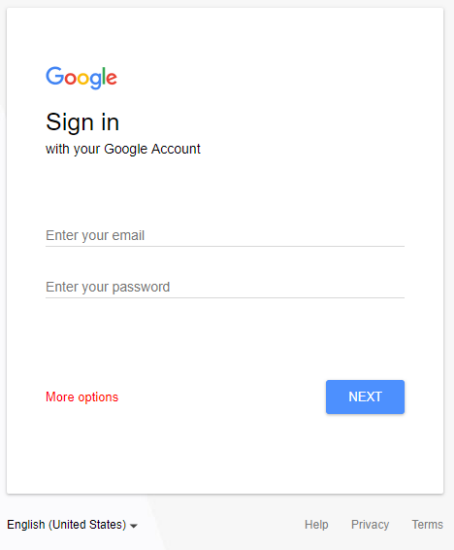
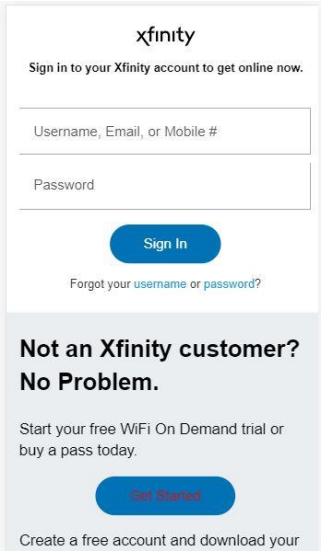
Captive Portal Honey Pot using Raspberry Pi Zero W

2019-04-02 – rgrokett

TODO PHOTO of Finished system





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
- 1 – micro momentary push button
  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.

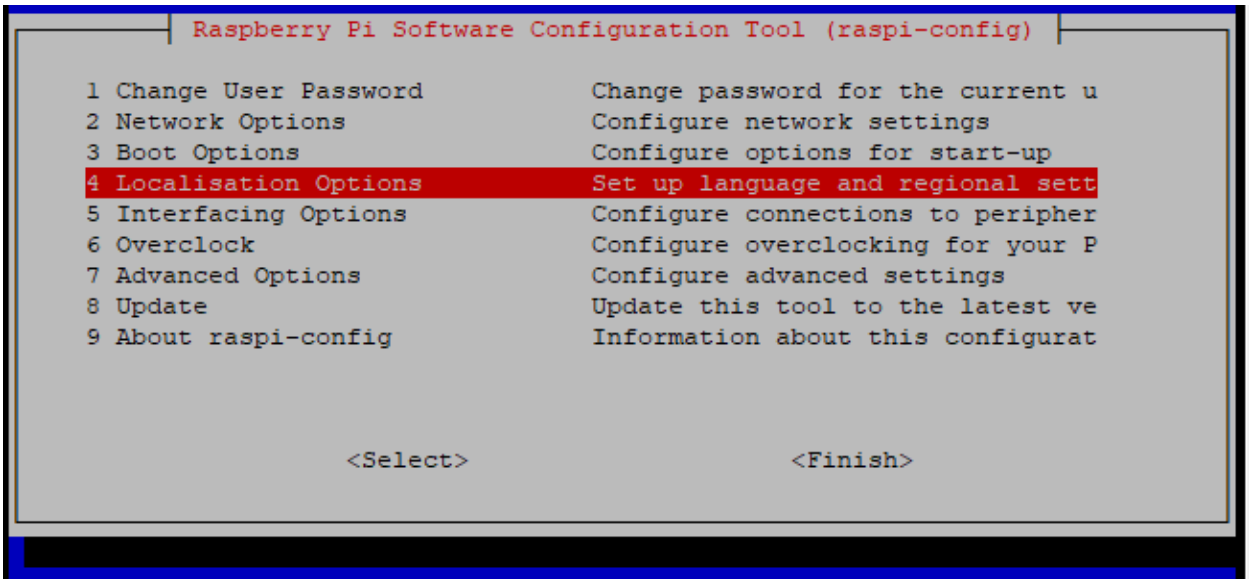
3. Power up your Pi using a 5V power supply.
   Wait until your Pi boots.

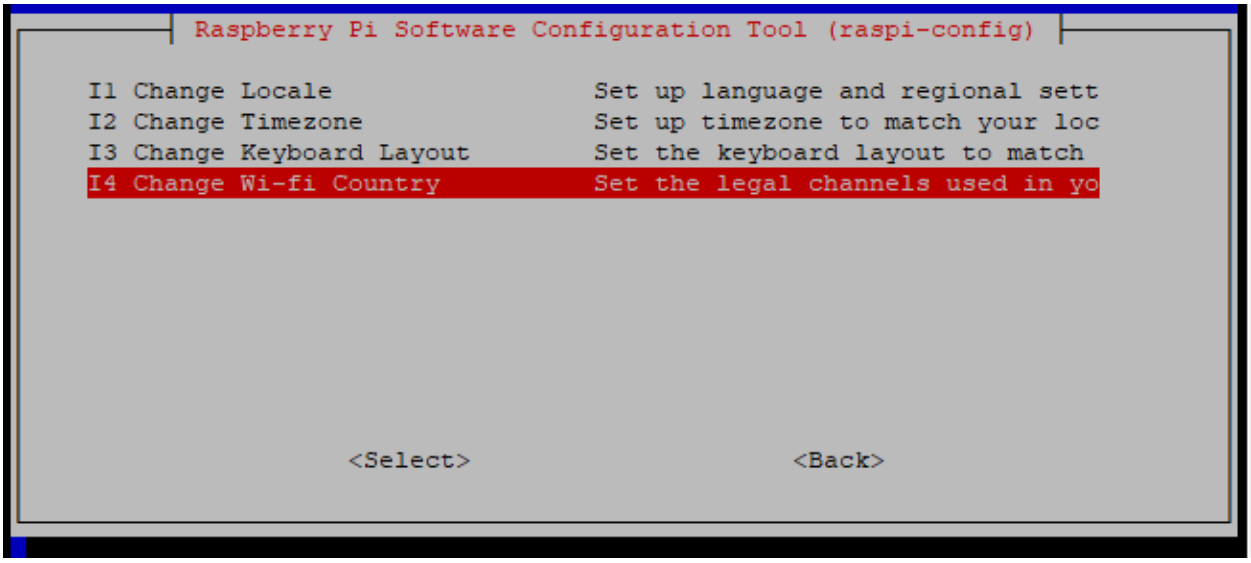
4. Login with pi/raspberry
5. At shell prompt, enter the following commands:

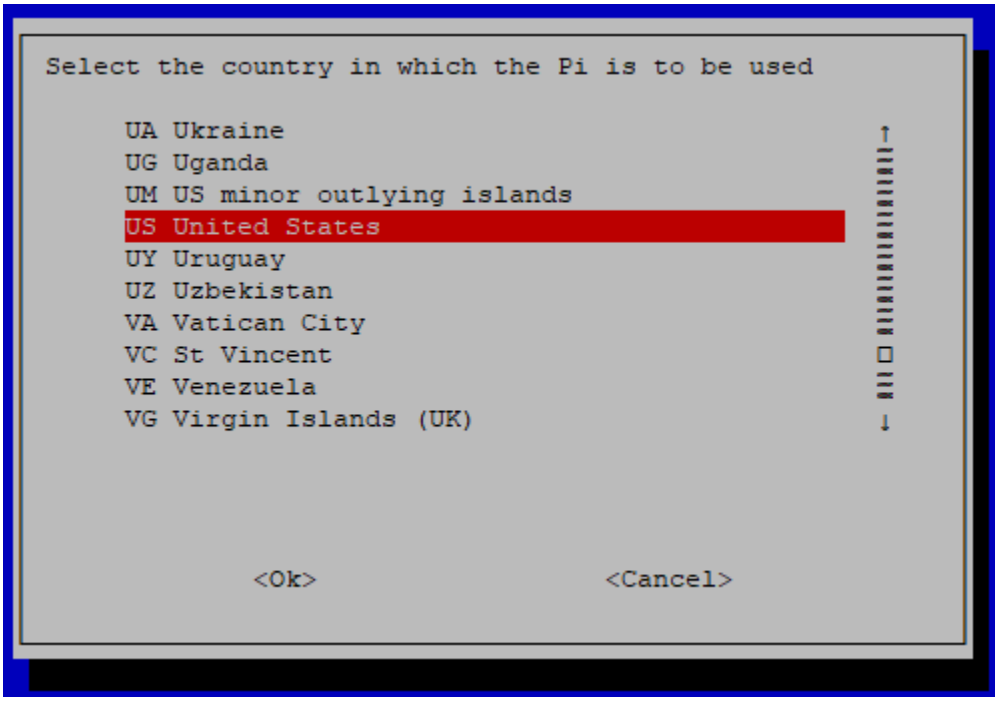
```
$ sudo apt update
$ sudo apt upgrade
$ sudo raspi-config
```

Change the User password

Change the WiFi country: Localization -> Change WiFi country

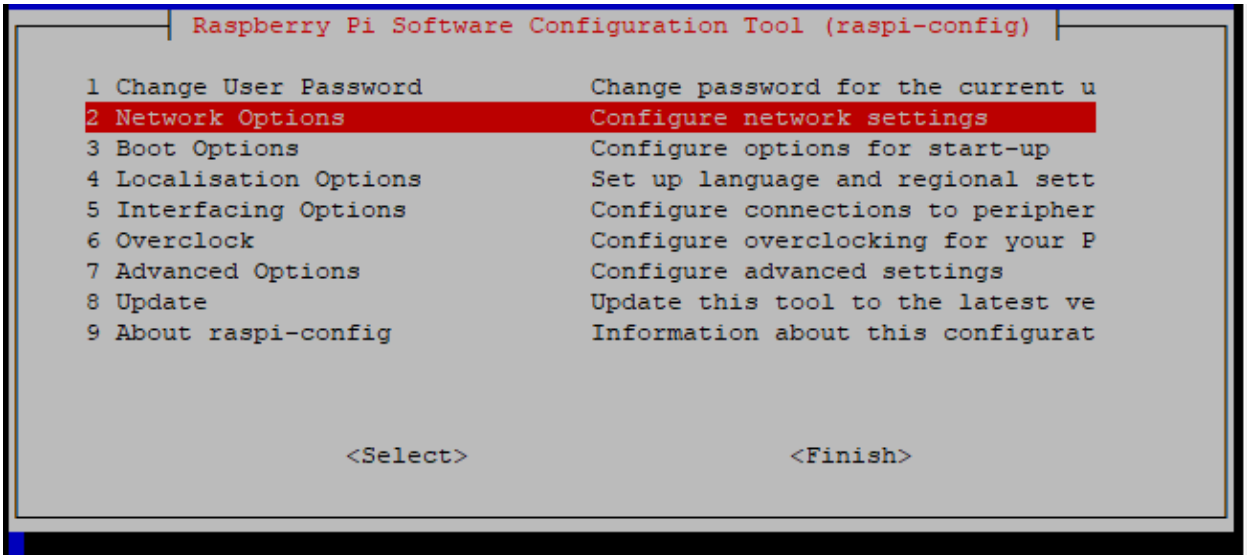


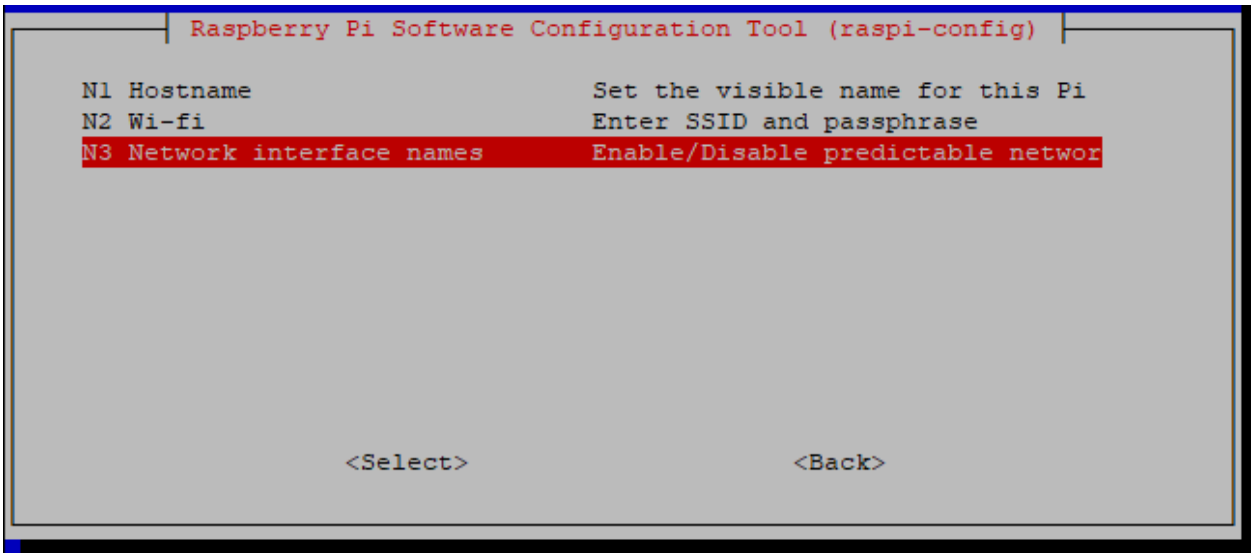


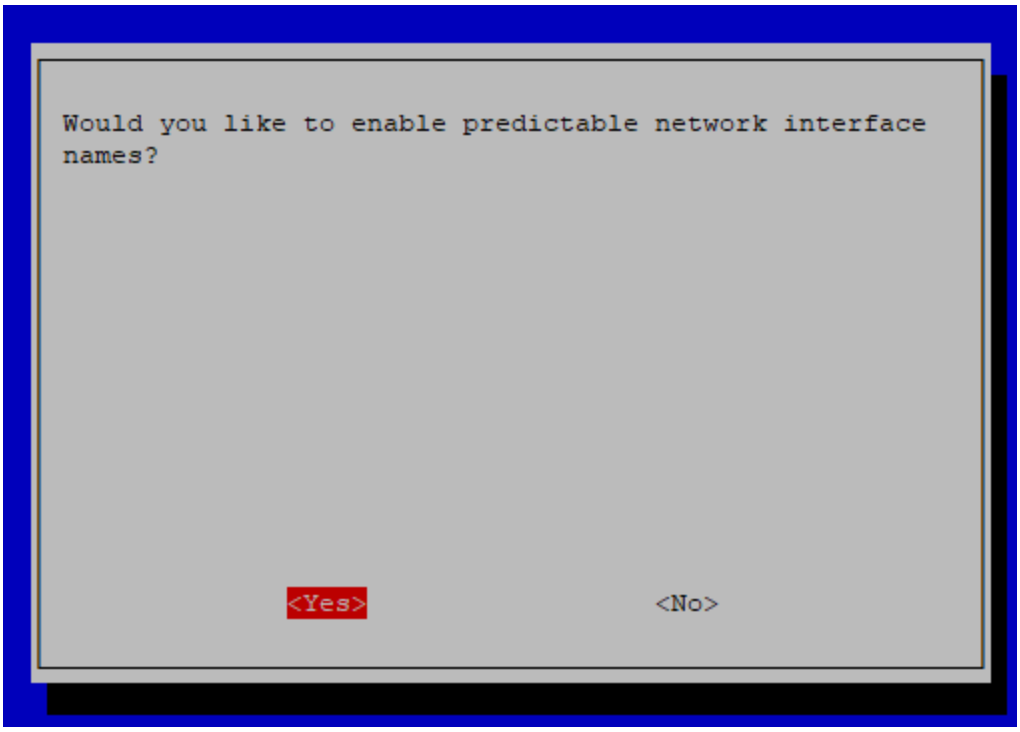


Set Network Interface names to Predictable:

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

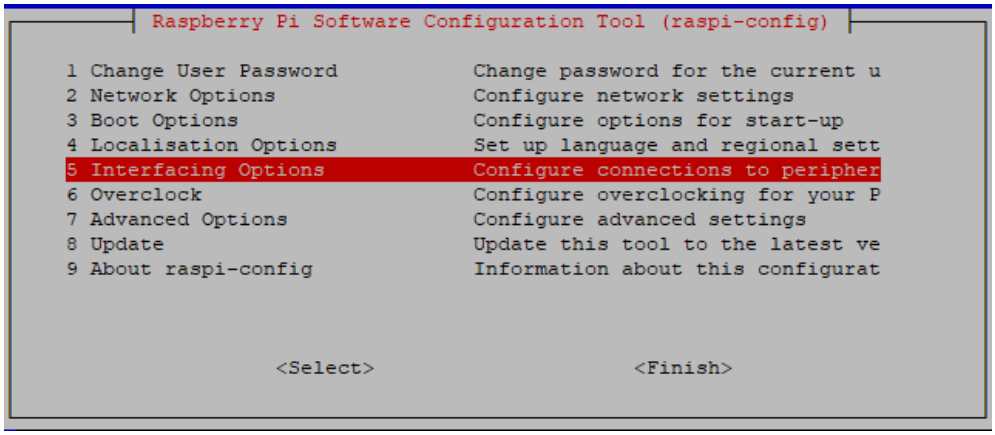

Raspberry Pi Software Configuration Tool (raspi-config)
1 Change User Password
Change password for the current u
2 Network Options
Configure network settings
3 Boot Options
Configure options for start-up
4 Localisation Options
Set up language and regional sett
5 Interfacing Options
Configure connections to peripher
6 Overclock
Configure overclocking for your P
7 Advanced Options
Configure advanced settings
8 Update
Update this tool to the latest ve
9 About raspi-config
Information about this configurat
<Select>
<Finish>

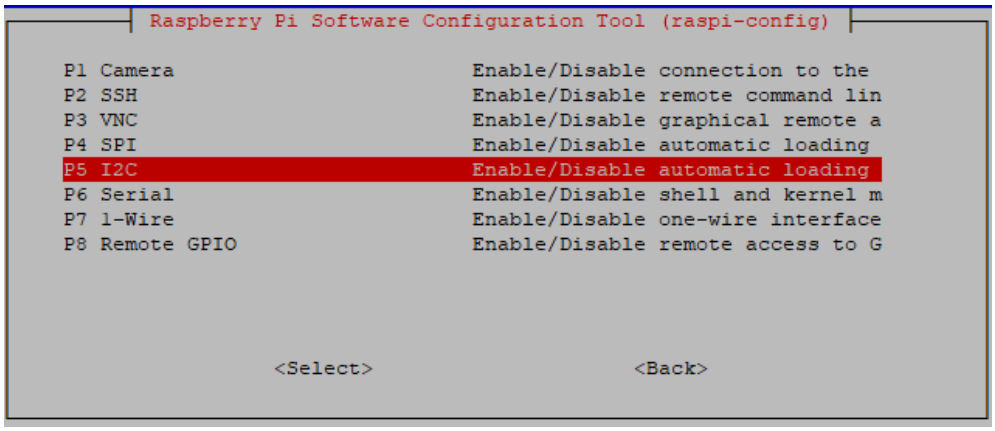

Raspberry Pi Software Configuration Tool (raspi-config)
N1 Hostname
Set the visible name for this Pi
N2 Wi-fi
Enter SSID and passphrase
N3 Network interface names
Enable/Disable predictable networ
<Select>
<Back>



6. Turn on I2C interface:

Interfacing Options -> I2C -> Yes
(Enable I2C interface. *See below screens*)





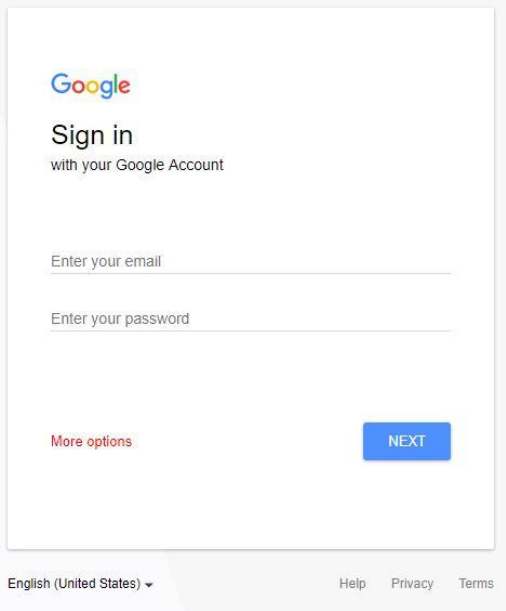
7. Once enabled, TAB to “Finish” and answer “Yes” to reboot.

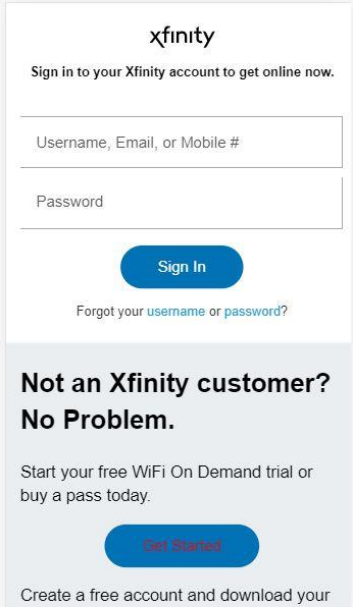
8. Add packages:

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

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





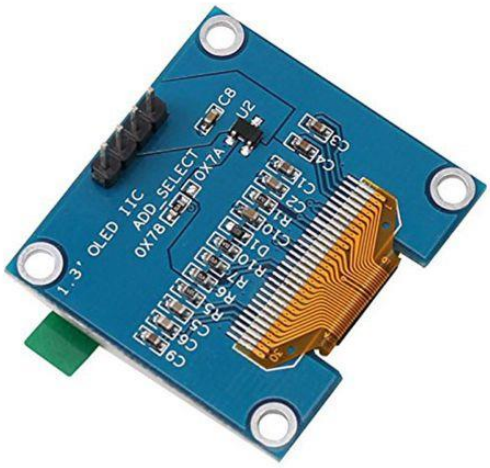
Optional: Adding OLED Display Hardware

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

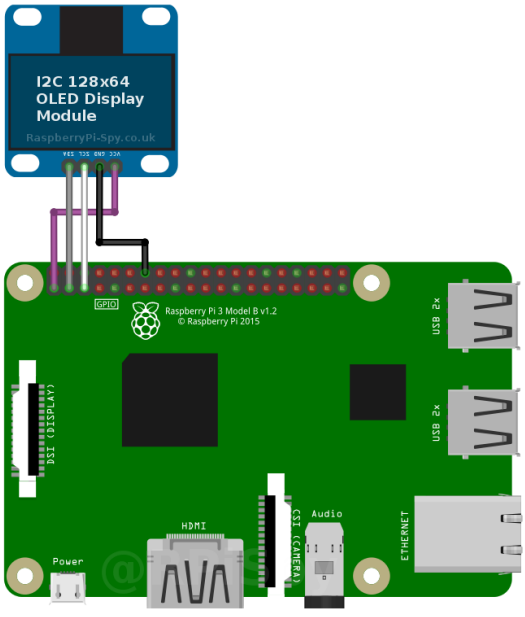
```
$ sudo shutdown now
```

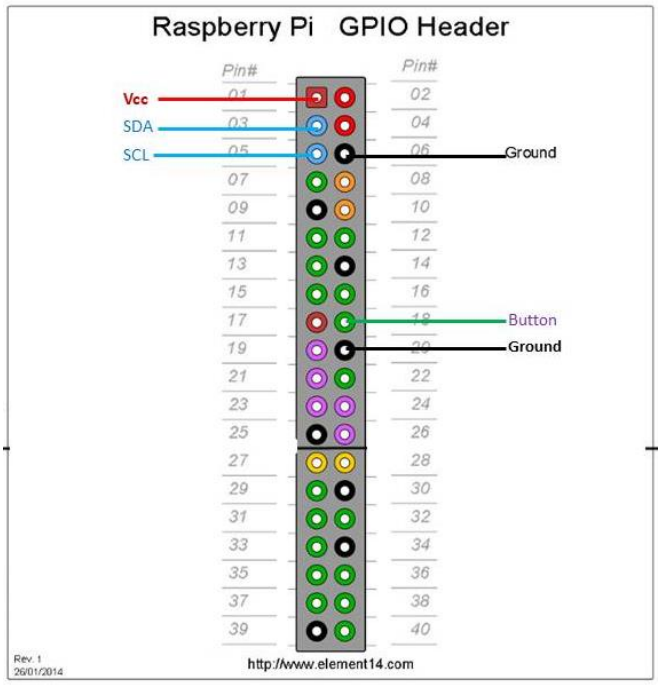
Unplug the 5V power adapter.

Add the screen using the info below.



OLED Pin	Pi Header Pin	Notes
Vcc	1	3.3V
Gnd	14	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

```
$ python testOLED.py
```

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

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.