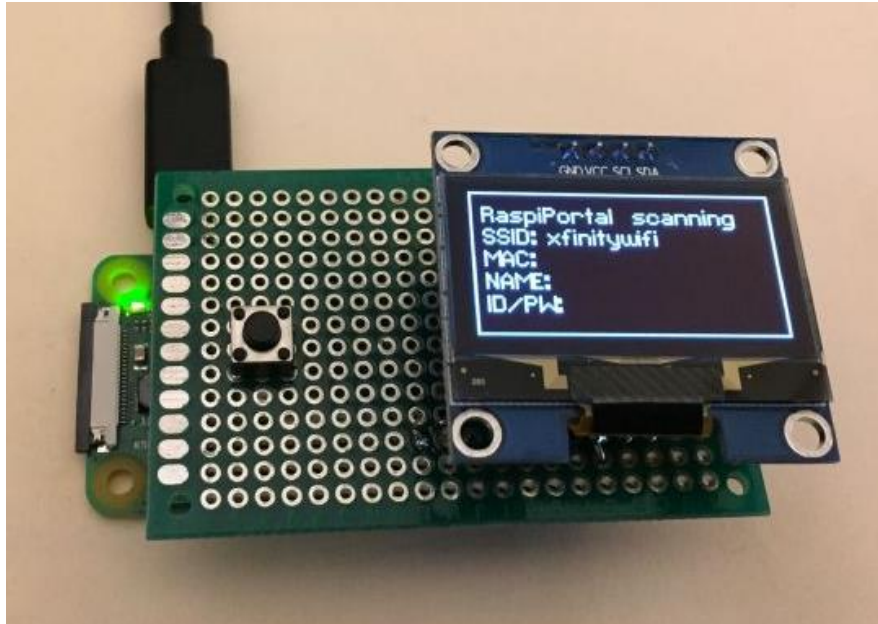



# Captive Portal Honey Pot using Raspberry Pi Zero W

2019-04-16 – rgrokkett






## Sign in

with your Google Account

[More options](#)

[NEXT](#)

English (United States) ▼   [Help](#)   [Privacy](#)   [Terms](#)



Sign in to your Xfinity account to get online now.

[Sign In](#)

[Forgot your username or password?](#)

### Not an Xfinity customer? No Problem.

Start your free WiFi On Demand trial or buy a pass today.

[Get Started](#)

Create a free account and download your

## Overview

This is a security related test project that allows you to set up a WiFi Access Point captive portal honey pot using a Raspberry Pi Zero W. (or other Raspberry Pi). This project adds a small OLED screen, battery power and case to a \$10 Pi Zero W for use in security auditing users via a social engineering attack.

It builds off the work done by BrainDead Security updated to run under Raspbian Stretch using PHP 7 and lets you select between two different captive portal emulations: Google login and Xfinity Wifi.

<https://braindead-security.blogspot.com/2017/06/building-rogue-captive-portal-for.html>

As noted on their web site, this is to demonstrate how a malicious WiFi access point can be built from simple and low cost components and how you should learn to detect and protect yourself against such attacks.

This project consists of configuring a base Raspbian Stretch Lite OS into a WiFi Access Point, then applying a captive portal web server. The display allows you to see any activity occurring during testing without logging into the server.

## Requirements

- Raspberry Pi Zero W
- 8 GB or larger SD Card
- 5V battery (such as for charging a phone)
- Raspbian Stretch Lite

### Temporarily need:

- 5V 2A Power supply for Raspberry
- USB keyboard for Raspberry (no mouse needed)
- HDMI monitor

### Optional OLED Display

If you would like the status display and Power Down button, add:

- I2C Serial 128x64 SH1106 OLED LCD  
[https://www.amazon.com/dp/B07BHHV844/ref=cm\\_sw\\_em\\_r\\_mt\\_dp\\_U\\_N9kpCbV14V130](https://www.amazon.com/dp/B07BHHV844/ref=cm_sw_em_r_mt_dp_U_N9kpCbV14V130)
- 1 – micro momentary push button  
[https://www.amazon.com/dp/B01GN79QF8/ref=cm\\_sw\\_em\\_r\\_mt\\_dp\\_U\\_61ltCbHBHTSKH](https://www.amazon.com/dp/B01GN79QF8/ref=cm_sw_em_r_mt_dp_U_61ltCbHBHTSKH)
- Wire, soldering equip, small box to put everything in.

You can access the Raspberry for initial setup using a keyboard and HDMI monitor. This is just temporary.

The final portal will only need the Zero W with SD card and 5V battery. Optionally, you can add the OLED display for status information.

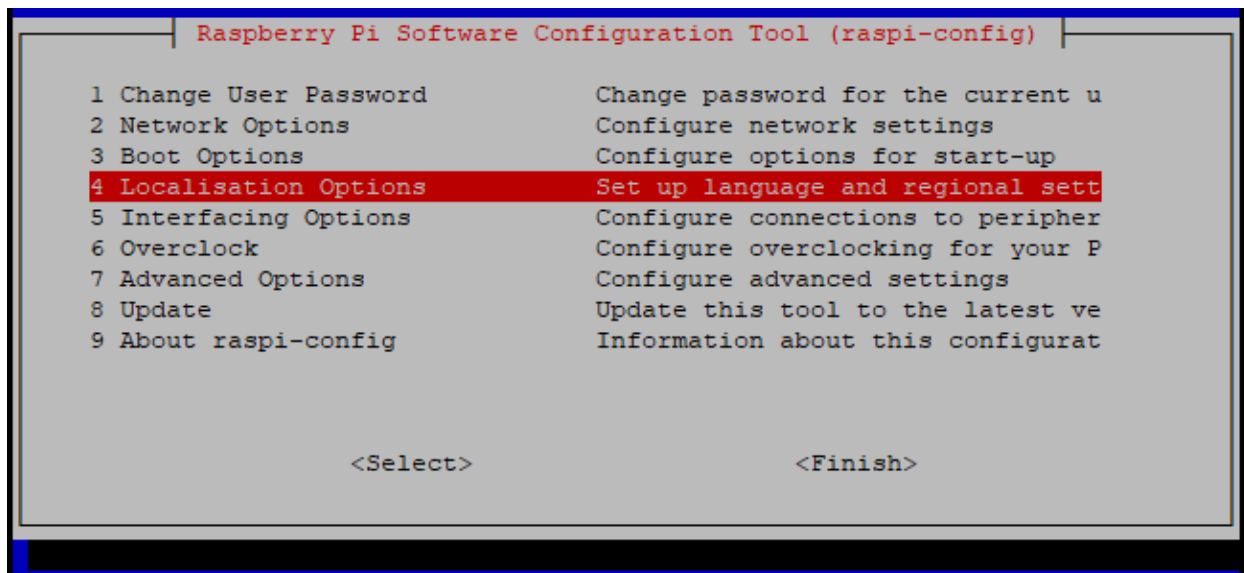
## Initial Setup Procedure

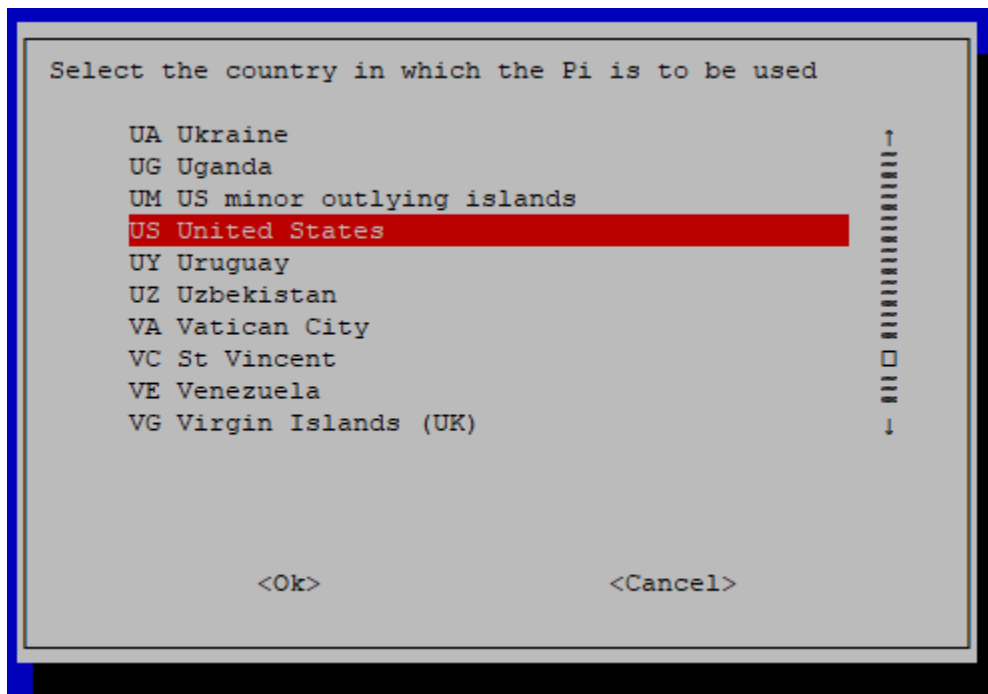
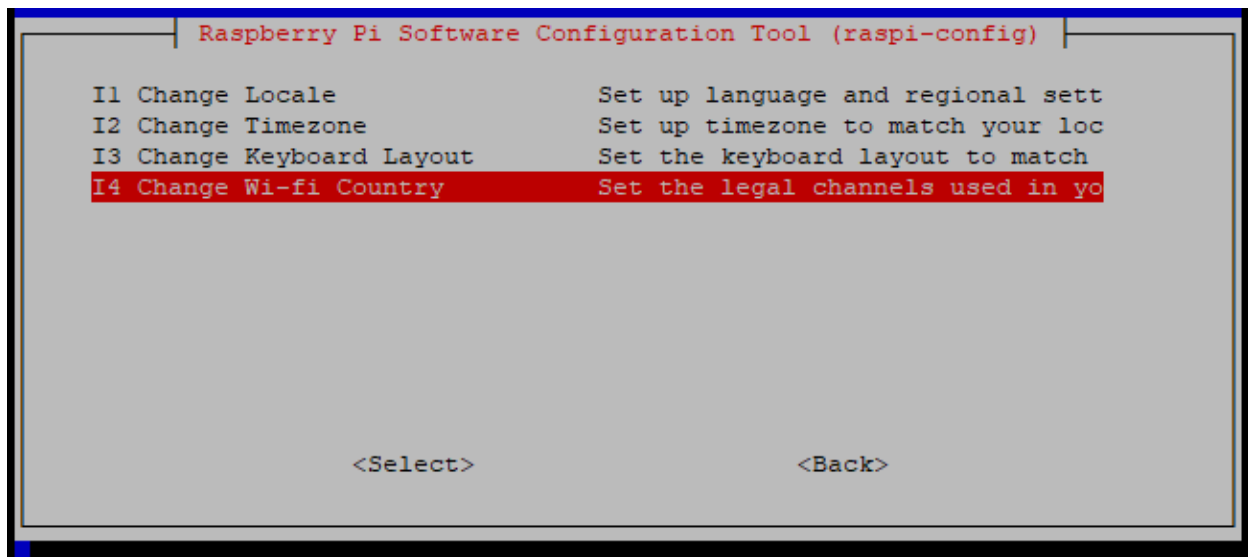
1. If you haven't already, install **Raspbian Lite** version onto a 8GB or larger microSD card. You DO NOT need the GUI version, as this project does not use the GUI.  
<https://www.raspberrypi.org/downloads/raspbian/>
2. Plug in a keyboard & HDMI monitor temporarily.  
Alternately, use a USB Ethernet Adapter.  
DO NOT use the WiFi as it will be altered by this installation and will not be accessible from your local WiFi network.
3. Power up your Pi using a 5V power supply.  
Wait until your Pi boots.
4. Login with pi/raspberry
5. At shell prompt, enter the following commands:

```
$ sudo apt update
$ sudo apt upgrade
$ sudo raspi-config
```

Change the User password

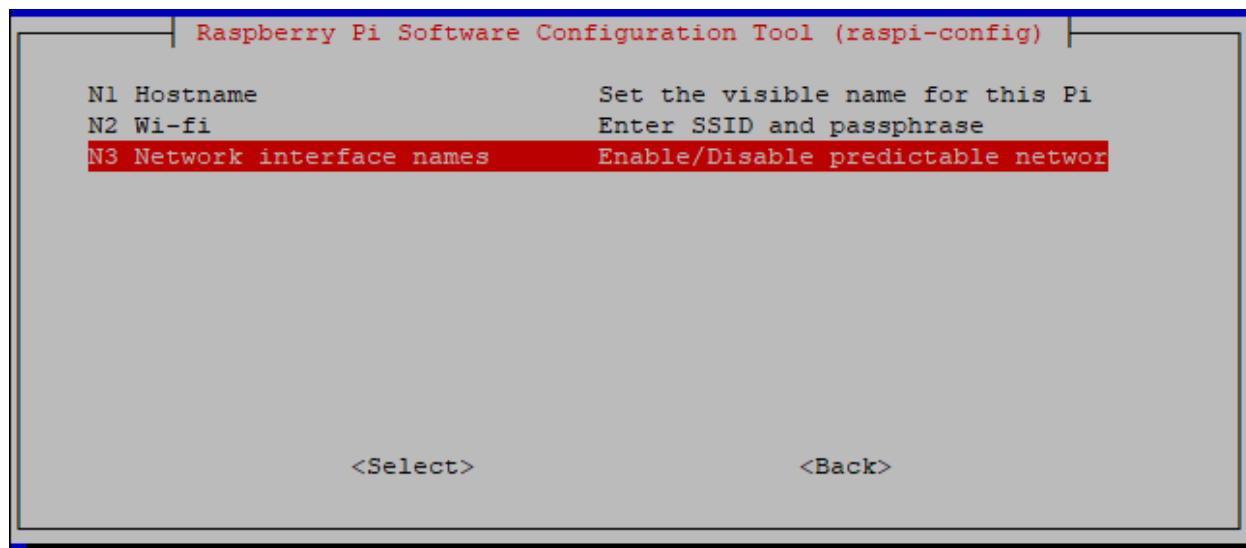
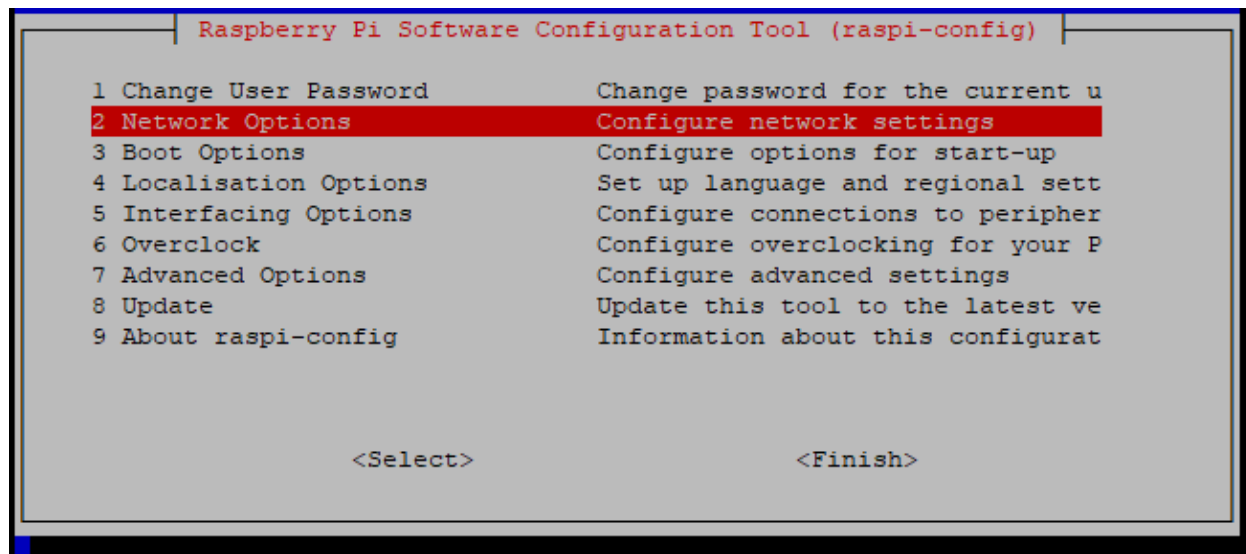
Change the WiFi country: Localization -> Change WiFi country





Set Network Interface names to Predictable:

Network Options -> Network Interface Names -> Enable (Yes)

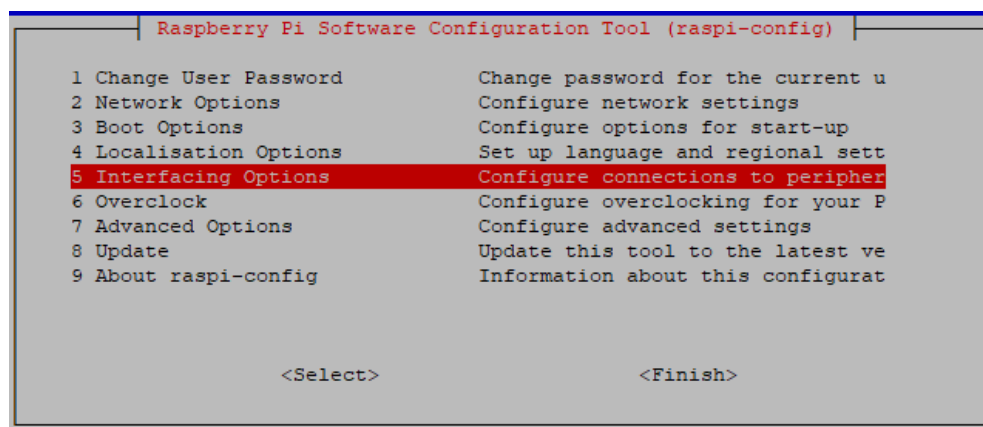


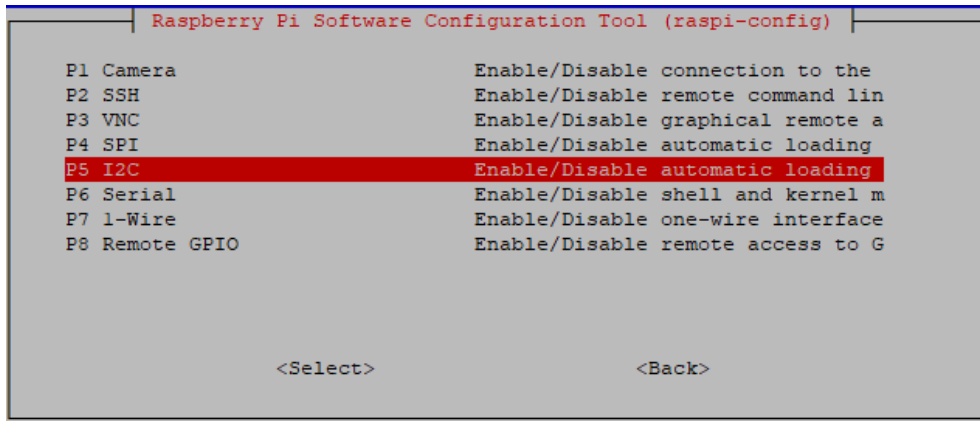


6. Turn on I2C interface:

Interfacing Options -> I2C -> Yes

(Enable I2C interface. *See below screens*)





7. Once enabled, TAB to "Finish" and answer "Yes" to reboot.

8. Add the Portal packages:

```
sudo apt-get install git
git clone https://github.com/rgrokett/rogue-captive
cd rogue-captive
sudo bash install.sh
sudo reboot
```

During installation, macchanger will ask whether or not MAC addresses should be changed automatically - choose "No". The startup script in rc.local will perform this task more reliably.

You select which type portal you want during installation. You can change by rerunning the install.sh script and then rebooting.

After reboot, look for an access point name displayed at the end of the install. Connecting to it from an Apple or Android device should automatically bring up a captive portal login screen.

## Testing Access Point and Captive Portal



You can try to connect (its open, no password) to the access point according to which one you installed, either xfinitywifi or Google Free Wi-Fi

A screenshot of the Google sign-in page. It features the Google logo at the top, followed by 'Sign in with your Google Account'. There are two input fields: 'Enter your email' and 'Enter your password'. Below the password field is a red 'More options' link. A blue 'NEXT' button is at the bottom right. At the bottom of the page, there's a language selector 'English (United States)' and links for 'Help', 'Privacy', and 'Terms'.A screenshot of the Xfinity sign-in page. It has the 'xfinity' logo at the top. Below it is the text 'Sign in to your Xfinity account to get online now.' There are two input fields: 'Username, Email, or Mobile #' and 'Password'. A blue 'Sign In' button is below the password field. A link 'Forgot your username or password?' is below the button. Below a horizontal line, it says 'Not an Xfinity customer? No Problem.' followed by 'Start your free WiFi On Demand trial or buy a pass today.' A blue 'Get Started' button is at the bottom. At the very bottom, it says 'Create a free account and download your'.

If you enter info into either screen, the data will be written to files at

```
/var/www/html/creds.txt  
/var/www/html/data.txt
```



Once active, you can still SSH into the Pi using Putty or ssh by connecting to the pi@10.1.1.1 via WiFi (you don't need to "sign in", just close your browser.)

You can also use a browser to access:

- a. Connect your laptop or wifi tablet to the SSID
- b. Ignore the Login screen
- c. Open browser to <http://10.1.1.1/data.txt>

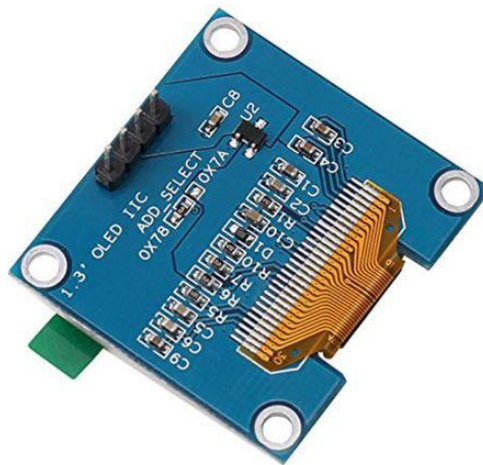
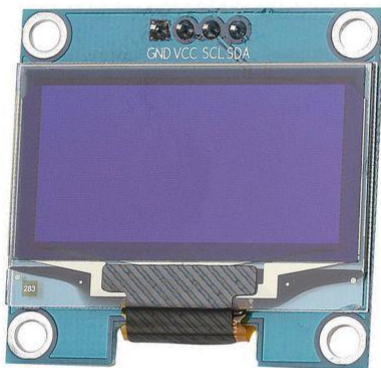
## Optional: Adding OLED Display Hardware

To add the OLED display and power off button, shutdown your pi and wire in the following:

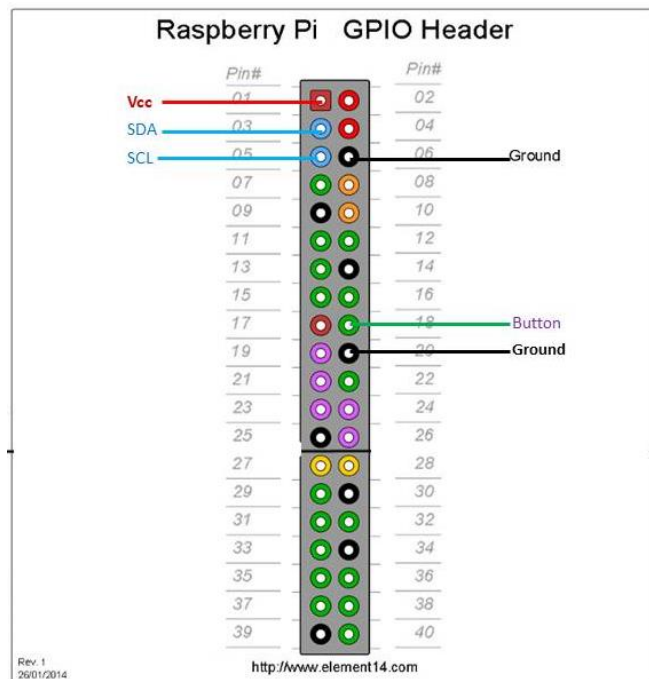
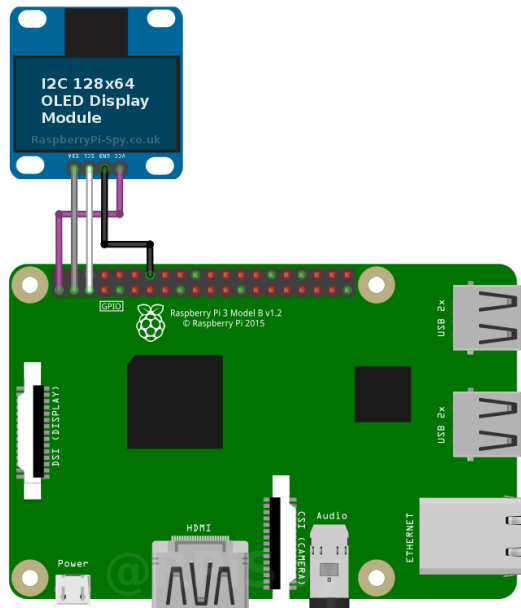
```
$ sudo shutdown now
```

Unplug the 5V power adapter.

Add the screen using the info below.



OLED Pin	Pi Header Pin	Notes
Vcc	1	3.3V
Gnd	6	Ground
SCL	5	I2C SCL
SDA	3	I2C SCA



### Install the OLED Software:

1. Power up the Pi using 5V power supply
2. Log in again using pi and your password
3. Run the install OLED script:

```
cd rogue-captive
bash installOLED.sh
sudo reboot
```

*NOTE: If you get **Red python Error** messages, be sure that your I2C interface is turned on via raspi-config (see previous section). Also reboot and then rerun the installOLED.sh script.*

4. Log back in and test the screen if needed.

```
$ python testOLED.py
```

You should see a simple “Hello World” test appear.

Otherwise, you should see a display similar to this:



The display shows the currently used SSID, MAC address, Device Name and any login credentials entered. New: Displays the number of unique devices that connected since last reboot.

For more information on OLED, check out these sources:

- <https://www.raspberrypi-spy.co.uk/2018/04/i2c-oled-display-module-with-raspberry-pi/>
- <https://github.com/rm-hull/luma.oled>
- <https://luma-oled.readthedocs.io/en/latest/intro.html#>

## Optional GPIO Power Down Button Wiring

You can add a momentary push button to trigger a graceful shutdown of the Pi. It is connected from a GPIO pin to Ground. When pushed, this will bring the GPIO pin to ground, which the python software will detect and execute a shutdown.

1. Shutdown the Pi and unplug the power  
`$ sudo shutdown now`
2. Wire up the button to the pins shown

Button	Pi Header Pin	GPIO
1	18	24
Gnd	20	Ground

3. Power up the Pi again and log back in
4. Test by pressing the button momentarily. The Pi should initiate a shutdown.  
Note that the screen will take a few seconds before it turns dark.
5. Remove power to completely shut down the system after the Green LED on the Raspberry Pi goes off.