# Assignment 1 – Pi-hole Report

**CEG 4399**

**Ashair Imran, 300071365**

**September 25, 2022**

## 1.0 Introduction

The Pi-hole, as described by its developers, is a “DNS sinkhole that protects your devices from unwanted content, without installing any client-side software. [It provides] network-wide ad blocking via your own Linux hardware.” In essence, it is an ad-blocker that functions by blocking domains that serve ads. It was created originally to be used with a Raspberry Pi, a small single-board computer that can be programmed for many purposes. However, as we will see throughout this report, the Pi-hole does not require a Raspberry Pi, and can be implemented using an Ubuntu server on a virtual machine.

Ubuntu is a Linux based OS and can be installed as an independent server. Although a Raspberry Pi would be ideal, we can instead use an Ubuntu server as it can be run for free on a virtual machine. The downside is that the virtual machine must be always running for as long as you want the Pi-hole to be active. Depending on the desktop or laptop used, keeping the virtual machine running will consume a lot more power than a single Raspberry Pi as the device hosting the virtual machine must stay powered on. The virtual machine hosting software of choice for this assignment is Oracle’s VM VirtualBox.

This report will first introduce and define DNS Servers, the Pi-hole, and how the Pi-hole integrates with a DHCP server. Then, the installation process will be covered as well as the configuration for single devices, and the hypothetical configuration with a whole network. Finally, the results of the Pi-hole will be covered, including the statistics retrieved, the discussion of the results, problems encountered, and solutions obtained.

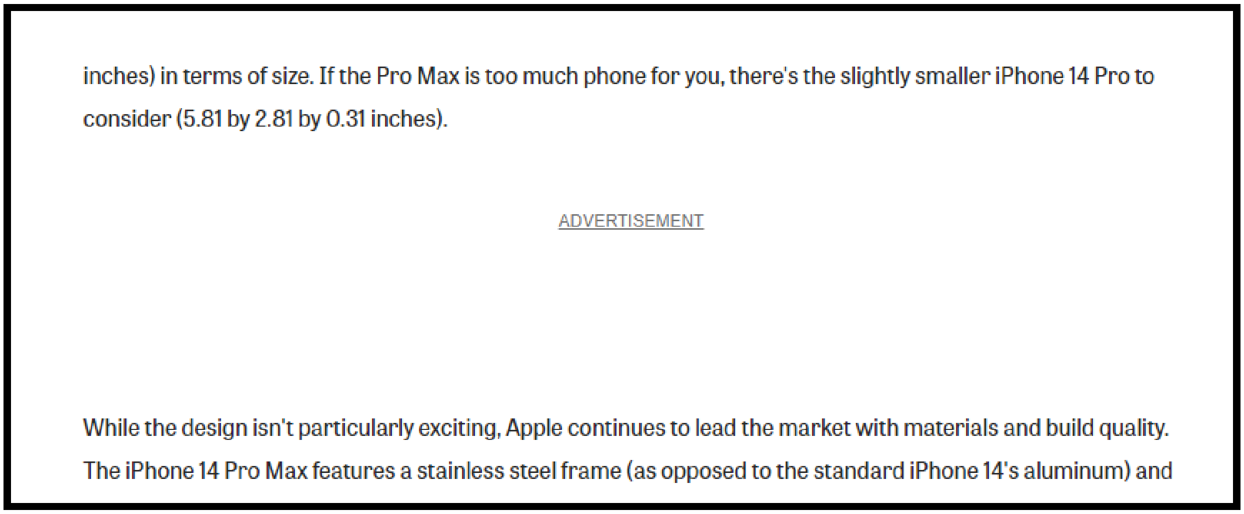
## 1.1 DNS Servers

DNS stands for Domain Name System. It is a system used to apply names to I.P addresses so that they can be easily identified. For example, ‘uottawa.ca’ is a domain name and the DNS would translate that domain name into it’s corresponding I.P address. DNS servers help computers connect to other computers and networks by receiving the domain name and finding the corresponding I.P address to make the connection. A DNS server is responsible for receiving these requests or “queries” from user machines and then resolving these queries by acquiring the correct IP.

For example, if I wished to visit ‘uottawa.ca’ and I typed this into the address search bar, there are a lot of things going on behind the scenes to make sure that my computer can make the connection to the webpage. First, my computer will send a query to my DNS server. The server will first ask the root server for the address of the top-level domain (TLD). In this case, the TLD is ‘.ca’. The DNS server will then perform a similar query to the TLD server for ‘.ca’. This TLD server will then return the address for the nameserver ‘uottawa’ which will finally provide the address for the server I was originally trying to connect to. Once the connection is made, the server can provide me with the content of the webpage. As you can see, much of your internet browsing traffic goes through your DNS server, so it is a crucial access point to implement content-blocking and security.

## 1.2 Pi-Hole

As was discussed earlier, the Pi-hole blocks unwanted content when browsing the internet through a “DNS sinkhole”. The Pi-hole acts as a local DNS server that manages all the DNS queries that your computer sends. Every query is compared with a list of ad-serving domains. If the domain is not on the list, then the DNS query is sent “upstream” to a proper DNS server that will retrieve the domain. If the domain that is queried is on the list, and therefore intended to be blocked, the Pi-hole will never send the query and therefore never retrieve the content from the blocked domain. What occurs is that the advertisement is replaced with white space, as seen below:



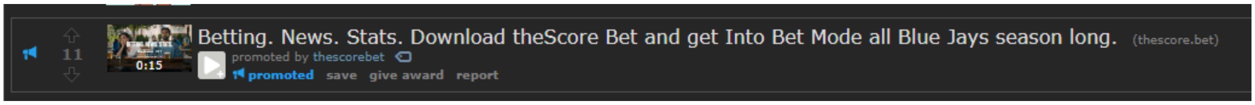
inches) in terms of size. If the Pro Max is too much phone for you, there's the slightly smaller iPhone 14 Pro to consider (5.81 by 2.81 by 0.31 inches).

ADVERTISEMENT

While the design isn't particularly exciting, Apple continues to lead the market with materials and build quality. The iPhone 14 Pro Max features a stainless steel frame (as opposed to the standard iPhone 14's aluminum) and

*Figure 1: A screenshot taken from a news article (https://www.pcmag.com/reviews/apple-iphone-14-pro-max) while Pi-hole is running on the device*

As seen in figure 1, the advertisement never appears as the ad-serving domain is blocked. The Pi-hole effectively acts as a filter that filters out unwanted domains. What remains is the HTML placeholder on the webpage. However, since the Pi-hole is based solely on blocking DNS queries, it should not be seen as the preeminent ad-blocker. Many popular websites, such as YouTube and Reddit, deliver ads from their own domain. This means that Pi-hole cannot block the ad-serving domain, because the ad-serving domain is also the content-serving domain. If you block the domain, you will not be able to access the website.



Betting. News. Stats. Download theScore Bet and get Into Bet Mode all Blue Jays season long. (thescore.bet)

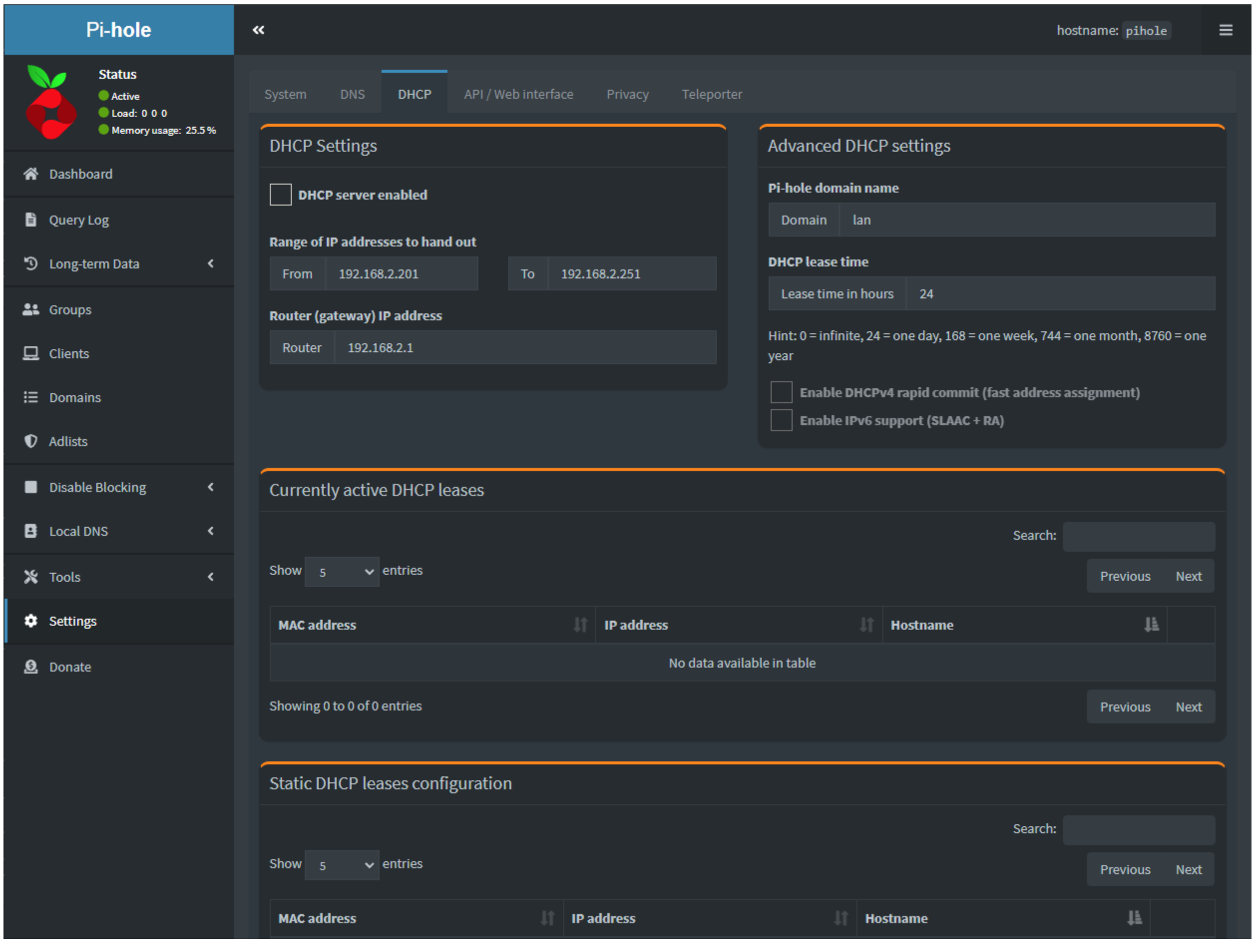
promoted by thescorebet

*Figure 2: A screenshot taken from reddit.com with Pi-hole active on the device*

Figure 2 shows an advertisement on reddit.com that has been delivered from the same domain that the rest of the content is delivered through. Although Pi-hole does not block all advertisements, it can be combined with other ad-blocking browser extensions to provide a completely ad-free experience when browsing the internet.

### 1.3 DCHP Server Integration

The Pi-hole also has compatibility to work as a DHCP server. DHCP stands for Dynamic Host Configuration Protocol and is a network protocol used on top of I.P to assign addresses automatically and dynamically. DHCP is used as an alternative to static I.P addresses and is used to avoid the manual network configuration of clients. Generally, static I.P addresses are used for servers because a static I.P makes it easier for clients to access the server. Pi-hole itself requires the use of a static I.P address, or a reserved DHCP address, to function properly. Although the Pi-hole server itself uses a static I.P, when installed, the Pi-hole can be configured as a DHCP server that can hand out I.P addresses from varying ranges on the network.



DHCP Settings

□ DHCP server enabled

Range of IP addresses to hand out

From 192.168.2.201 To 192.168.2.251

Router (gateway) IP address

Router 192.168.2.1

Advanced DHCP settings

Pi-hole domain name

Domain lan

DHCP lease time

Lease time in hours 24

Hint: 0 = infinite, 24 = one day, 168 = one week, 744 = one month, 8760 = one year

□ Enable DHCPv4 rapid commit (fast address assignment)

□ Enable IPv6 support (SLAAC + RA)

Currently active DHCP leases

| MAC address | IP address | Hostname |
|---|---|---|
| No data available in table | | |

Showing 0 to 0 of 0 entries

Static DHCP leases configuration

| MAC address | IP address | Hostname |
|---|---|---|

*Figure 3: A screenshot from the DHCP settings menu from the Pi-hole admin interface*

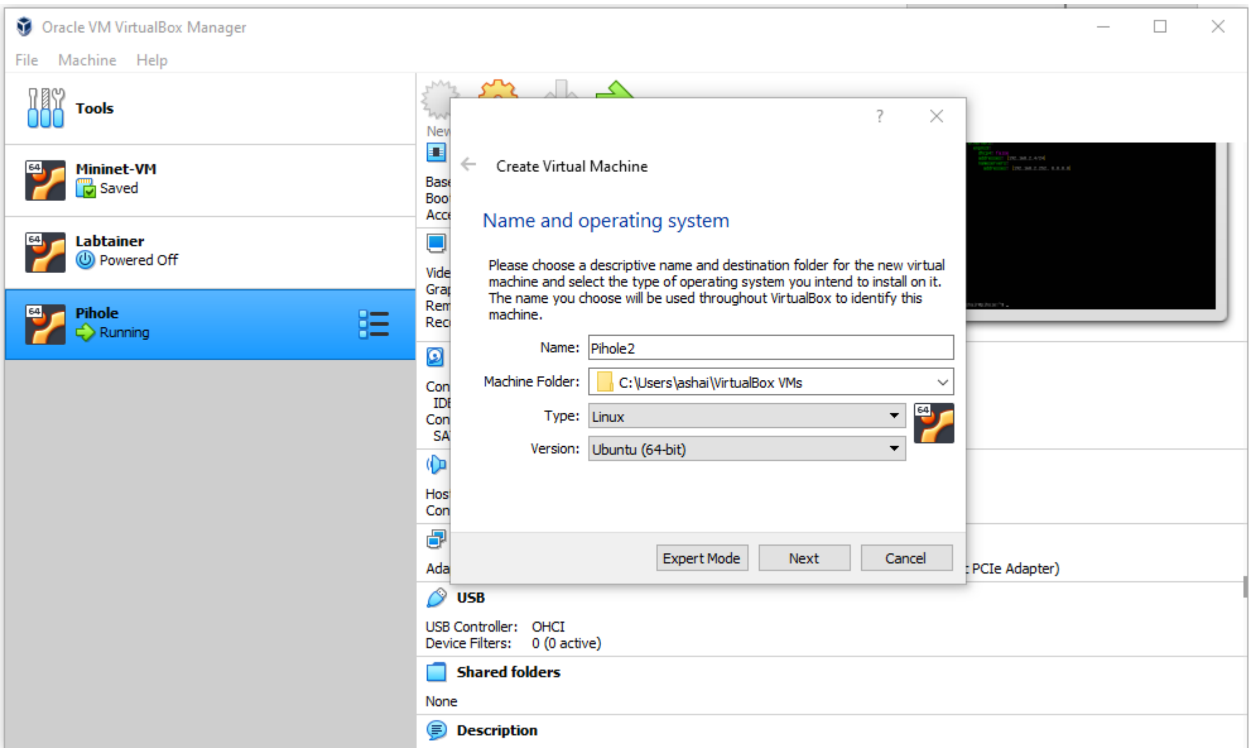
The Pi-hole admin interface has a wide selection of DHCP settings, as can be seen in figure 3. The Pi-hole will let you manage and configure DHCP leases, set its domain name, the DHCP lease time. IPv6 support, and more.

Typically, your router will act as a DHCP server to assign I.P addresses to the devices on that network. Some routers will not allow you to make the necessary router changes to apply Pi-hole to the entire network. By setting Pi-hole as a DHCP server, you can sometimes circumvent the need to make hardware modifications on the router.

## 2.0 Installation

As was discussed in the introduction, for the purposes of this project, the Pi-hole was installed on an Ubuntu server hosted on Oracle VM VirtualBox. A Raspberry Pi, although ideal, was not used for this project.

The first step was to install Oracle VM VirtualBox and download the latest Ubuntu LTS Server .iso file. This project used Ubuntu version 22.04.1. Then a new virtual machine was created in VirtualBox



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Pihole2

Machine Folder: C:\Users\ashai\VirtualBox VMs

Type: Linux

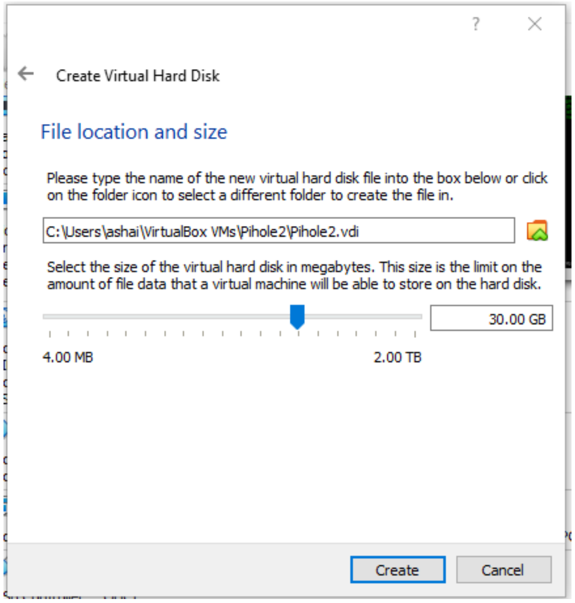
Version: Ubuntu (64-bit)

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders: None

*Figure 4: Virtual Machine creation menu in VirtualBox*

The default memory size of 1024 MB was used. A virtual hard disk was created using the VDI file type (VirtualBox Disk Image). 30GB of hard drive space was set as the limit so that there was enough space for Pi-hole to be installed onto the virtual machine.



Create Virtual Hard Disk

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

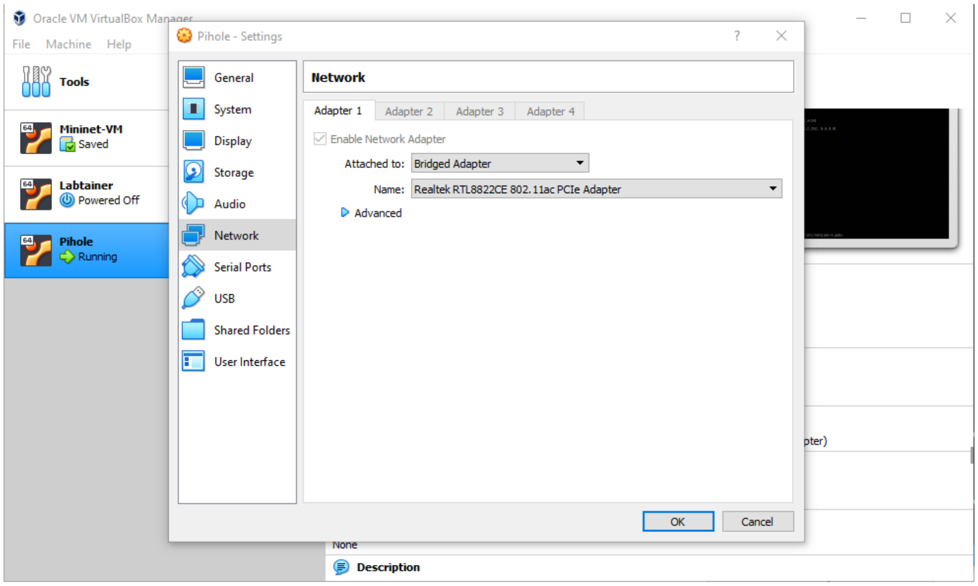
C:\Users\ashai\VirtualBox VMs\Pihole2\Pihole2.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

30.00 GB

*Figure 5: 30gb of hard drive space was allotted to have enough space to install Pi-hole*

Once the virtual machine was created, the network adapter is switched from NAT to "Bridged Adapter". This allows the server to use the I.P address of the device. Then the previously downloaded iso file for the Ubuntu server was applied to the VM and it was launched. The console opens into the Ubuntu setup. All the defaults were selected except that OpenSSH server was installed. One issue encountered was that the Ubuntu would not complete the installation unless the network was disabled. I opted to disable the network adapter on VirtualBox and to re-enable it post-installation to then configure the network manually. After disabling the network, Ubuntu was successfully installed.



Pihole - Settings

Network

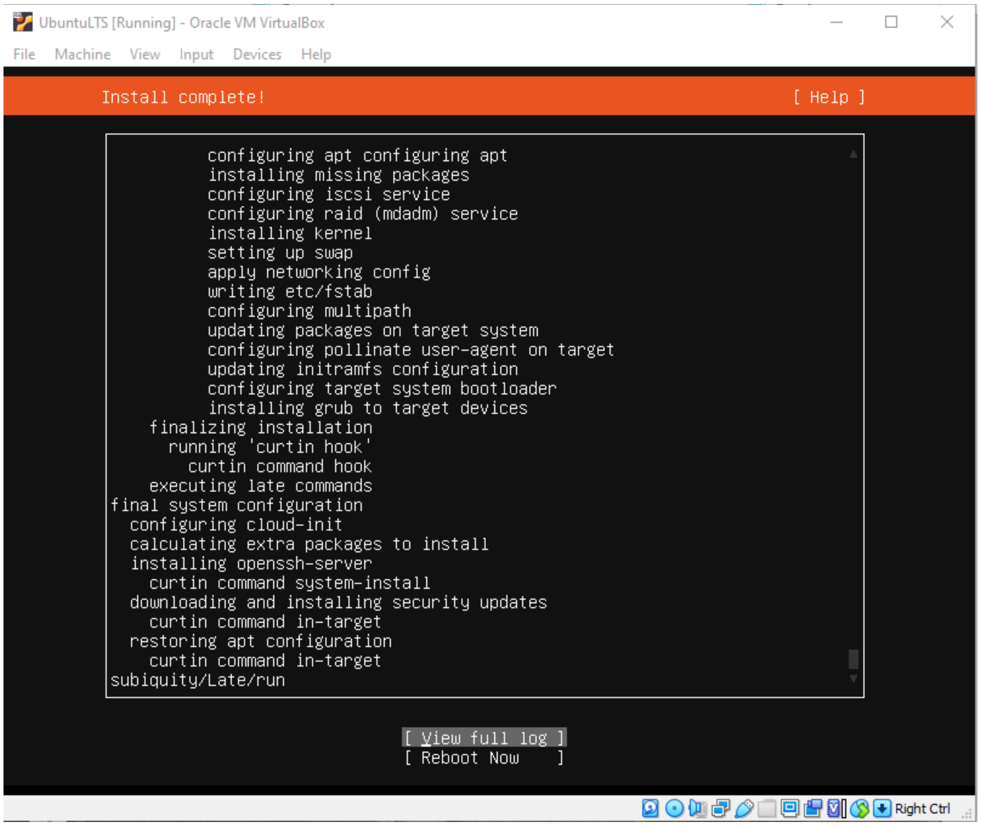
Adapter 1

☑ Enable Network Adapter

Attached to: Bridged Adapter

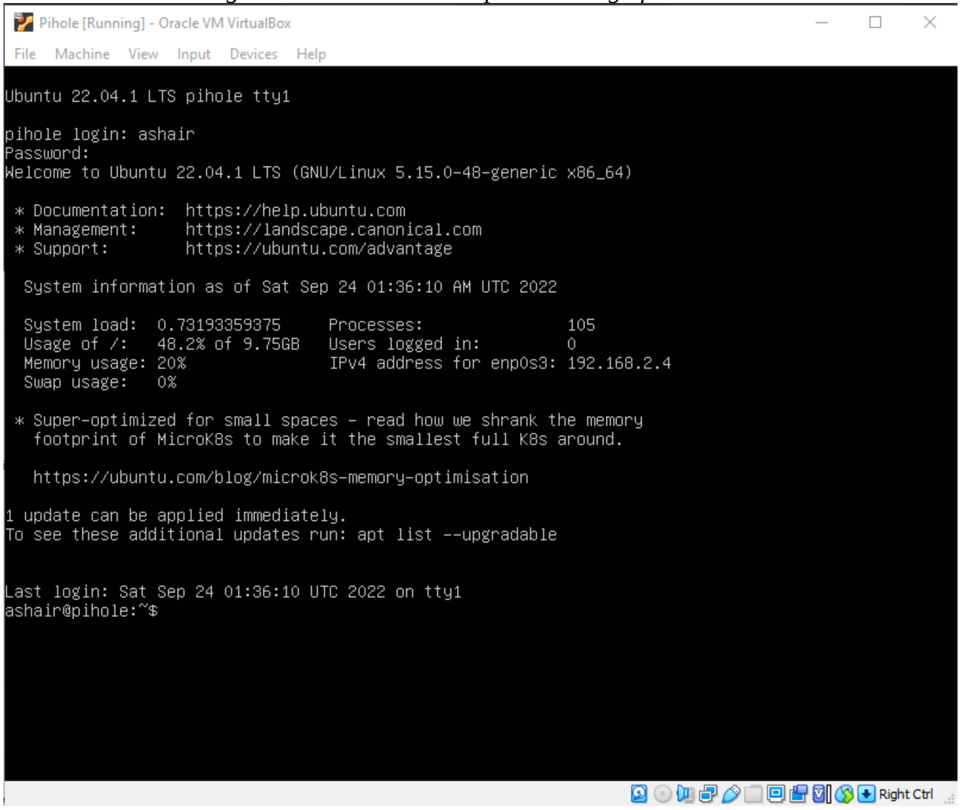
Name: Realtek RTL8822CE 802.11ac PCIe Adapter

*Figure 6: Set network adapter to Bridged Adapter. Disabled during installation due to bug and re-enabled post-installation.*


UbuntuLTS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
        Install complete!                                                [ Help ]

                     configuring apt configuring apt
                     installing missing packages
                     configuring iscsi service
                     configuring raid (mdadm) service
                     installing kernel
                     setting up swap
                     apply networking config
                     writing etc/fstab
                     configuring multipath
                     updating packages on target system
                     configuring pollinate user-agent on target
                     updating initramfs configuration
                     configuring target system bootloader
                     installing grub to target devices
               finalizing installation
                 running 'curtin hook'
                   curtin command hook
               executing late commands
           final system configuration
             configuring cloud-init
             calculating extra packages to install
             installing openssh-server
               curtin command system-install
             downloading and installing security updates
               curtin command in-target
             restoring apt configuration
               curtin command in-target
           subiquity/Late/run

                                  [ View full log ]
                                  [ Reboot Now    ]
```

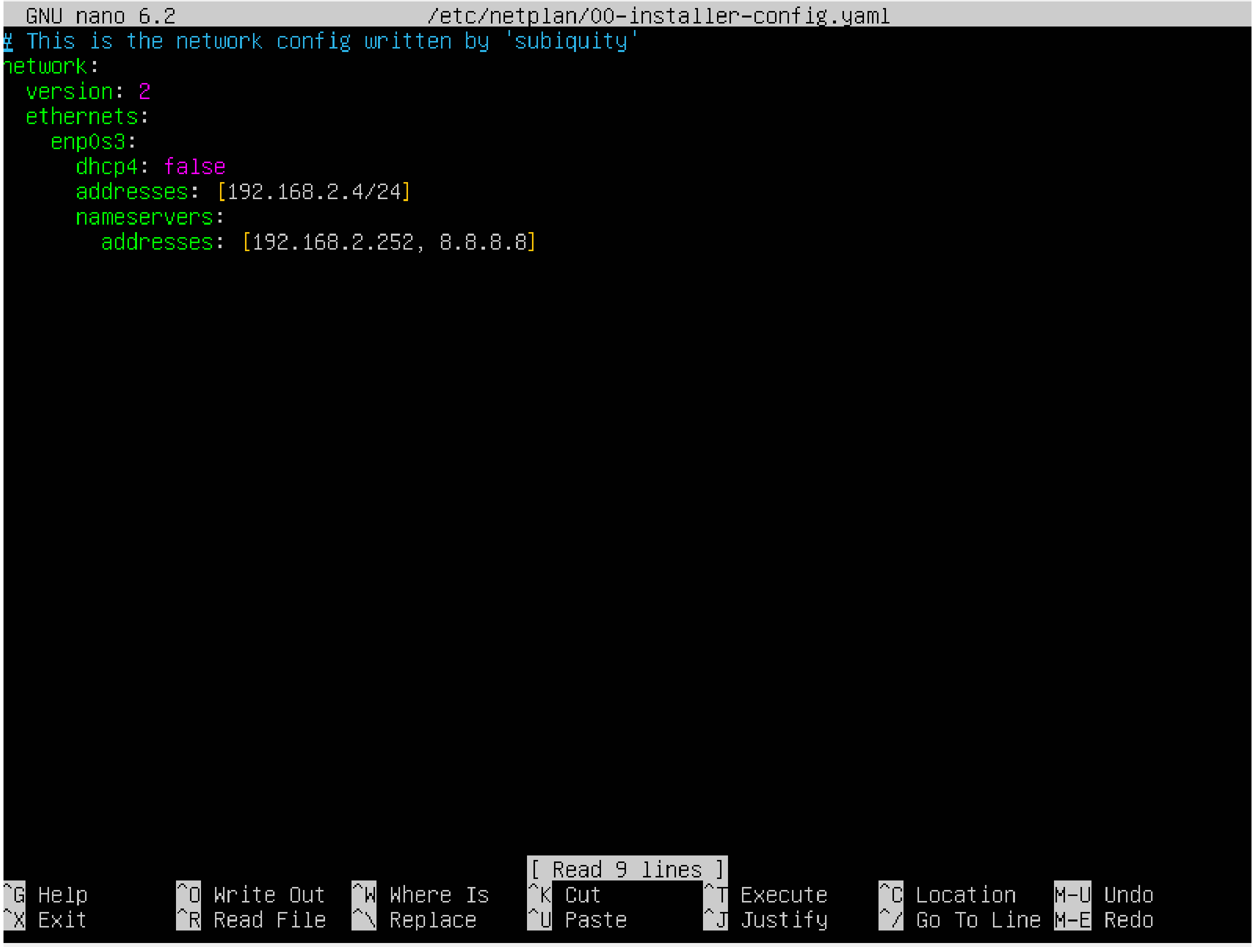
*Figure 7: Installation complete message for Ubuntu*


Pihole [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Ubuntu 22.04.1 LTS pihole tty1

pihole login: ashair
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Sep 24 01:36:10 AM UTC 2022

  System load:  0.73193359375     Processes:             105
  Usage of /:   48.2% of 9.75GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enp0s3: 192.168.2.4
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Sat Sep 24 01:36:10 UTC 2022 on tty1
ashair@pihole:~$
```

*Figure 8: The welcome message to the Ubuntu Server console*

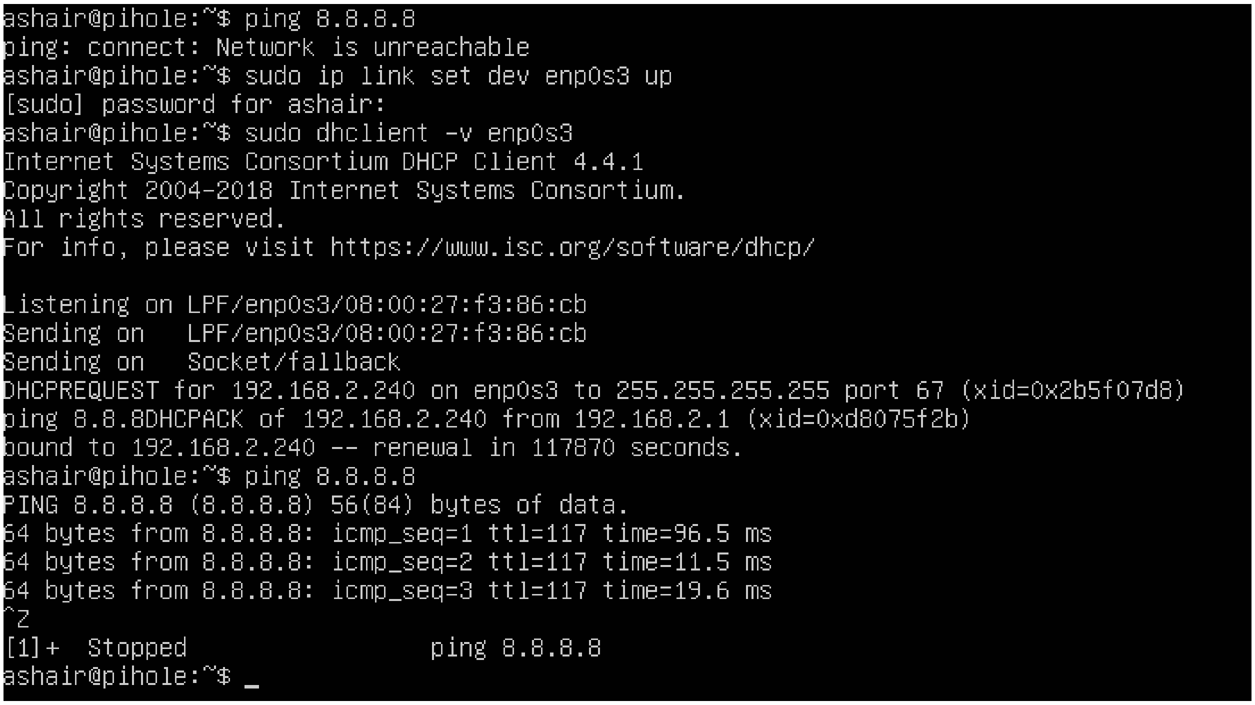
Since the network had to be disabled to complete the installation due to a bug, the next step was to manually configure the network. This may seem like a hassle, but Pi-hole requires a static I.P to function correctly (As shown in figure 11), and the method of setting a static I.P is similar to configuring the network I.E, we must modify the netplan in both cases. Using the command '*sudo nano /etc/netplan/*.yaml*' The empty netplan file was opened and configured as shown in figure 8 below.



```
  GNU nano 6.2                    /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: false
      addresses: [192.168.2.4/24]
      nameservers:
        addresses: [192.168.2.252, 8.8.8.8]
```

*Figure 9: The modified netplan file.*

In a typical Ubuntu installation, most of these values are automatically filled. The important thing to note is that that dhcp4 boolean variable is set to 'false'. As was discussed in the introduction section of the report, DHCP will set the server with a dynamic I.P, which is not what we desire. Setting dhcp4 to 'false' is very important for Pi-hole as it sets the Ubuntu server with a static I.P. The netplan is then applied with the command '*sudo netplan apply'*. However, we are still not connected to the network. We must apply two more commands to manually connect to the internet. These commands are '*ip link set dev enp0s3 up'* followed by '*dhclient -v enp0s3'* as shown in figure 9.

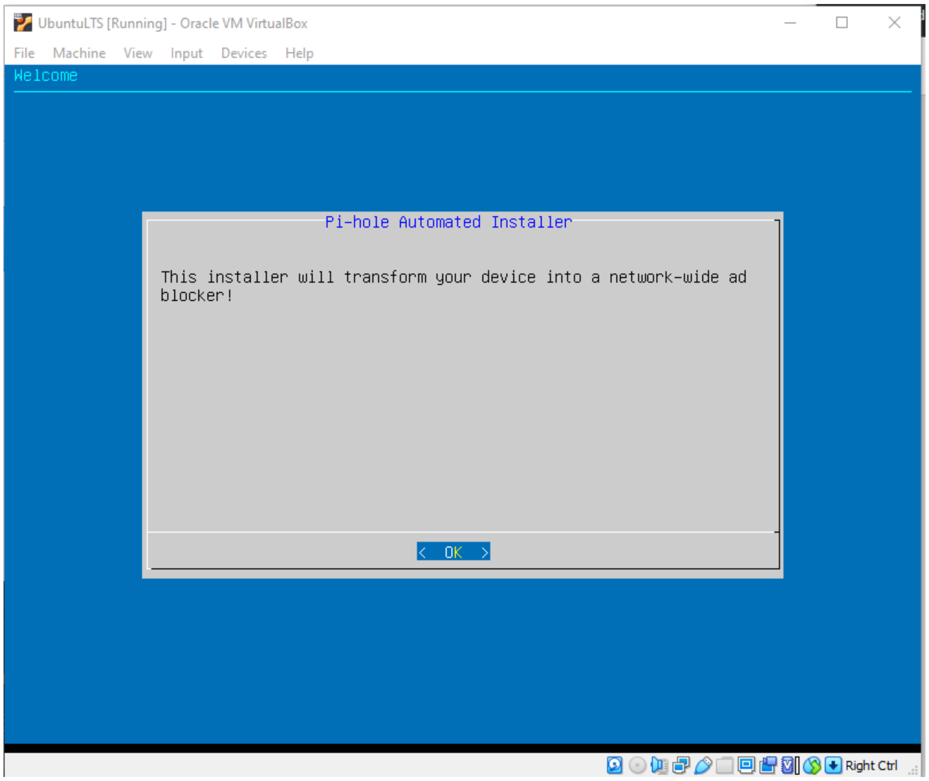


```
ashair@pihole:~$ ping 8.8.8.8
ping: connect: Network is unreachable
ashair@pihole:~$ sudo ip link set dev enp0s3 up
[sudo] password for ashair:
ashair@pihole:~$ sudo dhclient -v enp0s3
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:f3:86:cb
Sending on   LPF/enp0s3/08:00:27:f3:86:cb
Sending on   Socket/fallback
DHCPREQUEST for 192.168.2.240 on enp0s3 to 255.255.255.255 port 67 (xid=0x2b5f07d8)
ping 8.8.8DHCPACK of 192.168.2.240 from 192.168.2.1 (xid=0xd8075f2b)
bound to 192.168.2.240 -- renewal in 117870 seconds.
ashair@pihole:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=96.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=19.6 ms
^Z
[1]+  Stopped                 ping 8.8.8.8
ashair@pihole:~$ _
```

*Figure 9: Connecting server to the internet*

In figure 9 we can see that at the top of the console, we have tried to ping 8.8.8.8, which is the primary DNS for Google. We receive the message: ‘*Network is unreachable’*, however, after applying the two commands, we can successfully complete the pings. These two commands are effectively applying our I.P to the network interface.

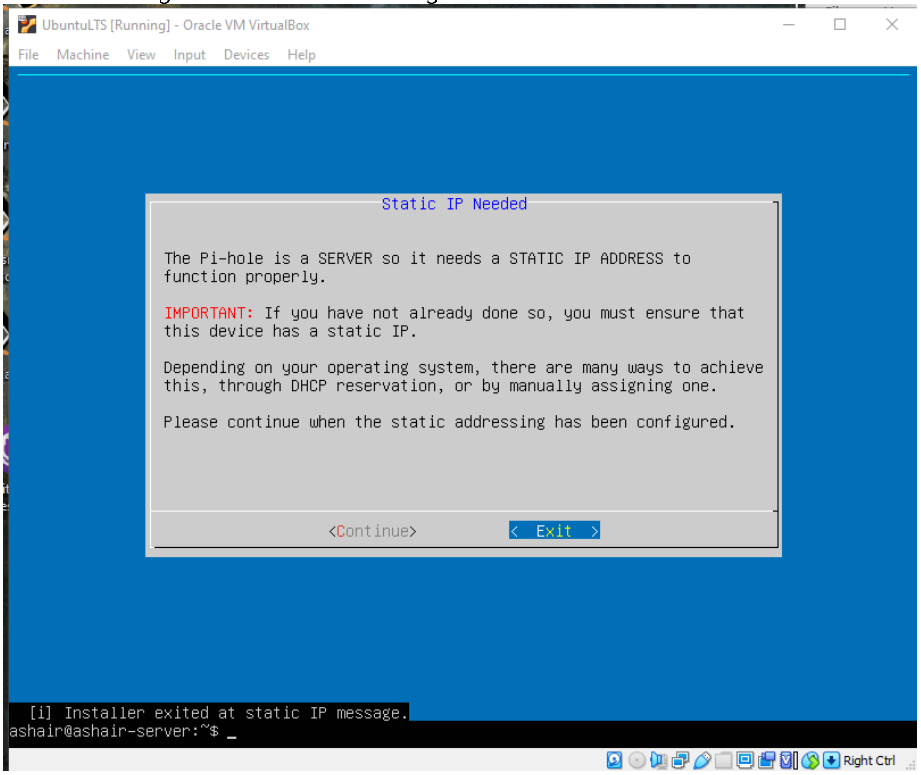
Now that we have installed Ubuntu and connected the server to the internet, we can now install Pi-hole with the command *‘curl -sSL https://install.pi-hole.net | bash’*. This launches the Pi-hole automated installer. All the defaults were selected for the installation. When asked which Upstream DNS Provider to use, Quad9 was selected. This decision will be elaborated on in the Discussion section of the report.


UbuntuLTS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Welcome
< OK >
Right Ctrl

Pi-hole Automated Installer

This installer will transform your device into a network-wide ad blocker!

*Figure 10: Welcome message to Pi-hole Automated Installer*


UbuntuLTS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
<Continue>
< Exit >
Right Ctrl

Static IP Needed

The Pi-hole is a SERVER so it needs a STATIC IP ADDRESS to function properly.

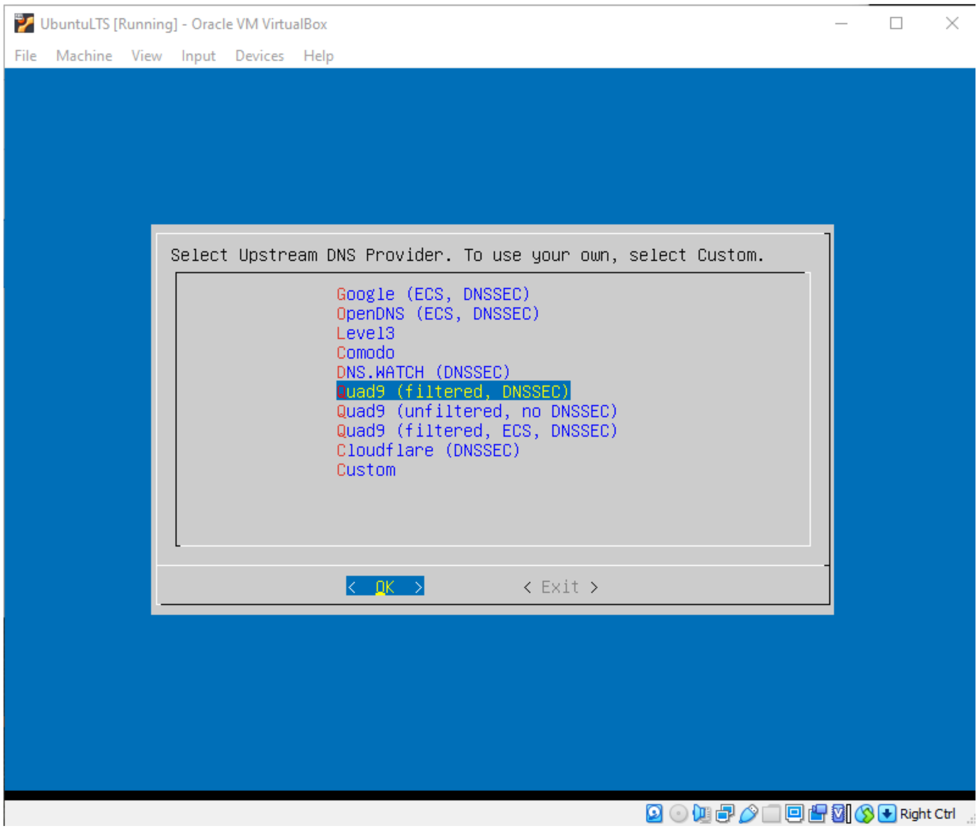
IMPORTANT: If you have not already done so, you must ensure that this device has a static IP.

Depending on your operating system, there are many ways to achieve this, through DHCP reservation, or by manually assigning one.

Please continue when the static addressing has been configured.

```
 [i] Installer exited at static IP message.
ashair@ashair-server:~$ _
```

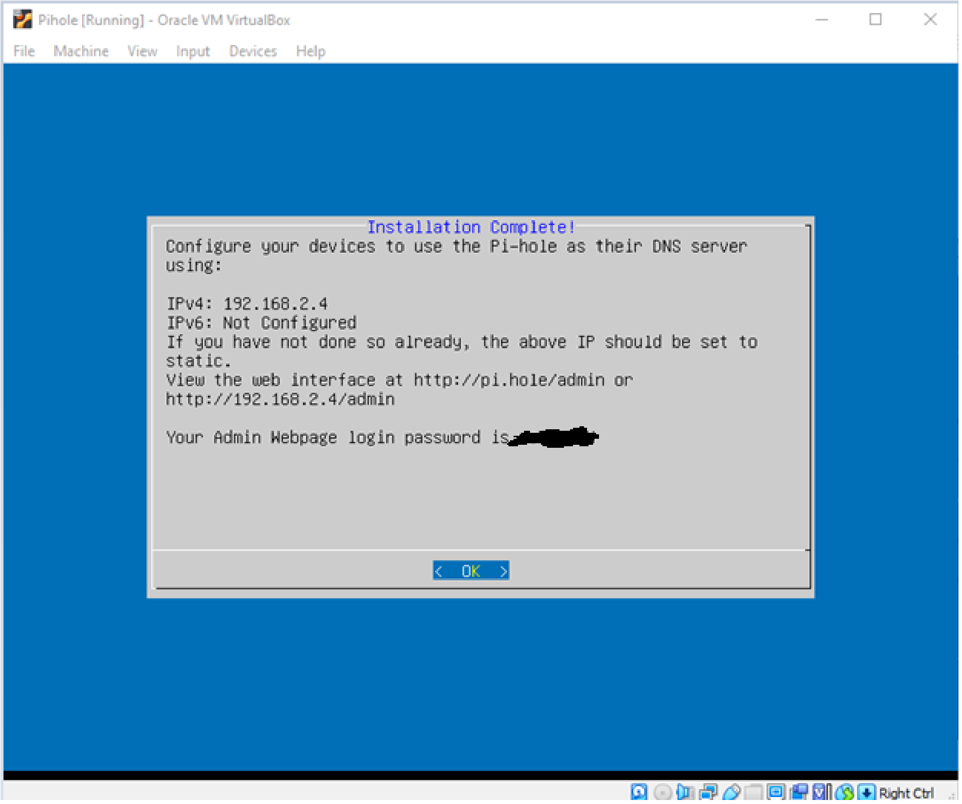
*Figure 11: Pi-hole requires a static IP address to function as a server.*



UbuntuLTS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
< OK >
< Exit >
Right Ctrl

```
Select Upstream DNS Provider. To use your own, select Custom.

                    Google (ECS, DNSSEC)
                    OpenDNS (ECS, DNSSEC)
                    Level3
                    Comodo
                    DNS.WATCH (DNSSEC)
                    Quad9 (filtered, DNSSEC)
                    Quad9 (unfiltered, no DNSSEC)
                    Quad9 (filtered, ECS, DNSSEC)
                    Cloudflare (DNSSEC)
                    Custom
```

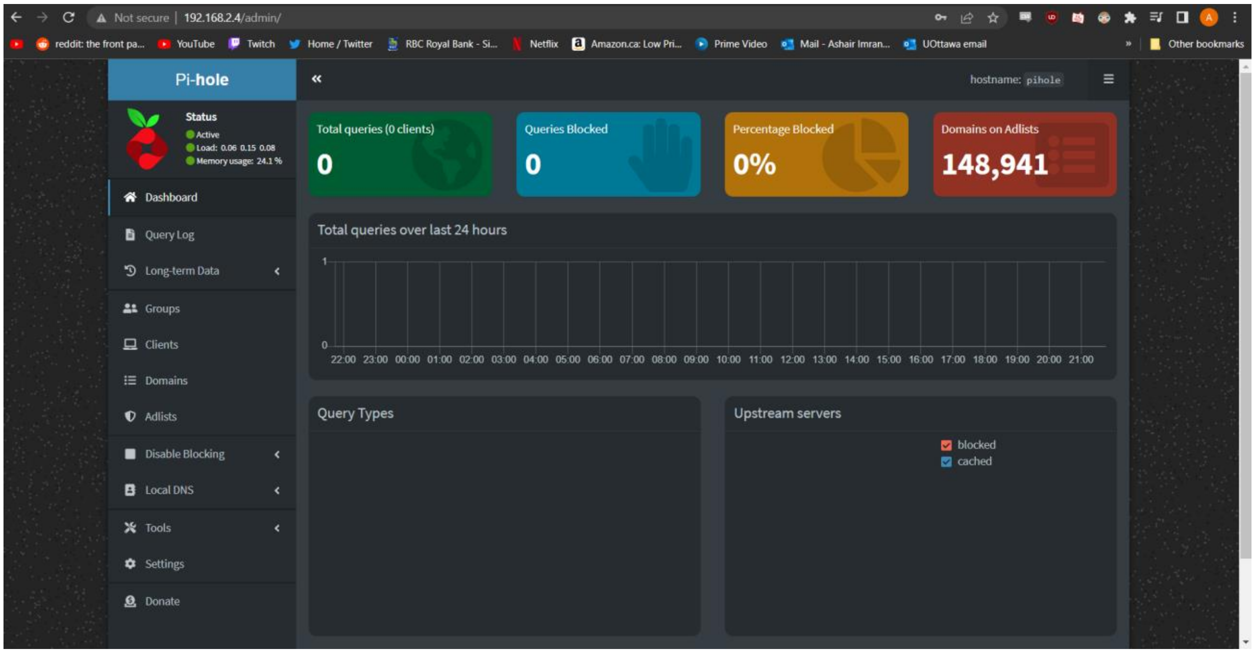
*Figure 12: Quad9 is selected as our Upstream DNS Provider*



Pihole [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
< OK >
Right Ctrl

```
                     Installation Complete!
Configure your devices to use the Pi-hole as their DNS server
using:

IPv4: 192.168.2.4
IPv6: Not Configured
If you have not done so already, the above IP should be set to
static.
View the web interface at http://pi.hole/admin or
http://192.168.2.4/admin

Your Admin Webpage login password is [redacted]
```

*Figure 13: The installation has been complete*



Not secure | 192.168.2.4/admin/

hostname: pihole

Status
Active
Load: 0.06 0.15 0.08
Memory usage: 24.1 %

Total queries (0 clients) 0

Queries Blocked 0

Percentage Blocked 0%

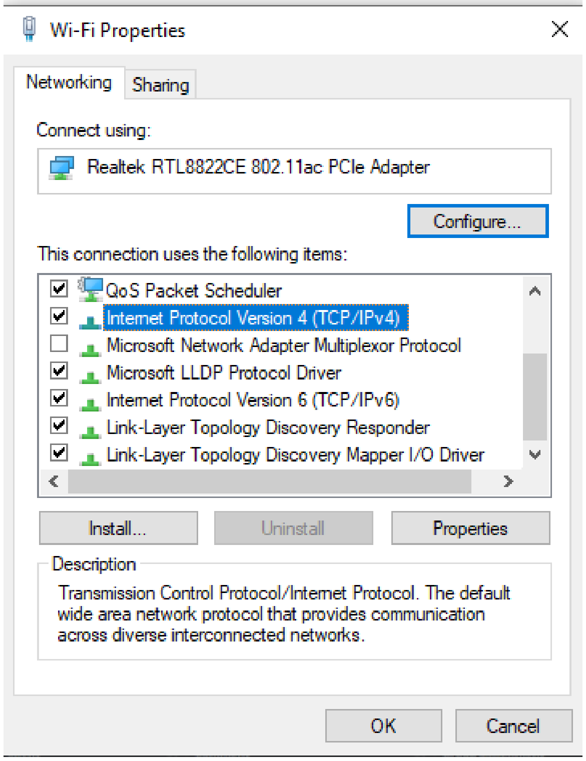
Domains on Adlists 148,941

*Figure 14: The admin interface can now be accessed on any web browser*

This concludes the installation Pi-hole on an Ubuntu server on a virtual machine. However, there are a few more configurations necessary so that we can use the Pi-hole as our local DNS when accessing the internet from our devices.

## 2.1 Single Device Configuration

The Pi-hole server that has been set up can be used on individual devices by changing the DNS server that the device uses on that device’s settings. For a windows PC, this is done by opening the control panel, going into the network settings, selecting your adapter that you are using, and going into the IPv4 properties, as shown in figure 15. Then you must apply the Pi-hole’s server address as the preferred DNS server for that adapter. This is shown in figure 16.



Wi-Fi Properties

Connect using:

Realtek RTL8822CE 802.11ac PCIe Adapter

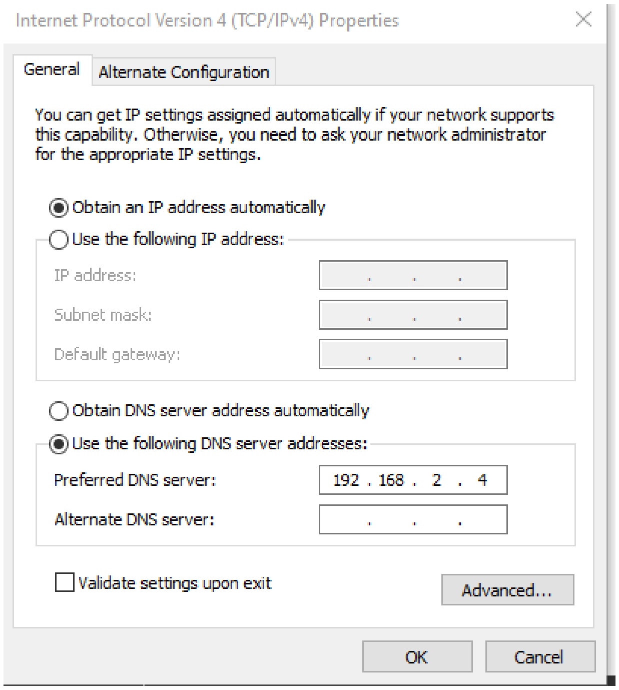
This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

*Figure 15: Selecting the IPv4 connection in the Wi-Fi properties menu*



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

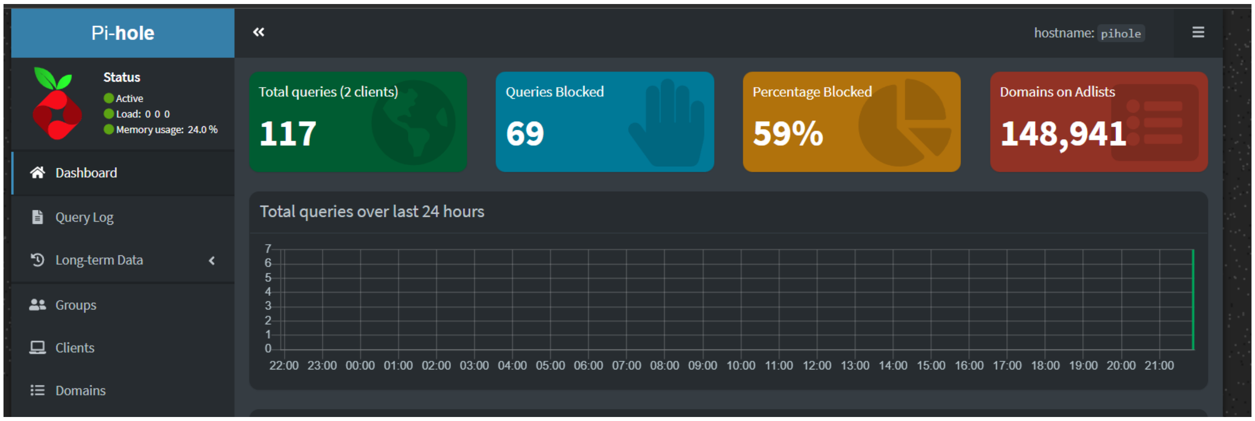
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 4

Alternate DNS server: . . .

□ Validate settings upon exit

*Figure 16: Manually applying the Pi-hole's address as the preferred DNS server*



Pi-hole

hostname: pihole

Status
Active
Load: 0 0 0
Memory usage: 24.0 %

Total queries (2 clients): 117

Queries Blocked: 69

Percentage Blocked: 59%

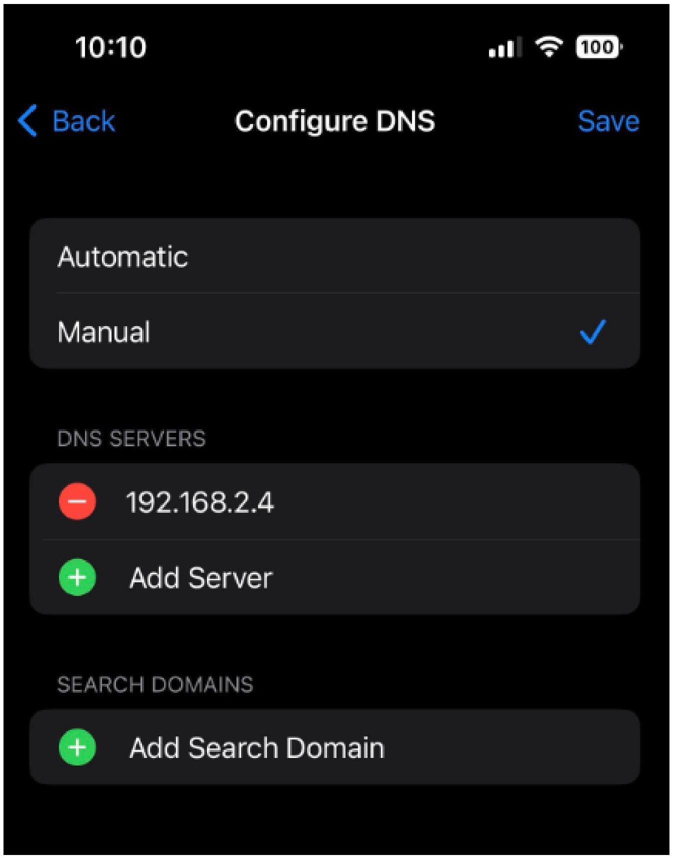
Domains on Adlists: 148,941

Total queries over last 24 hours

*Figure 17: The Pi-hole is now operating on a device*

Once the device has been configured to use the Pi-hole, the data will now be tracked on the admin interface, as shown in figure 17.

Each device has its own way of configuring it’s local DNS server. I also decided to use my Pi-hole server on my IOS phone. This was done by opening the Wi-Fi settings, selecting the information icon on your wi-fi network, and scrolling down to Configure DNS. The setting was set to manual and the DNS servers were replaced with the Pi-hole’s address, as shown in figure 18.



Configure DNS

Automatic

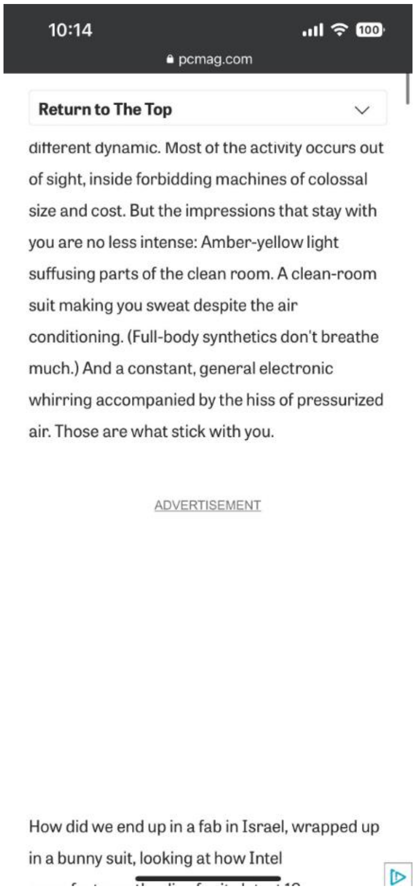
Manual ✓

DNS SERVERS

192.168.2.4

SEARCH DOMAINS

*Figure 18: Configuring iPhone to use Pi-hole*



different dynamic. Most of the activity occurs out of sight, inside forbidding machines of colossal size and cost. But the impressions that stay with you are no less intense: Amber-yellow light suffusing parts of the clean room. A clean-room suit making you sweat despite the air conditioning. (Full-body synthetics don't breathe much.) And a constant, general electronic whirring accompanied by the hiss of pressurized air. Those are what stick with you.

How did we end up in a fab in Israel, wrapped up in a bunny suit, looking at how Intel

*Figure 19: Pi-hole blocking advertisements on iPhone*

## 2.1 Router Configuration

It is also possible to configure your router to use the Pi-hole as it’s local DNS server. This would theoretically allow every device connected to the network to utilize the Pi-hole to block ad-serving domains.

**Disclaimer**: Unfortunately, under my current circumstances in student housing, I am not allowed to access the router gateway and modify any settings. I also did not want to use Pi-hole’s DHCP server settings as I reside with many people who all use the same network. However, I have access to the network gateway of my parent’s home (in Mississauga) as it is a Rogers network that uses the Ignite app which I conveniently had installed on my phone as I have used it before for port-forwarding. I will provide screenshots of the gateway settings from the app that would be necessary to theoretically use Pi-hole as the DNS server of choice. None of these settings were applied in practice.

The procedure to configure your router to use Pi-hole will vary with each ISP and router, but the basic procedure is similar. First you must log in to your network's gateway. I will be using Rogers for the sake of this project. Rogers no longer uses a gateway login on your web browser to access advanced settings. Instead, it is requirement to download the Rogers Ignite app to modify advanced router settings. Once you have access to your router's settings, navigate to the DNS server settings. Just like in the single device configuration, you must edit the DNS server of choice to the I.P address of your Pi-hole.

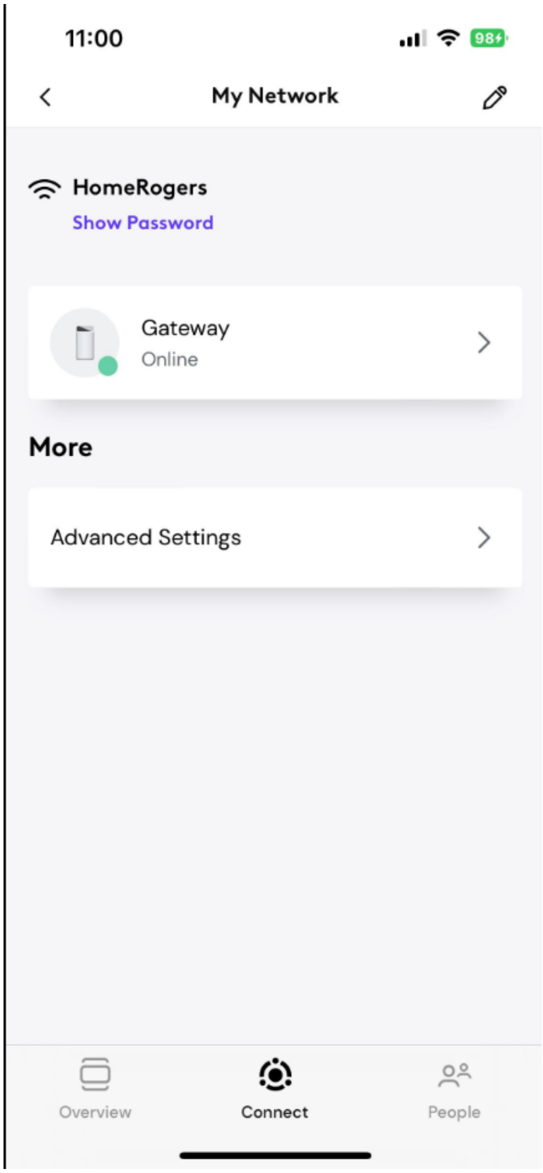
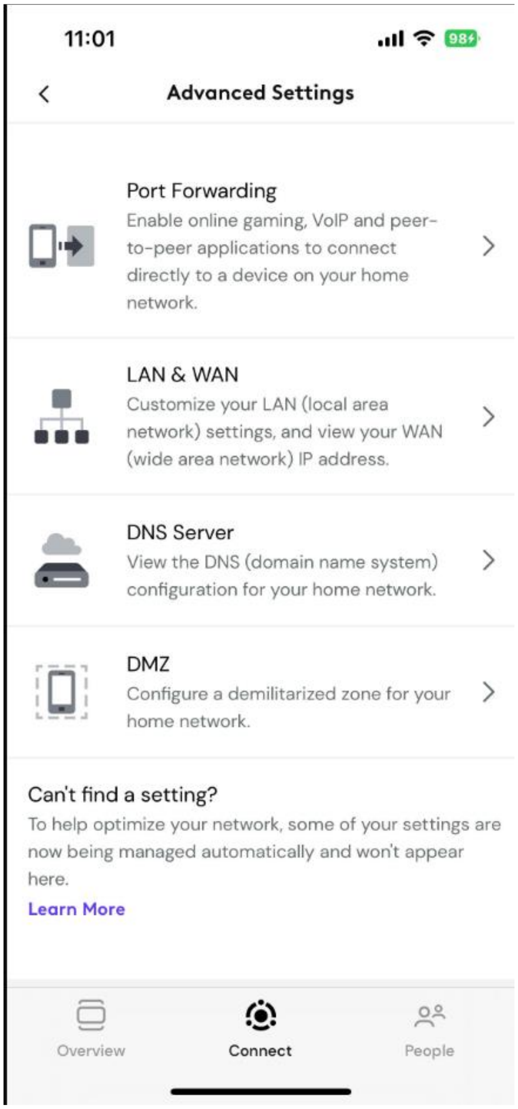


*Figure 20: Rogers Ignite app, home menu to log into the Gateway*



11:01

Advanced Settings

Port Forwarding

Enable online gaming, VoIP and peer-to-peer applications to connect directly to a device on your home network.

LAN & WAN

Customize your LAN (local area network) settings, and view your WAN (wide area network) IP address.

DNS Server

View the DNS (domain name system) configuration for your home network.

DMZ

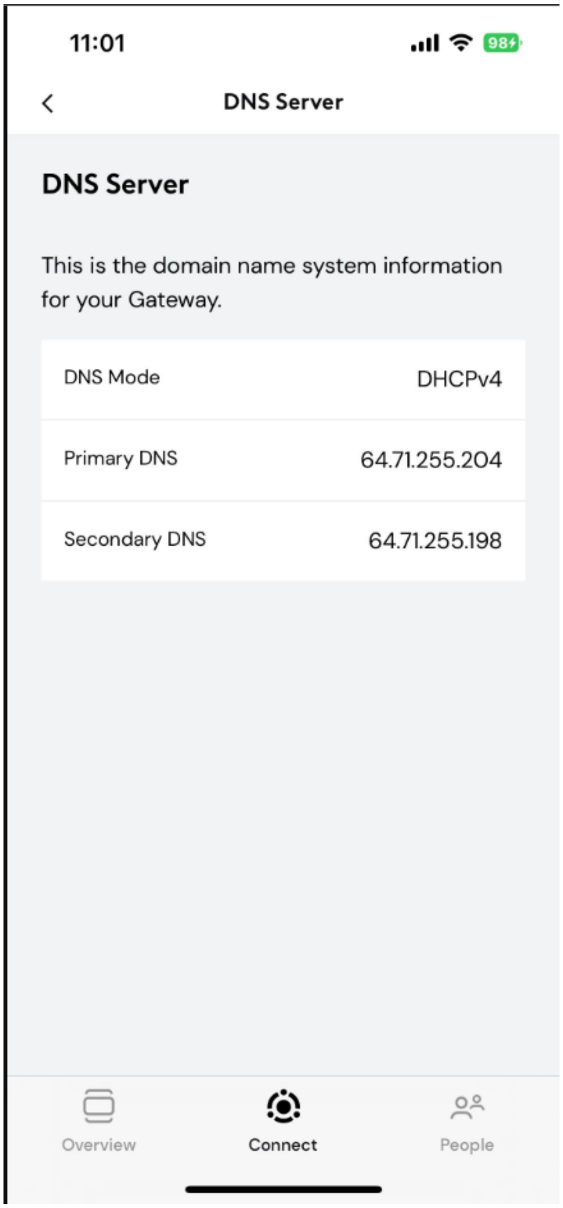
Configure a demilitarized zone for your home network.

Can't find a setting?

To help optimize your network, some of your settings are now being managed automatically and won't appear here.

Learn More

*Figure 21: Advanced Settings for the gateway. Here you can modify various aspects of the router including port forwarding and DNS server configuration*



DNS Server

This is the domain name system information for your Gateway.

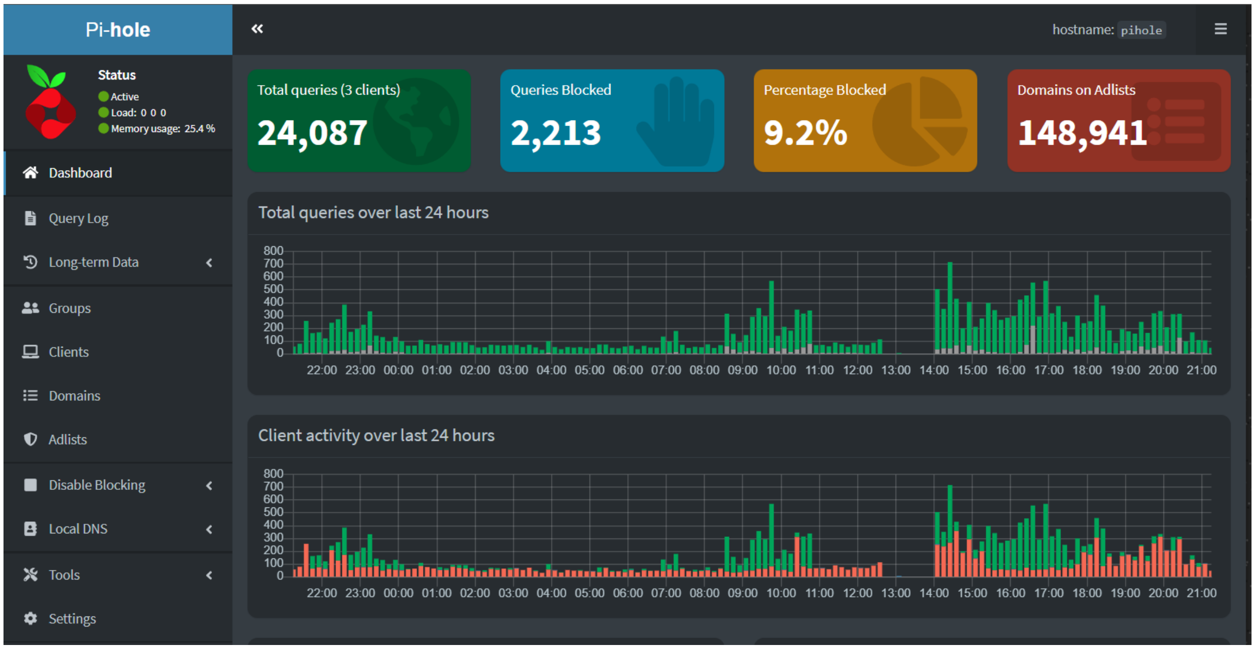
|  |  |
|---|---|
| DNS Mode | DHCPv4 |
| Primary DNS | 64.71.255.204 |
| Secondary DNS | 64.71.255.198 |

*Figure 22: The DNS server settings to be modified.*

The setting to be modified can be seen in figure 22. The default primary DNS should be changed from the default to the address of your Pi-hole. In this case, I would modify it to be 192.168.2.4 so that the entire router now routes all DNS queries form every device connected to it, through the Pi-hole.

## 3.0 Results

This section will cover the obtained results from the Pi-hole over the course of ~48 hours



hostname: pihole

Status
● Active
● Load: 0 0 0
● Memory usage: 25.4 %

Total queries (3 clients) 24,087

Queries Blocked 2,213

Percentage Blocked 9.2%

Domains on Adlists 148,941

*Figure 23: The Dashboard results*

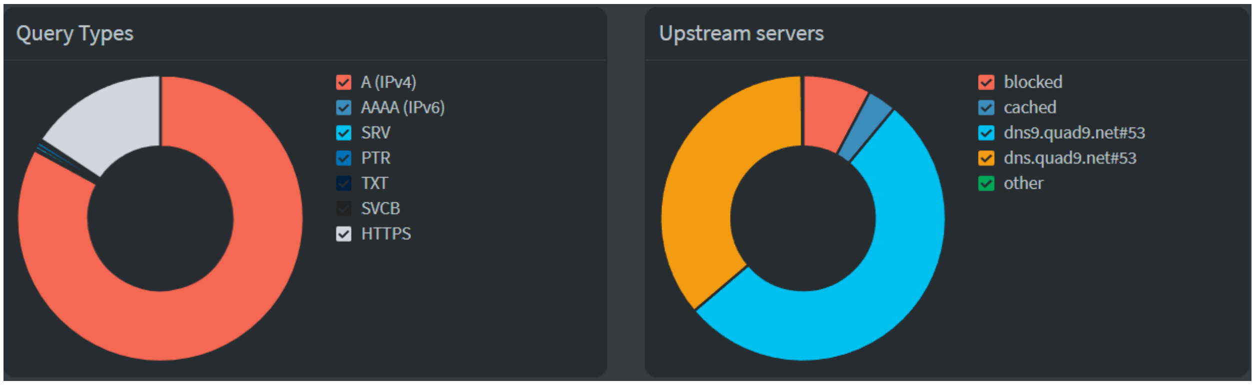


*Figure 24: Query Types and Upstream servers*

| Query Types | Percentage of Total Queries |
|---|---|
| A (IPv4) | 82.9% |
| HTTPS | 15.7% |
| AAAA (IPv6) | 0.2% |
| SRV | 0.4% |
| PTR | 0.5% |
| SVRCB | 0.3% |

*Table 1: Percentage of total queries for each query type*

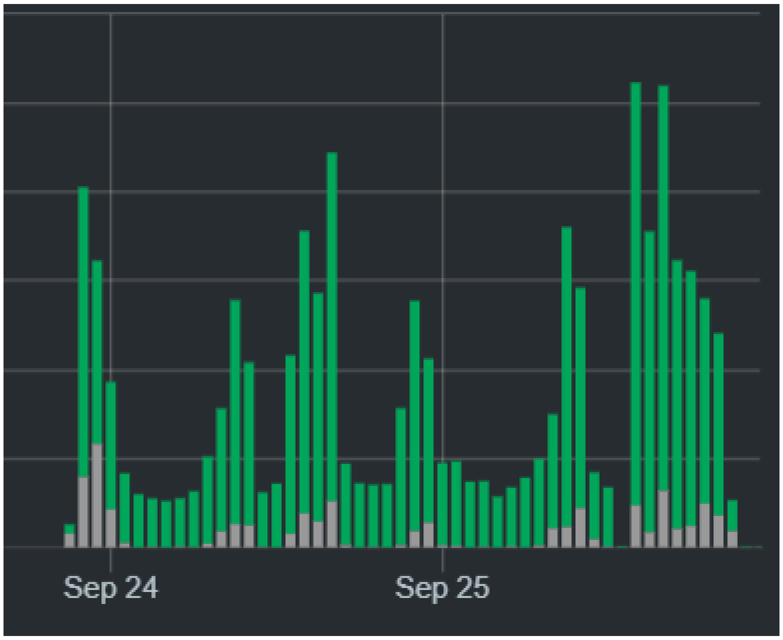
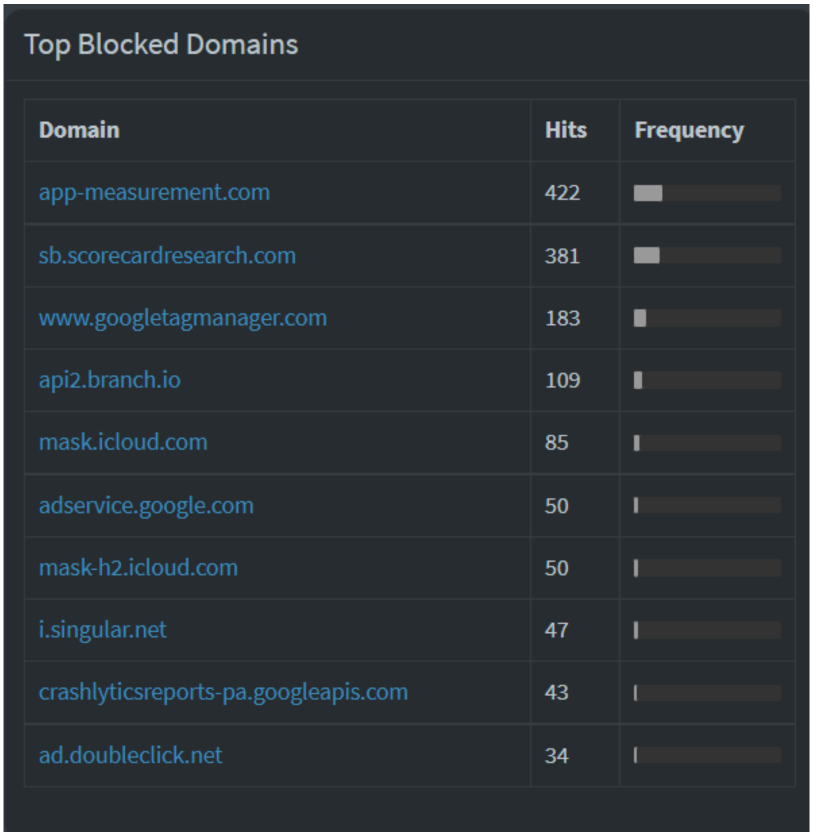


*Figure 25: Long term chart for all queries over 48 hours*



Top Blocked Domains

| Domain | Hits | Frequency |
|---|---|---|
| app-measurement.com | 422 | ▬ |
| sb.scorecardresearch.com | 381 | ▬ |
| www.googletagmanager.com | 183 | ▮ |
| api2.branch.io | 109 | ▮ |
| mask.icloud.com | 85 | ▮ |
| adservice.google.com | 50 | ▮ |
| mask-h2.icloud.com | 50 | ▮ |
| i.singular.net | 47 | ▮ |
| crashlyticsreports-pa.googleapis.com | 43 | ▮ |
| ad.doubleclick.net | 34 | ▮ |

*Table 2: Top blocked domains*

## 3.0 Discussion

The results from this project show many interesting insights into DNS queries and ad-blocking that I have never considered. Firstly, the sheer amount of DNS queries is staggering. 24,087 queries sent by two devices, which were used mutually exclusively. However, this number may be inflated, and thus the percentage blocked amount, of 9.2%, may be underselling the situation.

One primary reason for the large number of queries and small number of blocked queries is that the device connected to the Pi-hole, is also running the Pi-hole. This device must stay online throughout the night-time and the device had quite a few tabs open and applications running throughout the night. It can be seen from the above figures that there are many queries being sent during idle time, none of which are being blocked. The blocked queries only appear when the device is in active use. Another interesting reason for the large number of queries is that the biggest permitted domain, by far, was actually a chrome extension that retrieves emotes for the website Twitch. This extension alone generated 1,916 permitted queries. Finally, the websites that I personally use the most, serve ads via their own domains. As discussed earlier, websites such as YouTube and Reddit, will serve ads from unblockable domains. If Pi-hole were to block the domain serving the ads, they would also be blocking the domain that is serving the content.

One important aspect to discuss is that Quad9 was selected as our DNS upstream provider of choice. This is because Quad9 is dedicated to security and is known as the most secure DNS resolver. Quad9 is publicly funded and is shown to be 96% effective against blocked domains, 100% effective against phishing domains, and 92% effective against malware domains (Malicious Site Filters on DNS 2020). These numbers are far superior to it's contemporaries. Security is a very important aspect in all implementations of software and networking, so it is very important to consider it.

Overall, the results were quite eye-opening. If I were to do this experiment again. I would make sure to remove all of the chrome extensions and to close as many applications as possible during the night. Doing this would result in more practical data.

## 3.1 Problems Encountered

There were many problems encountered during this project. Most of these problems were encountered during the installation phase. This project was started with zero experience in linux, and a lot of research and troubleshooting was involved to run the Ubuntu server on the virtual machine. The biggest issue was figuring out how to set the server with a static I.P. Many of the resources that were used (All listed below in the Resources section) had outdated information or did not apply to my situation. I had to take away a little bit from each source and figure out the solutions by myself.

Another issue that I encountered, as mentioned during the installation phase was a bug that was encountered that prevented Ubuntu installation. This bug was caused by the network adapter being enabled, even though I was previously able to install Ubuntu just fine earlier that day.

Many inconsistent bugs and issues were encountered throughout the installation phase of this project. Although the installation may seem simple, it too many hours of troubleshooting to finally install Pi-hole on the virtual machine.

## 4.0 Conclusion

Overall, the project was a success. Pi-hole is a fantastic service that will block ad-serving domains and provide you with a more secure and clean browsing experience. Pi-hole can also be applied to your entire network to prevent ads from reaching every device on that network. However, Pi-hole is not a perfect solution and should be combined with other ad-blocking extensions to truly create an ad-free experience. The Pi-hole admin interface has many different settings and provides lots of data about the DNS queries made by your device. The data is eye-opening, and I would recommend everybody use Pi-hole to enhance their internet browsing experience.

## Resources and References

Pi-Hole Documentation
https://docs.pi-hole.net/

What is a DNS Server by Cloudflare
https://www.cloudflare.com/en-ca/learning/dns/what-is-a-dns-server/

What is DNS by Amazon
https://aws.amazon.com/route53/what-is-dns/

Pi-Hole DCHP FAQ
https://discourse.pi-hole.net/t/how-do-i-use-pi-holes-built-in-dhcp-server-and-why-would-i-want-to/3026

Malicious Site Filters on DNS in 2020
https://www.skadligkod.se/general-security/phishing/malicious-site-filters-on-dns-in-2020/

Linux Included: How to Install Pi-hole on Ubuntu
https://linuxincluded.com/install-pi-hole-on-ubuntu/

Ubuntu Tutorial: How to run Ubuntu desktop on a virtual machine
https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox#1-overview

How to setup static-ip on a VirtualBox Ubuntu Server
https://circuitcloud.in/setup-static-ip-on-virtualbox-ubuntu-server/

How to setup a Pi-Hole: Whole Home Ad-Blocking
https://www.youtube.com/watch?v=Ausz2j4jK5o

Superuser Query
https://superuser.com/questions/1353130/vm-got-10-0-x-x-address-instead-of-192-168-x-x-address

Quad9
https://www.quad9.net/

Vitux: How to configure a netplan on Ubuntu
https://vitux.com/how-to-configure-networking-with-netplan-on-ubuntu/