

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/326319875>

Pi Black Hole for Internet Advertisements

Experiment Findings · July 2018

DOI: 10.13140/RG.2.2.14553.01124

CITATIONS

0

READS

1,344

1 author:



Rhythm Kr Dasgupta

JIS COLLEGE OF ENGINEERING

15 PUBLICATIONS 2 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



interactive assistant robot [View project](#)



Torrent Box [View project](#)

Pi Black Hole for Internet Advertisements

(Securing DNS-over-HTTPS)

Rhythm Kr Dasgupta

Email: rhythmdas0@gmail.com

Abstract

Pi Black-hole is device collection of set of software packages that provide filtering and advertisement blocking for all internet services on your network. It alleviates what might traditionally be done via adblockers or per-device software because it blocks things at the DNS level. It uses dnsmasq, lighttpd, FTL and some other packages to tie all this together into a nice, easy-to-use web interface. Pi Black-hole application can be installed on any existing Linux device or VM.

Pi Black-hole utilizes several well-known and trusted internet blacklists and keeps them up-to-date. At the DNS level it can then thwart unwanted ads, malware domains and other unsavory internet denizens from appearing on any of your internet devices or computers.

Keyword: Pi, DNS, IPV4, IPV6, Internet Advertisement, DHCP Server.

1. Introduction:

Pi Black-hole home-based techs, like the inexpensive and energy-efficient Raspberry Pi, to protect all of the devices on your home network from unwanted content. For parents, Pi Black-Hole can be used to block certain domains at router level to ensure any children using devices in the home aren't accessing unsuitable material. But for network admins, Pi Black-Hole can be used as a network monitoring tool as well it can record all DNS queries sent to it so it is possible using the web interface to analyze and review traffic. This can be particularly helpful during any network investigation and it is also possible for Pi Back-Hole to increase network speed.

2. Methodology

Pi Black-hole is a little application that runs on the Raspberry Pi and block adverts at the DNS level, it can optionally act as your DHCP server as well.

Pi Black-Hole works at the DNS level. So, when an ad is blocked, it's actually prevented from being downloaded in the first place because the DNS query is intercepted. Since these ads images, videos, and sounds are not being downloaded, network will perform better. For better understanding, domains trying to spread malware through boughs 'Adobe Flash' updates can be blocked at Network level.

For devices such as Smart TVs which don't use a browser but still feature ads, these can also be blocked using Pi Black-Hole. Viewing YouTube videos on mobile phones, PlayStation and Xbox gaming consoles, all ads will be blocked.

3. Hardware for Pi Black-Hole

1. Raspberry Pi 3
2. 16GB (or greater) micro SD Card class 10 (or faster) (and a card reader, duh)
3. Power bank (5.0 volt)
4. External USB Hard Drive (the bigger the better) with an external power.
5. SSH Client (here I use Putty).

4. Software Configuration and Testing

Step 1: Upgrading the Pi

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

With this done, reboot the pi using;

```
sudo reboot
```

Step 2: Static IP Address for the Pi

The first thing needed to do was to set up a static IP. To do this edited the dhcpd.conf as follows:

```
sudo nano /etc/dhcpd.conf
```

Edit the configuration, then add the following to the end (using the settings specific to your network/IP):

```
interface eth0/wlan0
```

```
static ip_address=192.168.0.101
```

```
static routers=192.168.0.1
```

```
static domain_name_servers=192.168.1.1
```

Reboot the Pi (sudo reboot) and log back in via SSH.

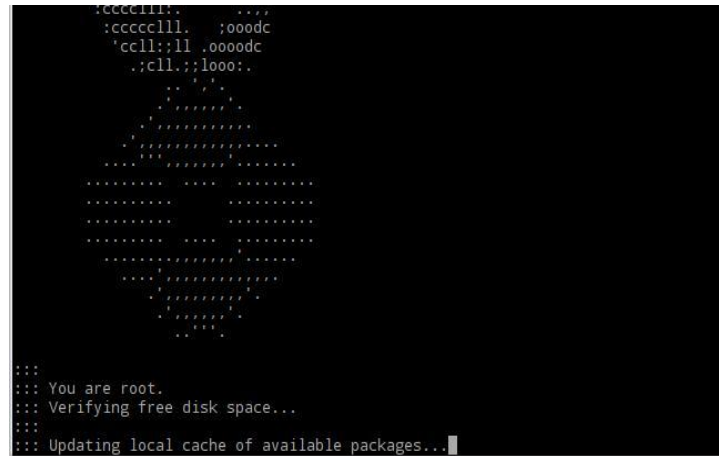
It's a good idea to set a static IP address for Pi—either in the Pi's own settings, or (preferably) on network's router (if the router allows to assign static IP addresses to devices based on MAC address).

Step 3: Setup Black Hole application

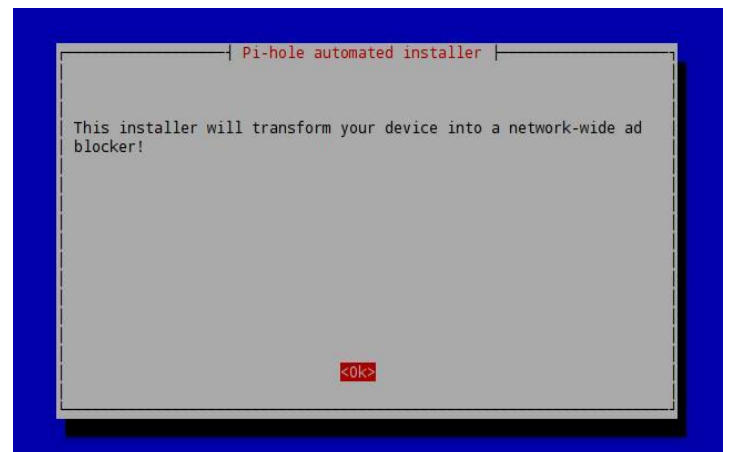
Pi-hole makes it as easy as possible to download and get running with a one-line script that starts up a menu-based installer.

```
curl -sSL https://install.pi-hole.net | bash
```

Pi Black-hole uses curl to download the installation script, which is then executed by the bash shell.

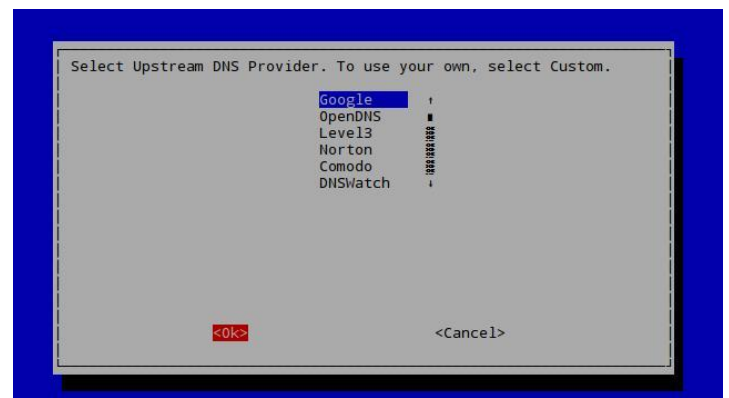


Installer will the proper privileges and confirm you have enough disk space.



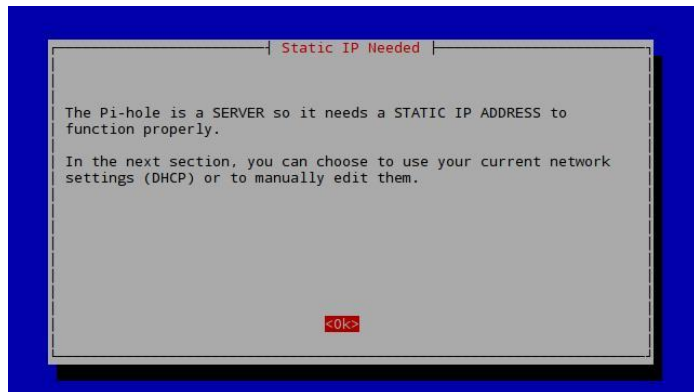
Setting up DNS on Pi-hole:

The very first step of the installation process is setting up Pi-hole's DNS passthrough.



Pi-hole will handle all of the DNS requests to block mobile ads itself, but it passes the rest along to another DNS provider. Google and OpenDNS are both safe choices.

If you need advanced privacy features like DNSSEC and DNSCrypt, Pi-hole recommends select Google or Norton DNS servers.

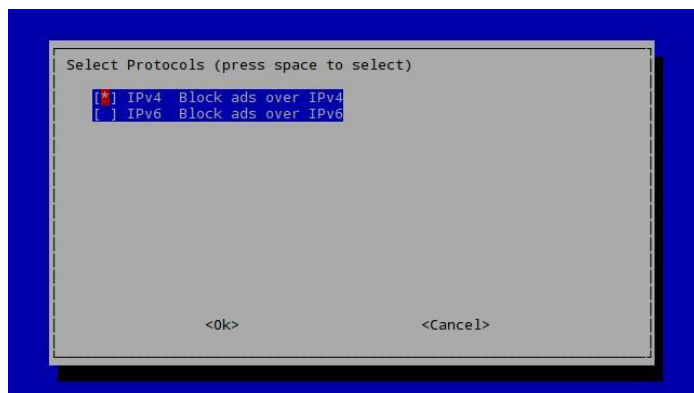


I chose to use Google's DNS servers with this install and added in OpenDNS and custom servers as a backup in a later step.

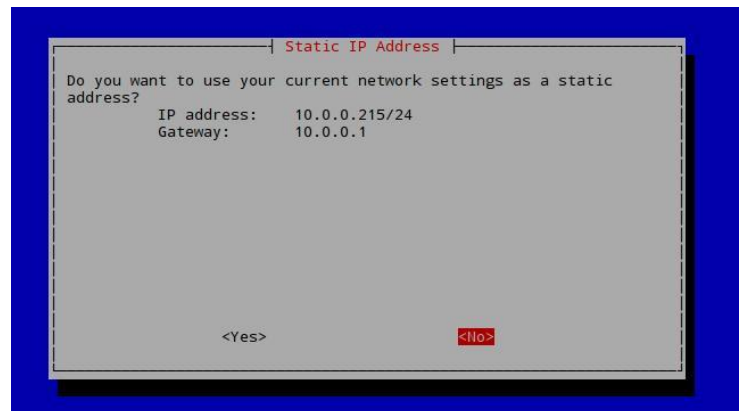
If you're using a VPN, you'll need to select Custom and enter your VPN provider's DNS servers. IPVanish users should set the custom DNS servers to 198.18.0.1 and 198.18.0.2. If you're using a different VPN provider, you'll need to search the web for their DNS servers or check your VPN configuration files.

Setting up network

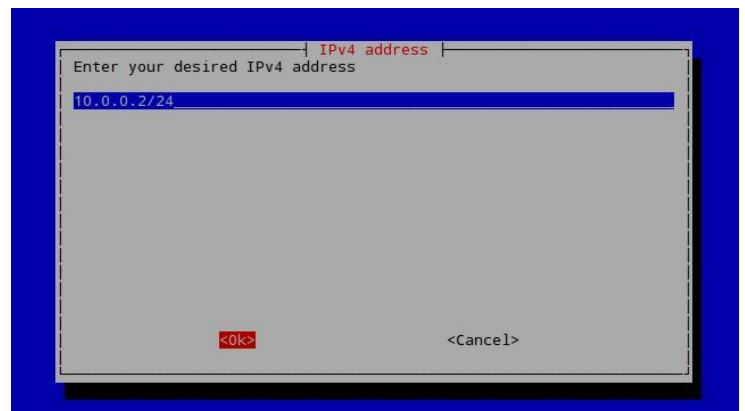
Pi-hole send DNS traffic, the next step is telling Pi-hole about your local network. You'll need to set the gateway address and assign Pi-hole a static IP.



Pi-hole will block mobile ads over both IPv4 and IPv6 networks.

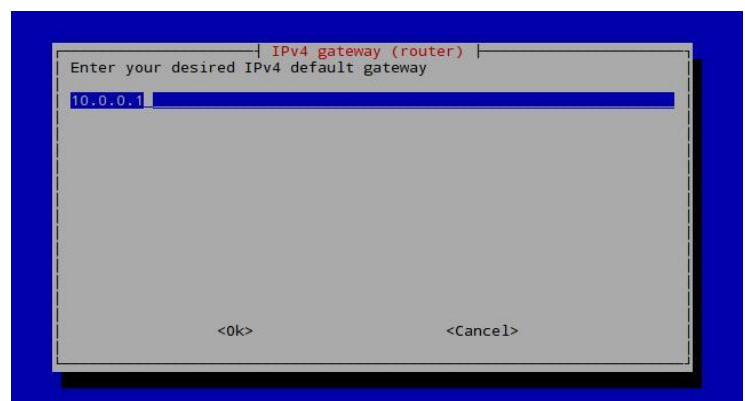


Next, assigned IP address static.



Set the IP address to x.x.x.2/24. In most cases this will be 192.168.1.2/24 or 10.0.0.2/24. Traditionally your gateway router is assigned x.x.x.1/24 and DNS servers are given an address very close to that.

Assigned the IPv4 default gateway

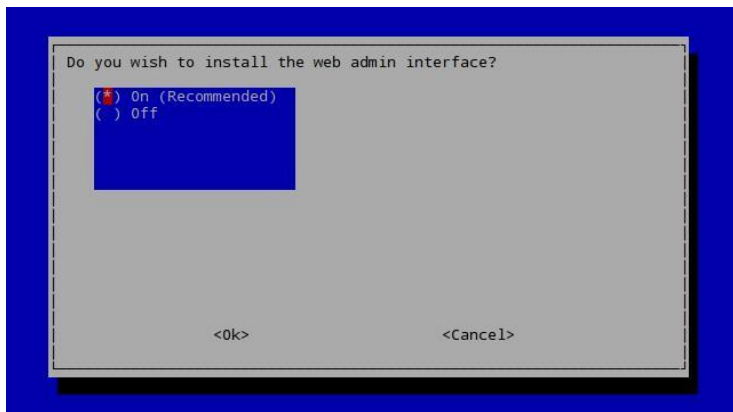


Specify router's IP address, it's the same one that Pi-hole showed you in a previous step.

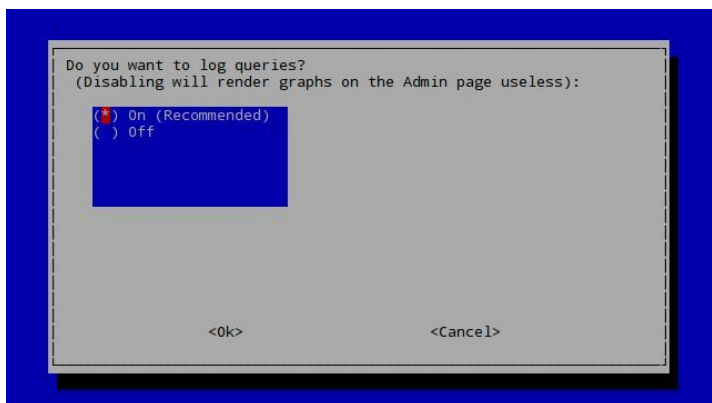


The final portion of the installation is focused on enabling or disabling a few core services in Pi-hole.

Install the web interface it manages Pi Black-hole after it's installed.



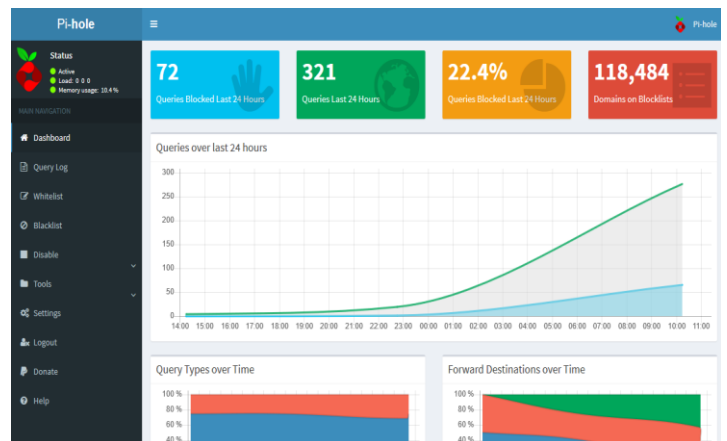
Enabled logging to make my graphs work properly. If running a bunch of different servers on Raspberry Pi, or if it's an old model, that can shut off logging to free up a bit more memory.



Disable logging if you're using Pi-hole with a VPN in order to protect your privacy. Pi-hole keeps real-time logs of which sites it blocks, and which ones are allowed through, in order to generate usage graphs—and these logs aren't encrypted.

```
...
::: IPv4 address: 10.0.0.2/24
::: IPv6 address:
::: Web Interface On.
::: Logging On.
:::
::: Checking for existing repository...
::: Cloning https://github.com/pi-hole/pi-hole.git into /etc/pihole... done!
:::
::: Checking for existing repository...
::: Cloning https://github.com/pi-hole/AdminLTE.git into /var/www/html/admin... done!
:::
::: Checking for bc... added to install list!
::: Checking for cron... installed!
::: Checking for curl... installed!
::: Checking for dnsmasq... added to install list!
::: Checking for dnsutils... added to install list!
::: Checking for iputils-ping... installed!
::: Checking for isof... added to install list!
::: Checking for netcat... added to install list!
::: Checking for sudo... installed!
::: Checking for unzip... installed!
::: Checking for wget... installed!
```

Configuring Pi Black-hole:



Most networks these days support IPv4 and IPv6. If an advertisement fails to deliver over IPv4, it can still be delivered via IPv6. Pi Black-hole can already use both protocols to block advertisements, but IPv6 is more complex so this is the first place you might run into issues with slowness when using it.

It will take a minute to generate the complete log, but you can follow the progress on your screen. You'll see a message when Pi-hole has finished generating the log.

6. Troubleshooting

Fixing HTTPS Issues That Cause Slow-Loading Pages

As mentioned previously, Pi-hole is only handling the DNS queries and doesn't know about the other protocols that are taking place. But we can use iptables to manage these protocols to prevent time-outs allowing Pi-hole work its magic.

There are several iptables rulesets you can put in place to optimize your Pi-hole's performance. These commands are explained in detail here, but at a high-level, they will prevent your Pi-hole from timing out over HTTP/HTTPS requests on ports 80/443, resulting in a faster browsing experience.

Fixing IPv6 Issues That Cause Slow-Loading Pages

Some ISPs do not hand out static IPv6 addresses. configured Pi-hole with an IPv6 address during installation and that address is later changed by your ISP, you now run into the problem the wrong (i.e. an invalid) IPv6 address in gravity.list.

Here are a couple of tips for troubleshooting Pi Back-hole if you run into problems.

It's not blocking ads

On two different Android devices, I needed to restart Chrome before the ads went away. You should also double-check your device's network settings to make sure Pi-hole is set as your primary DNS server.

I whitelisted a website and Pi-hole stopped blocking ads

You probably have an invalid or overly-broad wildcard in your whitelist. Whitelisting *.com or something similar can cause Pi-hole to stop working, so be as specific as you can when you allow a site to display ads.

I can't block ads in apps

Some apps come with embedded ads that are actually part of the programming. Since there's no need to look up an IP address and load them from the internet, there's no way for Pi-hole to block these mobile ads.

A good rule of thumb is that, if your app will display ads properly even in airplane mode, Pi-hole won't be able to block that ad.

Unfortunately, nothing can be done about apps with embedded ads using Pi-hole.

I need to generate debug information

On the official Pi-hole forums, which is the best place to go for support, you'll be encouraged to post debug information along with a description of your problem. Here's how to generate debug information for Pi-hole.

7. Conclusion

You now have a simple yet effective way of filtering any DNS request on network, but keep in mind that you might need to tweak your block lists a bit to suit your personal browsing habits.

To learn about another way of running Pi-hole, see this project that puts Pi-hole in a Docker container.

Or, to further enhance network security, find out how to enable DNSCrypt on your current Pi Black-hole installation to create a private and secure intranet.

9. Acknowledgements

This project required genuinely efforts. Nevertheless, it would not have been realizable without the assistance and help from many individuals and organizations. Various tutorials and resources given in the official website of Raspberry Pi have made initial works easier.

Last but not least, my thanks and appreciations also go to my brother come guide **Mr. Subhajit Roy** and **Mr. Moaz al Hosny** who have willingly helped me out with their abilities.

10. References

11. ["Pi-hole®: A black hole for Internet advertisements". Pi-hole®: A black hole for Internet advertisements. Retrieved 2018-04-15.](#)
12. ^ Jump up to:^{a b} ["Pi-hole is a black hole for internet ads #piday #raspberrypi @Raspberry Pi". Adafruit Industries - Makers, hackers, artists, designers and engineers!. 2016-03-04. Retrieved 2018-05-06.](#)
13. ^ Jump up to:^{a b} ["Turn A Raspberry Pi Into An Ad Blocker With A Single Command". Lifehacker Australia. 2015-02-17. Retrieved 2018-05-06.](#)
14. [Jump up^ Leathern, Rob \(2015-12-23\). "Block Ads on All Home Devices for \\$53.18". Rob Leathern. Retrieved 2018-05-06.](#)
15. [Jump up^ "Adblock Everywhere: The Raspberry Pi-Hole Way". MakeUseOf. Retrieved 2018-05-06.](#)
16. ^ Jump up to:^{a b} ["pi-hole/pi-hole". GitHub. Retrieved 2018-04-15.](#)
17. [Jump up^ "Pi-hole hardware kit". Pi-hole hardware kit. 2018-05-07. Retrieved 2018-05-08.](#)
18. [Jump up^ "Pi-Hole in the cloud · Cody Bunch". blog.codybunch.com. Retrieved 2018-05-06.](#)
19. ^ Jump up to:^{a b c d} ["Seven Things You May Not Know About Pi-hole". Pi-hole®: A black hole for Internet advertisements. 2017-05-12. Retrieved 2018-05-06.](#)
20. [Jump up^ "AdBlocking with Pi-Hole and Ubuntu 14.04 on VirtualBox". hbalagtas.blogspot.co.uk. Retrieved 2018-05-06.](#)
1. ["Ad-Blocking on Apple iOS9: Valuing End User Experiences - Catchpoint Blog". Catchpoint's Blog - Web Performance Monitoring. 2015-09-14. Retrieved 2018-05-06.](#)
2. ["Running a Network-wide Ad-blocker, and a Whole Lot More". CryptoAUSTRALIA Blog. 2017-11-02. Retrieved 2018-05-06.](#)
3. ["Block Millions Of Ads Network-wide With A Raspberry Pi-hole 2.0". Jacob Salmela. 2015-06-16. Retrieved 2018-04-15.](#)
4. [Jump up^ "Pi-hole: A Raspberry Pi Ad-Blocker with DNS Caching \(Ultra-fast\)". Jacob Salmela. 2014-06-11. Retrieved 2018-05-06.](#)
5. ^ Jump up to:^{a b} ["pi-hole/pi-hole; Contributors". GitHub. Retrieved 2018-05-06.](#)
6. [Jump up^ Jeffries, Adrienne \(2018-05-10\). "Inside the Brotherhood of the Ad Blockers". Bloomberg.](#)
7. [Jump up^ "pi-hole/pi-hole; The Origin Of Pi-hole". GitHub. Retrieved 2018-04-15.](#)
8. [Jump up^ "How does Pi-hole work?". Pi-hole Userspace. Retrieved 2018-05-06.](#)
9. [Jump up^ "What Really Happens On Your Network? Find Out With Pi-hole". Pi-hole®: A black hole for Internet advertisements. 2017-02-22. Retrieved 2018-05-06.](#)
10. [Jump up^ "Enjoy The Rio Olympics Ad-free With Pi-hole". Pi-hole®: A black hole for Internet advertisements. 2016-08-11. Retrieved 2018-05-06.](#)