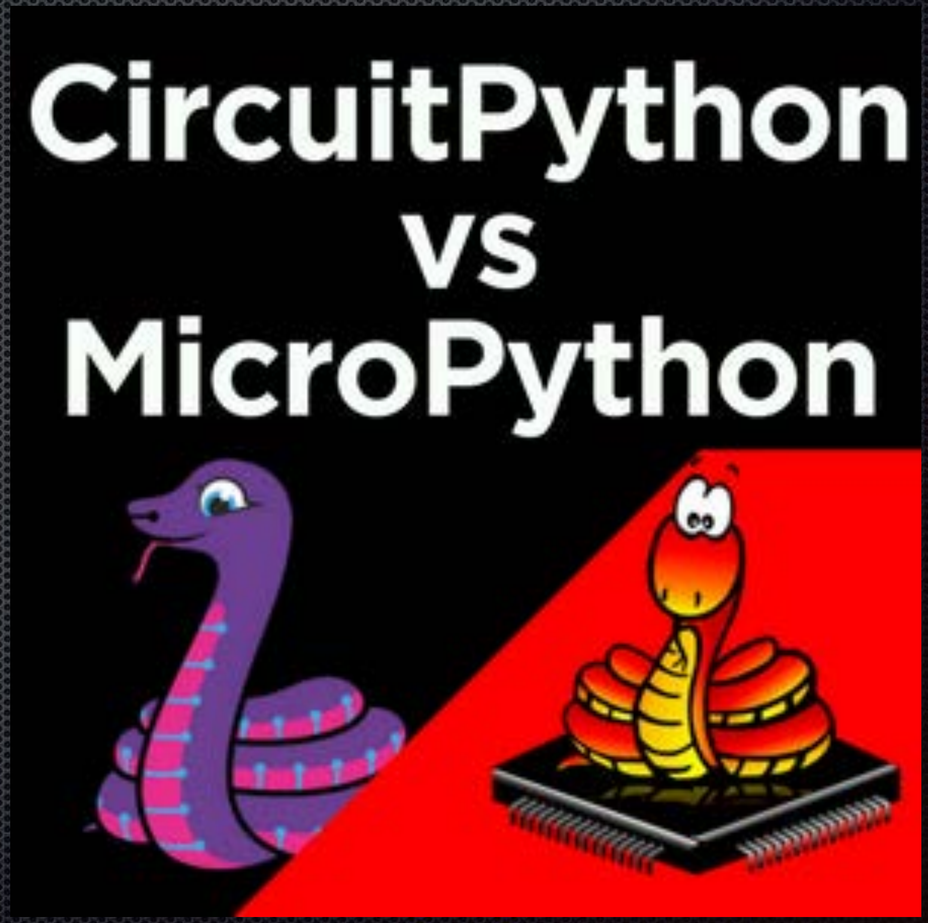
MicroPython

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



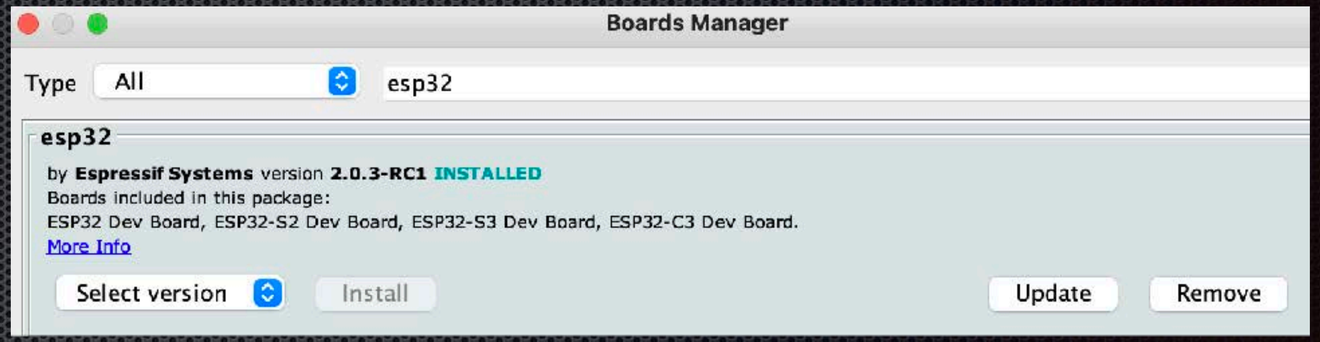
Why CircuitPython over MicroPython

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



Arduino

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




```
20// WiFi credentials
21const char* ssid = "NewHope-Secure";
```

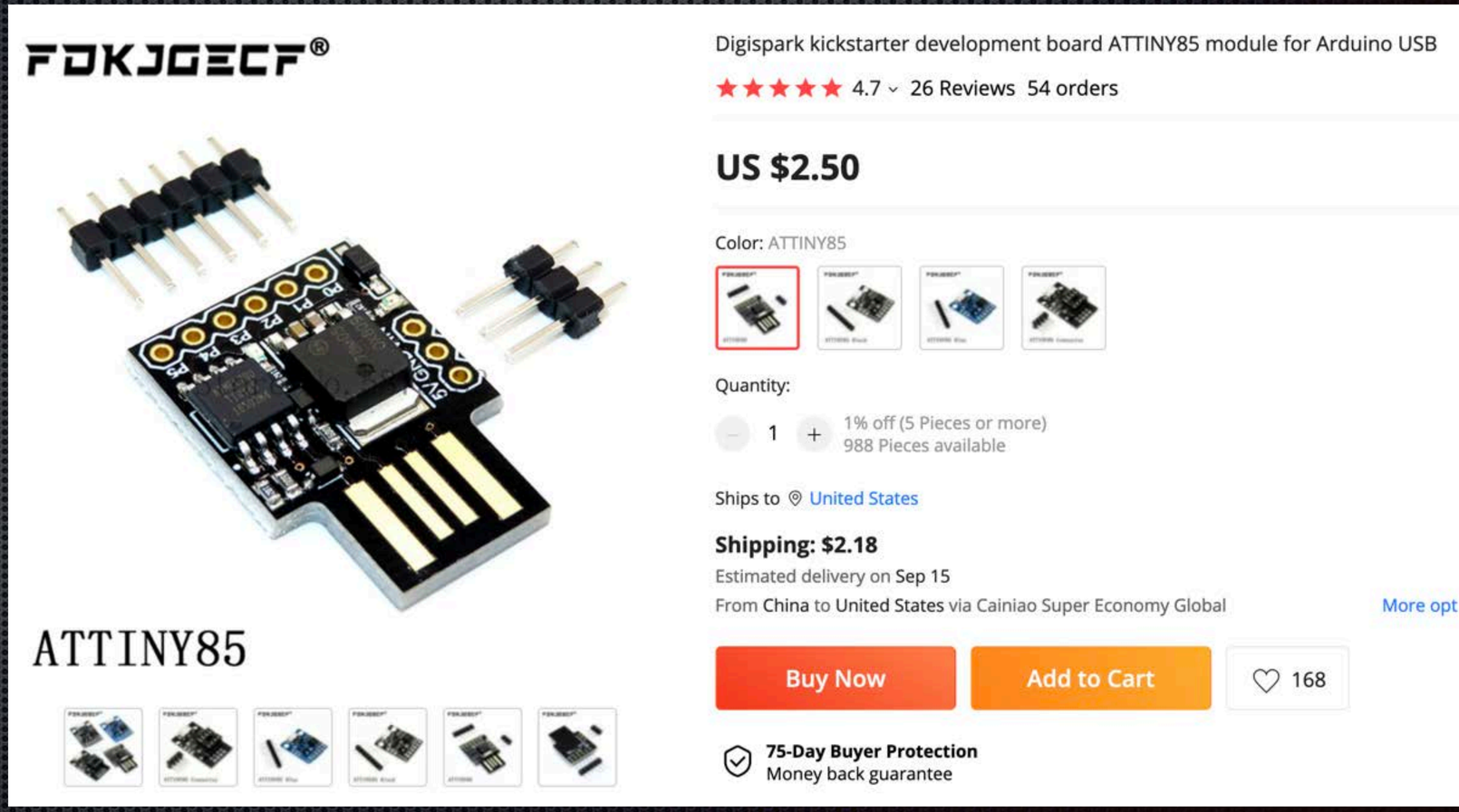
```
An error occurred while uploading the sketch
Hash of data verified.
Compressed 3072 bytes to 128...
Writing at 0x00008000... (100 %)
Wrote 3072 bytes (128 compressed) at 0x00008000 in 0.0 seconds (effective 528.9 kbit/s)...
Hash of data verified.

Leaving...
WARNING: ESP32-S2FNR2 chip was placed into download mode using GPIO0.
esptool.py can not exit the download mode over USB. To run the app, reset the chip manually.
To suppress this note, set --after option to 'no_reset'.
An error occurred while uploading the sketch
```

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!



Attiny85 BadUSB

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

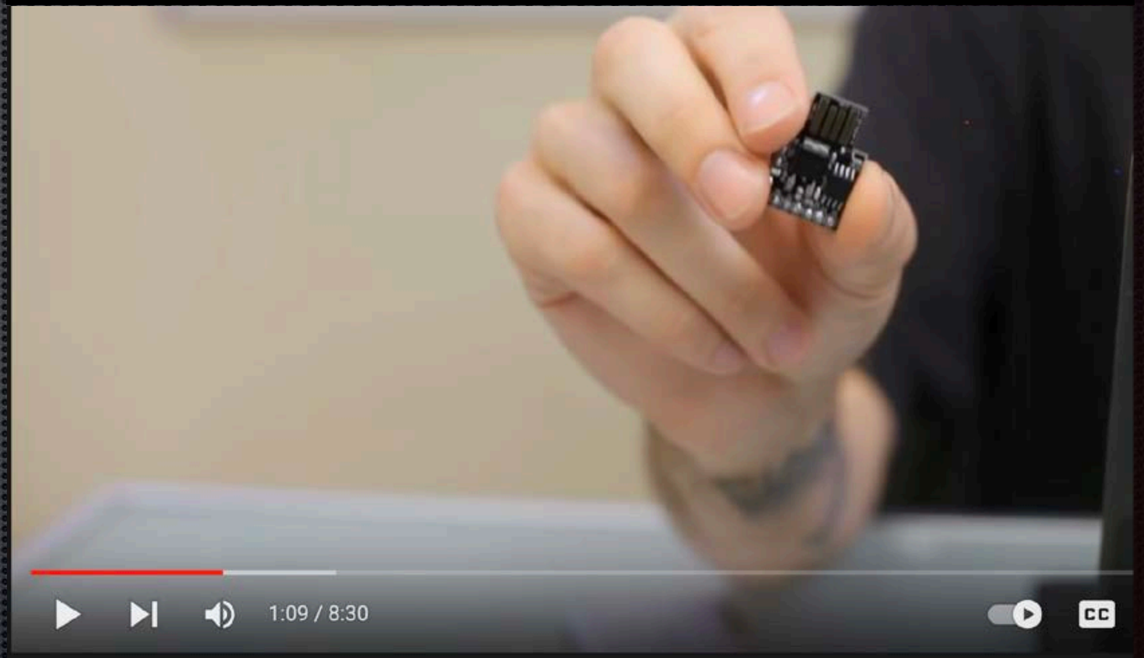
HOW TO

Run USB Rubber Ducky Scripts on a Super Inexpensive Digispark Board

BY KODY 11/22/2019 4:43 PM 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-ducky-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

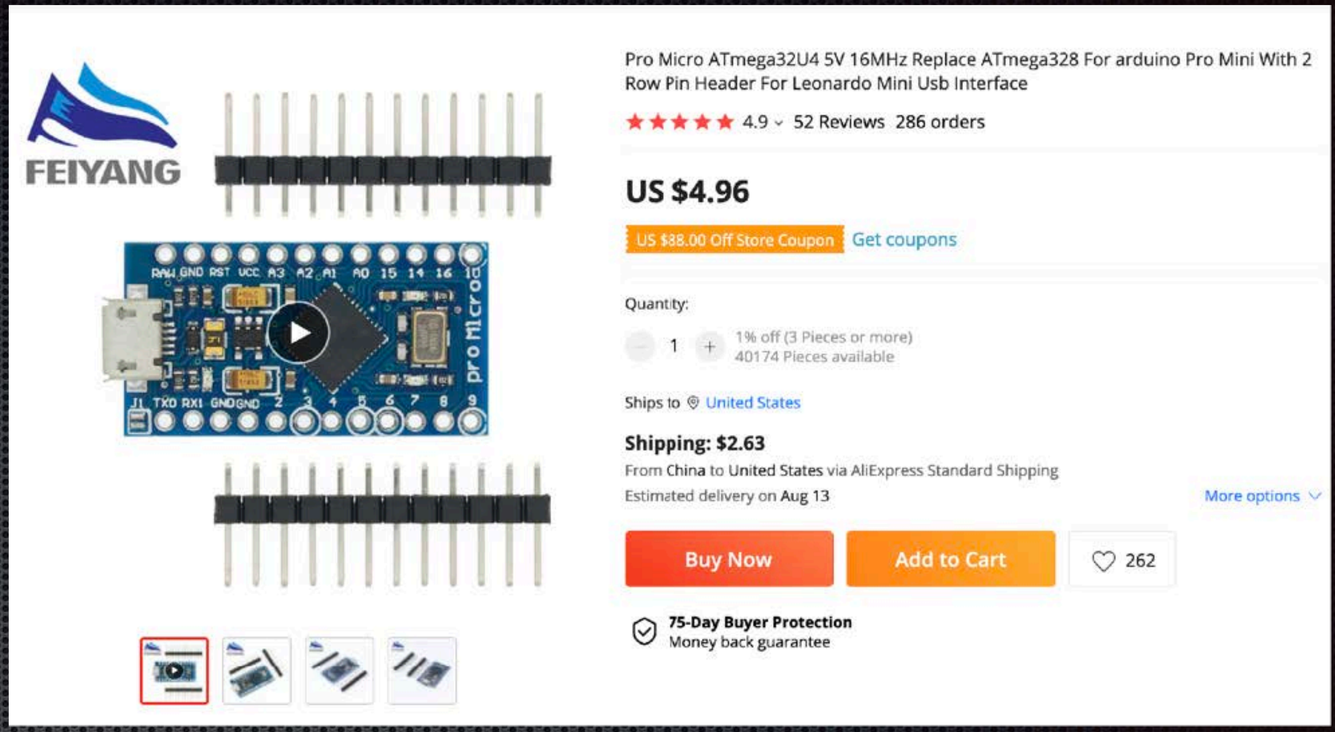
- Moves the mouse to prevent computer from locking
- Flashes via Arduino IDE
- Can also click
- Makes a good auto-clicker
- Actually works pretty well

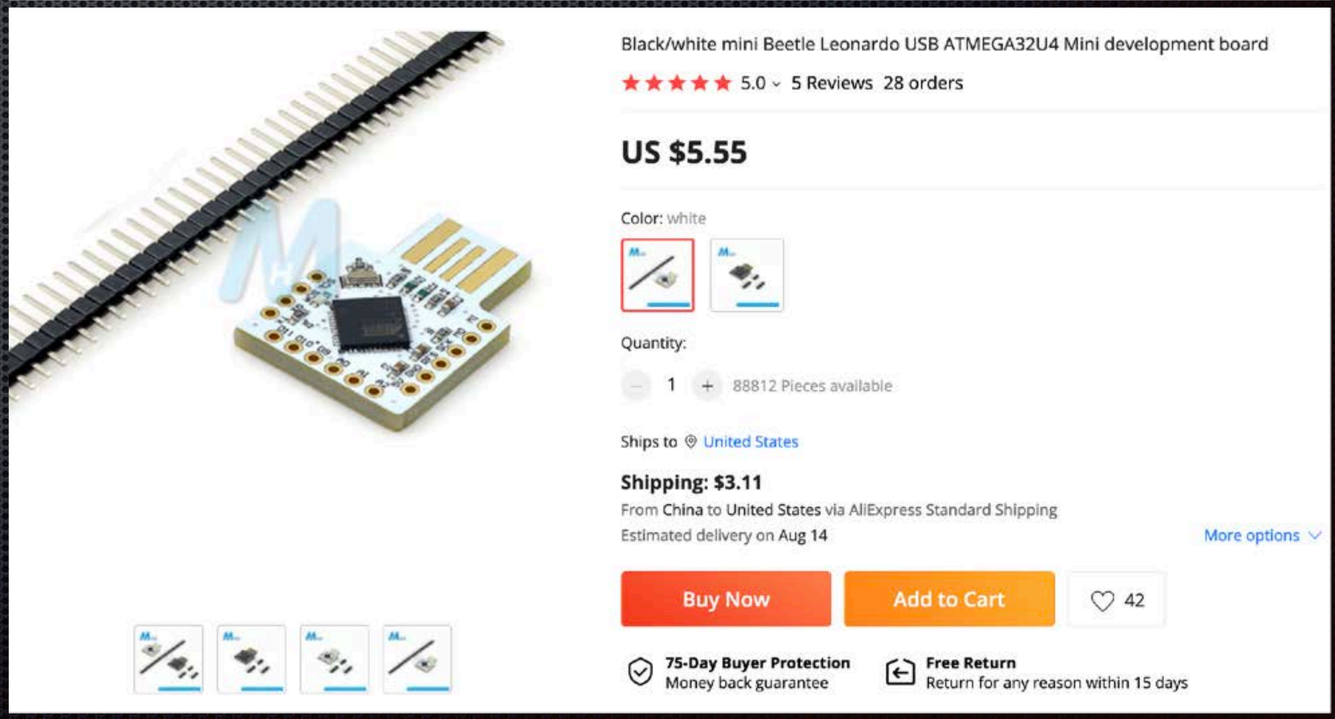
https://null-byte.wonderhowto.com/how-to/create-usb-mouse-jiggler-keep-target-computer-from-falling-asleep-prank-friends-too-0236798/

https://youtu.be/x4Ap-ypWdFo

Atmega32u4

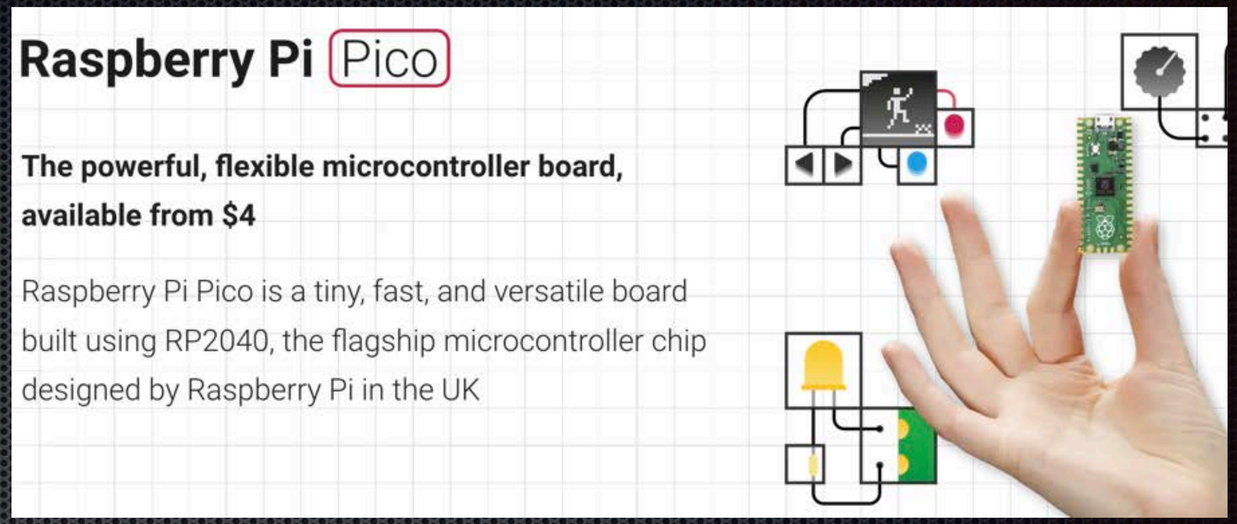
- Faster than the ATTiny
- Similar capabilities but less frustrating to work with
- Must be pre-flashed with payloads
- Only works as USB device, doesn't mount as USB storage
- No wireless anything, we'll come back to this

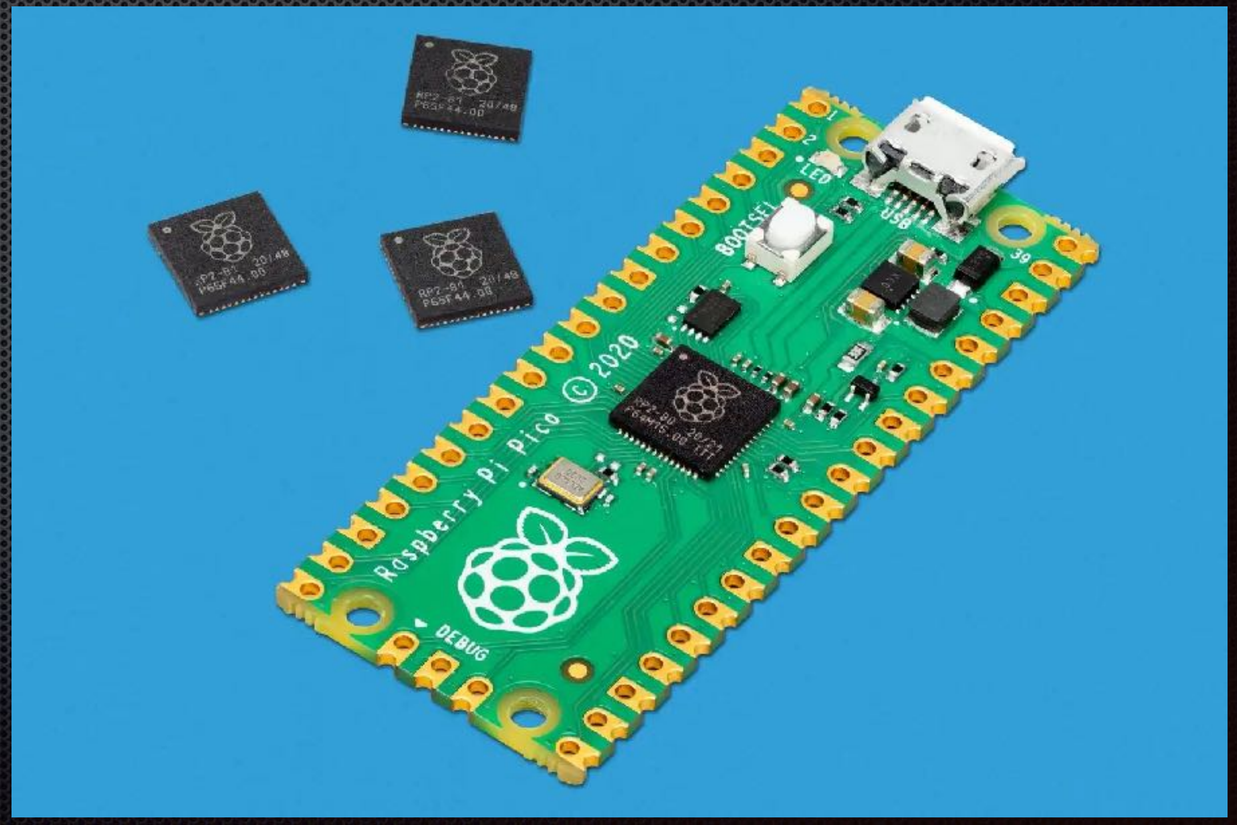




Raspberry Pi Pico

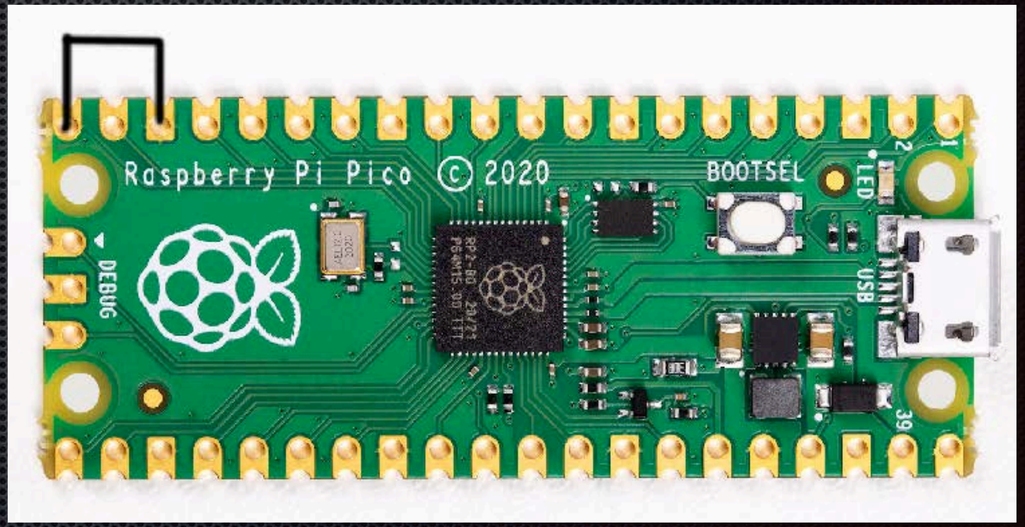
- Based on RP2040
- Native USB!
- Supports CircuitPython
- Supports Arduino IDE
- Mounts as USB drive
- No Wireless





PicoDucky

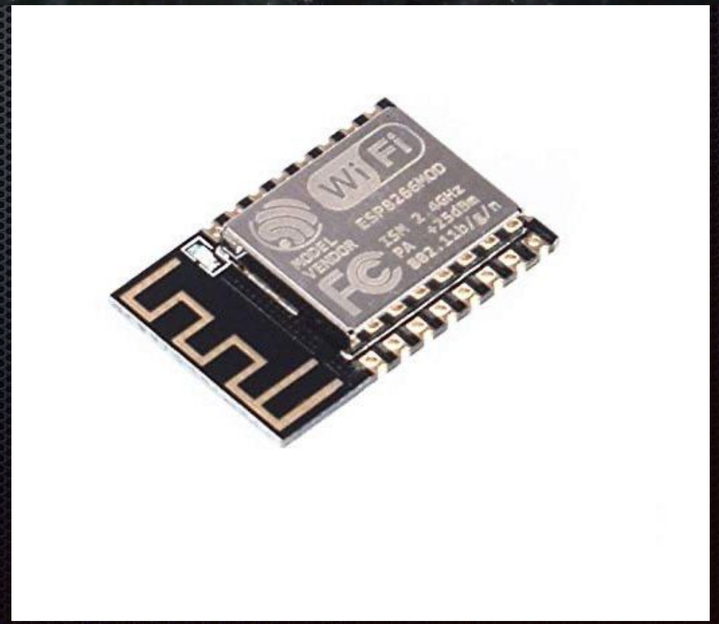
- Awesome CircuitPython project to parse DuckyScript & deliver payloads
- Created by Dave Bailey
- Mounts as USB drive to drag & drop payloads
- Supports multiple keyboards
- No screen or buttons to interface with
- Requires you to jump connections to switch between program & attack mode



https://github.com/dbisu/pico-ducky

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%

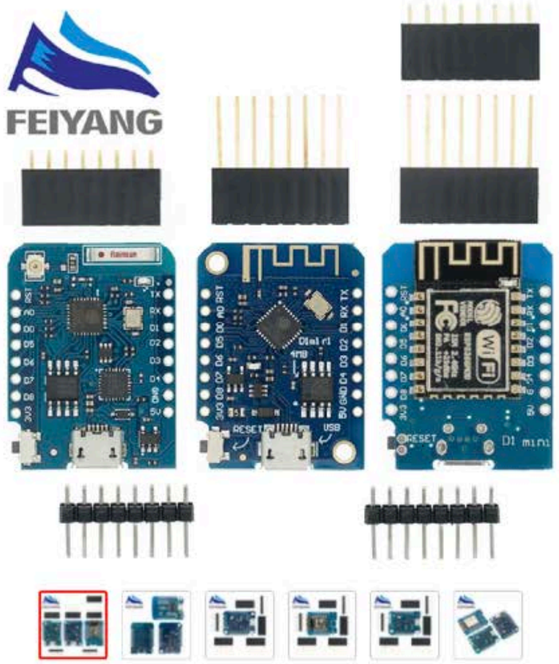
Color: NodeMcu V2 CP2102

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 | ♡ 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 | ♡ 4865

ESP8266 Deauther

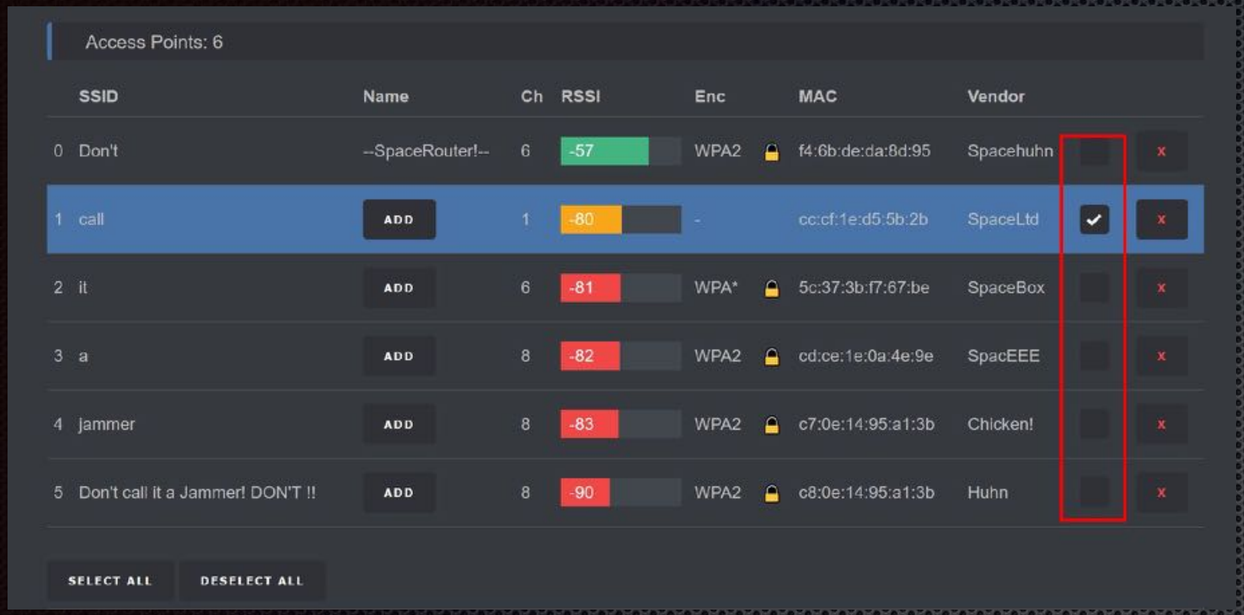
- Runs on the ESP8266
- Flash via binary file or Arduino IDE
- Offers a web & serial interface
- Scan for Wi-Fi Access Points
- Scan for Wi-Fi Clients
- Jam Wi-Fi Clients (protocol based jammer)
- Create fake AP's (Trick clients into trying to join)
- Create fake probe frames (Wi-Fi Pineapple detector)

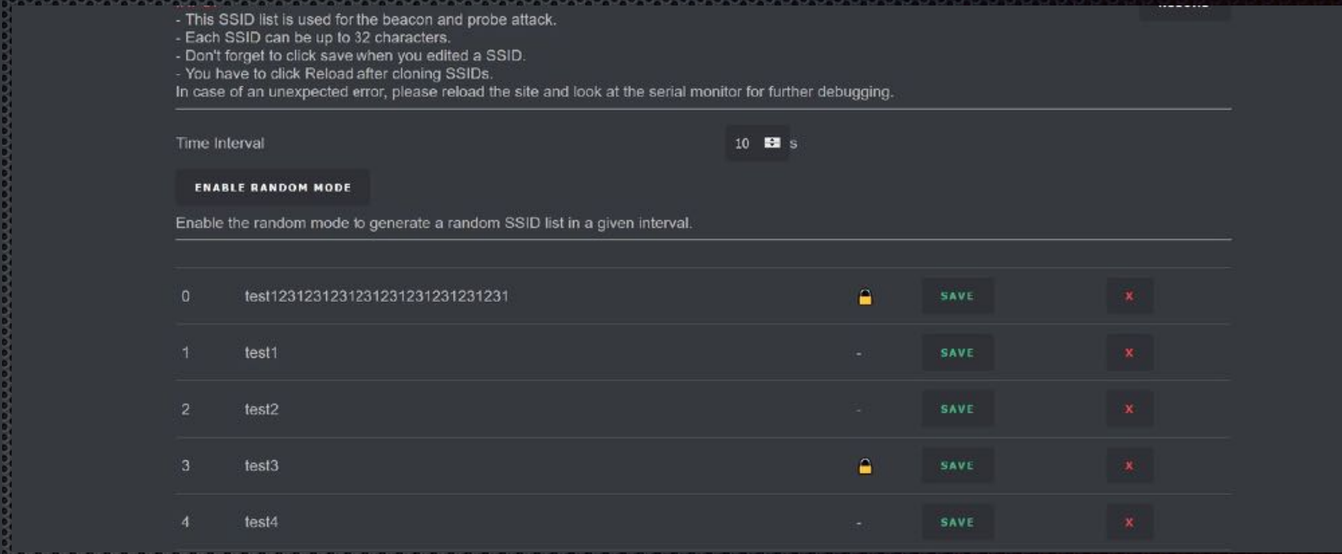
https://null-byte.wonderhowto.com/how-to/create-usb-mouse-jiggler-keep-target-computer-from-falling-asleep-prank-friends-too-0236798/

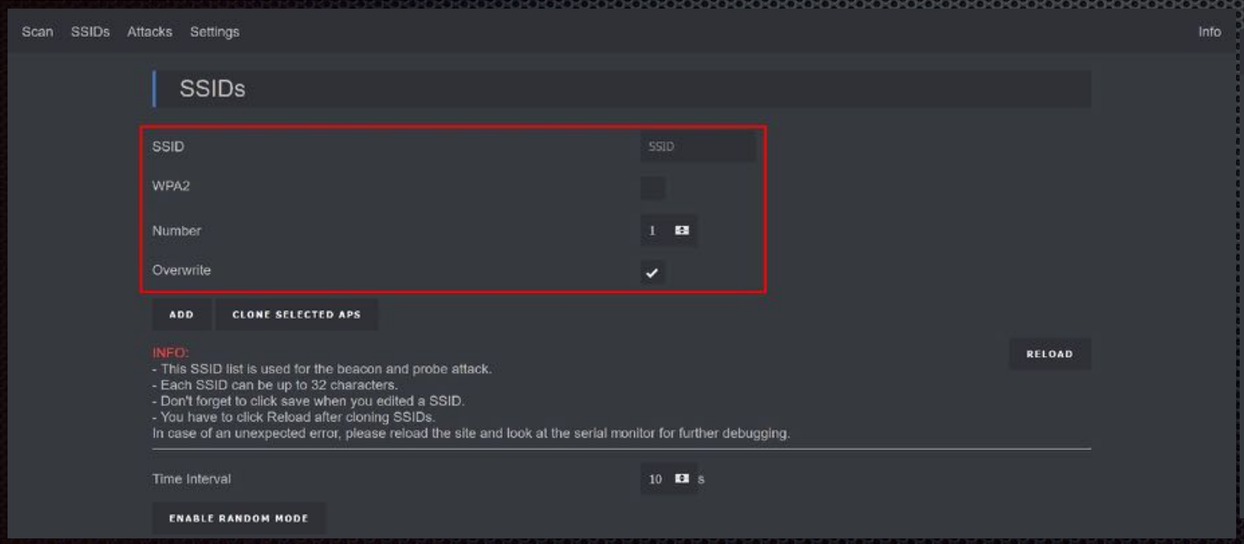
Feature	Version 2	Version 3
Web Interface	✅	
Display support	✅	
Serial Command Line	✅	✅
Scanner	✅	✅
Deauth attack	✅	✅
Beacon attack	✅	✅
Probe attack	✅	✅
Huhnitor support		✅
Signal strength scanner		✅
Authentication scanner		✅
Rogue AP		✅

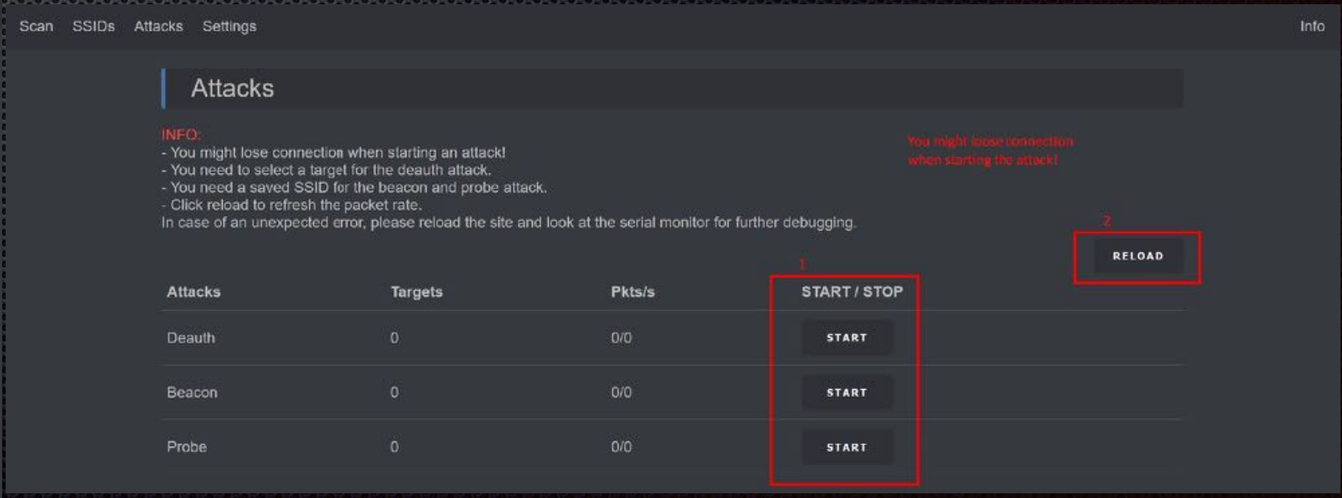
https://youtu.be/x4Ap-ypWdFo

ESP8266 Deauther Web Interface









ESP8266 Deauther V3

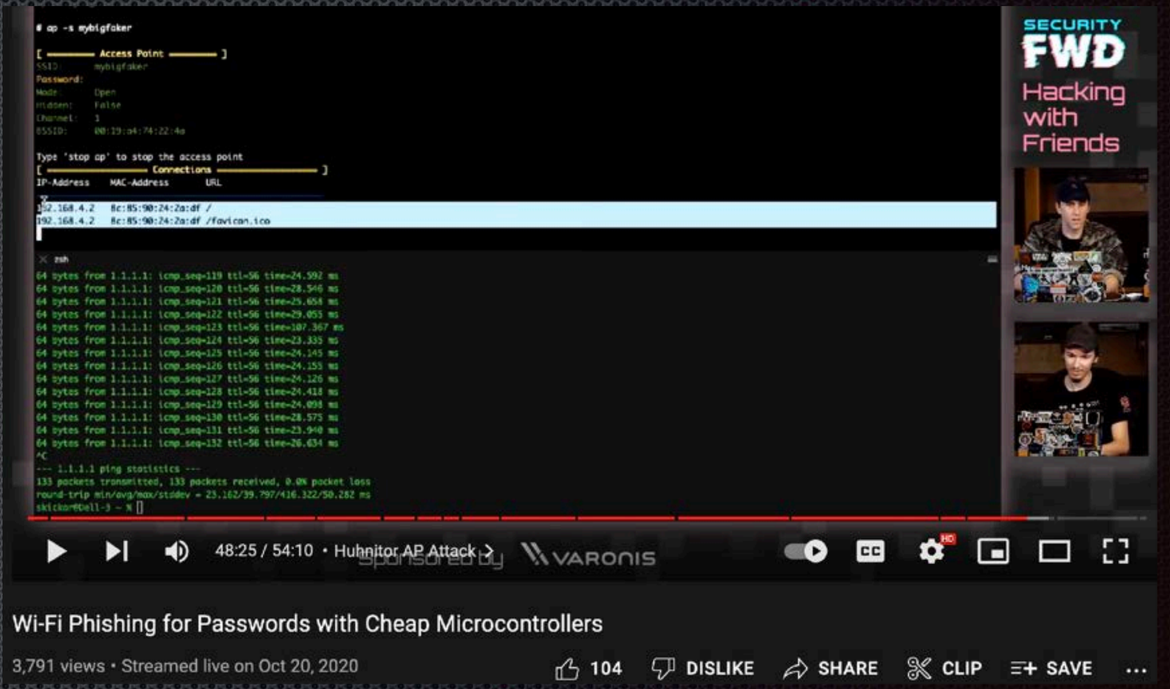
- Serial-only version of the Wi-Fi Deauther
- Execute advanced attacks with the radio free
- Supports Wi-Fi Phishing!
- Supports Rogue AP creation (no data)
- Supports beacon swarm attack

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

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 Wi-Fi Phishing

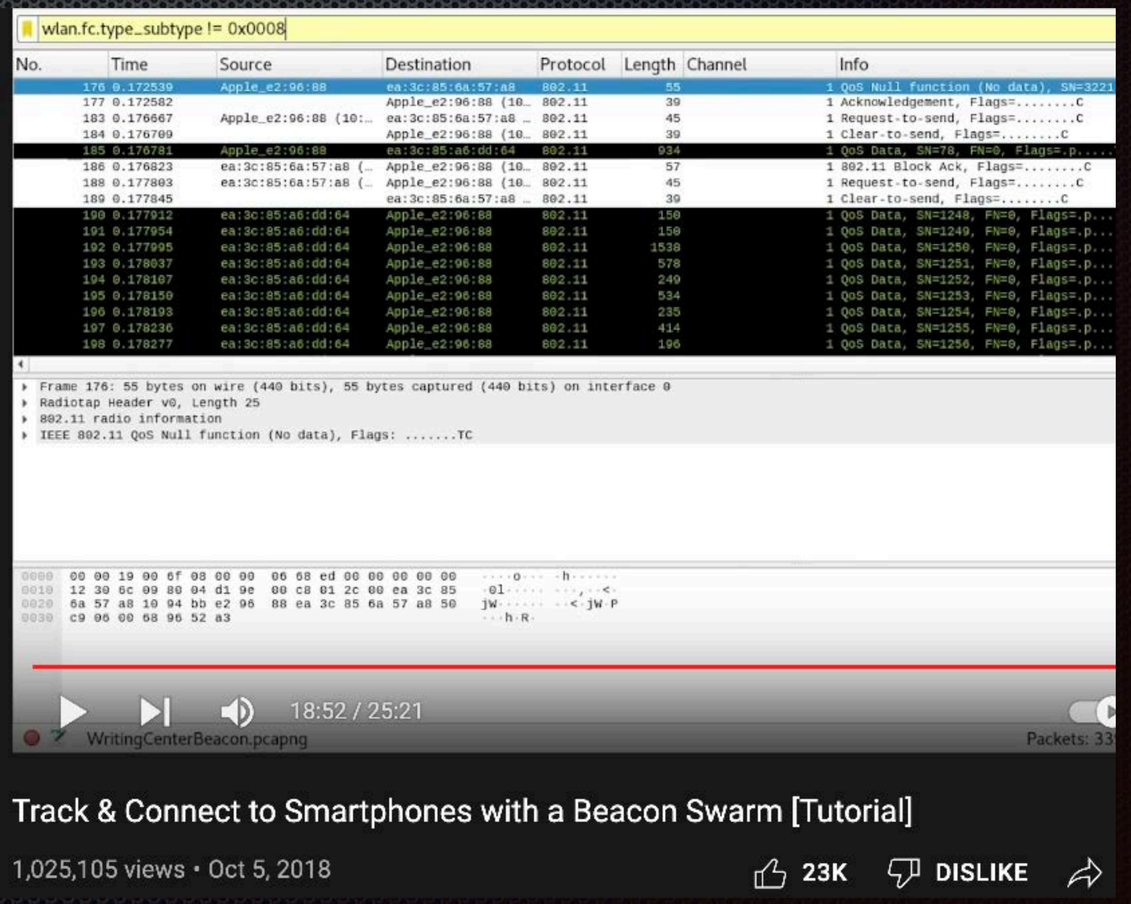
- Instead of an interface, we use Wi-Fi to make a phishing page
- First we scan & find a target AP with a client
- Deauthenticate client & create an open network with the same name
- Victim client connects to open network & see a fake router update page
- If they provide the password, deauthentication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



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



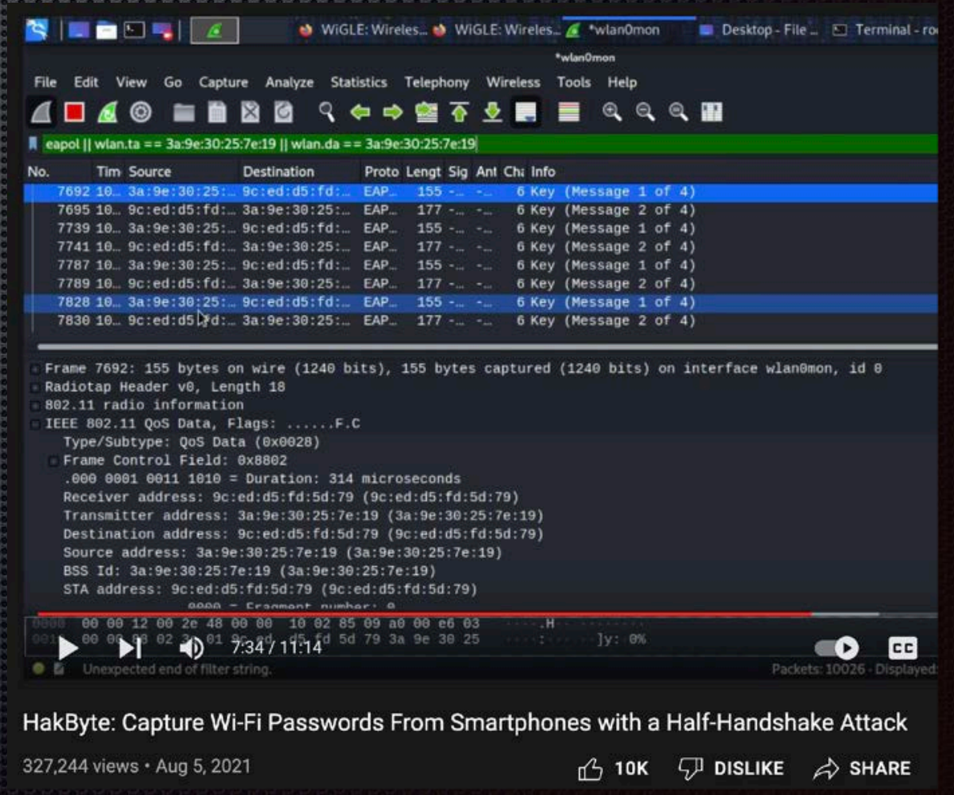
https://null-byte.wonderhowto.com/how-to/use-esp8266-beacon-spammer-track-smartphone-users-0187599/

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!

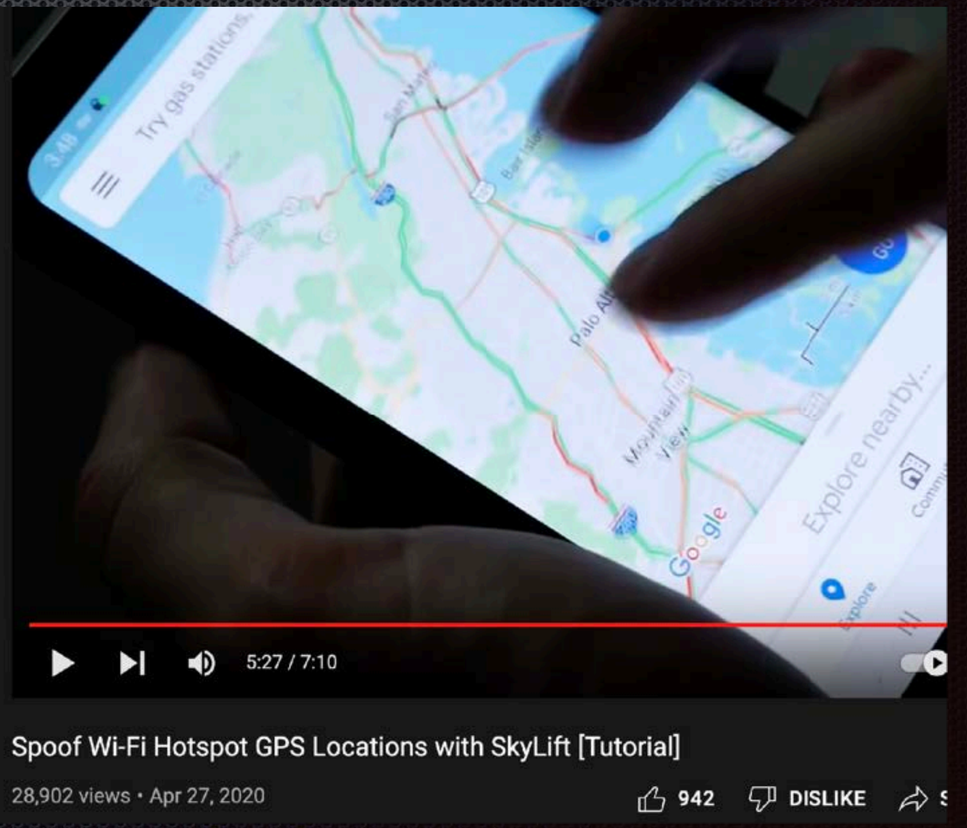
  *Computer required for this step
- Now I know your home/office Wi-Fi password



https://youtu.be/5guDKTc6Hak

aGPS Spoofing with Skylift

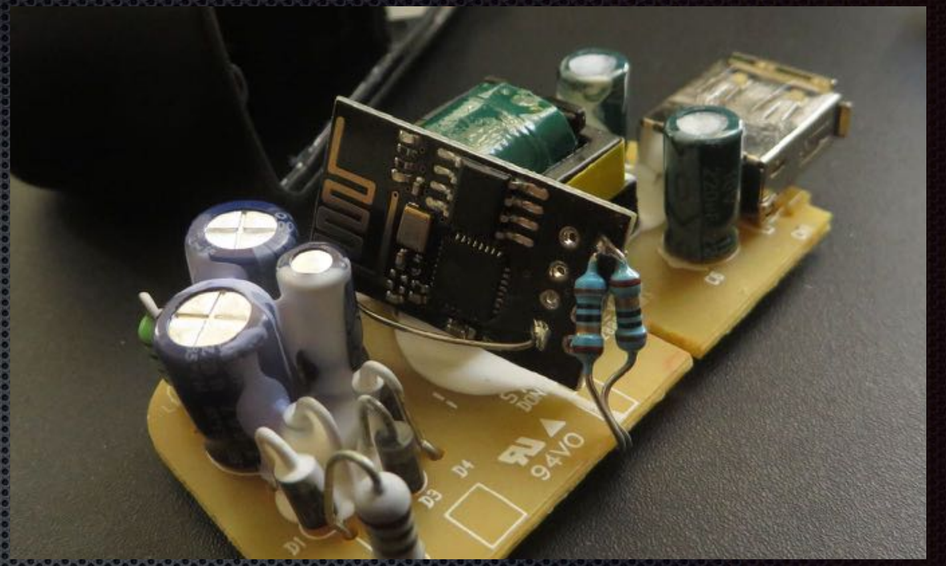
- Most phones get GPS coordinates faster by using Wi-Fi to find their location
- This projects spoofs the Wi-Fi network near Zuck's pool
- Devices will poor GPS reception will fall back to a location calculated by nearby Wi-Fi networks
- Successfully spoofed Zuck's pool location at a mall parking garage



https://youtu.be/X-ml7bLYWpk

https://nulb.app/x4q82

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

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

Remote ESP Bug Scanner Settings About

Known Devices

Name	BSSID	Manufacturer	RSSI

Clients

BSSID	Manufacturer	Channel	RSSI	Associated
78:0C:B8:EF:6A:05	Intel Corporate	0	-59	bcddc2b2bf58
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
6F:89:04:92:B9:E4	unknown	0	-74	981e19511e26
BF:49:62:C1:E8:60	unknown	1	-82	ffffffffffff
A6:9A:93:C7:74:E6	unknown	0	-93	da2a4ce376cb
38:F9:D3:8C:95:7C	unknown	0	-83	7cdb98d83457

https://youtu.be/1uSg9JoDGeU

Wardriving (or Warflying)

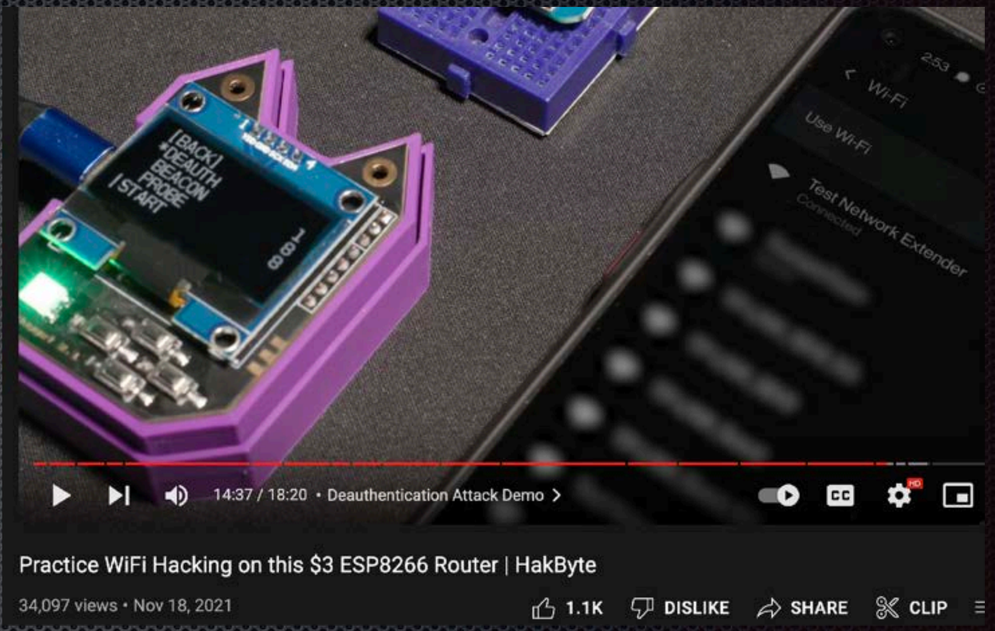
- Connect a $2 GPS, $1 SD card module & a $1.80 ESP8266
- Now we can wardrive!
- Stores seen networks, signal strength, & GPS location to SD card
- We mounted ours on a DJI mini 2
- Located a target smartphone by air!

https://youtu.be/oWNIWHT8q1A

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

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

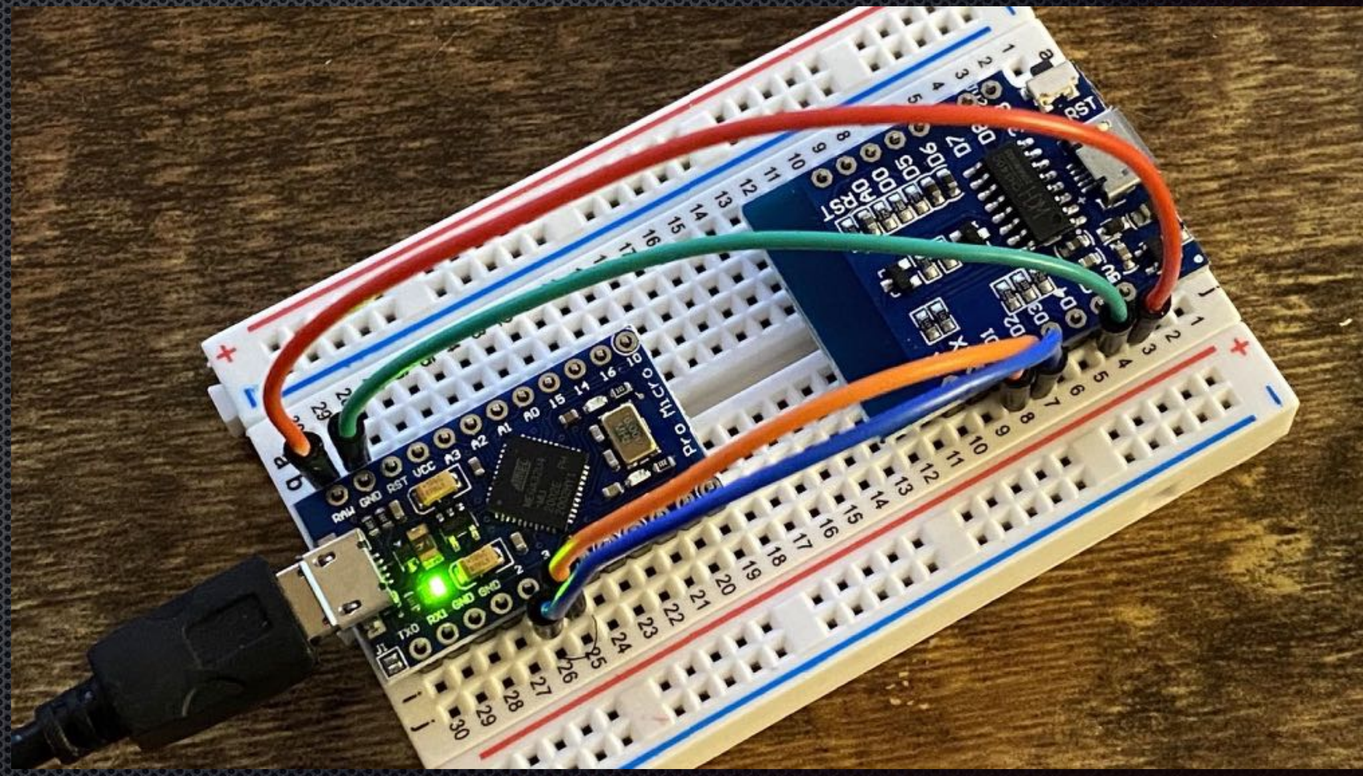
https://github.com/martin-ger/esp_wifi_repeater

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



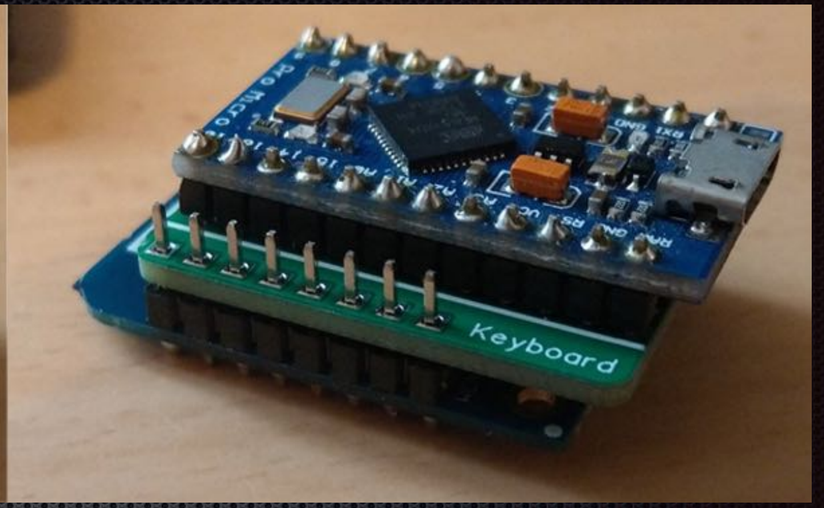
Wi-Fi Duck

- 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

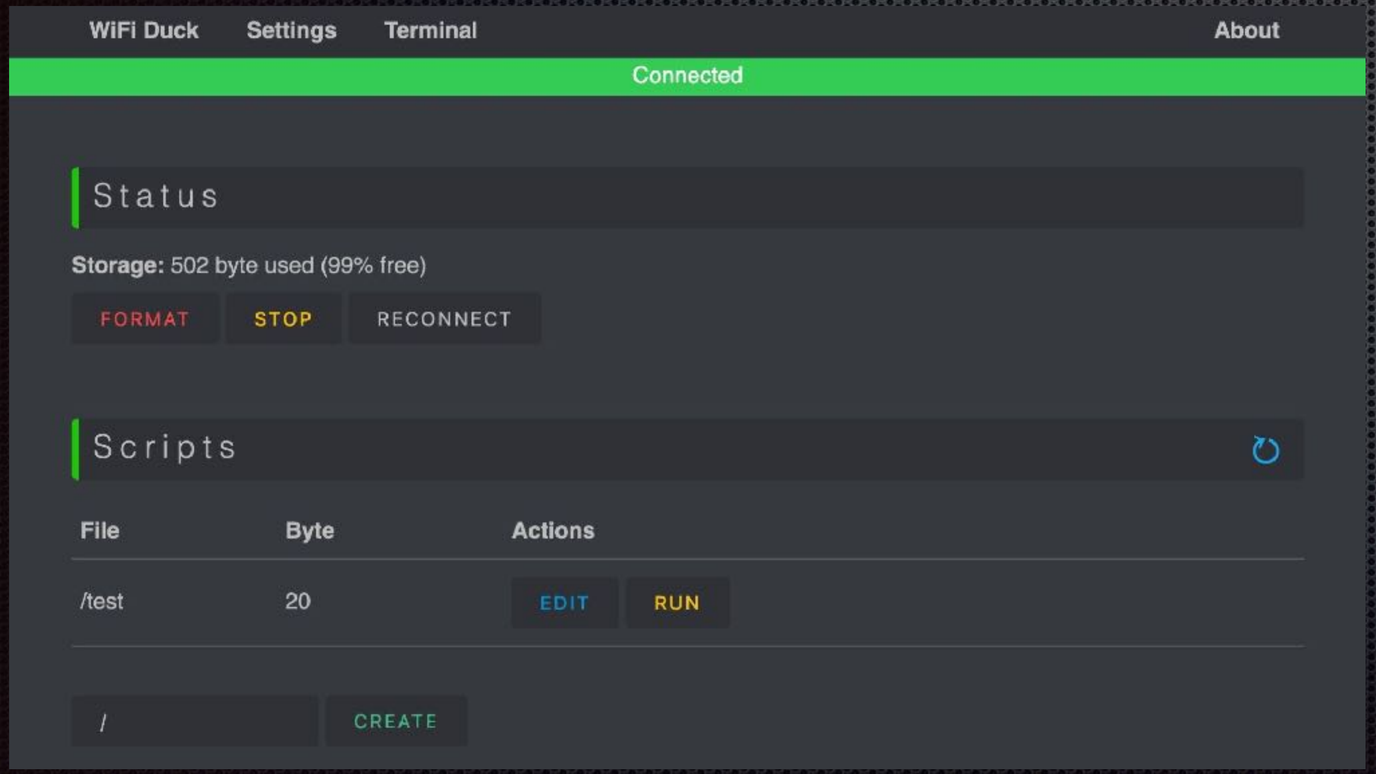
https://null-byte.wonderhowto.com/how-to/hack-computers-over-wi-fi-with-wifi-duck-payload-deliverer-0296285/

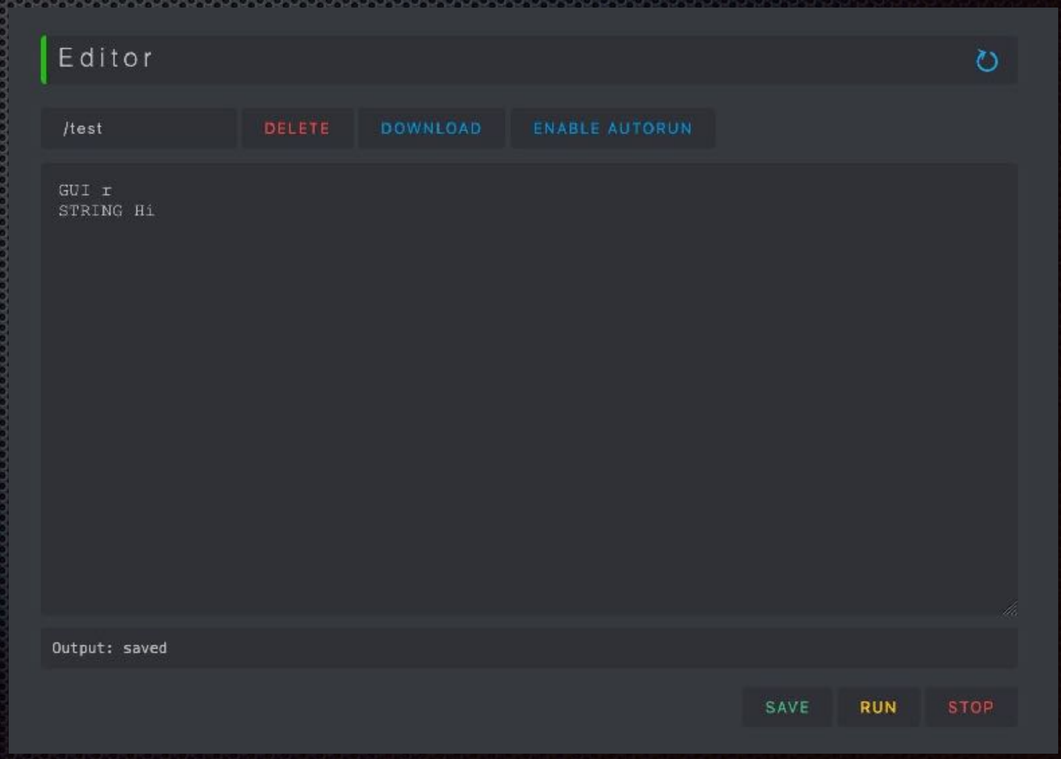
https://vimeo.com/381208724

Wi-Fi Duck



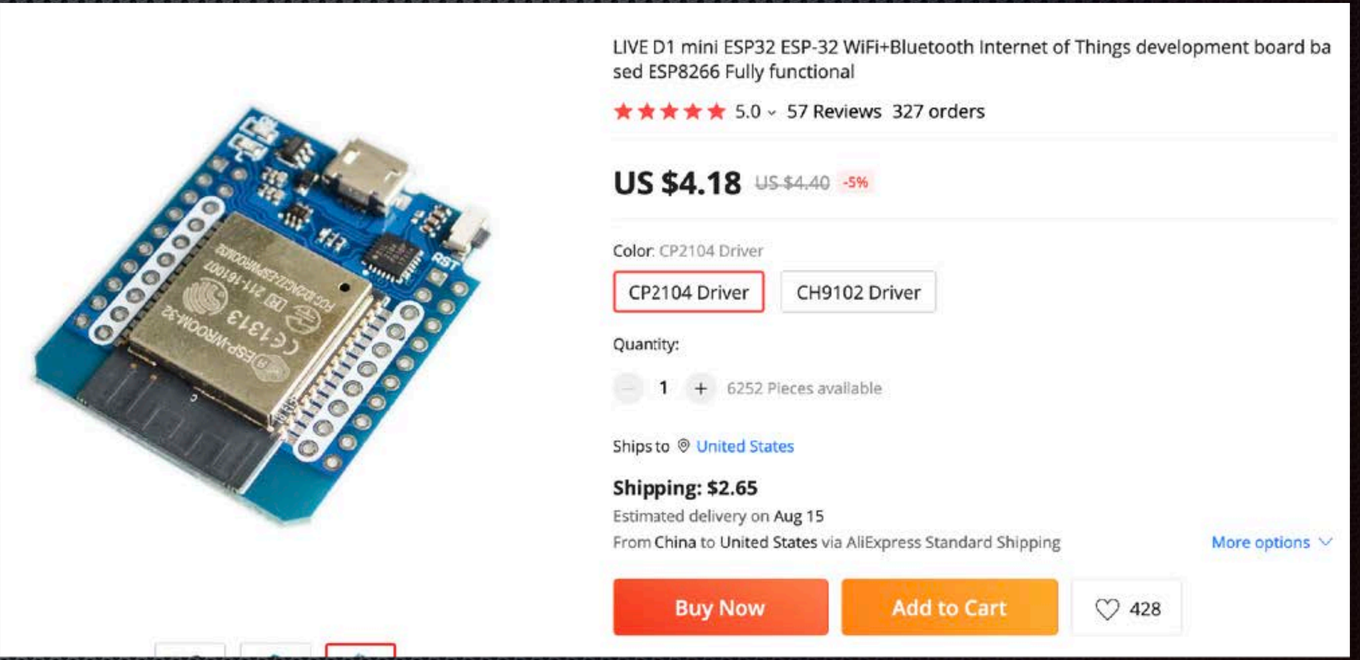
https://github.com/spacehuhntech/wifiduck





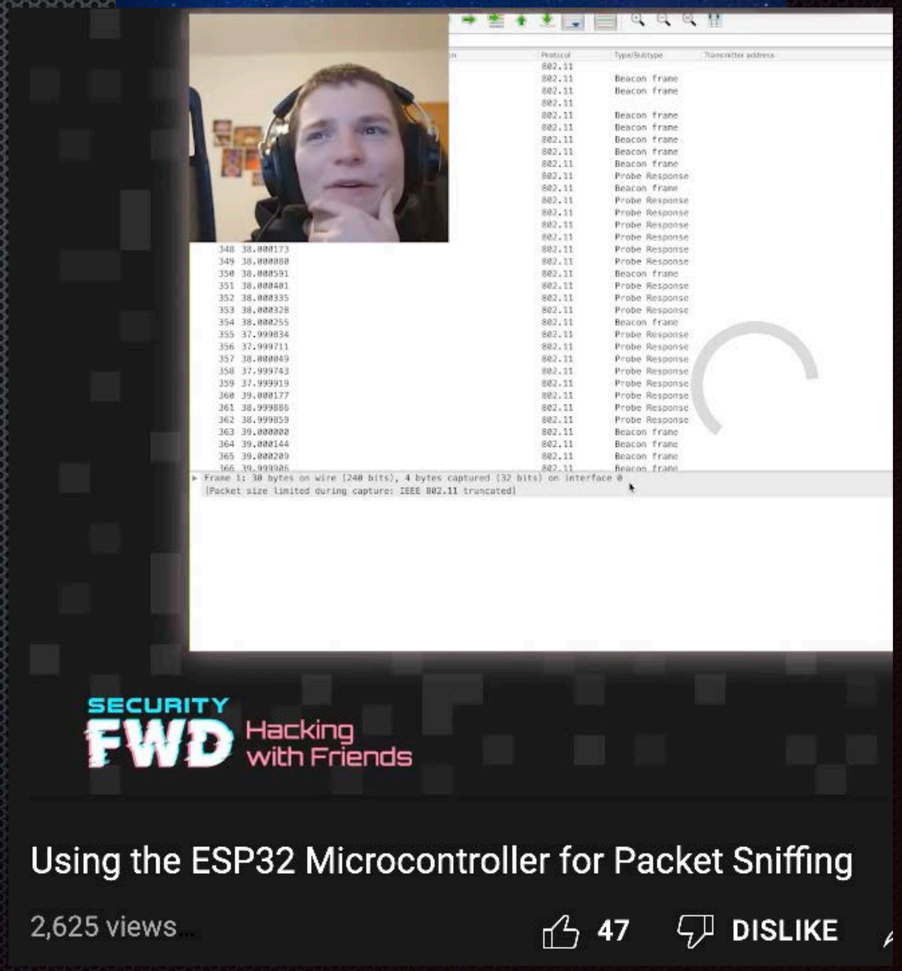
Esp32

- 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

- 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

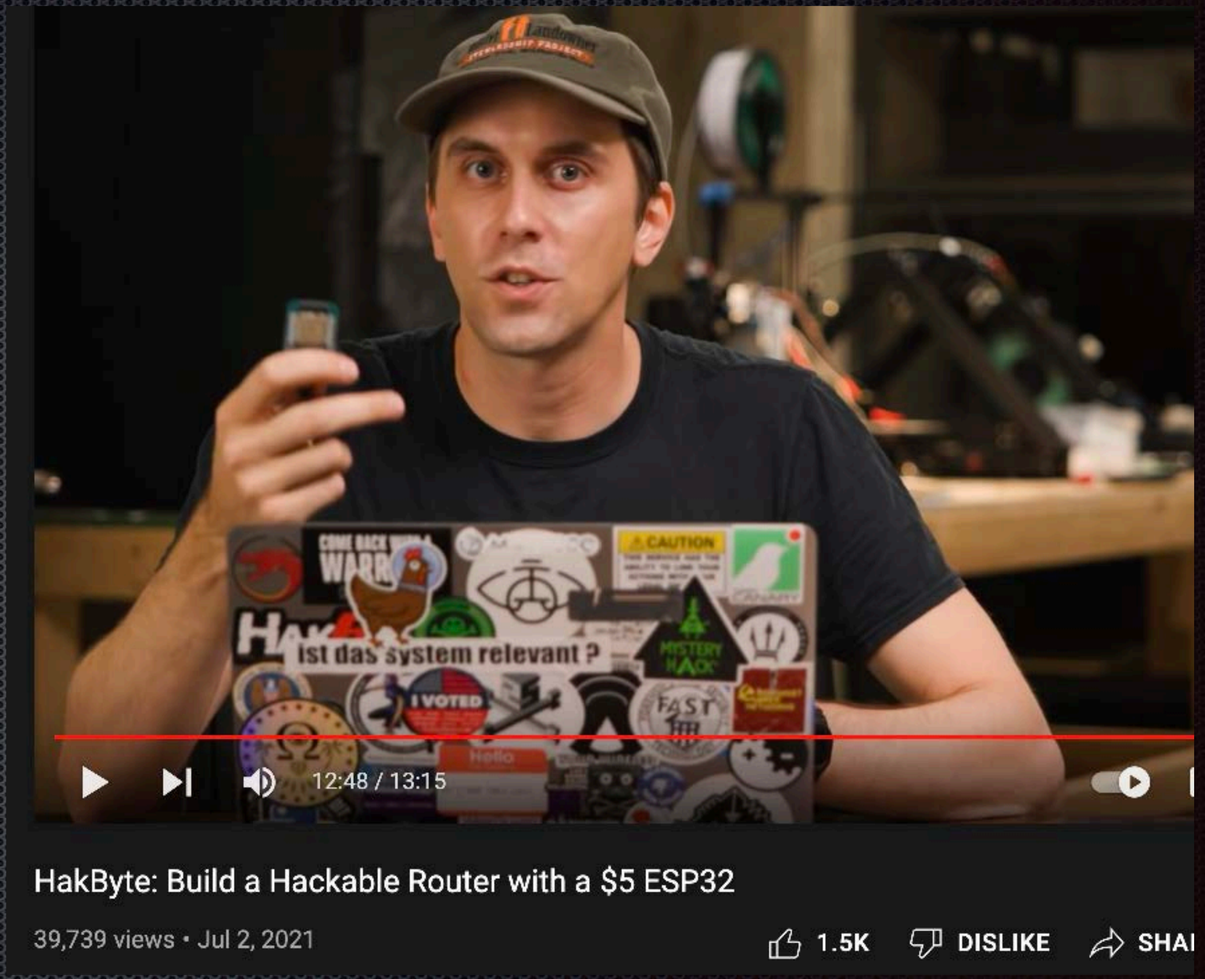


https://github.com/spacehuhn/ArduinoPcap

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

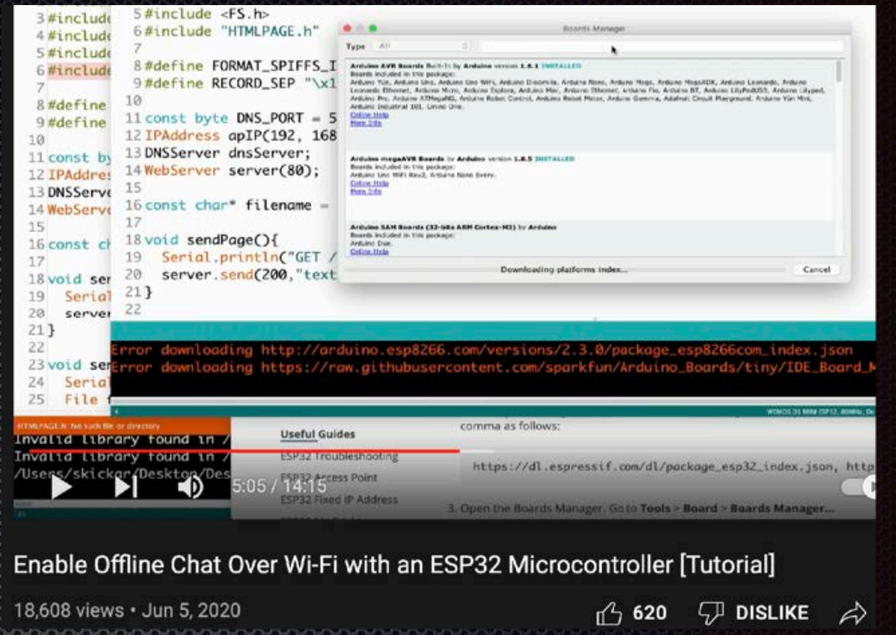


https://youtu.be/41Lymi6rXA8

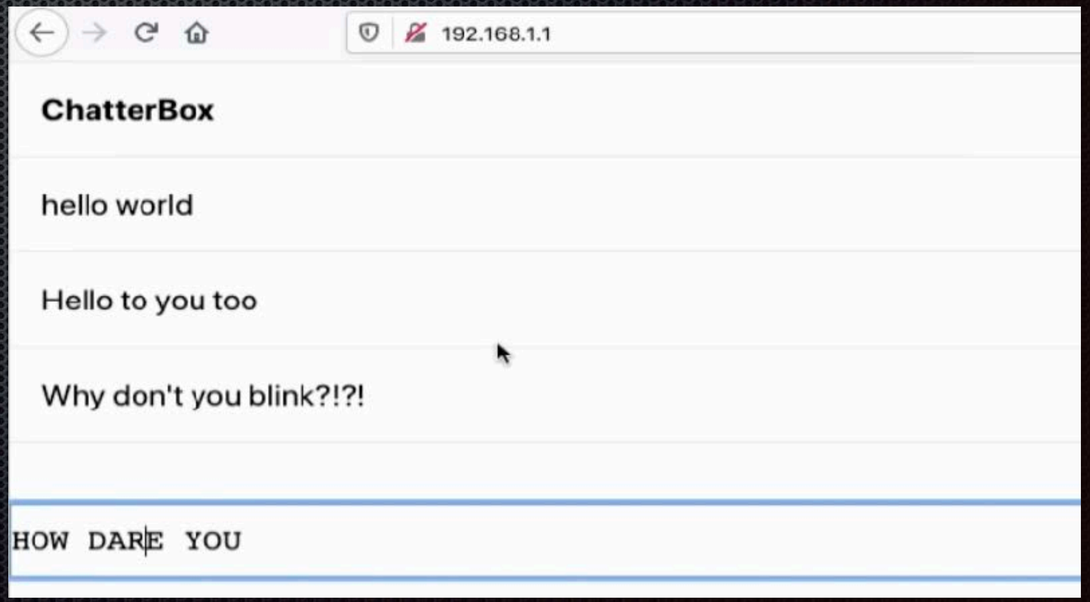
https://github.com/martin-ger/esp32_nat_router

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



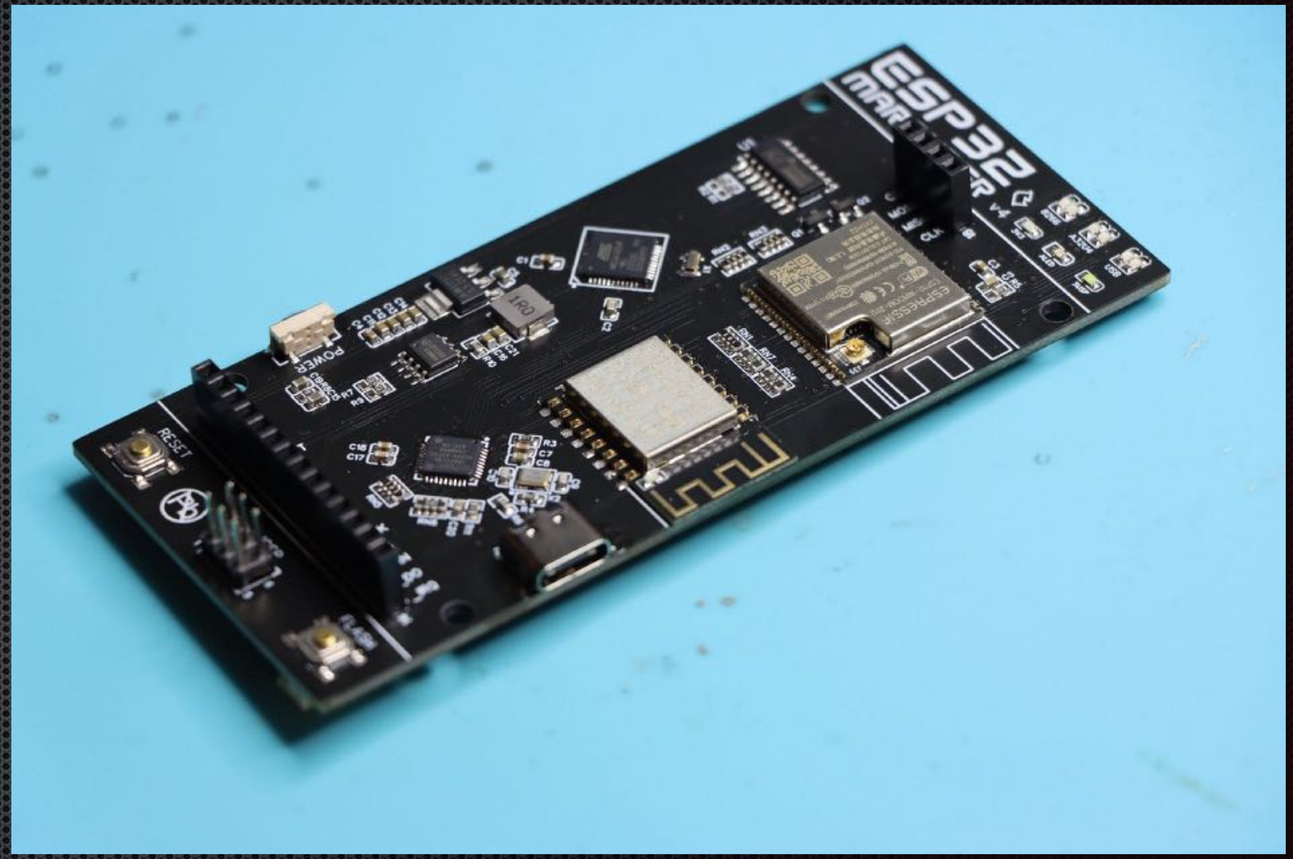
https://youtu.be/4CAokDIG_74



https://nulb.app/z6vu2

Esp8266 + ESP32

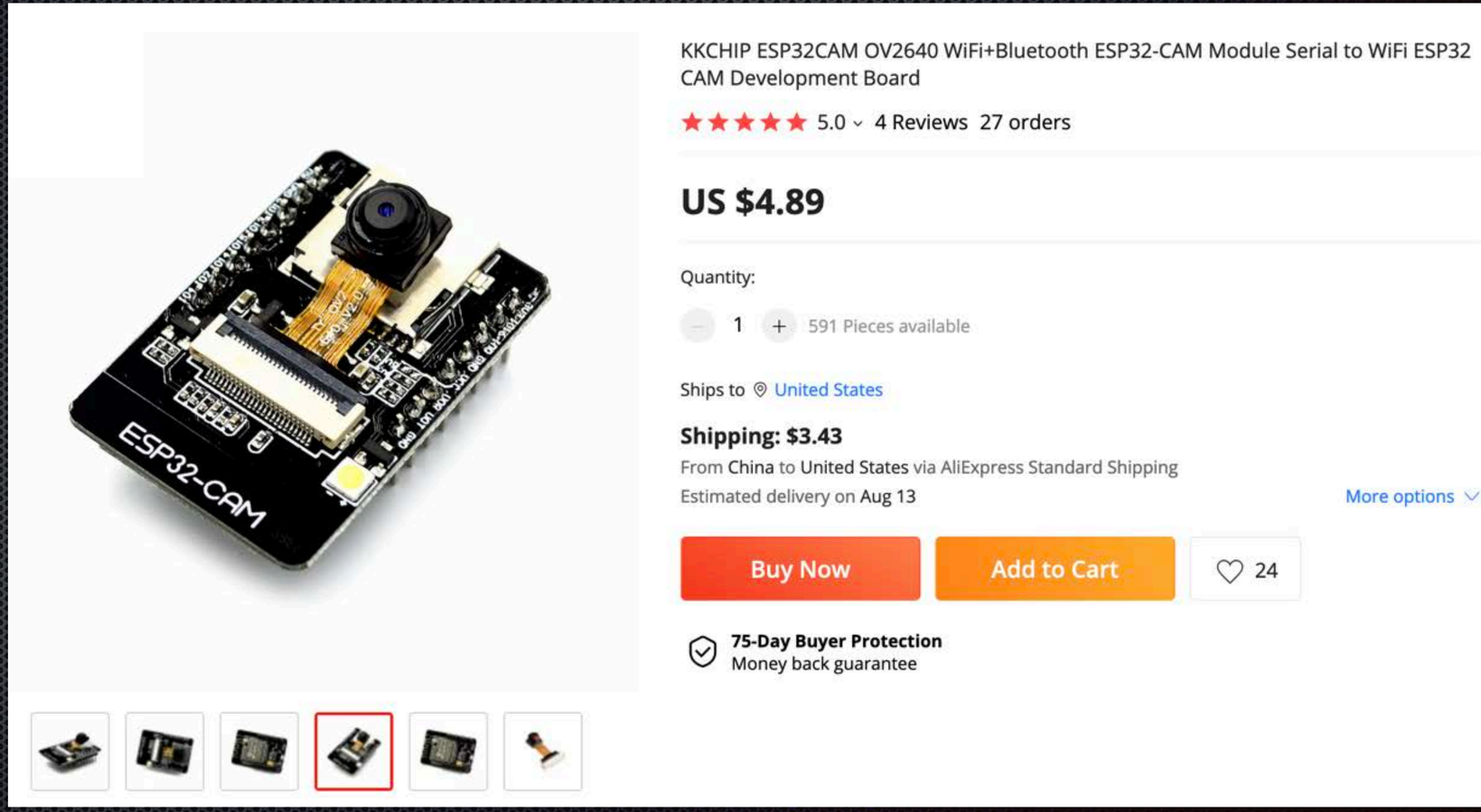
- By combining the ESP32 and ESP8266, we can get the advantages of both
- The ESP Marauder links these microcontrollers together
- Features deauthentication and handshake capture
- Ends up being kind of a multi tool without a specific focus
- Over our budget



https://github.com/justcallmekoko/ESP32Marauder

Esp32cam

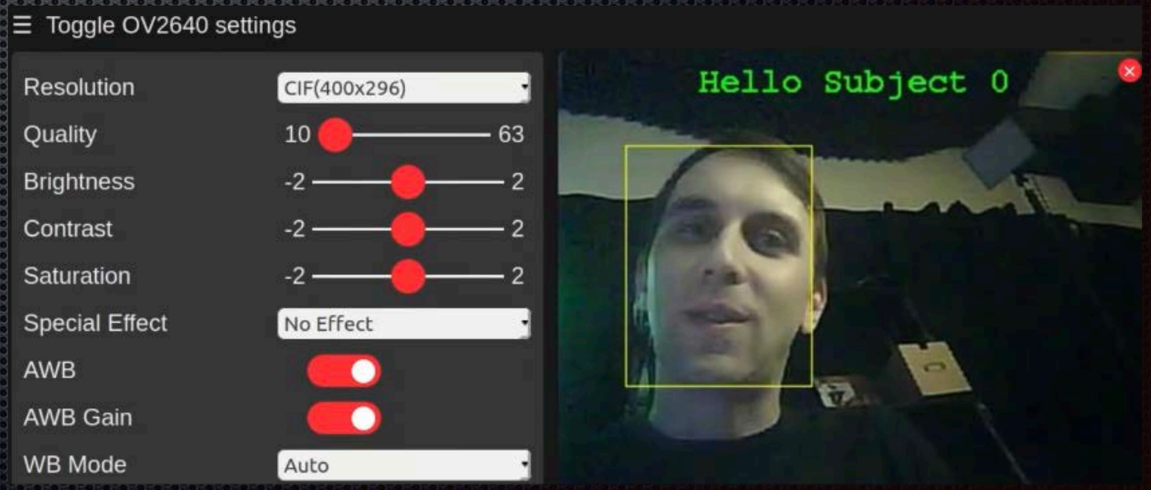
- Integrated camera with ESP32
- Easy to hide Wi-Fi enabled webcam
- Supports facial recognition
- No USB port (good luck)



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

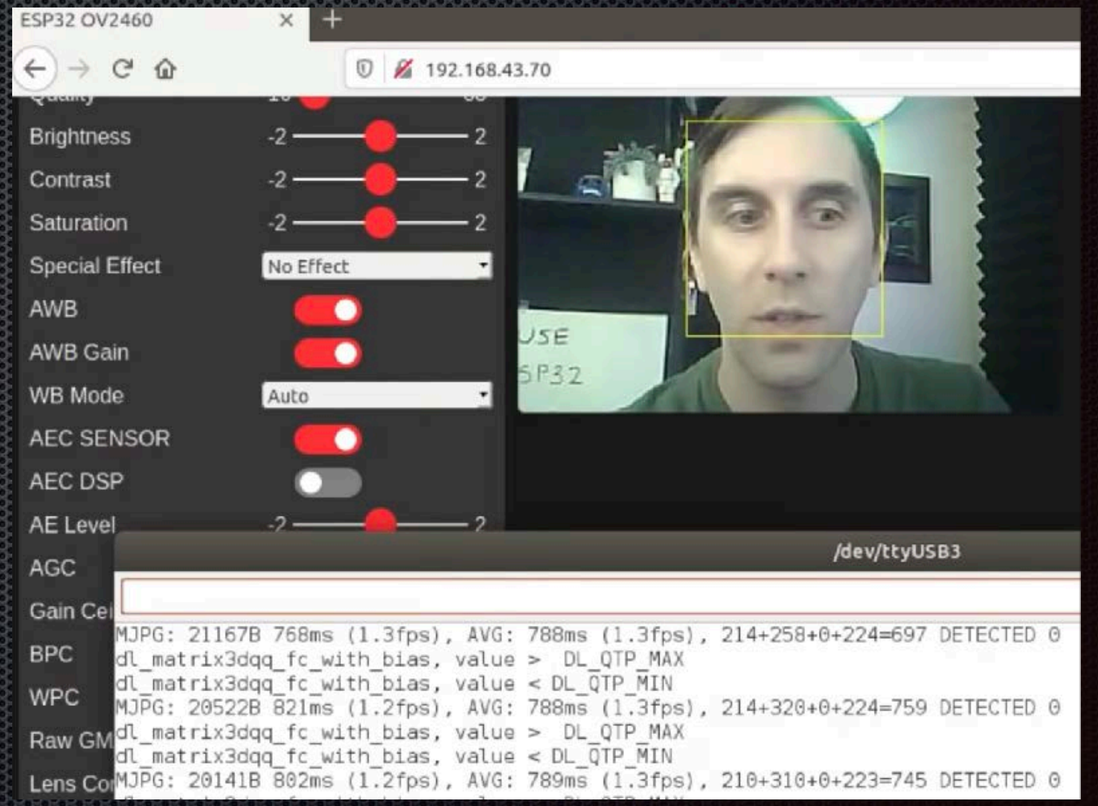
https://youtu.be/tx09GFGgVwA



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

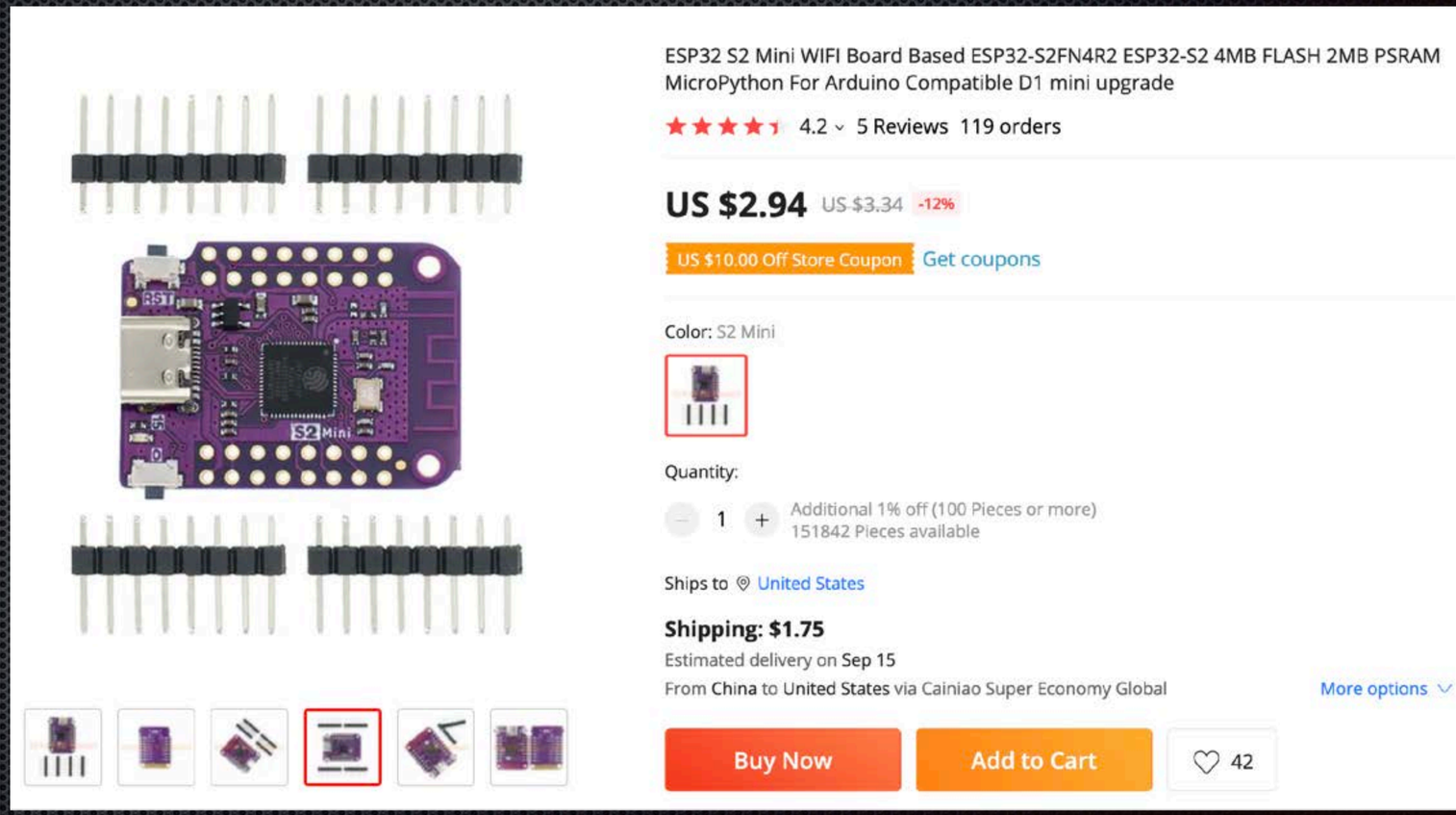


https://youtu.be/LOqVle9cnW8

https://nulb.app/x6ur7

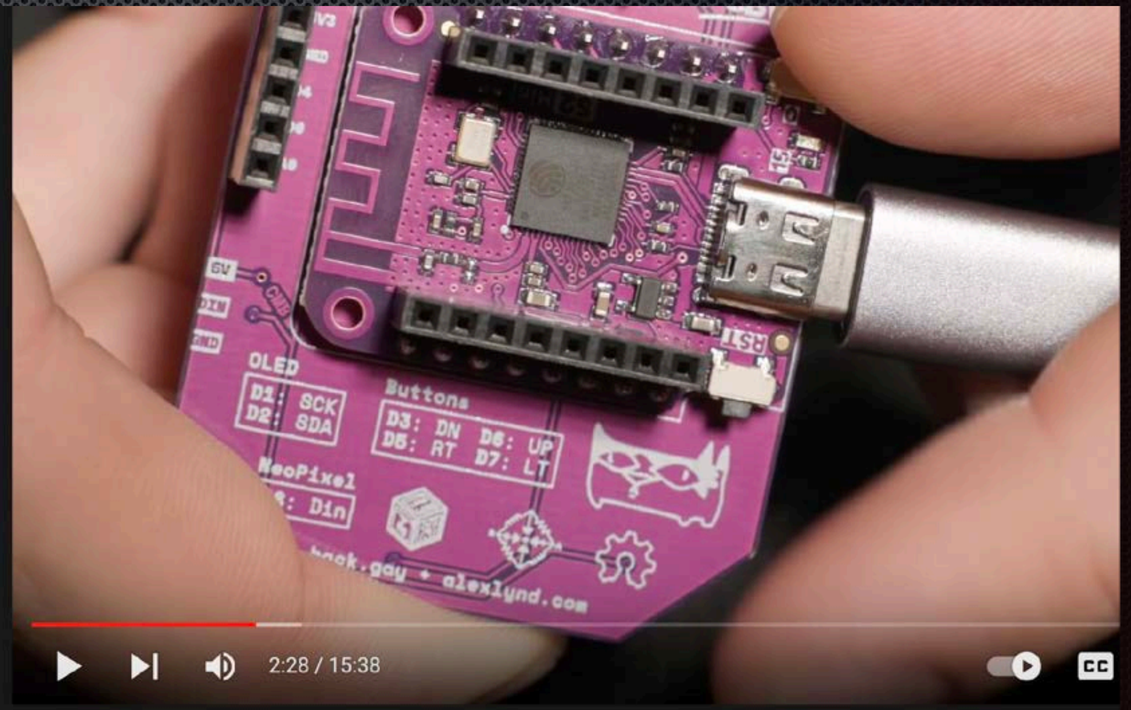
Esp32s2

- 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!



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://youtu.be/aZ8u56l3J3I

https://github.com/HakCat-Tech/S2-Nugget/blob/main/Mouse_Jiggler_Example.zip

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://youtu.be/hIRh_2IL7RY

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

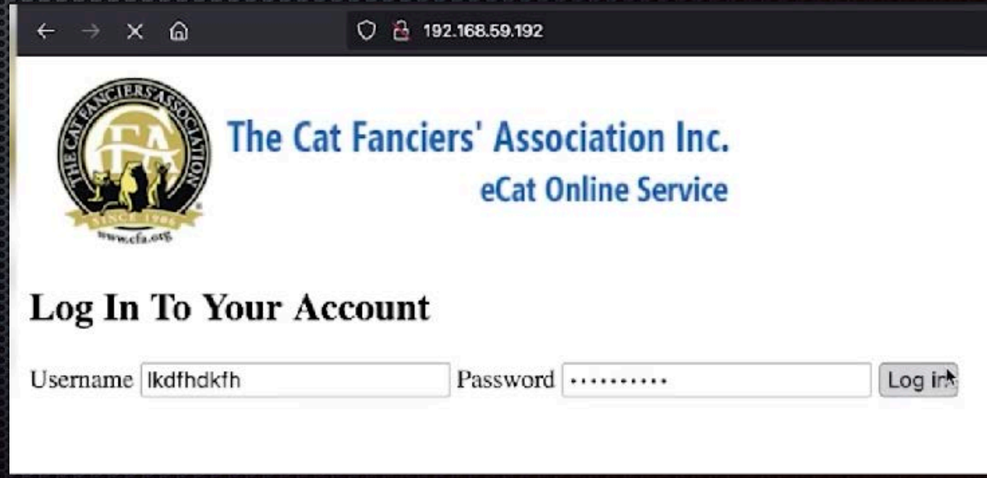
https://docs.hak5.org/rubber-nugget/

Damn Vulnerable Nugget

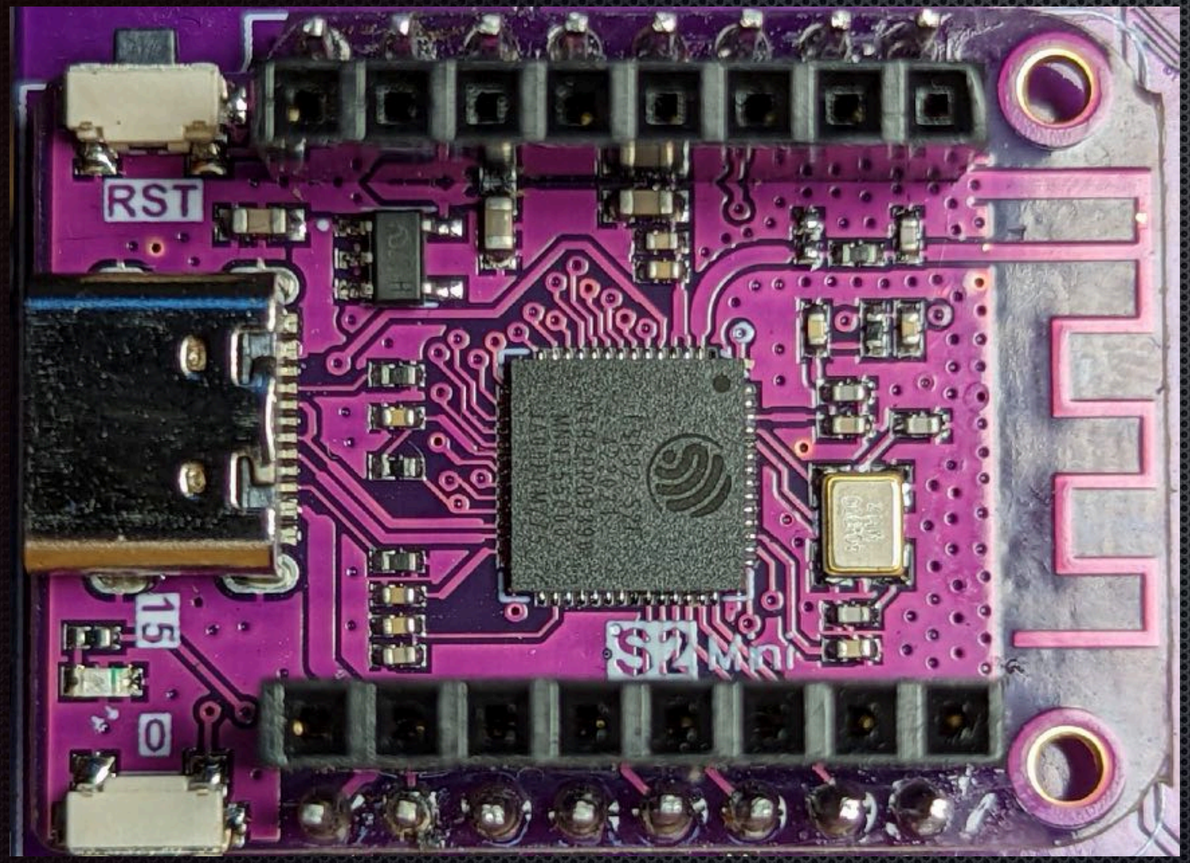
- The Damn Vulnerable Nugget is a simple vulnerable web app written in CircuitPython
- Users can attack it using OWASP Zap or Burpsuite to practice authentication attacks
- It picks a new password each time you run it
- Wet anime eyes to celebrate a win
- I wrote this!

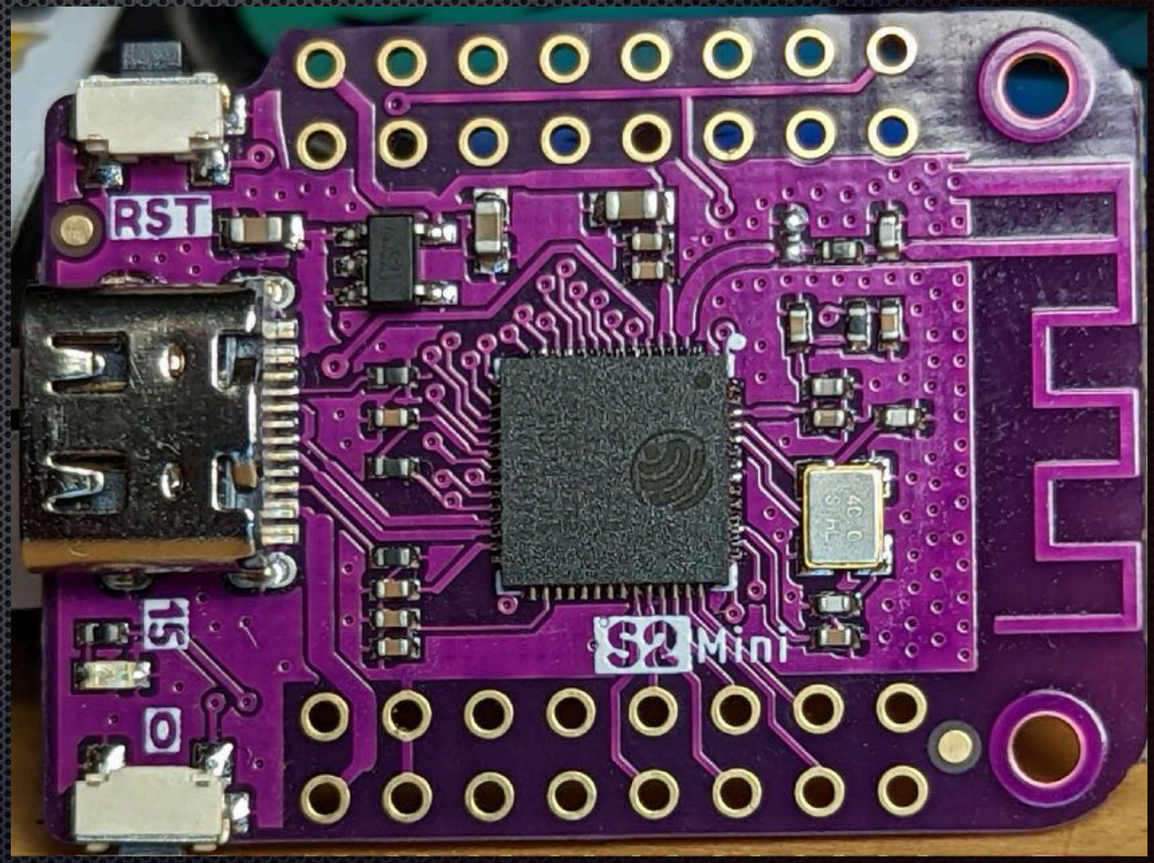
https://github.com/HakCat-Tech/DamnVulnerableNug

https://youtu.be/ArgRtCclThA



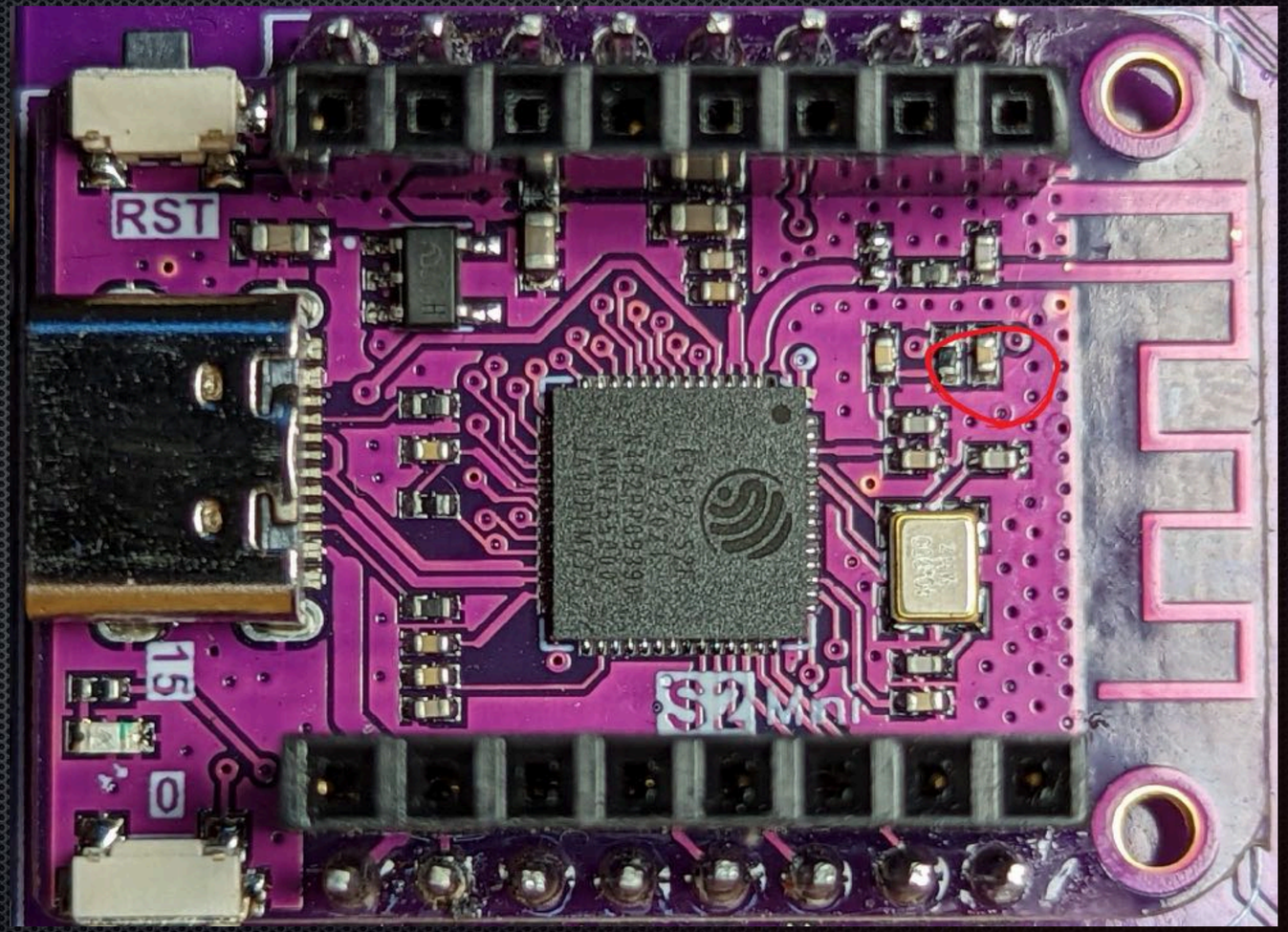
Comparing 2 S2 Mini Modules





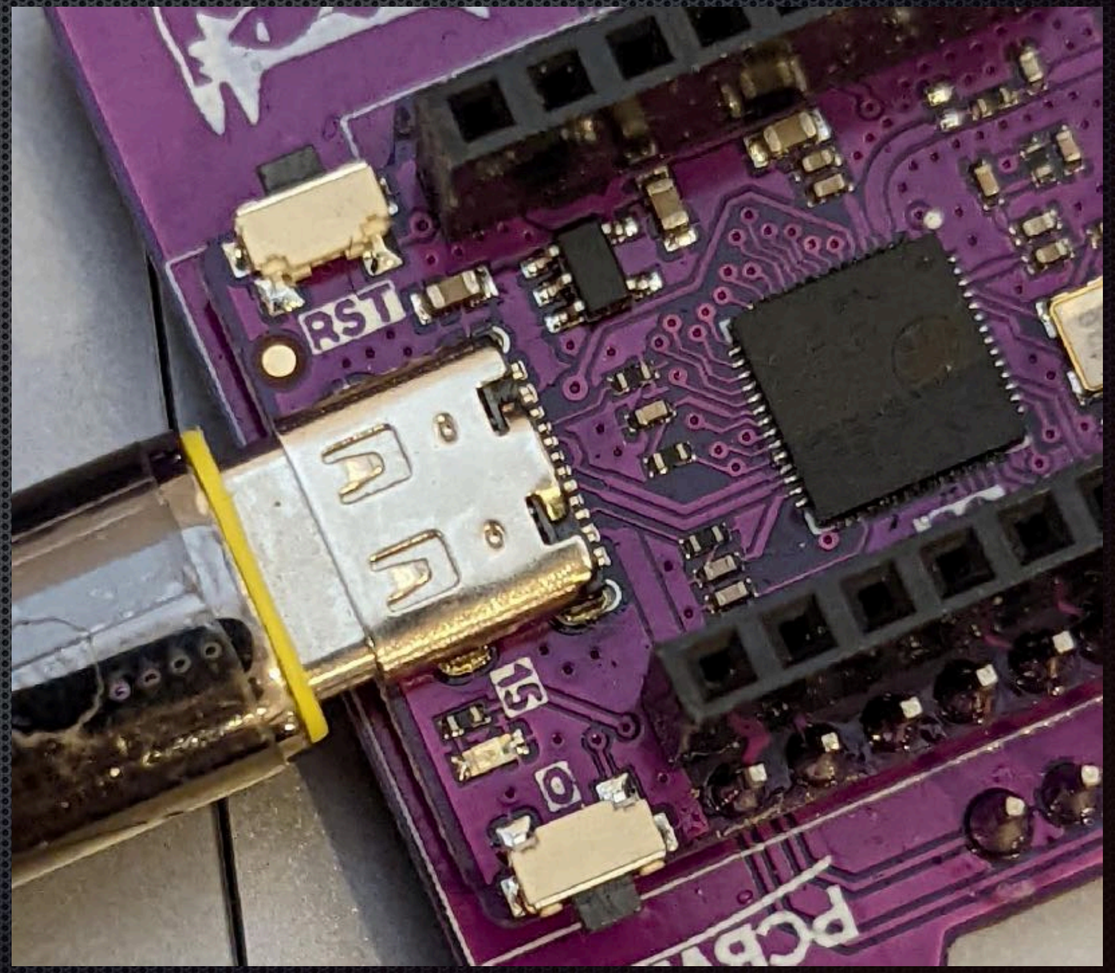
A bad S2 Mini Module

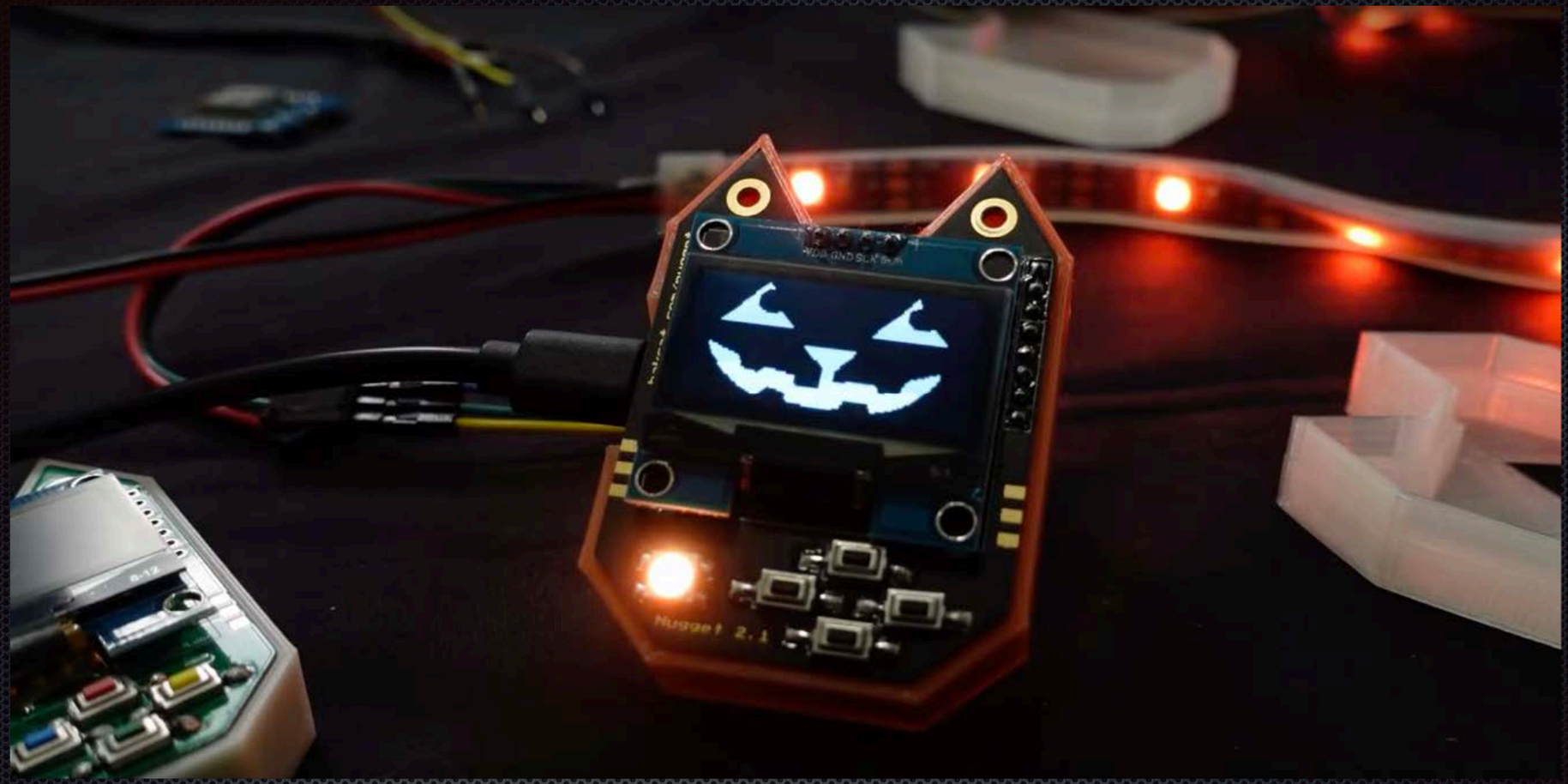
- This module has a single floating connection
- Causes power instability
- Cursed but fix is easy
- Adding solder blob to ground plane fixed it



ESP32s2 Limitations

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



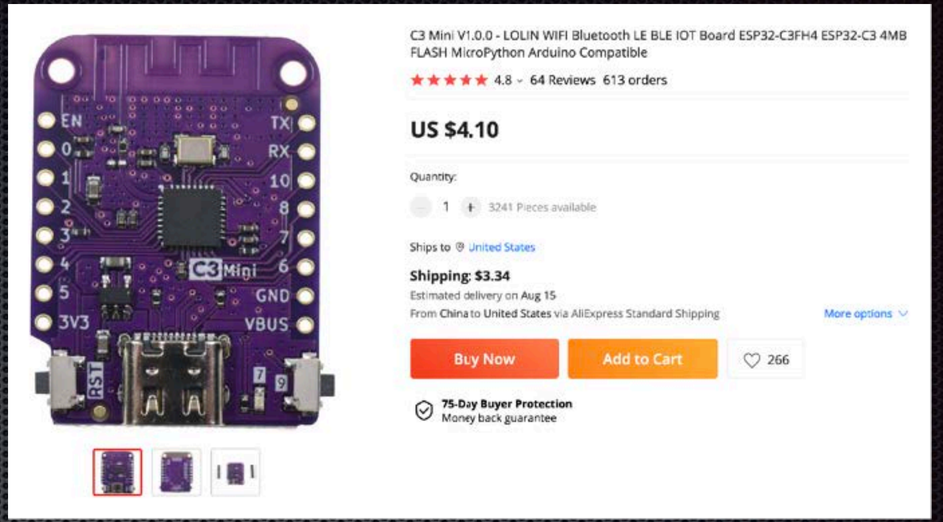


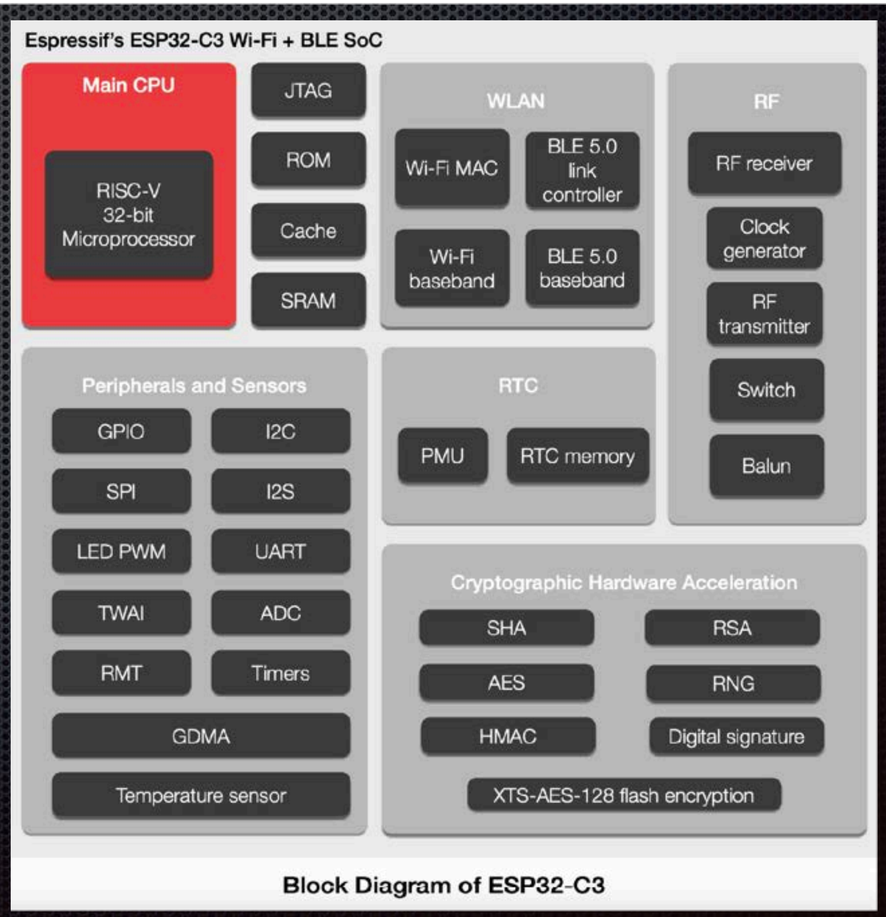
Future boards for hacking

Microcontrollers to pay attention to

Esp32c3

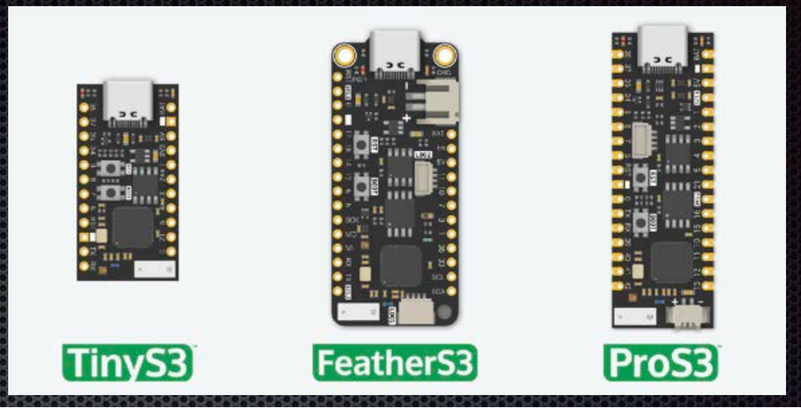
- Supports 2.4 GHz Wi-Fi
- Supports Bluetooth 5 (LE)
- No native USB

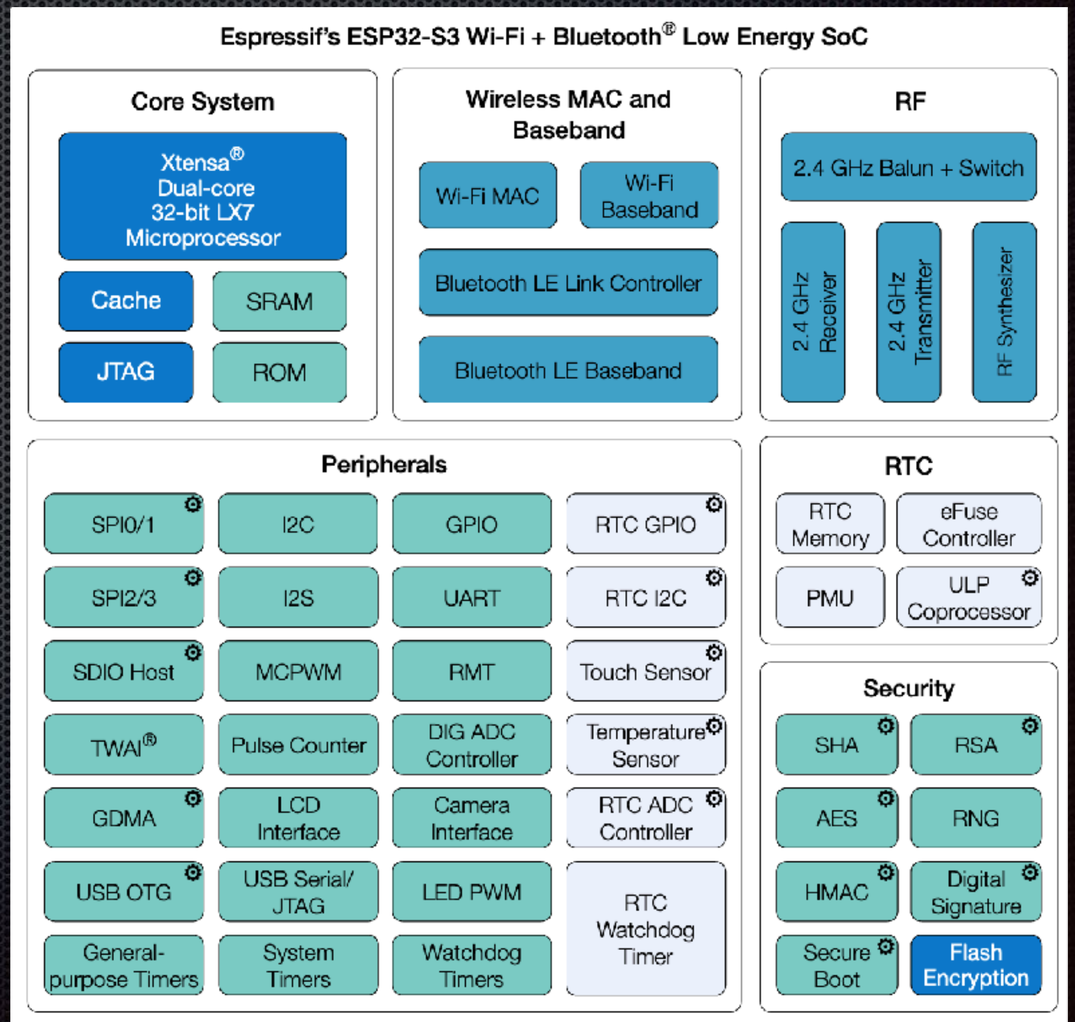




Esp32s3

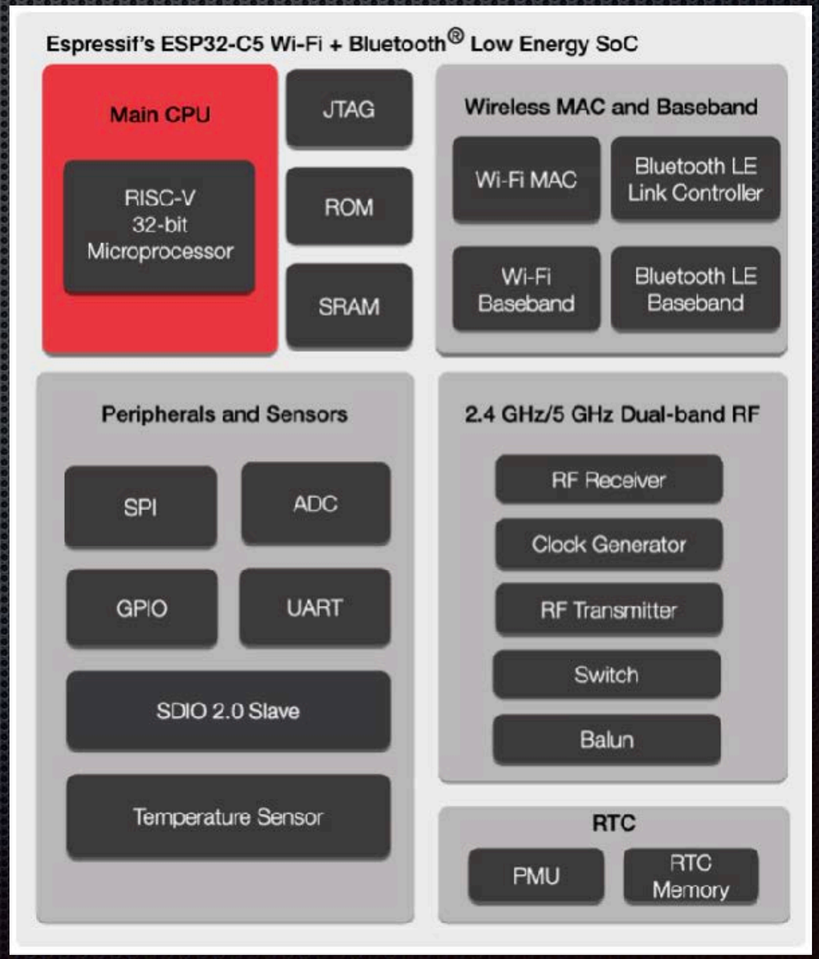
- New flagship model!
- Supports Bluetooth LE
- Supports 2.4 GHz Wi-Fi
- Supports native USB
- Supports the kitchen sink
- You can buy these now!





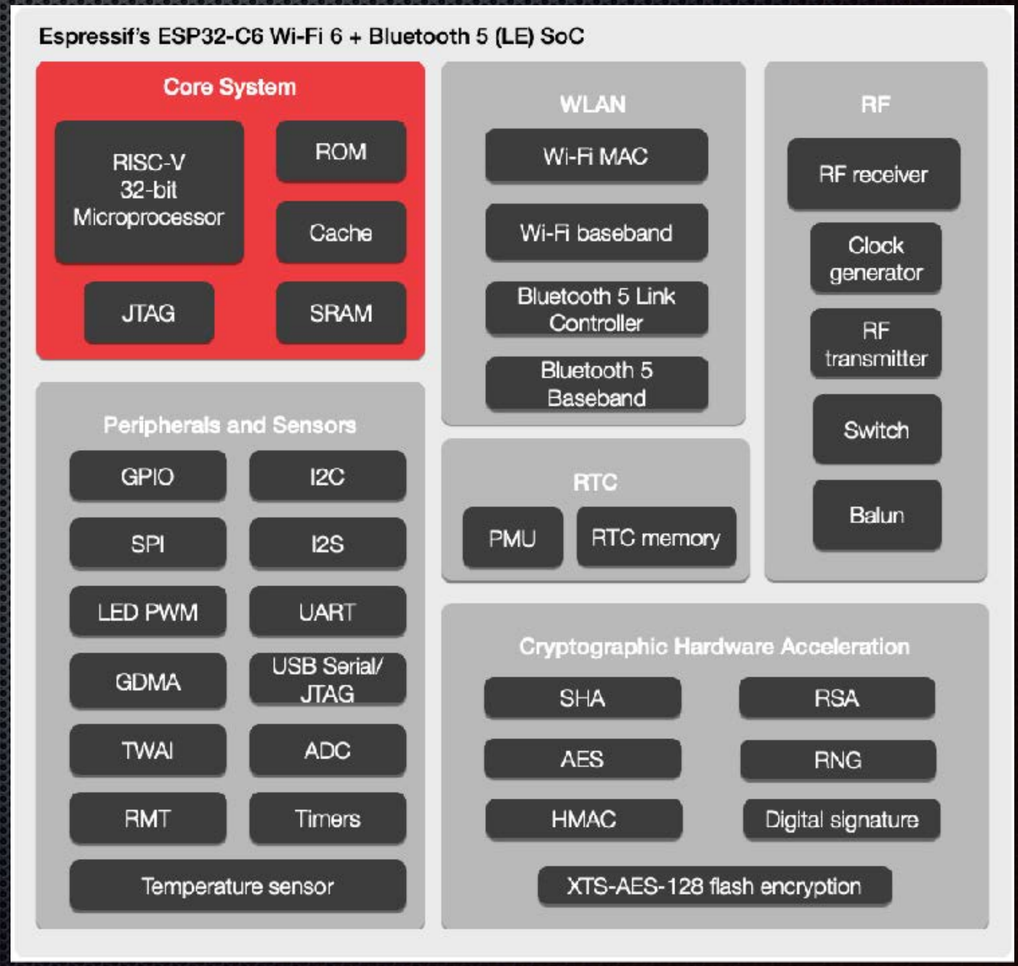
Esp32c5

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



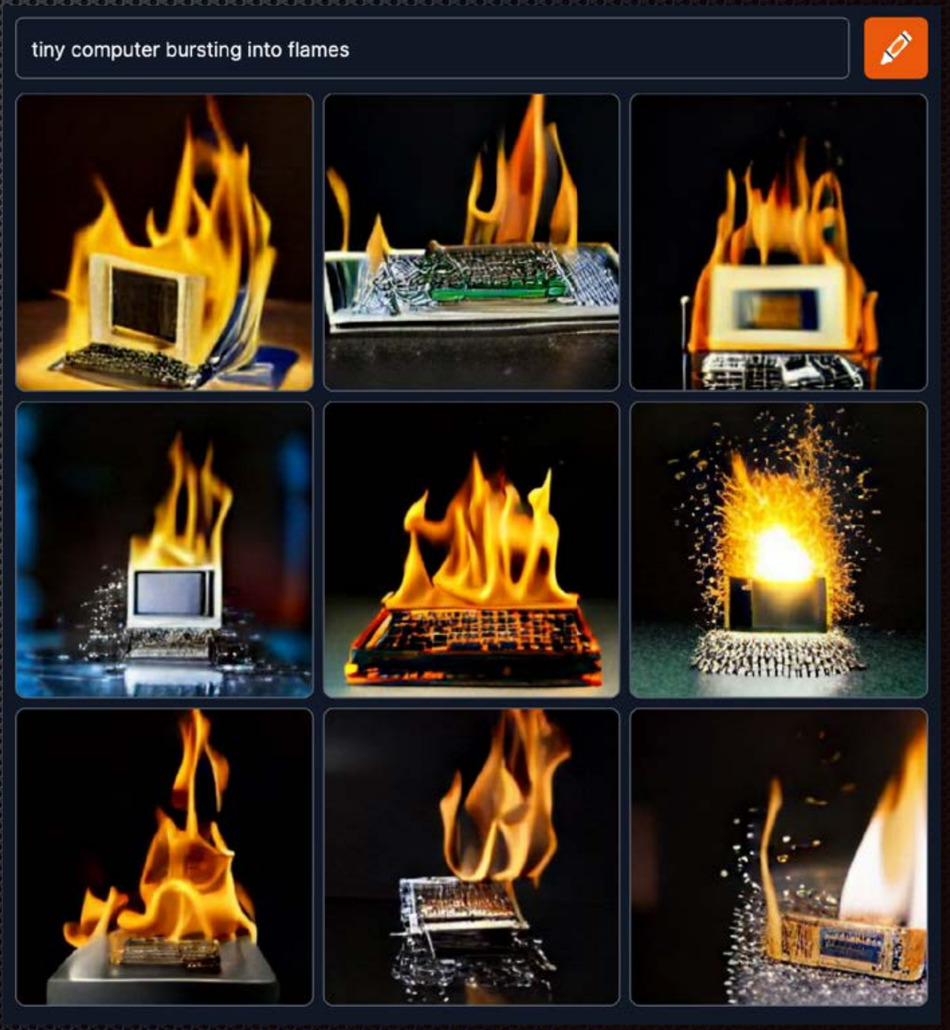
Esp32c6

- 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!