PiTOR

Ver: 0.1.3 - Date: 2013-08-14

Project repository: HTTPS://GITHUB.COM/HS5/PiTOR

Intended Audience

This PiTOR access point installation script is intended for the Journalist, Lawyer and Researcher in All of Us. Basically a TOR access point is not something you want to buy ready made from a company. Either make it yourself or have a friend do it. PiTOR provides useability; the chef installation and this manual.

What is PiTOR

PiTOR is single installation script that will install

- **Opscode Chef-Solo configuration management on the Raspberry Pi.**
- **A WiFi access point to the TOR Network (installation using Chef).**

It makes Raspberry Pi function as a connection between WLAN and Ethernet and send all internet traffic through TOR Onion routing.

Why use PiTOR

PiTOR allows using TOR without installing specific software on the PC or other device like tablet or smartphone. Throught this one device all pc's, laptops, tablets and smartphones can use TOR. Now it is up to the user to make good use of it.

As a result the device (your laptop, etc.) will not have traces of TOR use, this is good for going through customs, etc.

By installing and configuring with Chef, the installation and configuration can not only be repeated exactly, but also be scrutinized, extended and improved.

Contents

References

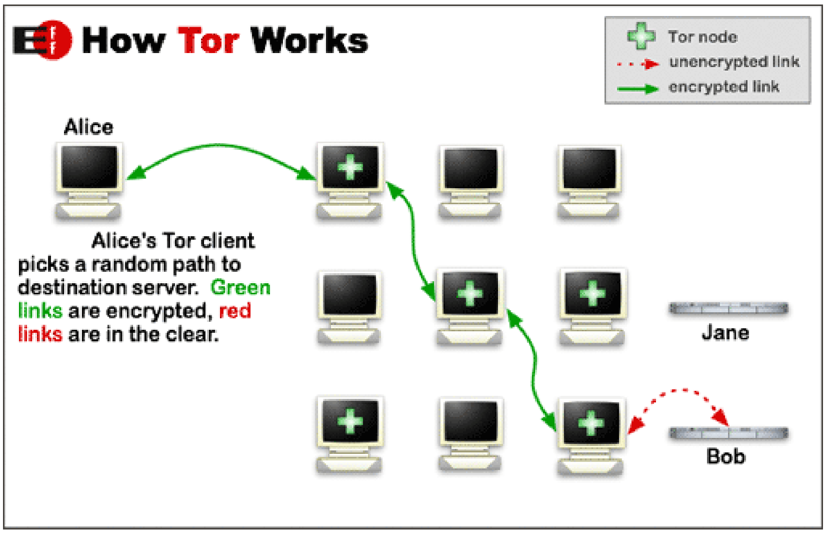
This Raspberry Pi TOR access point is based on the following information:

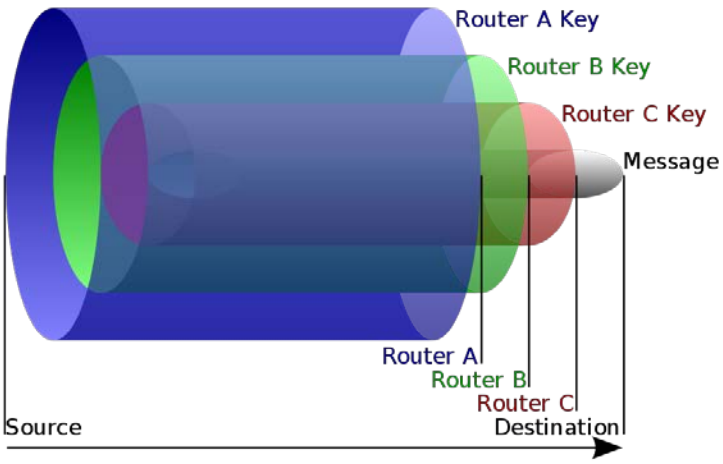
- **ADAFRUIT Onion Pi**: http://learn.adafruit.com/onion-pi/overview
- **Use Your Raspberry Pi as WiFi Bridge or AP**: http://en.tacticalcode.de/2013/03/use-your-raspberry-pi-as-wifi-bridge-or-ap.html
- **Howto setup RTL8188CUS on RPi as an Access Point:** http://blog.sip2serve.com/post/48420162196/howto-setup-rtl8188cus-on-rpi-as-an-access-point
- **German C't, 2013 Nr. 16, 15-7-2013.**

Also See:

TOR project: **https://www.torproject.org/**

Onion To: http://onion.to/


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob



Onion Routing

Basic how to use this script

1. Copy **setup_pitor.tar.gz** to the directory **/home/pi/** on the Raspberry Pi.
2. Uncompress (**tar xzvf setup_pitor.tar.gz**)
3. Edit the configuration file: **sudo nano /home/pi/setup_pitor/chef-repo/cookbooks/pitor/attributes /default.rb**
4. Go to the setup directory and run the setup script:
    a. **cd /home/pi/setup_pitor/**
    b. **sudo ./_ start_here_install_chef_wheezy_pitor.sh**

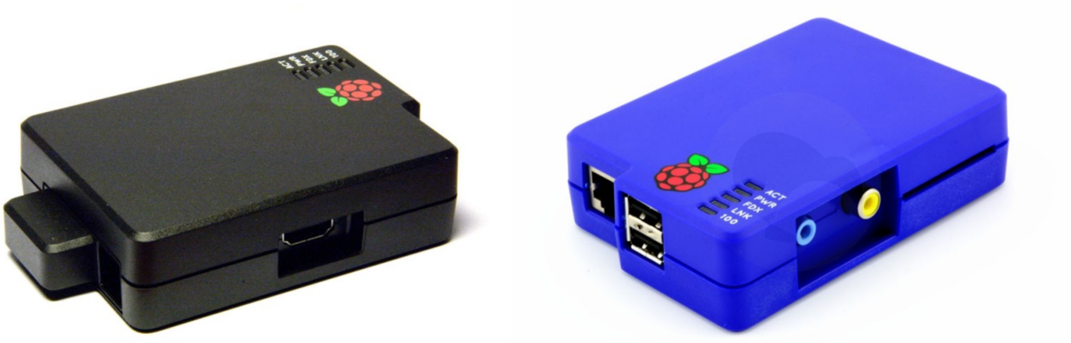
Hardware

Use a standard Pi setup:

- **Raspberry Pi B**
- **Heat Sink cooling set**
- **SD card**
    - **Samsung 32 GB SD-HCI** is a good one
    - A slower 8 or 16 GB SD Card may also be sufficient
    - Micro SD cards are slower than comparable full size SD cards

Case

- For this Raspberry Pi application the **Cyntech case** plus **SD cover** is a good choice:



-

WiFi dongle

- In the *Raspbian "Wheezy" image most WiFi drivers and firmware are included*

List of Raspberry Pi compatible WiFi dongles and their capabilites:

http://elinux.org/RPi_VerifiedPeripherals#USB_WiFi_Adapters

http://elinux.org/RPi_USB_Wi-Fi_Adapters

NOT ALL Dongles that are compatible with the Pi can be used as access point.

How to Check USB WiFi Dongle capabilities

Check model: lsusb

Check for driver loading
Example - realtek dongle: dmesg | grep rtl

Check driver: lsmod

After installing iw linux wifi utilities:
Check modem: iwconfig
WiFi capabilities: iwlist

At least need we need the AP-Mode capability

Power

We need a **USB Micro cable** (like for smartphones) and a **USB adapter > 1,2 Amp**.

A (Solar powered) battery > 1,2 Amp can also be handy.

Remarks on power:

- The micro USB connector is only a power input, and not an USB port.
- Without enough power (Amps) the Raspberry will not boot
- **Badly regulated power supplies are a cause of crashes and data corruption of the SD card. Having a well regulated power supply with enough available current is key to reliability.**
- Some people relate SD card crashes to just unplugging the USB power cord without first shutting down Linux.
- To perform a nice shutdown over SSH or the terminal: **sudo shutdown –h now**

Hama makes reasonable priced powerful USB power adapters, the "**Power Piccolino**" USB Charger delivers 2100 mA, and the "**Dual" USB Charger** delivers 3.1 A. (www.hama.com or Conrad). The standard **USB adapter for Apple iPad** delivers 2100mA.

Get system info

sudo –i
uname -a

```
free
df -H
cat /proc/cpuinfo
```

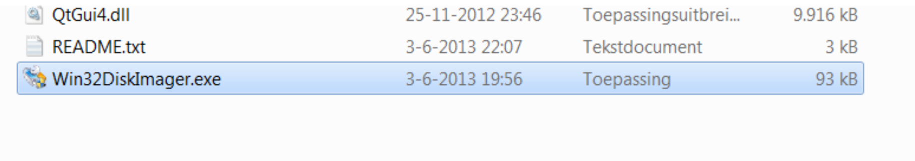
When Chef is installed: sudo ohai > sysinfo.txt

Install Operating System: Linux Debian - Wheezy

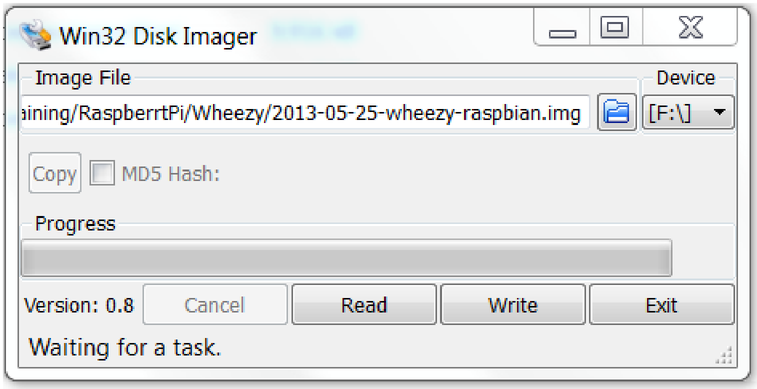
- Download Wheezy from: http://www.raspberrypi.org/downloads
- Unzip image

On a windows computer:

- Download win32diskimager-v0.8-binary.zip van: http://sourceforge.net/projects/win32diskimager/
- Unzip

- Insert SD Card
- Run: Win32DiskImager.exe
- 

QtGui4.dll	25-11-2012 23:46	Toepassingsuitbrei...	9.916 kB
README.txt	3-6-2013 22:07	Tekstdocument	3 kB
Win32DiskImager.exe	3-6-2013 19:56	Toepassing	93 kB

- 

Win32 Disk Imager

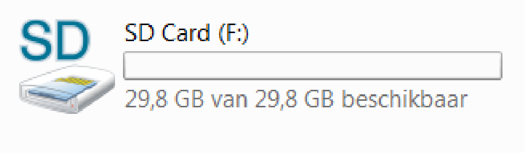
Image File: aining/RaspberrtPi/Wheezy/2013-05-25-wheezy-raspbian.img

Device: [F:\]

□ MD5 Hash:

Version: 0.8

Waiting for a task.

- Choose
  - Source Image
  - Destination Drive (DO NOT get this wrong! Check It)
  - 

SD Card (F:)

29,8 GB van 29,8 GB beschikbaar

It is possible and convenient to copy files to boot partition on the SD card x:\boot now.

Linux users can easily find what to do on the Internet.

On First Boot

- Expand Drive
- Enable SSH
- Set Password
- Set Keyboard Layout

Do:

1 Expand the drive

8 Advanced options

- **A4 Enable SSH**
- **A5 Update**

4 Internationalisation

- **13 Change Keyboard Layout – make this correct for the keyboard in use**

e.g. Logitech Generic - Keyboard layout: Other / English US / English US with Euro on 5

Run Raspberry Pi configuration anytime later with: sudo raspi-config

Turbo mode Pi documentation:

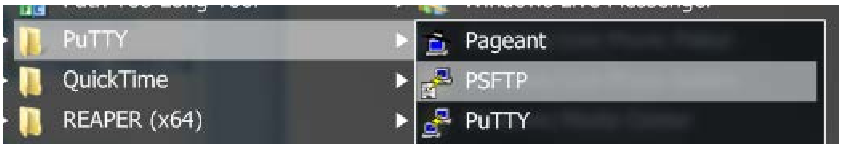
The combination of only applying turbo when busy, and limiting turbo when the BCM2835′s internal temperature reaches 85°C, means there will be no measurable reduction in the lifetime of your Raspberry Pi.

You can choose from one of five overclock presets in raspi-config, the highest of which runs the ARM at 1GHz. The level of stable overclock you can achieve will depend on your specific Pi and on the quality of your power supply; we suggest that Quake 3 is a good stress test for checking if a particular level is completely stable. **If you choose too high an overclock, your Pi may fail to boot, in which case holding down the shift key during boot up will disable the overclock for that boot, allowing you to select a lower level**.

Comparing the new wheezy image with 1GHz turbo enabled, against the previous image at 700MHz, **nbench reports 52% faster on integer, 64% faster on floating point and 55% faster on memory.**

Install software with PiTOR script

Use PUTTY / PSFTP to upload the file



Upload the file **setup_pitor.tar.gz** to **/home/pi/**

- **Start PSFTP** (Putty FTP)
- **open 10.10.10.163** (or whatever is the ip address of your Pi) and login: pi / raspberry
- **put d:\setup_ pitor.tar.gz** (d: is an example for the path where the file resides)

Or

1. copy the setup_ pitor.tar.gz file on a ms windows computer to /boot on the SD Card
2. copy it on the Raspberry Pi from the /boot directory to the home dir:
    - **cd ~**
    - **cp /boot/setup_ pitor.tar.gz .**

When the file is in the home dir, uncompress the file: **tar xzvf setup_ pitor.tar.gz**

When the setup_ pitor.tar.gz file is extracted to directory /home/pi/setup_pitor/ do the following:

1. Change to the setup directory: **cd ~/setup_pitor**
2. Yoiu MUST EDIT the configuration (at least set the WLAN password): **sudo nano /home/pi/setup_pitor/chef-repo/cookbooks/pitor/attributes/default.rb**
3. Run setup: **sudo ./_ start_here_install_chef_wheezy_pitor.sh**

The script will perform the complete install.

When the script is ready, reboot the Pi: **sudo shutdown -r now**

Install Manually

This is what the script does.

Install Chef

```
sudo apt-get update
sudo apt-get install rsync
sudo apt-get install ruby
sudo apt-get install ruby-dev
        if error: No such file to load: -mkmf
        caused by: Not installed ruby-dev
sudo gem install require
sudo gem install knife-solo
```

Install PiTOR packages

```
sudo apt-get update

## default present in Wheezy
sudo apt-get install apt-utils
sudo apt-get install curl
sudo apt-get install nano
sudo apt-get install rsync
sudo apt-get install unzip
sudo apt-get install wget

## Generic
sudo apt-get install makepasswd
sudo apt-get install tree

## Access point specific
sudo apt-get install bridge-utils
sudo apt-get install dnsmasq
sudo apt-get install hostapd
sudo apt-get install hostap-utils
sudo apt-get install iw
sudo apt-get install iptables-persistent
sudo apt-get install isc-dhcp-server
sudo apt-get install rfkill
sudo apt-get install tor
```

Configuration

All configuration can be understood by reading the config file templates and the default settings:

Config templates: /home/pi/setup_pitor/chef-repo/cookbooks/pitor/templates/**default/*.erb**

Settings: /home/pi/setup_pitor/chef-repo/cookbooks/pitor/**attributes /default.rb**

Templates and settings are connected in:

/home/pi/setup_pitor/chef-repo/cookbooks/pitor/**recipes/pitor_config.rb**

To Reconfigure PiTOR anytime

1) Edit: /home/pi/setup_pitor/chef-repo/**cookbooks/pitor/attributes /default.rb**
2) Run: . /home/pi/setup_pitor/pitor_config.sh

Security

You must:

- Secure all (ssh-)Logins with a **secure password**
  - **or disable ssh**
- Use a **strong network key**
- Use **WPA2**, Never use WEP!

If not configured well, the Pi functions as a Man-in-the-Middle device, making it easy for everyone on the network to eavesdrop on your traffic!

To change the password of the standard user run **raspi-config** or **passwd**

Raspbian default is: user=‘pi’, password=‘raspberry’

How to Use PiTOR

Internet security is a multi facetted venture.

- PiTOR only provides for IP nr obfuscation, the link is not known, that is all.
- A standard used browser will still give away who you are.

Two recommended ways to use PiTOR are:

1) **Install Firefox Portable on an external drive (e.g. USB 3.0 stick)**

   Or better:

2) **Use an immutable Virtual Machine with Firefox**

- For instance install the newest Ubuntu desktop on VirtualBox or VM Ware
- Make the VM restart clean every time, always revert to the fresh image on boot up
- **Store the VM on an external drive (e.g. USB 3.0 stick)**

Setup an immutable VirtualBox image

From the VirtualBox documentatiuon:

Immutable images only remember write accesses temporarily while the virtual machine is running; all changes are lost when the virtual machine is powered on the next time.

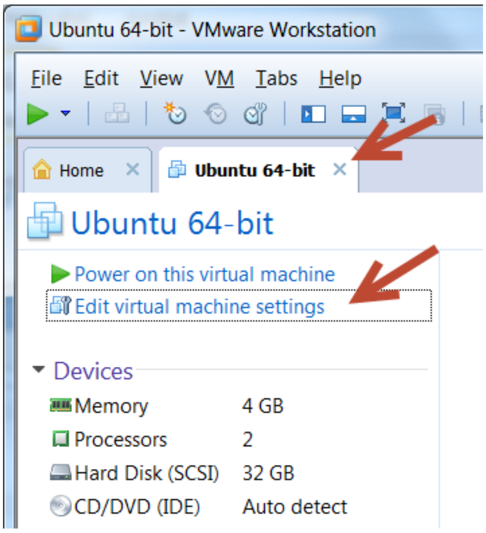
Creating an immutable image makes little sense since it would be initially empty and lose its contents with every machine restart. As a result, normally, you would first create a “normal” image and then, when you deem its contents useful, later mark it immutable.
If you take a snapshot of a machine with immutable images, then on every machine power-up, those images are reset to the state of the last (current) snapshot (instead of the state of the original immutable image).

To set a VM immutable we use VBoxManage. VBoxManage supports all the features that the graphical user interface gives you access to, but it supports a lot more than that. It exposes really all the features of the virtualization engine, even those that cannot (yet) be accessed from the GUI.

Set a VirtualBox VM to Immutable

a. **Open a DOS terminal: Start / Run / cmd**
b. **cd C:\Program Files\Oracle\VirtualBox**
c. **VBoxManage modifyhd PathToVM/VirtualMachineDisk.vdi --type immutable**

Setup an immutable VMWare image


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu 64-bit

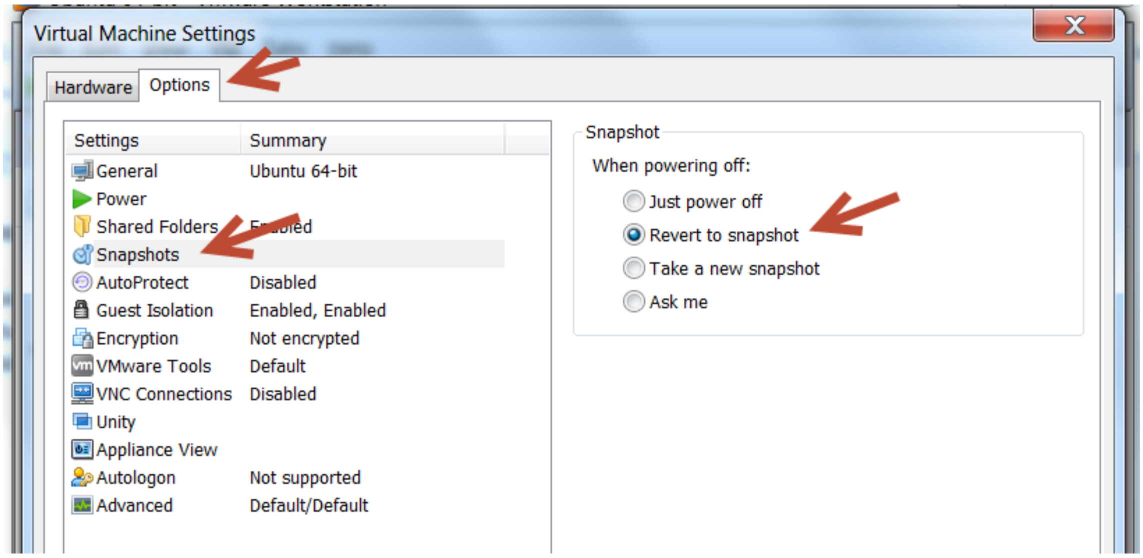
Ubuntu 64-bit

Power on this virtual machine

Edit virtual machine settings

Devices

Memory	4 GB
Processors	2
Hard Disk (SCSI)	32 GB
CD/DVD (IDE)	Auto detect



Settings	Summary
General	Ubuntu 64-bit
Power	
Shared Folders	Enabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	Enabled, Enabled
Encryption	Not encrypted
VMware Tools	Default
VNC Connections	Disabled
Unity	
Appliance View	
Autologon	Not supported
Advanced	Default/Default

Snapshot

When powering off:

○ Just power off

● Revert to snapshot

○ Take a new snapshot

○ Ask me

Install Firefox add-ons

a. **BetterPrivacy**
b. **NoScript**
c. **Cookie Monster**

Configure Firefox to always run in private mode:

Options / Privacy / History: Never Keep History

Do NOT use the TOR Firefox Browser

After the crackdown of the Freedom Hosting network on August 3, 2013, some servers were brought back on-line while being infected by the FBI with Javascript exploits.

This case has shown that the TOR browser is a specific target for authorities.

The crackdown of Freedom Hosting is a good thing because of the content of some services, according to the FBI Eric Eoin Marques, the operator of Freedom Hosting, was the "largest facilitator of child porn on the planet". However it also has shown the vulnerability of the browser and the importance of data that is stored by the browser.

Citates from an article on The Daily Dot:

Every Freedom Hosting website went down simultaneously at around 6:40am ET on Saturday morning, about the same time news of Marques's arrest hit the Internet. If and when the websites have returned since the downtime, many have been infected with Javascript exploits that may be able to identify visitors by grabbing a user's cookies, logins, and IP address to send "home"—which, in this case, is the Verizon-owned IP address 65.222.202.53. The previously unknown exploit only affects Firefox version 17, which is exactly the version Tor uses.

"The charges [against Eric Eoin Marques, the operator of Freedom Hosting] relate to images on a large number of websites described as being extremely violent, graphic and depicting the rape and torture of pre-pubescent children," reported The Independent.

http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/

Search

Use DuckDuckGo as search engine, they do not capture history: **https://duckduckgo.com/**

Do NOT use Google, Bing or other \`well known\` search engine.

Compile hostapd for Realtek RTL8192xC chipset

A precompiled hostapd for Realtek RTL8192xC chipsests is available in the PiTOR repository. But you can also decide to compile it yourself. To compile a fresh hostapd for Realtek chipsets, download the patched hostapd source file from the Realtek site and run make. To find the source search on the Realtek site for: RTL8192

This is what you want to download:
http://www.realtek.com.tw/downloads/downloadsView.aspx?Langid=1&PNid=48&PFid=48&Level=5&Conn=4&DownTypeID=3&GetDown=false&Downloads=true#RTL8188CUS

Unix (Linux)

Description	Version	Update Time	File Size	Download					
				Site 1	Site 2	Site 3	Site 4	Site 5	Site 6
Linux Kernel 2.6.18~2.6.38 and Kernel 3.0.8 Android 1.6~2.3 and 4.0	3.4.4_4749	2012/11/12	7308k	US1	HK1	US2	CN	UK1	US3

The file to download is: **RTL8192xC_USB_linux_v3.4.4_4749.20121105.zip**

This zip file contains a zip file with the source for the Realtek hostapd:

…\RTL8192xC_USB_linux_v3.4.4_4749.20121105\RTL8188C_8192C_USB_linux_v3.4.4_4749.20121105\wpa_supplicant_hostapd\wpa_supplicant_hostapd-0.8_rtw_20120803.zip

- Extract **wpa_supplicant_hostapd-0.8_rtw_20120803.zip** from **RTL8192xC_USB_linux_v3.4.4_4749.20121105.zip**
- Unzip **wpa_supplicant_hostapd-0.8_rtw_20120803.zip**
- cd … **\wpa_supplicant_hostapd-0.8_rtw_20120803\wpa_supplicant_hostapd-0.8\hostapd**
- **sudo make**
- **sudo make install**

The new compiled hostapd is: **/usr/local/bin/hostapd**
Copy it to the default install directory
sudo cp /usr/local/bin/hostapd /usr/sbin/hostapd

Test the Access Point

Check the network setup: **sudo ifconfig -a**

The result should show the wlan0 interface and an ip setting

Check internet connection: **ping** some known address

Check the hostapd setup:

hostapd -dd /etc/hostapd/hostapd.conf

Check iptables setup:

sudo iptables -t nat -S

sudo iptables -S

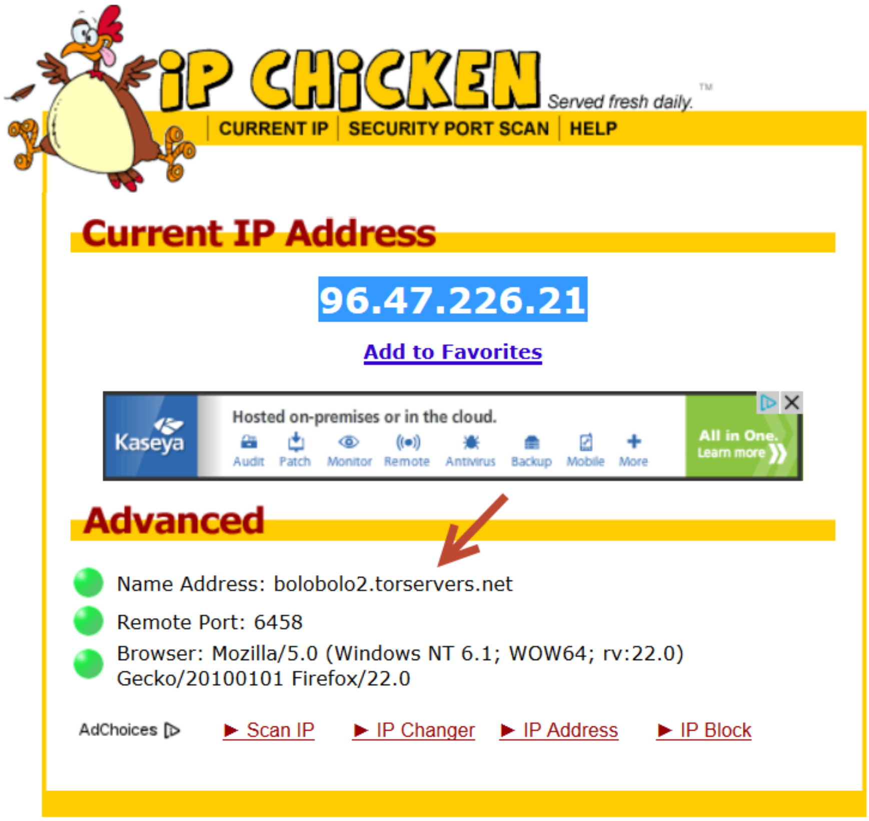
Check connection pc/laptop with Pi, on the pc: **ping 192.168.42.1**

Check the local dhcp server on the Pi, on the pc: **ping 8.8.8.8**

Check the current ip nr to test TOR onion routing: http://www.ipchicken.com

This should not be the i.p. nr of your internet provider.

On reloading the page the ip-nr should change.



Current IP Address

96.47.226.21

Add to Favorites

Advanced

● Name Address: bolobolo2.torservers.net

● Remote Port: 6458

● Browser: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0

Log Files

Check the TOR log files to see whether it is functioning:

/var/log/tor/log
/var/log/tor/notices.log

Test with a WiFi Network Tool

On Linux systems use Kismet; **www.kismetwireless.net**

Kismet is a passive sniffer. Unlike NetStumbler, which broadcasts a request for access points responding to the SSID name "ANY," Kismet does not send any packets at all. Instead, Kismet works by putting the wireless client adapter into RF monitor mode. While in so-called "rfmon" mode, the wireless client is not (and cannot be) associated with any access point. Instead, it listens to all wireless traffic. Consequently, your wireless card cannot maintain a functional network connection while under Kismet control.

Users often report that Kismet finds more APs than NetStumbler. This is because NetStumbler only knows about access points that respond to its "ANY" SSID probe request. Some network administrators configure their APs not to broadcast, or to "hide" their SSID. These do not respond to NetStumbler's probe. Because the AP blanks out its SSID, Kismet will detect its presence, but without a network name. However, when a legitimate client associates with that AP, its real SSID is included in the initial handshake. Because Kismet sees all network management traffic, it will pick up these packets and discover the SSID which was supposedly "hidden."

Whereas NetStumbler can provide at least some functionality with any wireless card supported by OS drivers, **Kismet functions only with network cards with drivers that support RF monitoring mode**. In general, this includes wireless cards based on the PRISM 2, 2.5, 3, and GT chipsets; older ORiNOCO cards without the HermesII chipset, such as the Orinoco Gold; and Atheros a/b/g chipsets.

In practice, there are dozens of wireless cards on the market, and it is not always obvious whether there are supported drivers available. Some of the more popular supported wireless adapters include the ORiNOCO Gold, the original Apple Airport (not Extreme) card, and Intel Centrino.

The Kismet Web site distributes pre-compiled binaries for Arm and MIPS platforms.

Configuring

Kismet is designed with a client/server architecture. While most users run both the client and server on the same machine and simply use Kismet as a local application, you can also run Kismet clients on remote systems. This way, one or more remote machines can see real-time data from the machine hosting the Kismet server.

On Raspberry Wheezy, the Kismet configuration files are found in **/etc/kismet**.

Before you can run Kismet for the first time, you may need to edit the primary configuration file, kismet.conf.

Inside, you will find the line:

```
suiduser=your_username_here
```

The conventional wisdom is that you should set the above to a local user under which you'll run Kismet. My experience in Ubuntu 5.10, using the Kismet package provided by Ubuntu, was that I could only run Kismet successfully as root. Attempts to run as a normal user did not work, and aborted due to various fatal errors. But this may vary on other platforms.

You also need to tell Kismet which “source,” or wireless adapter, to use. The basic syntax used in kismet.conf is:

```
source=type,interface,name
```

On my Ubuntu system with an Atheros-based Netgear WG511T card, my source configuration looks like this:

```
source=madwifi_ag,ath0,madwifi
```

Some alternative source lines for other cards include:

```
source=madwifi_b,ath0,madwifi

source=orinco,eth1,Orinoco

source=prism,wlan0,hostap

source=viha,en1,AirPort
```

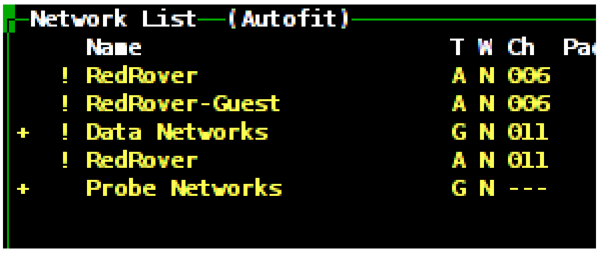
Where do these parameters come from? The Kismet documentation contains a section called “Capture Sources,” which includes a chart that lists the type and interface parameters for every supported chipset. The third parameter, name, can be set to anything you like for logging purposes.

Running Kismet

Unless you install a window-based GUI for Kismet such as KisMAC or GKismet, this is a text-based application. On my Linux system, I open a terminal window and launch Kismet as root:

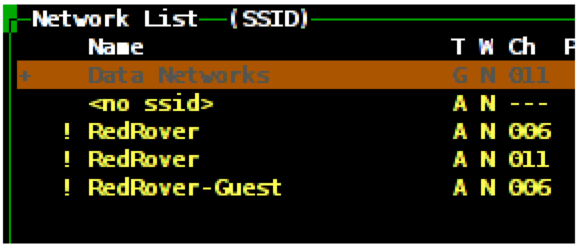
```
sudo kismet
```

As previously stated, my Ubuntu installation does not like running kismet as a normal local user. Depending on your platform, you may be able to launch kismet without the “sudo,” assuming you have configured kismet.conf appropriately.



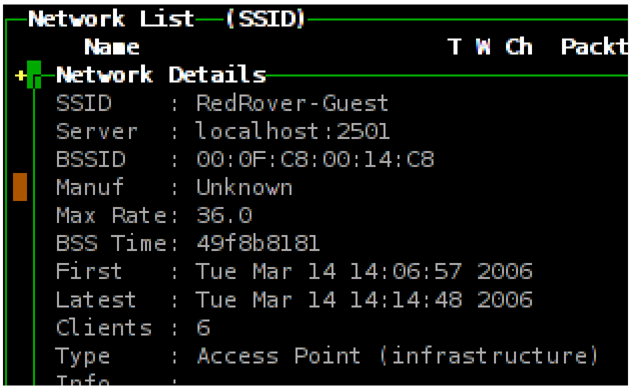
```
Network List—(Autofit)
      Name                        T W Ch  Pa
    ! RedRover                    A N 006
    ! RedRover-Guest              A N 006
+   ! Data Networks               G N 011
    ! RedRover                    A N 011
+     Probe Networks              G N ---
```

Kismet shows the list of detected wireless networks. They are initially sorted in “Autofit” mode, which does not present the networks in a specific order. Press “s” to bring up the sort menu, where you can order the SSID’s by name, chronology, and other criteria.



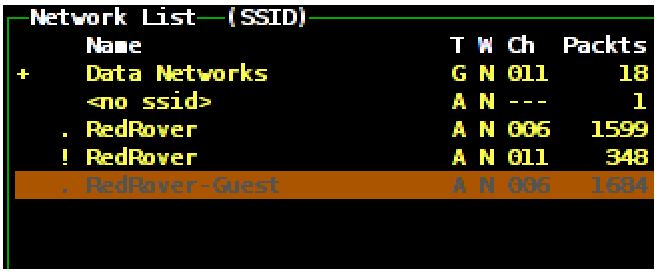
```
 Network List (SSID)
      Name                           T W Ch  P
 +    Data Networks                  G N 011
      <no ssid>                      A N ---
    ! RedRover                       A N 006
    ! RedRover                       A N 011
    ! RedRover-Guest                 A N 006
```

You can press “h” in Kismet to pop a chart of key commands. With the network names sorted, you can use the up/down arrow keys to navigate through the list. Press “i” on a network to see a detailed view of that particular network.



```
 Network List (SSID)
      Name                           T W Ch  Packt
 + Network Details
    SSID     : RedRover-Guest
    Server   : localhost:2501
    BSSID    : 00:0F:C8:00:14:C8
    Manuf    : Unknown
    Max Rate: 36.0
    BSS Time: 49f8b8181
    First    : Tue Mar 14 14:06:57 2006
    Latest   : Tue Mar 14 14:14:48 2006
    Clients  : 6
    Type     : Access Point (infrastructure)
```

Press the “l” key in Kismet to pop up signal strength data.



```
 Network List (SSID)
      Name                           T W Ch  Packts
 +    Data Networks                  G N 011     18
      <no ssid>                      A N ---      1
    . RedRover                       A N 006   1599
    ! RedRover                       A N 011    348
    . RedRover-Guest                 A N 006   1684
```

The wireless card power window is especially useful in troubleshooting wireless connections for source of noise, or optimizing locations of access points for maximizing signal strength within a space.

Further Fun

If you have a serial-based GPS receiver connected to a Kismet server, you can log and even map detected access points. You’ll need GPSD, if it's not already installed, to provide communications between the receiver and Kismet.

Kismet can play and/or speak audible alerts, which is particularly helpful when detecting wireless networks from a moving vehicle. In the kismet.conf file, you can configure .wav format sounds for alerts, including new network detection, new WEP network, new network traffic, junk traffic, GPS lock and lost.

Using the text-to-speech software Festival, Kismet can also speak its findings using customizable templates available in kismet.conf.

http://www.wi-fiplanet.com/tutorials/article.php/3595531

The **Wireless Extension (WE)** is a generic API allowing a driver to expose to the user space configuration and statistics specific to common Wireless LANs. The beauty of it is that a single set of tool can support all the variations of Wireless LANs, regardless of their type (as long as the driver support Wireless Extension). Another advantage is these parameters may be changed on the fly without restarting the driver (or Linux).

The **Wireless Tools (WT)** is a set of tools allowing to manipulate the Wireless Extensions. They use a textual interface and are rather crude, but aim to support the full Wireless Extension. There are *many other tools* you can use with Wireless Extensions, however Wireless Tools is the reference implementation.

- **iwconfig** manipulate the basic wireless parameters
- **iwlist** allow to initiate scanning and list frequencies, bit-rates, encryption keys...
- **iwspy** allow to get per node link quality
- **iwpriv** allow to manipulate the Wireless Extensions specific to a driver (private)
- **ifrename** allow to name interfaces based on various static criteria

Most **Linux distributions** also have integrated Wireless Extensions support in their networking initialisation scripts, for easier **boot-time** configuration of wireless interfaces. They also include Wireless Tools as part of their standard packages.

Wireless configuration can also be done using the Hotplug or uDev scripts and distribution specific support, this enable the proper support of any **removable wireless interface** (Pcmcia, CardBus, USB...).

Any versions of the Pcmcia package offer the possibility to do wireless configuration of Pcmcia and Cardbus card through thefile wireless.opts. This allow to fully integrate wireless settings in the Pcmcia scheme mechansism. However, this method is now deprecated in favor of distribution specific methods.

Please note that the Wireless Tools (starting with version 19) supports fully **IEEE 802.11** parameters and devices, support older style of devices and most proprietary protocols, and are prepared to handle HiperLan as well. More recent versions of course adds **more 802.11 support**.
But, unfortunately not all *drivers* support all these features...

ifscheme for Debian users

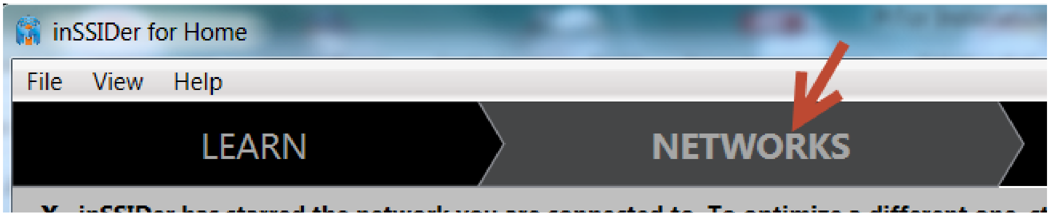
Users of the Debian distribution may want to use the **ifscheme** scripts to *manually* manage multiple configuration per wireless interface. Note that a Debian package exist, and is usually up to date, so you probably don't have much reason to pick the version here...

Windows

A well known now old tool for windows is NetStumbler. Bet there are quite a few newer network tools available for Windows. The free home version of “**inSSIDer for Home**” from **metaGeek** is an easy to use tool.

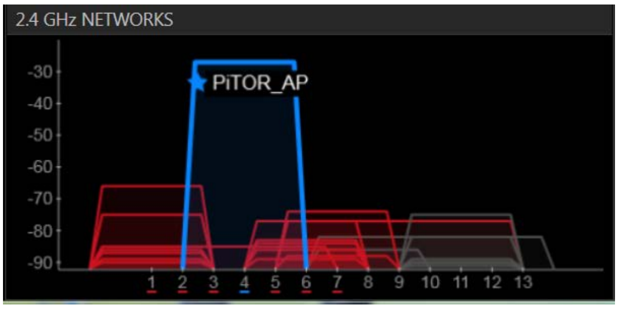
Download inSSIDer from: http://www.metageek.net/products/inssider/ and install it in the usual way.

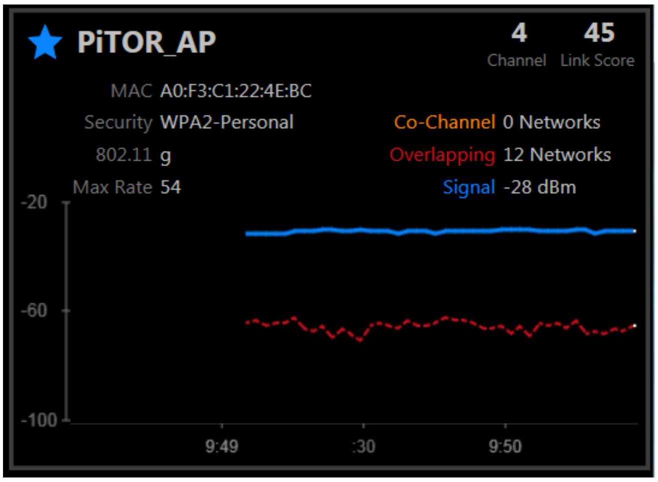
Start inSSIDer and open the Networks tab:



X inSSIDer has starred the network you are connected to. To optimize a different one, cl

If the PiTOR AP is available, you will see it.





PiTOR_AP

4 Channel

45 Link Score

MAC A0:F3:C1:22:4E:BC

Security WPA2-Personal

802.11 g

Max Rate 54

Co-Channel 0 Networks

Overlapping 12 Networks

Signal -28 dBm

This is also a good way to find the best channel setting for the AccesPoint by looking for a free or the least accessed channel (Co-Channel: 0 Networks).

Set this in the configuration file: /etc/hostapd/hostapd.conf, e.g. “channel=4”

Windows netsh

In modern Windows (Vista and later) the “netsh” command can be used to discover access points using the format below.

```
netsh wlan show networks mode=bssid
```

or write the result to a file:

```
netsh wlan show networks mode=bssid  >  wifi.txt
```

Vistumbler

Vistumbler is a script that uses netsh: www.vistumbler.net

Vistumbler did not work on my laptops.

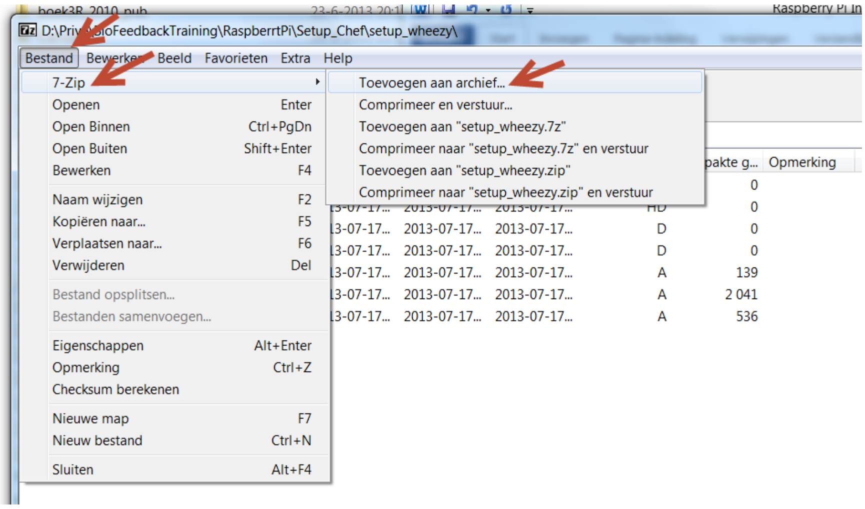
NetSurveyor

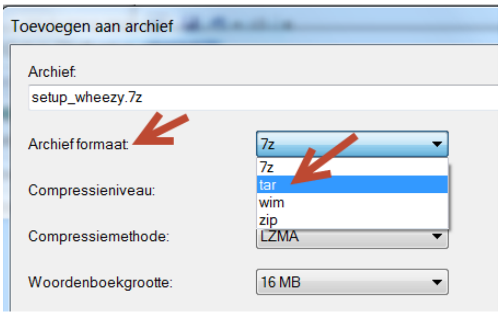
NetSurveyor is also a usable tool: http://nutsaboutnets.com/

Create tar.gz on Windows with 7Zip

Open 7ZIP application through start, or right Click on files

Add files to TAR Archive:





Archief: setup_wheezy.7z

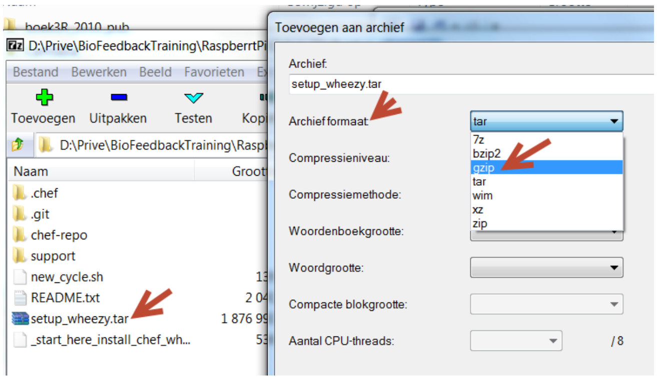
Archief formaat: 7z

Compressieniveau:

Compressiemethode: LZMA

Woordenboekgrootte: 16 MB

Compress the TAR with gzip to a tar.gz



Archief: setup_wheezy.tar

Archief formaat: tar

Compressieniveau:

Compressiemethode:

Woordenboekgrootte:

Woordgrootte:

Compacte blokgrootte:

Aantal CPU-threads: / 8

Chinese WiFi dongle

lsusb	ralink RT2870/RT3070
dmesg rt	registered new interface driver rt2800usb
lsmod	some drivers are loaded

iwconfig
iwlist