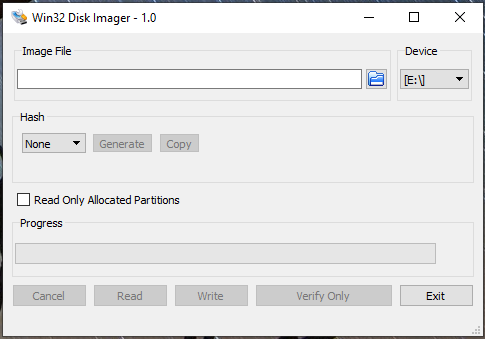
**CONFIGURING RASPBERRY PI AS AN ADBLOCKER FOR HOME NETWORK**

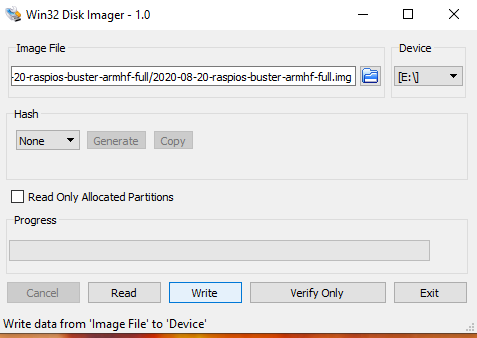
Raspberry PI can be used as a DNS server which would in turn be used as an AdBlock. The common domain names for the advertising sites can be added as a blacklist the sites thereby blocking all the ads right from websites to YouTube. This can also be used as a parental control device to block unwanted websites as well.

SYSTEM REQUIREMENTS –

* Raspberry PI
* SD Card
* Win32DiskImager - <https://sourceforge.net/projects/win32diskimager/>
* Raspberry PI buster image - <https://www.raspberrypi.org/downloads/raspberry-pi-os/>

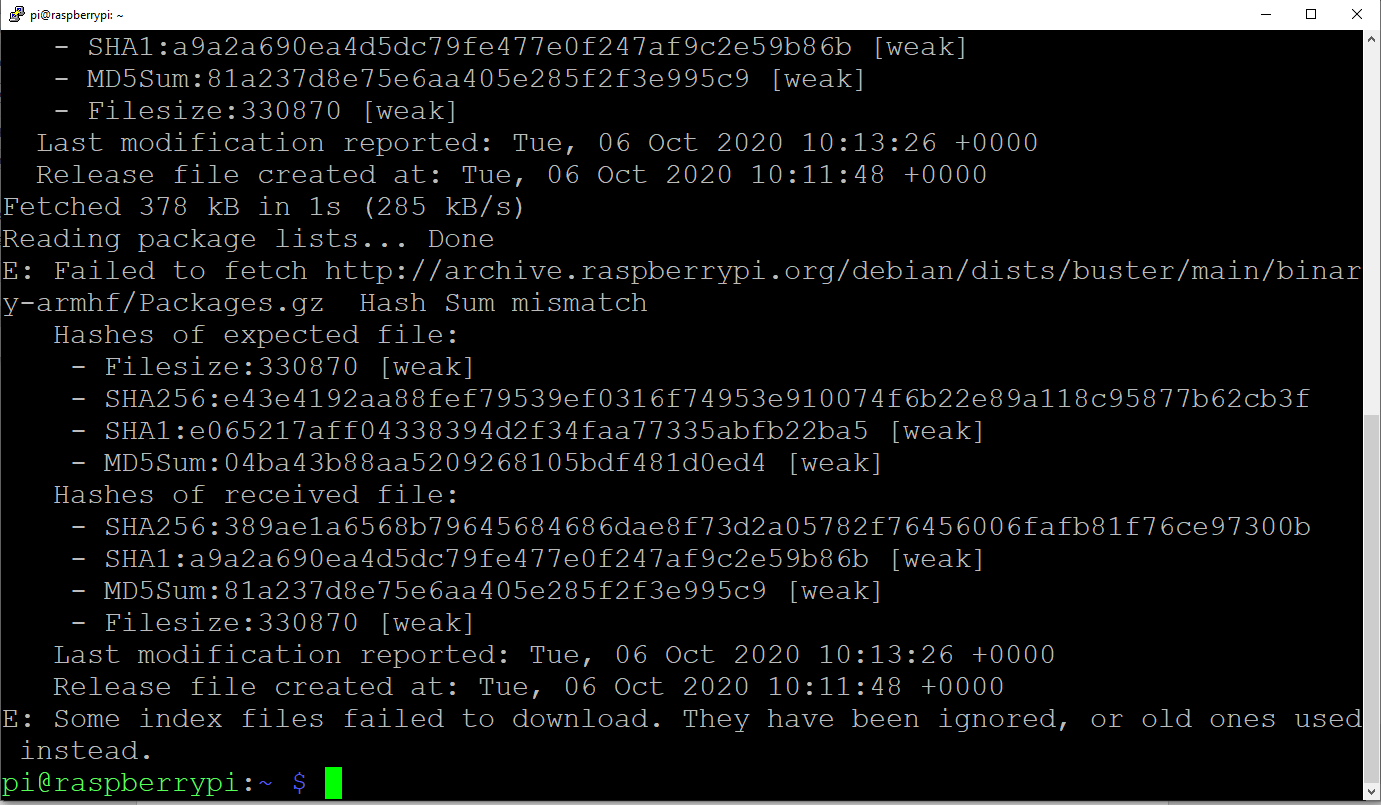
This should be good to start the configuration of Raspberry PI as an Adblocker. Below is a step by step guide with the screenshots and the various issues which one might face while configuring the pihole (Common name used for Adblocker on Raspberry PI).

1. Download and Install Win32DiskImager into your system.
2. Download the Raspberry PI Image and unzip the file with 7ZIP. Specifically, 7Zip because other programs corrupt the disk image file which is present inside the zip.
3. Format the SD card using any utility of choice (Diskpart, Disk manager, MiniTool etc)
4. Flash the image into the SD card as shown in below screenshots
   1. 
   2. Click on the folder icon to select the image. The drive is populated on the right side. Select it from the dropdown if the correct device is not show. Make sure not to erase other external drives which are also connected.
   3. Once the image is selected, click on the write button as shown



1. Once the image is flashed, insert the card in the Raspberry PI and power on the device. There is no physical power on button so only plugging the power cable would do the job.
2. If you are selecting the GUI version, connect a monitor and a keyboard to perform basic configurations after which you can switch over to the SSH mode for further operations.
3. After initial bootup the PI would ask for the password, punch in a strong password since this would be an internet facing device which you don’t want to be compromised.
4. Once done the packages of the PI would be updated, in case they are not run the below commands in sequence to update the packages. This would be needed later on since the PI hole script checks for the latest packages before running.
   1. sudo dpkg --configure -a
   2. sudo apt update
   3. sudo apt-get update
   4. sudo apt-get upgrade
5. Run the below command to pull down the code to install pihole or alternatively clone the repository from GitHub
   1. curl -sSL https://install.pi-hole.net | sudo bash

Note – Common errors faced while updating the packages in Raspbian Buster image



if you have problems with the packages it is most likely that there are sources missing in your sources list. Add the below lines to the sources list and run the apt update command again

**deb http://deb.debian.org/debian stretch main**

**deb-src http://deb.debian.org/debian stretch main**

**deb http://deb.debian.org/debian buster main**

**deb-src http://deb.debian.org/debian buster main**

**deb http://deb.debian.org/debian-security/ buster/updates main**

**deb-src http://deb.debian.org/debian-security/ buster/updates main**

**deb http://deb.debian.org/debian buster-updates main**

**deb-src http://deb.debian.org/debian buster-updates main**

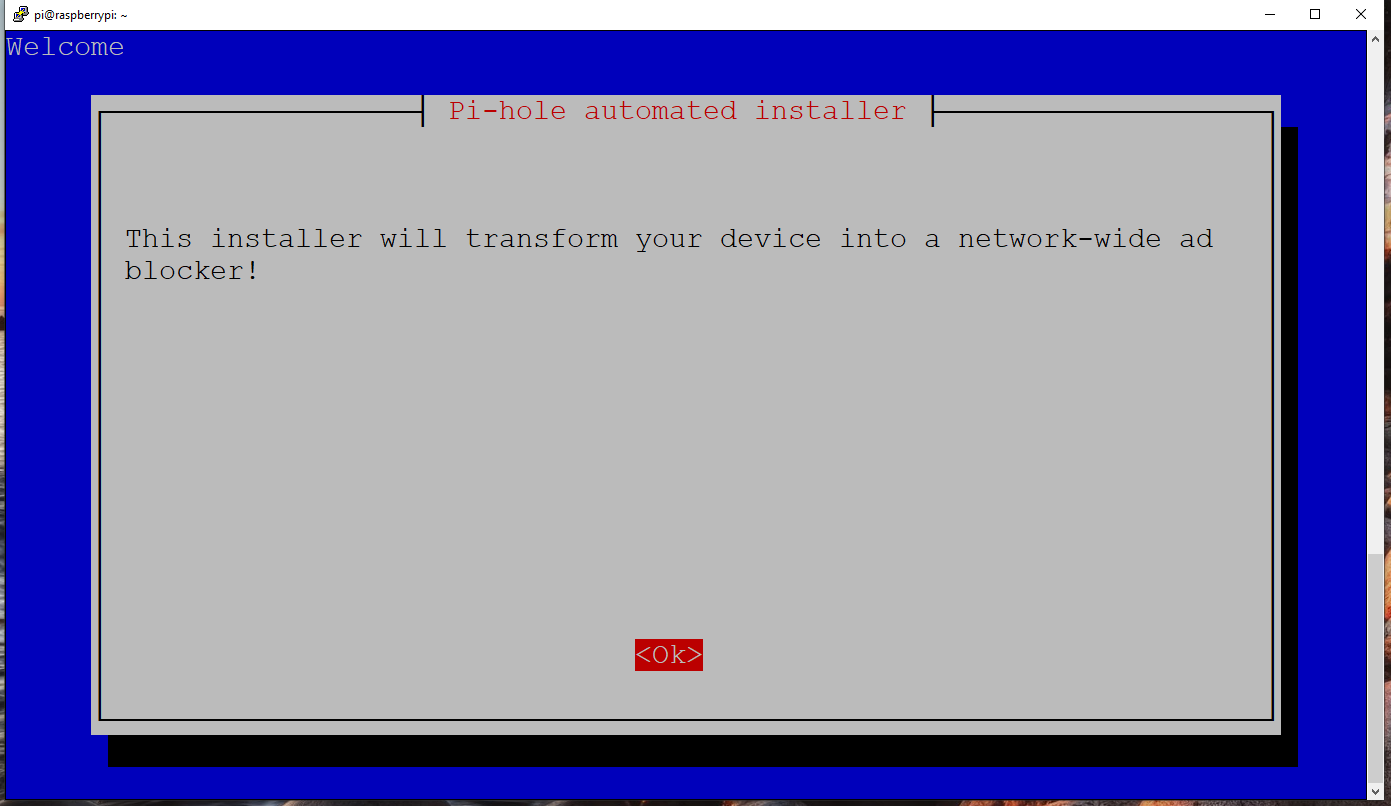
**# Uncomment line below then 'apt-get update' to enable 'apt-get source'**

**deb-src http://raspbian.raspberrypi.org/raspbian/ buster main contrib non-free $**

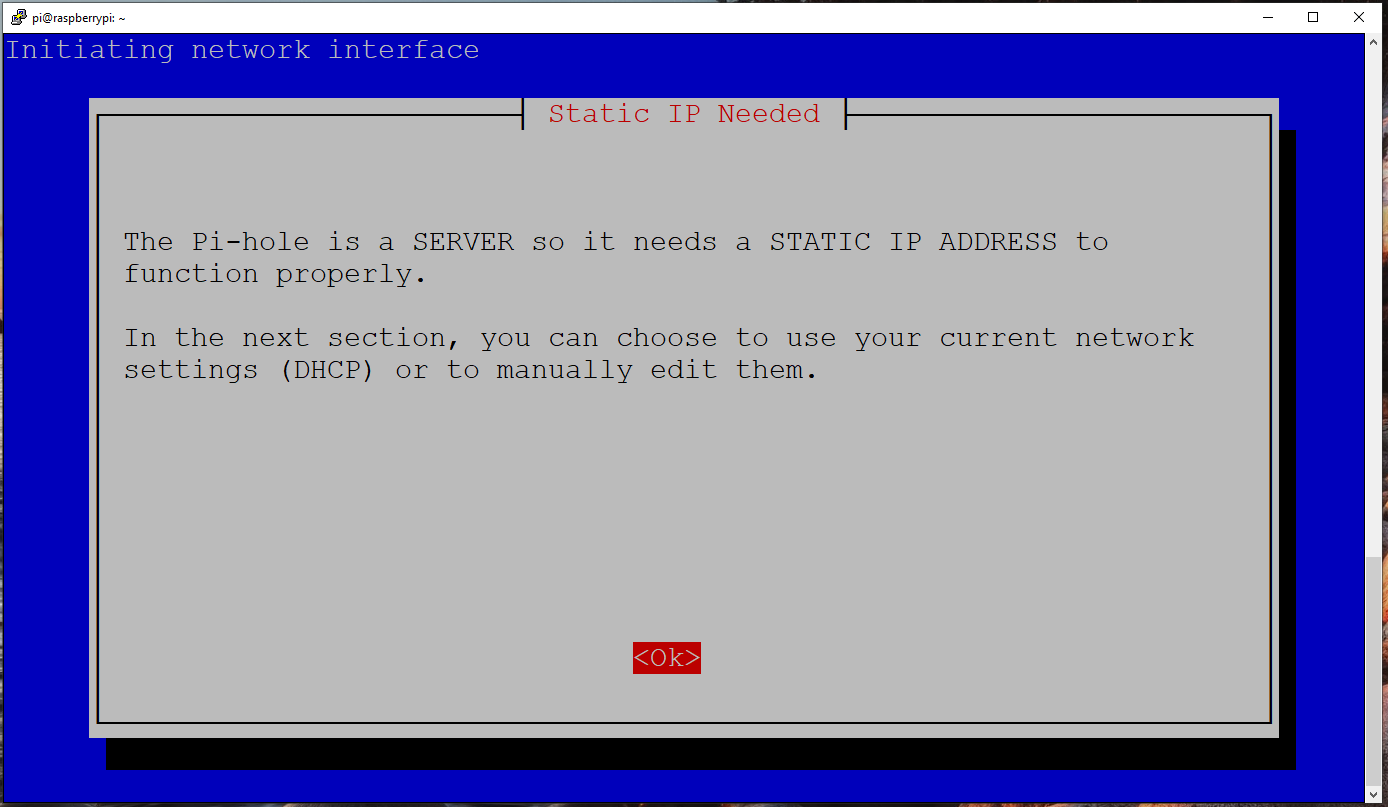
There might be one more error where it says the packages cannot be updated because the public keys are missing. The keys would be specifically mentioned in the console output. Run the below commands to add the keys to the repository and run the apt update command again.

sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys **key\_name**

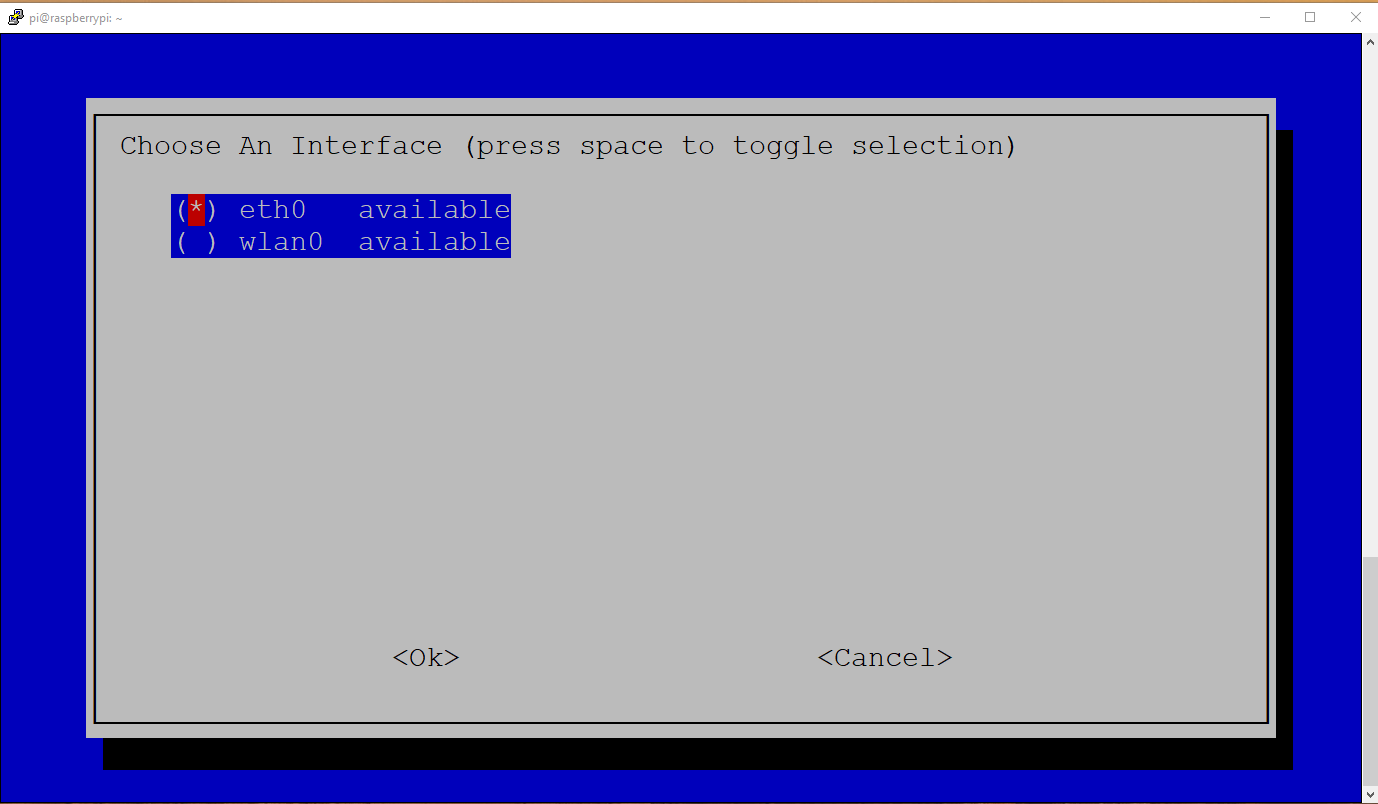
1. Running the curl command will bring up the below screen –



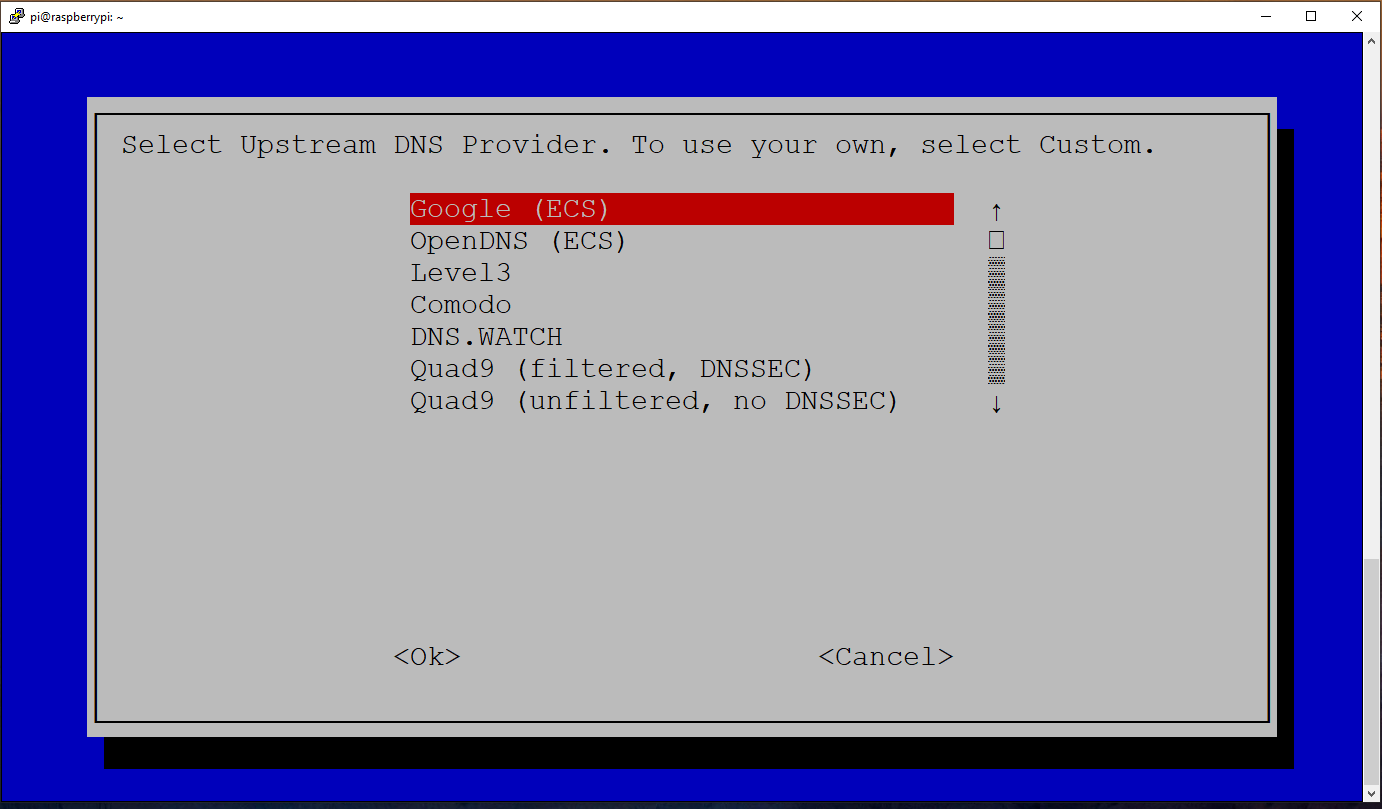
1. Click on Ok and proceed to the next screen
2. It would ask for the network settings, ideally the best approach is to have a static IP since you don’t want your DNS to change every now and then, click on Ok and proceed to the next screen



1. Select the interface of your choice
   1. **Eth0** if you intend to use the LAN port of the pi
   2. **Wlan0** if you want to connect pi over the wifi



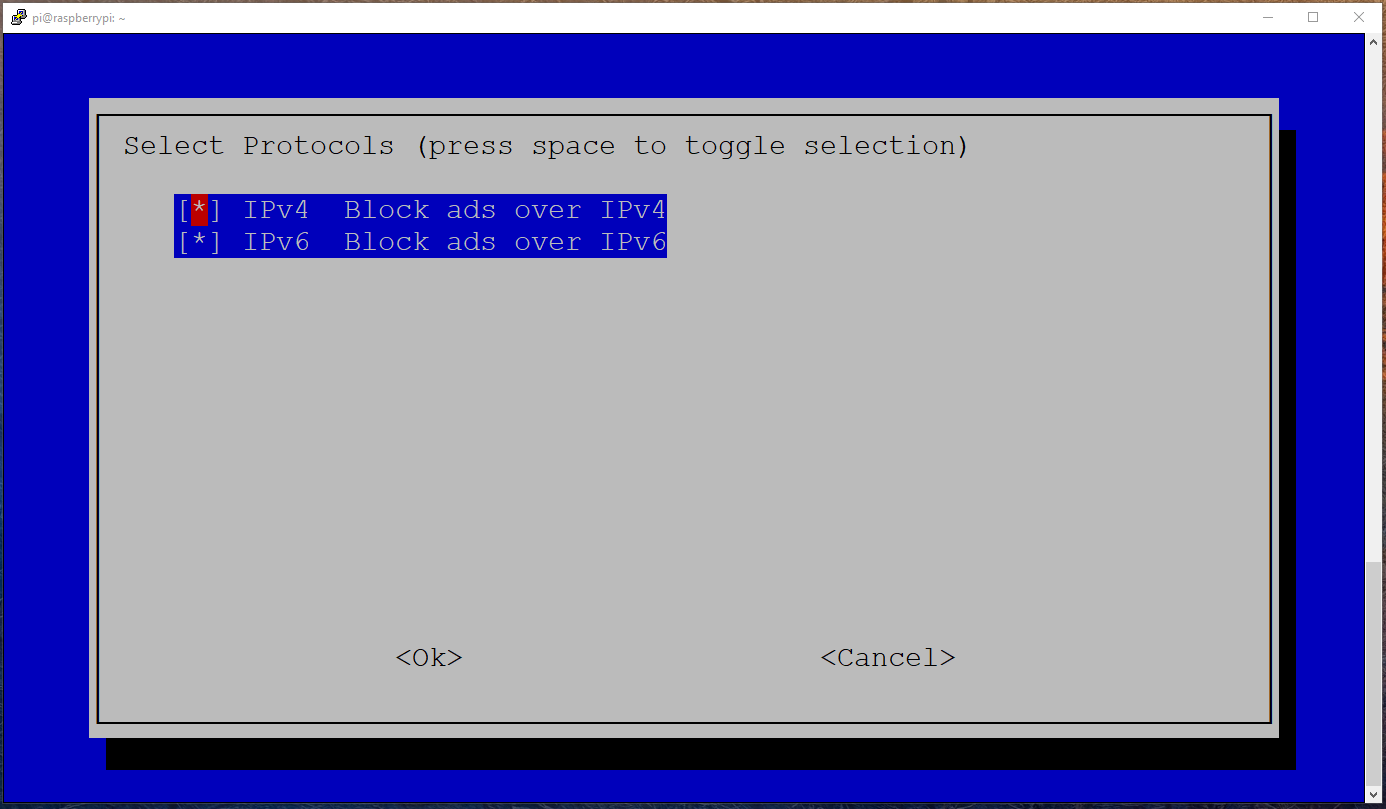
1. Next option is to choose the DNS server of choice, anything which suits you however preferred would be to use the Google DNS



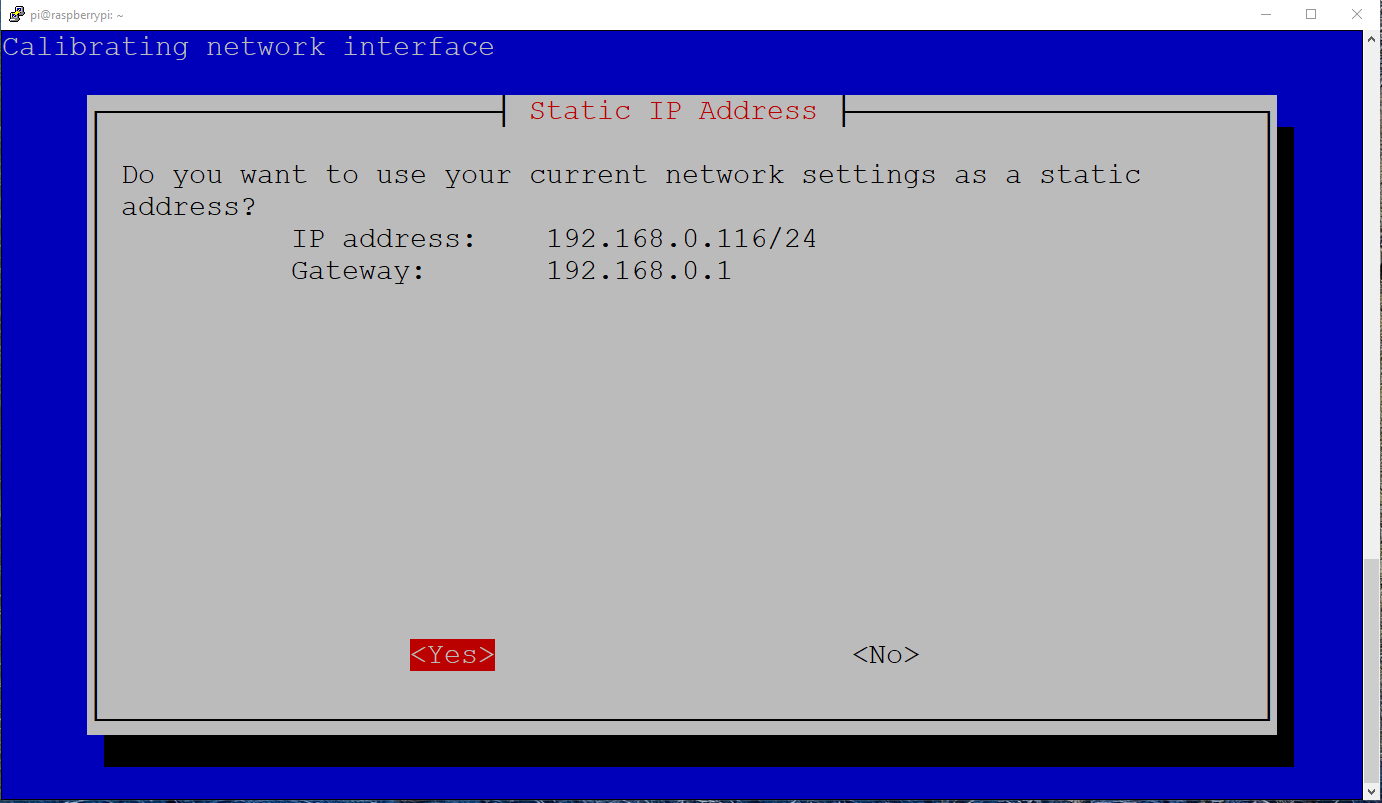
1. Next is the list of adblocker repositories. These are bare minimum to begin with however you can use other websites which I will show you in the subsequent steps.



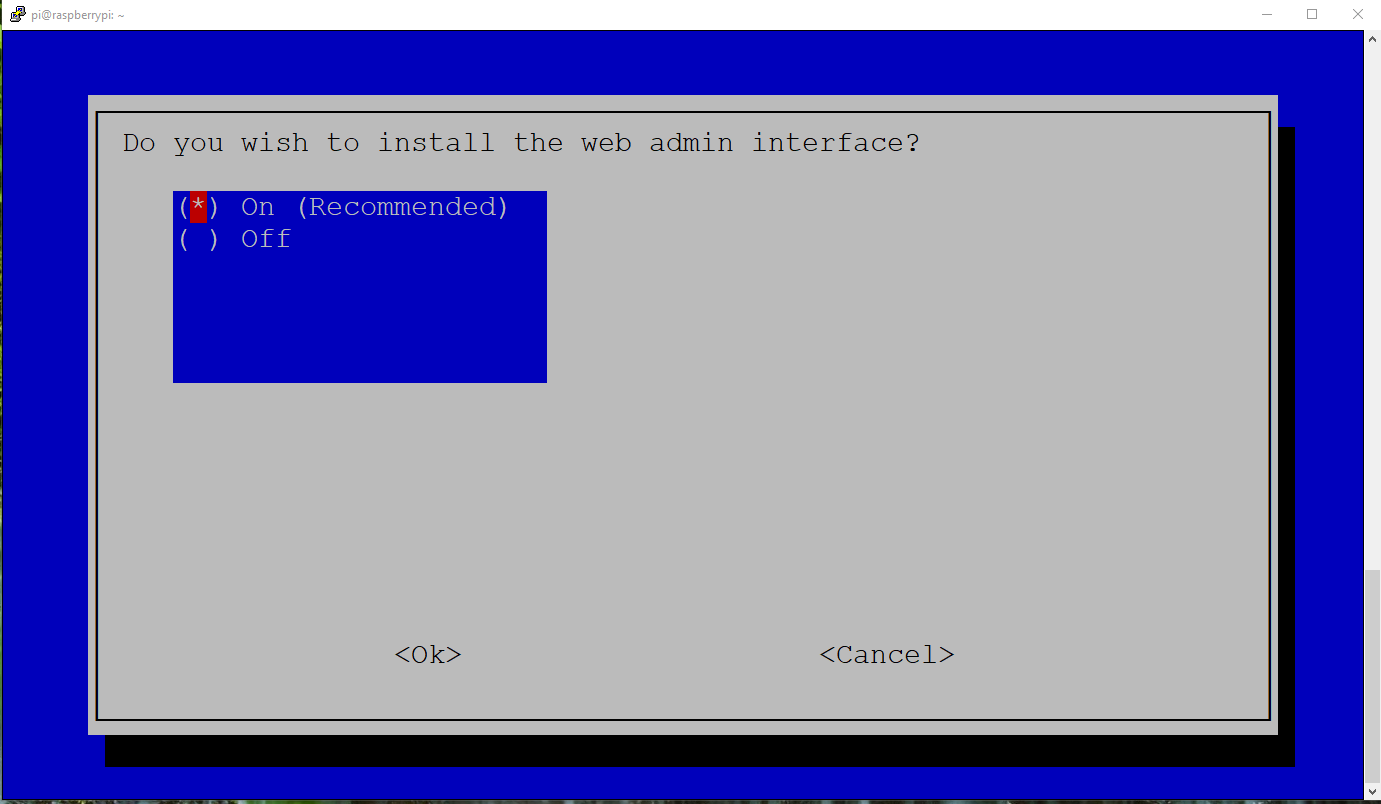
1. We would select both the options to block ads i.e. over IPv4 as well as IPv6

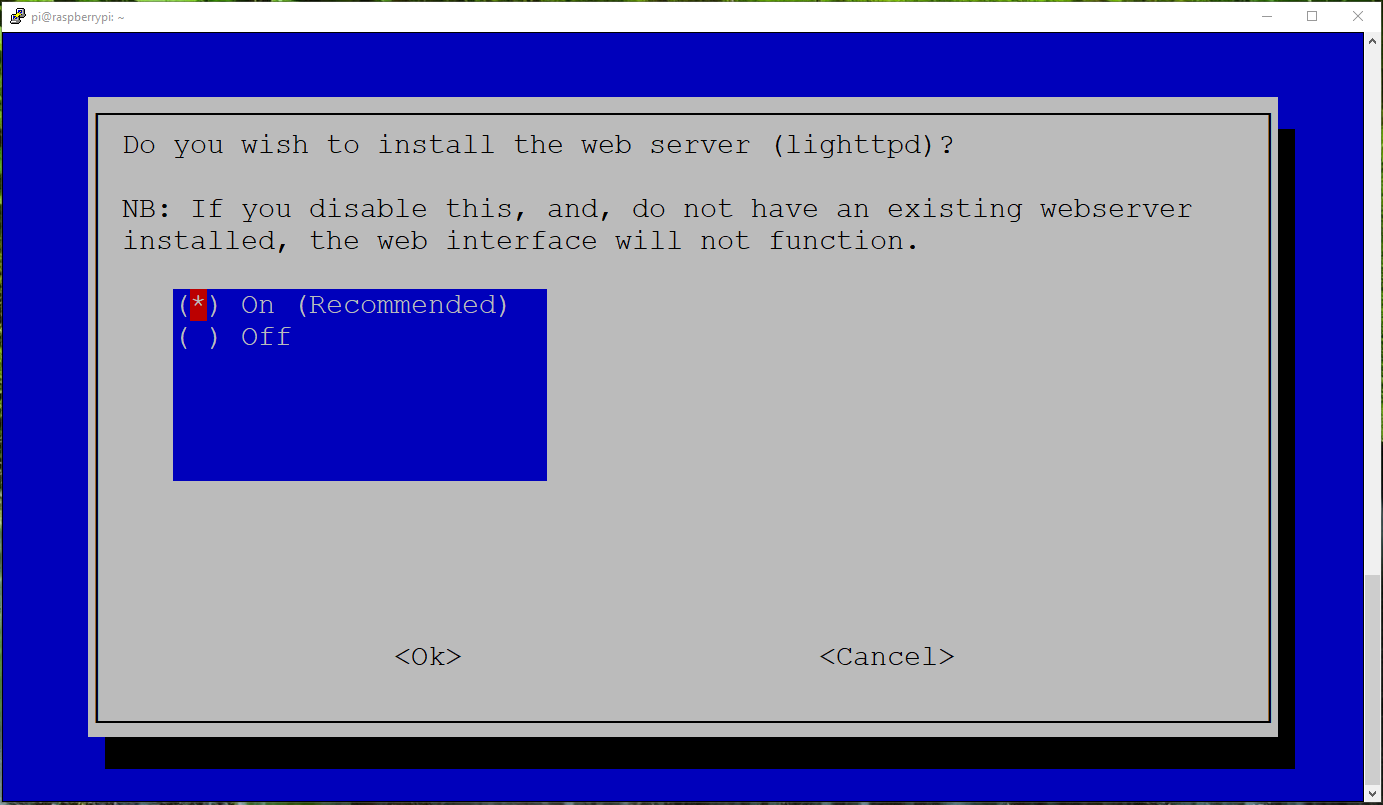


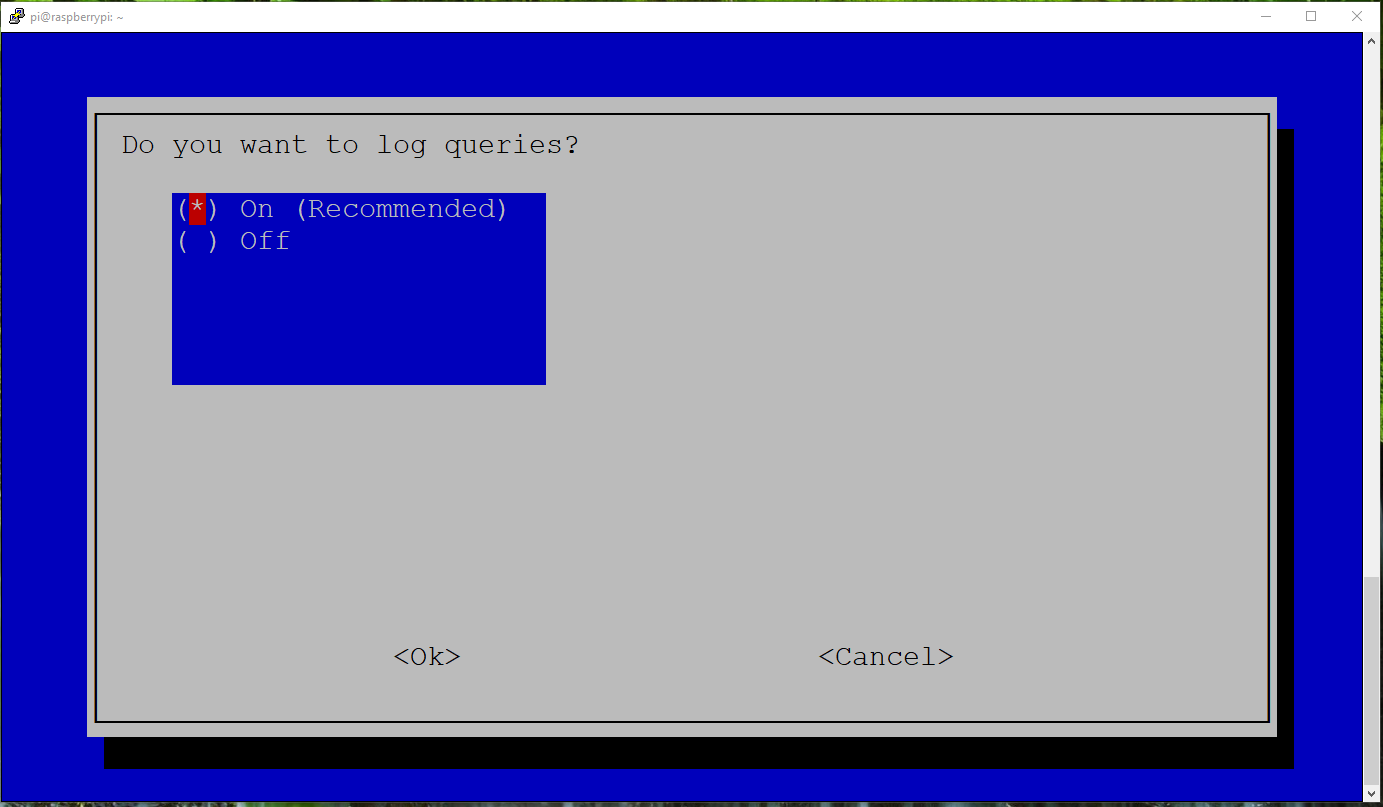
1. The pi would detect the network settings automatically, in case you want to change them click on No and configure the static IP which you want. The best option would be to configure a DHCP reservation in your router so that the IP does not change.



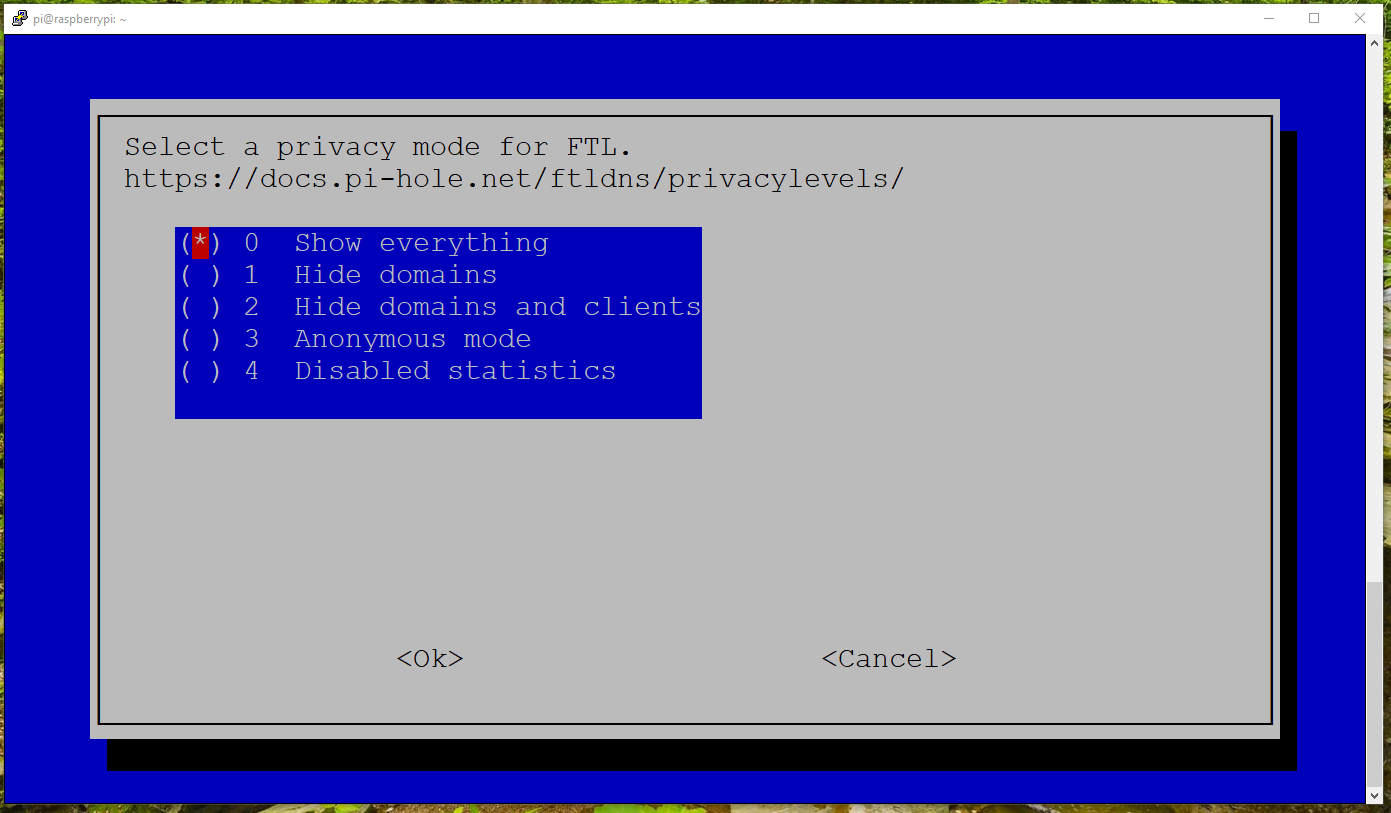
1. Once all the configurations are done, it would ask for standard installation options like the web admin interface, the web server i.e. lighthttpd and if we want to have a log of all the DNS quries.







1. The privacy mode shows what is to be displayed and what has to be hidden. I choose to show everything

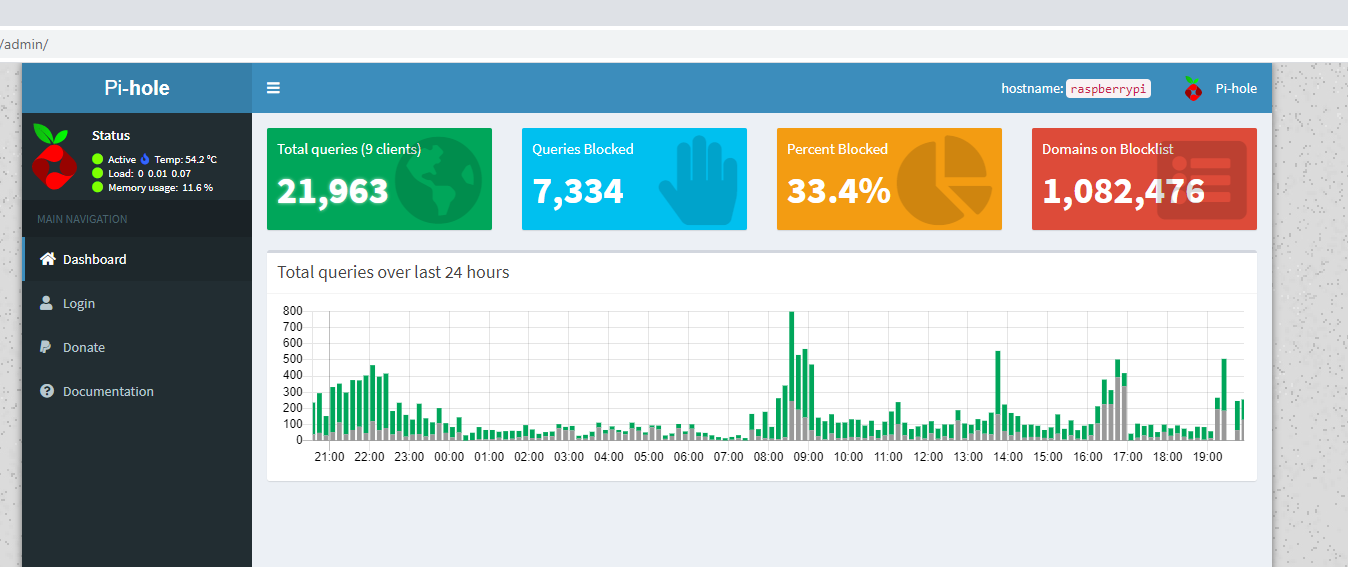


1. The Pi would start running the script based on the options provided and once done it would show the link to the admin page and the password. Please note that this password is not recoverable however we can change it with the command below

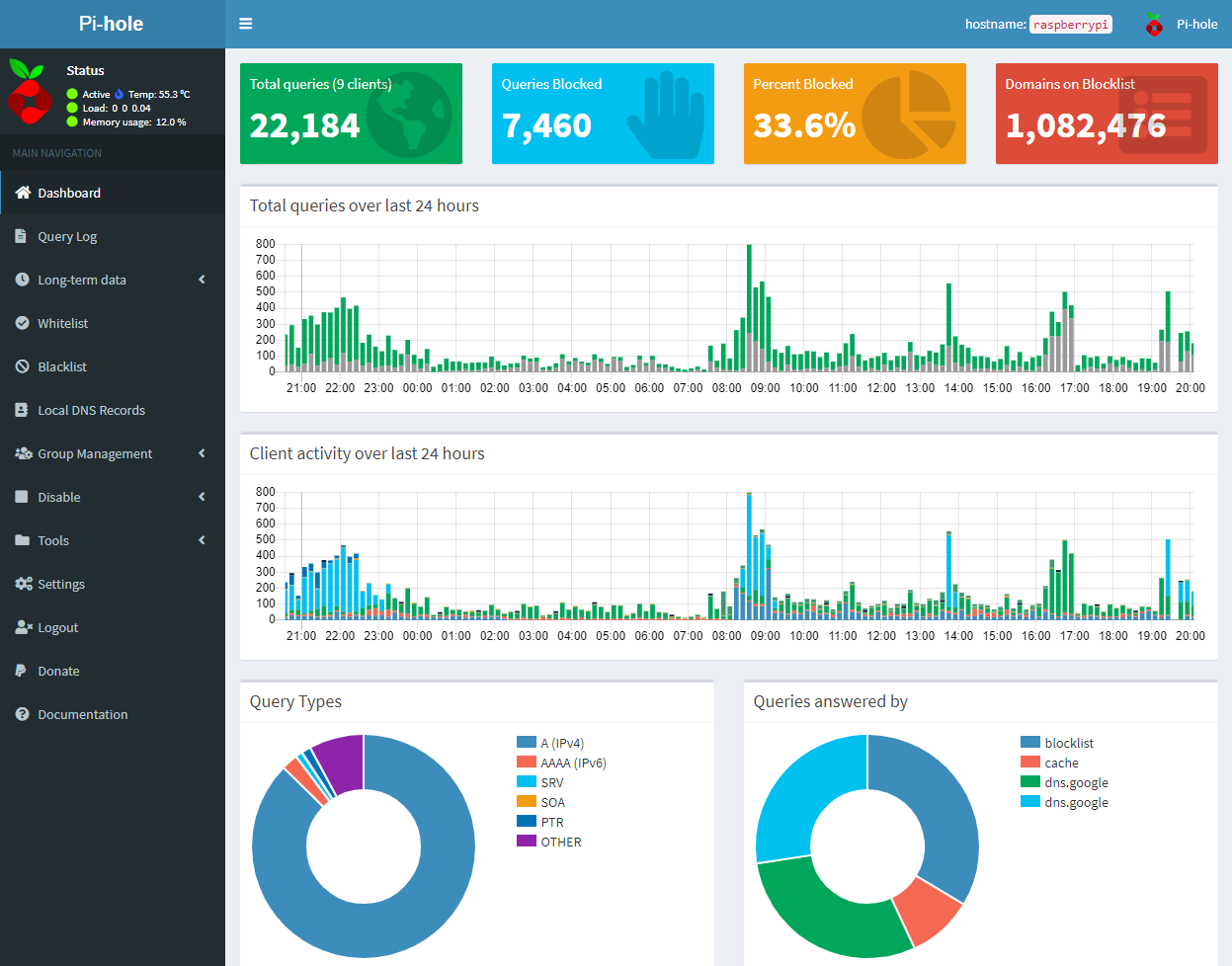
Sudo pihole -a -p **password**

Replace password with password of your choice or leave it blank if you don’t want any password(not recommended)

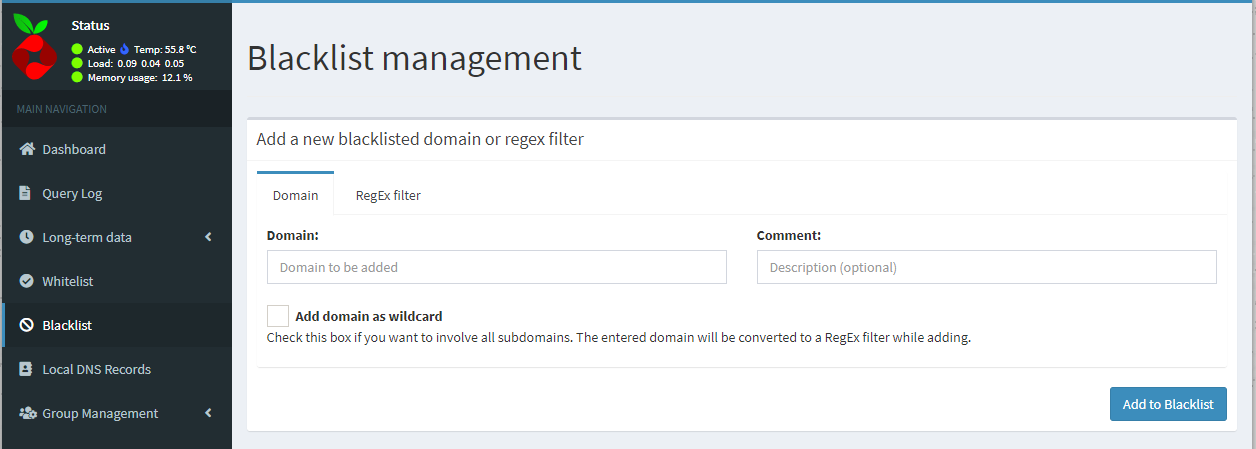
1. The admin page when initially launched shows as -



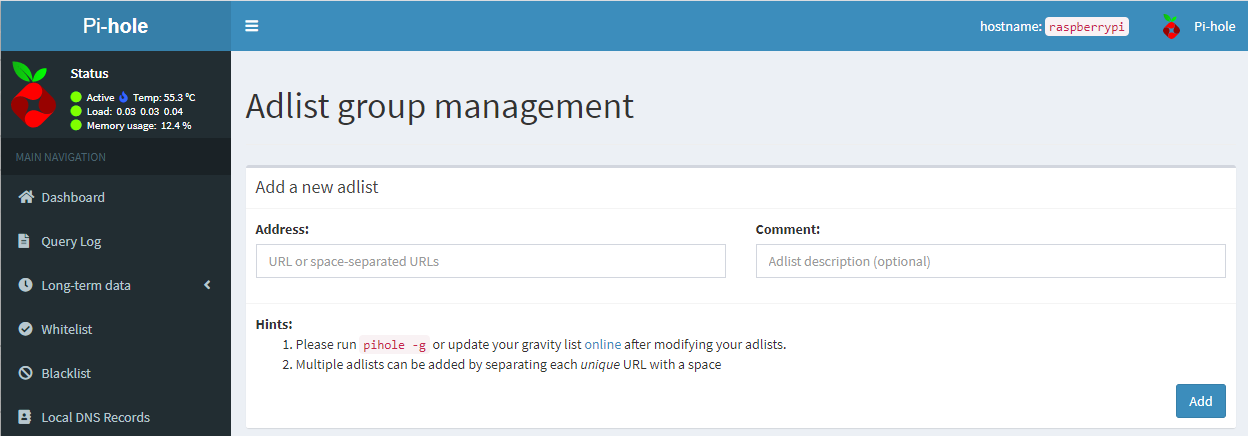
1. Click on login tab on the left to login to the page. Once logged in, the below dashboard would appear with a summary of all the client activity as well as the various options which can be configured.



1. The blacklist shows the list of websites which have been blocked, any website of choice can be added here, just type the domain name and click on add to blacklist. In case there are lots of websites, RegEx filters can be used to populate all them in one go.



1. The adlists page also has a list of common ad websites which can be blocked. Same procedure is followed to add the wesbites.



1. Common websites which can be used to configure ad websites –

<https://dbl.oisd.nl/>

<https://www.github.developerdan.com/hosts/>

<https://firebog.net/>

There are other websites and lists which are there in GitHub which can be populated to increase the scope.