DNS Blackholing with Pi-Hole

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

WHAT?

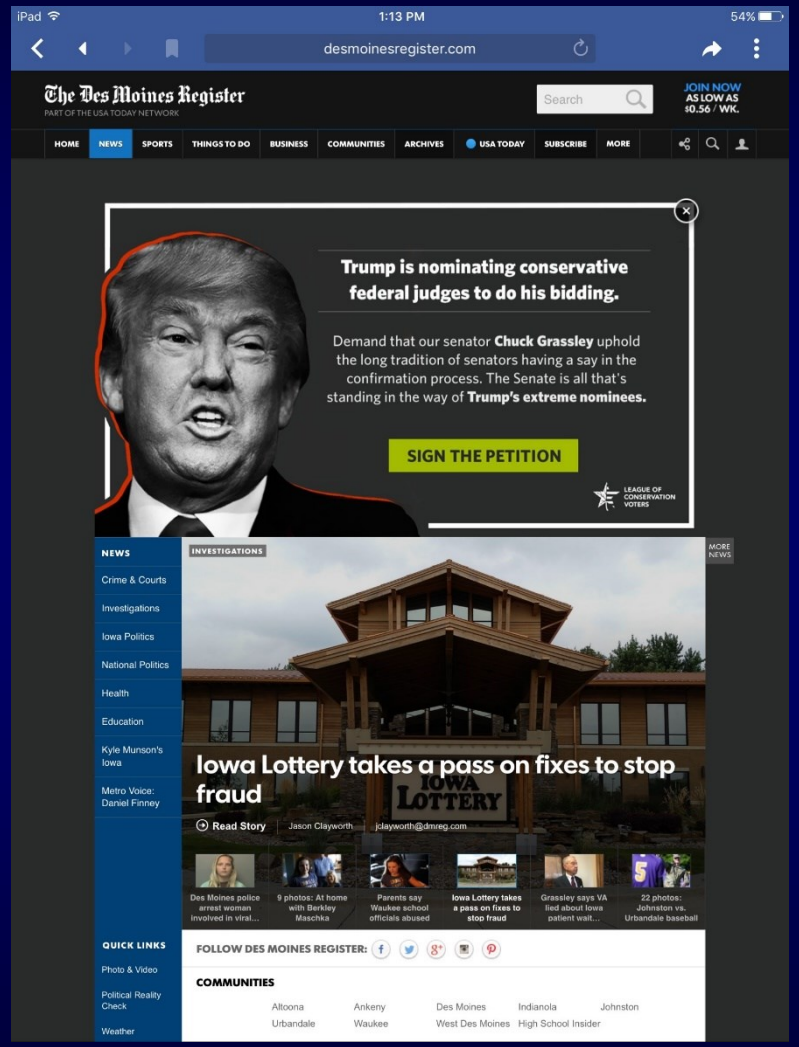
Create a system to block advertisement sites

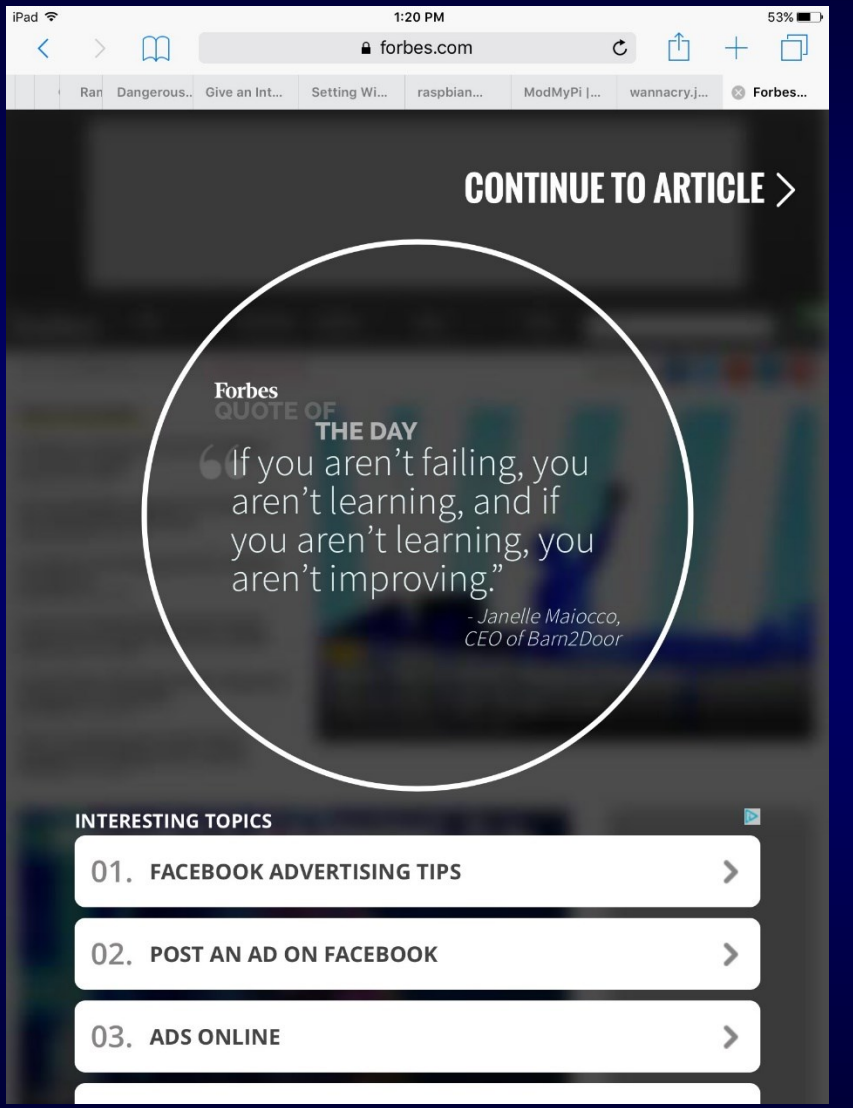
Create a system to block malware & C2 sites

Do this to protect the entire network, automatically

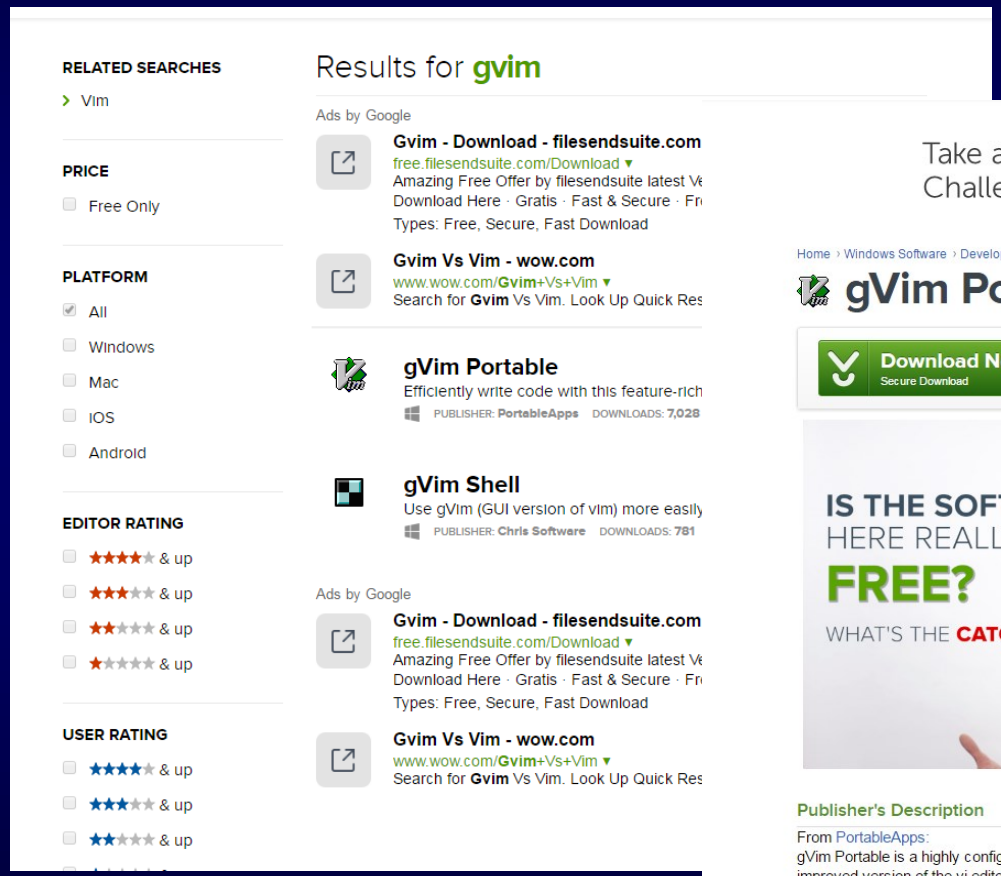
Do this for very little money

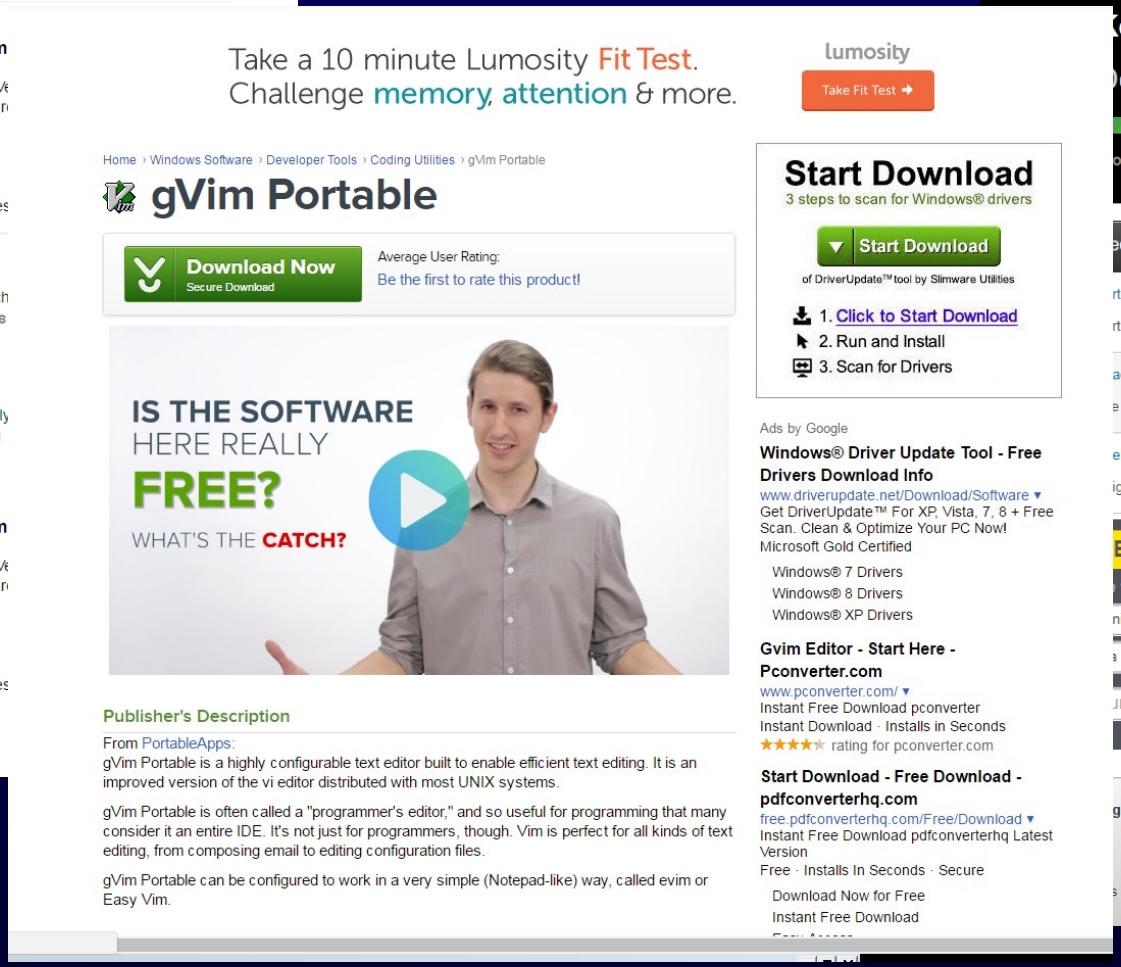
Adverts blocking your news story

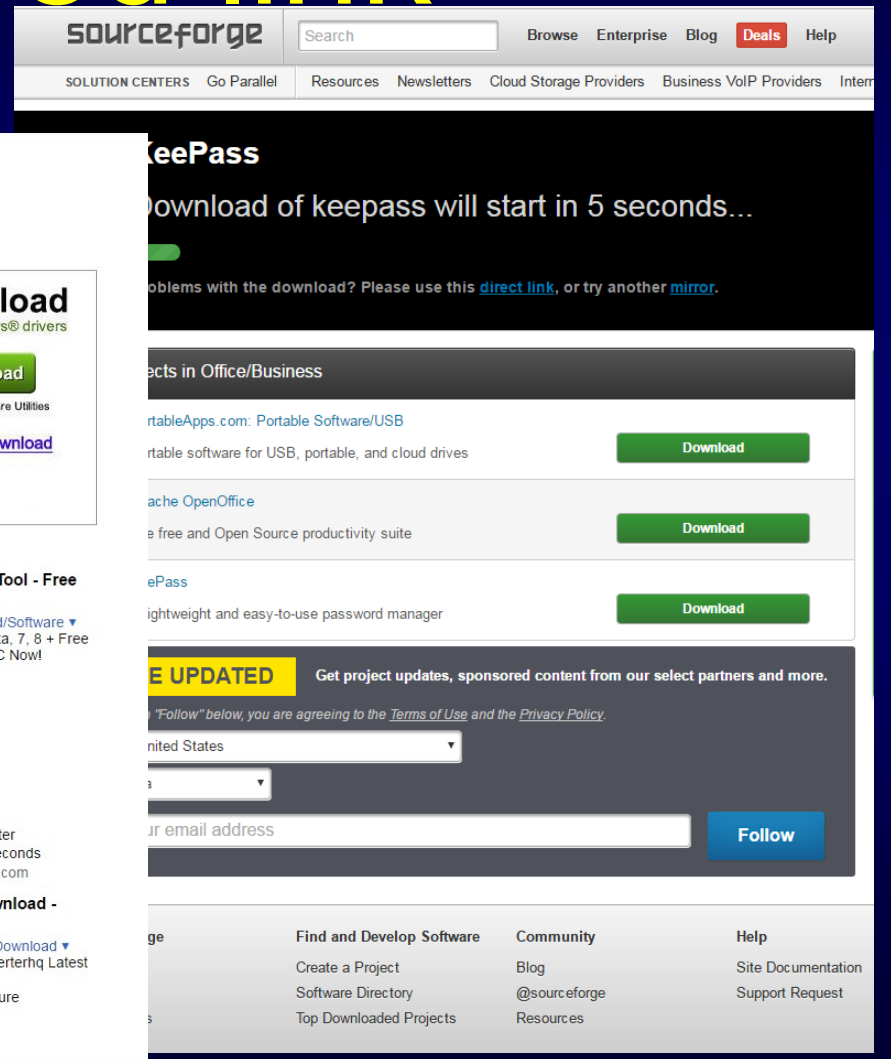




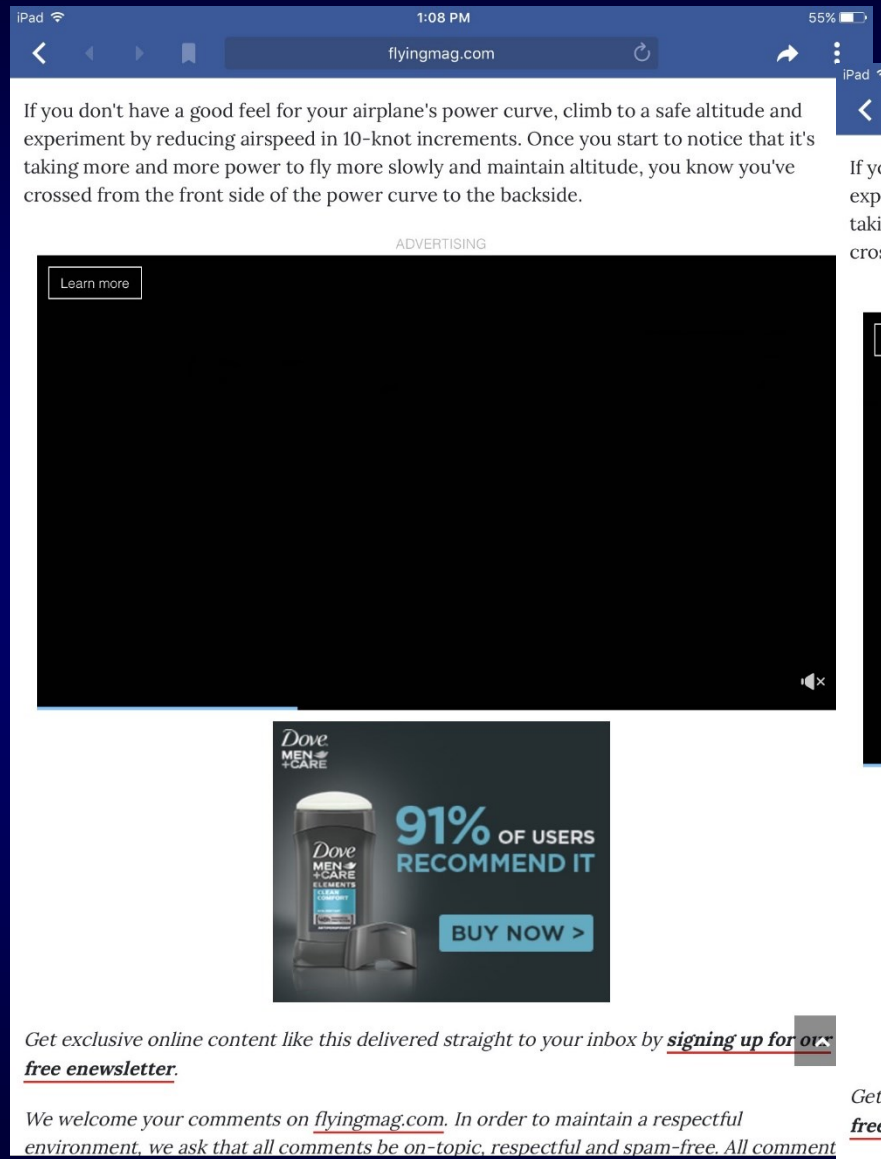
Adverts tricking you into clicking them instead of the desired link

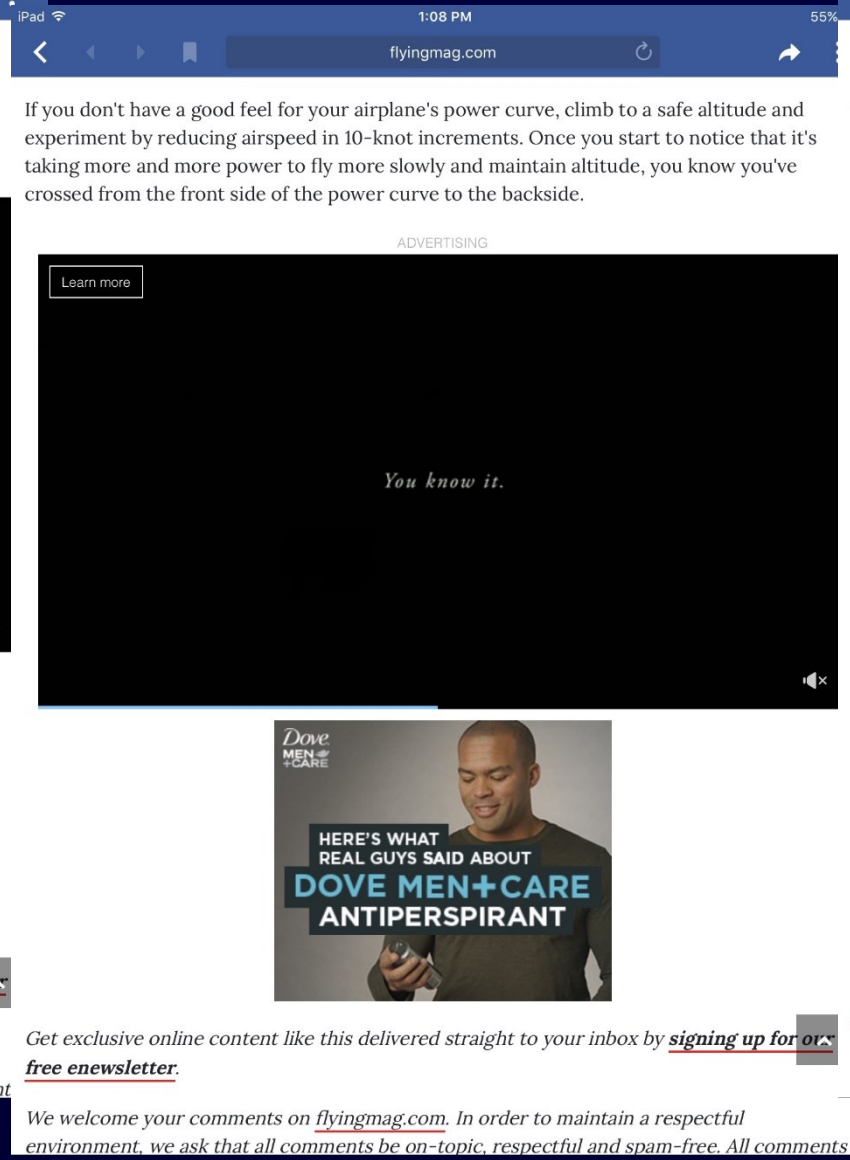


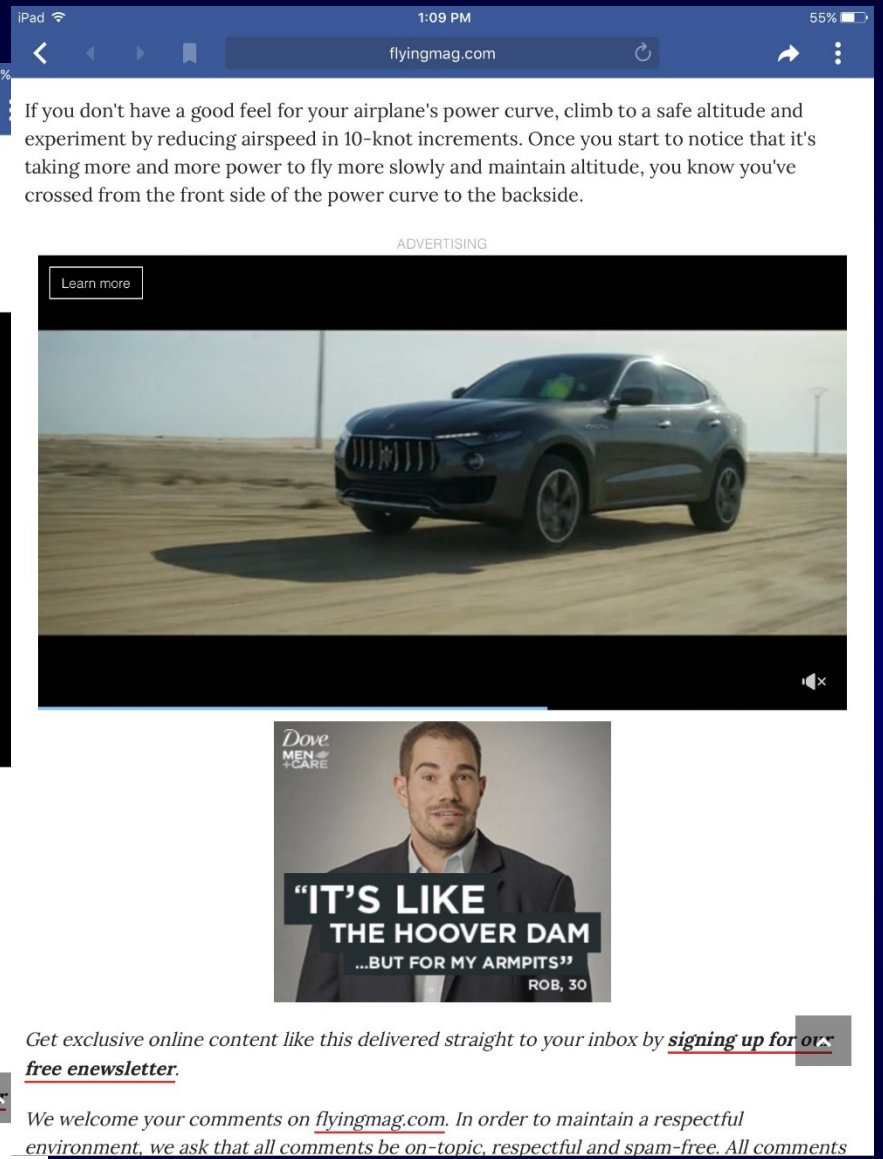




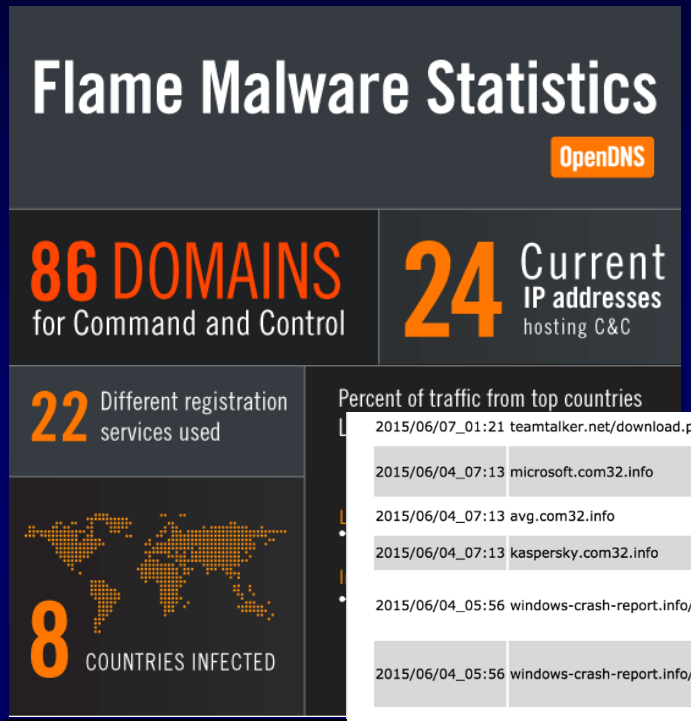
Adverts eating away at your bandwidth

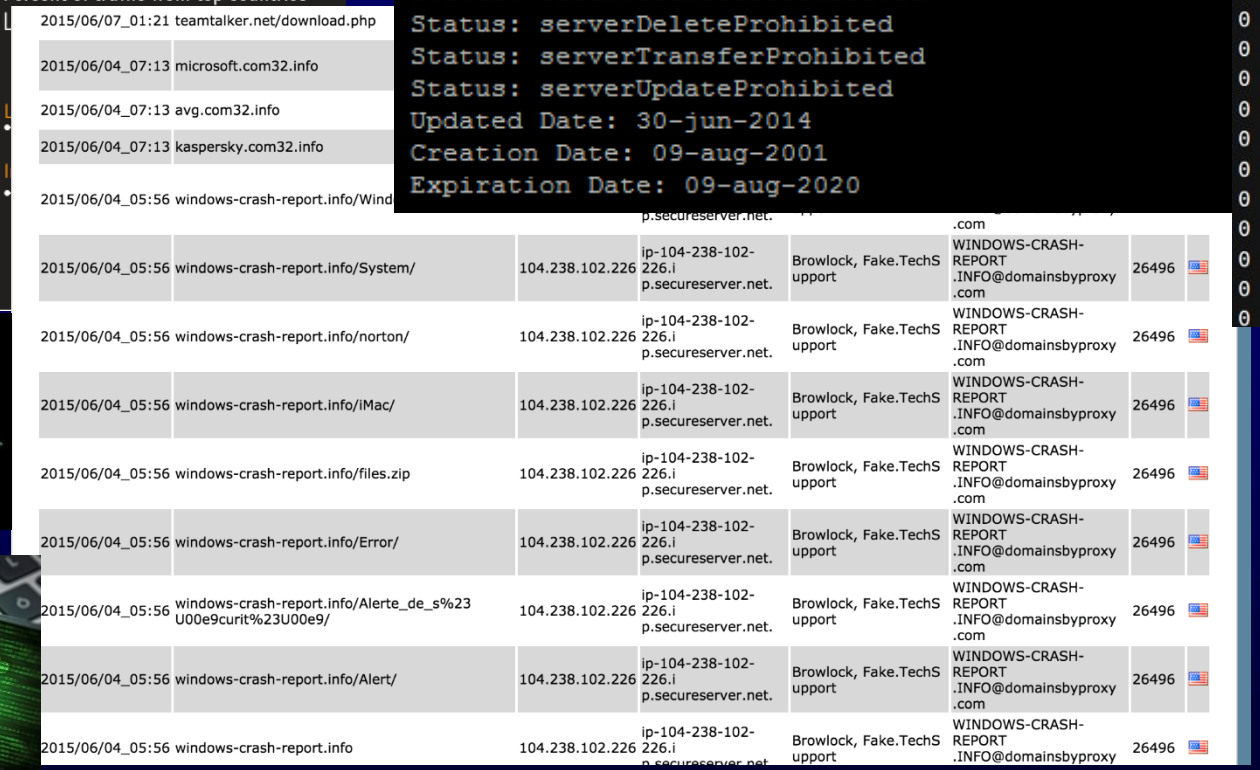






Want to block most malware from reaching out?

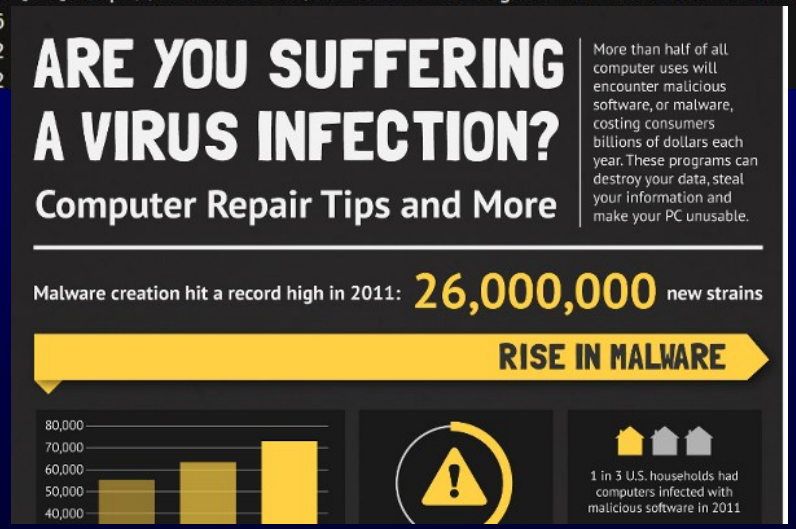




2015/06/07_01:21	teamtalker.net/download.php					
2015/06/04_07:13	microsoft.com32.info					
2015/06/04_07:13	avg.com32.info					
2015/06/04_07:13	kaspersky.com32.info					
2015/06/04_05:56	windows-crash-report.info/Wind		p.secureserver.net.		.com	
2015/06/04_05:56	windows-crash-report.info/System/	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info/norton/	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info/iMac/	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info/files.zip	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info/Error/	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info/Alerte_de_s%23U00e9curit%23U00e9/	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info/Alert/	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496
2015/06/04_05:56	windows-crash-report.info	104.238.102.226	ip-104-238-102-226.ip.secureserver.net.	Browlock, Fake.TechSupport	WINDOWS-CRASH-REPORT.INFO@domainsbyproxy.com	26496

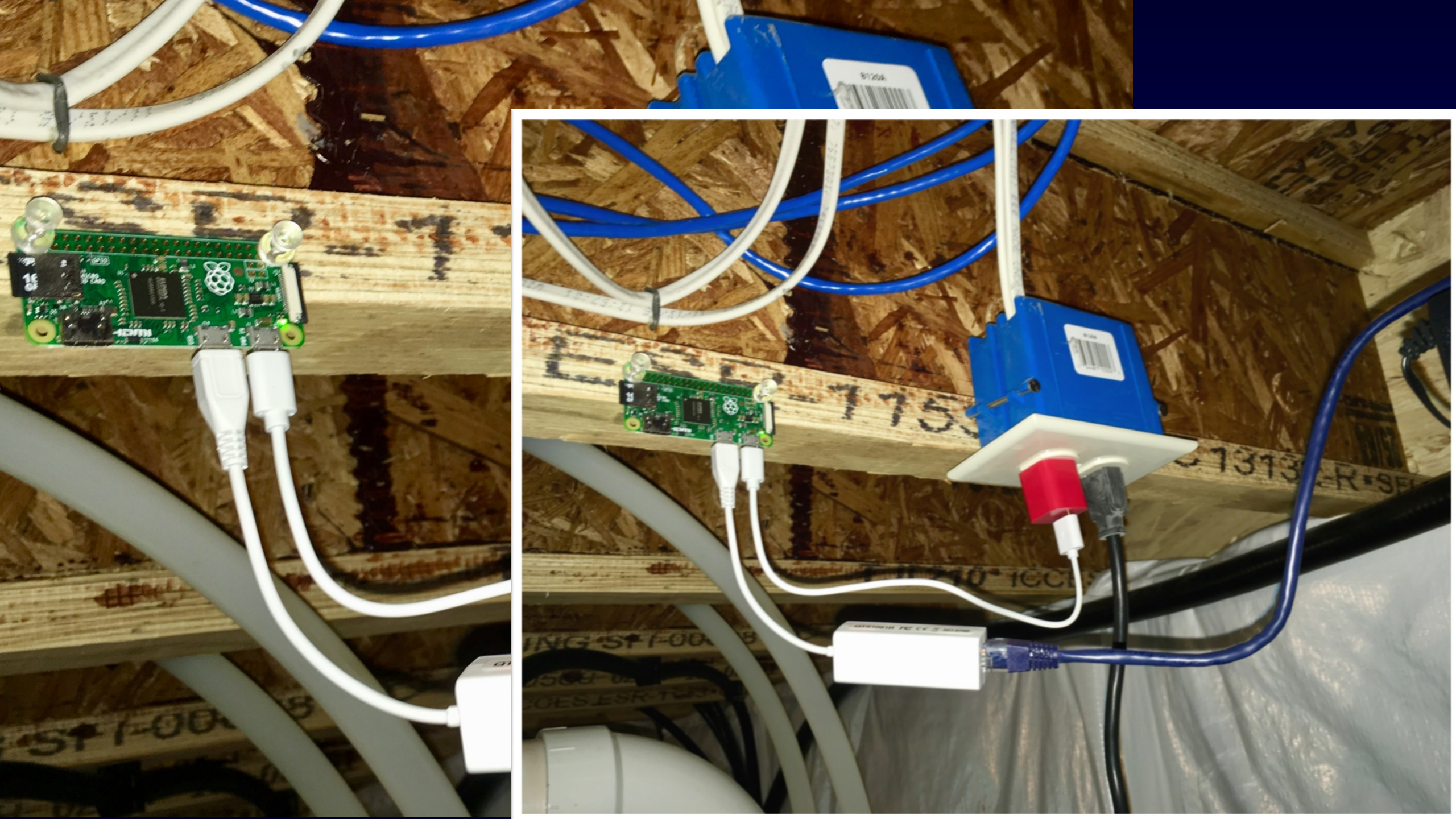
```
Domain Name: REDIRECTME.NET
Registrar: VITALWERKS INTERNET SOLUTIONS LLC DBA NO
Whois Server: whois.no-ip.com
Referral URL: http://www.no-ip.com
Name Server: NS7.MICROSOFTINTERNETSAFETY.NET
Name Server: NS8.MICROSOFTINTERNETSAFETY.NET
Status: clientTransferProhibited
Status: serverDeleteProhibited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

```
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
0 / 6
0 / 2
0 / 2
```

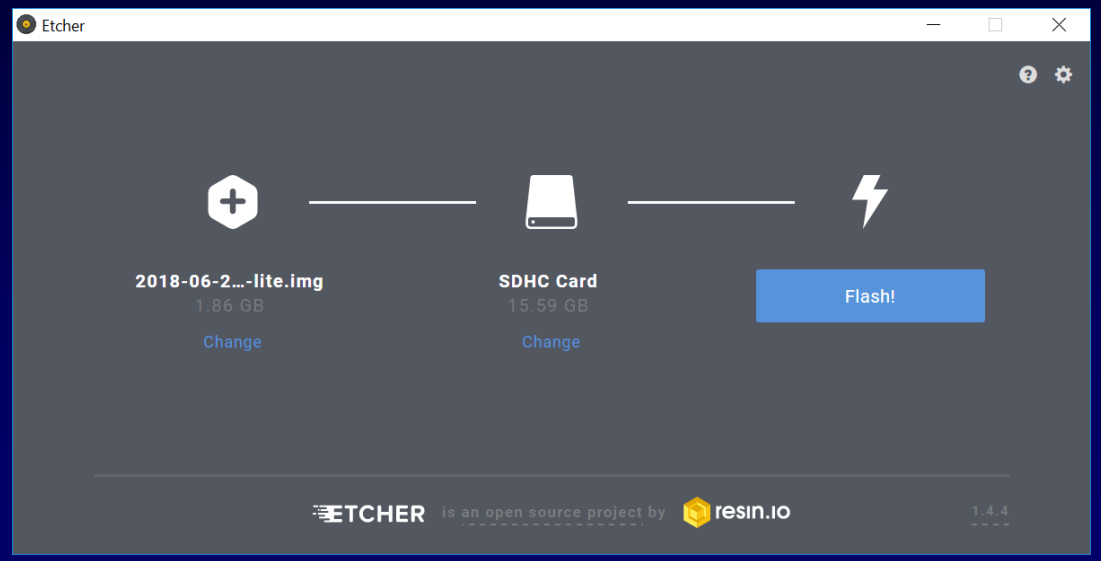


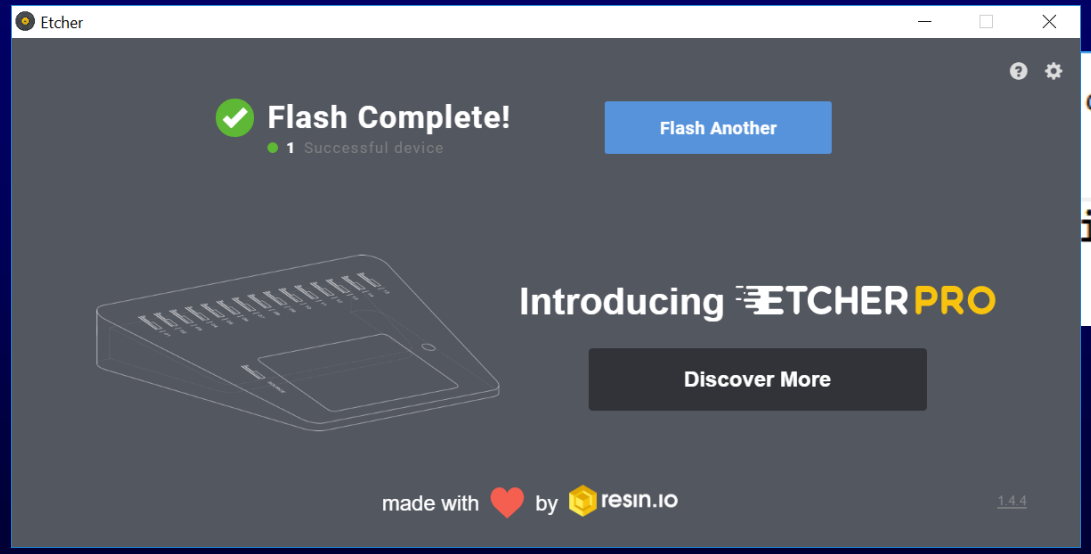
Good News!
I'll show you how.

Pi-hole™
Network-wide ad blocking
via your own hardware

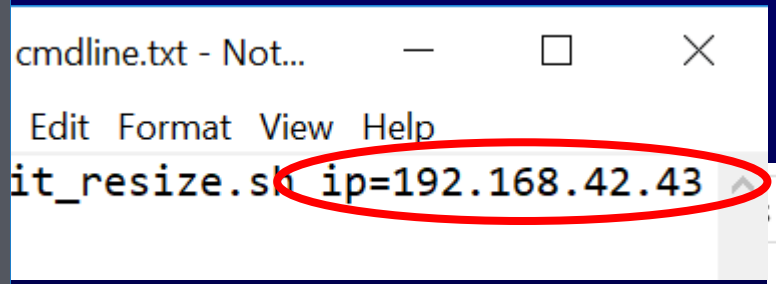


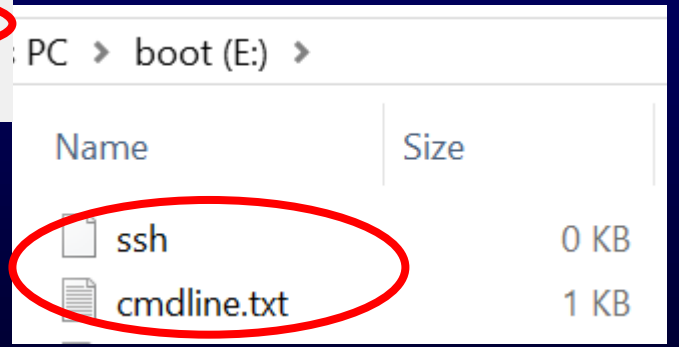
Prepare a Fresh Raspbian Lite





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.



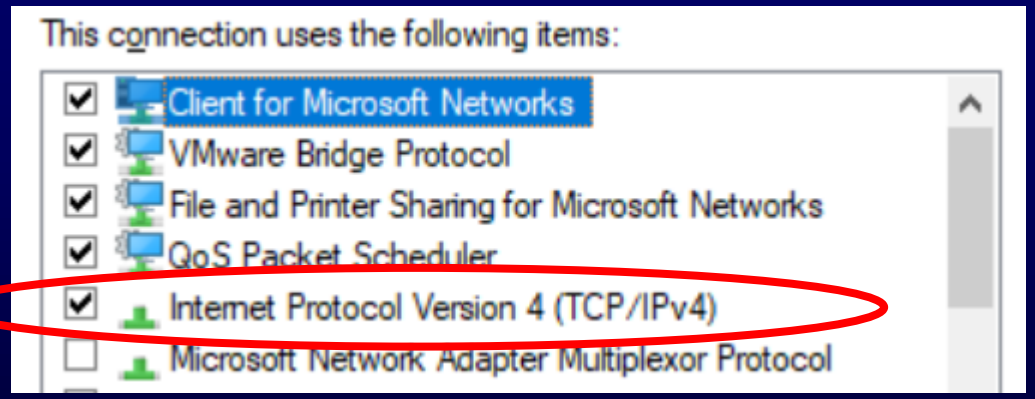


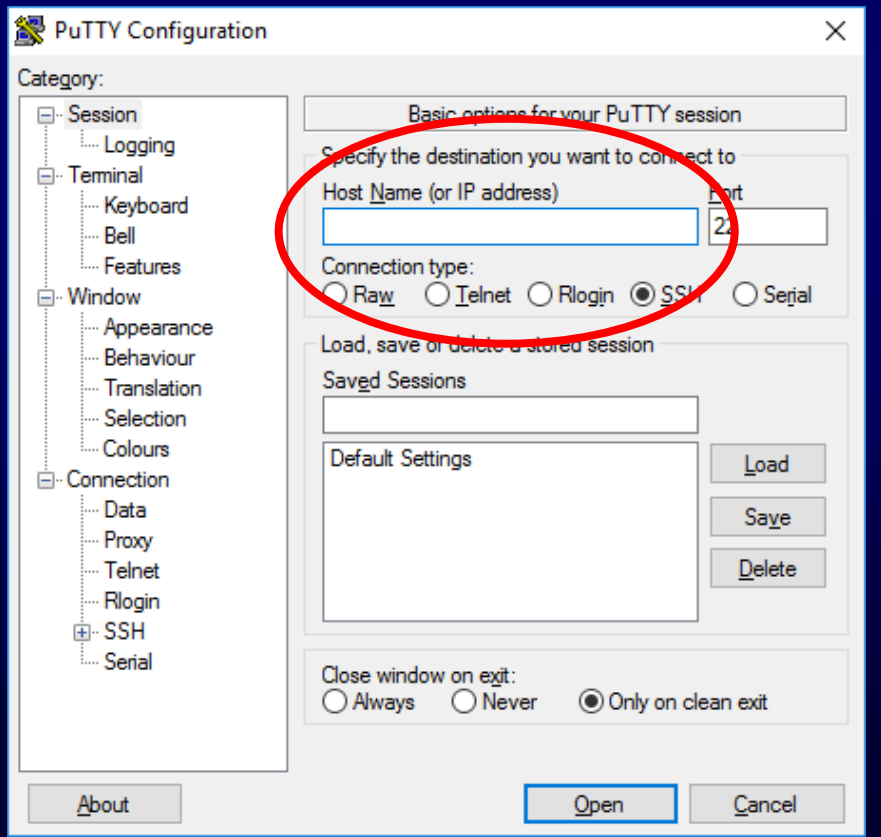
https://etcher.io/

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 `192.168.42.2XX`.
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
```

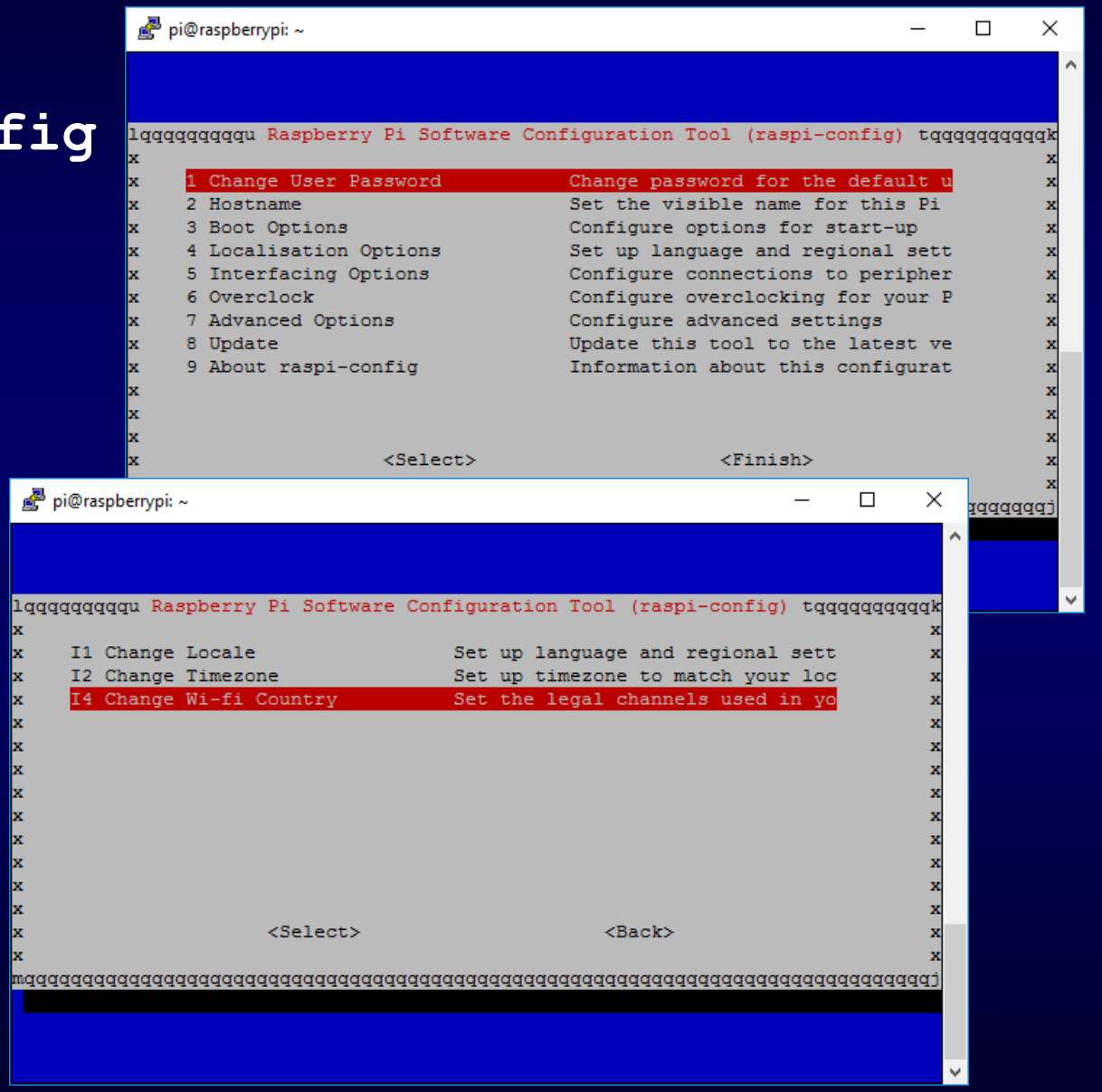
- Change the password

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

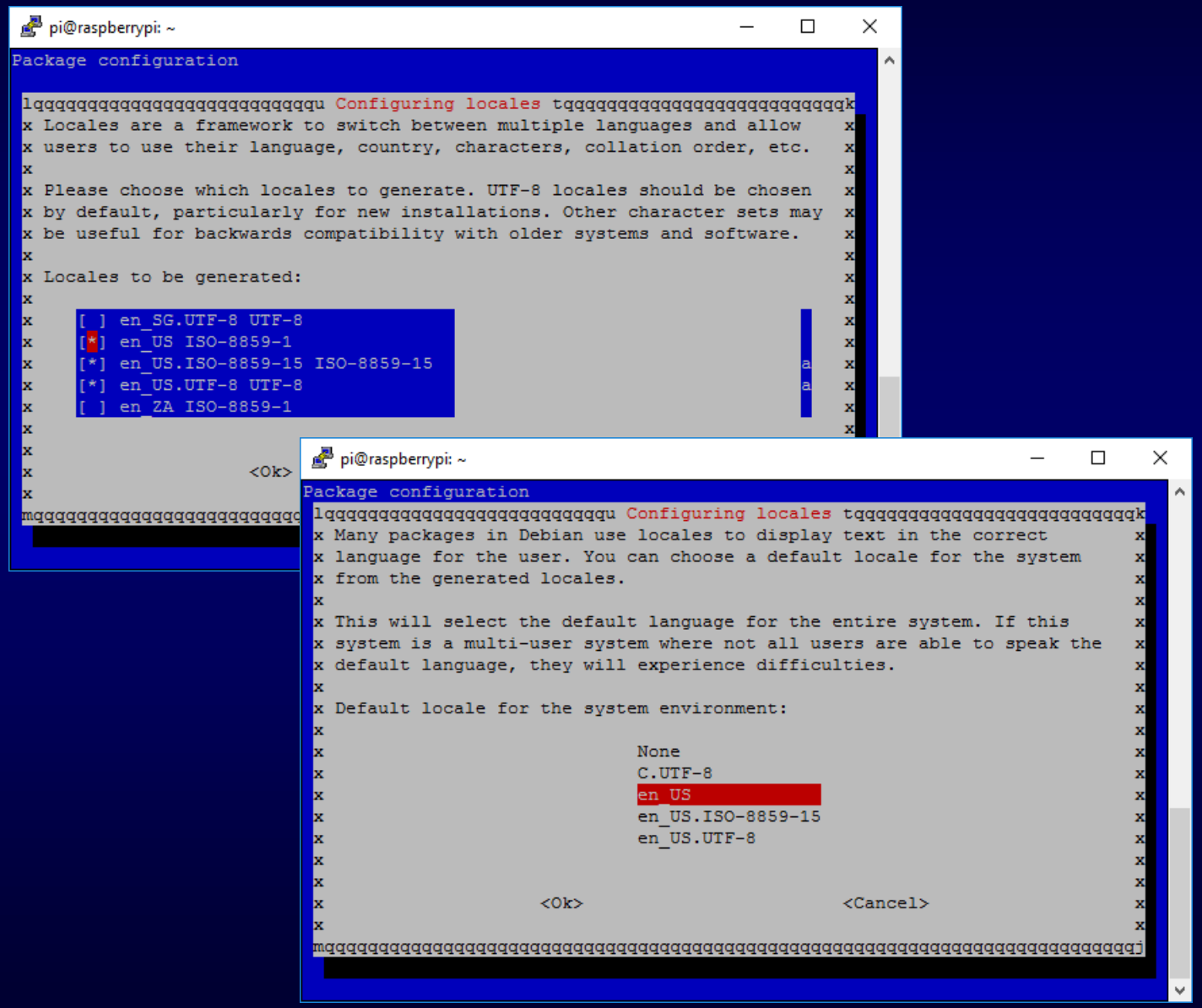
- Change the hostname

(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



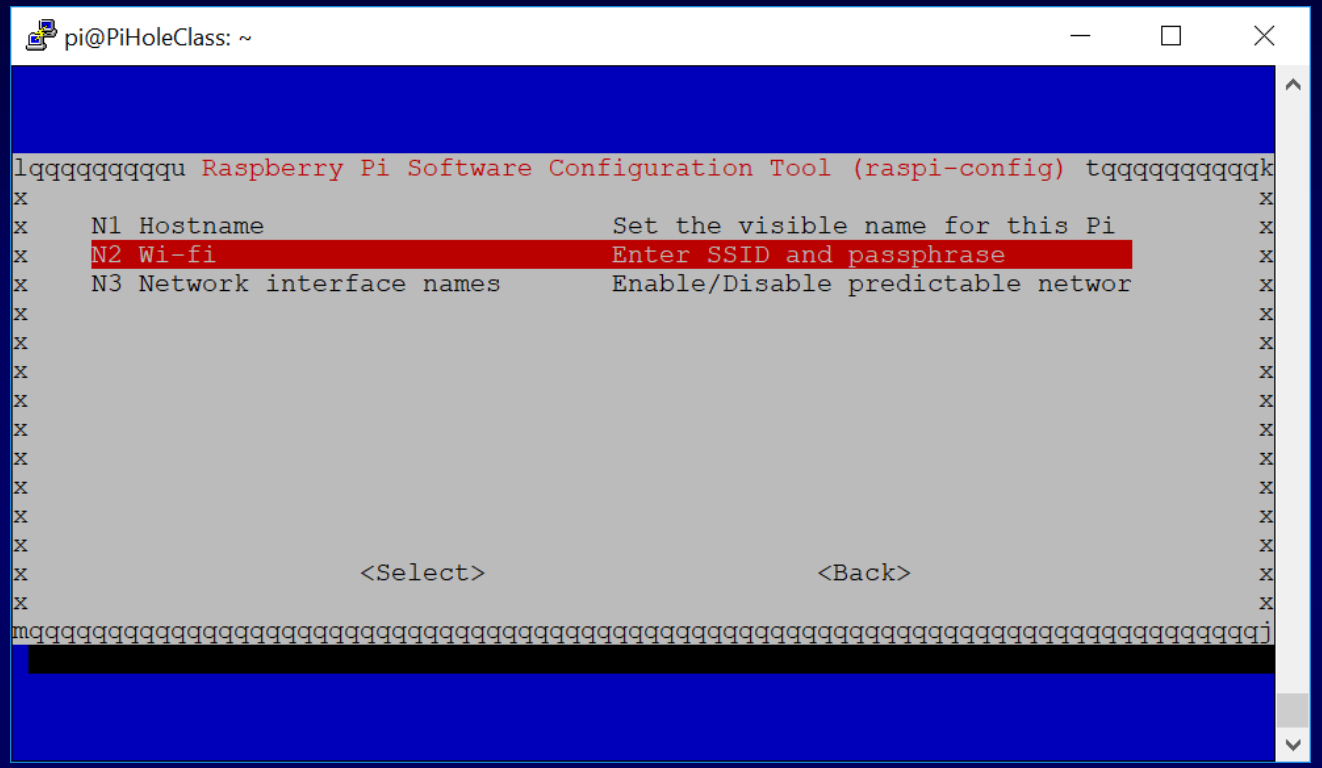
Basic Config continued



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

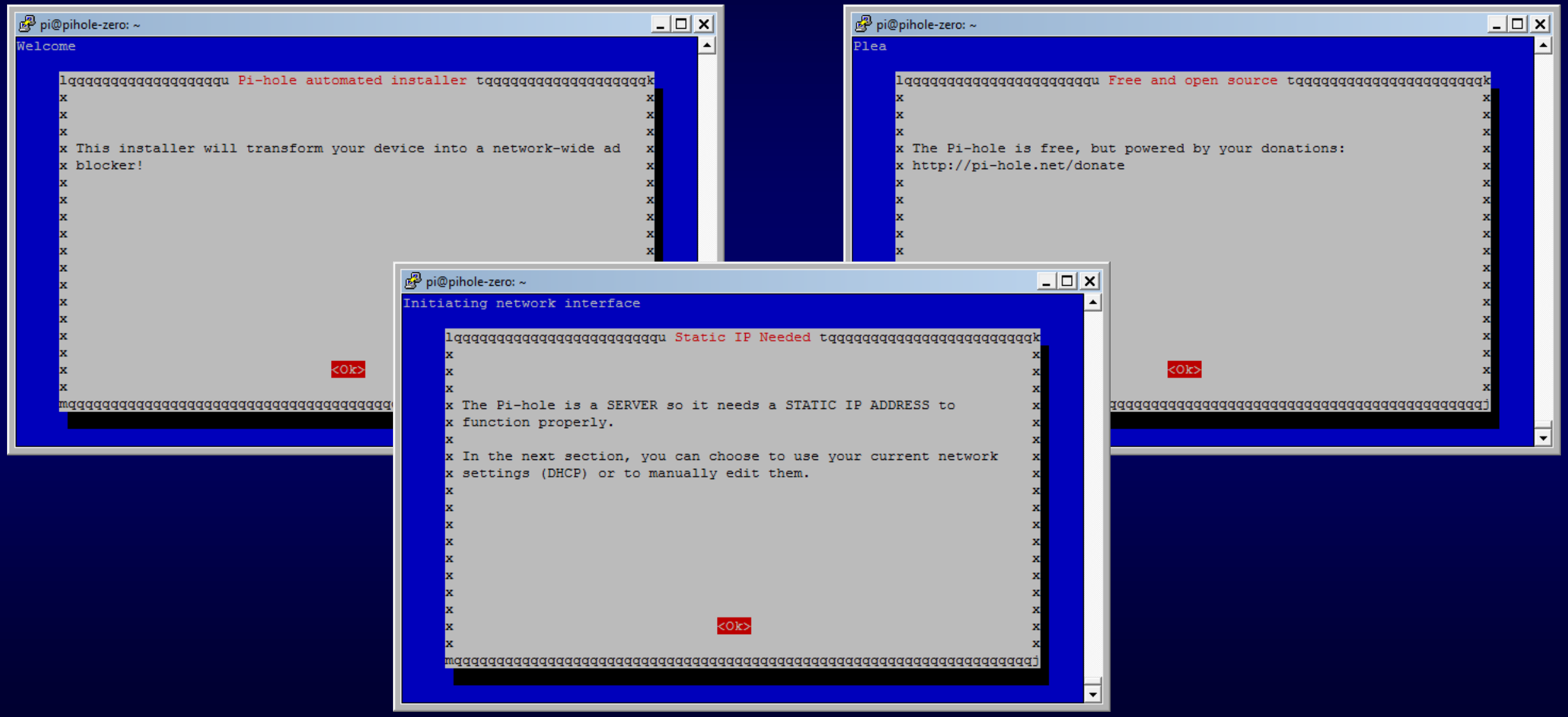
```
$ git clone --depth 1 https://github.com/\
    pi-hole/pi-hole.git  Pi-Hole
$ cd Pi-Hole
$ less automated\ install/basic-install.sh

$ sudo bash automated\ install/basic-install.sh
```

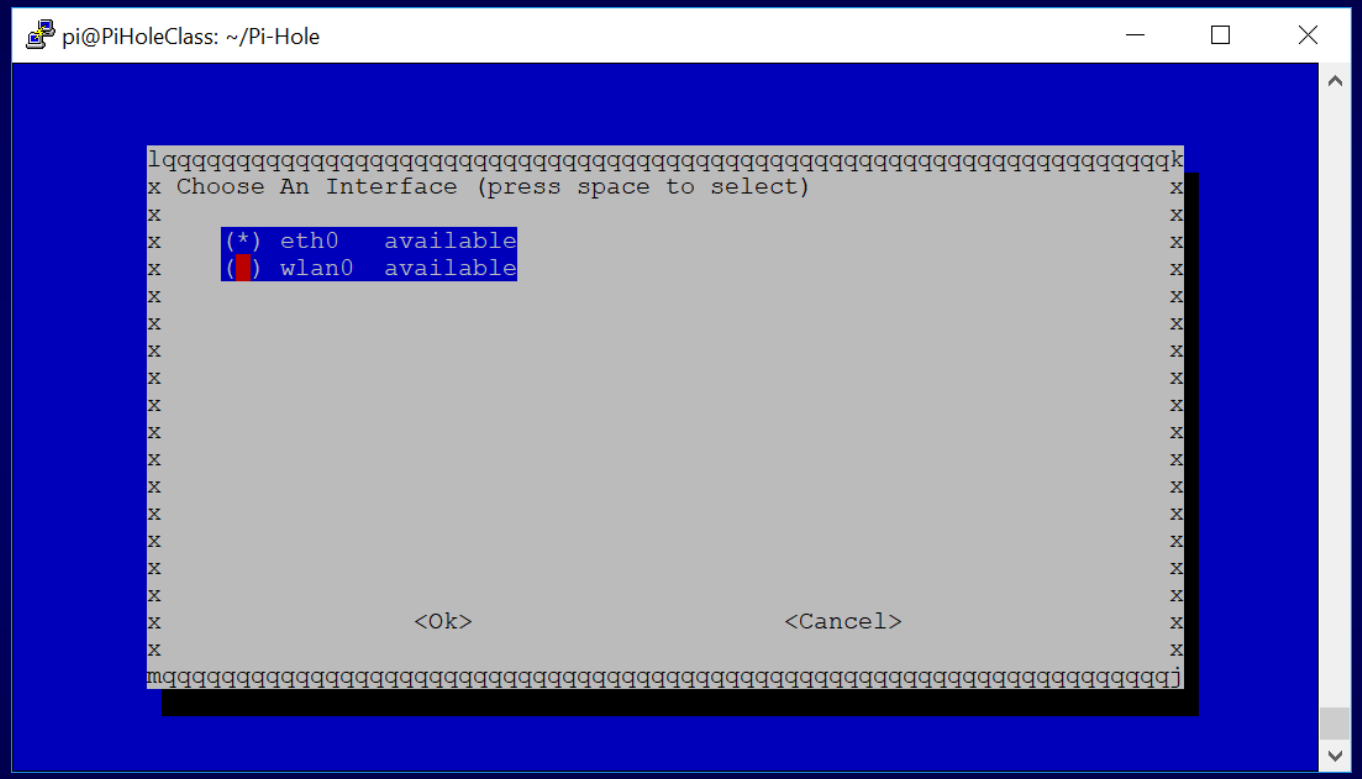
← We start by cloning the git repository, then we examine the install script before finally running it as root.

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



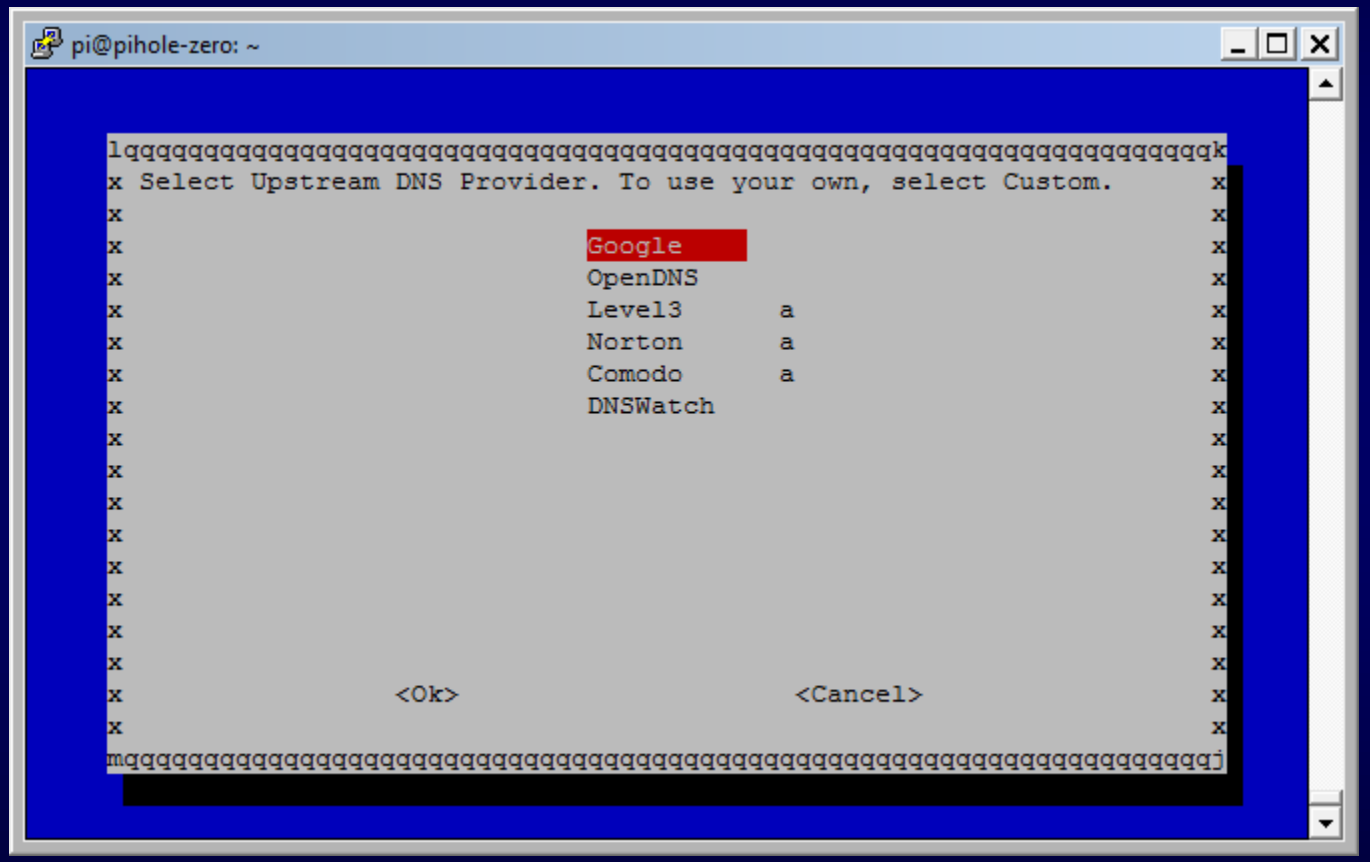
Choose Interface



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`?

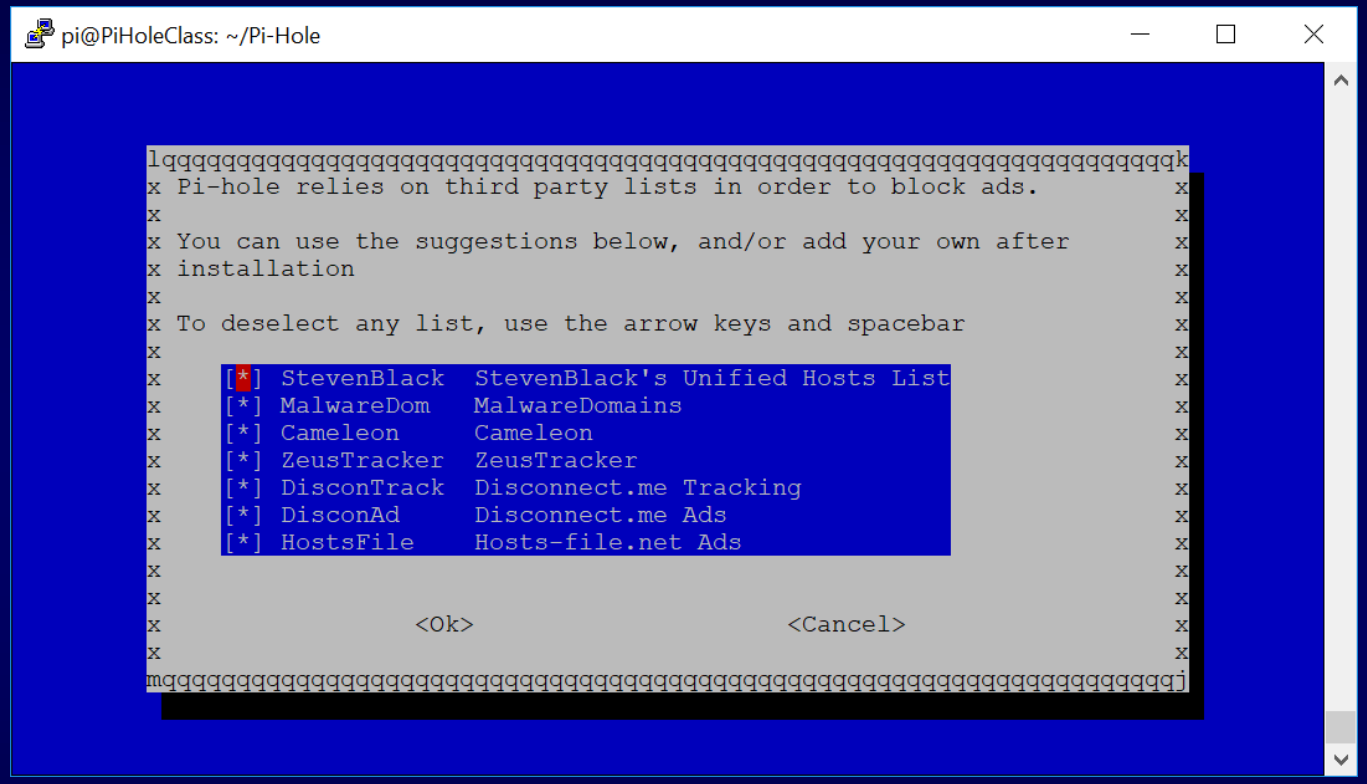
Choose Upstream DNS Provider



- 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

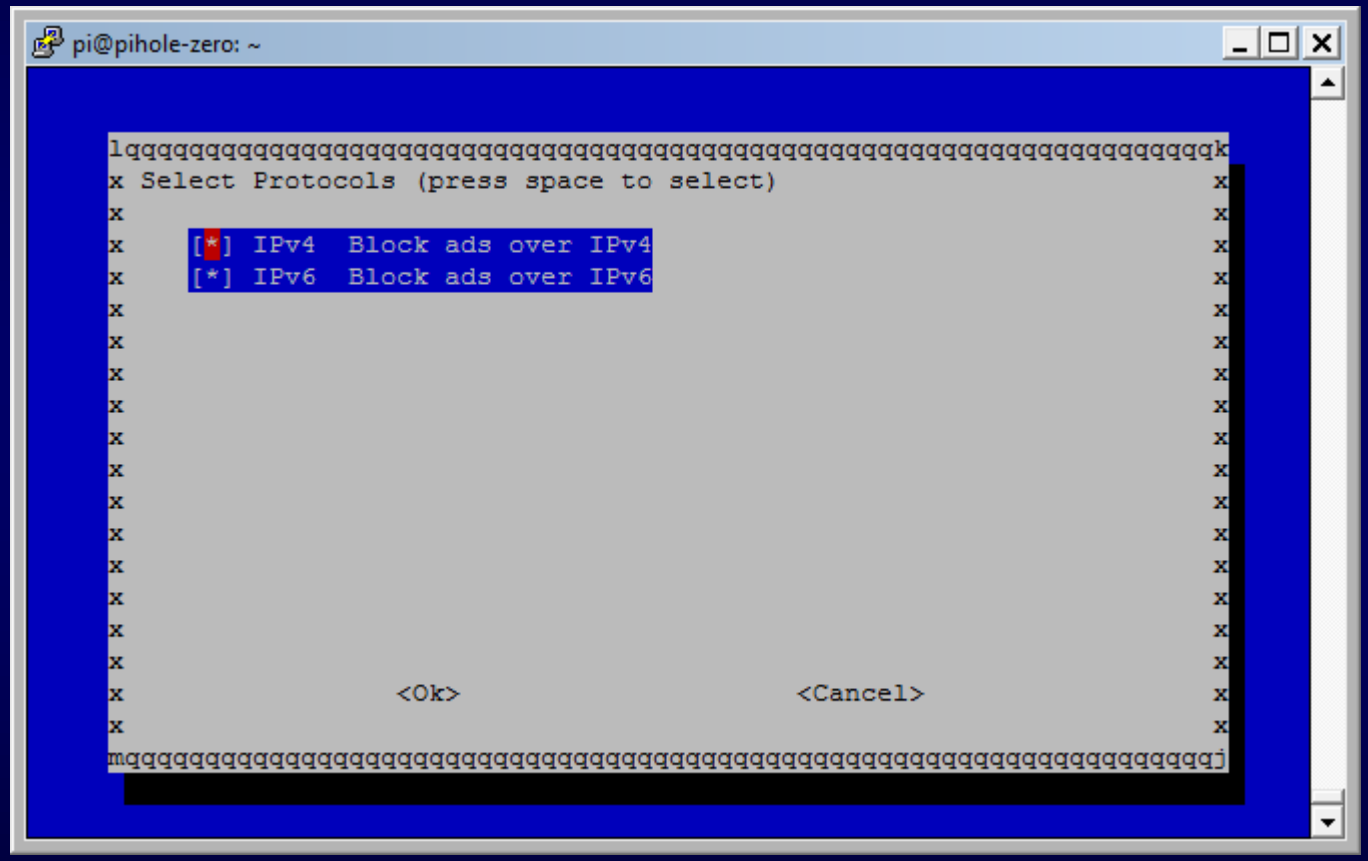


You can choose lists to include from the default set provided on the next screen. If you wish to add or remove any later, you can still do this via the web admin portal.

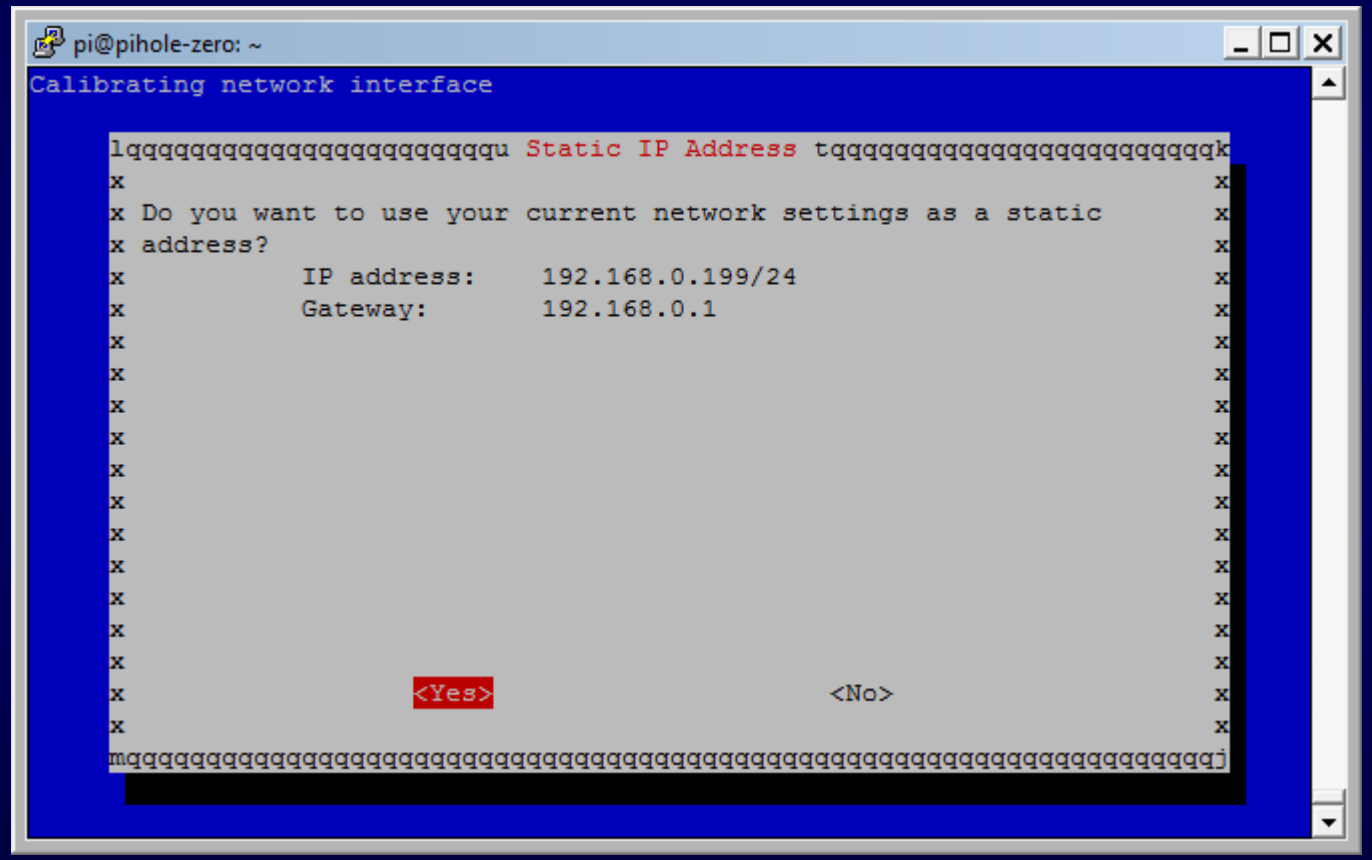
IPv4 and/or IPv6

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

What are reasons for/against also enabling IPv6?



Static IP Address

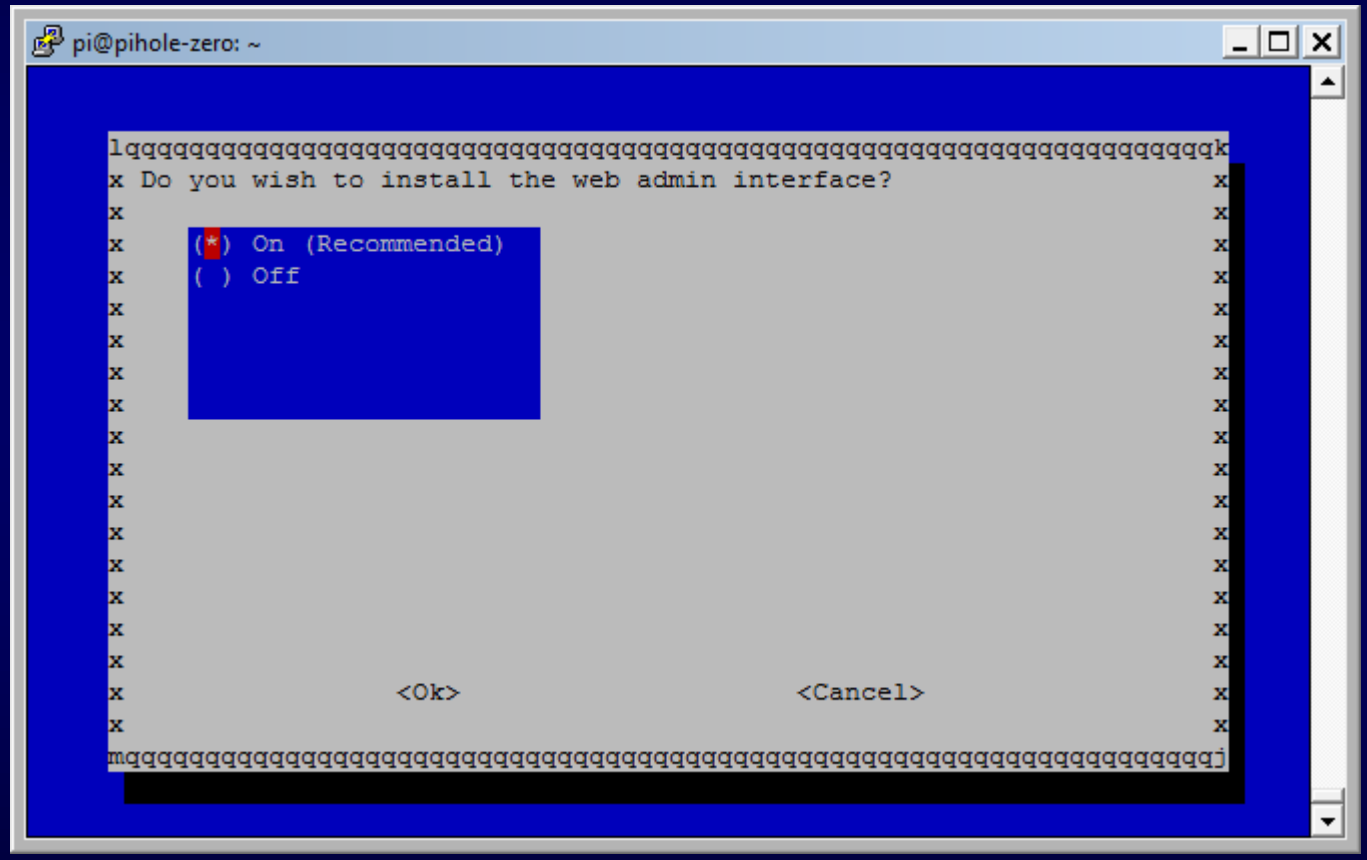


- If you choose <Yes> what you see on the screen is what you get.
- If you choose <No> you'll get a dialog to enter your desired IPv4 address.
- This WILL change your existing system settings.

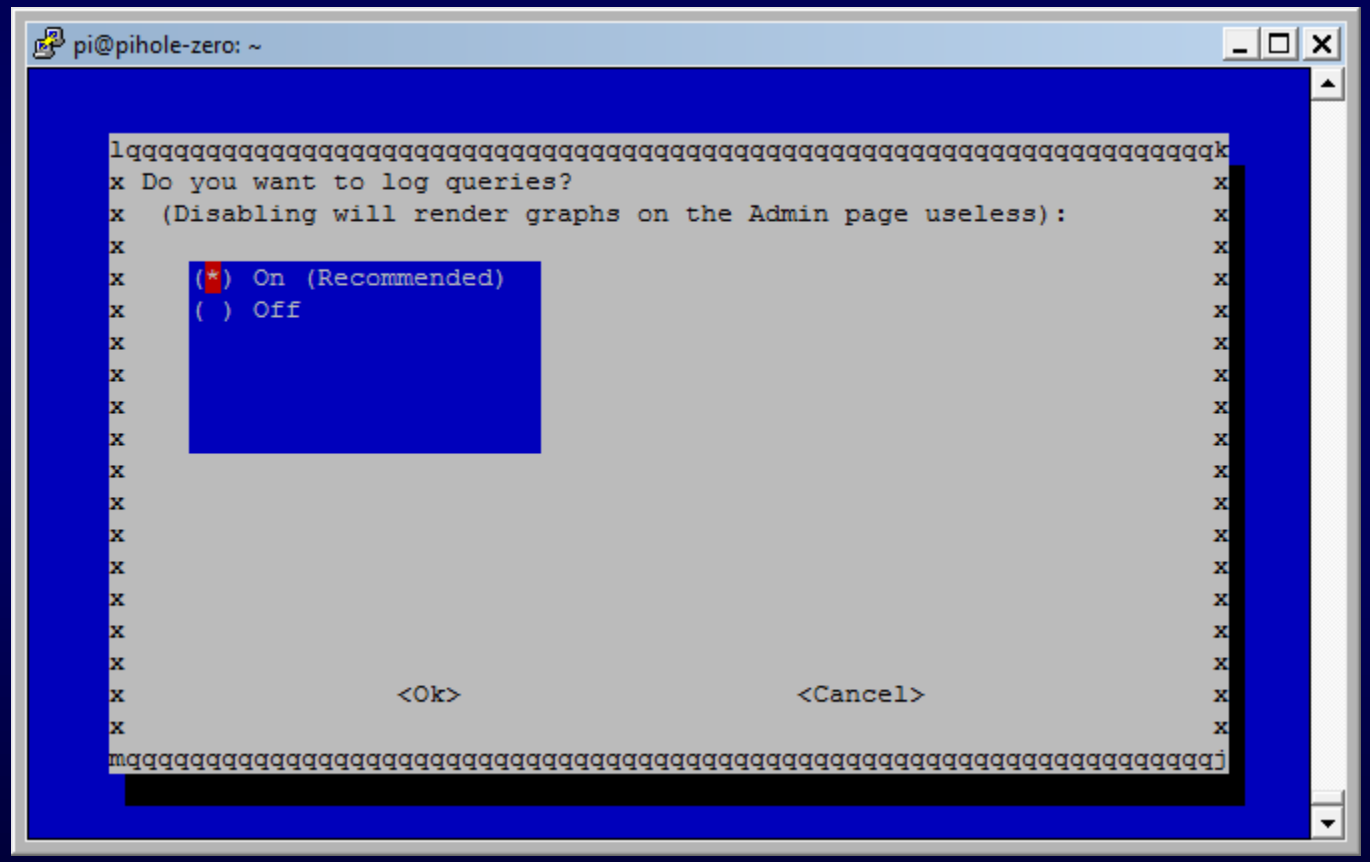
- This MIGHT generate an IP conflict message.
  KNOW YOUR NETWORK!

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.

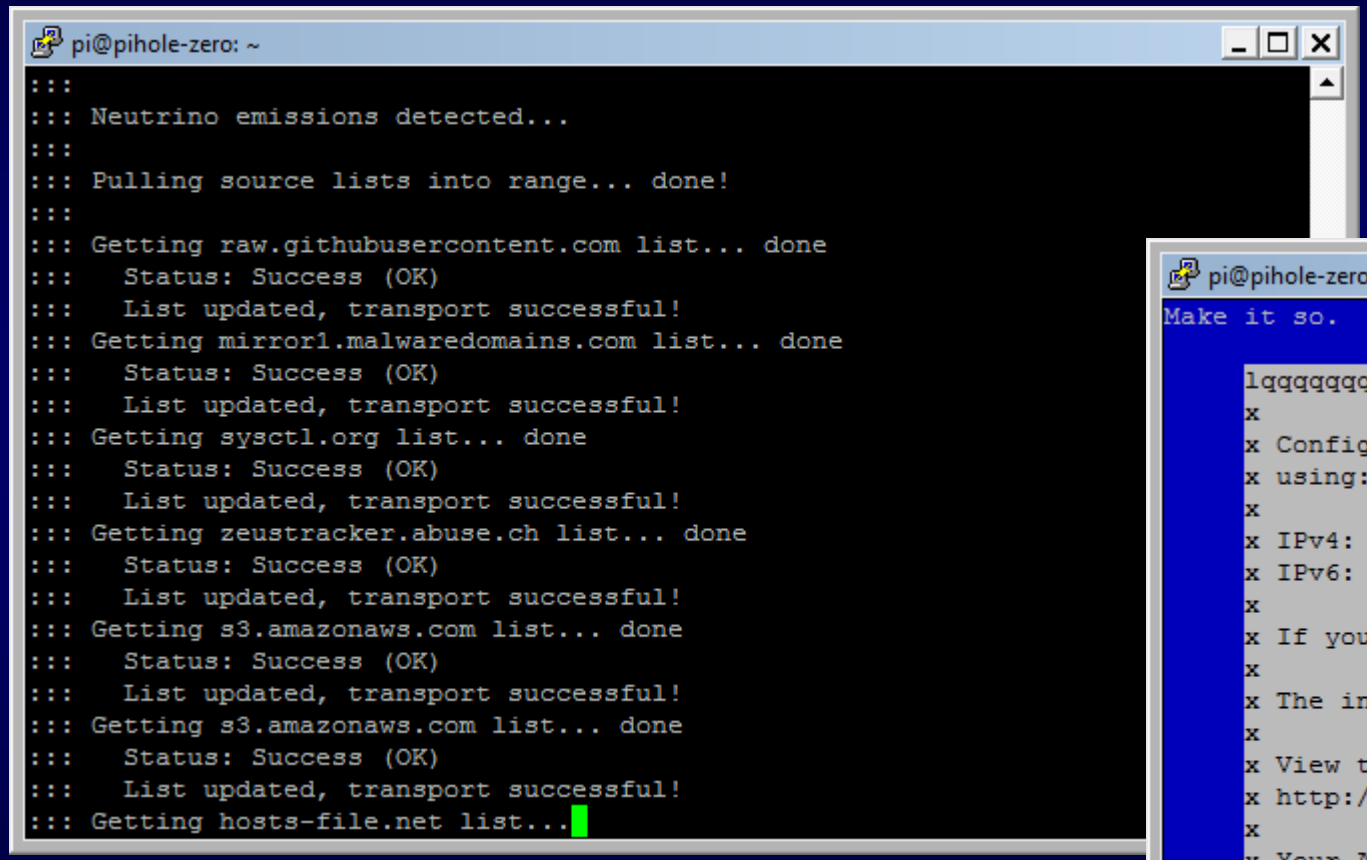


Want to Log Queries?

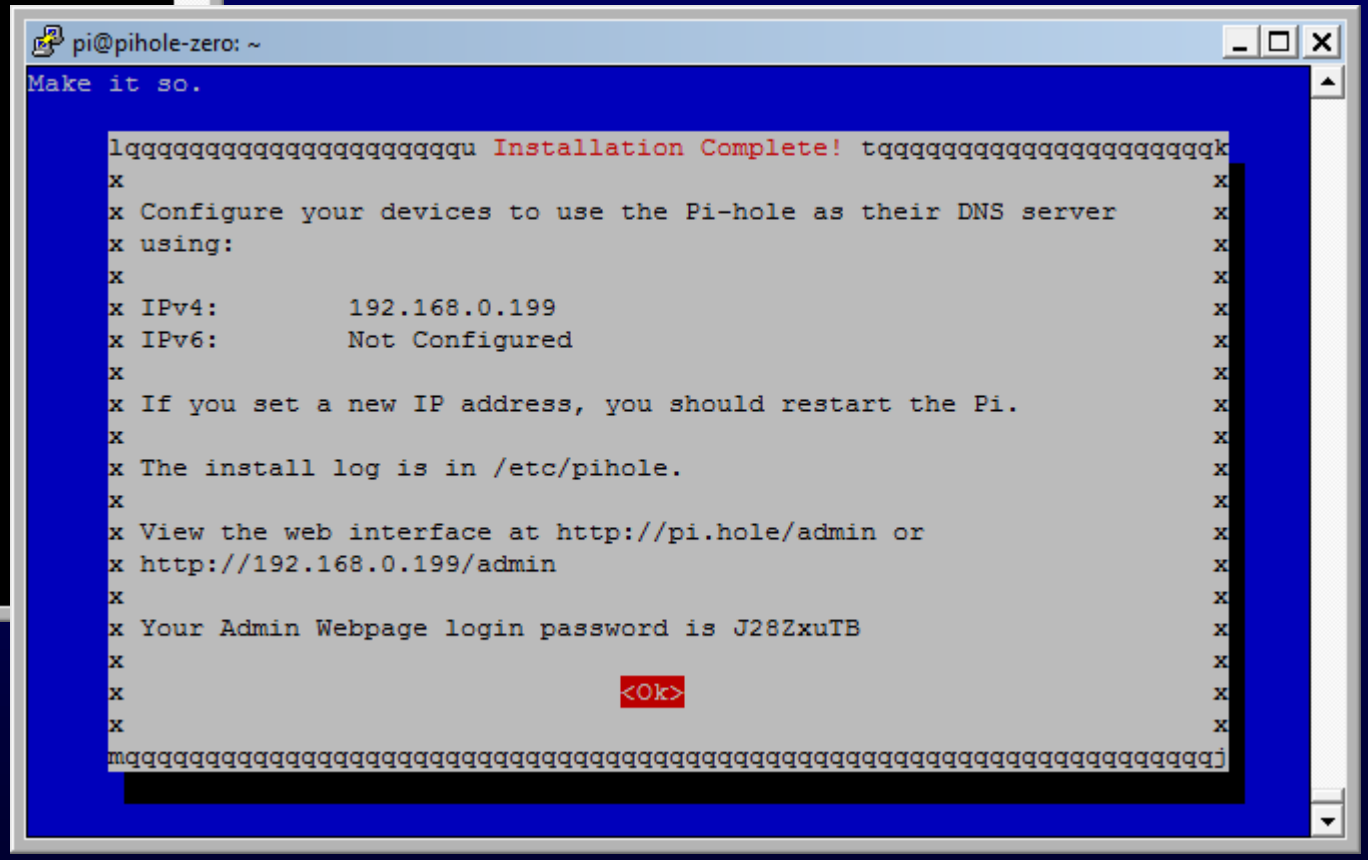


Why YES, I think it's a lovely idea (I'll explain more later).

Sit & Wait
(have a drink)



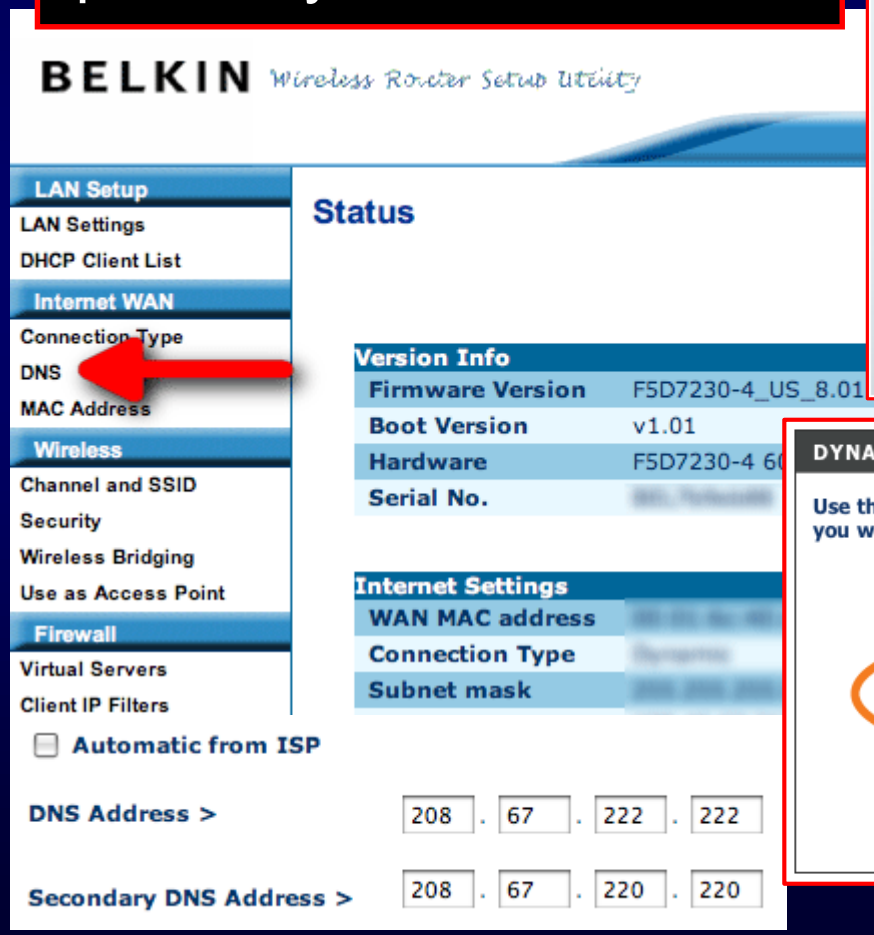
Verify IP address & record the password (into your KeePass right?).

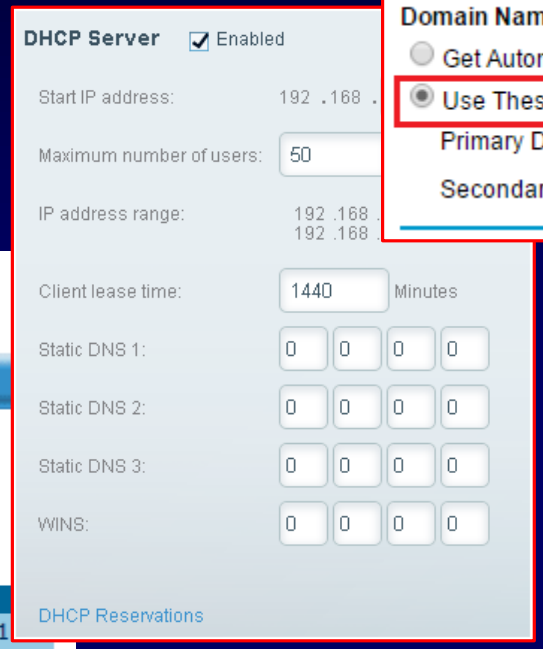


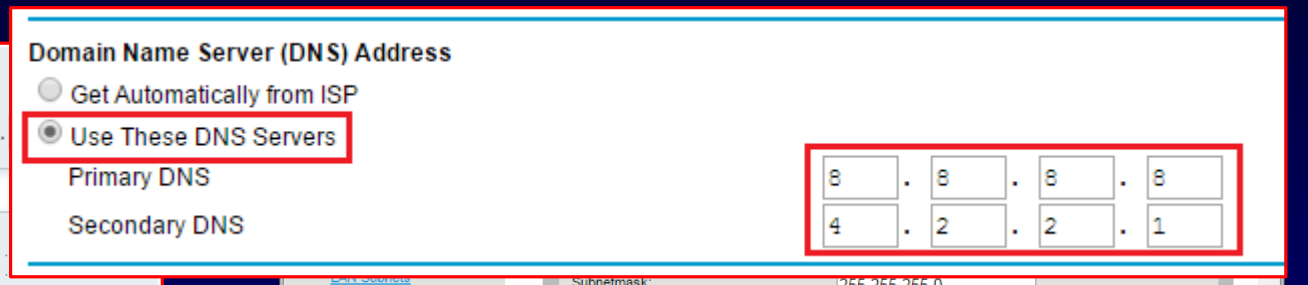
The script is doing all the heavy work.

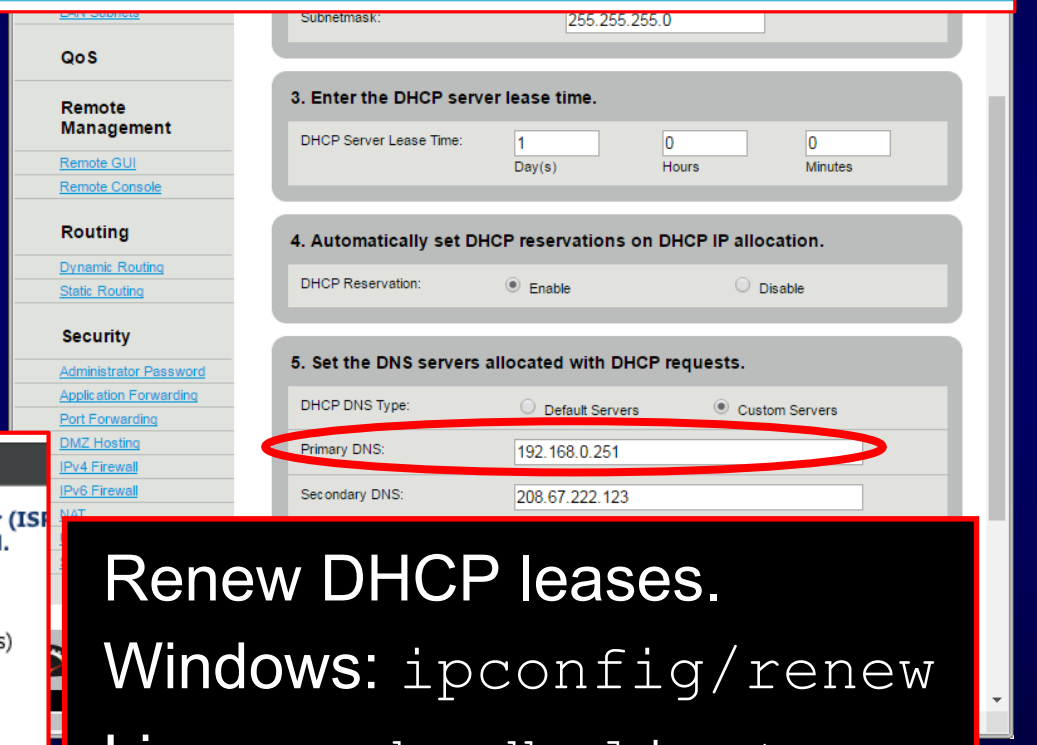
Now Point DNS Queries To Pi-Hole

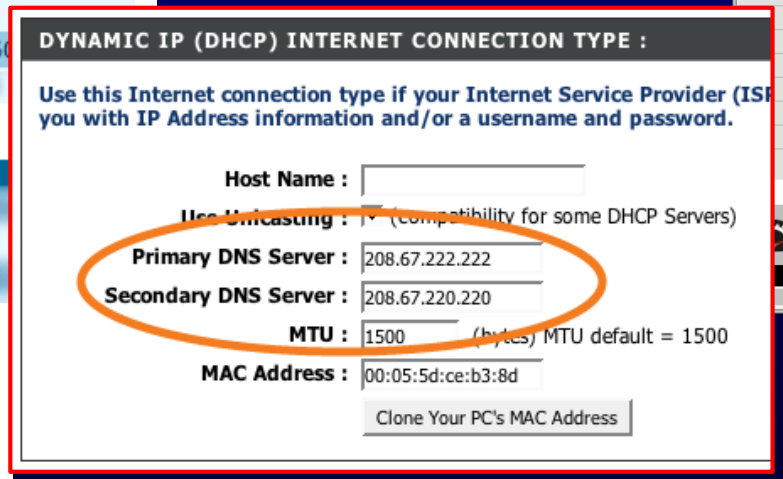
Find your router's DNS setting and change it to point at your Pi-Hole's IP.











Renew DHCP leases.

Windows: `ipconfig/renew`

Linux: `sudo dhclient`

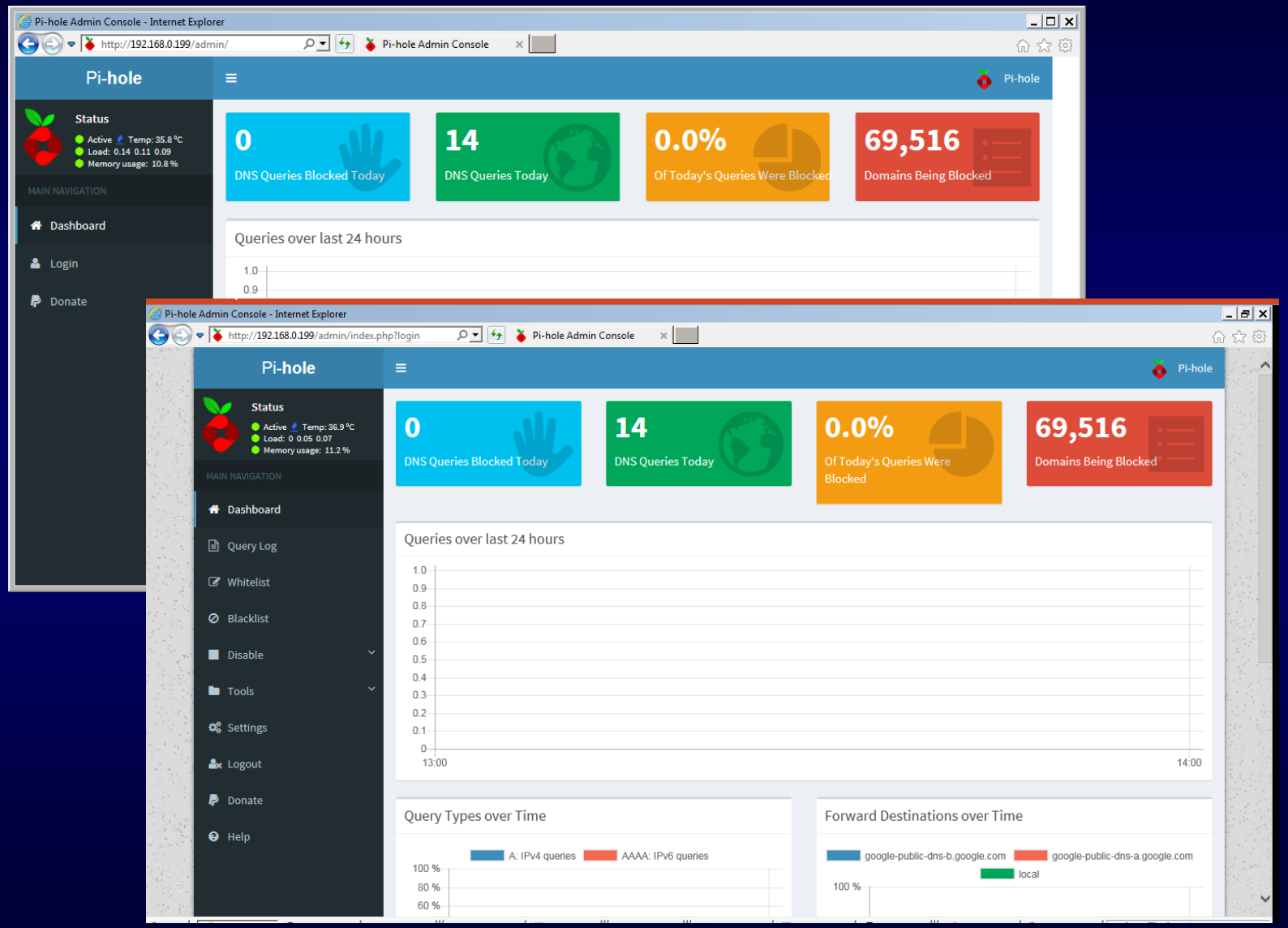
Other: unplug/plugin or off/on

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



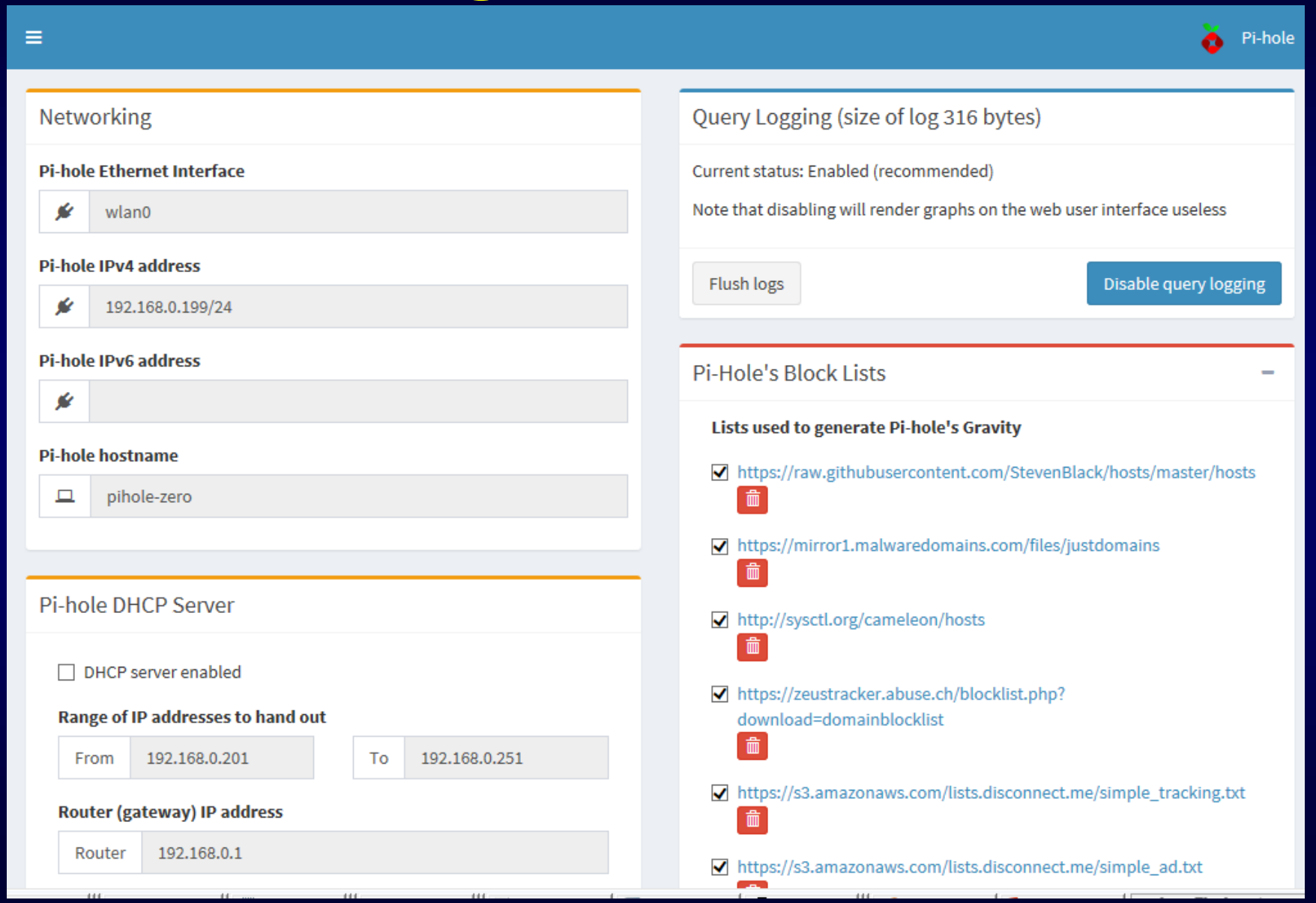
Open a web browser and go to `HTTP://<YOUR IP>/admin`

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.

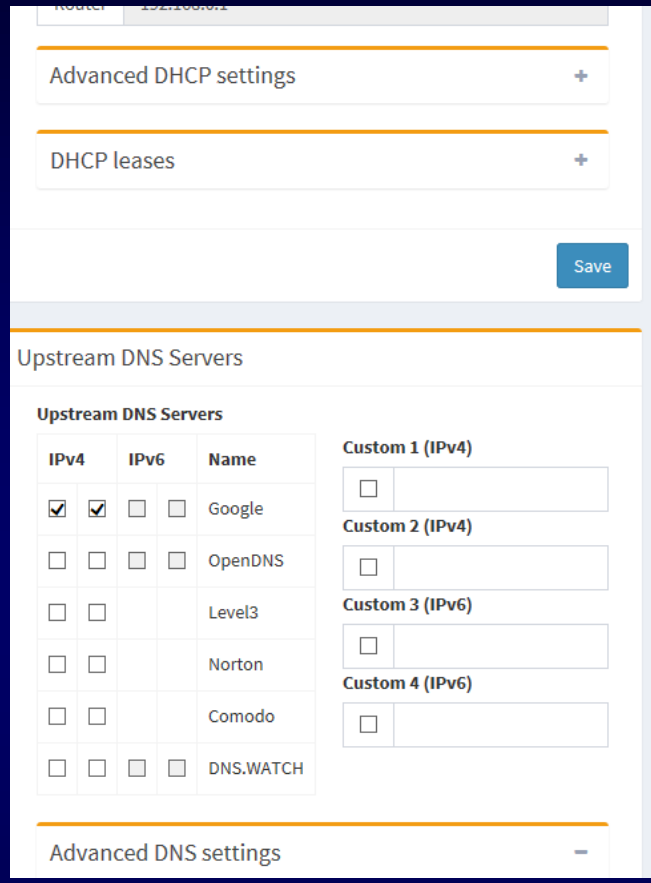
Settings

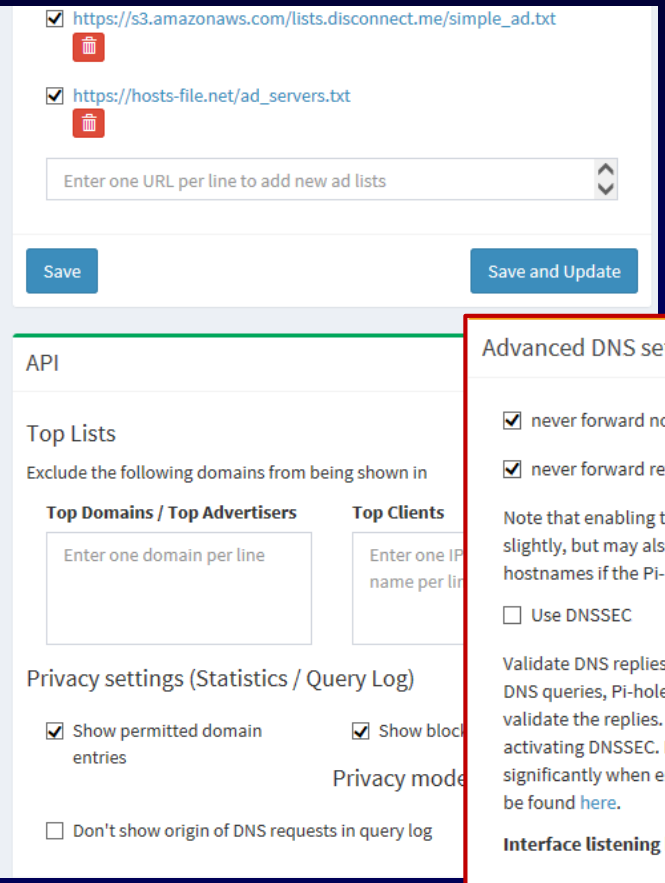
- Most of this you won't want to change. If you need to use the built-in DHCP server, here's where you can do it.
- On the right side you can see the Pi-Hole's various Block Lists. We'll talk about adding new sources shortly.

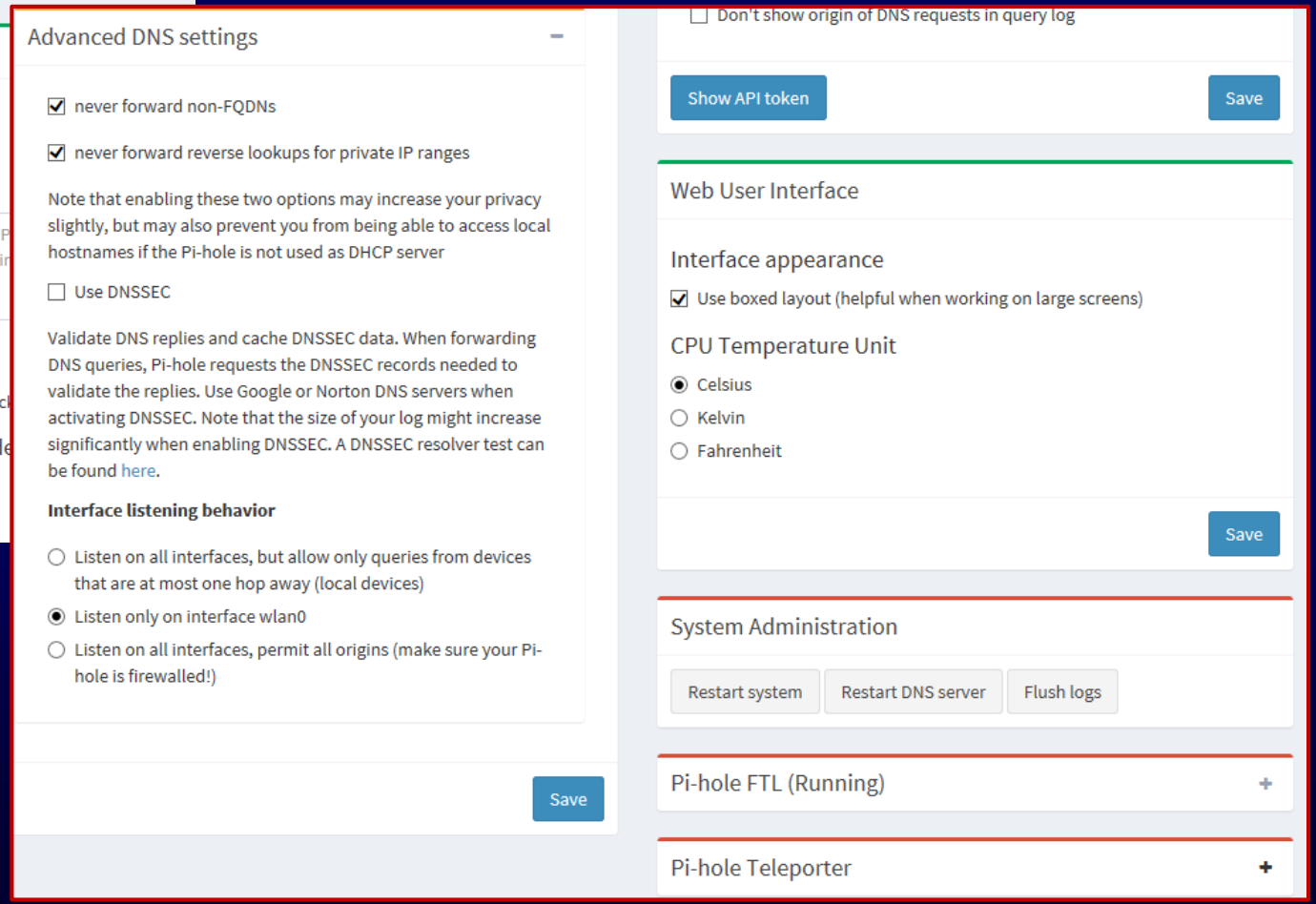


More Settings

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







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?