

DNS Blackholing with Pi-Hole

aka: How To Block Unwanted Ads & Malware on your network for cheap

WHAT?

Create a system to block advertisement sites

Create a system to block malware & C2 sites

Do this to protect the entire network, automatically

Do this for very little money

Adverts blocking your news story

With the right SUPPORT

SEE THE FILM

AMERICAN FAMILY INSURANCE®

ranker.com 1:10 PM 55%

The Des Moines Register
PART OF THE USA TODAY NETWORK

Trump is nominating conservative federal judges to do his bidding.

Demand that our senator Chuck Grassley uphold the long tradition of senators having a say in the confirmation process. The Senate is all that's standing in the way of Trump's extreme nominees.

SIGN THE PETITION

LEAGUE OF CONSERVATION VOTERS

NEWS INVESTIGATIONS

Iowa Lottery takes a pass on fixes to stop fraud

IOWA LOTTERY

FOLLOW DES MOINES REGISTER:

COMMUNITIES

Altoona Urbandale Ankeny Waukee Des Moines West Des Moines Johnston Indianola High School Insider

desmoinesregister.com 1:13 PM 54%

CONTINUE TO ARTICLE >

Forbes QUOTE OF THE DAY

If you aren't failing, you aren't learning, and if you aren't learning, you aren't improving.

- Janelle Maiocco, CEO of Barn2Door

INTERESTING TOPICS

01. FACEBOOK ADVERTISING TIPS
02. POST AN AD ON FACEBOOK
03. ADS ONLINE

forbes.com 1:20 PM 53%

Adverts tricking you into clicking them instead of the desired link

RELATED SEARCHES

- Vim

PRICE

- Free Only

PLATFORM

- All
- Windows
- Mac
- iOS
- Android

EDITOR RATING

- ★★★★★ & up
- ★★★★★ & up
- ★★★★★ & up
- ★★★★★ & up

USER RATING

- ★★★★★ & up
- ★★★★★ & up
- ★★★★★ & up

Results for gvim

Ads by Google

- Gvim - Download - filesendsuite.com
free.filesendsuite.com/Download ▾
Amazing Free Offer by filesendsuite latest V
Download Here · Gratis · Fast & Secure · Fr
Types: Free, Secure, Fast Download
- Gvim Vs Vim - wow.com
www.wow.com/Gvim+Vs+Vim ▾
Search for Gvim Vs Vim. Look Up Quick Res
- gVim Portable
Efficiently write code with this feature-rich
PUBLISHER: PortableApps DOWNLOADS: 7,028
- gVim Shell
Use gVim (GUI version of vim) more easily
PUBLISHER: Chris Software DOWNLOADS: 781

Ads by Google

- Gvim - Download - filesendsuite.com
free.filesendsuite.com/Download ▾
Amazing Free Offer by filesendsuite latest V
Download Here · Gratis · Fast & Secure · Fr
Types: Free, Secure, Fast Download
- Gvim Vs Vim - wow.com
www.wow.com/Gvim+Vs+Vim ▾
Search for Gvim Vs Vim. Look Up Quick Res

Take a 10 minute Lumosity **Fit Test**. Challenge **memory**, **attention** & more.

lumosity
[Take Fit Test ▶](#)

gVim Portable

Download Now Secure Download
Average User Rating:
Be the first to rate this product!

IS THE SOFTWARE HERE REALLY FREE?  WHAT'S THE CATCH?

Publisher's Description

From PortableApps:
gVim Portable is a highly configurable text editor built to enable efficient text editing. It is an improved version of the vi editor distributed with most UNIX systems.
gVim Portable is often called a "programmer's editor," and so useful for programming that many consider it an entire IDE. It's not just for programmers, though. Vim is perfect for all kinds of text editing, from composing email to editing configuration files.
gVim Portable can be configured to work in a very simple (Notepad-like) way, called evim or Easy Vim.

SOURCEFORGE [Browse](#) [Enterprise](#) [Blog](#) [Deals](#) [Help](#)

SOLUTION CENTERS Go Parallel [Resources](#) [Newsletters](#) [Cloud Storage Providers](#) [Business VoIP Providers](#) [Intern...](#)

KeePass
Download of keepass will start in 5 seconds...
Problems with the download? Please use this [direct link](#), or try another [mirror](#).

PortableApps.com: Portable Software/USB [Download](#)
Portable software for USB, portable, and cloud drives

Apache OpenOffice [Download](#)
A free and Open Source productivity suite

ePass [Download](#)
Lightweight and easy-to-use password manager

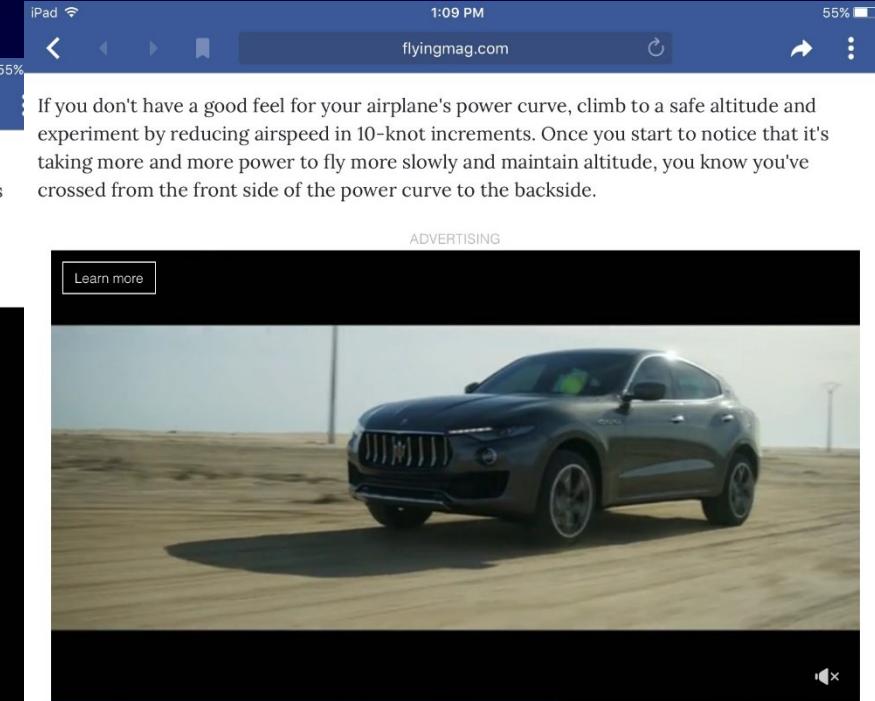
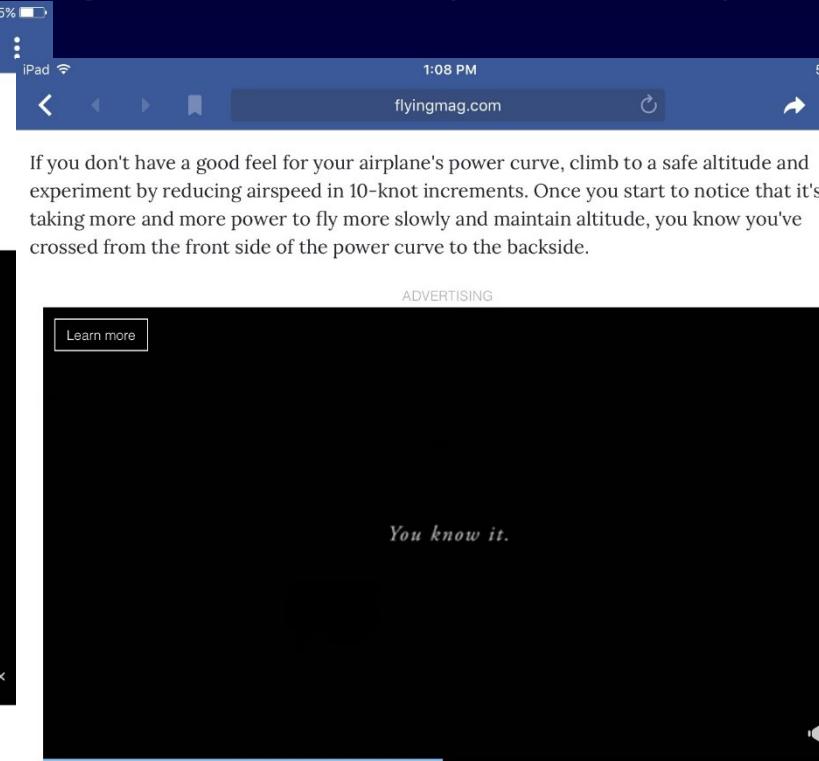
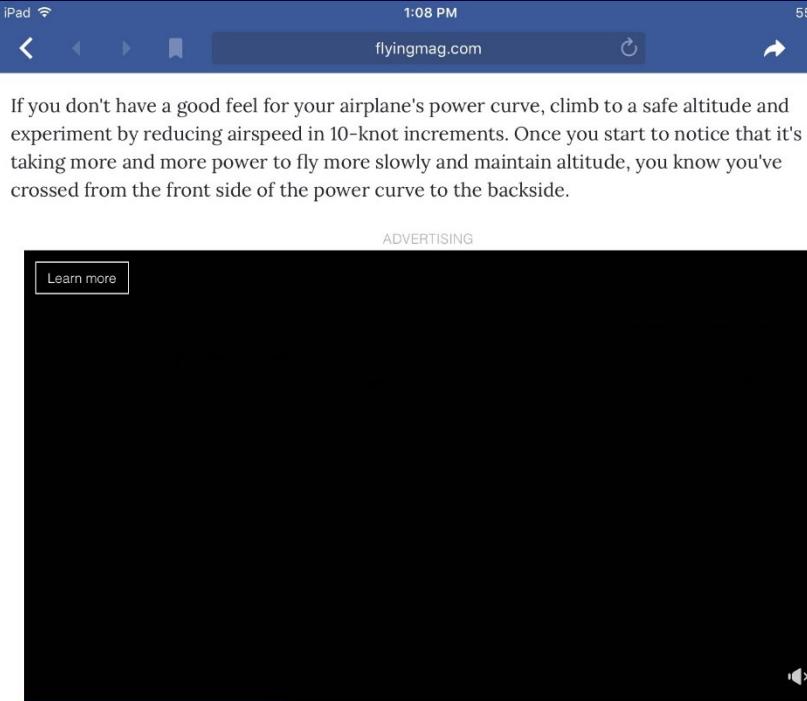
E UPDATED Get project updates, sponsored content from our select partners and more.
"Follow" below, you are agreeing to the [Terms of Use](#) and the [Privacy Policy](#).

United States
Your email address
[Follow](#)

Find and Develop Software [Create a Project](#) [Blog](#) [@sourceforge](#)
Community [Software Directory](#) [Top Downloaded Projects](#) [Resources](#)

Help [Site Documentation](#) [Support Request](#)

Adverts eating away at your bandwidth



Get exclusive online content like this delivered straight to your inbox by [signing up for our free enewsletter](#).

We welcome your comments on [flyingmag.com](#). In order to maintain a respectful environment, we ask that all comments be on-topic, respectful and spam-free. All comments

Get exclusive online content like this delivered straight to your inbox by [signing up for our free enewsletter](#).

We welcome your comments on [flyingmag.com](#). In order to maintain a respectful environment, we ask that all comments be on-topic, respectful and spam-free. All comments

Get exclusive online content like this delivered straight to your inbox by [signing up for our free enewsletter](#).

We welcome your comments on [flyingmag.com](#). In order to maintain a respectful environment, we ask that all comments be on-topic, respectful and spam-free. All comments

Want to block most malware from reaching out?

Flame Malware Statistics

OpenDNS

86 DOMAINS
for Command and Control

24 Current
IP addresses
hosting C&C

22 Different registration
services used

Percent of traffic from top countries

2015/06/07_01:21	teamtalker.net/download.php
2015/06/04_07:13	microsoft.com32.info
2015/06/04_07:13	avg.com32.info
2015/06/04_07:13	kaspersky.com32.info
2015/06/04_05:56	windows-crash-report.info/Wind

8 COUNTRIES INFECTED

malware, virus, infection, trojan, spyware, phishing, hacking, intruder, spam, firewall, detection, hacker, network, target, crime, internet, security, service, attack, infected, computer, terrorism, malware, virus, infection, trojan, spyware, phishing, hacking, intruder, spam, firewall, detection, hacker, network, target, crime, internet, security, service, attack, infected, computer, terrorism



Domain Name: REDIRECTME.NET
Registrar: VITALWERKS INTERNET SOLUTIONS LLC DBA NO
Whois Server: whois.no-ip.com
Referral URL: http://www.no-ip.com
Name Server: NS7.MICROSOFTINTERNETSafety.NET
Name Server: NS8.MICROSOFTINTERNETSafety.NET
Status: clientTransferProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 30-jun-2014
Creation Date: 09-aug-2001
Expiration Date: 09-aug-2020

2015/06/04_05:56	windows-crash-report.info/System/	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info/norton/	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info/iMac/	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info/files.zip	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info/Error/	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info/Alerte_de_s%23U00e9curit%23U00e9/	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info/Alert/	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA
2015/06/04_05:56	windows-crash-report.info	104.238.102.226	ip-104-238-102-226.i.p.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT .INFO@domainsbyproxy.com	26496	USA

0 / 3 [7]hxxp://131.155.81.158/rasta01.exe Netherlands 131.155.81.158
0 / 6 [8]hxxp://fuhxodyz.ru/rasta01.exe Belarus 93.125.67.95
0 / 0 [9]hxxp://www.philchor-nb.de/demo/rasta01.exe Germany
0 / 2 [10]hxxp://ikqydkod.ru/rasta01.exe Ukraine 109.251.141.23
0 / 2 [11]hxxp://aro0eq.hozfezbe.ru/rasta01.exe Russian Federation
0 / 6 [12]hxxp://bopefidi.ru/rasta01.exe Russian Federation 2.94.27.238
0 / 2 [13]hxxp://ycsycxyd.ru/rasta01.exe Ukraine 46.119.193.89
0 / 2 [14]hxxp://sojouvyc.ru/rasta01.exe Ukraine 31.128.74.7
0 / 2 [15]hxxp://vadlubiq.ru/rasta01.exe Ukraine 109.162.84.6
0 / 2 [16]hxxp://kazlyjva.ru/rasta01.exe Malaysia 58.26.182.98
0 / 2 [17]hxxp://funfubap.ru/rasta01.exe Taiwan 114.35.239.185
0 / 2 [18]hxxp://goryzcob.ru/rasta01.exe Ukraine 109.87.254.247
0 / 2 [19]hxxp://motbajsi.ru/rasta01.exe Ukraine 91.196.61.56
0 / 6 [20]hxxp://xymkapaq.ru/rasta01.exe Latvia 89.201.53.86
0 / 2 [21]hxxp://hupjiwuc.ru/rasta01.exe Ukraine 195.114.156.254
0 / 6 [22]hxxp://runevfoh.ru/rasta01.exe Ukraine 5.248.34.57
0 / 2 [23]hxxp://virerceb.ru/rasta01.exe Argentina 190.227.181.203

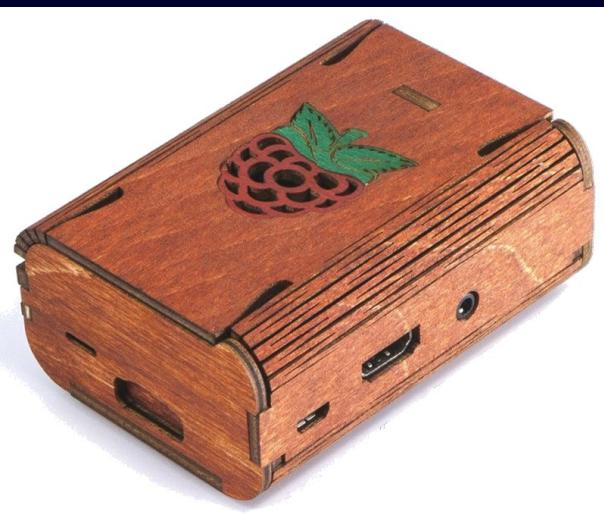
ARE YOU SUFFERING A VIRUS INFECTION? Computer Repair Tips and More

More than half of all computer users will encounter malicious software, or malware, costing consumers billions of dollars each year. These programs can destroy your data, steal your information and make your PC unusable.

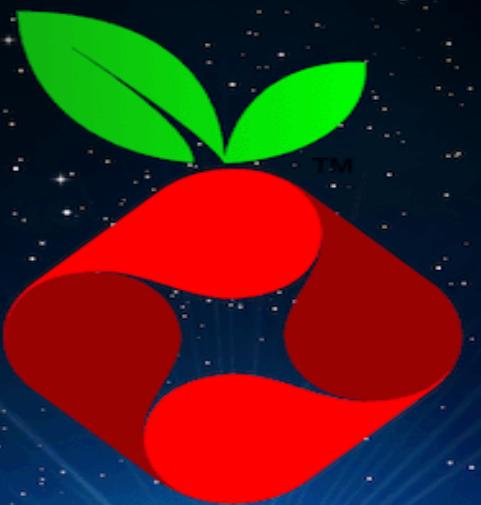
Malware creation hit a record high in 2011: **26,000,000** new strains

RISE IN MALWARE





Good News!
I'll show you how.

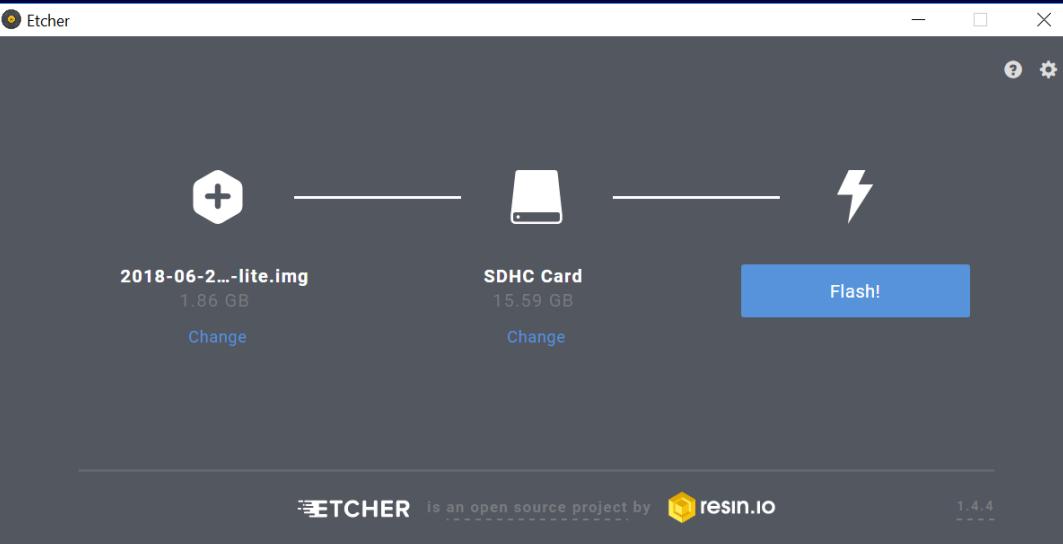


Pi-hole™

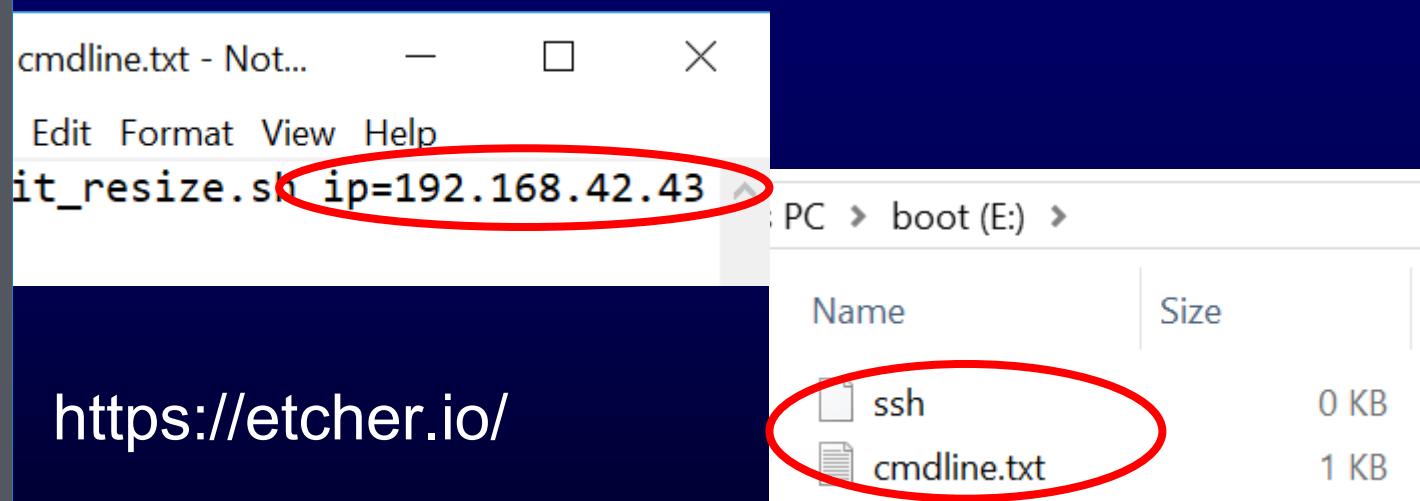
Network-wide ad blocking
via your own hardware



Prepare a Fresh Raspbian Lite



After writing the image, you might have to eject and re-insert the disk, create an empty file named “ssh” (use a new text file but remove the .txt extension) on the boot (root) of the drive (in my example it would be the “H:\ssh”). Open the cmdline.txt file and append to the end of the first line “ ip=192.168.42.1XX” where XX is your student number.

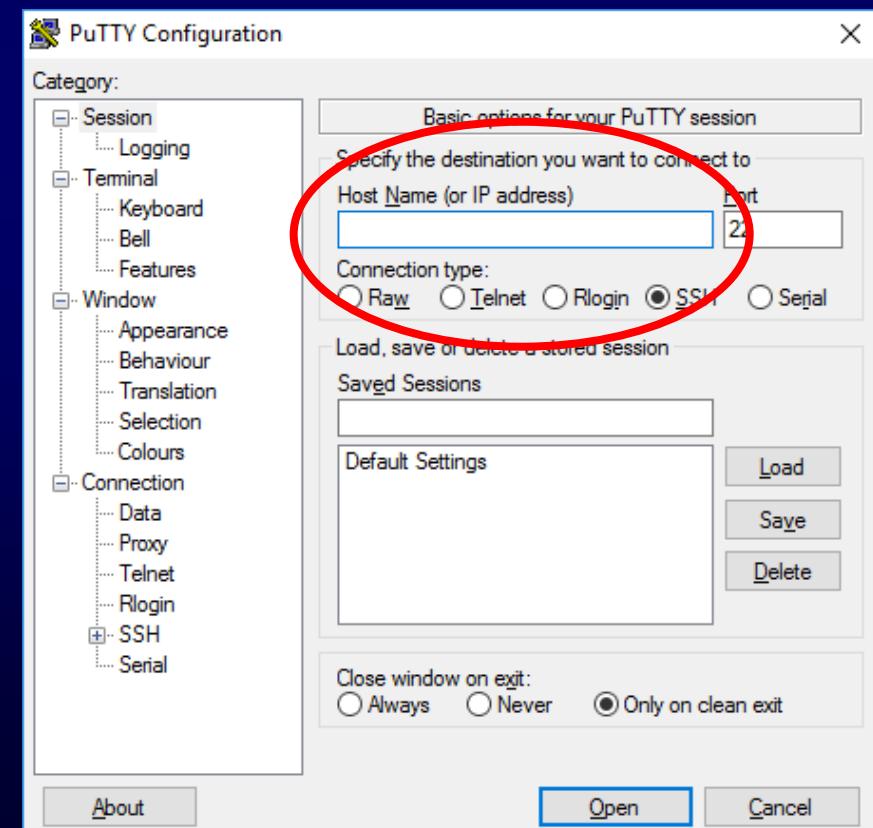
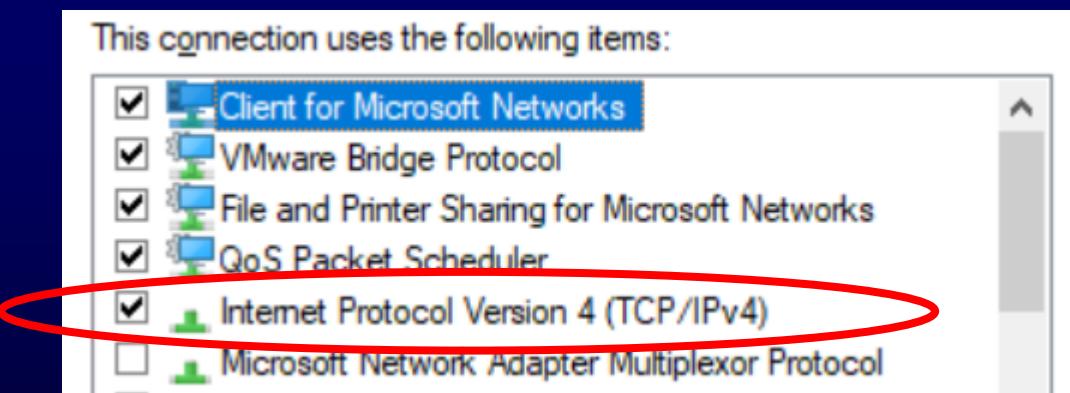


Prepare a Fresh Raspbian Lite

Eject the disk, put it in the Pi, boot your Pi-3, wait a few minutes. While you're waiting for the Pi to boot, set your laptop's wired IP address to 192.168.42.2~~xx~~.

In Windows10 go to “Control Panel -> Network and Sharing Center”, click on “Change adapter settings”, right-click on your Ethernet icon and choose “Properties”. Choose “Internet Protocol Version 4 (TCP/IPv4)”, click “Properties” and set the IP.

Launch puTTY and connect to your Pi.



Basic Raspbian Lite Configuration

- First things first, start the config program!

```
pi@raspberrypi:~ $ sudo raspi-config
```

- Change the password

(make it strong, but be sure you remember it!)

- Change the hostname

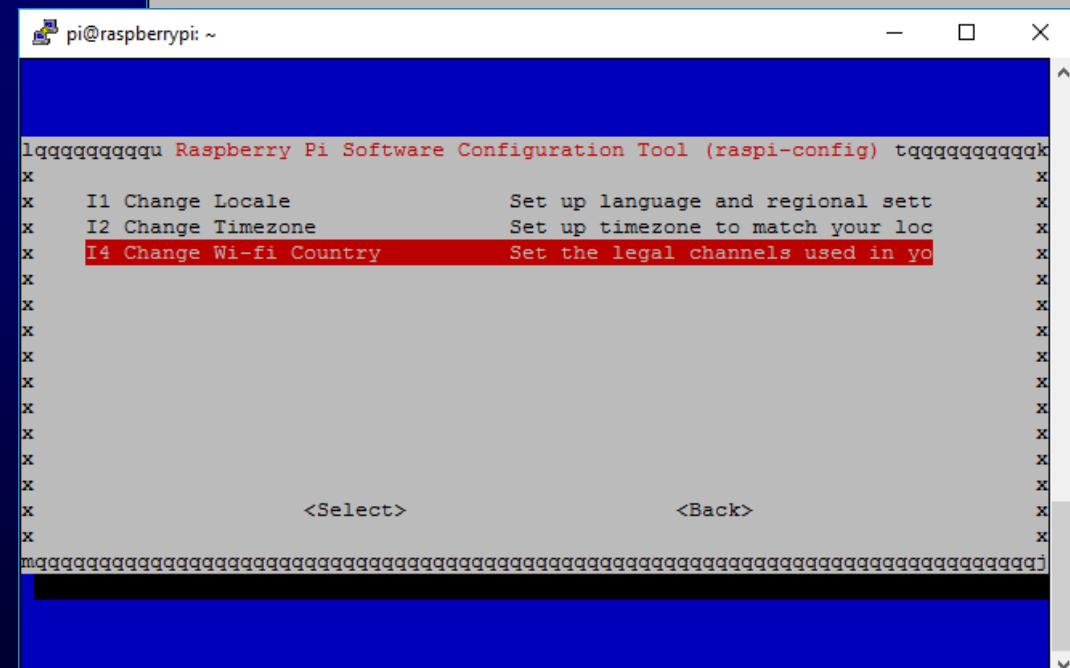
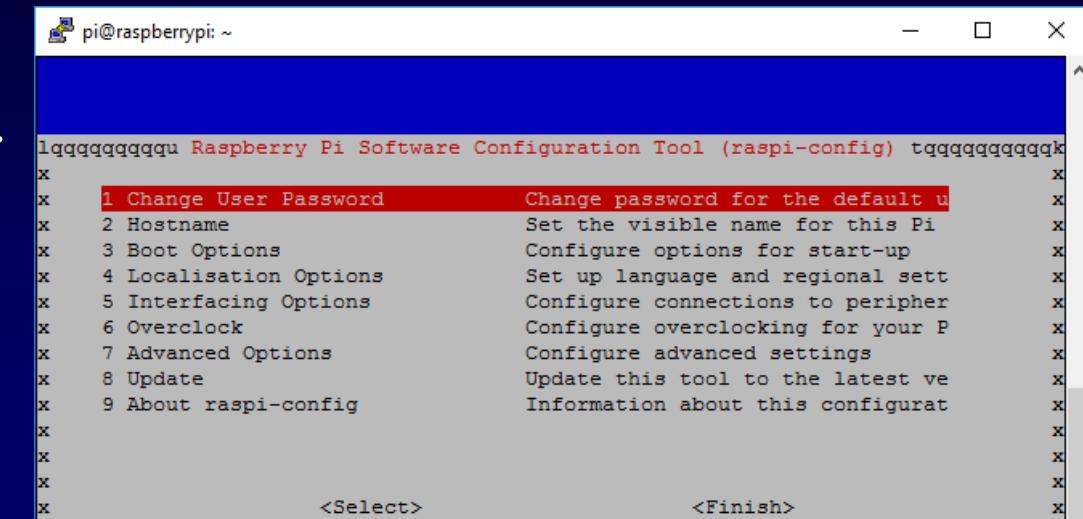
(for class please use your lastname/nickname)

- Go into the Localisation Options

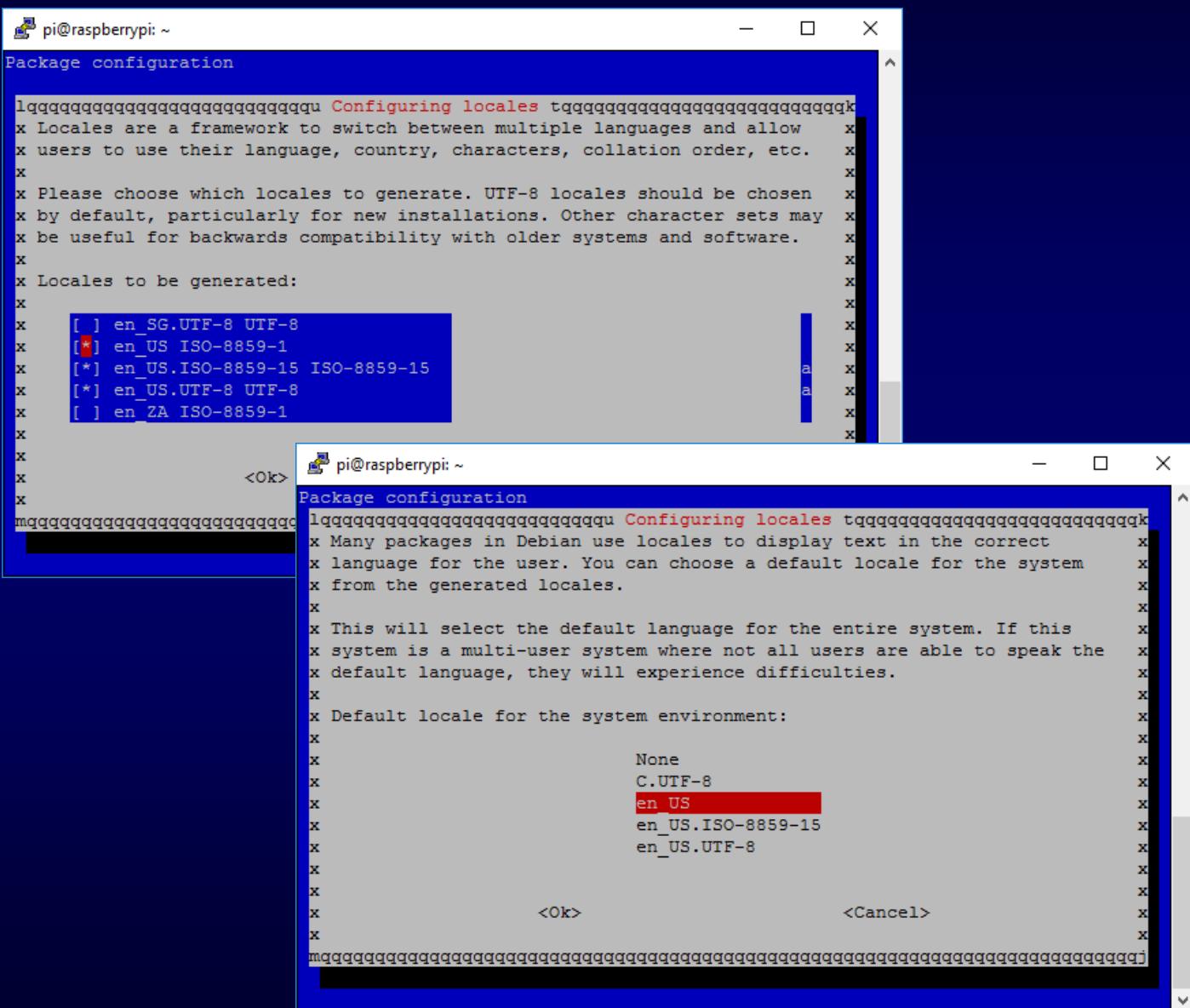
- Set the Timezone

- Set the Wi-Fi Country

- Change Locale is on next slide



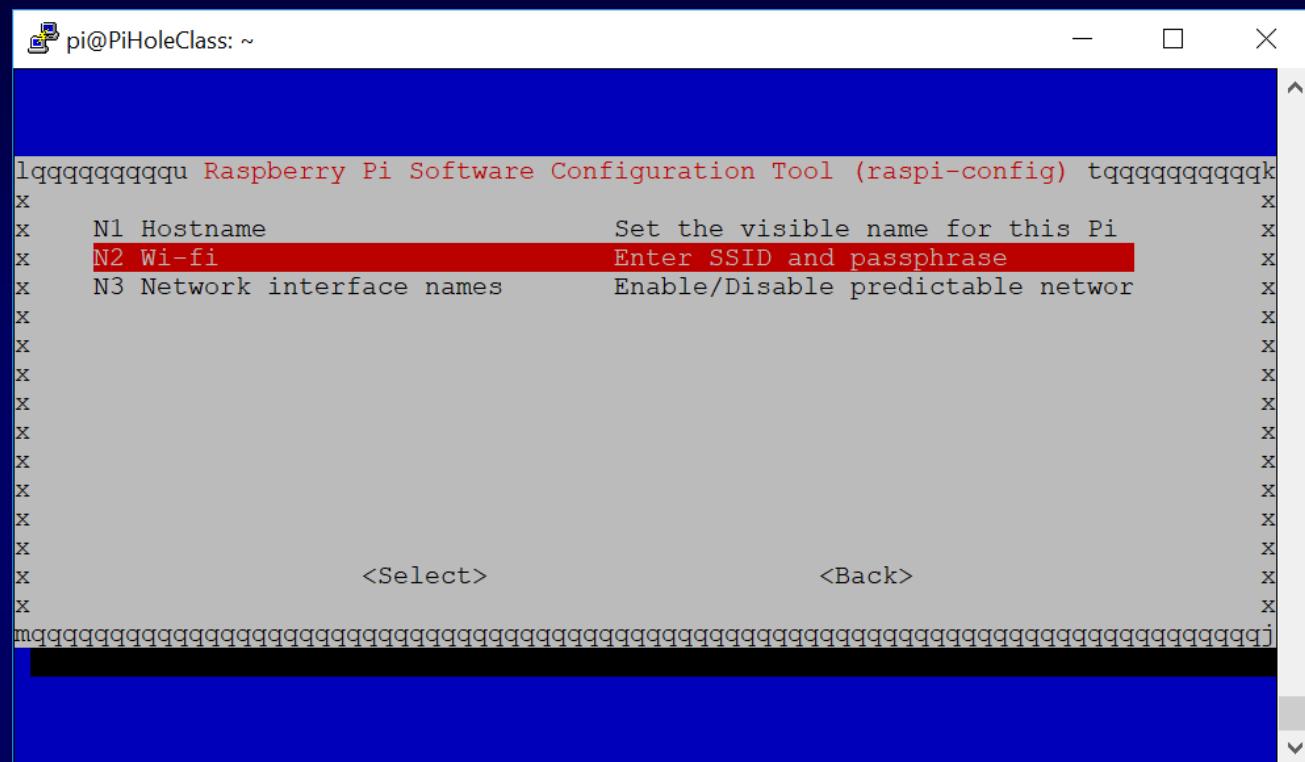
Basic Config continued



Under “Change Locale” scroll down to the en_GB and deselect these, then select the three en_US options. For the default locale, choose “en_US” and continue.

Really, Still Basic Configuration

- Enable predictable network interface names.
- Set the WiFi SSID and Passphrase.
- When back to the original config menu, select <Finish> and the Pi will reboot. Wait a minute, then reconnect by ssh'ing in with the new password.



Add DNS & Apply Updates/Patches

Edit the `/etc/resolv.conf` file to add the screen to the right onto the end. This will allow the installation scripts to resolve DNS names until we get FTLDNS running on the Pi-Hole.

```
$ sudo vi /etc/resolv.conf  
nameserver 8.8.8.8
```

Update the OS & install git by issuing these commands (they will take a long time and lots of text will scroll by).

```
$ sudo apt-get update  
$ sudo apt-get -y upgrade  
$ sudo apt-get -y dist-upgrade  
$ sudo apt-get -y install git
```

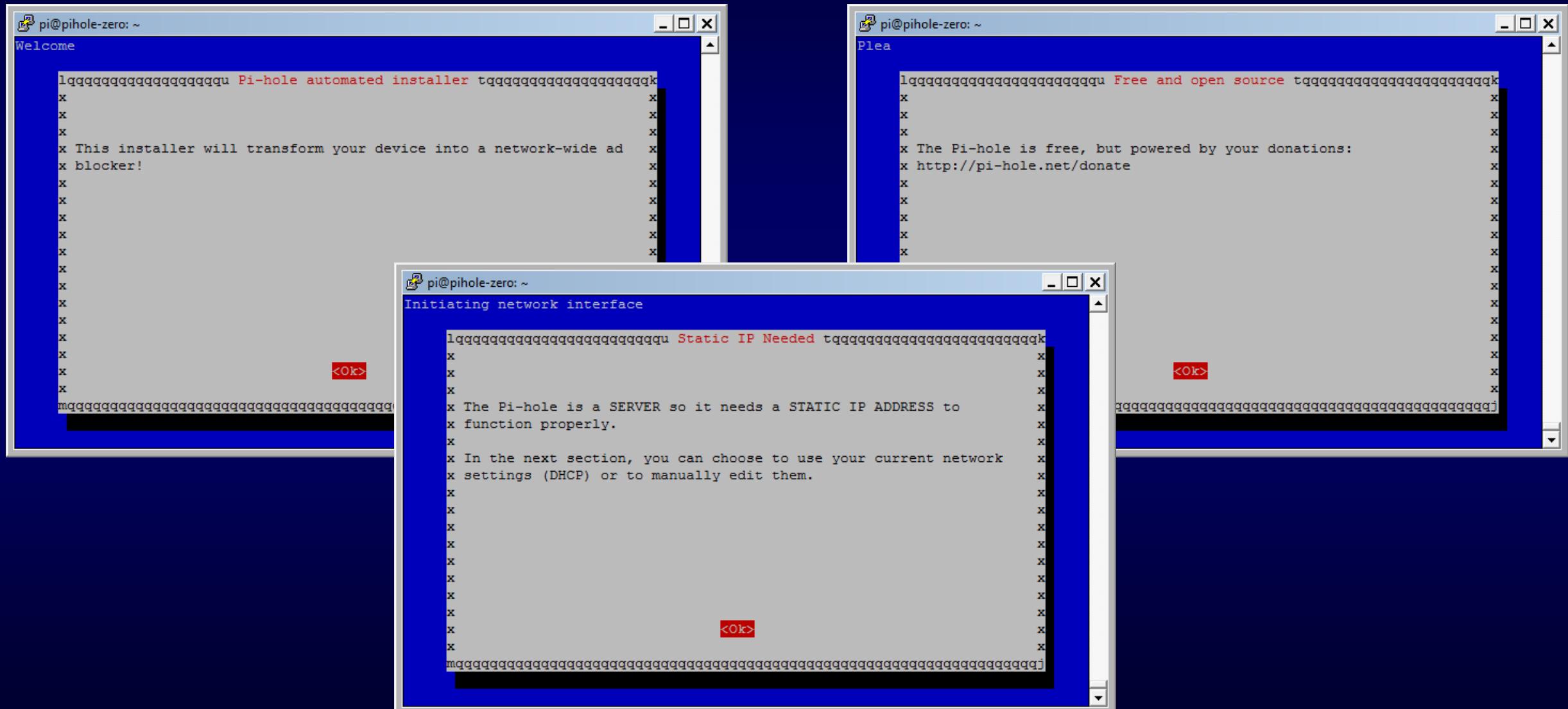
And Now The Part You've All Been Waiting For

```
$ git clone --depth 1 https://github.com/\\  
    pi-hole/pi-hole.git Pi-Hole  
$ cd Pi-Hole  
$ less automated\\ install/basic-install.sh  
  
$ sudo bash automated\\ install/basic-install.sh
```

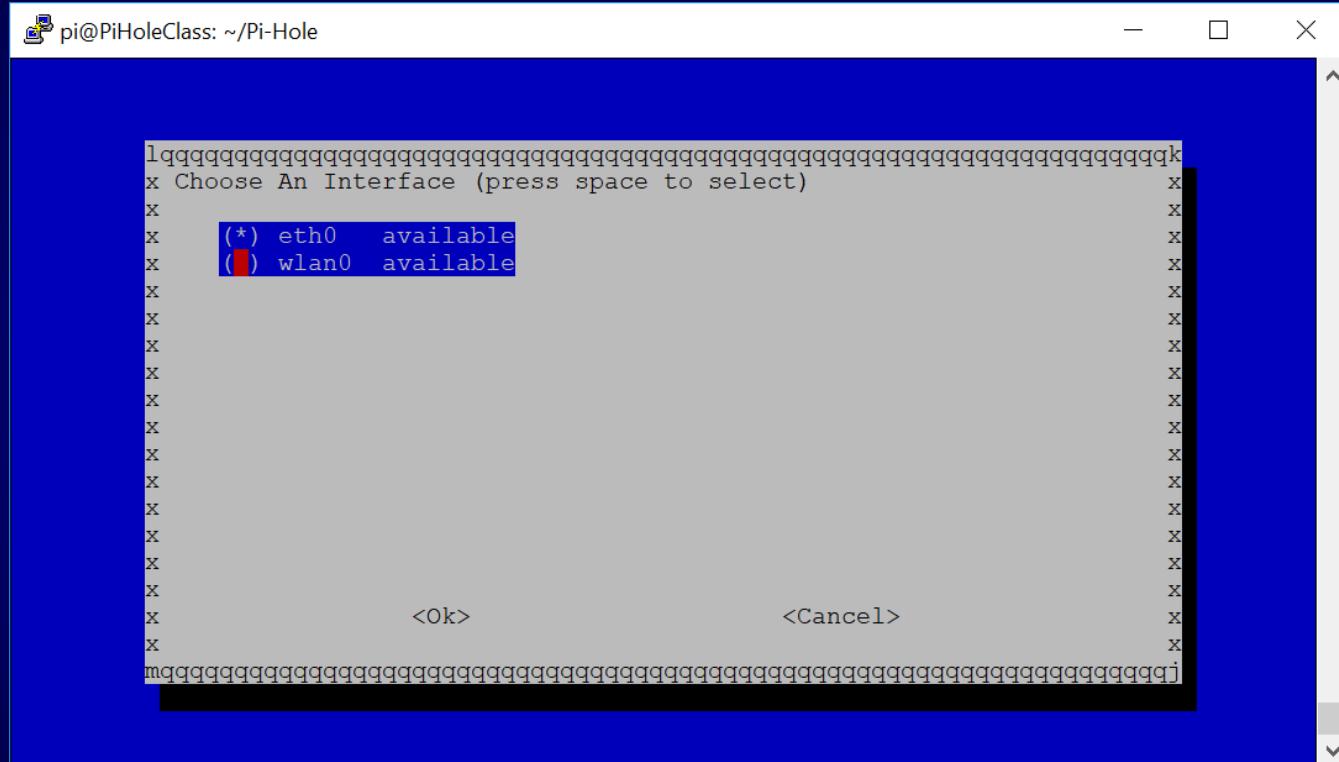
← We start by cloning the git repository, then we examine the install script before finally running it as root.

There are alternative methods to install Pi-Hole, but if you are concerned with security at all you should be thoroughly reviewing any script downloaded from the internet before executing it, ***ESPECIALLY*** as root! I very ***HIGHLY*** encourage you to (after class) review the install script and research any/all pieces of software installed by Pi-Hole; as G.I.Joe said, “Knowing is half the battle!”

3 Basic Confirmation Dialogs



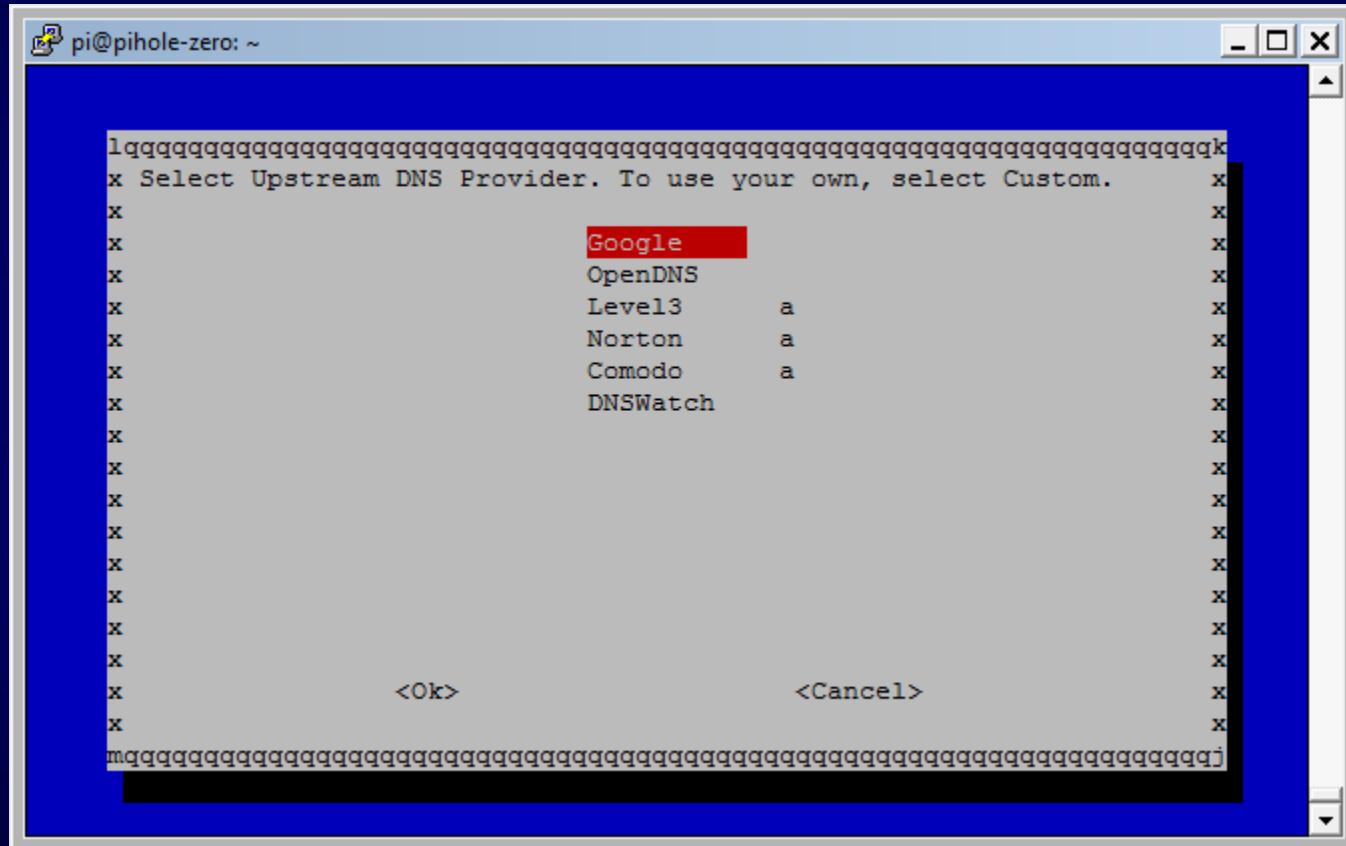
Choose Interface



This window won't appear if you only have one interface, but we have two in class.

For this class we'll use wlan0.
At home/work you should use eth0 though. What reasons can you think of to use eth0 instead of wlan0?

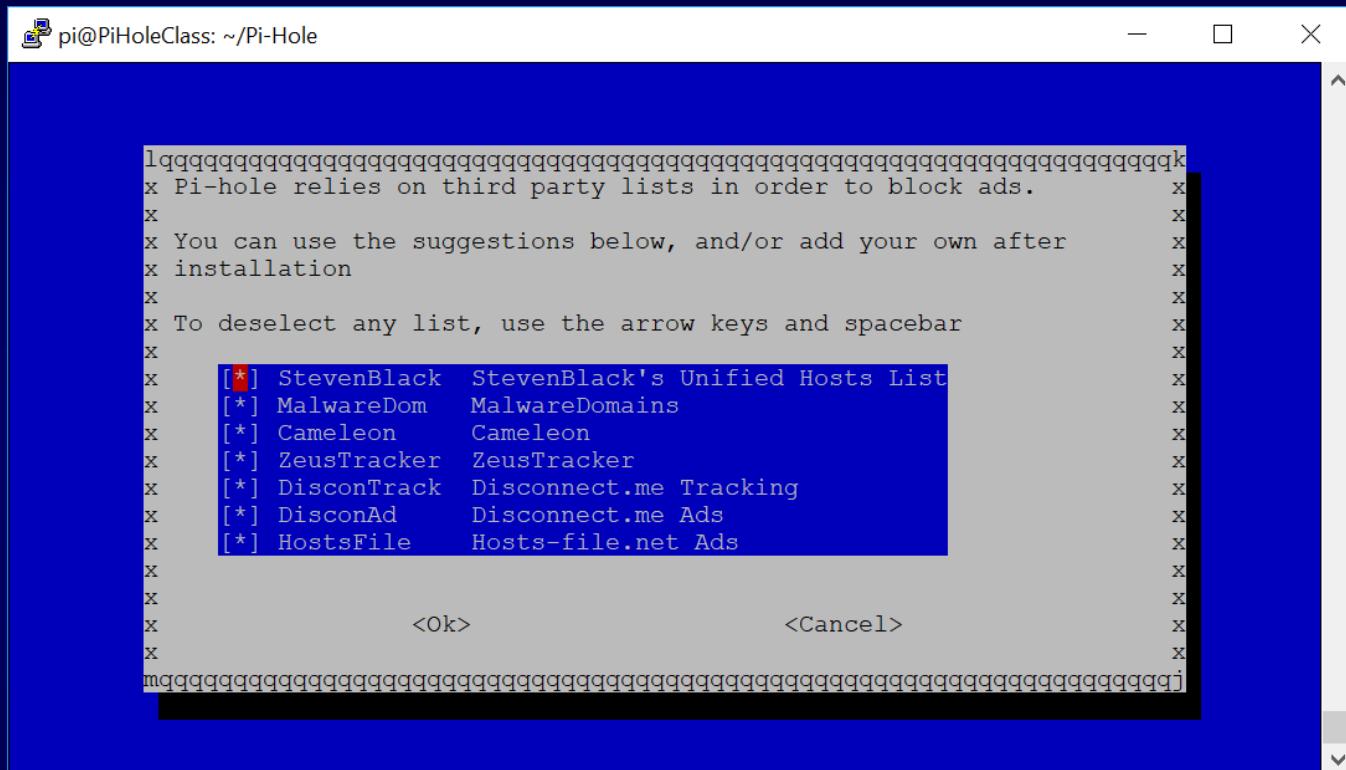
Choose Upstream DNS Provider



- Google (8.8.8.8/8.8.4.4)
- OpenDNS
- Level3 *
- Norton *
- Comodo *
- DNSWatch

Why is your local ISP probably
NOT your best choice?

Choose Block Lists

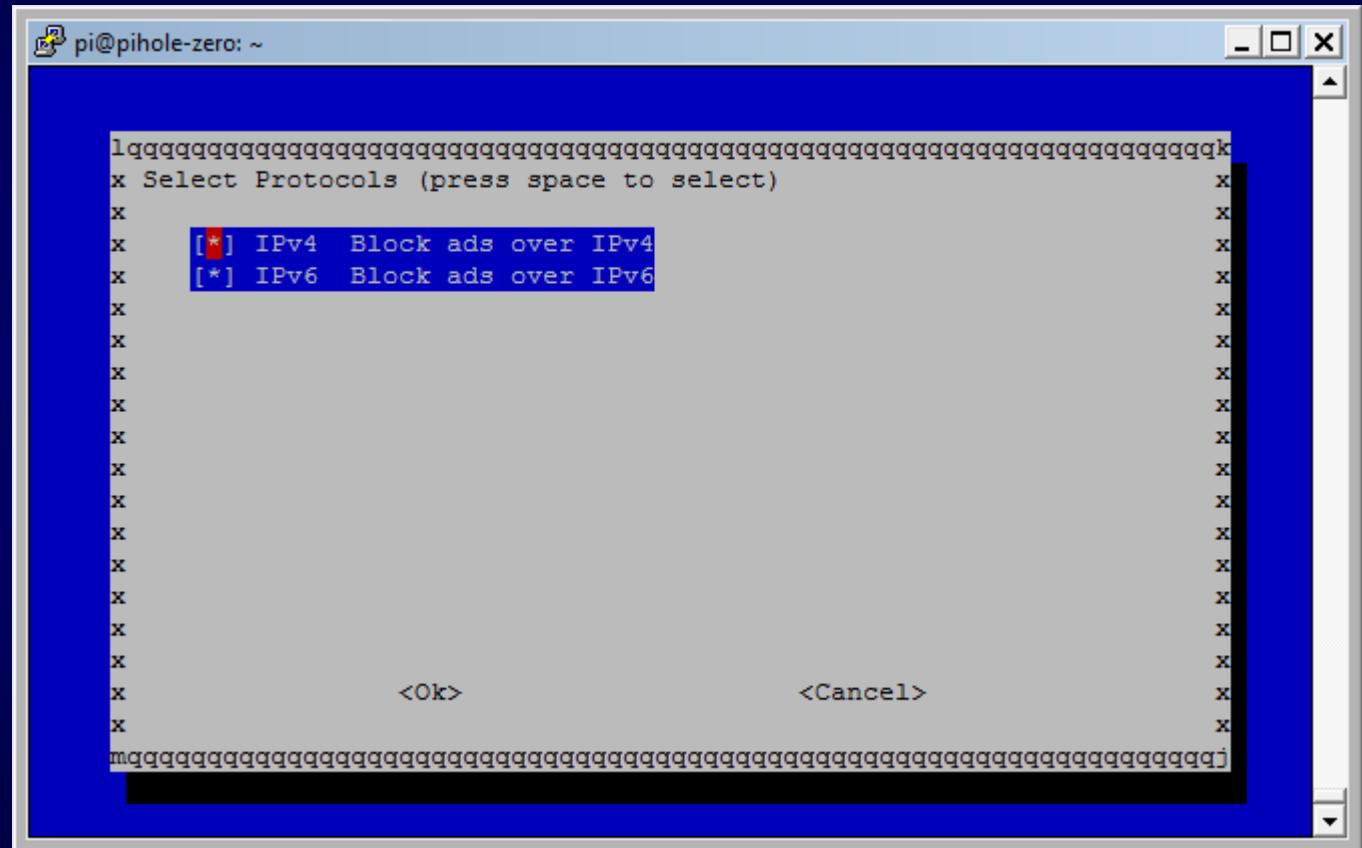


You can choose lists to include from the default set provided on the next screen. If you wish to add or remove any later, you can still do this via the web admin portal.

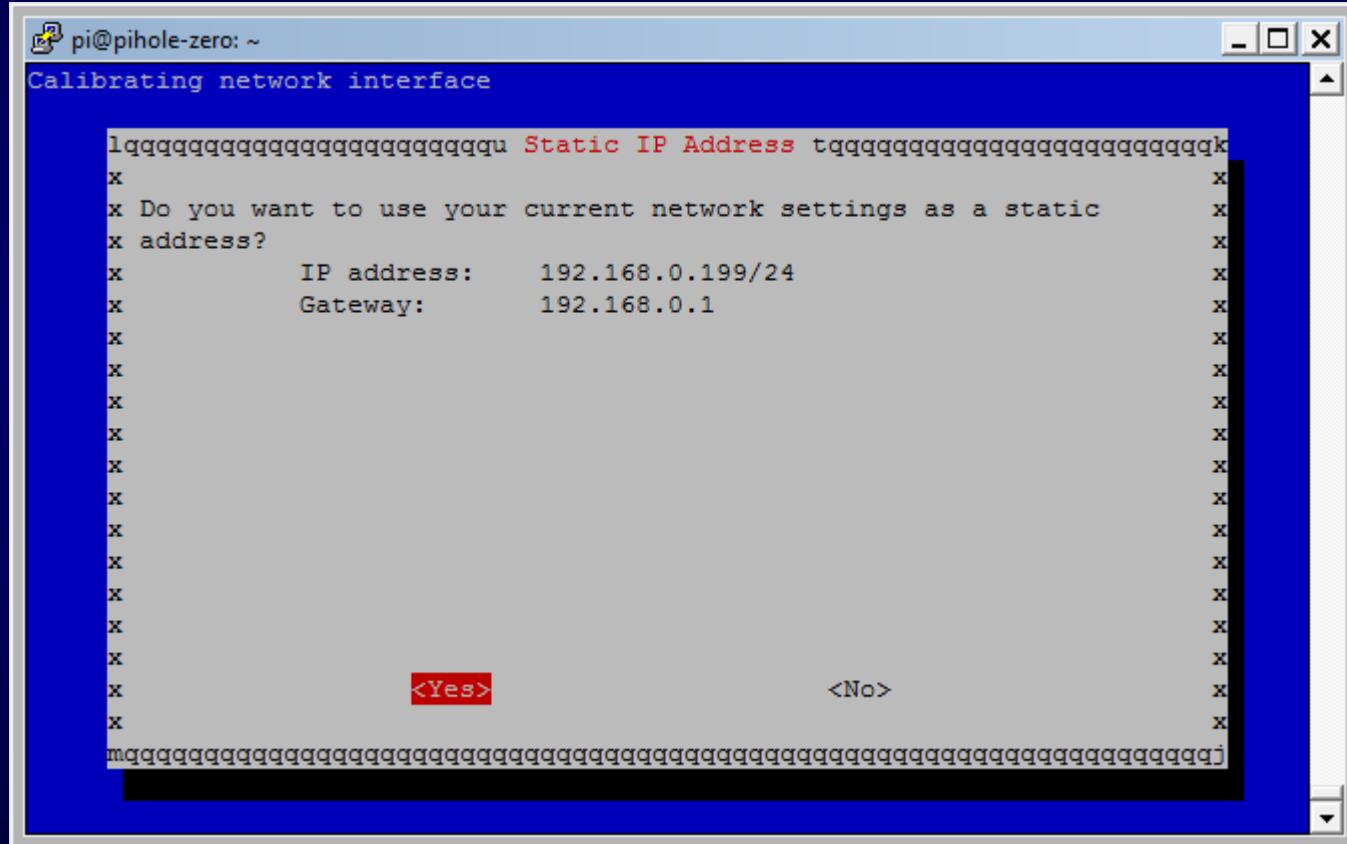
IPv4 and/or IPv6

For most implementations today
in the U.S. only IPv4 is needed.

What are reasons for/against also enabling IPv6?



Static IP Address

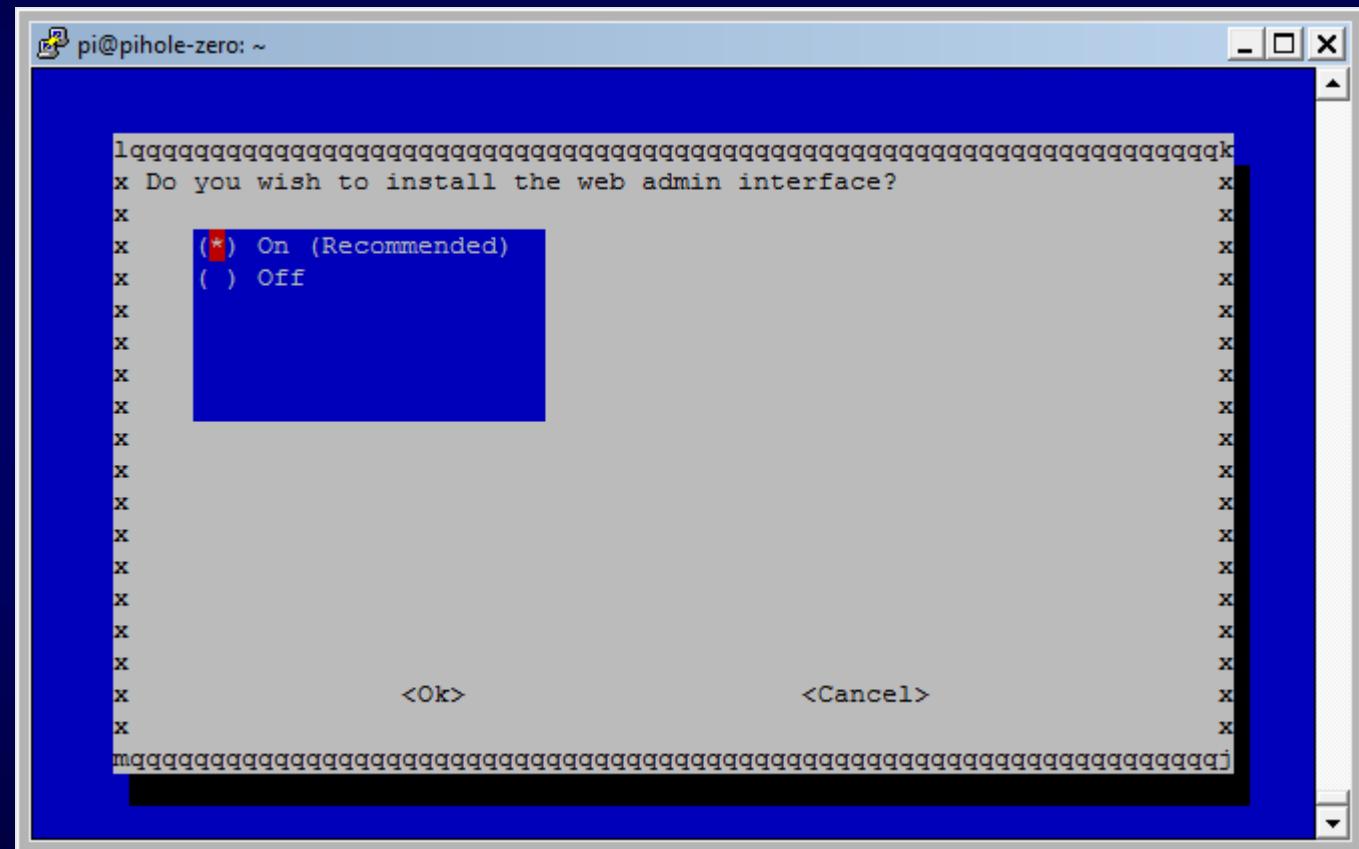


- If you choose <Yes> what you see on the screen is what you get.
 - If you choose <No> you'll get a dialog to enter your desired IPv4 address.
 - This WILL change your existing system settings.
 - This MIGHT generate an IP conflict message.

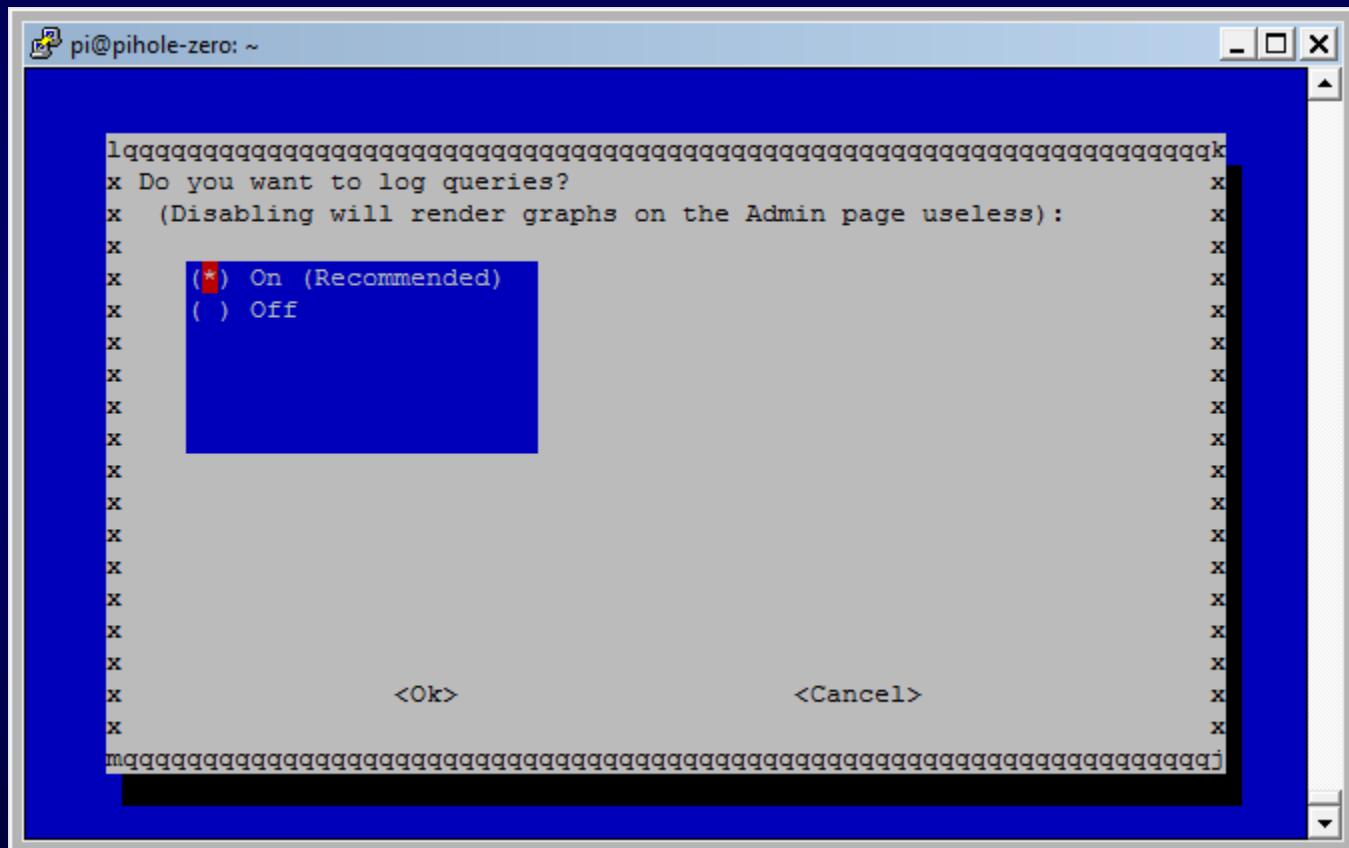
KNOW YOUR NETWORK!

Web Admin?

Well, yes you want the web admin interface. When you get to the point where you don't want the web interface you'll be teaching other people DNS Blackholing.



Want to Log Queries?



Why YES, I think it's a lovely idea (I'll explain more later).

Sit & Wait (have a drink)

```
pi@pihole-zero: ~
:::
::: Neutrino emissions detected...
:::
::: Pulling source lists into range... done!
:::
::: Getting raw.githubusercontent.com list... done
:::   Status: Success (OK)
:::   List updated, transport successful!
::: Getting mirror1.malwaredomains.com list... done
:::   Status: Success (OK)
:::   List updated, transport successful!
::: Getting sysctl.org list... done
:::   Status: Success (OK)
:::   List updated, transport successful!
::: Getting zeustracker.abuse.ch list... done
:::   Status: Success (OK)
:::   List updated, transport successful!
::: Getting s3.amazonaws.com list... done
:::   Status: Success (OK)
:::   List updated, transport successful!
::: Getting s3.amazonaws.com list... done
:::   Status: Success (OK)
:::   List updated, transport successful!
::: Getting hosts-file.net list... 
```

The script is doing all the heavy work.

Verify IP address & record the password (into your KeePass right?).

Now Point DNS Queries To Pi-Hole

Find your router's DNS setting and change it to point at your Pi-Hole's IP.

BELKIN Wireless Router Setup Utility

LAN Setup

- LAN Settings
- DHCP Client List
- Internet WAN**
- Connection Type
- DNS** (Red Arrow)
- MAC Address
- Wireless
- Channel and SSID
- Security
- Wireless Bridging
- Use as Access Point
- Firewall
- Virtual Servers
- Client IP Filters
- Automatic from ISP
- DNS Address >**
- 208 . 67 . 222 . 222
- Secondary DNS Address > 208 . 67 . 220 . 220

DHCP Server Enabled

Start IP address: 192 . 168 .

Maximum number of users: 50

IP address range: 192.168.192.168

Client lease time: 1440 Minutes

Static DNS 1: 0 0 0 0

Static DNS 2: 0 0 0 0

Static DNS 3: 0 0 0 0

WINS: 0 0 0 0

Domain Name Server (DNS) Address

Get Automatically from ISP

Use These DNS Servers

Primary DNS

Secondary DNS

Subnetmask: 255.255.255.0

3. Enter the DHCP server lease time.

DHCP Server Lease Time: 1 Day(s) 0 Hours 0 Minutes

4. Automatically set DHCP reservations on DHCP IP allocation.

DHCP Reservation: Enable Disable

5. Set the DNS servers allocated with DHCP requests.

DHCP DNS Type: Default Servers Custom Servers

Primary DNS: 192.168.0.251 (Red Circle)

Secondary DNS: 208.67.222.123

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) gives you with IP Address information and/or a username and password.

Host Name :

Use Unicasting : (compatibility for some DHCP Servers)

Primary DNS Server : 208.67.222.222 (Red Circle)

Secondary DNS Server : 208.67.220.220

MTU : 1500 (bytes) MTU default = 1500

MAC Address : 00:05:5d:ce:b3:8d

Clone Your PC's MAC Address

Renew DHCP leases.

Windows: ipconfig/renew

Linux: sudo dhclient

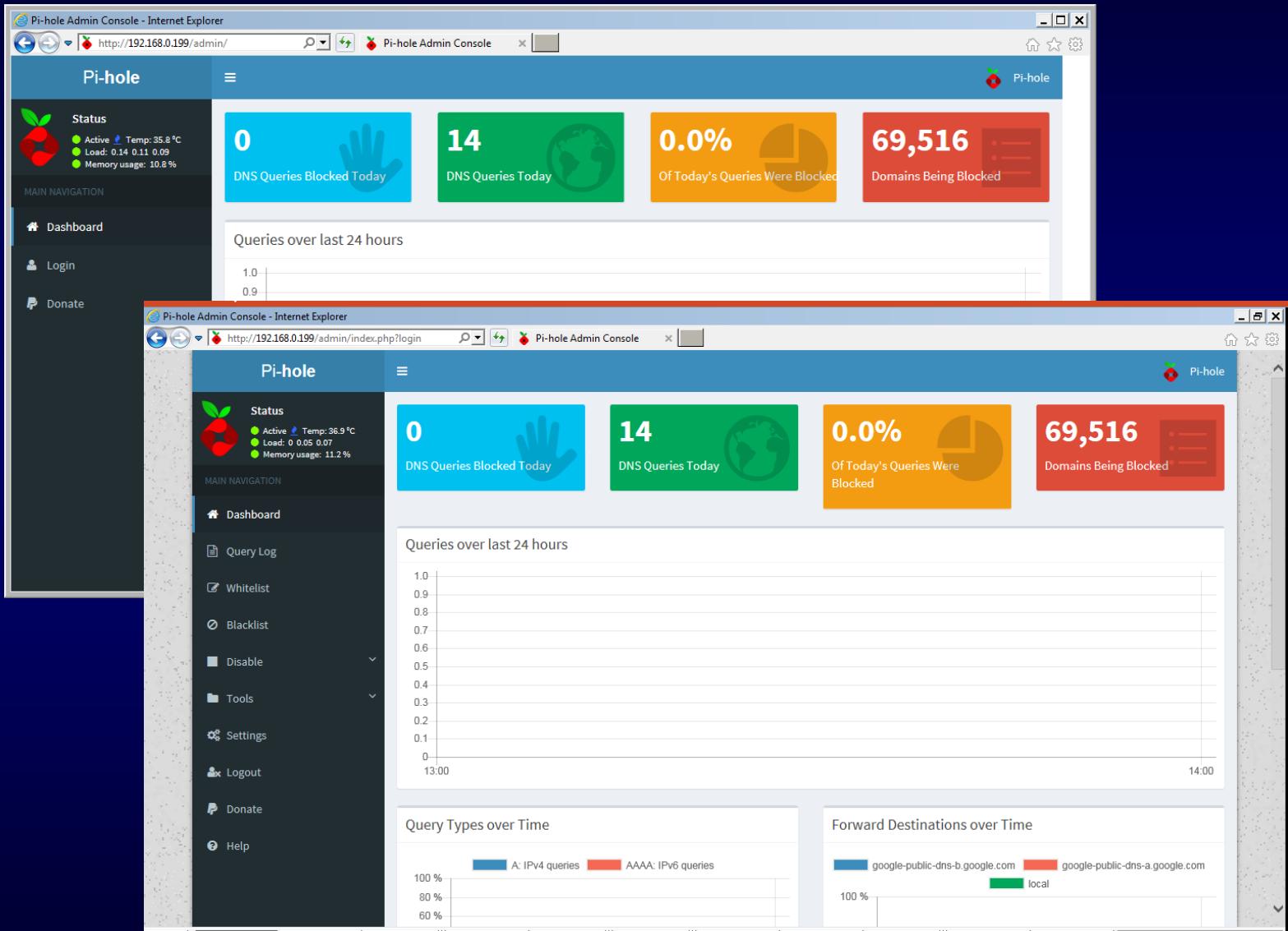
Other: unplug/plugin or off/on

That's It!

All of your devices are now filtering their DNS queries through the Pi-Hole. Most advertisements are now blocked, many malware programs are now prevented from dialing back home. What more do you want?

Just Kidding!!!

Now Let's Look At The GUI



Open a web browser and go to `HTTP://<YOUR IP>/admin`. Click on “Login” and enter the password provided during your installation. More information is provided.

Go ahead and take a few minutes to look around the GUI, but try not to make any changes to the settings yet.

Settings

- Most of this you won't want to change. If you need to use the built-in DHCP server, here's where you can do it.
- On the right side you can see the Pi-Hole's various Block Lists. We'll talk about adding new sources shortly.

The screenshot shows the Pi-hole Settings interface. On the left, there are two main sections: "Networking" and "Pi-hole DHCP Server". The "Networking" section contains fields for "Pi-hole Ethernet Interface" (set to wlan0), "Pi-hole IPv4 address" (set to 192.168.0.199/24), "Pi-hole IPv6 address" (empty), and "Pi-hole hostname" (set to pihole-zero). The "Pi-hole DHCP Server" section has a checkbox for "DHCP server enabled" which is unchecked, and fields for "Range of IP addresses to hand out" (From: 192.168.0.201, To: 192.168.0.251) and "Router (gateway) IP address" (Router: 192.168.0.1). On the right, there are two sections: "Query Logging (size of log 316 bytes)" and "Pi-Hole's Block Lists". The "Query Logging" section shows "Current status: Enabled (recommended)" and a note that disabling will render graphs useless, with buttons for "Flush logs" and "Disable query logging". The "Pi-Hole's Block Lists" section is titled "Lists used to generate Pi-hole's Gravity" and lists several sources with checkboxes and delete icons: https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts, https://mirror1.malwaredomains.com/files/justdomains, http://sysctl.org/cameleon/hosts, https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist, https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt, and https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt.

More Settings

The screenshot shows the 'Upstream DNS Servers' section. It includes a table for 'Upstream DNS Servers' with columns for IPv4, IPv6, and Name. Predefined lists like 'Custom 1 (IPv4)', 'Custom 2 (IPv4)', 'Custom 3 (IPv6)', and 'Custom 4 (IPv6)' are listed. Below this is an 'Advanced DNS settings' section.

The screenshot shows the 'Ad lists' configuration. It displays two checked URLs: 'https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt' and 'https://hosts-file.net/ad_servers.txt'. A text input field for adding new URLs is also present. Buttons for 'Save' and 'Save and Update' are at the bottom.

Below are advanced DNS settings which will become more important in securing DNS in the near future!

The screenshot highlights the 'Advanced DNS settings' section, which contains options like 'never forward non-FQDNs' and 'never forward reverse lookups for private IP ranges'. It also includes a note about DNSSEC validation and interface listening behavior. Other sections shown include 'Web User Interface' (with 'Interface appearance' and 'CPU Temperature Unit' options), 'System Administration' (with buttons for 'Restart system', 'Restart DNS server', and 'Flush logs'), and 'Pi-hole FTL (Running)' and 'Pi-hole Teleporter' sections.

Above is where you can change your upstream DNS servers.

Additional lists

You can add any additional lists you want, but be careful to review them/know what's going to be in them. Would you really want to add this list? :

https://mirror1.malwaredomains.com/files/url_shorteners.txt

Some I use/recommend:

- <https://mirror1.malwaredomains.com/files/spywaredomains.zones>
- <https://mirror1.malwaredomains.com/files/freewebhosts.txt>
- <http://securemecca.com/Downloads/hosts.txt>
- <https://raw.githubusercontent.com/reek/anti-adblock-killer/master/anti-adblock-killer-filters.txt>
- <https://pgl.yoyo.org/adservers/serverlist.php?hostformat=bindconfig;showintro=0;zonefilename=/etc/bind/null.zone.file;mimetype=plaintext>

Blacklists / Whitelists

Blacklists:

- Want to block Facebook/MySpace?
- Block all .ru or .cn sites?
- What about the blocking the ex's website so you don't troll him/her when you're drunk?
- Remember, the Blacklist is manual, so if you later come up with a reason to visit a Russian website, you need to update the list.

Whitelists:

- You actually like a certain ad site?
- What about blocking all URL shorteners EXCEPT one or two you trust?
- Someone came up with a business need to visit one Dynamic DNS site?
- ← Same applies to the Whitelist. When the exception is no longer needed, you must remove it manually.

Food For Thought

- Know your network!
- Look for sudden spikes in DNS requests.
- New Top Domain? Why?
- Top Clients list: why is the “smart” thermostat suddenly making a lot of DNS requests?
- Try using the Blacklist to prevent automatic updates for Windows 10 if the reboots annoy you. **
- Know your network!!!

- Know your network!
- You can run Pi-Hole on almost any Linux OS, why not VM it for your corporate environment?
- Feed the logs to your SIEM.
- Use DNS logs to track infections.
- Instead of resolving blocked DNS entries to the Pi-Hole, send them to a HoneyPot/HoneyNetwork and monitor the activity.
- Know your network!!!

QUESTIONS?

