

# PiTOR

Ver: 0.1.2 - Date: 2013-08-5

**Project repository: [HTTPS://GITHUB.COM/HS5/PI TOR](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 .....                                     | 3  |
| Basic how to use this script .....                   | 4  |
| Hardware .....                                       | 4  |
| Case .....   | 4  |
| WiFi dongle.....                                     | 4  |
| How to Check USB WiFi Dongle capabilities .....      | 5  |
| Power .....  | 5  |
| Get system info .....                                | 5  |
| Install Operating System: Linux Debian - Wheezy..... | 6  |
| On First Boot.....                                   | 7  |
| Install software with PiTOR script .....             | 8  |
| Install Manually .....                               | 9  |
| Install Chef .....                                   | 9  |
| Install PiTOR packages.....                          | 9  |
| Configuration.....                                   | 10   |
| To Reconfigure PiTOR anytime.....                    | 10   |
| Security.....  | 10   |
| How to Use PiTOR .....                               | 11   |
| Setup an immutable VirtualBox image.....             | 11   |
| Setup an immutable VMWare image .....                | 12   |
| Install Firefox add-ons .....                        | 12   |
| Search .....   | 13   |
| Compile hostapd for Realtek RTL8192xC chipset.....   | 14   |
| Test the Access Point.....                           | 15   |
| Log Files .....                                      | 16   |
| Test with a WiFi Network Tool .....                  | 17   |
| Create tar.gz on Windows with 7Zip .....             | 18   |
| Isorecorder .....                                    | <b>Fout! Bladwijzer niet gedefinieerd.</b> |

## References

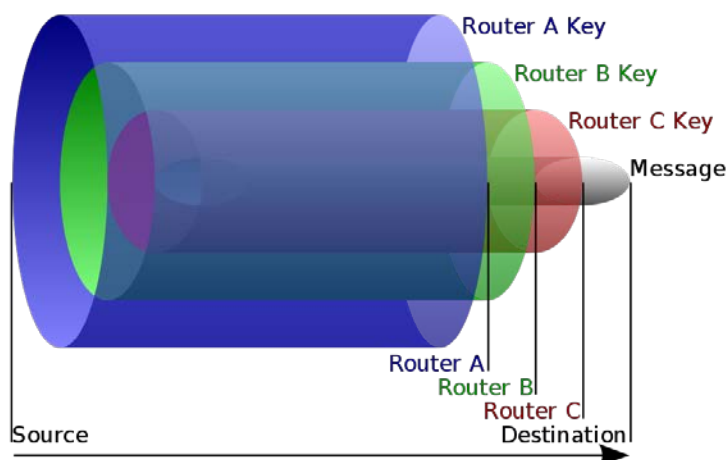
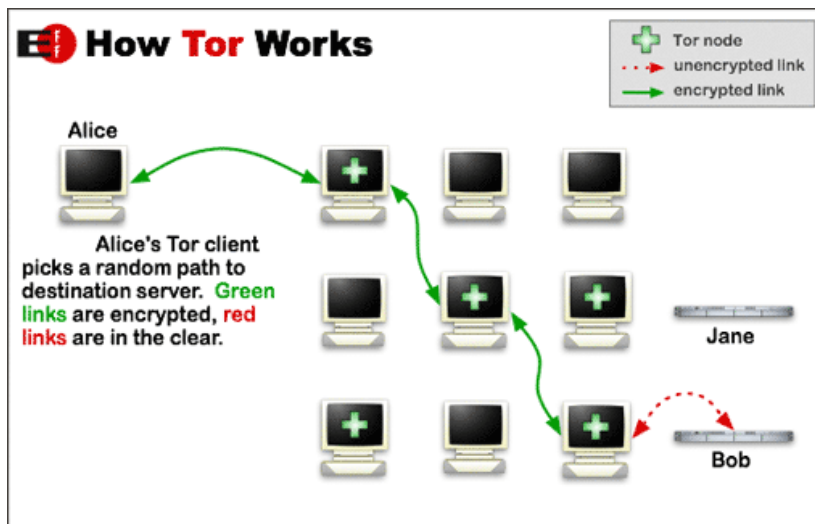
This Raspberry Pi TOR access point is based on the following information:

- **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/>



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**
- **Cooling set**
- **SD card**
  - o **Samsung 32 GB SD-HCI** is a good one
  - o A slower 8 or 16 GB SD Card may also be sufficient
  - o 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 capabilities:

[http://elinux.org/RPi\\_VerifiedPeripherals#USB\\_WiFi\\_Adapters](http://elinux.org/RPi_VerifiedPeripherals#USB_WiFi_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 realtek dongle: `dmesg | grep rtl`

After installing iw linux wifi utilities:  
WiFi capabilities: `iw list`

## 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](http://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`

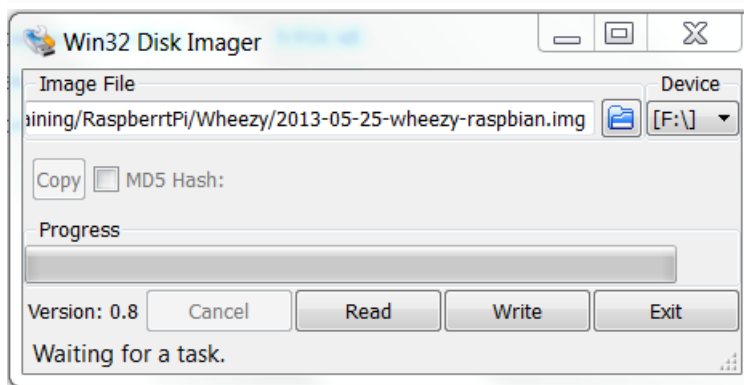
## Install Operating System: Linux Debian - Wheezy

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

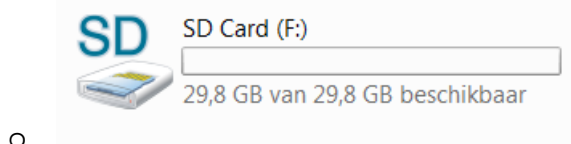
On a windows computer:

- 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    |



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



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:**

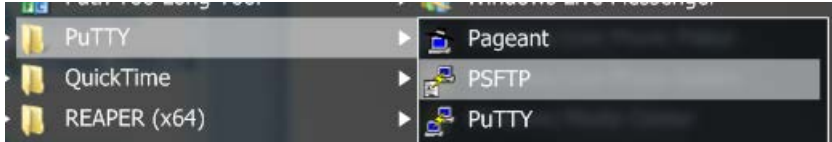
The combination of only applying turbo when busy, and limiting turbo when the BCM2835's internal temperature reaches 85°C, means there will be no measurable reduction in the lifetime of your Raspberry Pi.

**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. You 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 faceted 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.

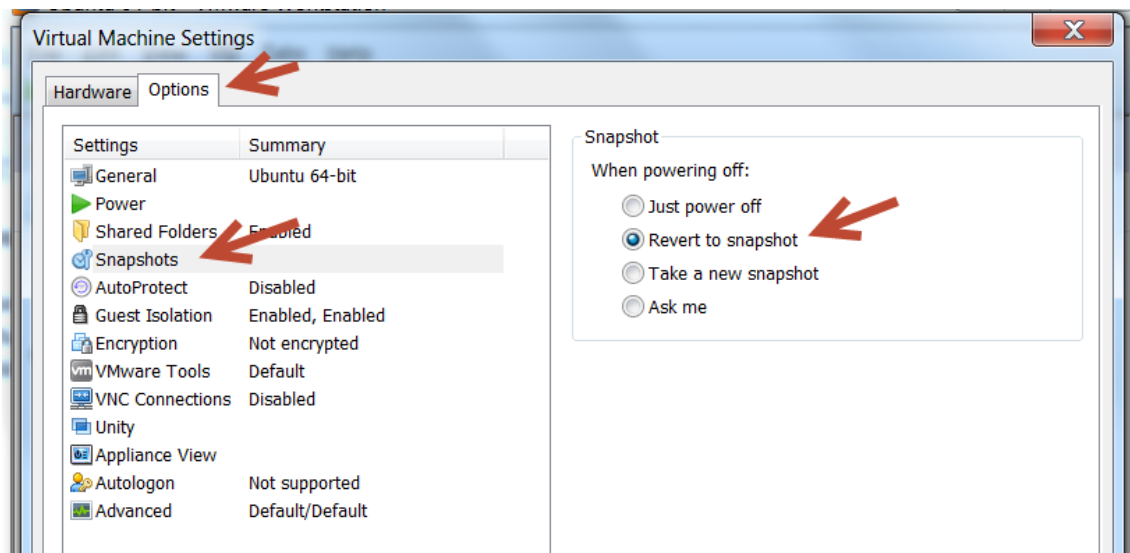
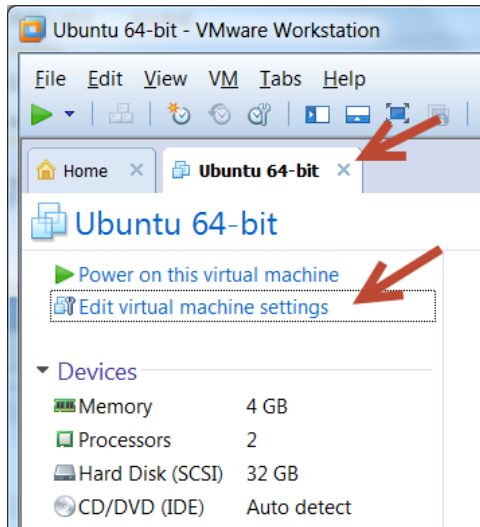
*If you take a snapshot of a machine with immutable images, then on every machine power-up, those images are reset to the state of the last (current) snapshot (instead of the state of the original immutable image).*

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



## 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 chipsets 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)

| <u>Description</u>                          | Version    | <u>Update Time</u> | 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 | 3.4.4_4749 | 2012/11/12         | 7308k     | <u>US1</u> | <u>HK1</u> | <u>US2</u> | <u>CN</u> | <u>UK1</u> | <u>US3</u> |
| Android 1.6~2.3 and 4.0                     |            |                    |           |            |            |            |           |            |            |

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.**



# iP CHICKEN

Served fresh daily.™

[CURRENT IP](#) | [SECURITY PORT SCAN](#) | [HELP](#)


## Current IP Address

**96.47.226.21**

[Add to Favorites](#)



## Advanced



- Name Address: bolobolo2.torserver.net
- Remote Port: 6458
- Browser: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0

[AdChoices](#) ▶ [Scan IP](#) ▶ [IP Changer](#) ▶ [IP Address](#) ▶ [IP Block](#)

## 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

Linux users know how to do this.

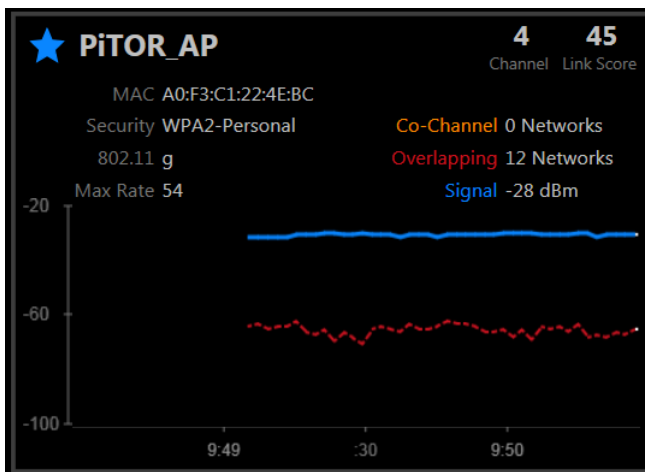
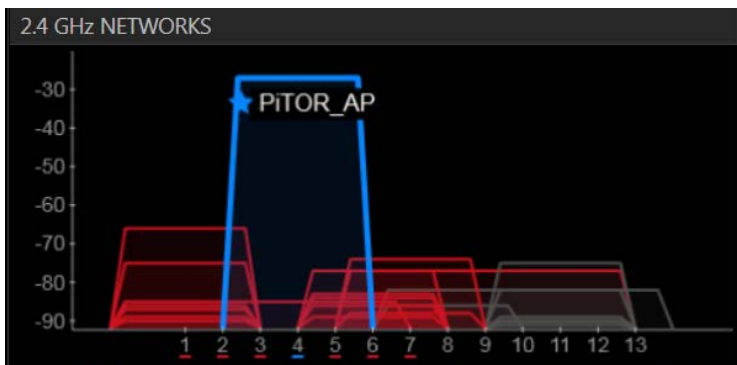
There are quite a few network tools available for Windows. The free home version of “inSSIDer for Home” from metaGeek is an easy to use tool.

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

Start inSSIDer and open the Networks tab:



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



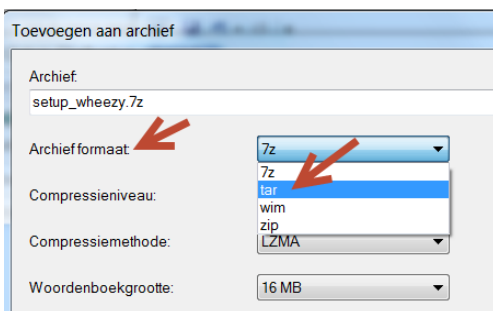
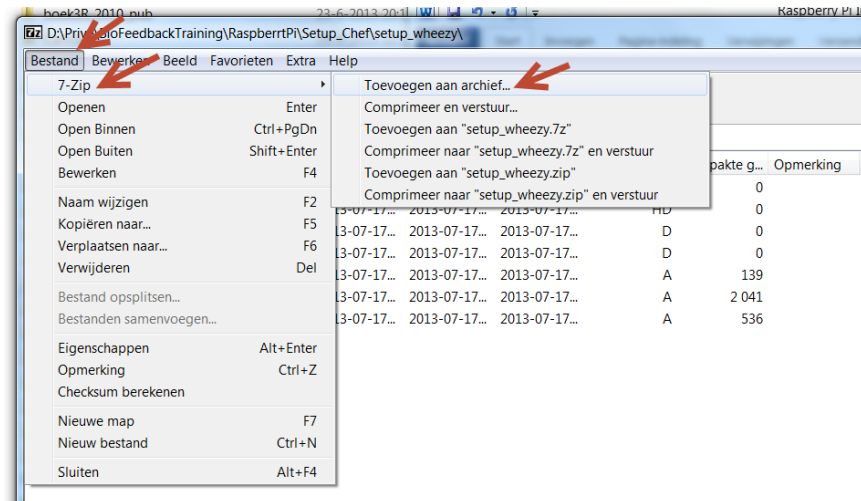
This is also a good way to find the best channel setting for the AccesPoint by looking for a free or the least accessed channel (Co-Channel: 0 Networks).

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

# Create tar.gz on Windows with 7Zip

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

Add files to TAR Archive:



Compress the TAR with gzip to a tar.gz

