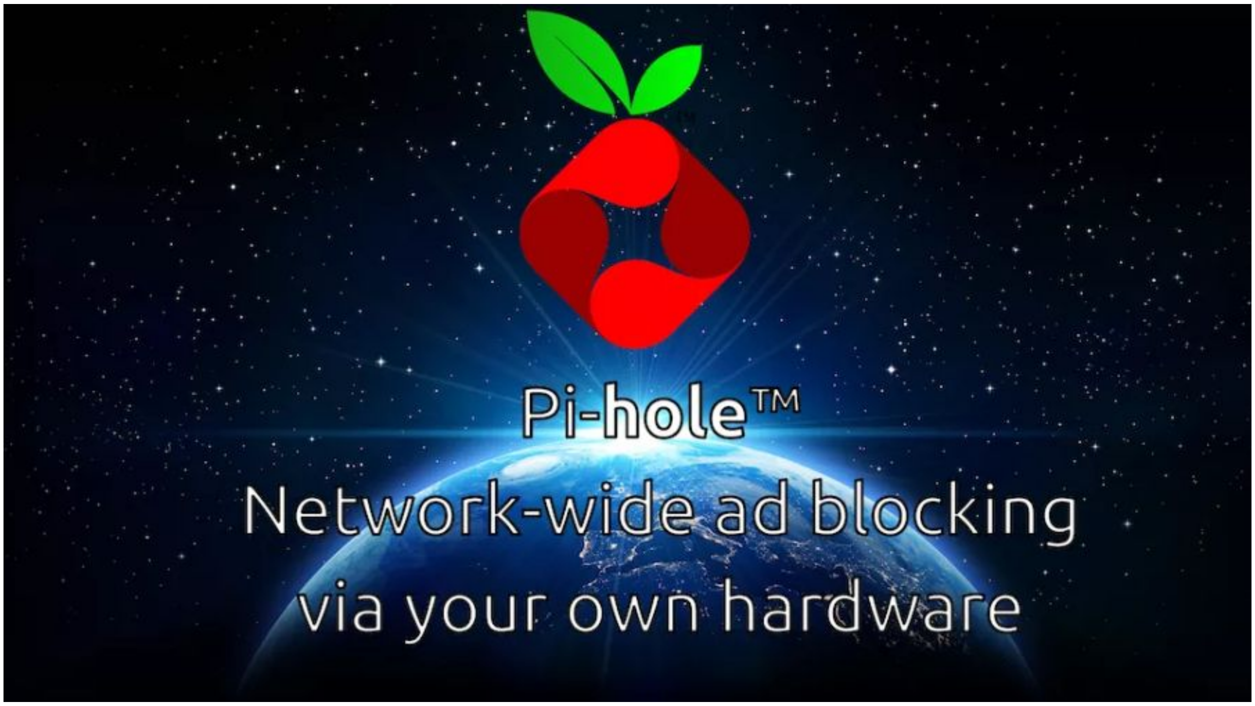
Raspberry Pi-Hole



Bilel Ben Romdhane
Landon Ross
Tanya Wong
Harneik Dhanota

Executive Summary

Our project is on a software called Pi-Hole. Within this project we cover the core concepts of the Pi-Hole, how the Pi-Hole works, how to install it for your own use, our Wireshark evidence, and the references we used. Pi-Hole is a Network-level blocking server that allows you to block ads in non-traditional placed such as mobile apps and smart TVs, regardless of hardware or OS. The Pi-Hole software is ran off of a Raspberry Pi. Through the Raspberry Pi we installed RaspBian (the operating system). After we installed the OS we were able to add the Pi-Hole.

We undertook this project to show how you can block ads on any device, even in apps, because the Pi-Hole works at the DNS level. The Pi-hole software acts as a forwarding DNS server,which means if it doesn't know where a domain is, it has to forward your query to another server that does. Through the installation of the Pi-hole, you set up where the ad-serving domains are so that it doesn't forward those requests to you. We think it's important to block ad traffic because its intrusive and slows down your browsing experience. Since ads are blocked before they are downloaded, your network will have better performance. It also reduces the cellular data usage because you can pair the Pi-hole with a VPN so you can take your adblocker on the go.

After installing and configuring the Pi-hole on the Raspberry Pi, we found that it is very successful in blocking advertisements throughout various websites. Blocking advertisements expedited our overall browsing experience because it didn't have to download those pesky advertisements. Websites look a lot simpler and cleaner without pop-ups and gifs of advertisements, which also helps business get less distracted and improve productivity.

Core Concepts

Pi-Hole can be used for various reasons. It can be used at homes, schools, businesses, etc. Since it is a network-level blocking server that allows you to block ads. It can benefit any who uses Pi-Hole after it is successfully installed.

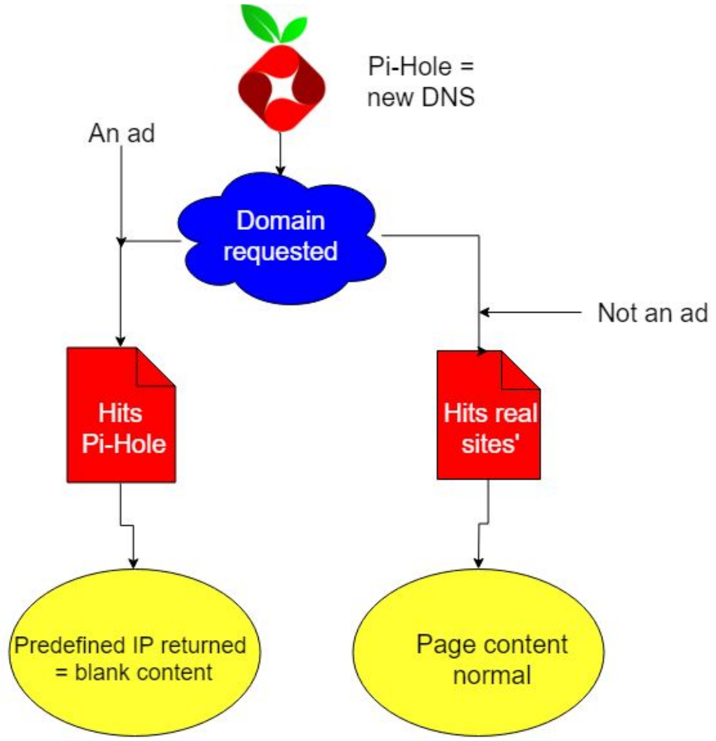
Another way to view Pi-Hole is that it is a DNS filter, or a phone book, essentially Pi-Hole will take all requests and check whether the IP address returned is the actual page versus an ad domain. For example, say we type in youtube.com. Without using Pi-Hole, the DNS server matches the name of the IP and results the result to the browser, along with advertisements that are embedded on that page. However, if Pi-Hole is implemented, the request will go through the Pi-Hole DNS server. While the browser is being told where to fetch the pages, the advertisements' IP address is also trying to be fetched. But with Pi-Hole, it sees that the IP address is apart of the ad domain blacklist, so instead of the ad being returned, a blank spot will show up instead. This means the main content of the page loads just fine, but the advertisements are never shown.

This can be helpful in a home environment because unlike ad blocking extensions, Pi-Hole is a bit better. Better might be stretching it a little bit, but with how Pi-Hole is set up and works, it can be effective on improving browsing experience and amount of data used. The way ad blocking extensions works is that it downloads the ad IP, but it just hides the ad from the user's point of view. However, the keyword is that it still downloads, whereas Pi-Hole works at the DNS lever and stops the download. Also with Pi-Hole, parents will not need to worry about ads showing on any device, because unlike ad blocking it belongs to a browser, but Pi-Hole is linked to the router so that all devices connected will be able to reap the benefits.

The same can be said for businesses since it will improve the speed and the amount of data used. However, another effective use of Pi-Hole is that employees will be less distracted on websites. It is inevitable that some companies rely on going on the Internet for their company, but will the way cookies work. It is easy for employees to be distracted since ads similar to what they are looking at will pop up and they may want to click into the ads. But with Pi-Hole all ads are blocked so they will not see any distractions and only the main content of the page they are on.

Some jargon that may be mentioned for Pi-Hole is DNS, DHCP, static IP, IPv4, and IPv6. DNS stands for Domain Name System, basically it is a database that contains IP addresses that identifies its' respective website. DHCP stands for Dynamic Host Configuration Protocol, it is a network protocol that automatically assigns IP addresses to a computer or any device that is connected to the Internet. A static IP address is an IP address that is manually configured for a device, the keyword is static which means it does not change. IPv4 and IPv6 is the same, the only difference is that v6 is a successor of v4 since it uses 128-bit addresses because v4 was running out of Internet addresses. IP, or Internet Protocol, is used to assign an unique IP address to a device when it is trying to access the Internet.

The diagram below is an illustration of how Pi-Hole works:



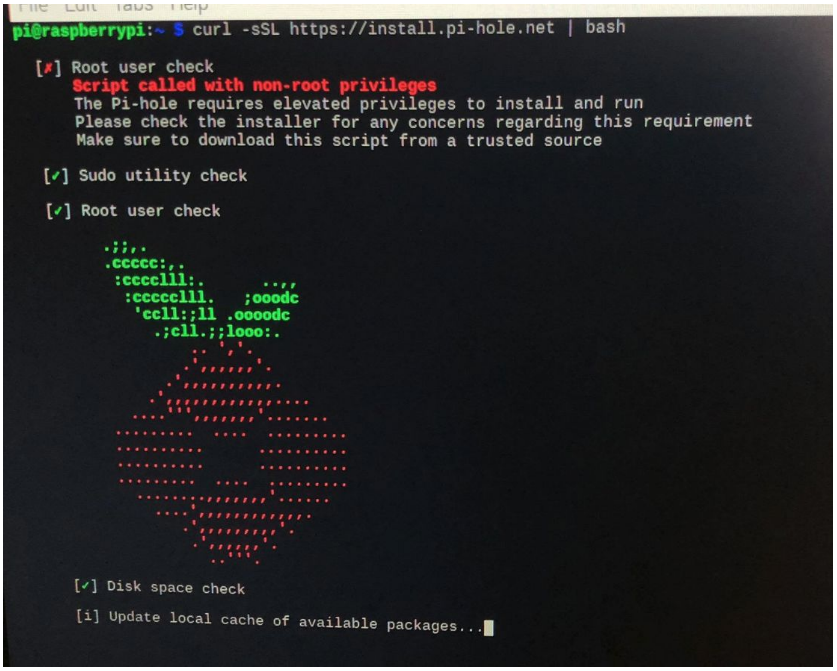
The diagram can be roughly explained like this:

1. your PC: I want to access something on whatever.com
2. your PC: Do I already know where that is?
   Yes -> start the connection to the known IP address;
   No -> your PC now asks its DNS server (Pi-Hole) where whatever.com is.
3. DNS server: Is that domain in the blacklist?
   Yes -> respond with Pi-Hole's IP address.
   No -> continue
4. DNS server: Do I know where whatever.com is already?
   Yes -> respond with IP address;
   No -> continue
5. DNS server now asks its own upstream DNS server for the answer.
6. DNS server (Pi-Hole) responds to your PC with the IP address it received in the previous step.

How to install Pi-Hole tutorial

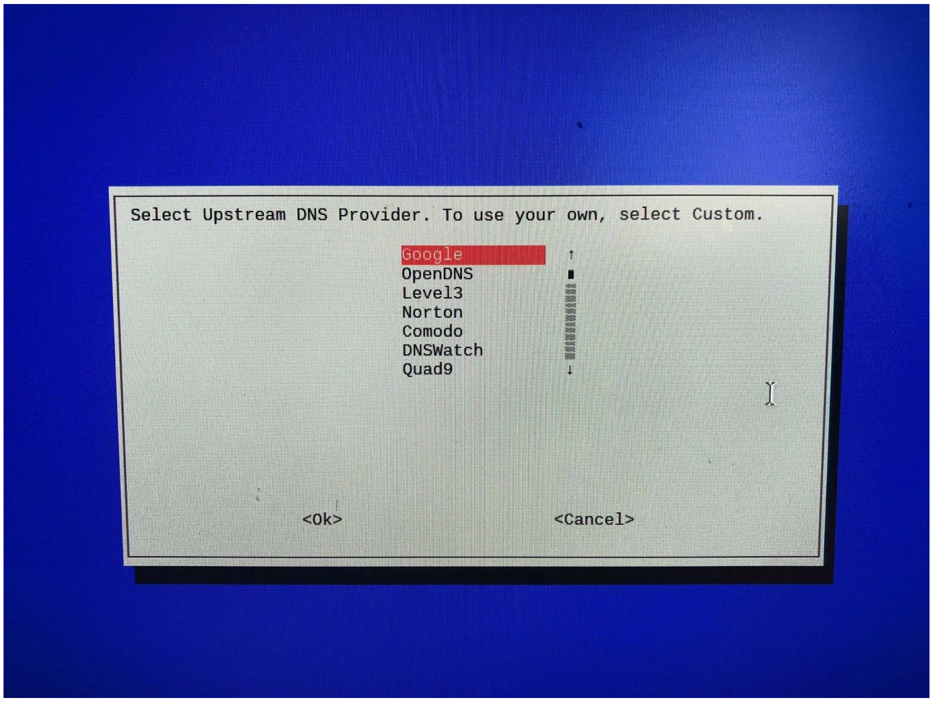
Step 1: Download the Raspbian OS from raspberrypi.org/downloads and use an image burning program such as Etcher to flash the OS to a Micro SD card, and then insert SD card into your raspberry pi device

Step 2: Plug raspberry pi into display with keyboard and mouse. Open terminal and run the following command without quotation marks “curl -sSL https://install.pi-hole.net | bash”. The following should ensue:



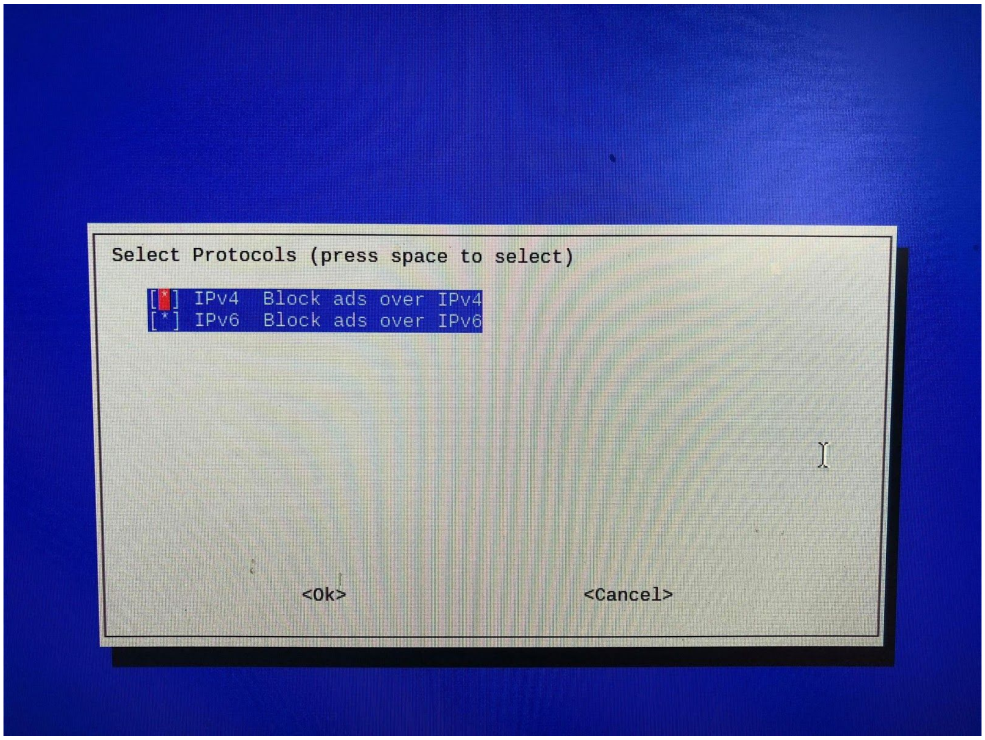
```
pi@raspberrypi:~ $ curl -sSL https://install.pi-hole.net | bash

  [✗] Root user check
      Script called with non-root privileges
      The Pi-hole requires elevated privileges to install and run
      Please check the installer for any concerns regarding this requirement
      Make sure to download this script from a trusted source

  [✓] Sudo utility check

  [✓] Root user check

        .;;,.
        .ccccc:,.
         :cccclll:.      ..,,
          :ccccclll.   ;ooodc
           'ccll:;ll .oooodc
             .;cll.;;looo:.

  [✓] Disk space check

  [i] Update local cache of available packages...
```

Step 3: You will be met with the installer prompt. It will inform you that the Pi-Hole is a server so it must have a static IP address to work correctly. You will then have to select to use your current home network DHCP (Dynamic host configuration protocol) or to use other settings. In our case, we defaulted to use Googles DNS settings.



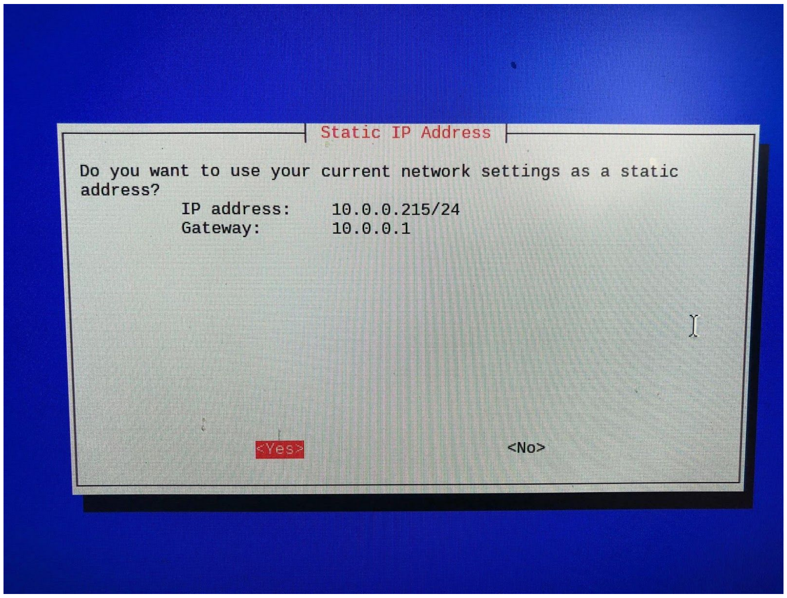
```
Select Upstream DNS Provider. To use your own, select Custom.

                    Google
                    OpenDNS
                    Level3
                    Norton
                    Comodo
                    DNSWatch
                    Quad9

          <Ok>                      <Cancel>
```

Step 4: The installation will ask if you want to block Ads on your home network via IPv4, or IPv6. You can also select both if your network supports IPv6.



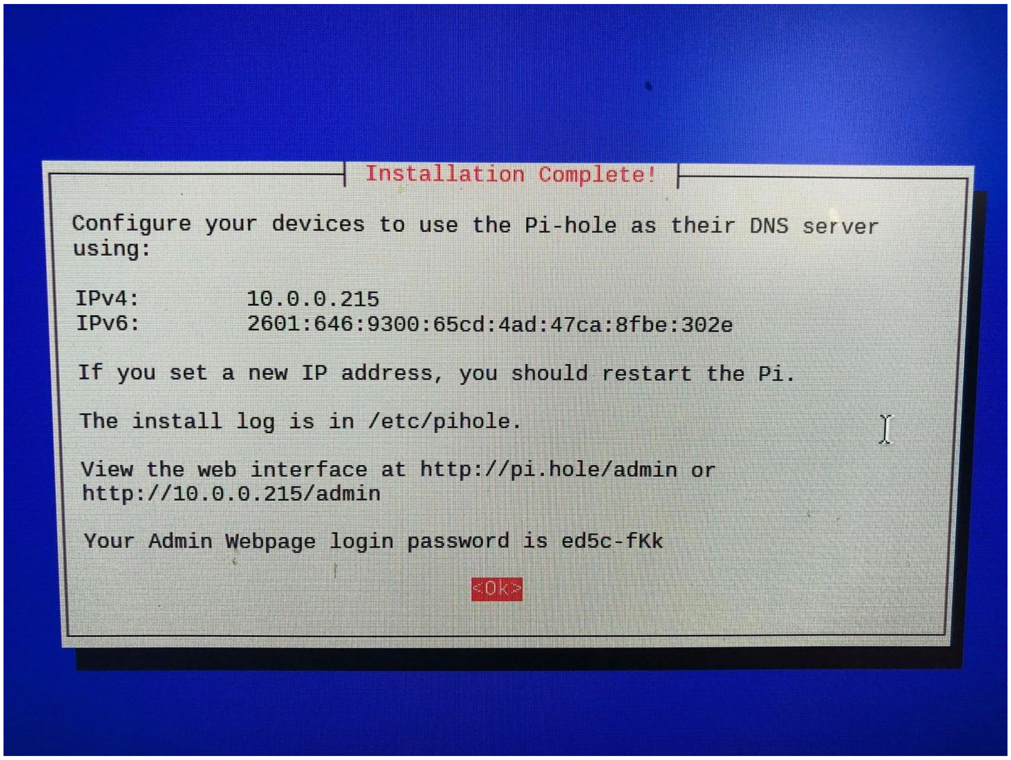
```
Select Protocols (press space to select)

   [*] IPv4  Block ads over IPv4
   [*] IPv6  Block ads over IPv6

          <Ok>                      <Cancel>
```

Step 5: The installation will ask if you want to use your Pi's current network settings as the static address. Select yes. The following screen will ask you if you want to install the Web Admin interface. Select yes as that is recommended as well.



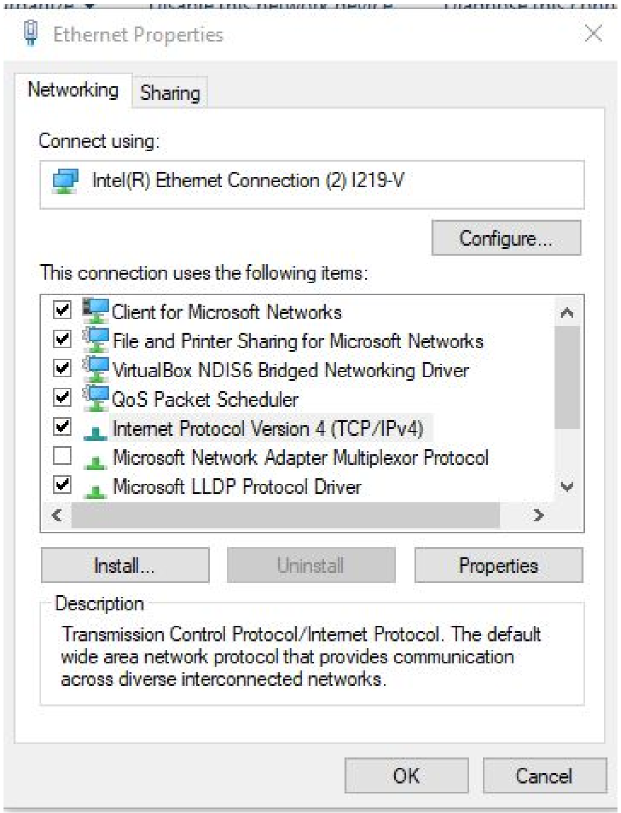
```
Do you want to use your current network settings as a static
address?
          IP address:    10.0.0.215/24
          Gateway:       10.0.0.1
```

Step 6: The installation should be complete now. It will give you the information needed to login to the admin web interface via the Pi-Hole's IP address.



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

IPv4:        10.0.0.215
IPv6:        2601:646:9300:65cd:4ad:47ca:8fbe:302e

If you set a new IP address, you should restart the Pi.

The install log is in /etc/pihole.

View the web interface at http://pi.hole/admin or
http://10.0.0.215/admin

Your Admin Webpage login password is ed5c-fKk
```

Step 7: Finally, we must configure our device such as desktop or laptop to use the Pi-Hole as their DNS server. This will vary depending on operating systems, in our case, we used windows 10. Go to control panel -> Network and Internet -> Network and Sharing Center -> Change adapter settings, and right click on the wireless or wired adapter you're using. Click properties, Click on IPv4, then properties again, and under DNS settings use the pihole IP address just as shown. And you're done!



Ethernet Properties

Networking | Sharing

Connect using:

Intel(R) Ethernet Connection (2) I219-V

Configure...

This connection uses the following items:

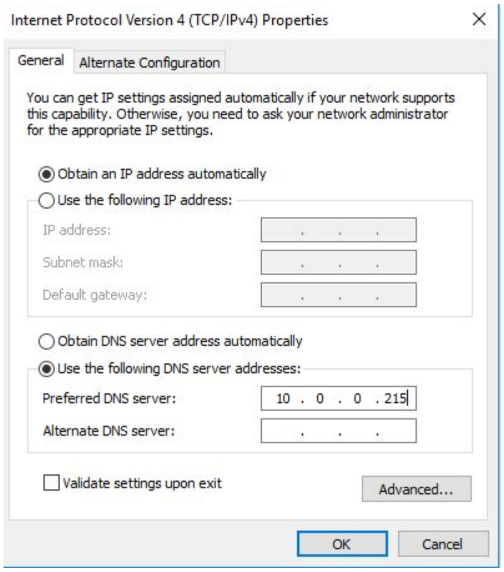
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Install... | Uninstall | Properties

Description

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

OK | Cancel



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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: 10 . 0 . 0 . 215

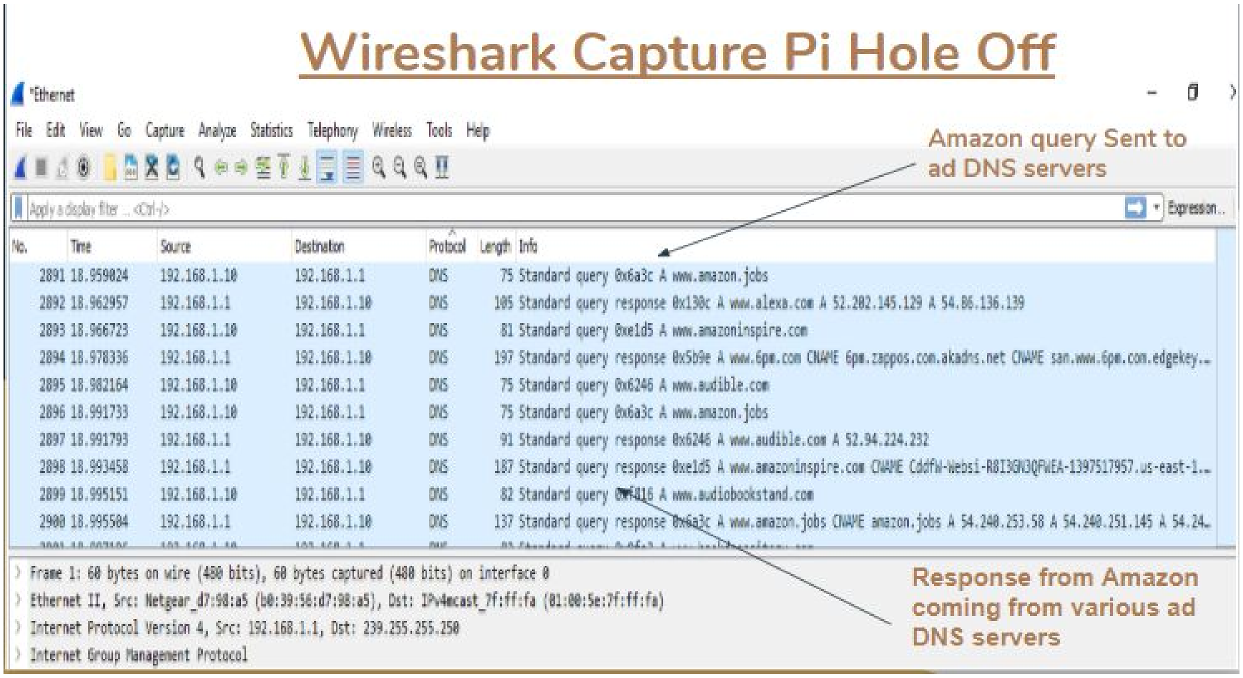
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK | Cancel

Wireshark Evidence



Wireshark Capture Pi Hole Off

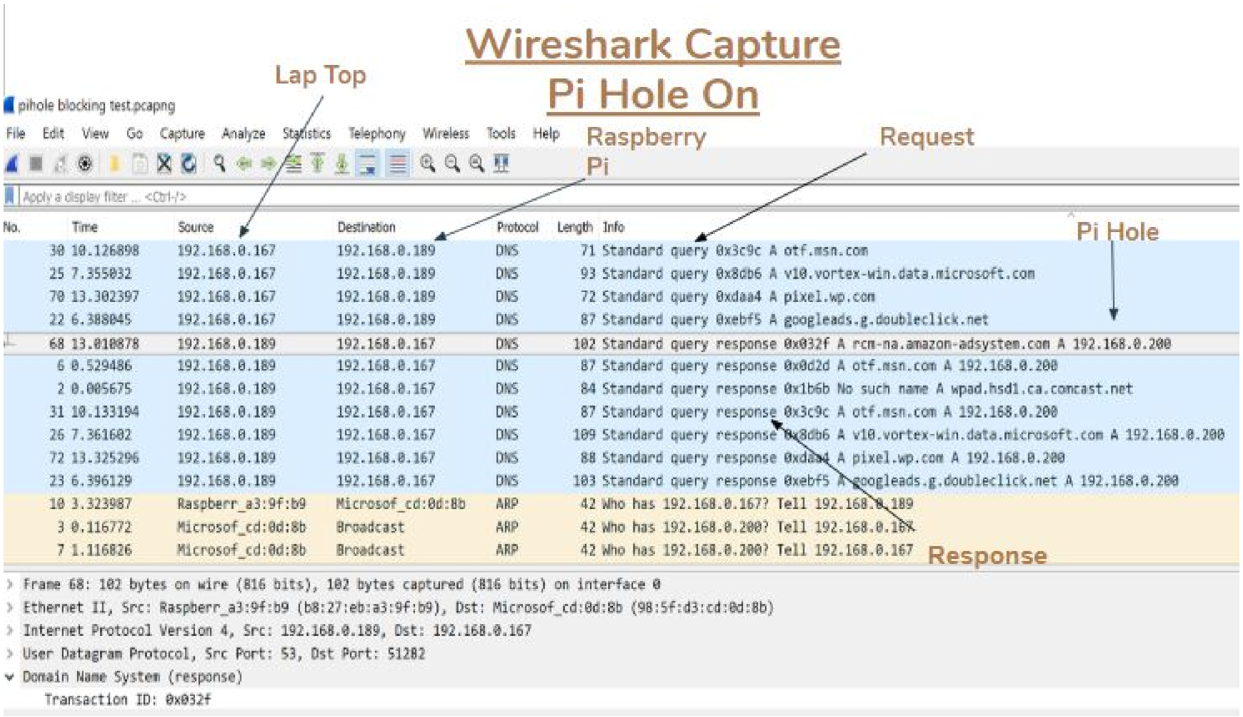
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

Amazon query Sent to ad DNS servers

```
No.   Time       Source        Destination   Protocol Length Info
 2891 18.959024  192.168.1.10  192.168.1.1   DNS       75 Standard query 0x6a3c A www.amazon.jobs
 2892 18.962957  192.168.1.1   192.168.1.10  DNS      105 Standard query response 0x130c A www.alexa.com A 52.202.145.129 A 54.86.136.139
 2893 18.966723  192.168.1.10  192.168.1.1   DNS       81 Standard query 0xe1d5 A www.amazoninspire.com
 2894 18.978336  192.168.1.1   192.168.1.10  DNS      197 Standard query response 0x5b9e A www.6pm.com CNAME 6pm.zappos.com.akadns.net CNAME san.www.6pm.com.edgekey...
 2895 18.982164  192.168.1.10  192.168.1.1   DNS       75 Standard query 0x6246 A www.audible.com
 2896 18.991733  192.168.1.10  192.168.1.1   DNS       75 Standard query 0x6a3c A www.amazon.jobs
 2897 18.991793  192.168.1.1   192.168.1.10  DNS       91 Standard query response 0x6246 A www.audible.com A 52.94.224.232
 2898 18.993458  192.168.1.1   192.168.1.10  DNS      187 Standard query response 0xe1d5 A www.amazoninspire.com CNAME CddfW-Websi-R8I3GN3QFWEA-1397517957.us-east-1...
 2899 18.995151  192.168.1.10  192.168.1.1   DNS       82 Standard query 0x[illegible]816 A www.audiobookstand.com
 2900 18.995504  192.168.1.1   192.168.1.10  DNS      137 Standard query response 0x6a3c A www.amazon.jobs CNAME amazon.jobs A 54.240.253.58 A 54.240.251.145 A 54.24...

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Netgear_d7:98:a5 (b0:39:56:d7:98:a5), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
> Internet Group Management Protocol
```

Response from Amazon coming from various ad DNS servers

When the Pi Hole is not activated and you send a request query for Amazon.com you will get back tons of responses from various DNS servers which are associated with Amazon. Amazon essentially routes all your request queries through Ads DNS servers, these servers in return route that traffic back to Amazon which it displays on its start up page. You would see Ads for websites like the ones listed above audiobookstand.com etc.


Wireshark Capture
Pi Hole On
Lap Top
Raspberry Pi
Request
Pi Hole
Response
pihole blocking test.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source             Destination        Protocol  Length Info
   30 10.126898   192.168.0.167      192.168.0.189      DNS        71 Standard query 0x3c9c A otf.msn.com
   25 7.355032    192.168.0.167      192.168.0.189      DNS        93 Standard query 0x8db6 A v10.vortex-win.data.microsoft.com
   70 13.302397   192.168.0.167      192.168.0.189      DNS        72 Standard query 0xdaa4 A pixel.wp.com
   22 6.388045    192.168.0.167      192.168.0.189      DNS        87 Standard query 0xebf5 A googleads.g.doubleclick.net
   68 13.010878   192.168.0.189      192.168.0.167      DNS       102 Standard query response 0x032f A rcm-na.amazon-adsystem.com A 192.168.0.200
    6 0.529486    192.168.0.189      192.168.0.167      DNS        87 Standard query response 0x0d2d A otf.msn.com A 192.168.0.200
    2 0.005675    192.168.0.189      192.168.0.167      DNS        84 Standard query response 0x1b6b No such name A wpad.hsd1.ca.comcast.net
   31 10.133194   192.168.0.189      192.168.0.167      DNS        87 Standard query response 0x3c9c A otf.msn.com A 192.168.0.200
   26 7.361602    192.168.0.189      192.168.0.167      DNS       109 Standard query response 0x8db6 A v10.vortex-win.data.microsoft.com A 192.168.0.200
   72 13.325296   192.168.0.189      192.168.0.167      DNS        88 Standard query response 0xdaa4 A pixel.wp.com A 192.168.0.200
   23 6.396129    192.168.0.189      192.168.0.167      DNS       103 Standard query response 0xebf5 A googleads.g.doubleclick.net A 192.168.0.200
   10 3.323987    Raspberr_a3:9f:b9  Microsof_cd:0d:8b  ARP        42 Who has 192.168.0.167? Tell 192.168.0.189
    3 0.116772    Microsof_cd:0d:8b  Broadcast          ARP        42 Who has 192.168.0.200? Tell 192.168.0.167
    7 1.116826    Microsof_cd:0d:8b  Broadcast          ARP        42 Who has 192.168.0.200? Tell 192.168.0.167

> Frame 68: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: Raspberr_a3:9f:b9 (b8:27:eb:a3:9f:b9), Dst: Microsof_cd:0d:8b (98:5f:d3:cd:0d:8b)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 192.168.0.167
> User Datagram Protocol, Src Port: 53, Dst Port: 51282
v Domain Name System (response)
    Transaction ID: 0x032f
```

In the wireshark capture you can see that all DNS protocol packets have a request (query) and response pair of packets. Wireshark shows that all request packets are going to 192.168.0.189 this is the IP address of the raspberry pi itself. If you look closely at the response packets you will see they are coming from the raspberry pi at 192.168.0.189 but they are associated with 192.168.0.200 which is the "Black hole" for advertisements that Pi hole creates. The pi holes DNS has a list of domains which are associated with advertisers and spam and every domain on that list is blocked which means the packets are knocked down and will not return in the response. The pi hole shoots out the sanitized response packets to the raspberry pi which in return shoots these packets out to the ip address at 192.168.0.167 which is the laptop that is used to browse the internet. The end user will see an ad free page on their physical screen, and they can have a hassle free experience browsing.

References

“Pi-Hole®: A Black Hole for Internet Advertisements.” *Pi-Hole®: A Black Hole for Internet Advertisements*, pi-hole.net/.

https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

Faq-bot, and PromoFaux. "How Do I Configure My Devices to Use Pi-hole as Their DNS Server?" *Pi-hole Userspace*. N.p., 18 Oct. 2016. Web. 01 July 2018. <https://discourse.pi-hole.net/t/how-do-i-configure-my-devices-to-use-pi-hole-as-their-dns-server/245>.

https://www.makeuseof.com/tag/adblock-everywhere-raspberry-pi-hole-way/