

Halloween Hacking

Soldering, Coding, WiFi Hacking, & More!

[HakCat x Null Space Labs]
Alex Lynd 10/23/2022

```
Oct 16 03:38
Sample.ino - Halloween-Workshop - Visual Studio Code
Arduino Board Configuration X
Selected Board: Generic: ESP8266 Module (undefined)
CPU Frequency: 80 MHz
VTables: Flash

()_
ALTOP LEFT);
Now, (0)

55, 69, 0));
men_nugg_bits;

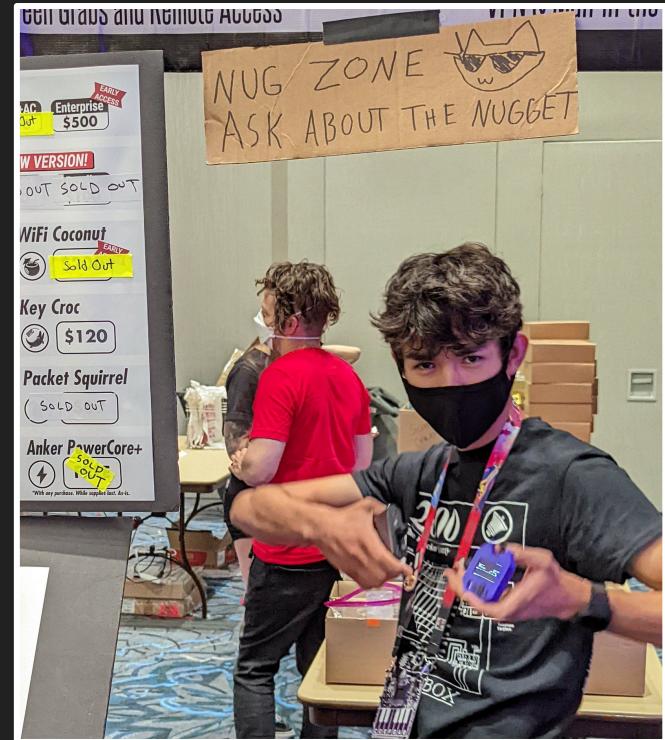
0));
hing and trying again... SSID
(not associated) 00:F6:20:65:6E:B9 -66 0 + 1 390 1956 prozac
effective 125.1 kbit/s...
Quitting...
alex@spooky:~$ cle

CH 11 JI passed hour 58:15:38 MPA2 CCMP PSK
SSID 0 11 130 WPA2 CCMP PSK
-72 2 12408 138 0 10 130 WPA2 CCMP PSK
-78 70 26525 709 0 11 195 WPA2 CCMP PSK
-77 2 18394 467 0 11 720 WPA2 CCMP PSK
-67 100 28312 17587 2 11 195 WPA2 CCMP PSK
-77 37 23254 1353 0 11 195 WPA2 CCMP PSK
-88 8 414 22 0 11 195 WPA2 CCMP PSK
-88 0 99 26 0 11 195 WPA2 CCMP PSK
-78 0 0 545 0 1 195 WPA2 CCMP PSK
-80 0 126 0 0 11 540 WPA2 CCMP PSK
-80 0 8862 1049 0 0 11 195 WPA2 CCMP PSK
-79 0 9492 1949 0 0 11 195 WPA2 CCMP PSK
-79 0 13 0 0 11 720 WPA2 CCMP PSK
STATION PHR Rate Lost Frames Notes Probes
prozac
① Do you want to install the recommended extensions for C++?
Ln 13, Col 45  Spaces: 4  UTF-8  LF_C_
```

Who am I?

Hi! I'm Alex Lynd, a hardware developer & cybersecurity content creator!

- Hacking & InfoSec Videos on Hak5
- Full-Stack Product Designer @ HakCat
- I work on open-source projects like the USB Nugget, and specialize in prototyping with microcontrollers.
- Signals Intelligence & WiFi Hacking research



What we're doing today

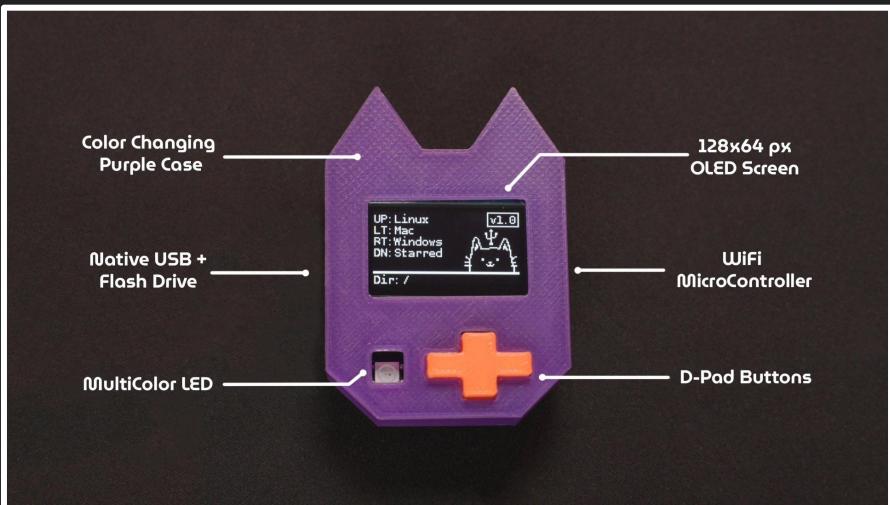
- Learning about WiFi security: defensive & offensive
- Soldering & assembling your own Nugget
- Creating a WiFi-reactive Halloween Light project
- Learning to program in CircuitPython
- Trying some basic WiFi hacking



What is the Nugget?

The Nugget is a cat-themed device that makes it easy to learn about hacking!

- 128 x 64 Display
- Reactive RGB LED
- D-Pad buttons
- Plug & Play Hardware
- WiFi Capable
- Native USB: Host & Device



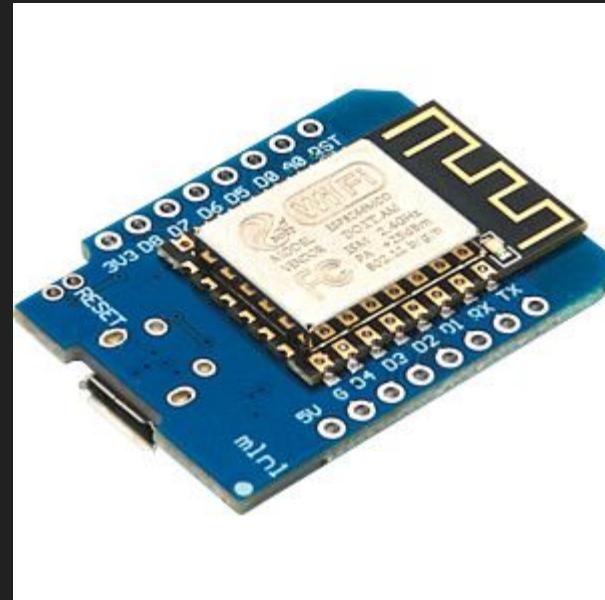
USB Nugget vs WiFi Nugget

	USB Nugget	WiFi Nugget
WiFi AP & Client	Yes	Yes
WiFi Reconnaissance	Yes	Limited
WiFi Hacking	No	Yes
Hardware Expansion	Yes	Limited
Native USB	Yes	No
CircuitPython	Yes	No
Arduino	Yes	Yes

What's under the hood? (WiFi Nugget)

The WiFi Nugget is power by the **ESP8266** microcontroller which offers:

- WiFi (AP & Client mode)
 - Limited Hardware Expansion
 - WiFi Attack Capabilities



What's under the hood? (USB Nugget)

The USB Nugget is powered by the **ESP32-S2** microcontroller which offers:

- WiFi (AP & Client mode)
- **Native USB**
 - Emulate USB Devices
 - Flash Storage
- **Easy Hardware Expansion**
- **Full Packet Capture Ability**



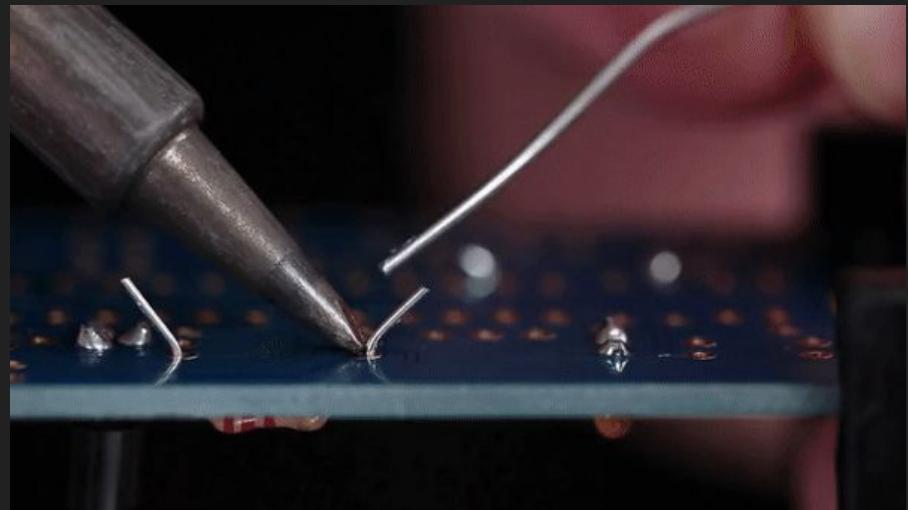
Soldering Skills Class

1 Hour - Build your own USB Nugget!

What is Soldering?

Soldering is an assembly technique that lets us mount components on circuit boards.

- **Solder** is used to attach components to the PCB.
- A **soldering iron** is used to heat up the circuit board and the components at the same time.
- Solder hardens and lets us create a stable electrical connection.



Soldering through hole components

Common Soldering Tools

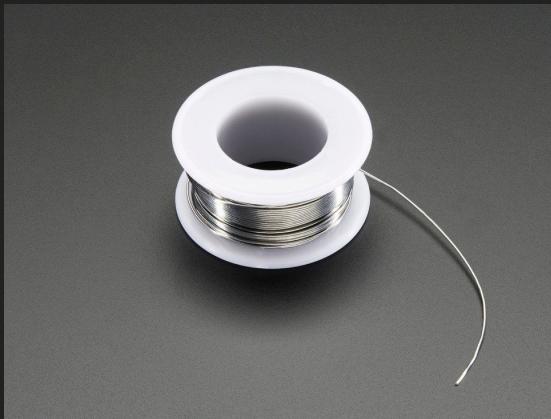


Soldering Iron



Solder Sucker (for screw-ups)

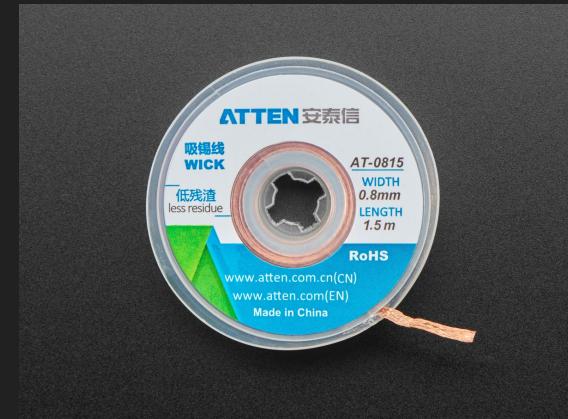
Soldering Materials



Solder



Solder Flux



Solder Wick

Soldering techniques

Through-hole (THT)

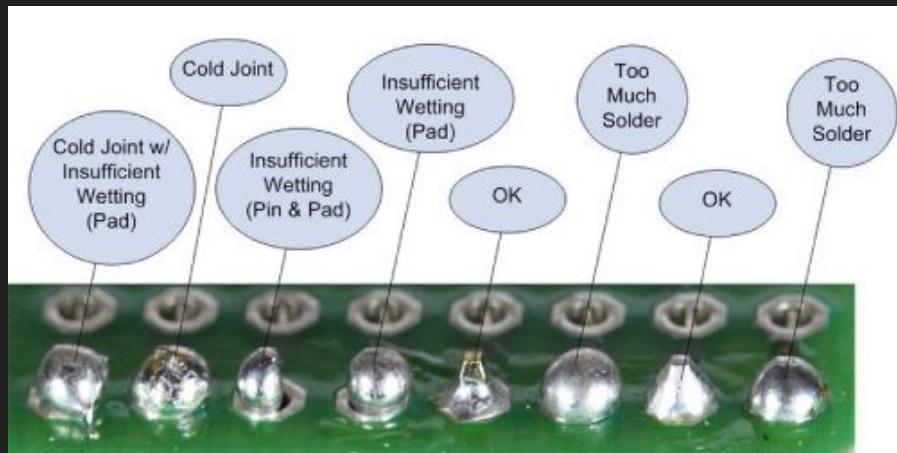
- Easy to assemble by hand
- Bigger components
- Parts mounted *through* board

Surface Mount (SMD)

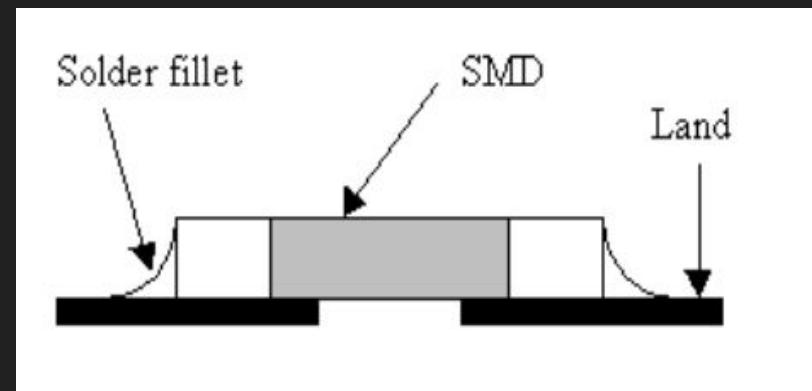
- Cheaper parts but **smaller**
- Easier for machines to assemble
- Components mounted on the surface of PCB
- Sometimes needs specialized tools



Good solder joints

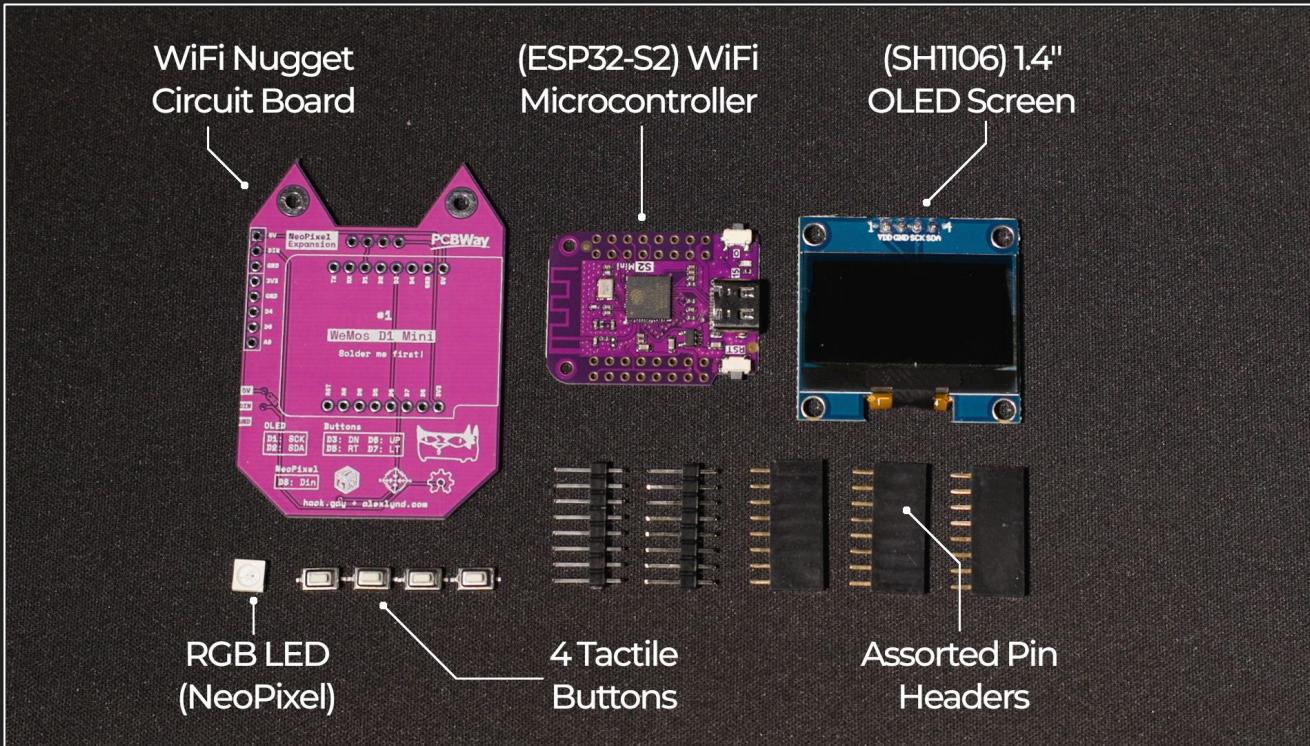


Through-hole joints

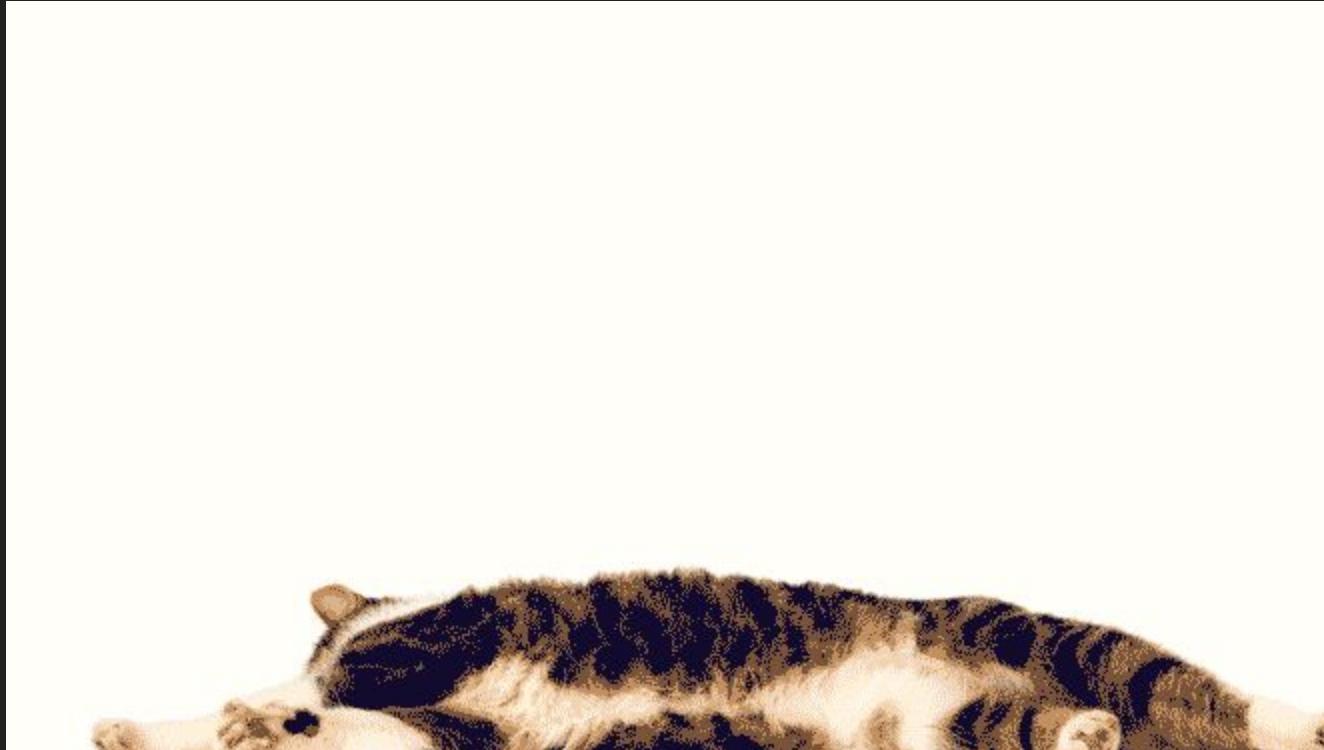


Surface mount pads

What's in your Nugget Kit



Your Nugget is Ready to Hack!



Halloween Lights

1 Hour

Mini Project: Reactive Halloween Lights

We're going to create Halloween Lights that react to WiFi traffic and detect attacks!

But first, we're going to create a simple light flasher program to:

- Learn basic CircuitPython
- Learn to connect hardware
 - Lights
 - Screen
 - Buttons



What is CircuitPython?

CircuitPython is a simple programming language that runs on microcontrollers.

<https://circuitpython.org/>

- Programming tool in your pocket
- Run instant commands
- Control hardware & sensors
- Beginner-friendly syntax
- Great for quick prototypes



Installing CircuitPython

1. Download CircuitPy binary:

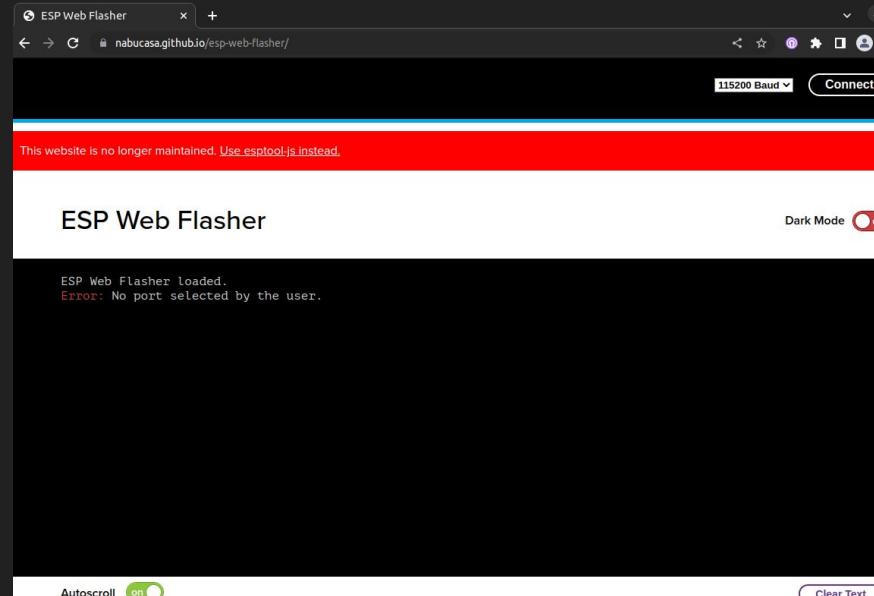
https://circuitpython.org/board/lolin_s2_mini/

2. Place Nugget into Flash Mode

3. Use the Web Flasher to upload the binary:

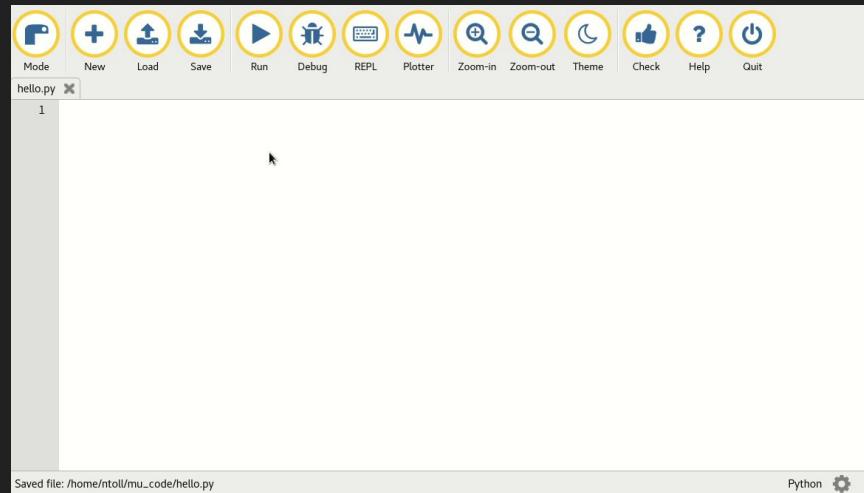
<https://nabucasa.github.io/esp-web-flasher/>

[Full Instructions Here](#)



Installing Mu Editor

- We'll be using Mu Editor to edit & run scripts on the Nugget!
- Download Mu Editor:
<https://codewith.mu/>

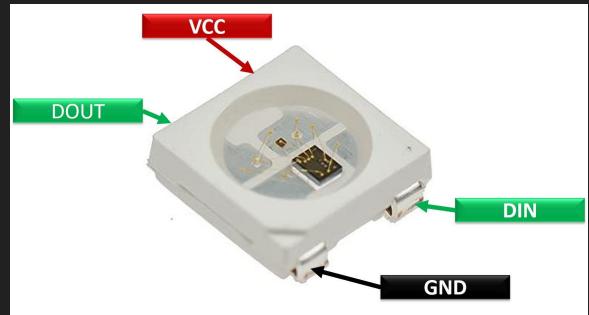




Individually Addressable LED's

WS2812B LED's are chainable RGB lights

- Popular in consumer light strips
- Individually addressable
- Low voltage
- Single pin connection

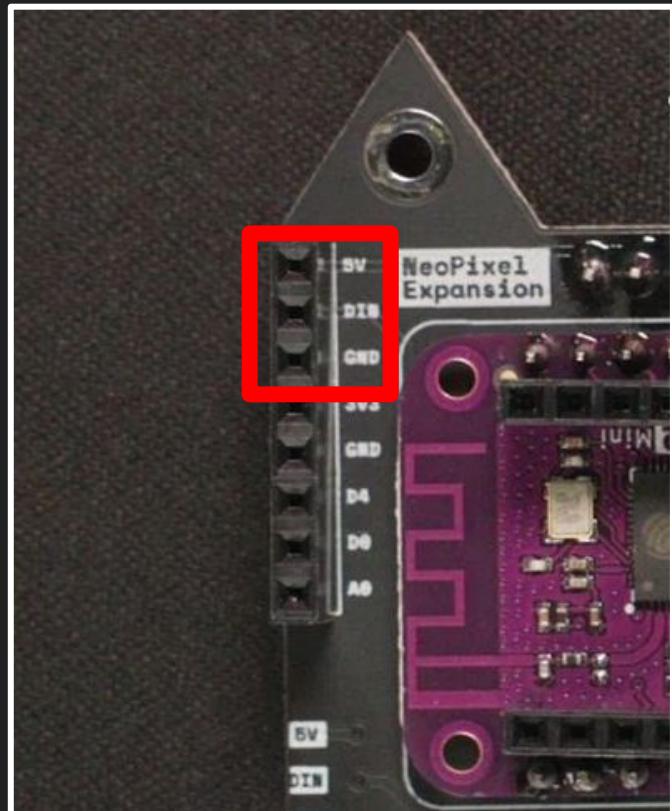




Connecting Your Light Strip



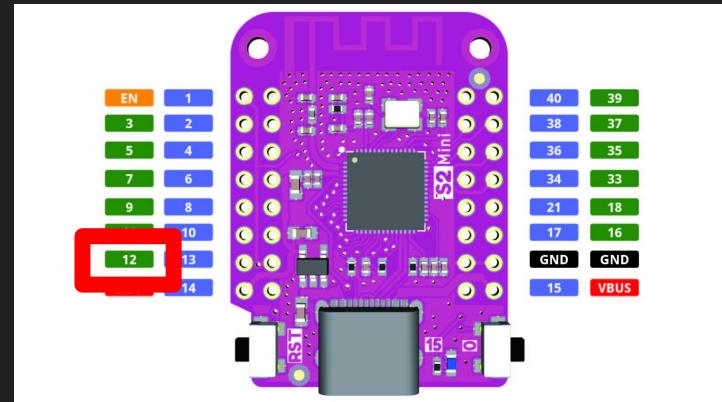
Connect DIN to DIN on the Nugget





Basic Program Logic

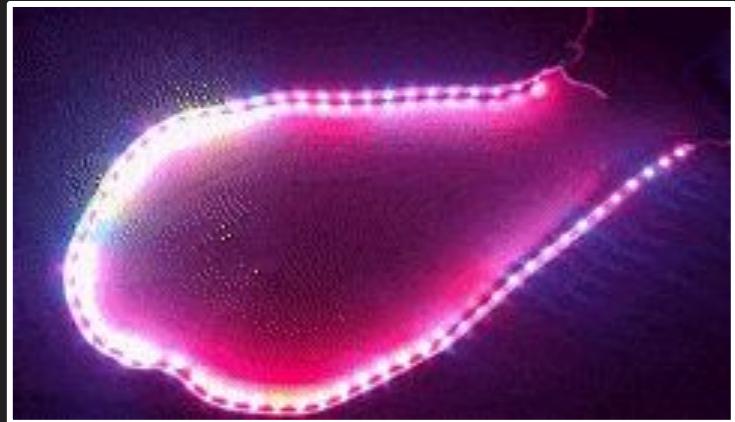
- Tell CircuitPython what pin the strip is plugged in to
- Tell it how many lights there are
- Choose an RGB color
- Use the NeoPixel library to display a solid color on each light
- Try using a loop to set the entire strip



Installing Libraries

<https://github.com/HakCat-Tech/Nugget-Workshops>

We can use code libraries to handle
animations for us.





Animations

<https://learn.adafruit.com/circuitpython-led-animations/basic-animations>

<code>solid</code>	<code>rainbow</code>
<code>blink</code>	<code>sparkle</code>
<code>pulse</code>	<code>chaser</code>
<code>colorcycle</code>	<code>rainbowchase</code>
<code>chase</code>	<code>rainbowcomet</code>
<code>comet</code>	<code>rainbowsparkle</code>
<code>pulse</code>	<code>sparklepulse</code>

Quick Break

In the next part of the workshop, we'll talk about WiFi attacks and reconnaissance techniques, and create the reactive light strip!



WiFi Hacking Class

1 Hour

WiFi Attacks

WiFi Attacks typically happen when a hacker jams a network, or connects without permission.

Why?

- Steal online data & web credentials
- Free network proxy for cybercrime
- Gain access to internal network & exploit devices

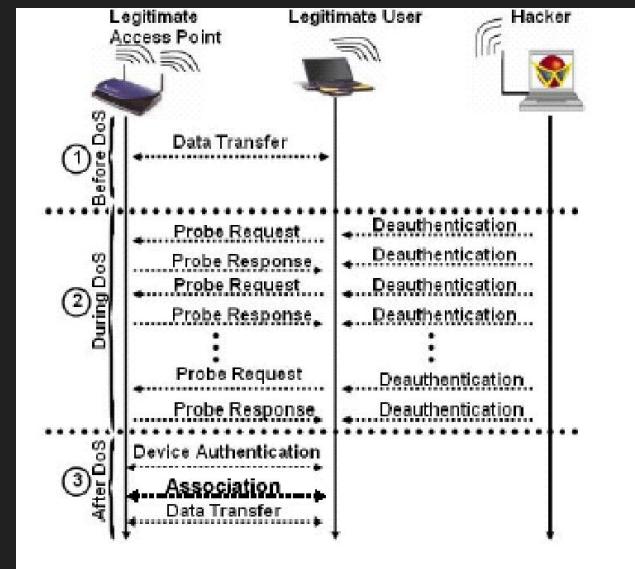




Deauthentication Attacks

Deauth attacks take advantage of the WiFi protocol by spoofing disconnection packets from a legitimate network.

- User gets kicked off network
- When they rejoin, a hacker can capture the hashed WiFi password (handshake)
- Useful for jamming wireless cameras & IOT devices
- Can't be traced down to attacker



Common WiFi Attacks

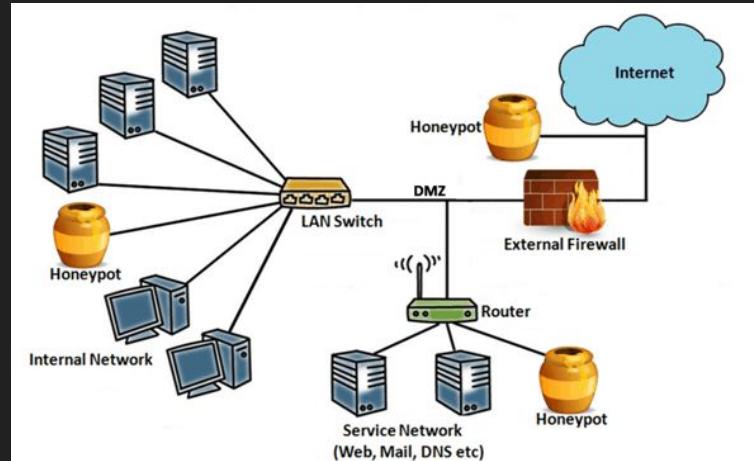
- **KARMA Attack**
 - Uses probe requests to spoof networks you've connected to in the past
- **Offline Handshake Cracking**
 - Uses deauth attack to capture handshake when victim reconnects to WiFi
- **Rogue Access Point**
 - Unauthorized AP connected to a network
- **Evil Twin**
 - Emulates a legit network but overpowers the signal strength
- **PMKID Attack**
 - Allows extraction of password key without deauthentication





Detection & Mitigation

- Forestall attacks w/ **secure credentials** & latest router firmware
- Forestall attacks w/ **WPA-3**: Protected Management Frames
- Detect & stop attacks with a **Wireless Intrusion Detection System (WIDS)**
- Detect breach with **Honeypots**





WiFi Reconnaissance

WiFi Reconnaissance lets us surveil wireless traffic for suspicious activity.

- Detect Deauth frames
- Profile common attacks like KARMA & Evil Twins

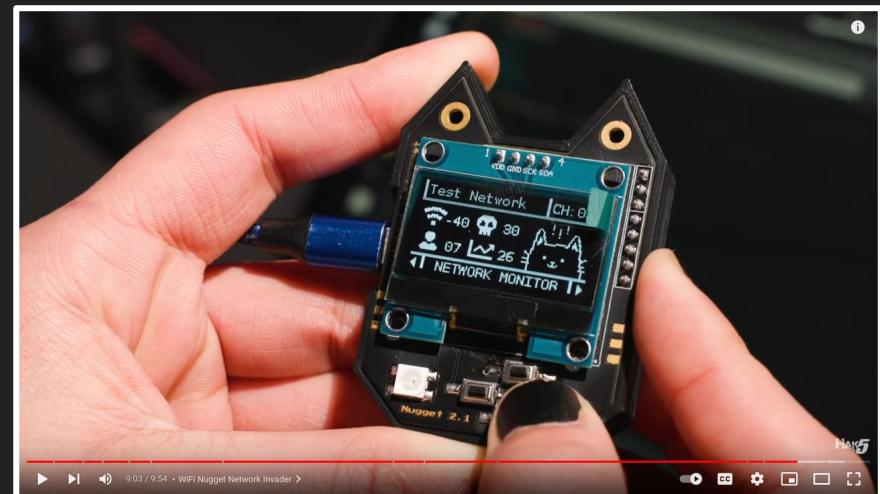
Common tools include Aircrack for recon, and Wireshark for analysis.



Promiscuous Mode

Promiscuous mode allows WiFi devices to see all nearby traffic.

- Networks and clients in the area
- Previously connected networks
- WiFi Attacks





Deauth Detector

Since we can run promiscuous WiFi scans on the Nugget, this means we can sniff for Deauth Attacks!

Try uploading [packetmonitor.py](#) to monitor incoming WiFi packets!



🏆 Challenge

1. Create a hotspot on your phone, and use CircuitPython to find the MAC address of your access point.
2. Create a filter for only packets coming from that device.
3. Add your own animation & graphics once the access point is under attack!



Taking it Further

USB Nugget HID Attack Software

The USB Nugget OS lets you run keystroke injection attacks while getting reactive cat-themed feedback on-screen!

Come to future workshops to learn how to use it!

- Reactive feedback: LED & Screen
- Supports DuckyScript Classic
- Built-in USB Flash Drive
- Remote attacks with WiFi
- Emulate USB devices



Thanks for coming!

Follow [@alexlynd](#) for upcoming events
& check out [hakcat.com](#) for more info.