I. PURPOSE

Build your very own Raspberry Pi TOR device to encrypting and anonymizing your internet traffic.

II. HOW TO

Building Your Own Device

STEP 00

Things that you need:

- Raspberry Pi 3
- Image Raspbian onto an SD card

note: *This project is originally made by KNOW HOW by @PadreSJ, @Cranky_Hippo, and @Anelf3 – twit.tv/shows/know-how/episodes/301*

STEP 01

First of all let's configure the Pi

Open the Terminal and type:

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

Change the default password
```
-- Select option 1
type an strong password :D
```

STEP 02 – TURN YOUR RASPI INTO AN ACCESS POINT

A github user by the name of "Harry Allerston" created a script to automate the process.

Open the Terminal and type:

```
pi@raspberrypi:~$ cd /opt
pi@raspberrypi:/opt$ sudo git clone https://hithub.com/unixabg/RPI-
Wireless-Hotspot.git
                                    …
pi@raspberrypi:/opt$ cd RPI-Wireless-Hotspot/
pi@raspberrypi:/opt/RPI-Wireless-Hotspot/$ sudo ./install
                                    …
This script will make changes to your system which may break some
applications and may require you to reimage your SD card. Are you sure
```

```
that you wish to continue? [y/N] y
Configuring DHCP
Do you want to use preconfigured DNS servers? [y/N] y
Do you wish to use Unblock-Us DNS servers? [y/N] y
Synchronizing state of udhcpd.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable udhcpd
Configuring interfaces
Configuring hostapd
Do you want to use the wifi defaults of password=0123456789A,
ssid=RaspberryPiFi, and channel=8? [y/N] N
Please enter a new password at least 8 characters long (length is not
checked):
Please enter the new password again:
Please enter a new ssid: AP01-TOR
Please enter a new channel from 1 to 11: 11
You selected channel 11.
Are you using an rtl871x chipset (such as one purchased via adafruit?
(if in doubt, select no) [y/N] N
Configuring NAT
Configuring iptables
Do you require chromecast support for unblock-us? [y/N] N
Initialising access point
Initialising DHCP server
=================== Configuration complete! ====================
++++++++++++++++  REBOOTING in 10 SECONDS  ++++++++++++++++++++
```

Your Pi will reboot.
If you have any issue with **hostapd.service unsmask the service to allow starting from boot and ruin **./install** again.*

```
pi@raspberrypi:~$ sudo systemctl unmask hostapd.service
```

STEP 03 – INSTALL AND CONFIGURE TOR

Install TOR

Open the Terminal and type the following command to update the repositories and install tor.

```
pi@raspberrypi:~$ sudo apt-get update
                                    …
pi@raspberrypi:~$ sudo apt-get install tor
                                    …
```

Configure TOR

```
pi@raspberrypi:~$ sudo nano /etc/tor/torrrc
      *Add the following just below the first set of comments
Log notice file /var/log/tor/notices.log
     VirtualAddrNetwork 10.192.0.0/10
     AutomapHostsSuffixes .onion,.exit
     AutomapHostsOnResolve 1
     TransPort 9040
     TransListenAddress 192.168.42.1
     DNSPort 53
     DNSListenAddress 192.168.42.1
```

Save and exit the document.

STEP 04 – CONFIGURE IPTABLES

Dump all the old rules from the iptables:

```
pi@raspberrypi:~$ sudo iptables -F
pi@raspberrypi:~$ sudo iptables -t nat -F
```

**iptables lets you configure the rules of the Linux Kernel Firewall.*
**It allow you to define how packets are treated.*
**We're using it to route traffic througth TOR*

Route DNS through the TOR:

```
pi@raspberrypi:~$ sudo iptables -t nat -A PREROUTING -i wlan0 -p udp
--dport 53 -j REDIRECT --to-ports 53
```

Route all TCP traffic through the TOR:

```
pi@raspberrypi:~$ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp
--syn -j REDIRECT --to-ports 9040
```

Check the routes:

```
pi@raspberrypi:~$ sudo iptables -t nat -L
```

Save the new rules to the NAT table

```
pi@raspberrypi:~$ sudo sh c "iptables save > /etc/iptables.ipv4.nat"
```

Create log file:

```
pi@raspberrypi:~$ sudo touch /var/log/tor/notices.log
```

**touch creates an empty file*

```
pi@raspberrypi:~$ sudo chown debian-tor /var/log/tor/notices.log
```

**chown changes the ownership of a file, so that TOR can use it.*

```
pi@raspberrypi:~$ sudo chmod 644 /var/log/tor/notices.log
```

**chmod is the "change mode" command its changes permissions*

LAST STEP

Start the TOR service:

```
pi@raspberrypi:~$ sudo service tor start
```

Check if it's runnig:

```
pi@raspberrypi:~$ sudo service tor status
```

Change the service to start on boot:

```
pi@raspberrypi:~$ sudo update-rc.d tor enable
```

Check if you are using tor browsing *check.torproject.org*