

# Wi-Fi Tricks with Ghost ESP



If you're interested in learning about wi-fi and Bluetooth networking but you can't afford a Flipper Zero, this workshop is for you! Ghost ESP is a network analysis/testing tool that can run on a low-cost ESP32 microcontroller, as well as variants including the ESP32-C3. Ghost ESP offers wi-fi scanning, custom SSID beacons, captive portal mode, BLE scanning, and even deauth attacks (for demo/testing purposes).

It's super easy to get started! In this workshop we'll install Ghost ESP on our ESP32 & ESP32-C3 devices using the ESPressoFlash web flasher. Then we'll interact with Ghost ESP using the Ghost ESP web serial console or the Arduino IDE.

*Note: The reality of the situation is that using this software without permission at work could get you fired. Messing with financial or government networks could get you sent to prison for several decades. Just something to keep in mind.*

Here's the current GitHub repo for the Ghost ESP project:

[https://github.com/jaylikesbunda/Ghost\\_ESP](https://github.com/jaylikesbunda/Ghost_ESP)



# Add your user to the dialout group (Linux only)

In order to flash the Ghost ESP firmware to your device you'll need access to the USB serial ports. If you're using Linux, there's a good chance you'll need to add your user to the dialout group to make this work.

Open a terminal window and run the following command (case-sensitive). You'll be prompted to enter your password.

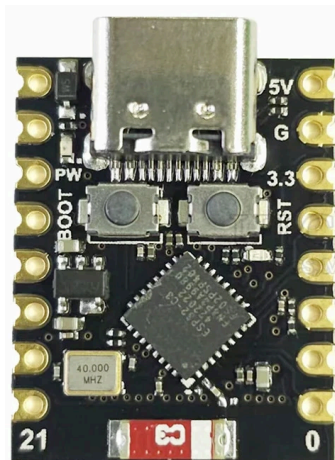
```
sudo usermod -a -G dialout $USER
```

Now reboot your computer with the following command:

```
systemctl reboot
```

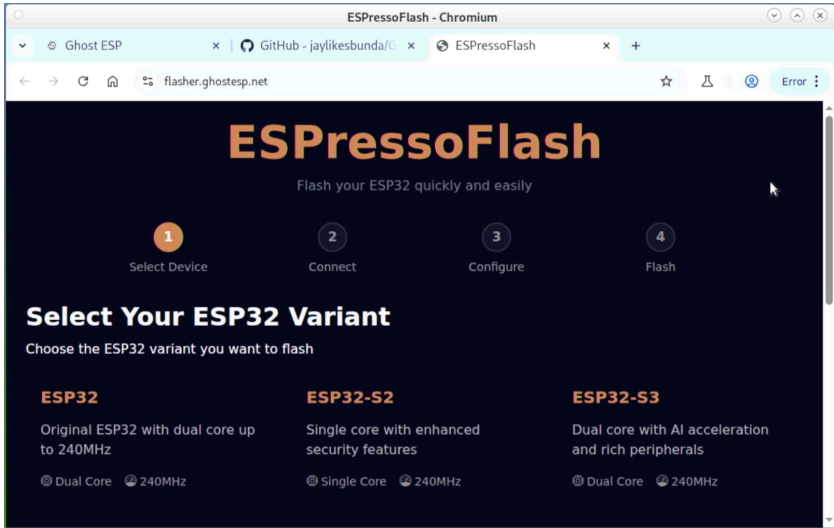
# Flash Ghost ESP to your device

Press the **BOOT** button on your ESP32 device while plugging it into your computer. Once it's connected you can release the button.

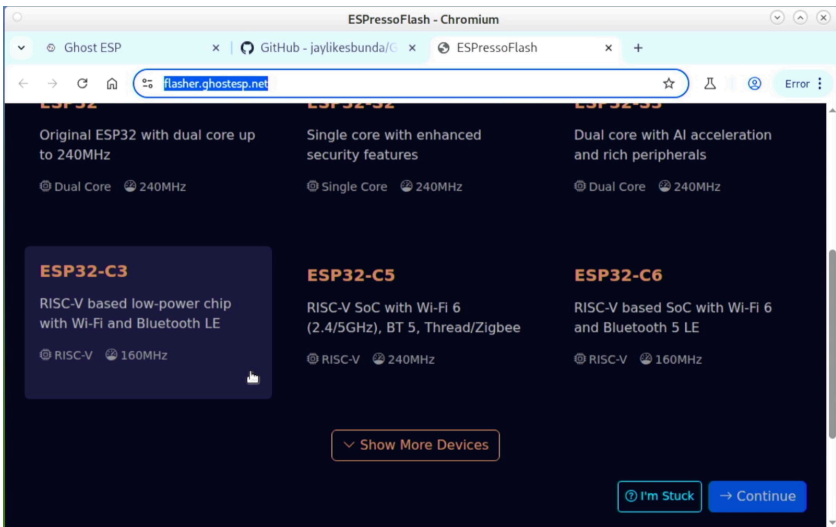


Open Google Chrome or Chromium and go to the following URL:

**`https://flasher.ghostesp.net`**



Select the ESP32 variant you're using, then click **Continue**.

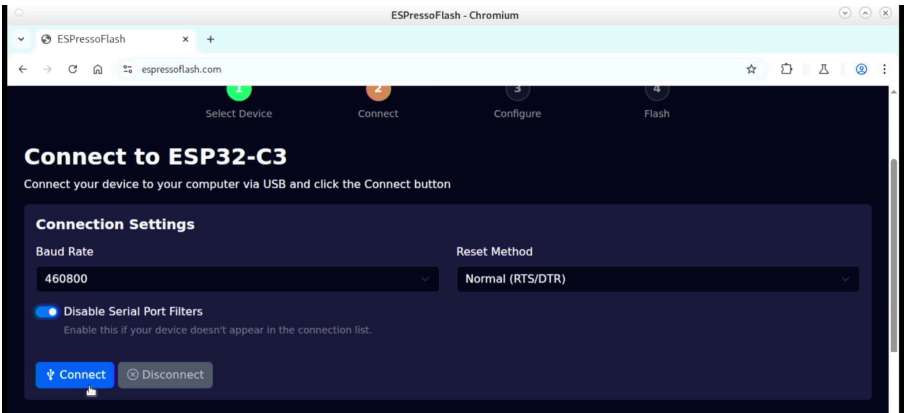




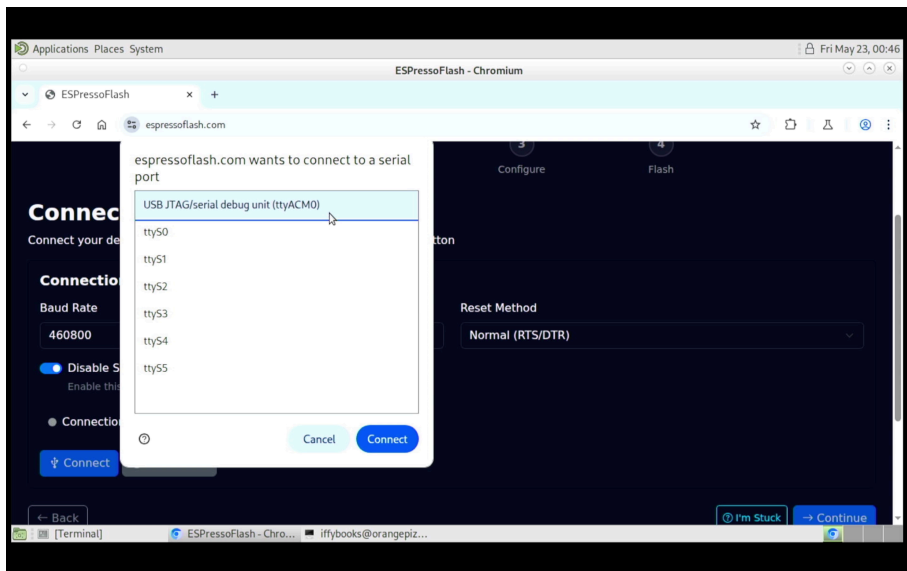
Set the baud rate to 460800.



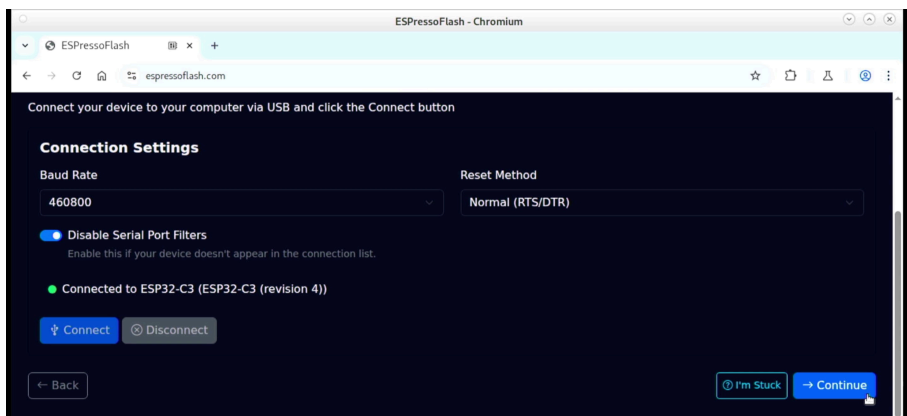
Enable the **Disable Serial Port Filters** option, then click **Connect**.



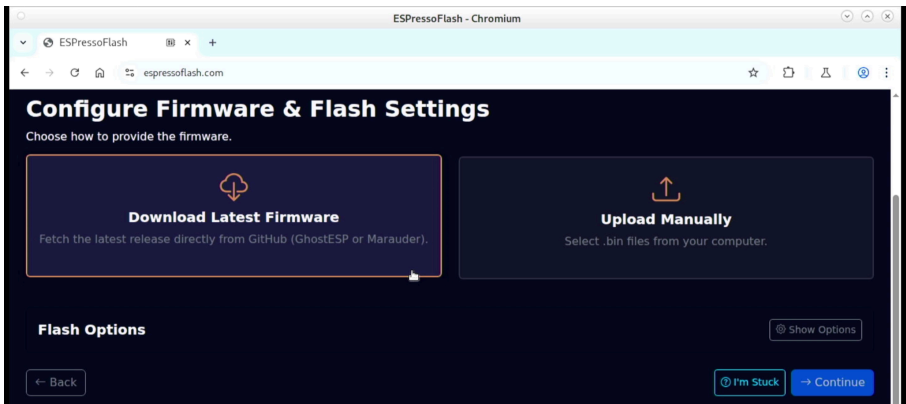
You'll see a list of USB serial ports. If you recognize your device, select it and click **Connect**. (If you aren't sure, unplug your ESP32 device and plug it back in to see which one it is.)



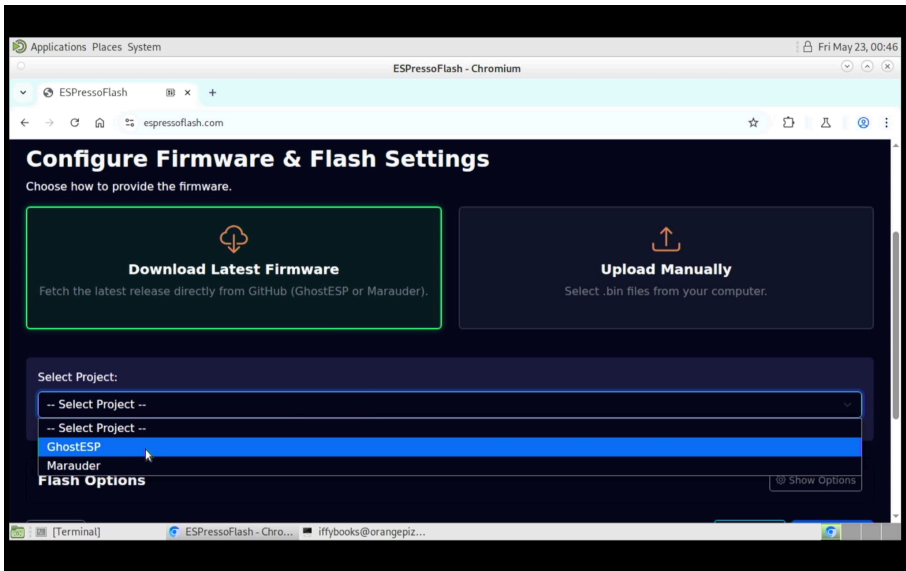
Once your ESP32 device is connected, click **Continue**.



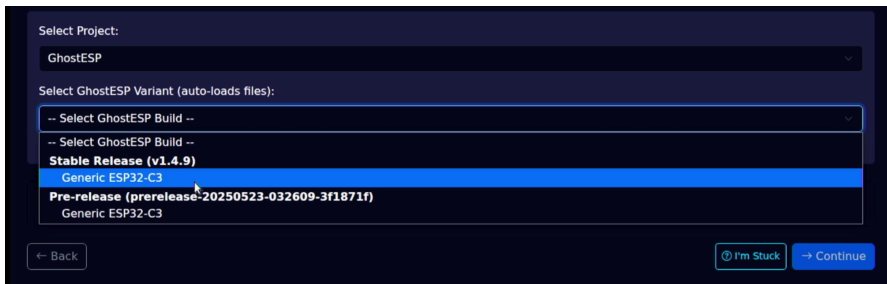
# Select Download Latest Firmware.



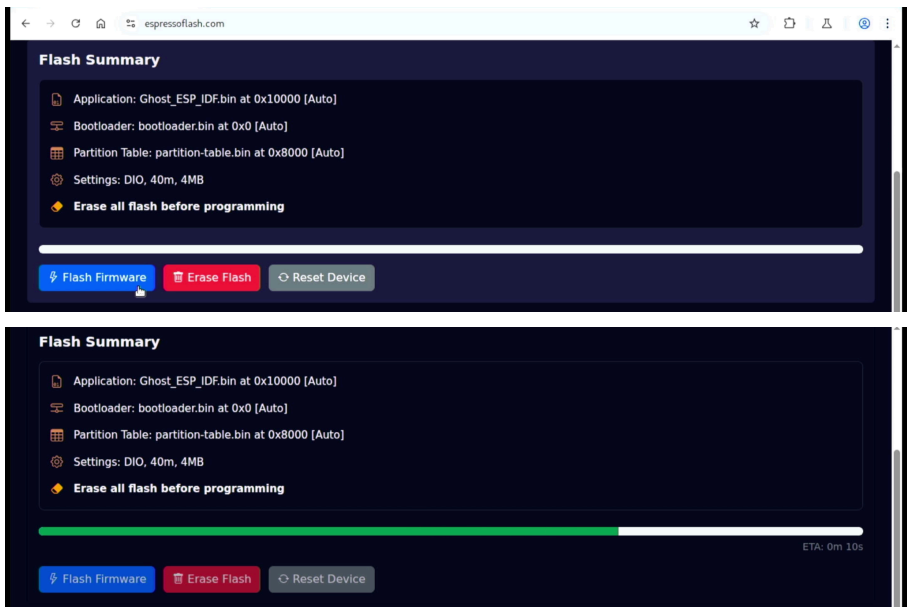
From the **Select Project** dropdown menu, select **GhostESP**.



In the **Select GhostESP Variant** dropdown menu, select the latest stable release.



Click **Flash Firmware** and wait for the flashing process to complete.



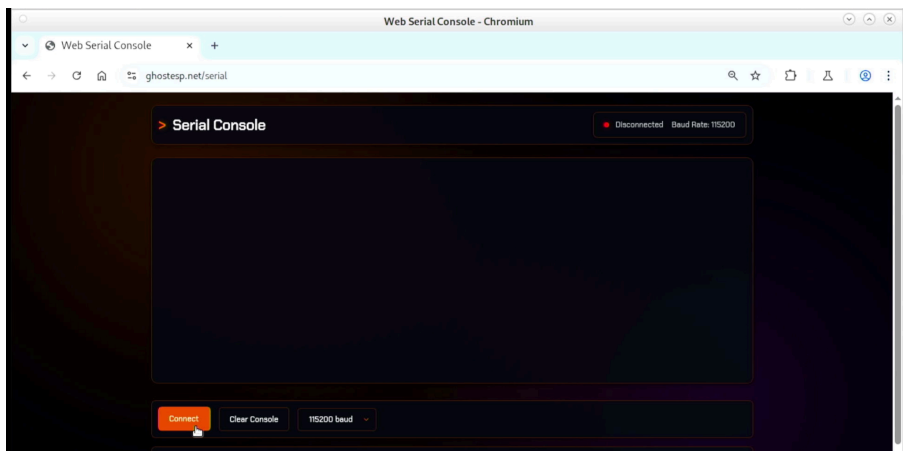
**!** After flashing is completed, unplug your ESP32 device and plug it back in. You'll need to wait 30 seconds or so for it to power on the first time.

# Control Ghost ESP via web serial console

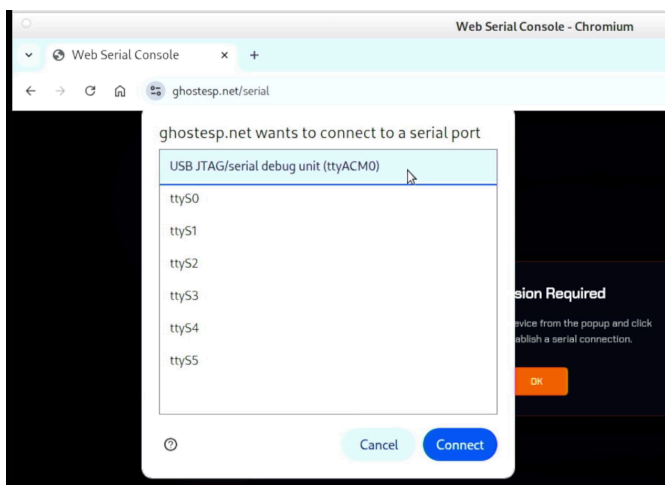
Open Chromium or Google Chrome and go to the following URL to open the web serial console:

**<https://ghostesp.net/serial>**

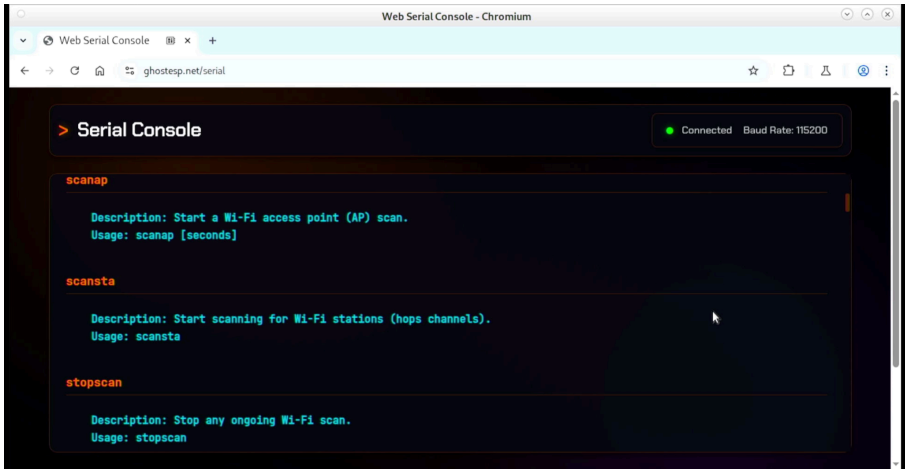
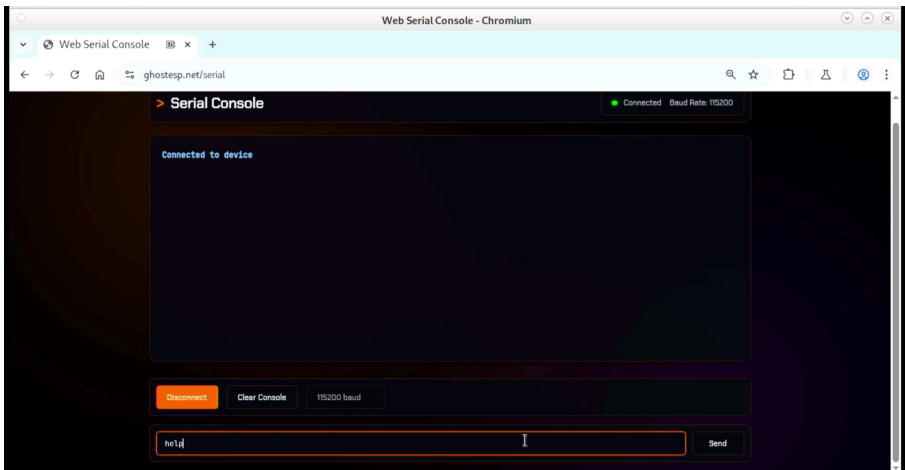
Click **Connect**.



Select your device's serial port from the list and click **Connect**.



Type **help** at the prompt and click **Send**.



# Set your SSID & password

Before we go any further, you should set a new SSID (Service Set Identifier) for your Ghost ESP device, i.e., the name of the wi-fi access point it creates. (The default SSID and password are both "GhostNet", incidentally.)

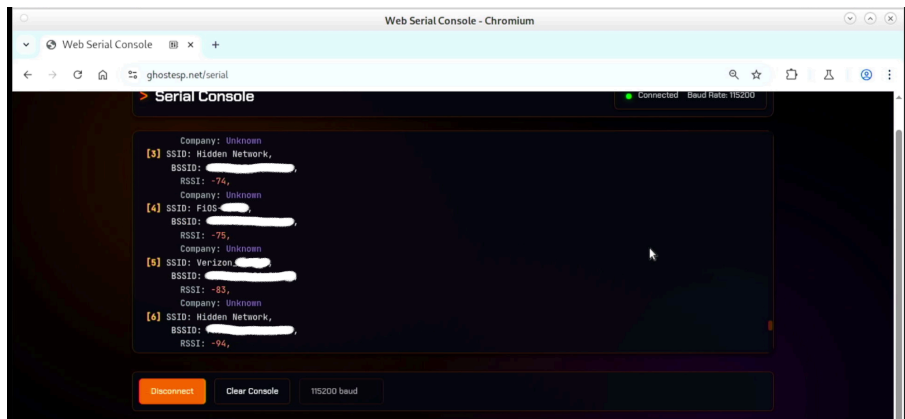
In the serial console window, type **apcred** followed by a unique **SSID name** and the **password** you'll use, separated by spaces. Here's an example:

```
apcred Giraffe_Net frameplaidrain480
```

# Scan for wireless access points

Run the following command to scan for wireless access points (APs).

```
apscan
```



By default, your device will scan for wi-fi networks for 5 seconds. You can run the following command to scan for 30 seconds:

```
apscan 30
```

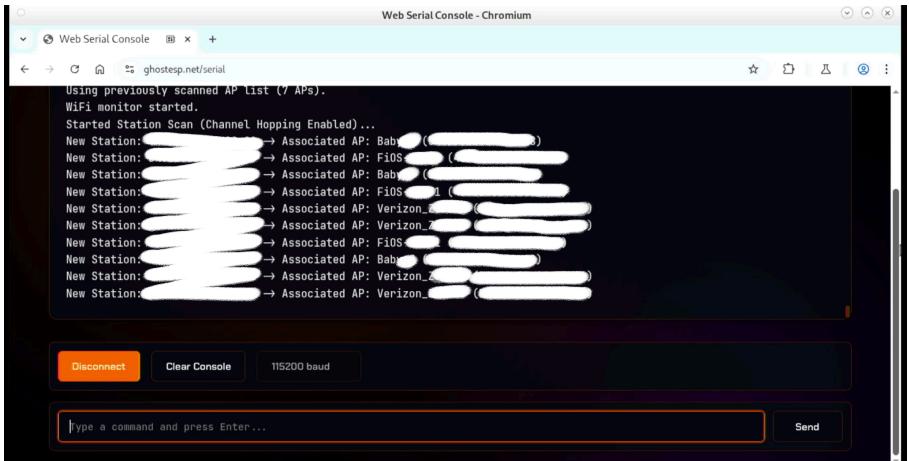
Run the following command to view wi-fi APs in a compact format:

```
list -a
```

## Scan for wi-fi stations

In the language of wireless networking, a "station" is any device connected to a wi-fi network, such as a computer or phone. To view info on wi-fi stations in your immediate area, you can use this command:

```
scansta
```



The station scan will keep running until you stop it with the following command:

```
stopscan
```

Run the following command to view wi-fi stations in a compact format:

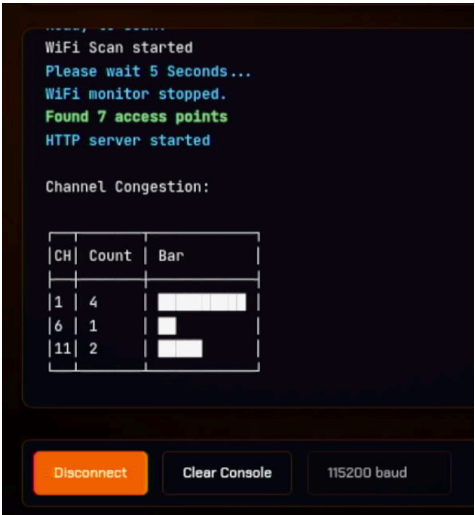
```
list -s
```



# Visualize network congestion

Run this command to view how much traffic there is on each wi-fi channel:

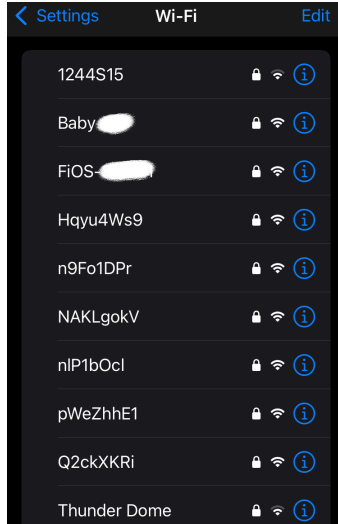
**congestion**



# Make SSID Beacon Spam

Ghost ESP's beacon spam feature lets you broadcast one or more wi-fi SSIDs that don't actually work. The following command creates a lot of fake wi-fi networks with random names:

```
beaconspam -r
```



Use this command to stop broadcasting fake wi-fi networks:

```
stopspam
```

This command creates a fake wi-fi network called BlahBlahBlah.

**beacomspam BlahBlahBlah**



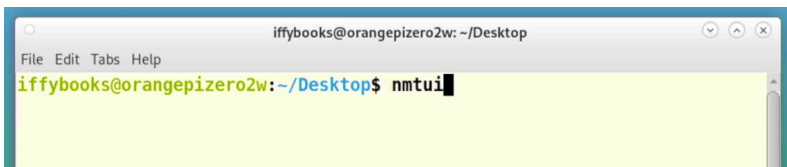
You can potentially use this feature for propaganda / self-promotion purposes, but people are likely to find it annoying. So use your judgment.

## Connect to Ghost ESP wi-fi AP

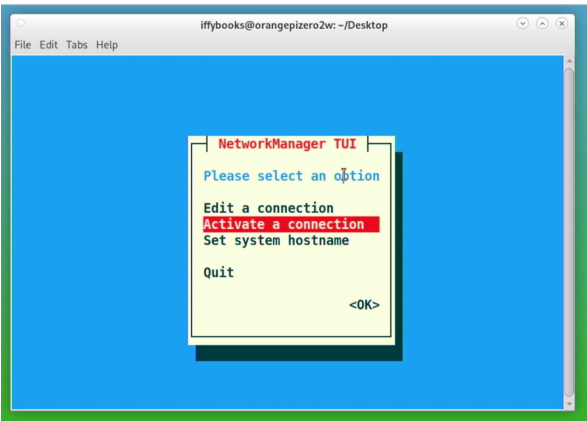
Next you'll control your Ghost ESP device via wi-fi AP. If you're using a laptop, go to your wi-fi settings and connect to the network with the SSID you chose earlier.

If you're using a lab computer at Iffy Books, follow these steps to connect to a wi-fi network:

Open a terminal window and run the command **nmtui** to launch the Network Manager text user interface.



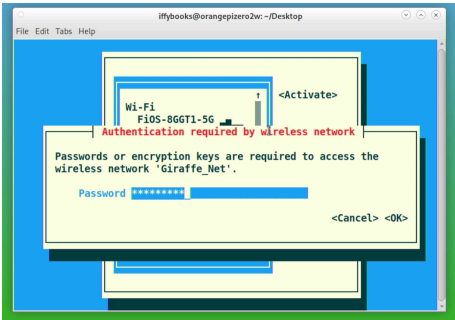
Use the arrow keys to select **Activate a connection** and press **enter**.



Select your device's SSID and press **enter**.



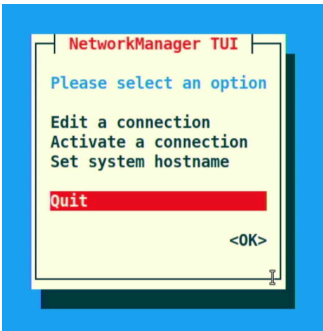
Enter your password, use the arrow keys to select **OK**, and press **enter**.



Select **Back** and press **enter**.



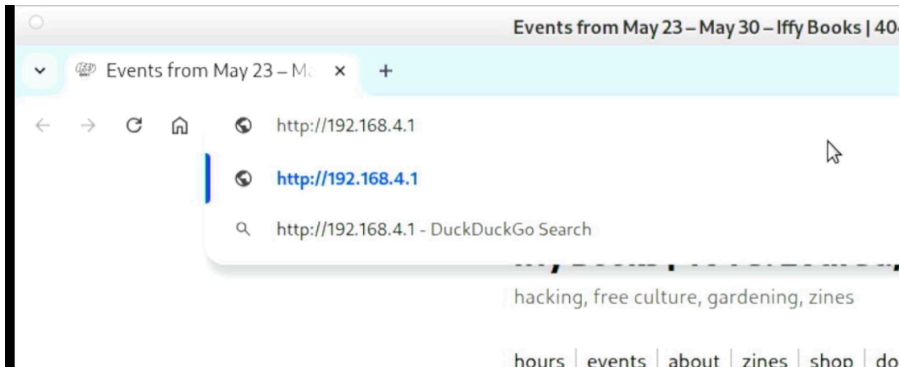
Select **Quit** and press **enter** to close the Network Manager TUI.



# Open the Ghost ESP browser interface

Open a web browser and go to the following address:

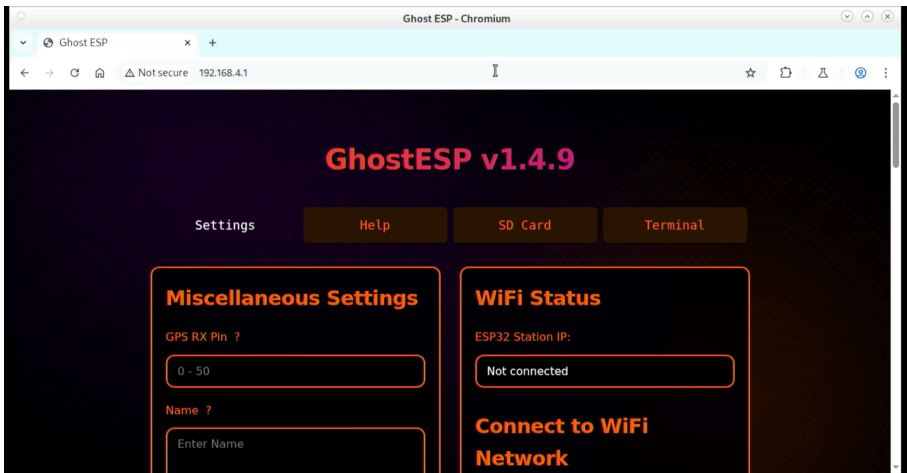
**http: //192.168.4.1**



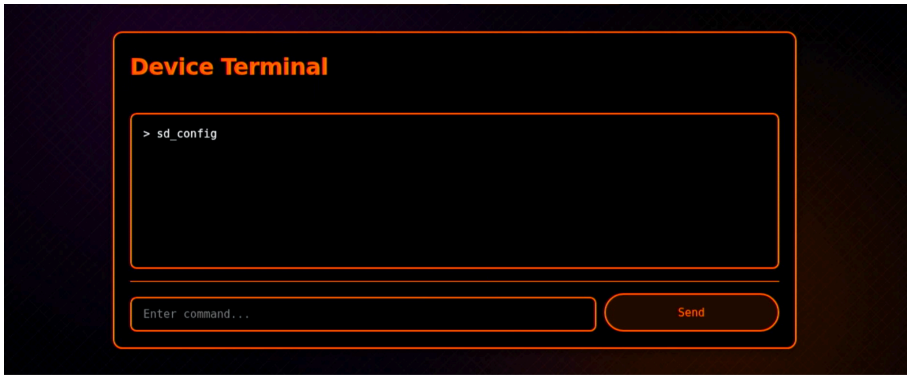
You'll be prompted to enter a username and password. The username is your SSID and the password is the one you set earlier.



You're in the Ghost ESP browser interface!

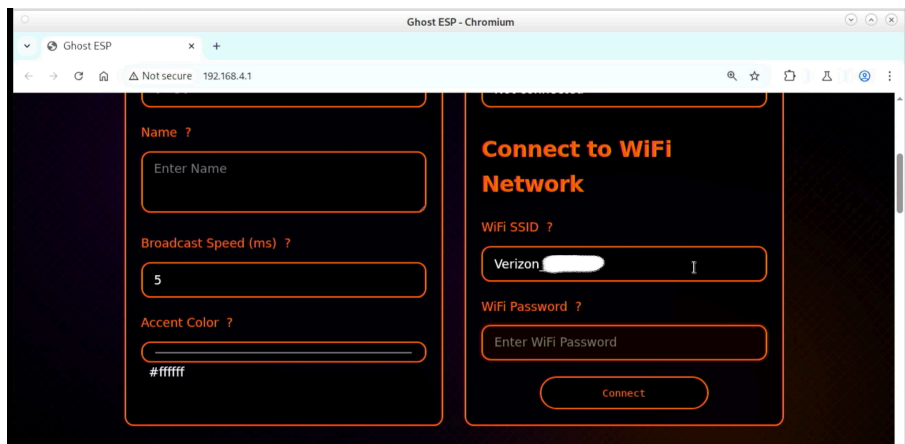


The most important part is the **Terminal** tab, where you can run commands like the ones we've been using in the web serial console.



# Connect Ghost ESP device to local wi-fi network

Scroll down to Connect to WiFi network and enter the SSID and password for the router you're using (such as your home router, which you use to connect to the internet).



The screenshot shows a web browser window titled "Ghost ESP - Chromium" with the address bar displaying "Not secure 192.168.4.1". The page content is divided into two main sections. The left section contains three configuration options: "Name ?" with an input field containing "Enter Name", "Broadcast Speed (ms) ?" with an input field containing "5", and "Accent Color ?" with a color picker showing "#ffffff". The right section is titled "Connect to WiFi Network" in orange. It contains two input fields: "WiFi SSID ?" with the text "Verizon" and a cursor, and "WiFi Password ?" with the text "Enter WiFi Password". Below these fields is a "Connect" button.

# Scan ports on your local network

Run the following command to scan for common ports on the local network:

```
scanports local -C
```



# Open Questions

- Can we get the evil portal (captive portal) feature working? There's supposedly a default HTML file included with the firmware, but we haven't been able to get it working.
- Does the network printing feature work?
- Does the SD card feature work? We've been trying with an SD card breakout board, which requires recompiling the firmware to turn on SPI mode. But so far we haven't had success.

You can find the Ghost ESP wiki here:

[https://github.com/jaylikesbunda/Ghost\\_ESP/wiki](https://github.com/jaylikesbunda/Ghost_ESP/wiki)



Ghost ESP revival Discord:

<https://discord.gg/5cyNmUMgwh>



An article on improving the antenna on the ESP32-C3:

<https://peterneufeld.wordpress.com/2025/03/04/esp32-c3-supermini-antenna-modification>

