WELCOME TO CIALUG

- Website: http://cialug.org
- Email list
- IRC/Slack
- Meetings the third Wednesday of the month at place TBA (watch list server, website, and IRC/Slack)

WE ARE LOOKING FOR PRESENTERS AND TOPICS

ABOUT ME

- By day a Sr Software Developer at a large Agriscience company (formerly green colored, now blue)
- By night linux nerd with a networking issue
- Twitter @adenner
- Email: denner@gmail.com
- Slides posted to https://denner.co

TOR/SSH JUMP SERVER

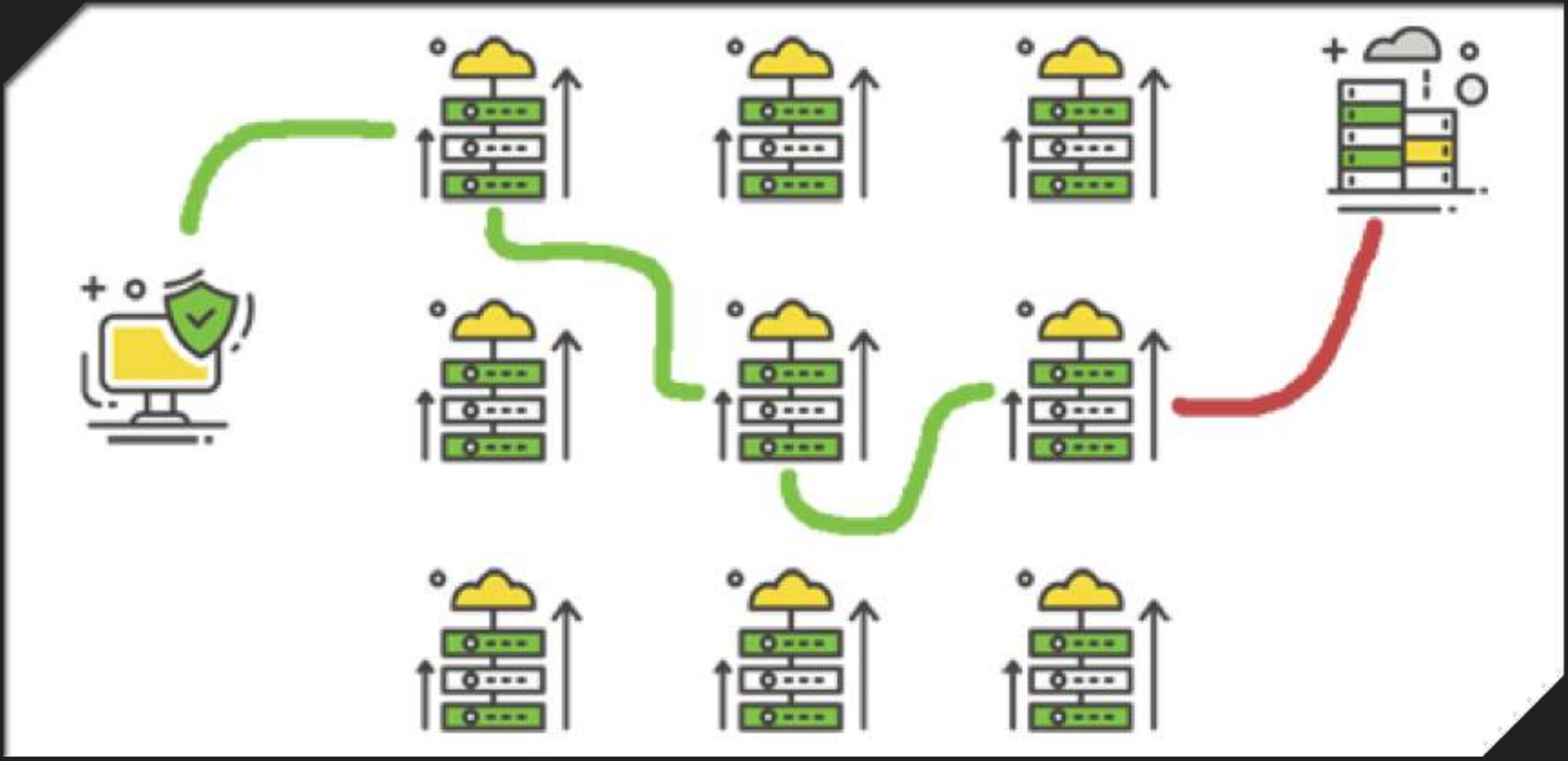
RASPBERRY PI

FIRST A COUPLE OF THINGS…

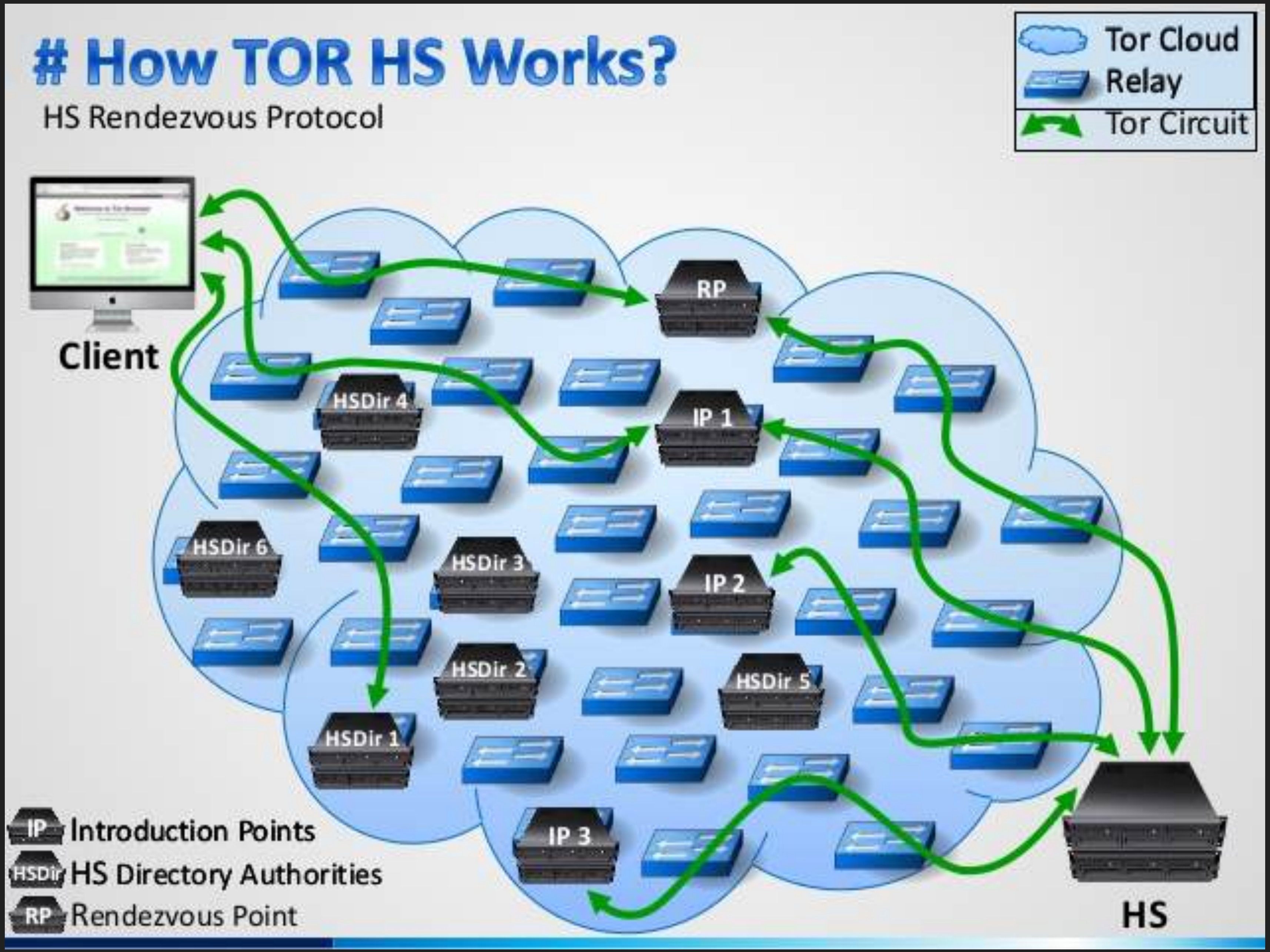
INTRO

TOR IN A NUTSHELL

- “Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.”

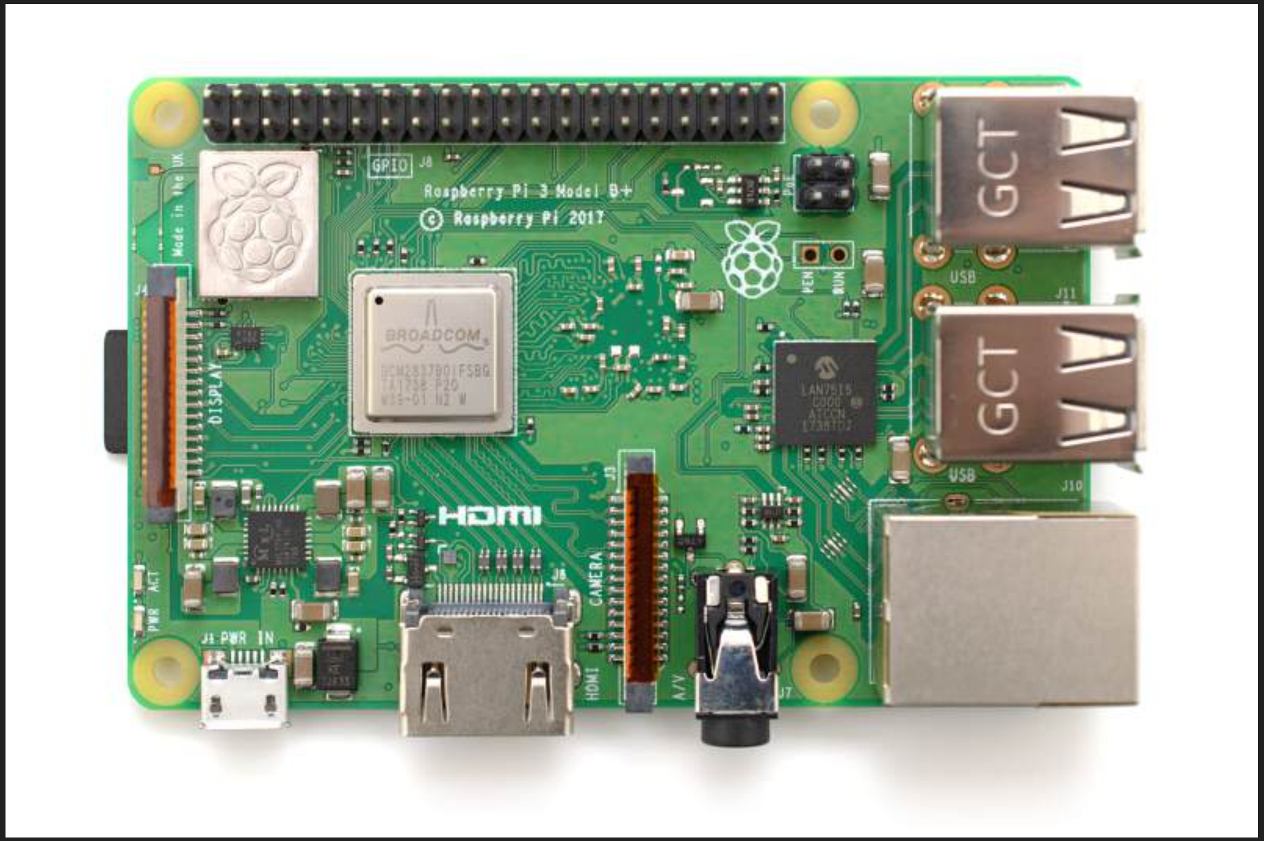


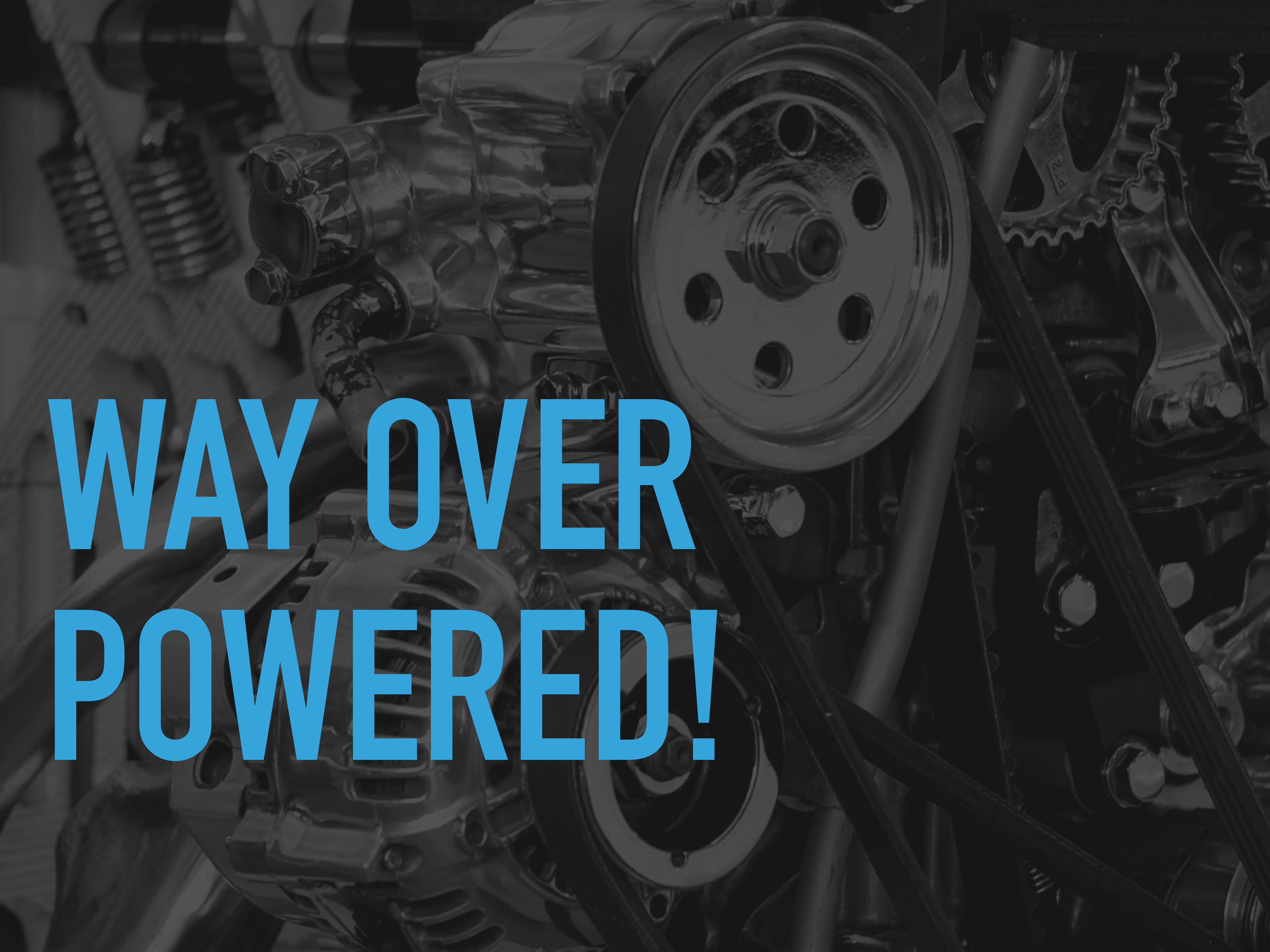
USING ONION SERVICES



PI B VERSION 3+

- Released March 14 2018
- ArmV8-A (32/64 bit)
- Broadcom BCM2837B0 SOC
- VFPv4 +NEON FPU
- 4x Cortex A53 @ 1.4 GHZ CPU
- 1gb of RAM (Shared with GPU)
- 10/100/1000 Mbit/s Ethernet[68] (real speed max 300 Mbit/s[80]), 802.11b/g/n/ac dual band 2.4/5 GHz wireless, Bluetooth 4.2 LS BLE

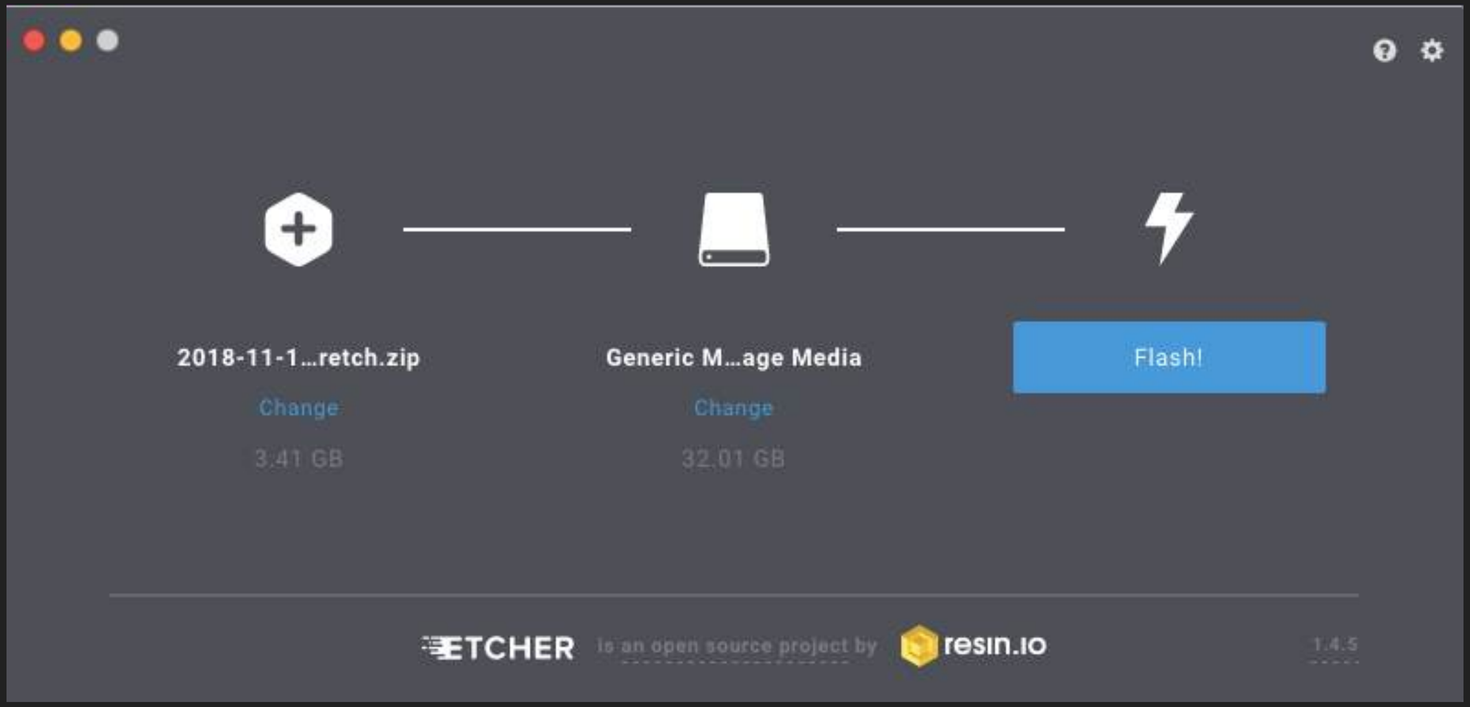




WAY OVER POWERED!

I HAVE MY PI, NOW WHAT?

- Download Rasberian from https://www.raspberrypi.org/downloads/raspbian/
- Use etcher to flash the micro-sd card



2018-11-1...retch.zip

3.41 GB

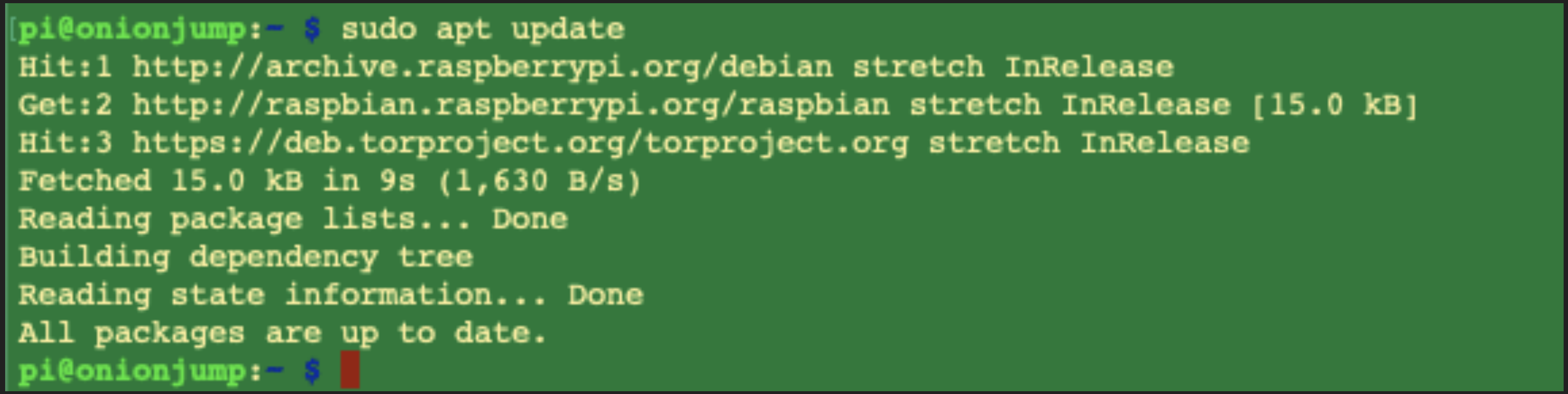
Generic M...age Media

32.01 GB

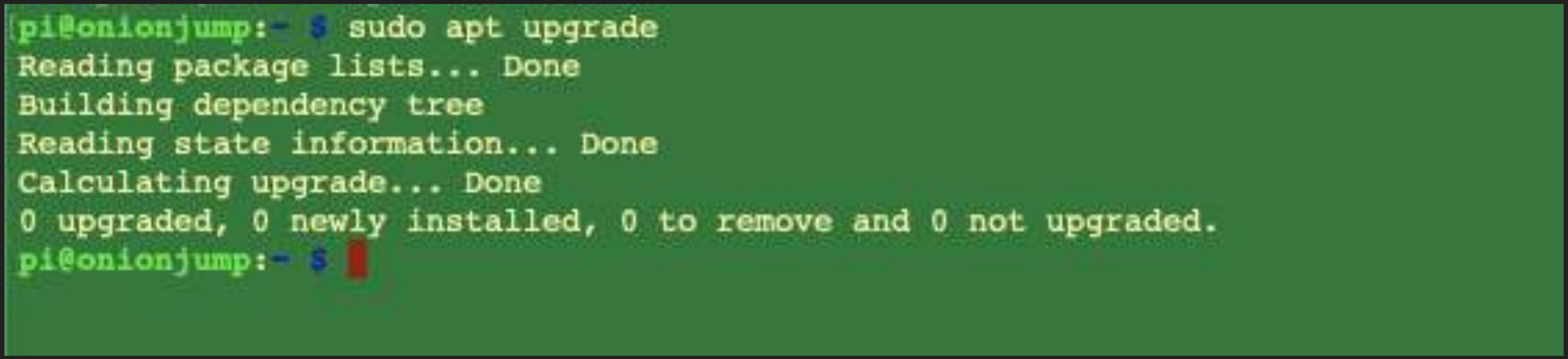
SO I SCREWED UP AND NOW EVERYTHING IS BROKEN!

- Don’t worry, it is easy to do, keep notes of what you did and you can always just re-flash the memory card over again!
- I somehow accidentally removed apt from the machine trying to install gpg2 (the second time around it worked just fine)

UPDATE OS



```
pi@onionjump:~ $ sudo apt update
Hit:1 http://archive.raspberrypi.org/debian stretch InRelease
Get:2 http://raspbian.raspberrypi.org/raspbian stretch InRelease [15.0 kB]
Hit:3 https://deb.torproject.org/torproject.org stretch InRelease
Fetched 15.0 kB in 9s (1,630 B/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
pi@onionjump:~ $
```

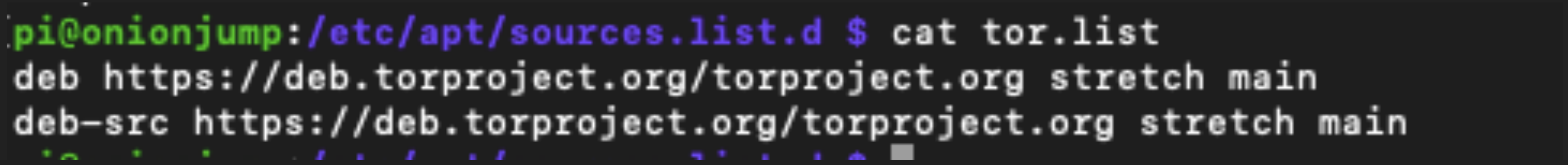


```
pi@onionjump:~ $ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
pi@onionjump:~ $
```

ADD TOR TO THE APT-SOURCE

- Note: “**Raspbian is not Debian.** Tor might run fine on the Raspberry Pi 2 / 3 but not the first generation Pi. These packages might be confusingly broken for Raspbian users, since Raspbian called their architecture armhf but Debian already has an armhf.”

- Use directions on https://www.torproject.org/docs/debian.html.en

- 

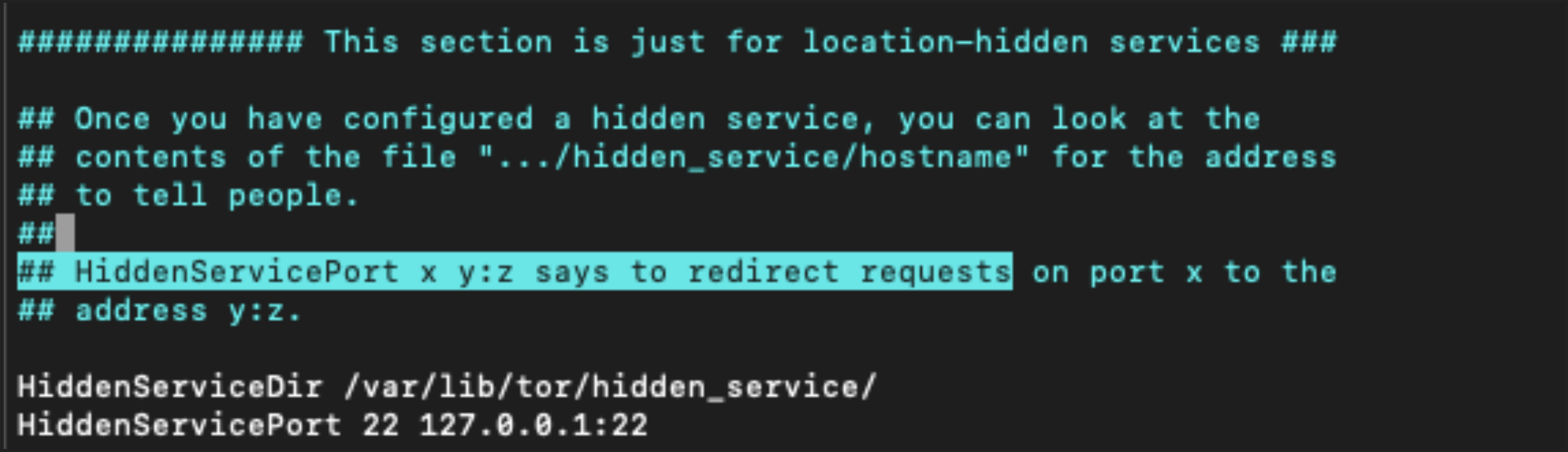
```
pi@onionjump:/etc/apt/sources.list.d $ cat tor.list
deb https://deb.torproject.org/torproject.org stretch main
deb-src https://deb.torproject.org/torproject.org stretch main
```

FINISH INSTALLING TOR

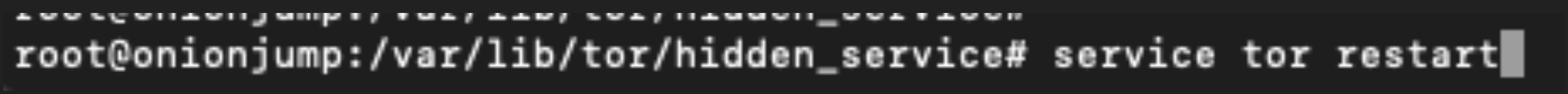
```
# apt install gnupg2

# gpg2 --recv A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89
# gpg2 --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-key add -

# apt update
# apt install tor deb.torproject.org-keyring

# apt install vim
```

CONFIGURE TOR

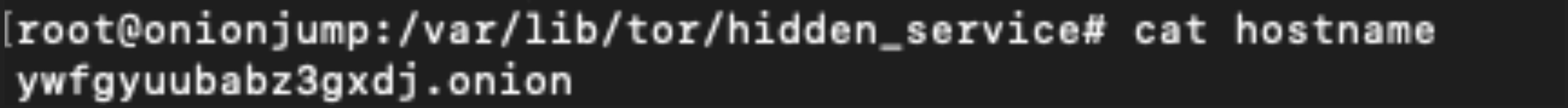
- vim /etc/tor/torrc



```
################ This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 22 127.0.0.1:22
```

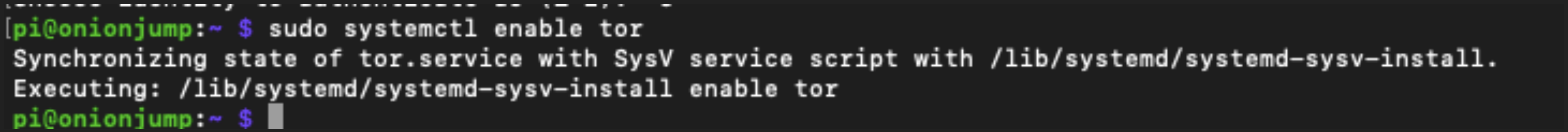


```
root@onionjump:/var/lib/tor/hidden_service#
root@onionjump:/var/lib/tor/hidden_service# service tor restart
```



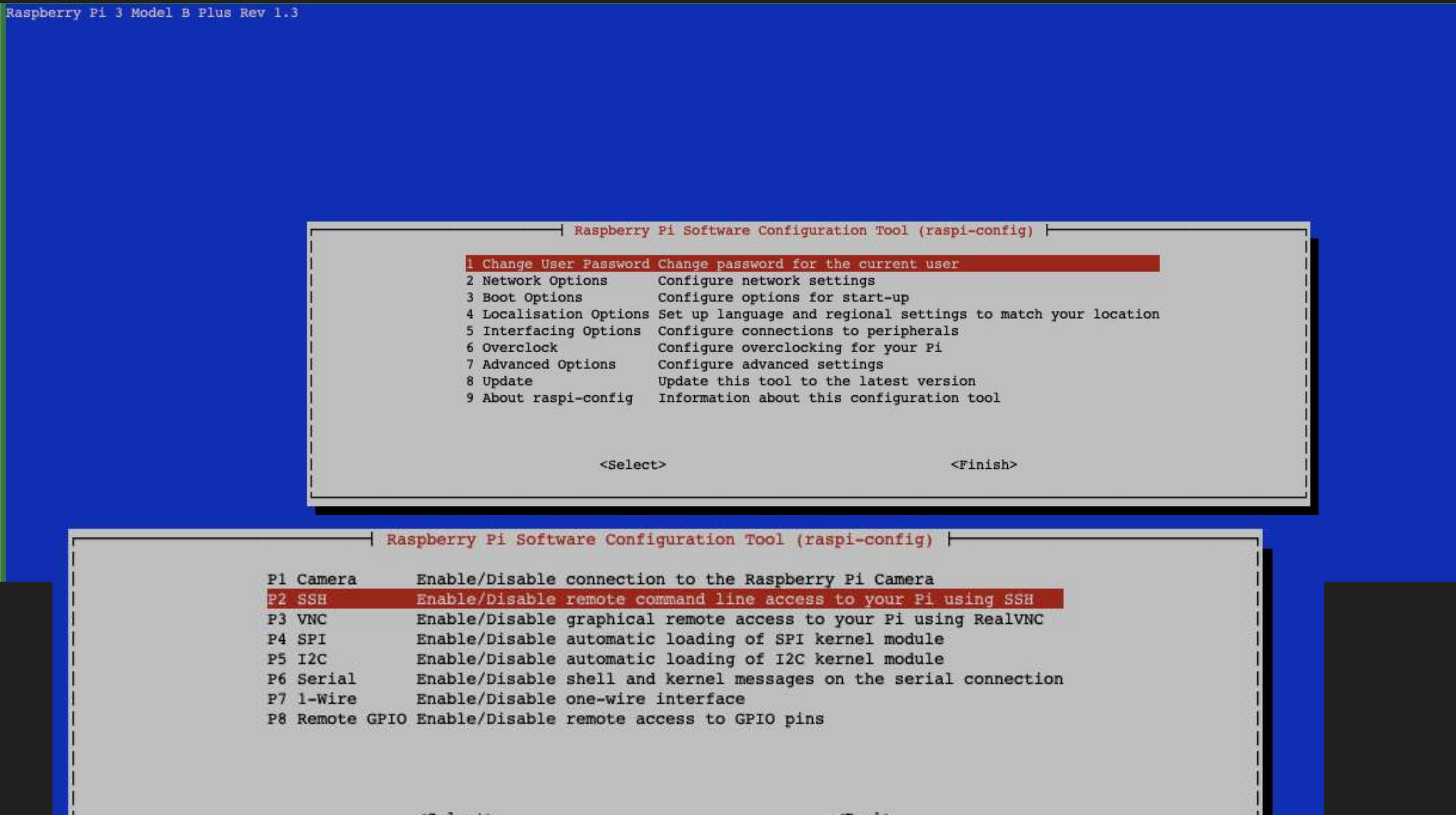
```
[root@onionjump:/var/lib/tor/hidden_service# cat hostname
ywfgyuubabz3gxdj.onion
```

SET TOR TO RUN AT STARTUP



```
[pi@onionjump:~ $ sudo systemctl enable tor
 Synchronizing state of tor.service with SysV service script with /lib/systemd/systemd-sysv-install.
 Executing: /lib/systemd/systemd-sysv-install enable tor
 pi@onionjump:~ $ 
```

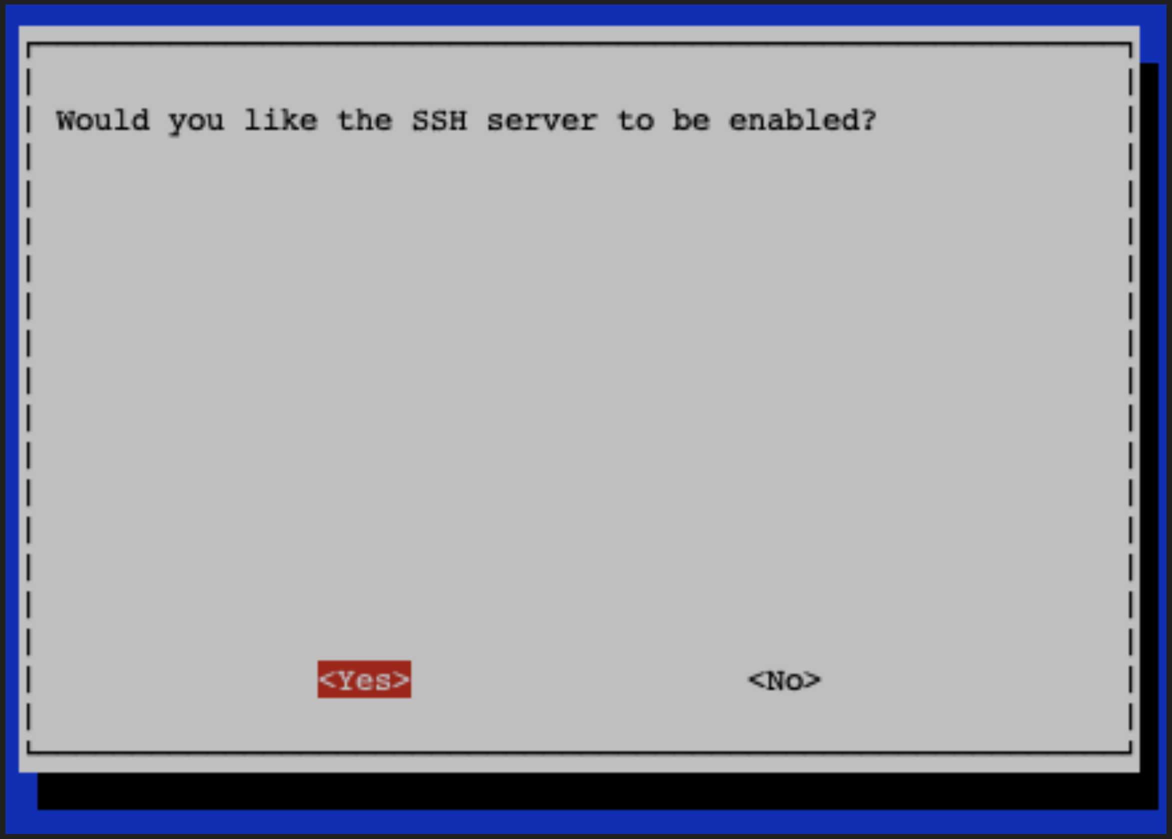
ENABLE SSH



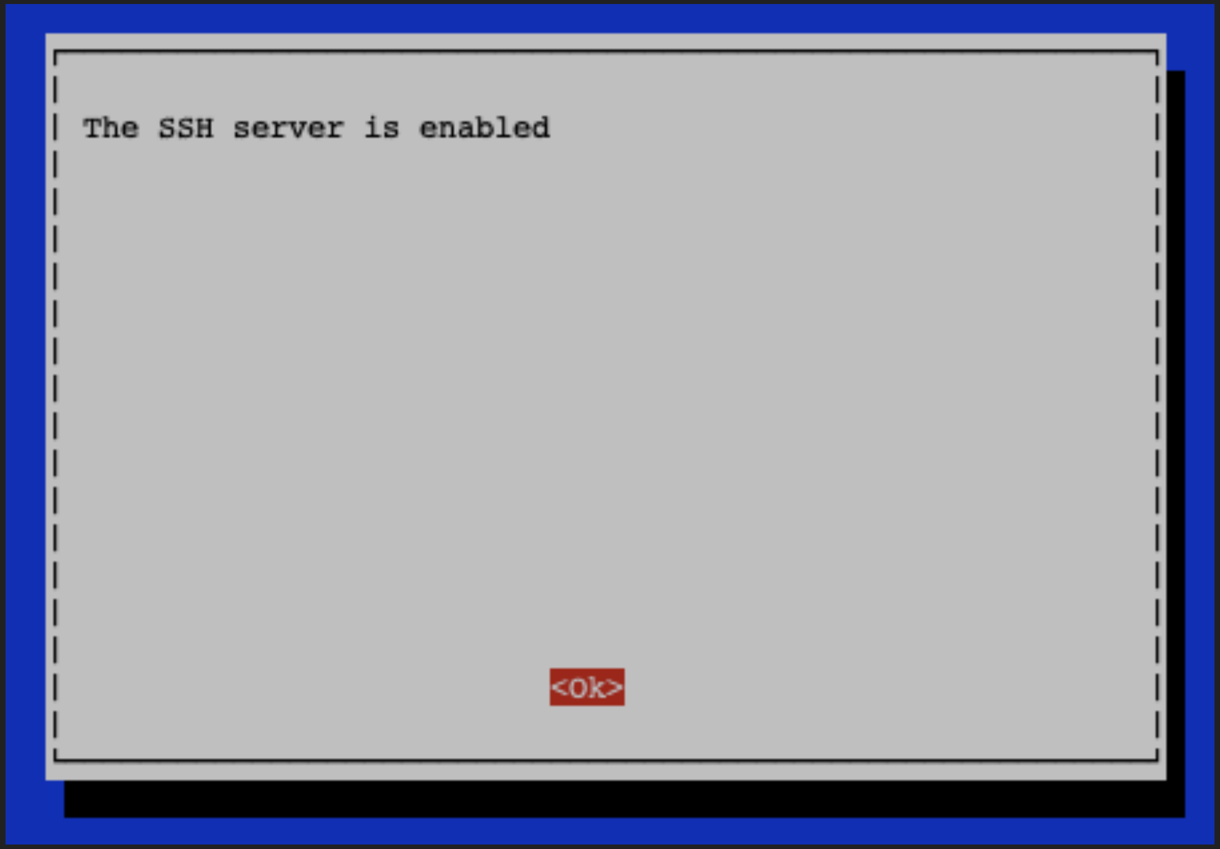
```
Raspberry Pi 3 Model B Plus Rev 1.3
```

```
┤ Raspberry Pi Software Configuration Tool (raspi-config) ├

1 Change User Password Change password for the current user
2 Network Options      Configure network settings
3 Boot Options         Configure options for start-up
4 Localisation Options Set up language and regional settings to match your location
5 Interfacing Options  Configure connections to peripherals
6 Overclock            Configure overclocking for your Pi
7 Advanced Options     Configure advanced settings
8 Update               Update this tool to the latest version
9 About raspi-config   Information about this configuration tool

                 <Select>                      <Finish>
```

```
┤ Raspberry Pi Software Configuration Tool (raspi-config) ├

P1 Camera      Enable/Disable connection to the Raspberry Pi Camera
P2 SSH         Enable/Disable remote command line access to your Pi using SSH
P3 VNC         Enable/Disable graphical remote access to your Pi using RealVNC
P4 SPI         Enable/Disable automatic loading of SPI kernel module
P5 I2C         Enable/Disable automatic loading of I2C kernel module
P6 Serial      Enable/Disable shell and kernel messages on the serial connection
P7 1-Wire      Enable/Disable one-wire interface
P8 Remote GPIO Enable/Disable remote access to GPIO pins
```



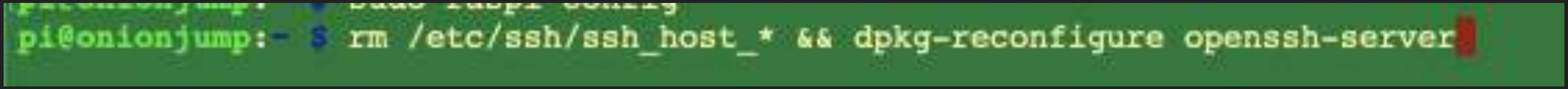
Would you like the SSH server to be enabled?



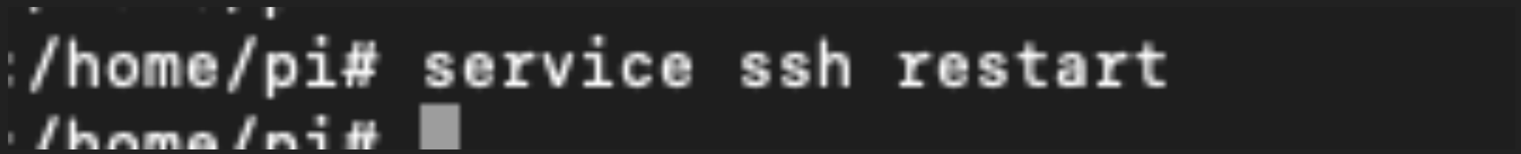
The SSH server is enabled

REGENERATE SSH KEYS

- Since this is all from a disk image, we need to regenerate ssh keys

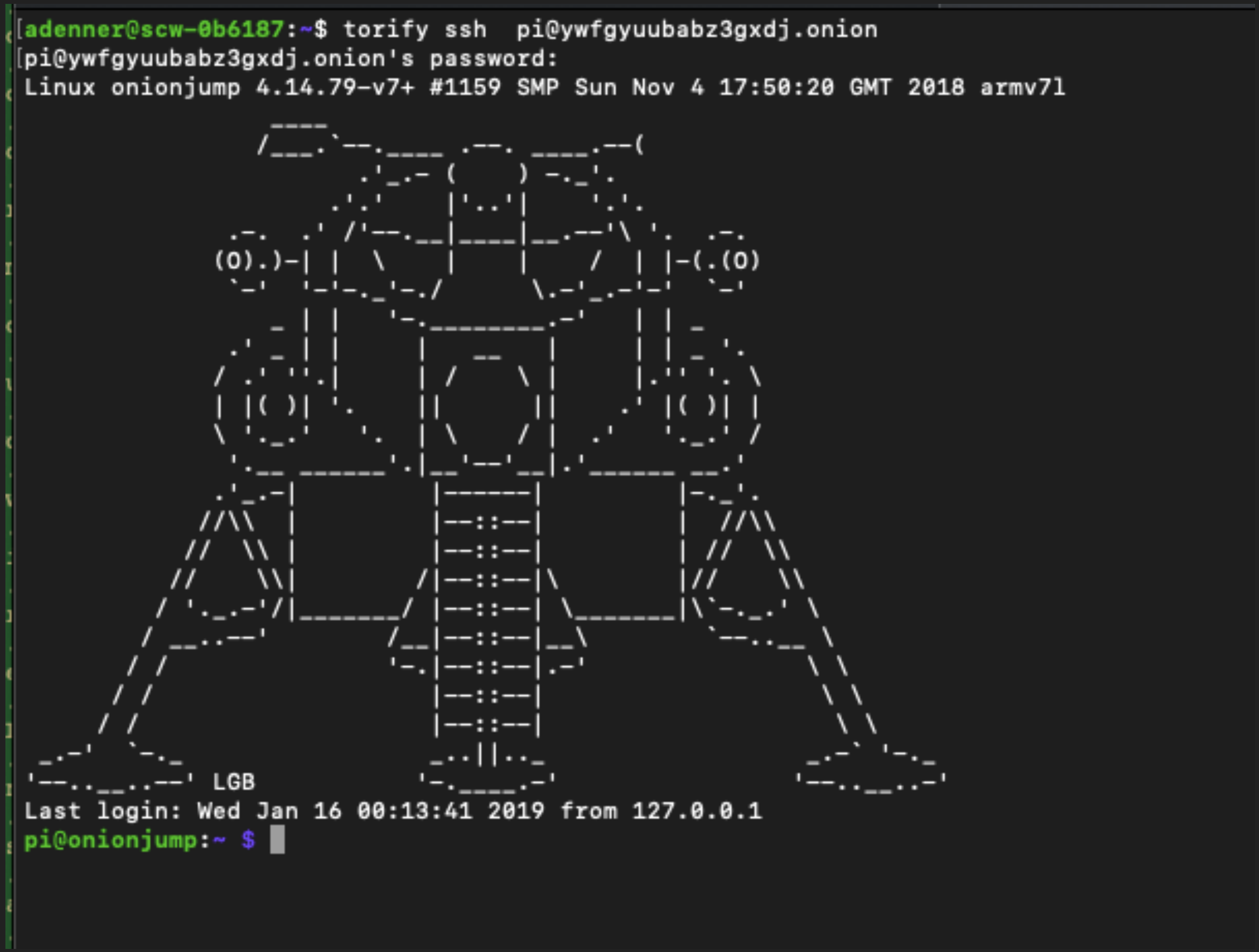


```
pi@onionjump:~ $ sudo raspi-config
pi@onionjump:~ $ rm /etc/ssh/ssh_host_* && dpkg-reconfigure openssh-server
```



```
:/home/pi# service ssh restart
:/home/pi#
```

NOW WE CAN SSH



```
adenner@scw-0b6187:~$ torify ssh  pi@ywfgyuubabz3gxdj.onion
pi@ywfgyuubabz3gxdj.onion's password:
Linux onionjump 4.14.79-v7+ #1159 SMP Sun Nov 4 17:50:20 GMT 2018 armv7l
                 ____
                /___.`--.____ .--. ____.--(
                       .'_.- (    ) -._'.
                     .'.'    |'..'|    '.'.
              .-.  .' /'--.__|____|__.--'\ '.  .-.
             (O).)-| |  \    |    |    /  | |-(.(O)
              `-'  '-'-._'-./      \.-'_.-'-'  `-'
                 _ | |   '-.________.-'   | | _
              .' _ | |     |   __   |     | | _ '.
             / .' ''.|     | /    \ |     |.'' '. \
             | |( )| '.    ||      ||    .' |( )| |
             \ '._.'   '.  | \    / |  .'   '._.' /
              '.__ ______'.|__'--'__|.'______ __.'
             .'_.-|         |------|         |-._'.
            //\\  |         |--::--|         |  //\\
           //  \\ |         |--::--|         | //  \\
          //    \\|        /|--::--|\        |//    \\
         / '._.-'/|_______/ |--::--| \_______|\`-._.' \
        / __..--'        /__|--::--|__\        `--..__ \
       / /               '-.|--::--|.-'               \ \
      / /                   |--::--|                   \ \
     / /                    |--::--|                    \ \
 _.-'  `-._                 _..||.._                  _.-` '-._
'--..__..--' LGB           '-.____.-'                '--..__..-'
Last login: Wed Jan 16 00:13:41 2019 from 127.0.0.1
pi@onionjump:~ $ 
```

SO SLOW!

REVERSE SSH

- https://blog.devolutions.net/2017/3/what-is-reverse-ssh-port-forwarding

```
ssh –f –N –T –R 2210:localhost:22 username@yourMachine.com
```

- **-f:** tells the SSH to background itself after it authenticates, saving you time by not having to run something on the remote server for the tunnel to remain alive.
- **-N:** if all you need is to create a tunnel without running any remote commands then include this option to save resources.
- **-T:** useful to disable pseudo-tty allocation, which is fitting if you are not trying to create an interactive shell.

```
Ssh -p 2210 localhost
```

LIVE DEMO