

# TOR BROWSER

GUIDE FOR BEGINNERS -  
HOW TO BE  
ANONYMOUS ONLINE



AARON MILLER

# TOR BROWSER

GUIDE FOR BEGINNERS -  
HOW TO BE  
ANONYMOUS ONLINE



AARON MILLER

## TABLE OF CONTENTS

**1. Description**

**2. Application**

**3. Structure and principles of work.**

**4. Setup of Tor**

**Tor for Ubuntu**

**Tor for Mac**

**5. Configuring and running in bridge mode**

**6. Tuning in the proxy mode**

**7. Relay mode**

**8. Adjustment and work with the Vidalia Polipo shell**

**9. The usage on Smartphone**

**10. How to check Tor operation?**

## 1. Description

Some words about situation as an introduction

Lately the interest to the anonymous network of Tor grows constantly. And there are quite enough reasons.

“Democratic reforms” in the world go at full speed. Now the governments practically of all countries consider that they have a right to decide, where the citizens can walk to, what to watch and what to read. Packs of laws, “with the best motives” stamped by the council and parliaments, determine sharper the borders of reservations within the limits of which the existence of users in a global Network is possible now.

**”A danger foreseen is half avoided”**

The authorities take care of moral health of the citizens and about the cleanness of their thoughts paternally. That is very touching. But as usual, nobody finds the time to ask citizens’ opinion. And more users in the Internet begin to feel that the limits imposing by official authority begin to “reap in shoulders”. And search means to change a situation.

One more tensing moment is Edward Snowden’s exposures from that clear that total shadowing of the special services after all and everybody has already become a really world scope. Certainly, a great number of people has nothing to hide, but it is extremely unpleasant to realize that you are under the permanent hubcap of “The Big Brother”, every your step is watched and fixed, and someone regularly tries to delve in your dirty linen. And nobody absolutely doesn’t care about for what purpose he does it, with good or bad intentions.

Tor is a web-browser that provides free and open Internet. Tor has own system of proxy-servers, that allows anonymously unite with a few networks simultaneously, providing protection from listening. Tor is an anonymously-virtual tunnel network that gives an in cipher information transfer.

Using the browser of Tor, the clients of the Internet have the opportunity of maintenance of anonymity in a network during the visit of different online resources, during blogging, sending reports, and also during work with other online applications.

In autumn 2011 the developers of web-browser of Tor got a reward that can be compared on meaningfulness with Oscar in the world of the cinema, Fund of free POE gave out this bonus them, and in spring 2012 - reward of EFF Pioneer Awards.



## 2. Application

More and more people try to save inviolability of private life from special services, which poke their nose into other people's affairs. More people try to get rid of from the "paternal caring" of officials from the state and want to realize the constitutional right to decide independently, where to walk, what to choose, where to look and what to do.

And here anonymous network of Tor comes for help. As it can provide separately human being a considerable weakening of persuasive attention and at the same time taking away almost all limits on moving on World Wide Web. Tor will hide your personality in Network, all that you will do in the Internet and all sites that you will visit. And also it will allow you to go round all blocking your favorite web-sites with lightness, carefully inflicted to us by favorite governments, which consider sincerely, that know us better.

In addition, the network of Tor has another small practical bonus. It often allows going round such annoying thing, as ban on IP on different web sites. These are trifles, but very pleasant.

Private persons use the browser of Tor; especially it is popular among those, who aim to protect the confidential personal information, and also to protect access to the blocked data. Due to the hidden services the users of Tor are able to create independently web-sites and other electronic resources, besides the place where a server is really located, is hidden carefully.

The Web-browser of Tor is very often used by journalists with the purpose of communicating with informants safely. Well-known user of this browser is Edward Snowden, transmitting with the help of Tor different information to the news agencies and Internet resources.

The employees of non-governmental organizations use the web-browser of Tor in order to be connected to the special web sites in their foreign business trips, not wishing to advertize their working activity.

Tor is much liked by civil activists from Fund of electronic borders, seeing this browser that gives possibility to protect base civil laws and freedoms in a world network. Different corporations use Tor for safe analysis of work of their competitors at the market. Also the web-browser of Tor is used by the different special services in order to provide secrecy during execution of special tasks.

### 3. Structure and principles of work.

#### Anonymous outgoing connections

So, what is it anonymous network of Tor? Tor is an abbreviation of “The Onion Router”. If someone is interested in boring technical details then visit the page of Tor in Wikipedia and examine it. If you want to make it easier then visit just the same page in Lurk more. But I try to explain it more quickly.

Though this network is functioned on the base of usual Internet, the information doesn't move directly from you to the server and back as in “big” network, and everything is banished through a long chain of special servers and ciphered many times in each stage. As a result the final recipient, that is you, becomes completely anonymous for the sites – instead of your real address there is shown absolutely wrong, not having to you any relation. All your movements can't be traced, as well as what you did. And interception of your traffic becomes absolutely useless too.

It is the theory. In practice everything sometimes is not so optimistic. We will talk about all possible problems later. You are tired from long and boring introduction, aren't you? Are you short of temper to set up and try to use this miracle? So, let's start!

The general system of Browser Tor allows its users to start on their computers separate so-called “Onion” Proxy-servers which after that connect to the main Tor servers, organizing Tor web-chains (they use multilevel coding). All data packets going through the system pass through 3 split-level proxy-servers, and its choice generates accidentally.

Before sending a packet, the one is being successively coded using three keys. The first pack of network gets the data package, and then it encodes the “top” layers of the code (similar to peeling the onion) and gets to know where it should send the data packet further. Other two network packs do the same thing.

In inner Tor networks traffic is being redirected between routers, and then it finally reaches the output final point, where already encoded data reaches home server. After that traffic from recipient goes backwards to the final Tor network points.

## **Anonymous hidden services**

In 2004 Tor started to make servers anonymous, hiding their location in the World Wide Web using special options of anonymous network. It is possible to gain access to some hidden services only using Tor client.

The access to hidden services can be gained with using special pseudo-domains of the top level “.onion”. Tor networks identify them anonymously and send the data to some special hidden services. These hidden services process the data using usual software, which is tuned right for listening of closed interfaces. Such domain “.onion addresses” are generated on the opened server key and composed of 16 numbers and Latin letters.

## **Restrictions**

Tor is aimed to hide client's connection to server. But complete hiding conceptually can't be achieved, because coding here is just a way of achieving anonymity in the Internet. To gain a higher level of privacy, it is necessary to have additional communication hardware protection. Also it is preferable to use stenography methods while coding data.

## **Basic advantages of Tor Browser**

Tor browser has the following advantages:

Access to ANY web site from ANY part of the Earth, no matter what provider is;

Tor browser changes client's IP, so complete anonymity is guaranteed;

The browser is very easy to install and its usage is absolutely free;

Networks of Repeaters can be used as well;

Protection from web tailing threatening to data privacy;

Security threatening functions are automatically blocked;

Protection packet cannot to be installed. It is started from all the devices, even portable.

Basic disadvantages of Tor

Tor Browser also has some disadvantages:

Too low loading speed;

Not all the videos can be played;

Rather low security.

## 4. Setup of Tor

**Tor for Windows.** Downloading of Tor Browser Bundle.

Open any browser (Mozilla Firefox, Internet Explorer or other) and enter in an address line: <https://www.torproject.org/projects/torbrowser.html.en>. If you find Tor Browser Bundle by means of the searching system, make sure in the rightness of the address.



Push the large violet button “DOWNLOAD”, to set up the file of installation of the program Tor Browser Bundle.



A web site will define your operating system automatically; loading of necessary file will begin. If for some reasons you want to load the file of installation for other operating system, you can choose a necessary version from a list.

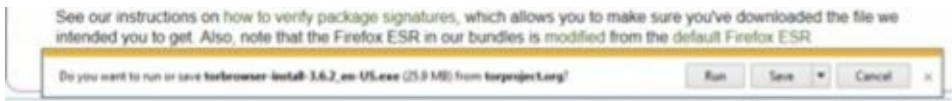
### Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

Language	Microsoft Windows (3.6.2)	Mac OS X (3.6.2)	Linux (3.6.2)
English (en-US)	32/64-bit (.sig)	32-bit (.sig)	32-bit (.sig) • 64-bit (.sig)
العربية (ar)	32/64-bit (.sig)	32-bit (.sig)	32-bit (.sig) • 64-bit (.sig)



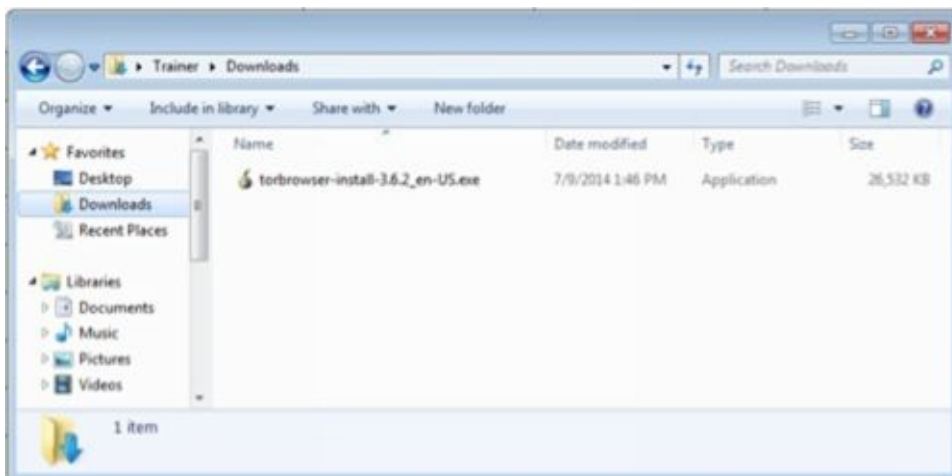
Many browsers will ask confirmation of your intention to get a file. Internet Explorer 11 displays the field with the orange framing in the lower part of window of browser.



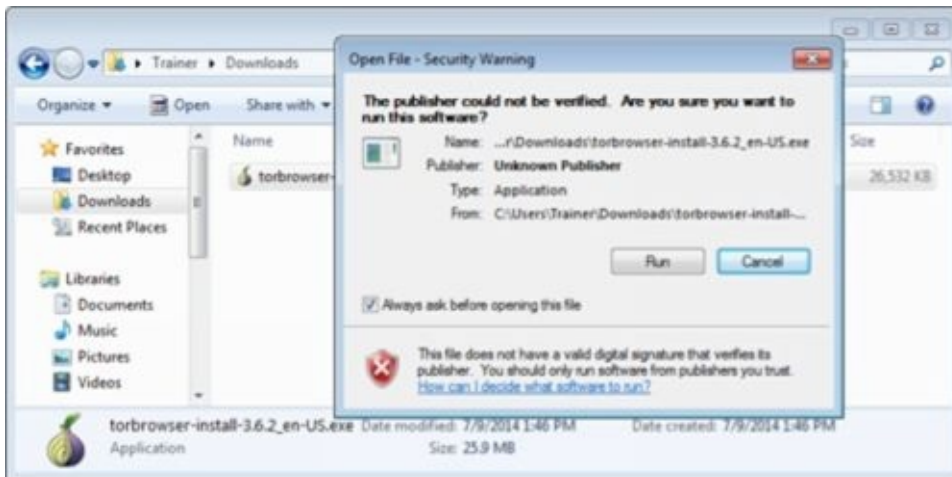
At first it is recommended to save a file on a disk independently of your browser. Push the button “Save”. Here is shown the program Tor Browser Bundle version 5.0.4, which was actual during writing this text. Now, probably, fresher version of the program is accessible.

## Setup of Tor Browser Bundle

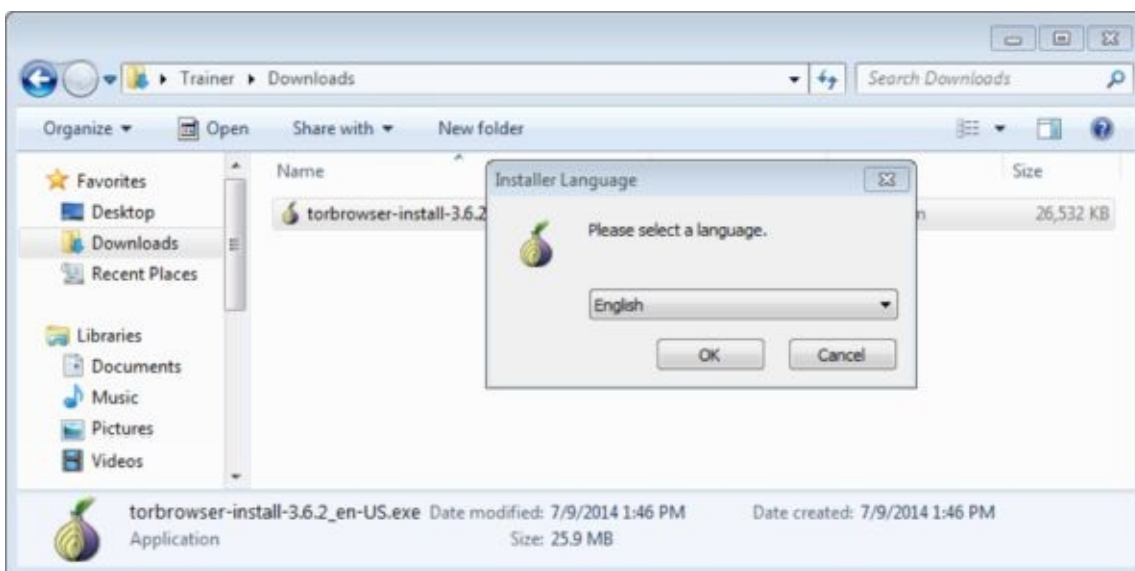
When the loading finishes you, maybe, will be suggested to open a folder where file was stored in. By default it is a folder “Downloads”. Start the file torbrowser-install-3.6.2 en-US.exe by a double click.



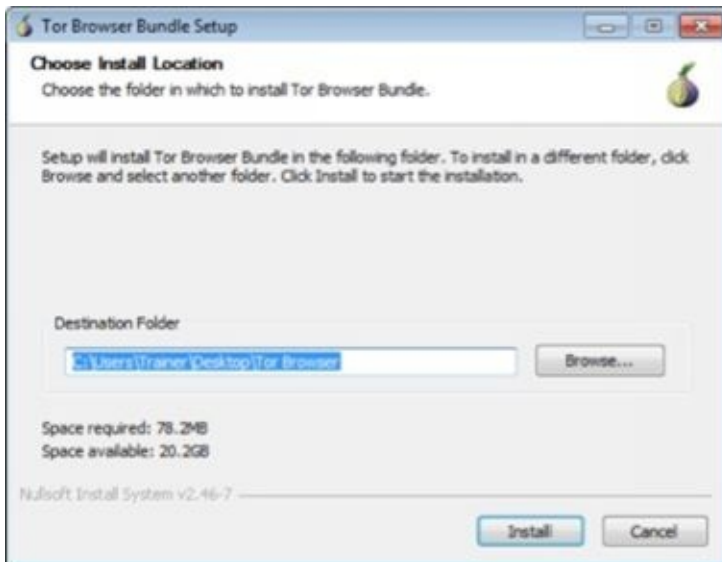
After a double click on the file of installation a window will be opened with warning of origin of the program. It is always needed to take seriously such warnings. It is important to make sure, that you can trust the set software, that you got an authentic copy from an official web site on a safe communication channel. You know in this case, that you need and where to get the program. Downloading was taken from the safe HTTPS web site of project Tor. Press “Run”.



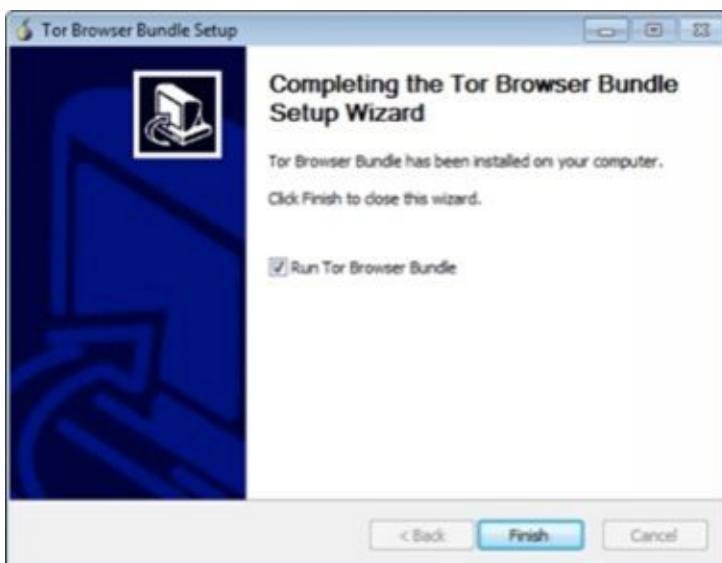
The window of choice of the language of Tor Browser Bundle will be opened. Choose a language from a few variants and press “OK”.



In a next window it is suggested to choose a folder for setting of Tor Browser Bundle. By default a desktop is indicated. It is possible to change the place of setting, but while we leave an address without changes.



You will see a window reporting about completion of setting. Push the button “Finish”. Tor Browser will be started automatically. While clean a mark in the point of “Run Tor Browser Bundle”. We will go back to the use of Tor Browser Bundle after a while. If you forgot to clean a mark and the program Tor Browser was started, simply close a window.



Tor Browser Bundle will not be set in the system, as other programs, and will not be displayed in a menu “Starting” of your computer.



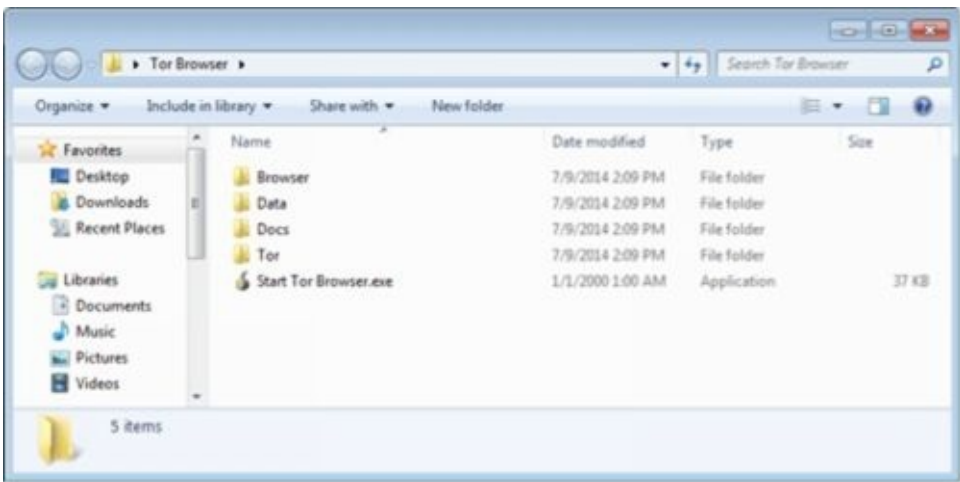
**Use of Tor Browser Bundle**

**First start of Tor Browser**

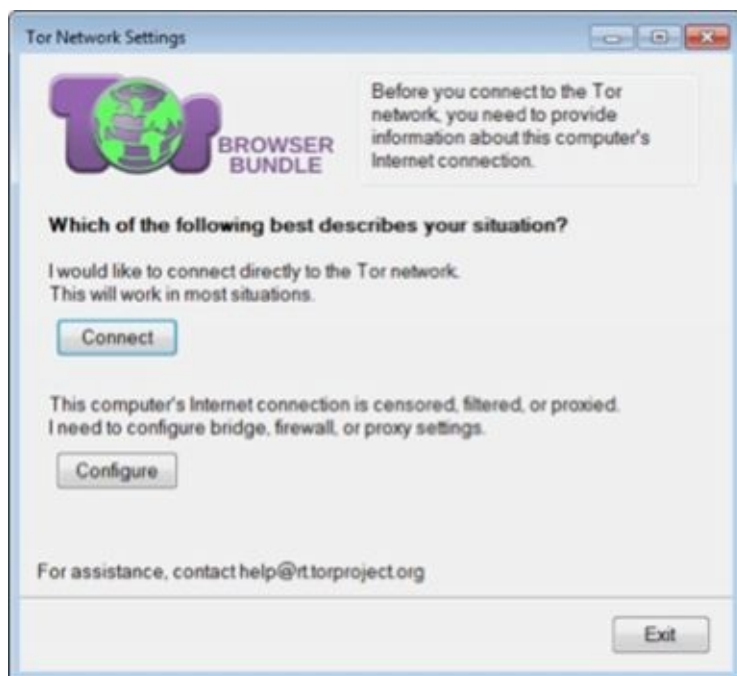
Upon completion of setting we decided not to start Tor Browser, therefore now you will start the program for the first time. If you followed all instructions in the process of setting, then you will see on your desktop a folder named “Tor Browser”.



Open the folder “Tor Browser” and double click will start the file “Start Tor Browser”.



At the first start of Tor Browser you will see a window that will allow you if it is necessary to change some tuning. Maybe, you will want to go back to them later, and while try to connect to the network of Tor, pushing the button “Connect”.

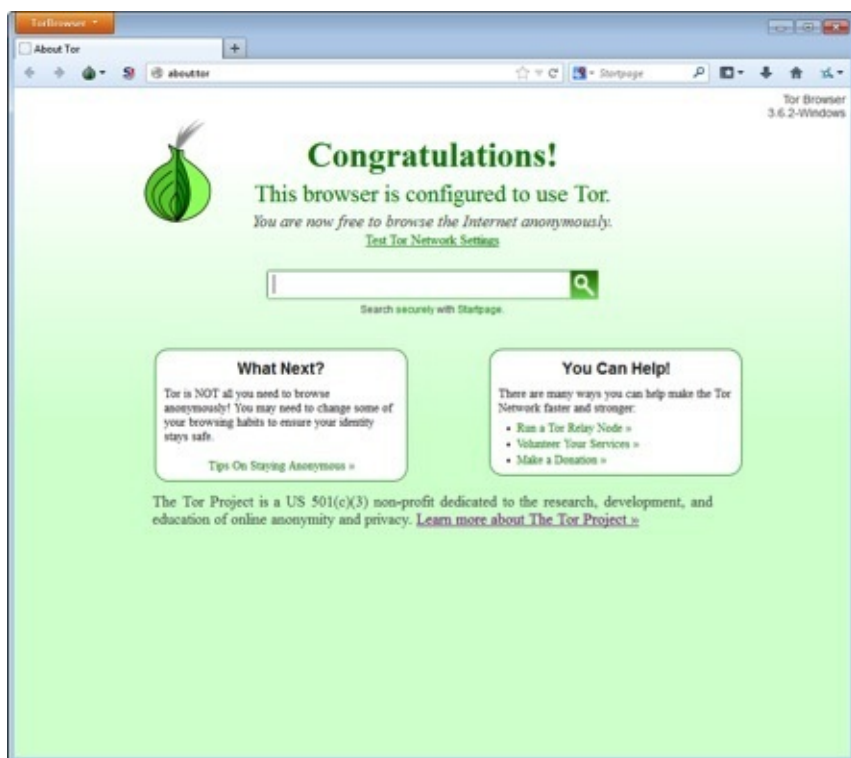


After that a new window will appear with green field, which at the start of Tor will be opened a bit longer.



At the first start of Tor Browser it may need very little more time, that usual, but show patience. In a few minutes Tor Browser will tune connection. A web-browser will appear that will congratulate you with successful start.





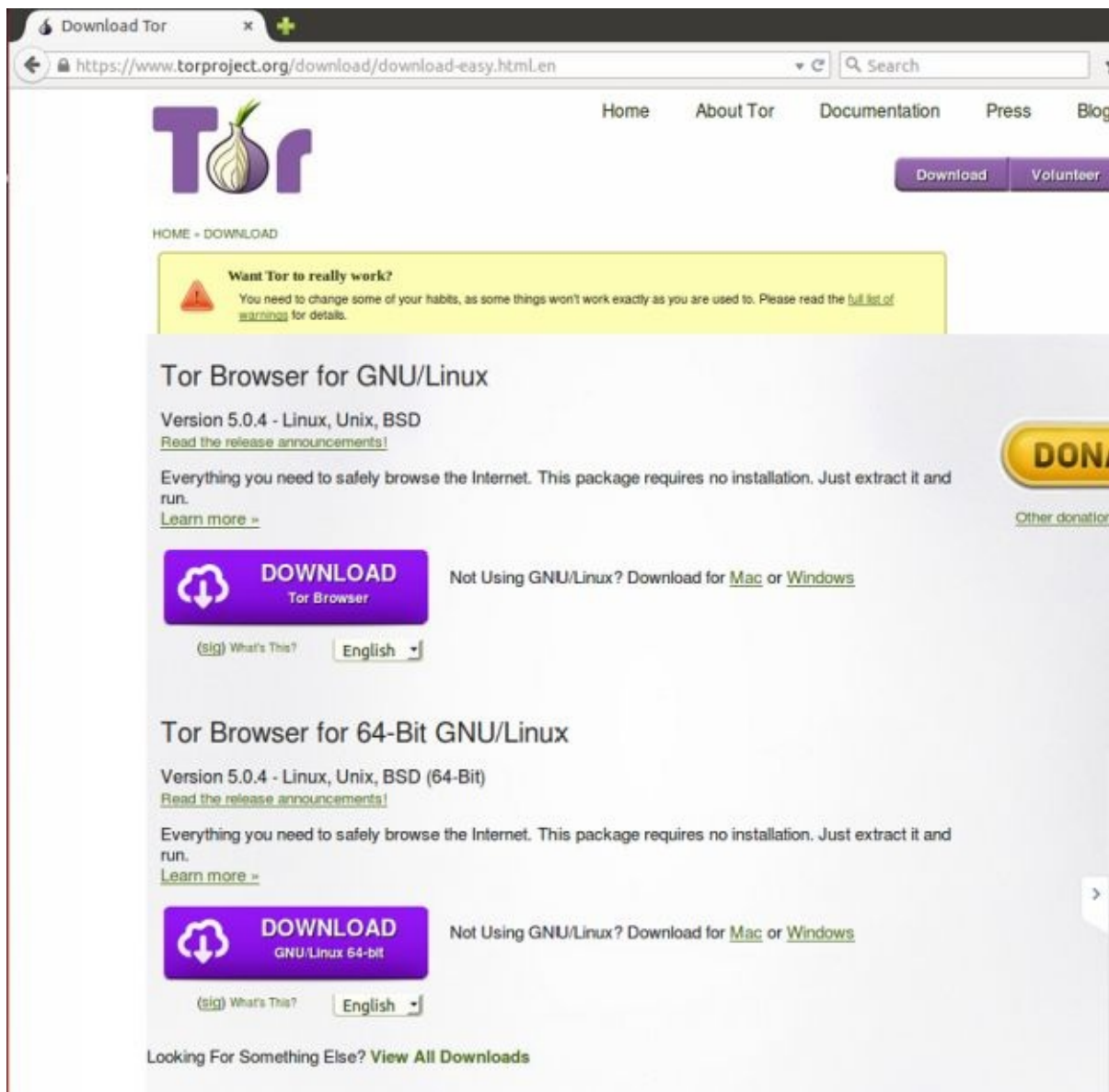
## Tor for Ubuntu

To set up Tor Browser in Ubuntu is to download it from official site. It is the most correct and right way.

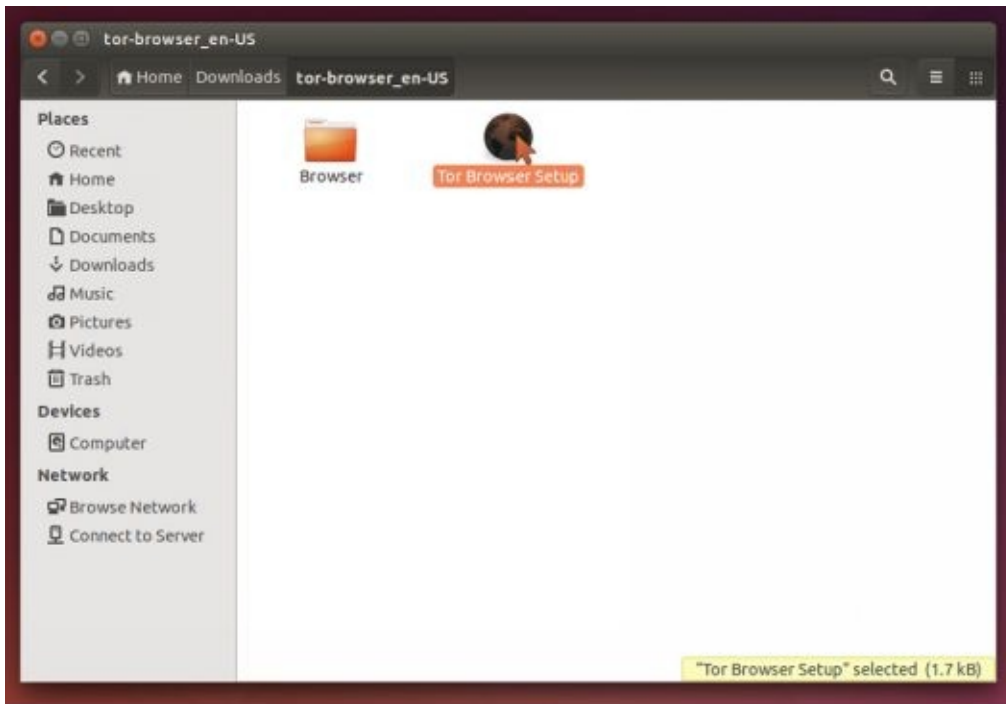
The most correct and right way to set up Tor Browser is to download it from official site

<https://www.torproject.org/download/download-easy.html.en>

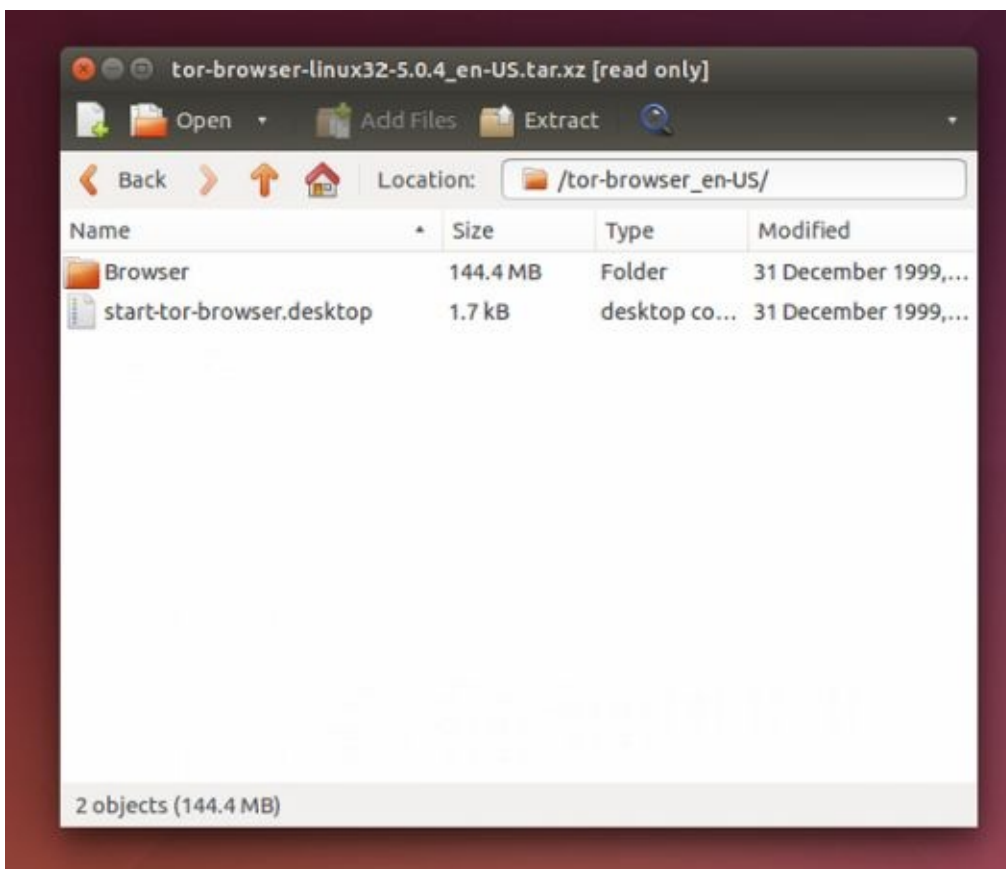
Choose the version the version according to architectural system, choose Eng and download:

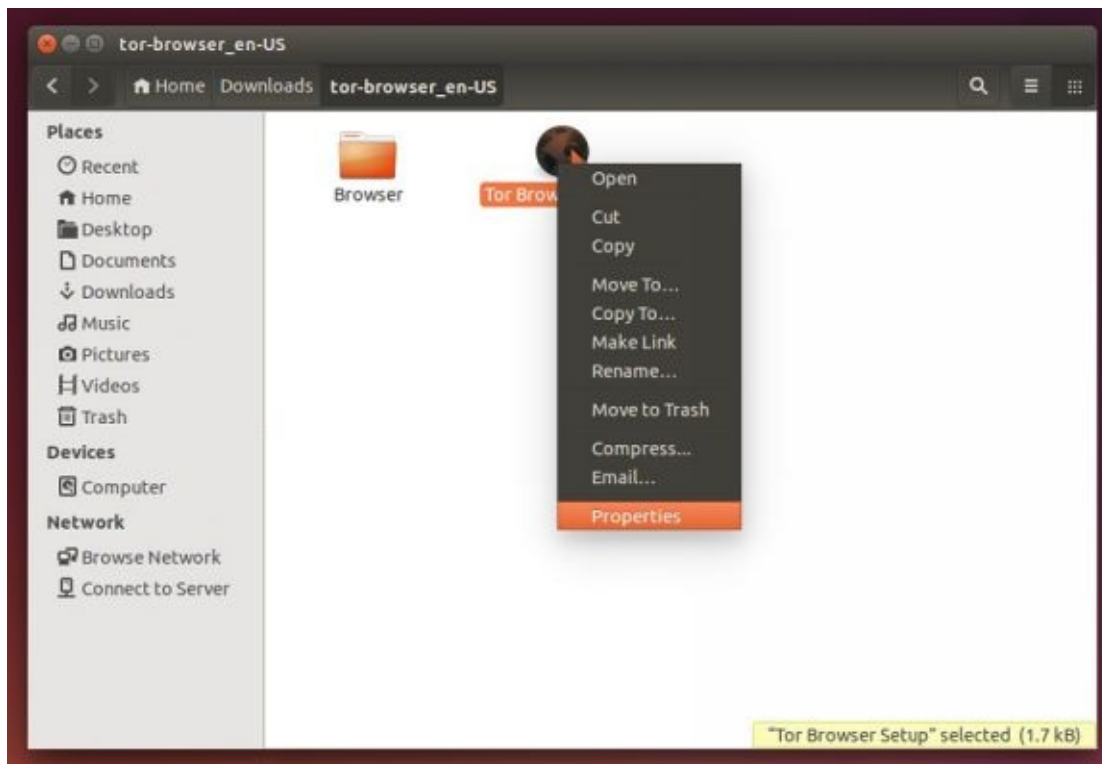


The screenshot shows the Tor Project website's download page. At the top, there's a navigation bar with links for Home, About Tor, Documentation, Press, and Blog. A large Tor logo is on the left, and 'Download' and 'Volunteer' buttons are on the right. Below the logo, a yellow warning box states: 'Want Tor to really work? You need to change some of your habits, as some things won't work exactly as you are used to. Please read the [full list of warnings](#) for details.' The main content area is titled 'Tor Browser for GNU/Linux' and 'Version 5.0.4 - Linux, Unix, BSD'. It includes a link to 'Read the release announcements!' and a paragraph: 'Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.' Below this is a large purple 'DOWNLOAD Tor Browser' button. To the right of the button, it says 'Not Using GNU/Linux? Download for [Mac](#) or [Windows](#)'. At the bottom of the button area, there are links for '(sig) What's This?' and a language dropdown set to 'English'. The same structure is repeated for 'Tor Browser for 64-Bit GNU/Linux' with 'Version 5.0.4 - Linux, Unix, BSD (64-Bit)'. At the very bottom, it says 'Looking For Something Else? [View All Downloads](#)'.

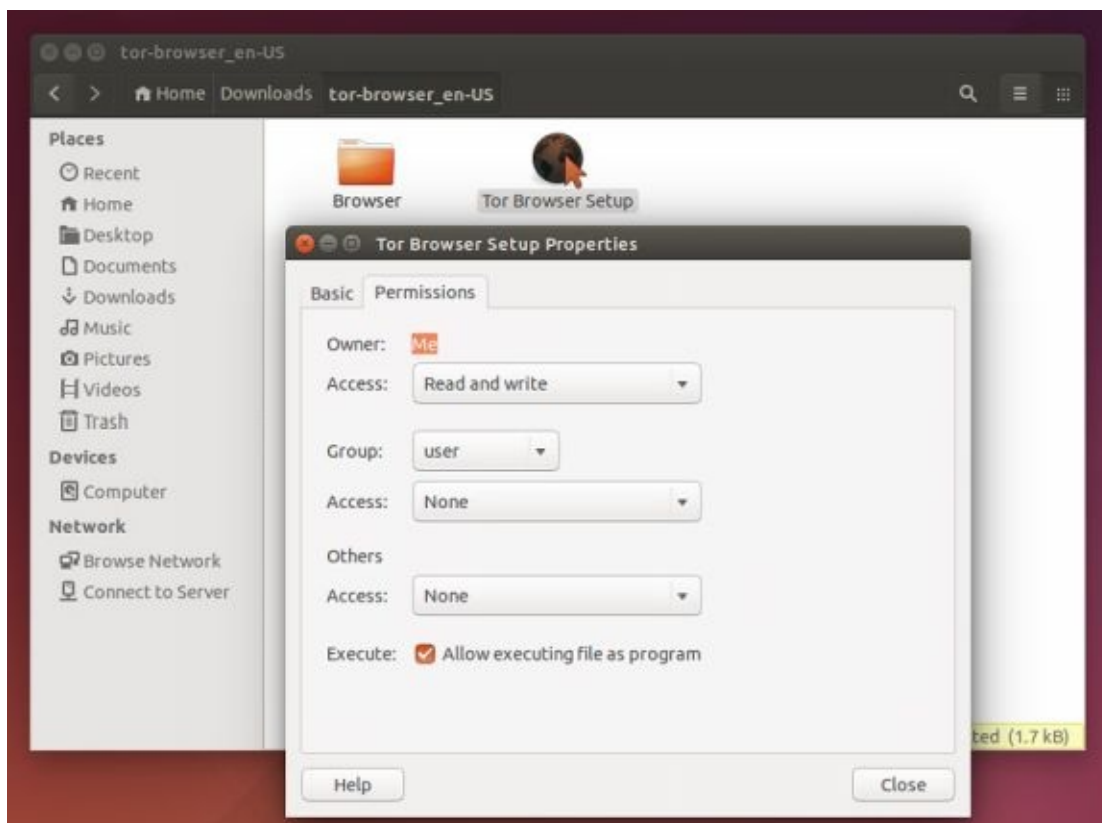


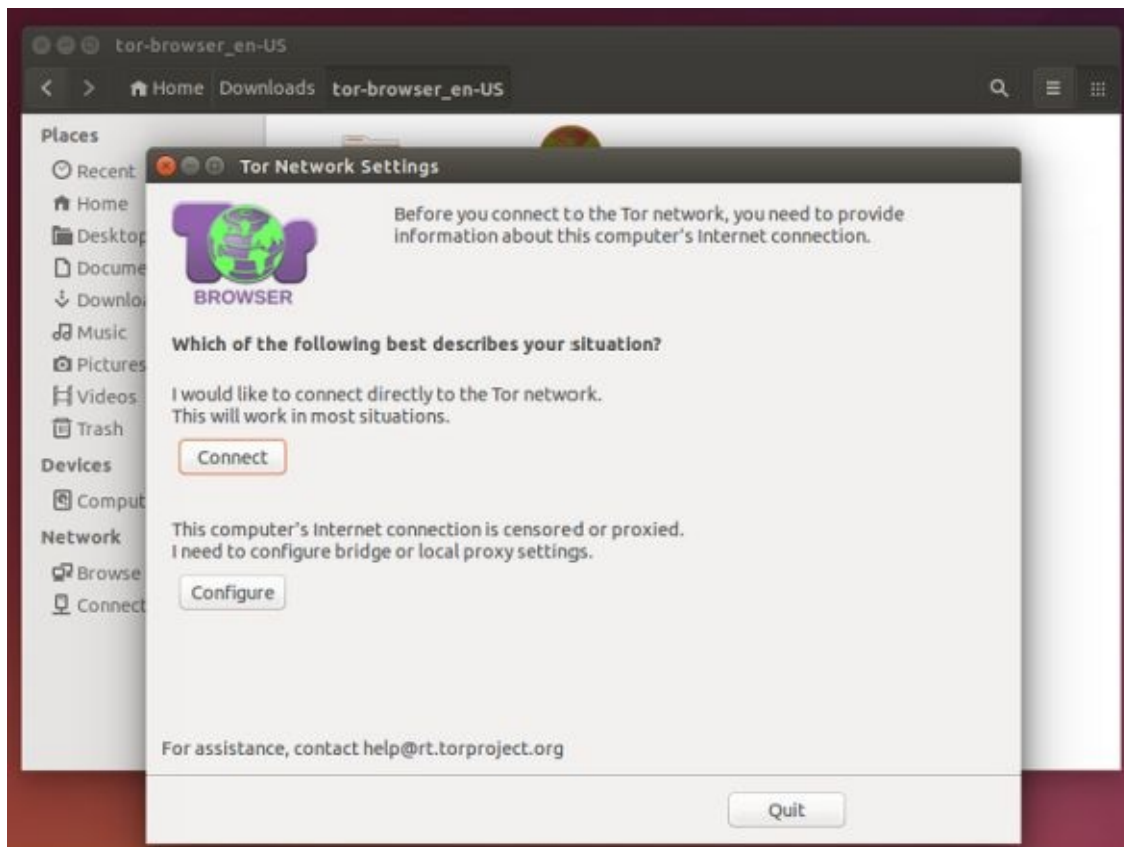
Unpack downloaded achieves in home catalogue, move into it: there will be the following executing file





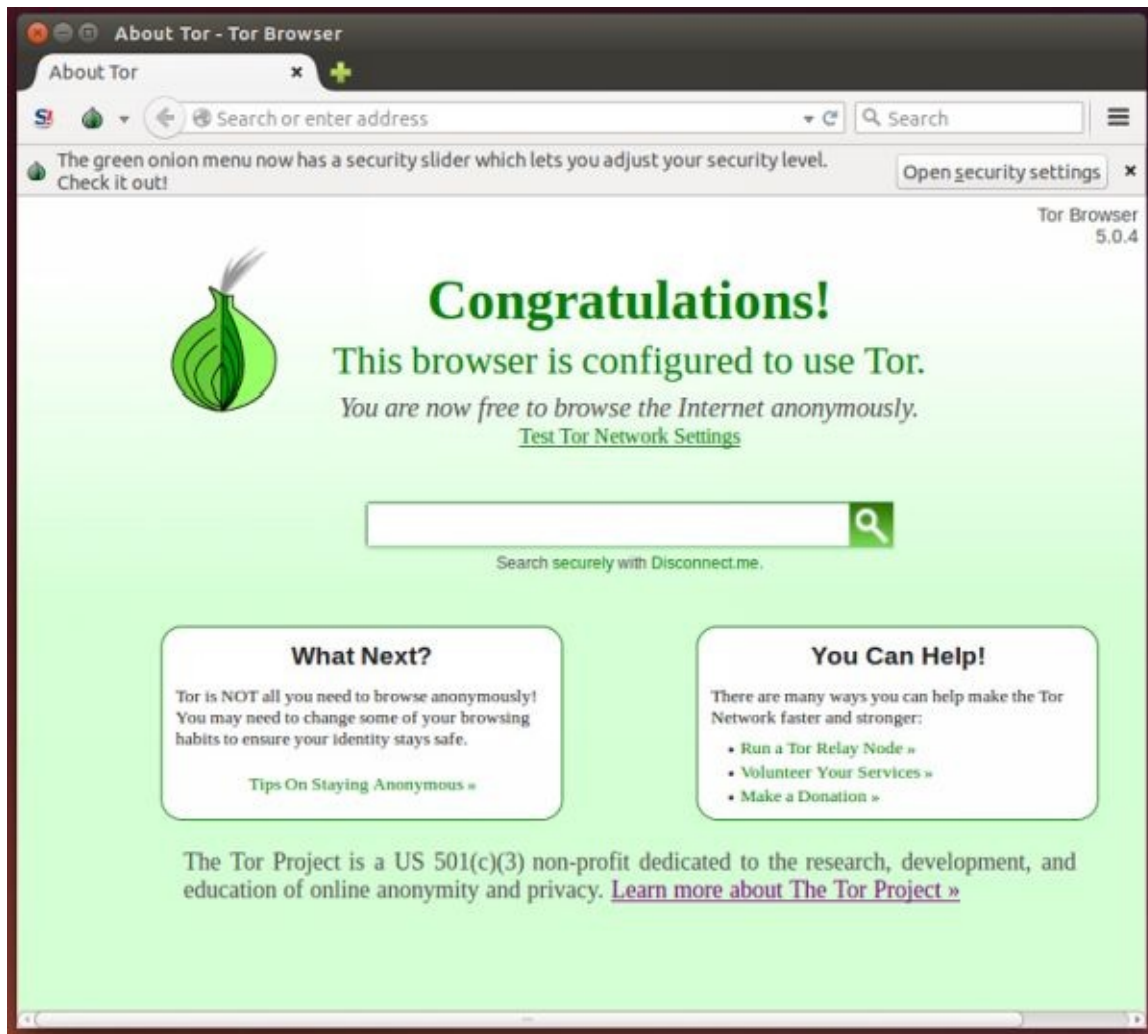
We expose the permission to execution in the properties







That's all; now, double click on this file will open Tor Browser

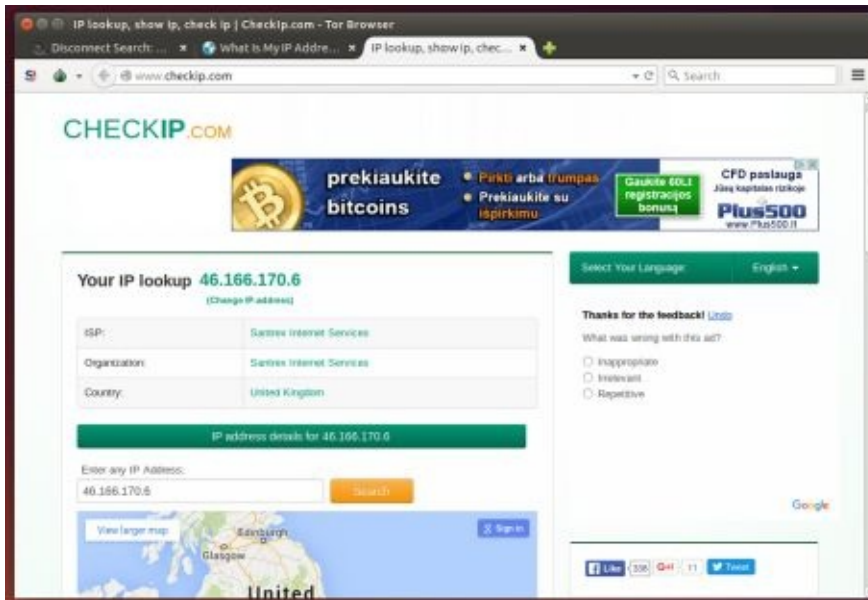


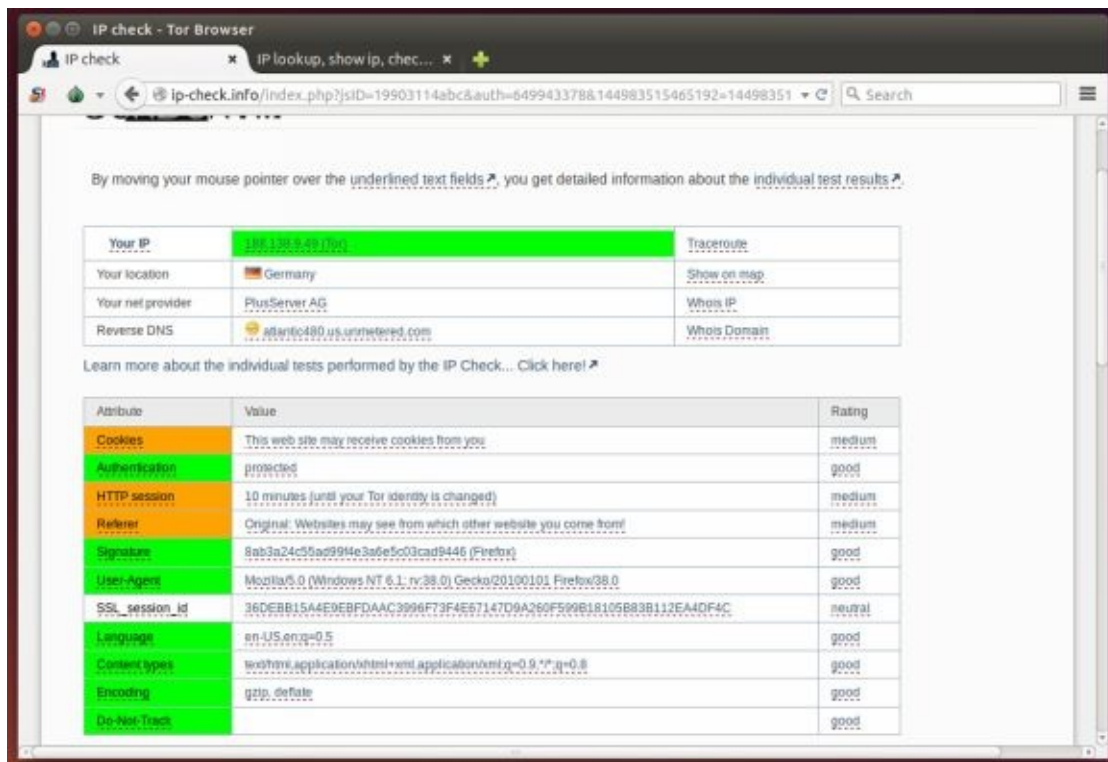
If after double click Tor Browser doesn't open, and instead of that text editor opens, you should allow execution of scripts in settings of the file manager Nautilus:

If you want to create a label on the appendix in the main Dash menu, you can read on the Internet it.

Start Tor Browser we move to the site for checking IP.

And if everything is all right, we will see something like this





*Where am I from? Of course, from the Germany, and moreover, the operation system is “Windows”*

Installation of Tor Browser in Ubuntu 14.04-12.04 in the repository

Installation option from a repository not of the latest version: in order to install Tor Browser Bundle in Ubuntu, open the terminal and do the following steps according to your system

For Ubuntu 32-bit:sudo add-apt-repository ppa:upubuntu-com/tor

sudo apt-get update

sudo apt-get install tor-browser

sudo chown \$USER -Rv /usr/bin/tor-browser/

For Ubuntu 64-bit:sudo add-apt-repository ppa:upubuntu-com/tor64

sudo apt-get update

sudo apt-get install tor-browser

sudo chown \$USER -Rv /usr/bin/tor-browser/

That's all, the program is installed and you can find it with the help of menu Dash

**Other languages of Tor Browser Bundle when installation is from repository**

Tor Browser is Firefox of stable version, we will change other languages

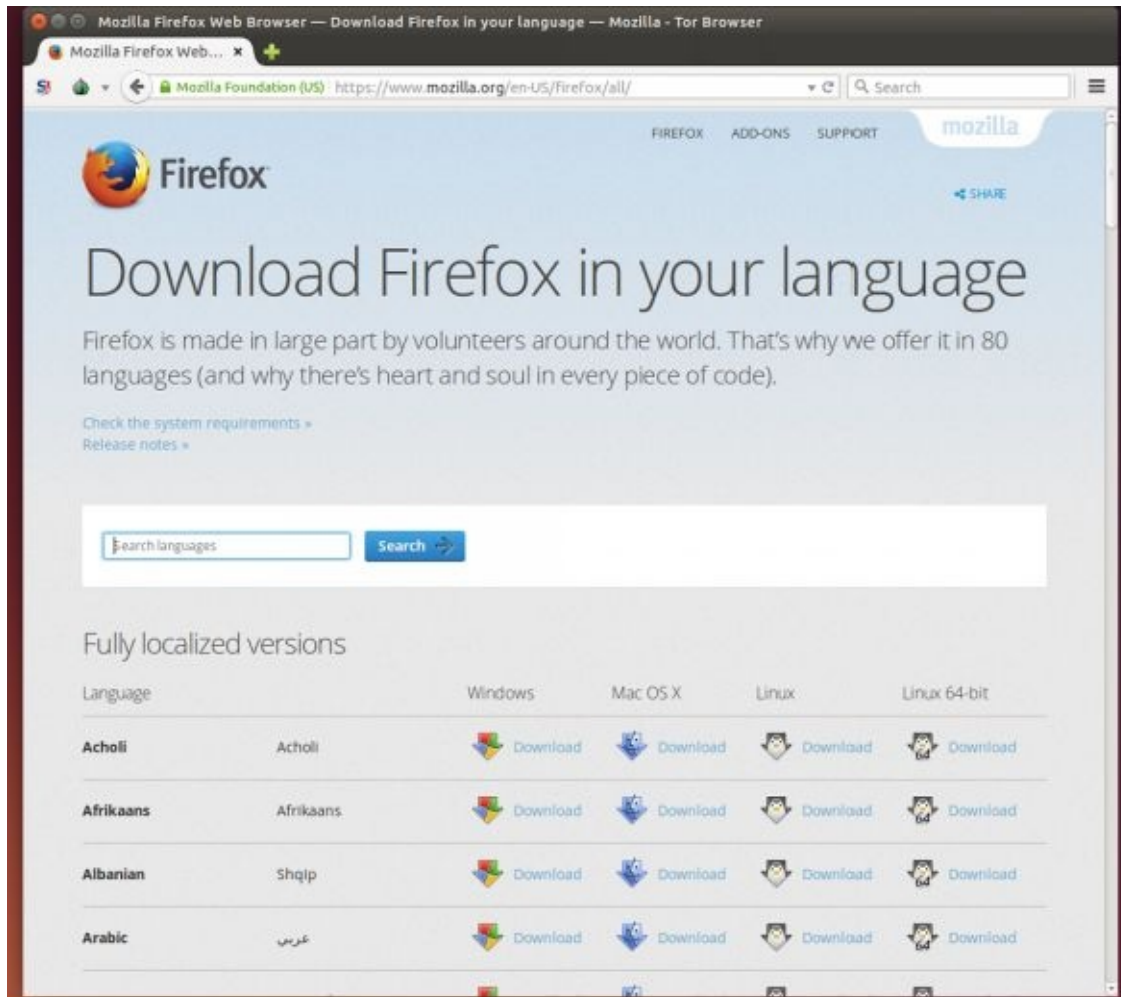
Remove in the insert Help-About Tor Browser



Look at the version of browser and move on the page with other languages

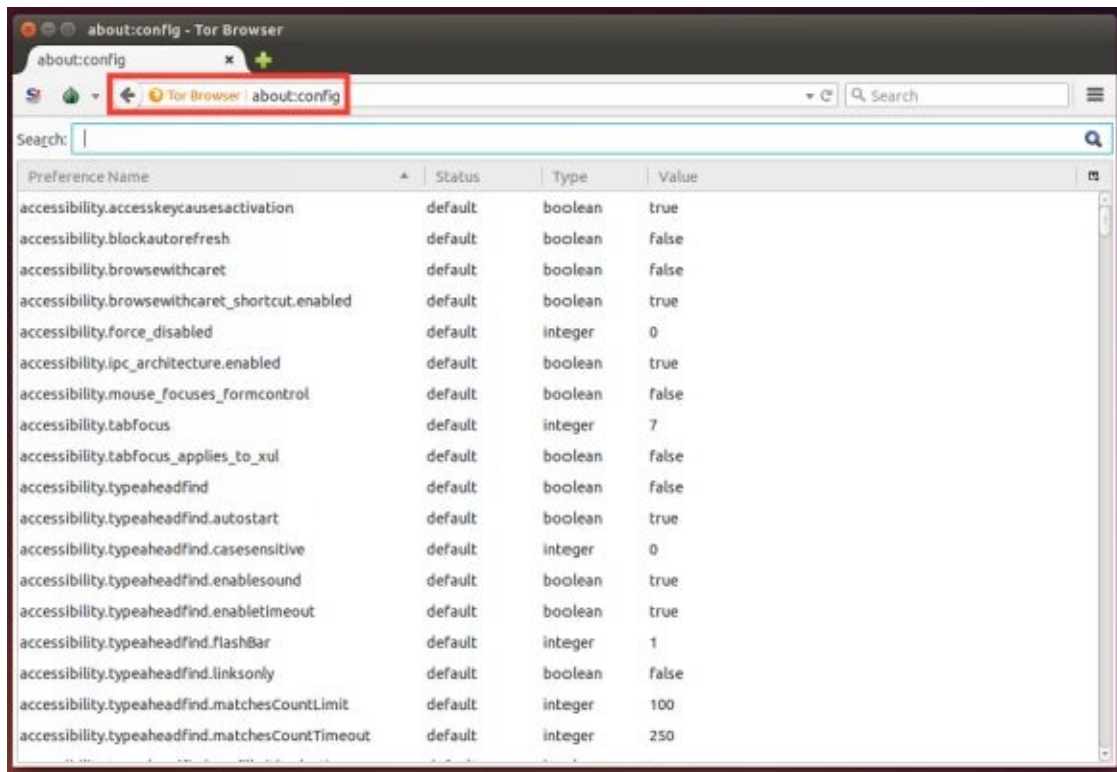
[Mozilla-Firefox](https://www.mozilla.org/en-US/firefox/all/)

Opposite your version of browser download the package with **other languages** and install it

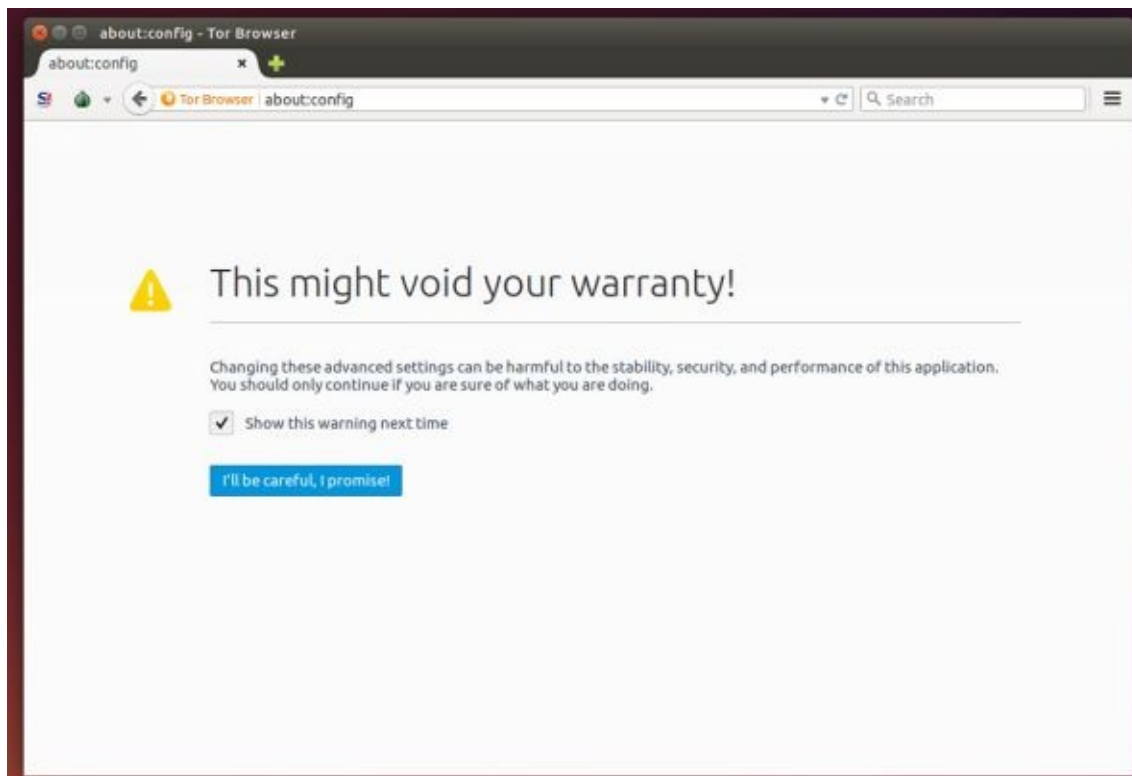




Then enter in the line of address  
*about:config*

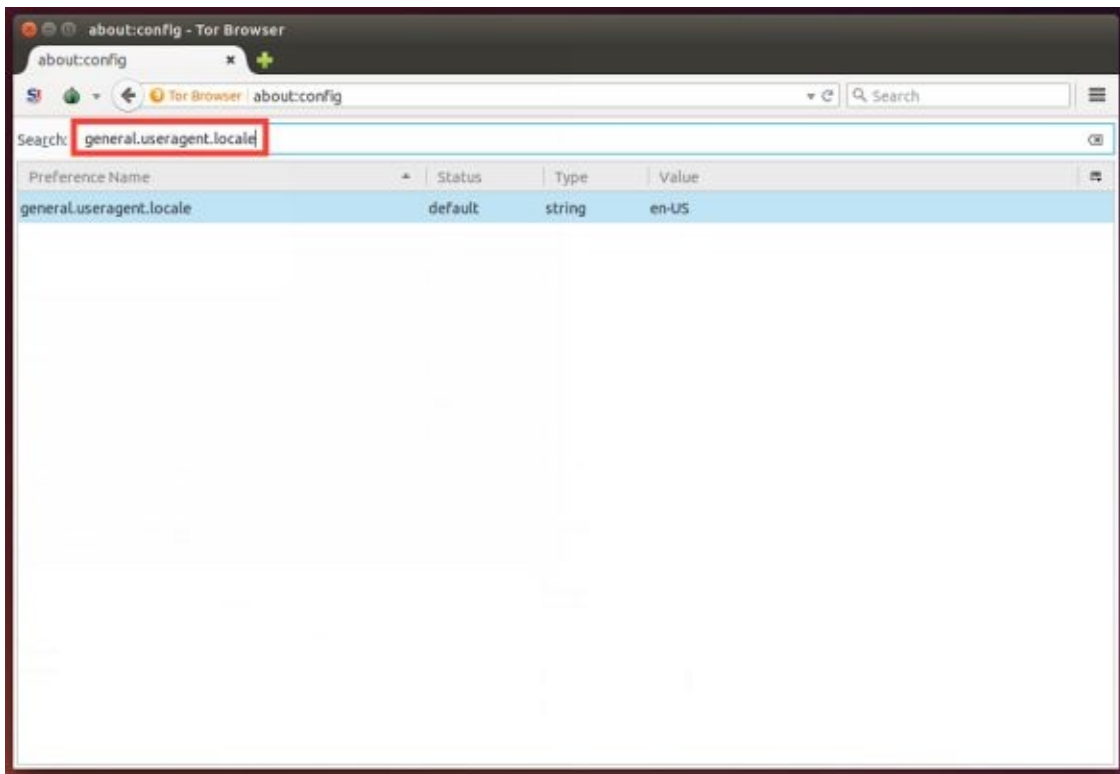


Agree that we will be careful *"I'll be careful, I promise!"*

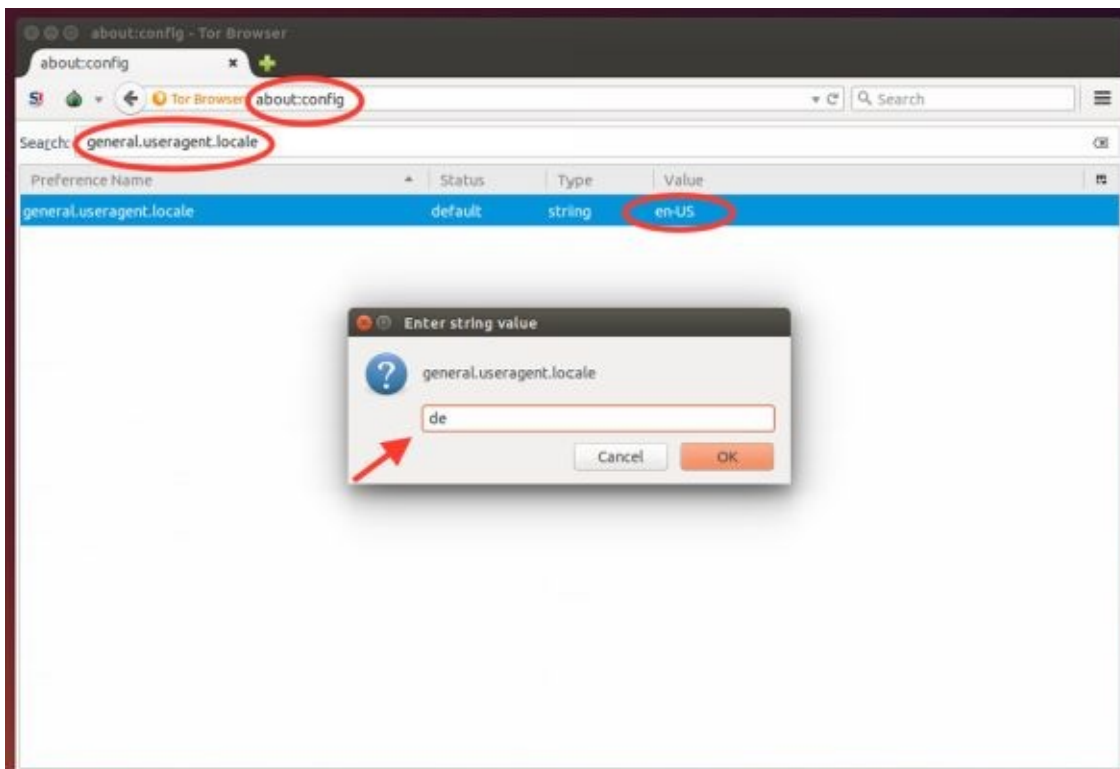


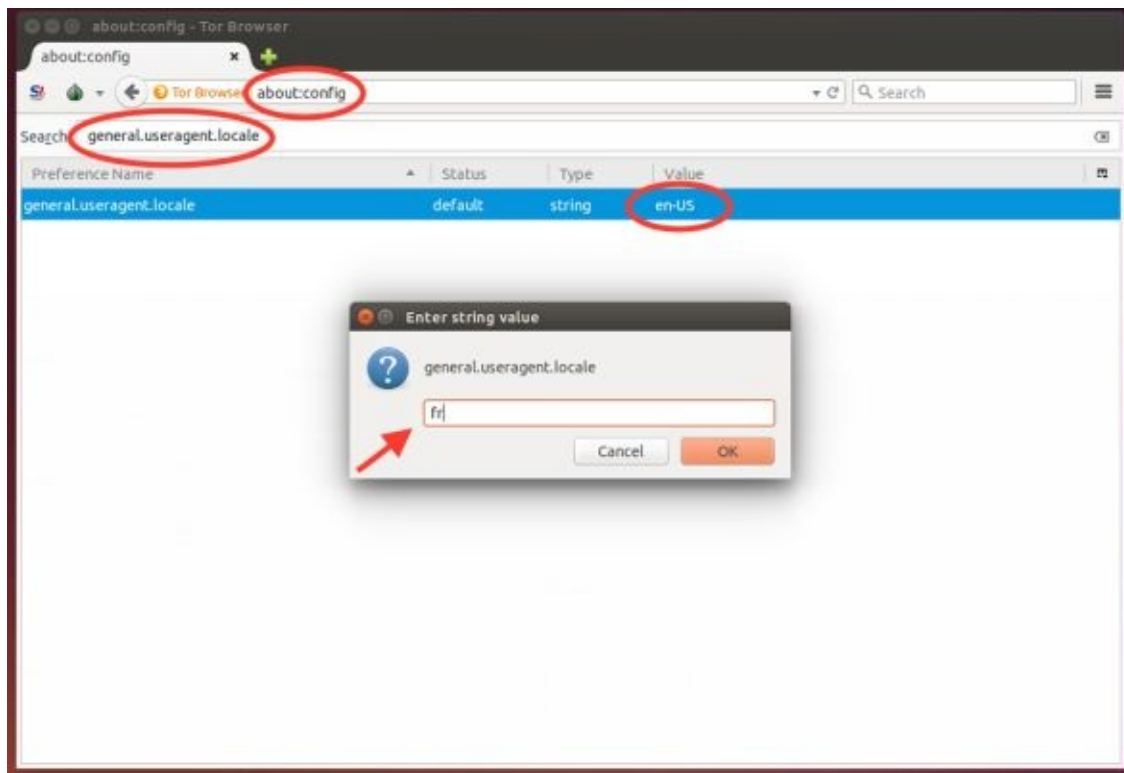
Then enter in the line of search

***general.useragent.locale***



And change the meaning of this parameter from en-US on de (fr)





That's all, and now you just restart Tor Browser.

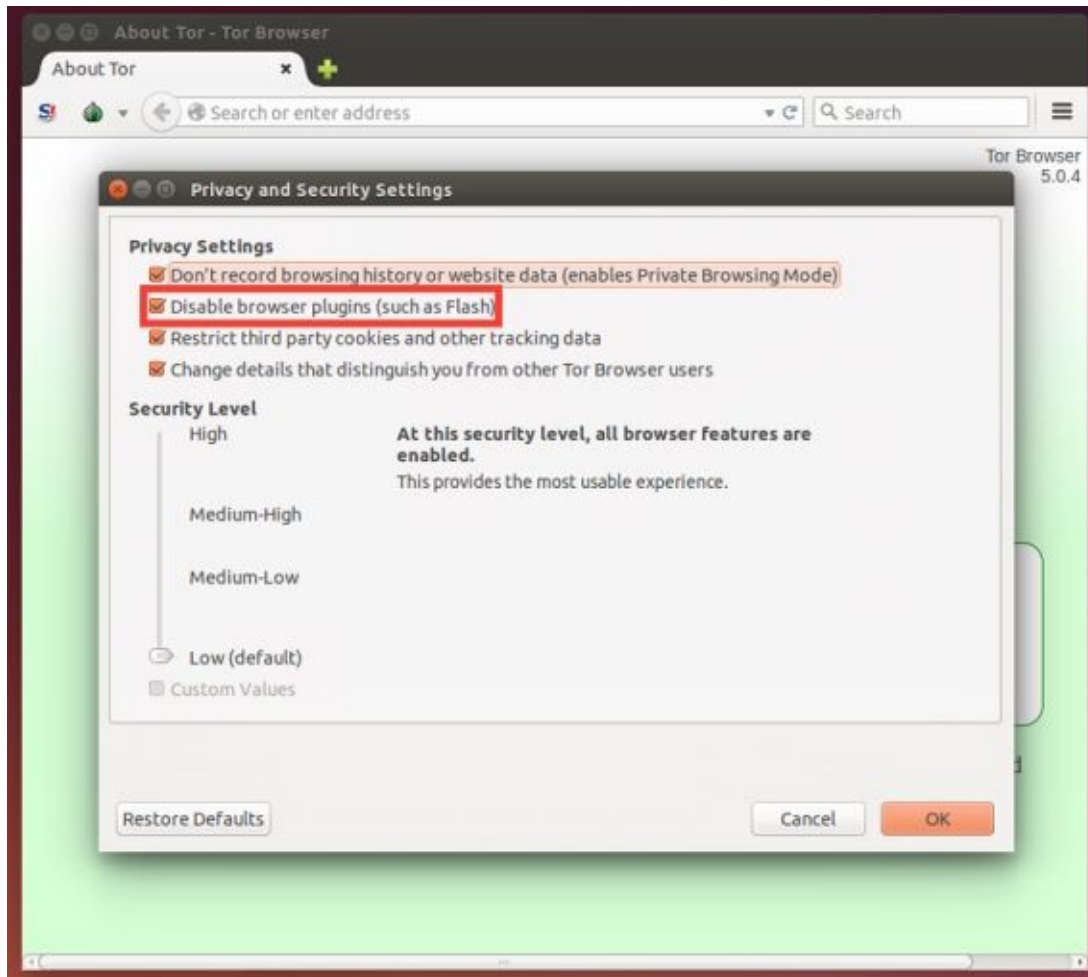
Now it is possible anonymously “to wander about the networks”

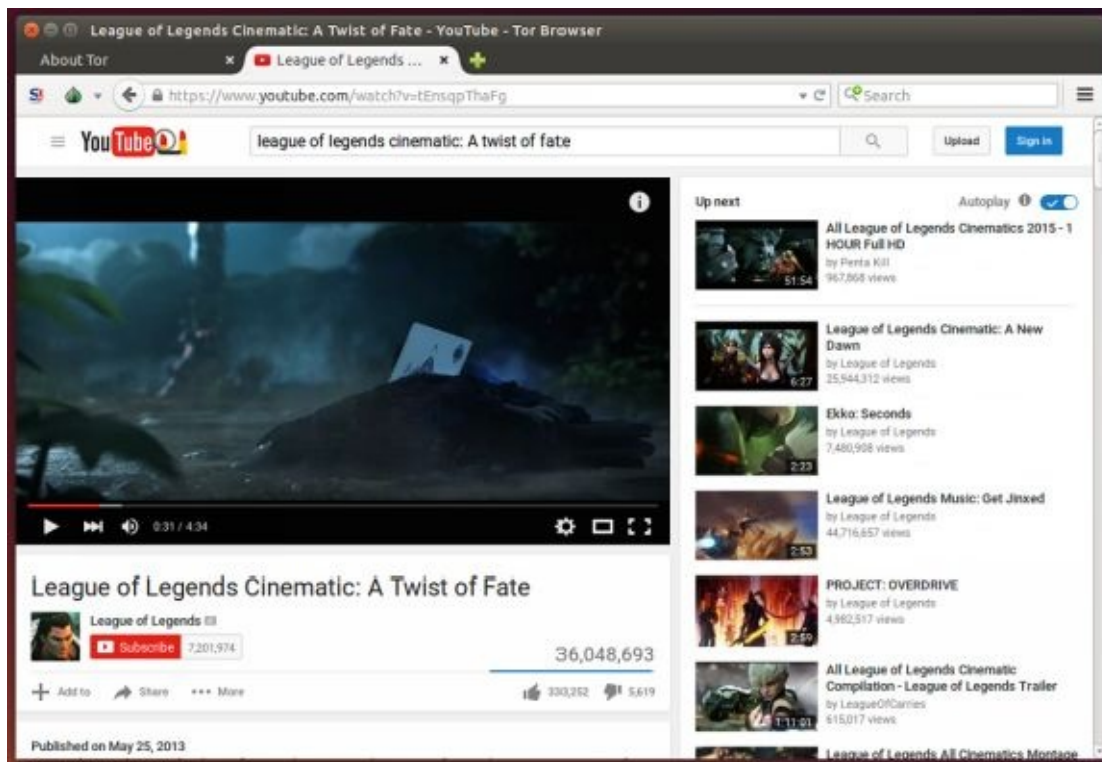
## Turn on Flash Plugin and JavaScript in Tor Browser

If you want to watch flash movies in this browser, it is easy to turn on it. Also it is possible to allow execution of scripts. But in this case the safety is minimized!

I don't advise to do it confirmed paranoiacs.

So, if you want flash begins to work





Move in “Tools” – “Additions”

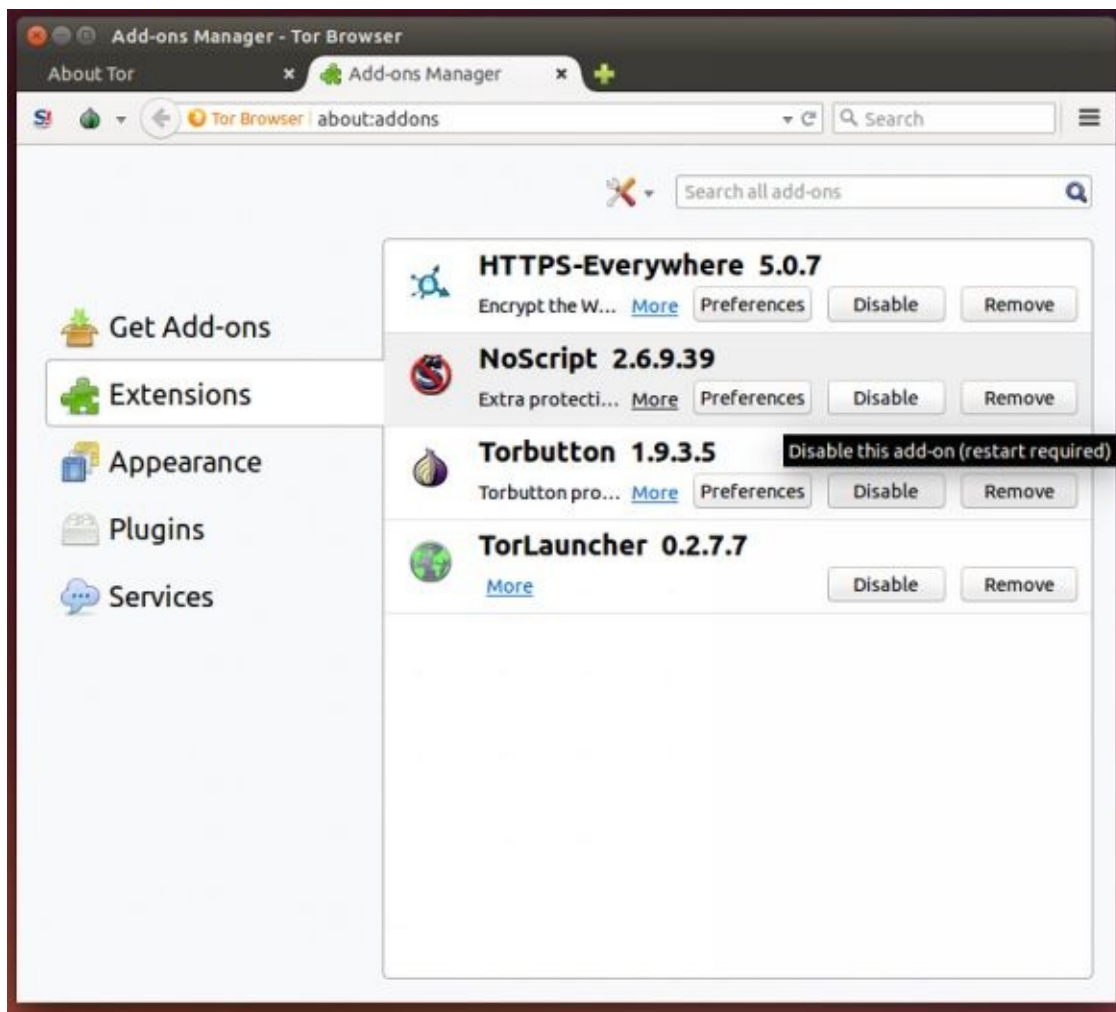
On the insert “Plug-ins” switch on Shockwave flash.



That’s all, now move on your favourite site and watch videos online, for the example on YouTube.



Also, here in the point “Expansions” it is possible to turn off the expansion, which blocks scripts on the sites:



That's all, now it is possible to watch also flash videos and scripts will be executed.

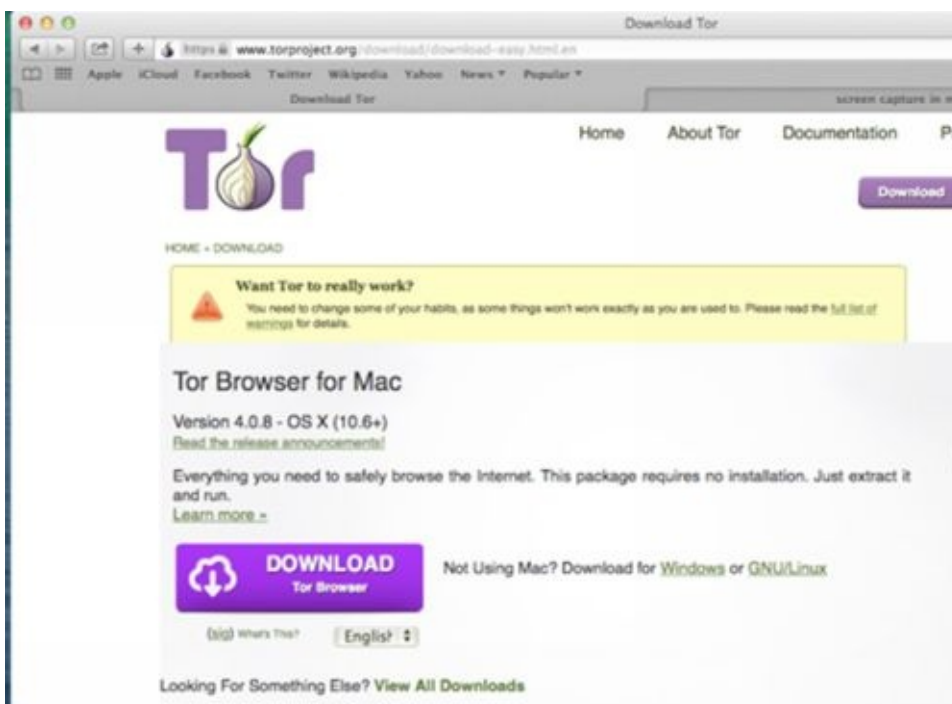
But I repeat, this everything breaks safety, for the sake of what we also install this program.

## Tor for Mac

### Receipt of Tor Browser Bundle

Open any browser (Mozilla Firefox, Safari or other) and enter in an address line: <https://www.torproject.org/projects/torbrowser.html.en>. If you find Tor Browser Bundle by means of the searching system, you will make sure in the rightness of the got address.

Push the large violet button “DOWNLOAD”, to get the installation of the file of program Tor Browser Bundle.



The website will define automatically your operating system; loading of the necessary file will begin. If for any reason you want to load the installation file for other operating system, you can choose the necessary version from the list.

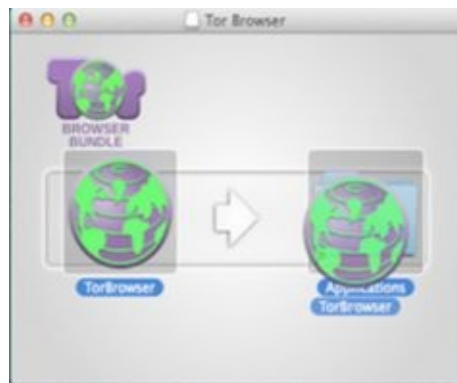
If you use Safari, downloading of Tor Browser Bundle will begin. If you use Firefox you will be offered to open or save a file. It is always better to save a file, that's why pushing the button “Save”. In this instance Tor Browser Bundle version 4.0.8 is presented, being actual in the moment of publication of this guidance. To the moment of reading, maybe, fresher version of the program will appear.

## Setup of Tor Browser Bundle

After completion of downloading, maybe, you will be suggested to open a folder where file was stored in. By default it is a folder of “Downloads”. Start the file Tor browser - 4.0.8 - osx32 \_ en - US.dmg by a double click.



A window will appear suggesting to set Tor Browser Bundle by dragging the program in the folder of applications. Do it.

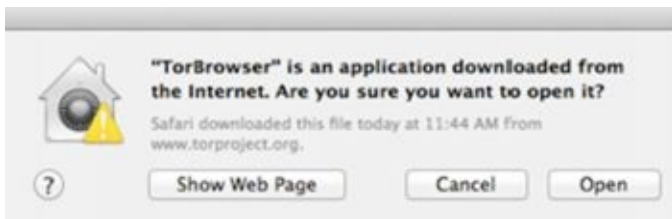


Now the program Tor Browser is set in the folder of applications.

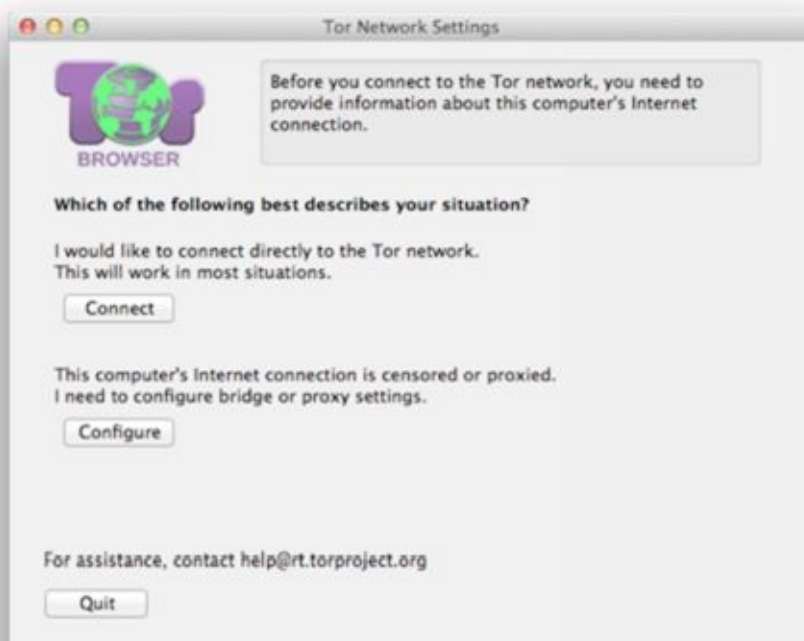
## Use of Tor Browser Bundle

To start Tor Browser in the first time, find the program in Finder or (in more update versions of OS X) in Launchpad.

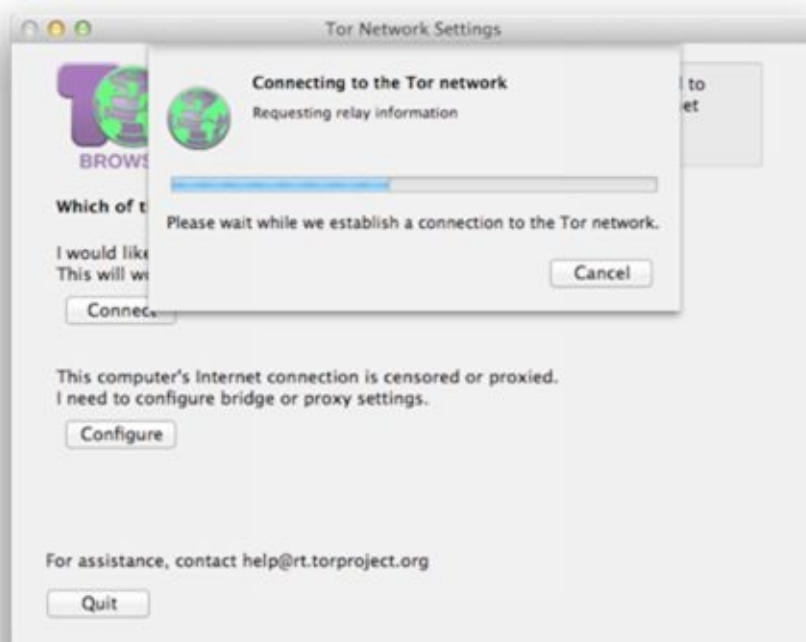
After click on the icon of Tor Browser a window will appear with warning of origin of the program. It is needed to take seriously such warnings. It is important to make sure, that you can trust the set software, got a true copy from an official web-site on a safe communication channel. You know in this case, what you need and where to get the program. Downloading was made from the protected HTTPS web-site of project Tor. Press “Open”.



At the first start of Tor Browser you will see a window that will allow you if it is necessary to change some tuning. Maybe, you will want to go back to it later, but while try to be connected to the network of Tor, pushing the button “Connect”.



After it a new window will appear with a green field that at the start of Tor will be opened a bit longer.



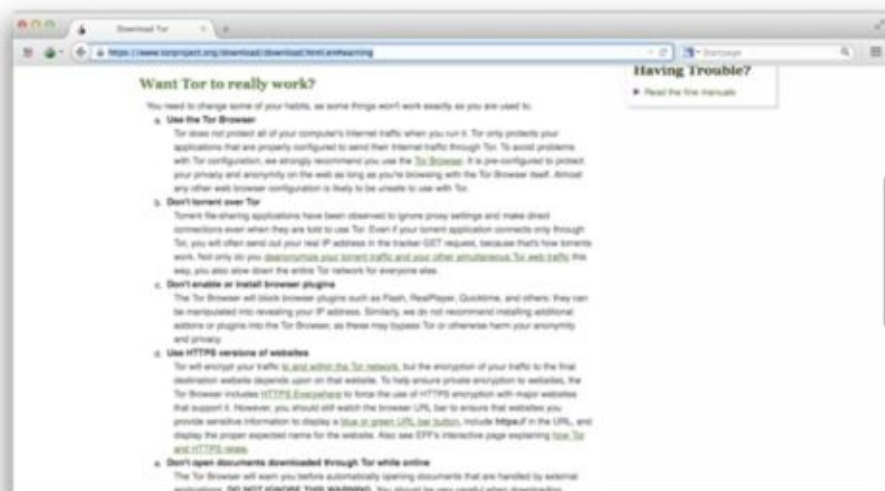
At the first start of Tor Browser it may need more time, than usually, but be patient. In a few minutes Tor Browser will connect. A web-browser will appear that will congratulate you with successful start.



You can check, whether you are connected to the network of Tor, visiting [check.torproject.org](https://check.torproject.org). If you are connected, a web site will report: “Congratulations. This browser is configured to use Tor”.



Web surfing through the network of Tor has some differences from ordinary work in the Internet. We recommend you to follow these advices for correct work in the web via Tor and for maintenance of your anonymity.



Now you are ready to the anonymous surfing through the network of Tor.

## 5. Configuring and running in bridge mode

### Installing Tor in bridge/relay mode

The installing itself is extremely simple – it is enough to download the distribution and run the setup.

There are two types of distribution: Tor Browser Bundle and Vidalia Bridge Bundle. Tor Browser Bundle is aimed just for safe browsing the Web. Vidalia Bridge Bundle allows not only safely access the Web but also widens Tor network using your PC.

#### 1. Warning of failing to run Tor bridge service:

```
[Warning] Could not bind to 0.0.0.0:443: Address already in use
[WSAEADDRINUSE].
```

Is Tor already running?

The reason is that the same port on the same computer was used by Skype. The problem can be solved in the following way: Vidalia Control Panel -> Settings -> Sharing -> Basic Settings -> Relay Port: here you should change 443 for another value, for example 4444 (This one wasn't used by any software)

#### 2. Warning of GEOIP files absence:

```
[Warning] Failed to open GEOIP file C:\Documents and Settings\User\Application
Data\tor\geoip. ...
```

```
[Warning] Failed to open GEOIP file C:\Documents and Settings\User\Application
Data\tor\geoip6. ...
```



The matter is that geoip and geoip6 files suddenly appeared in other directory, C:\Documents and Settings\User\Local Settings\Application Data\Tor. This problem can be solved by simple copying files to the proper directory.

### 3. Warning of impossibility to connect to bridge server from outside:

[Warning] Your server (aa.bb.cc.dd:4444) has not managed to confirm that its ORPort is reachable. Please check your firewalls, ports, address, /etc/hosts file, etc.

The reason is that D-Link router provides the Internet connection via NAT. To make port 4444 visible outside via global IP aa.bb.cc.dd, it is necessary to configure port forwarding from LAN out.

Tor-D-Link-port-forwarding.

### 4. Notice that your contact info is not set.

[Notice] Your ContactInfo config option is not set. Please consider setting it, so we can contact you if your server is misconfigured or something else goes wrong.

You do not have to set your contact info but you can do that. It can be done in Vidalia Control Panel -> Settings -> Sharing -> Basic Settings -> here you should fill the Nickname and Contact Info (your e-mail).

### 5. Warning of setting the “wrong” time:

[Warning] Received directory with skewed time (server ‘82.94.251.203:443’):

It seems that our clock is ahead by 56 minutes, 7 seconds, or that theirs is behind. Tor requires an accurate clock to work: please check your time, timezone, and date settings.

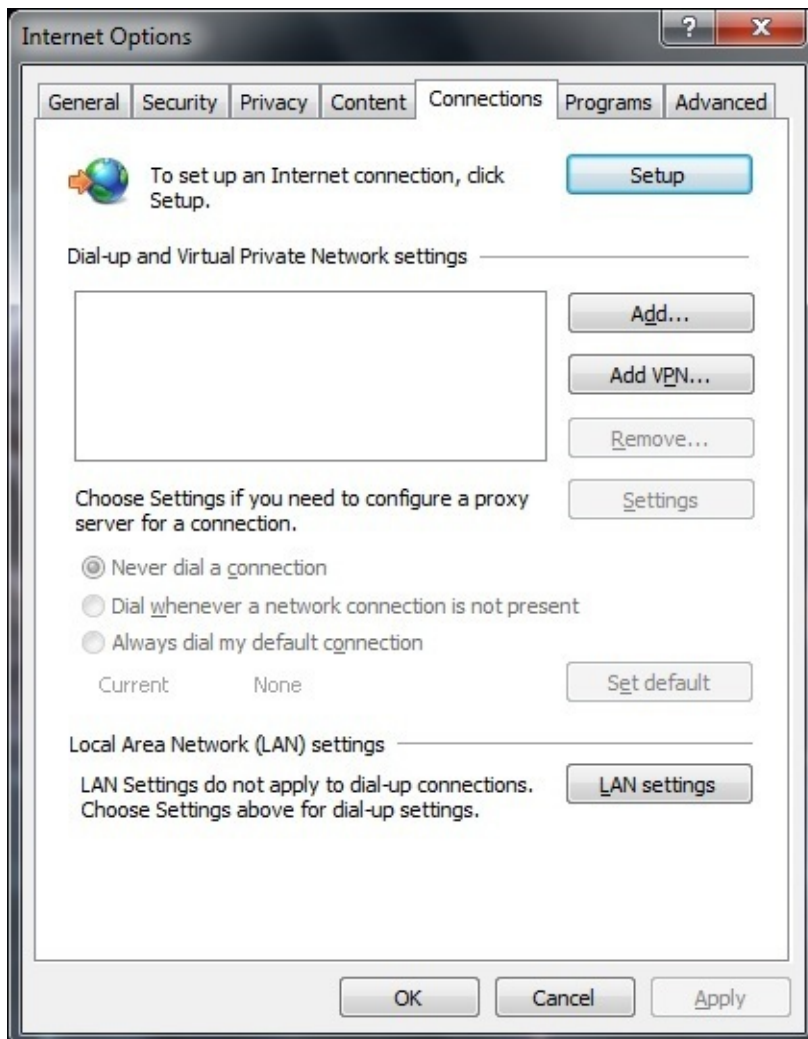
The time strangely differs almost for an hour (my clock is put forward for 56 minutes), as though a problem is in summer/winter time. The reason is some bug in Tor server. How to fix it:

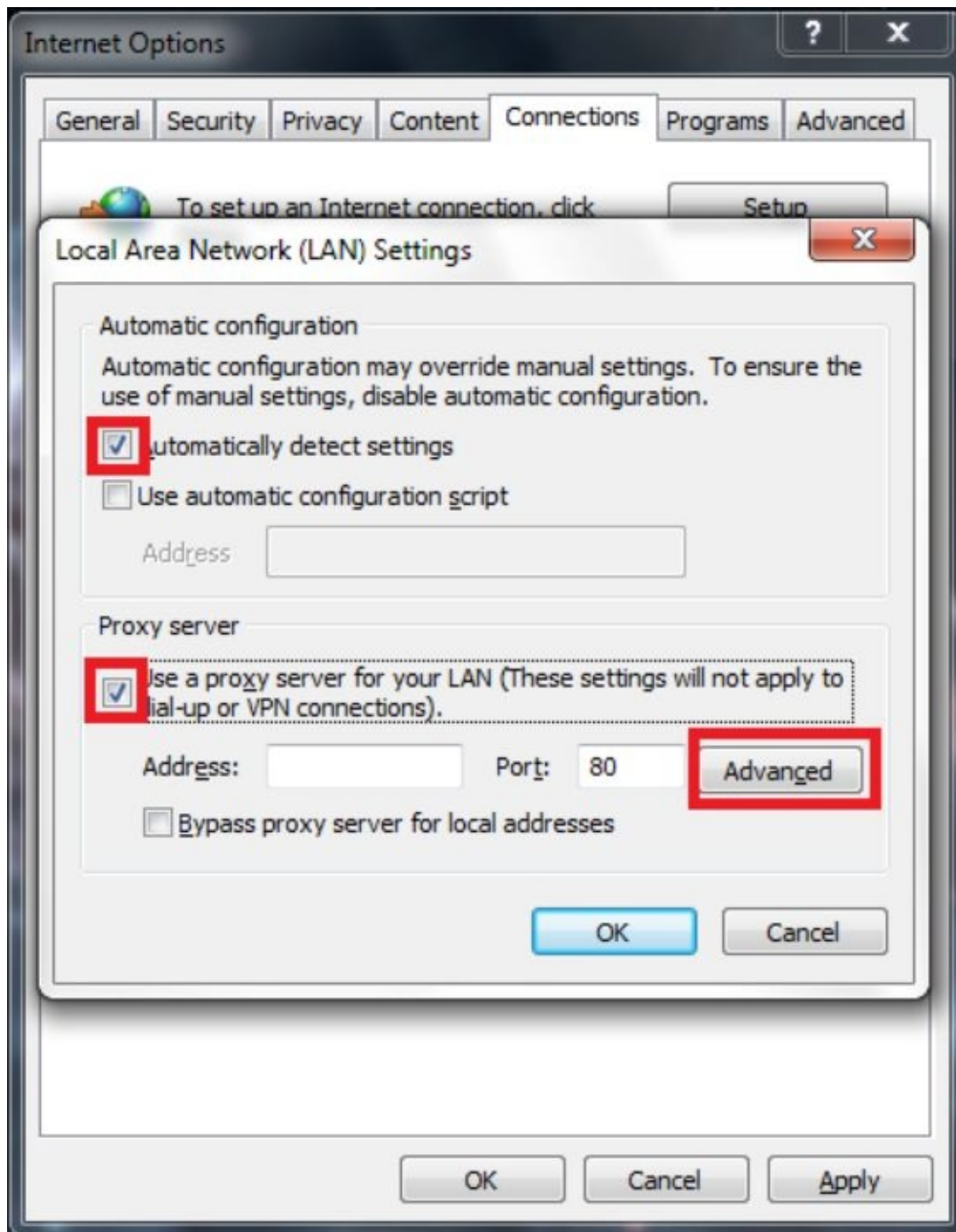
1. Run Tor system and wait for its complete loading (the moment when Tor sets the connection and its onion icon in the tray becomes green)
2. Open time and date settings and set the time an hour earlier or later. The actual connection will be lost but it will reset in some time.
3. Wait for about 15 minutes and then return the time back. The connection will be lost again but then Tor will be back in the normal mode.

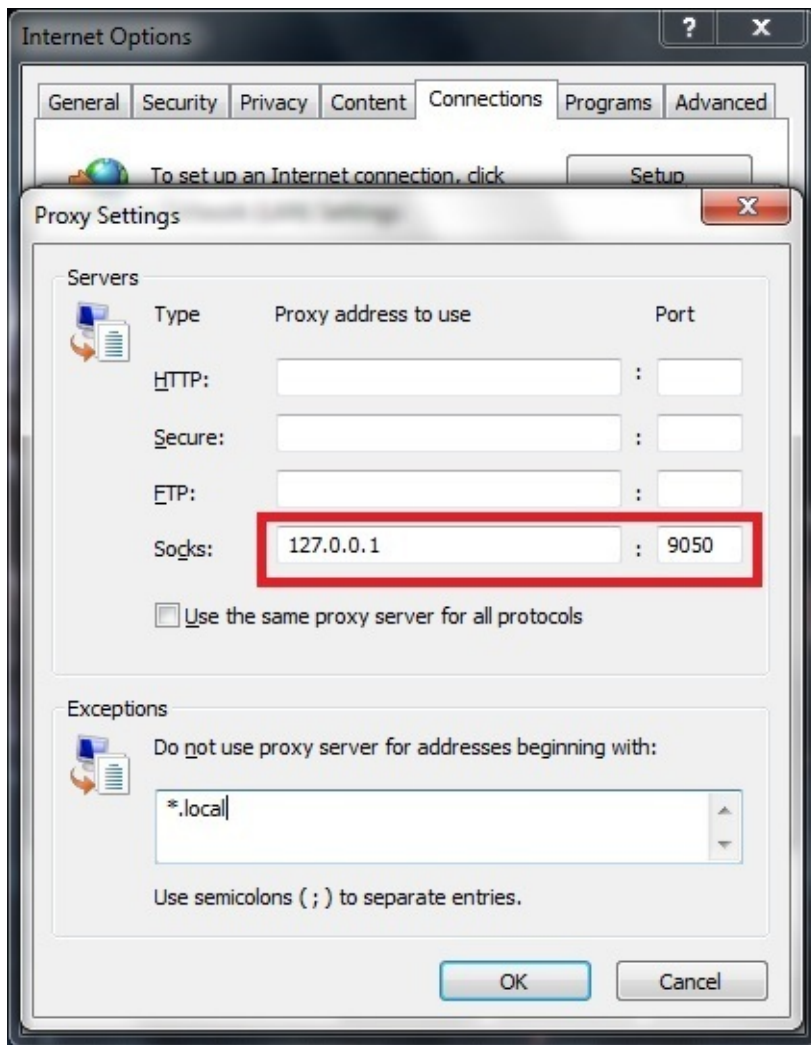
## 6. Tuning in the proxy mode

### How to configure proxies in Internet Explorer.

In OS of Windows 7 it is necessary to visit control Panel, then to pass to Properties of browser, further the Connecting inset, in a right lower corner to press on Tuning of network. You need to mark the field “Proxy-server”, then open “In addition”, and into an inset expose digital values shown on a picture.







Explorer works via Tor.

### **How to configure proxies in Google Chrome.**

Firstly it needs that it will be the “default browser” on Your PC. Further:

#### **Default browser**

The default browser is currently Google Chrome.

We press on to “Change configuration of proxy-server”. Insert for tuning Internet-explorer must go out (see the screenshot).

## How to configure proxies in Opera

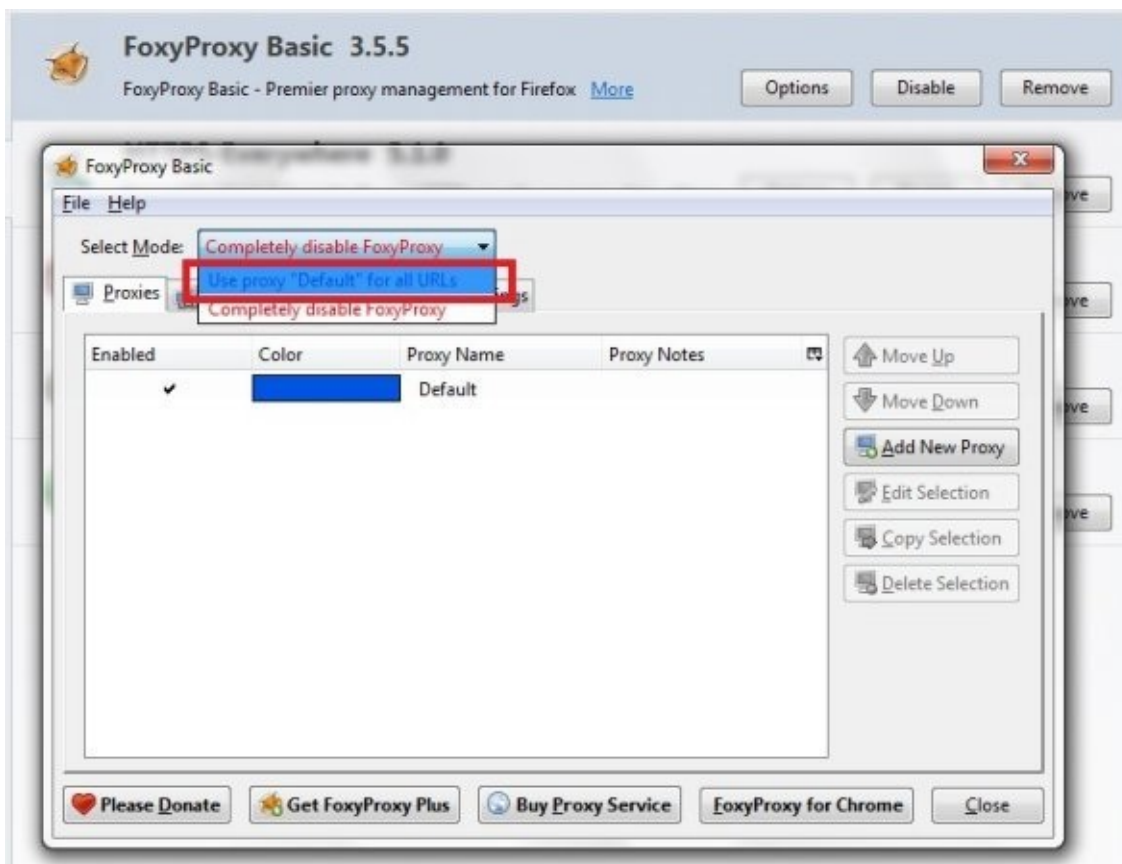
It is necessary to enter “settings” and propose them in accordance with the operating version of browser. We mark the part of Socks, further it is necessary to enter next numerical data: 127.0.0.1: 9050

## How to configure proxies in Mozilla Firefox.

The user needs this plugin (<https://addons.mozilla.org/en/firefox/addon/foxyproxy-basic/?src=search>). It should be set up in “Expansions”.



After setting of plugin you should choose chooses: “Tor proxies for all addresses”.



Further you should propose the settings.

FoxyProxy Basic - Proxy Settings

General Proxy Details

☐ Direct internet connection (no proxy)

☒ Manual Proxy Configuration

Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?

Host or IP Address: 127.0.0.1 Port: 9050

☒ SOCKS proxy ☐ SOCKS v4/4a ☒ SOCKS v5

Authentication

Username: Password: Password - again: Domain (optional - NTLM only):

☐ Use System Proxy Settings

☐ Automatic Proxy Configuration

☐ by WPAD ☒ by PAC

Automatic proxy configuration URL: http(s):// ftp:// file:// relative://

☐ Detect proxy settings automatically every 60 minutes

Notifications

☒ Notify me about proxy auto-configuration file loads

☒ Notify me about proxy auto-configuration file errors

OK Cancel

There must be not “forbidden web-sites” now.

If you want to know IP-address, appeal to <http://www.checkip.com> (ip-check.info)

When a user works by means of Tor, an address is different from that got for a provider.



**Congratulations. This browser is configured to use Tor.**

Your IP address appears to be: 94.242.228.108

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Atlas](#).

[Donate to Support Tor](#)

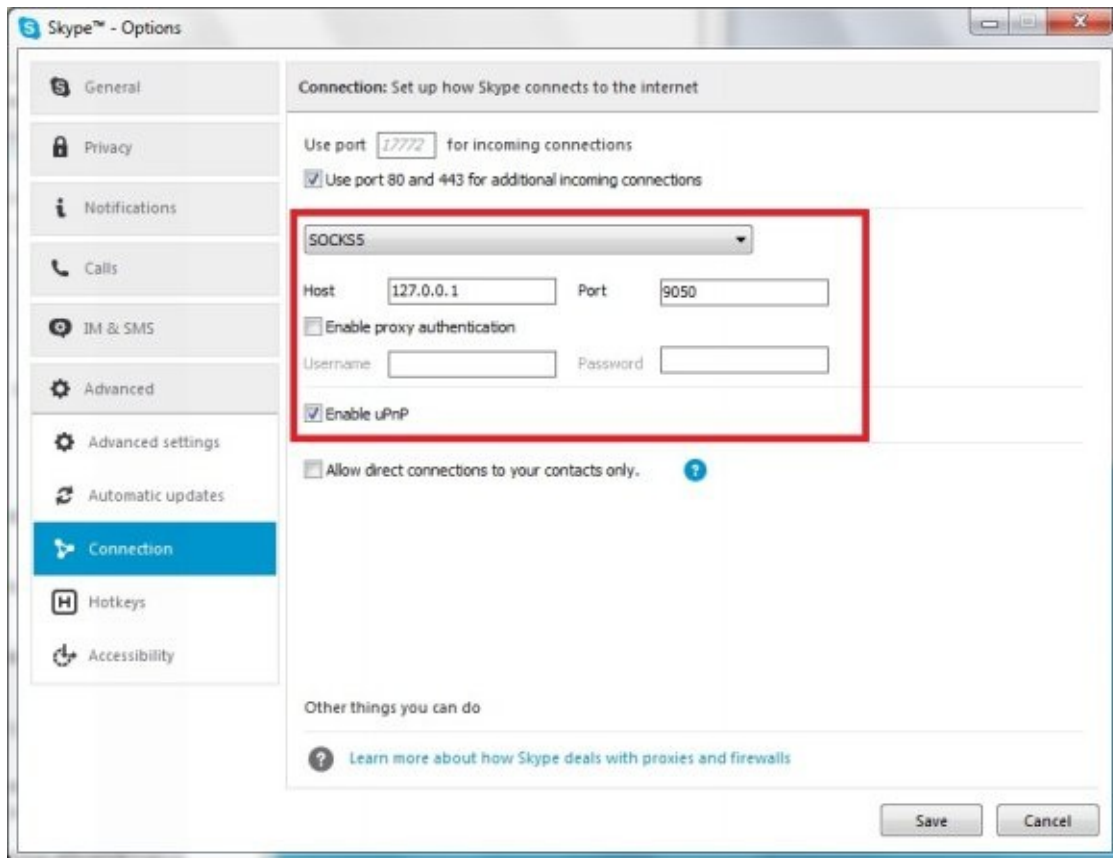
[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn More](#) - JavaScript is enabled.

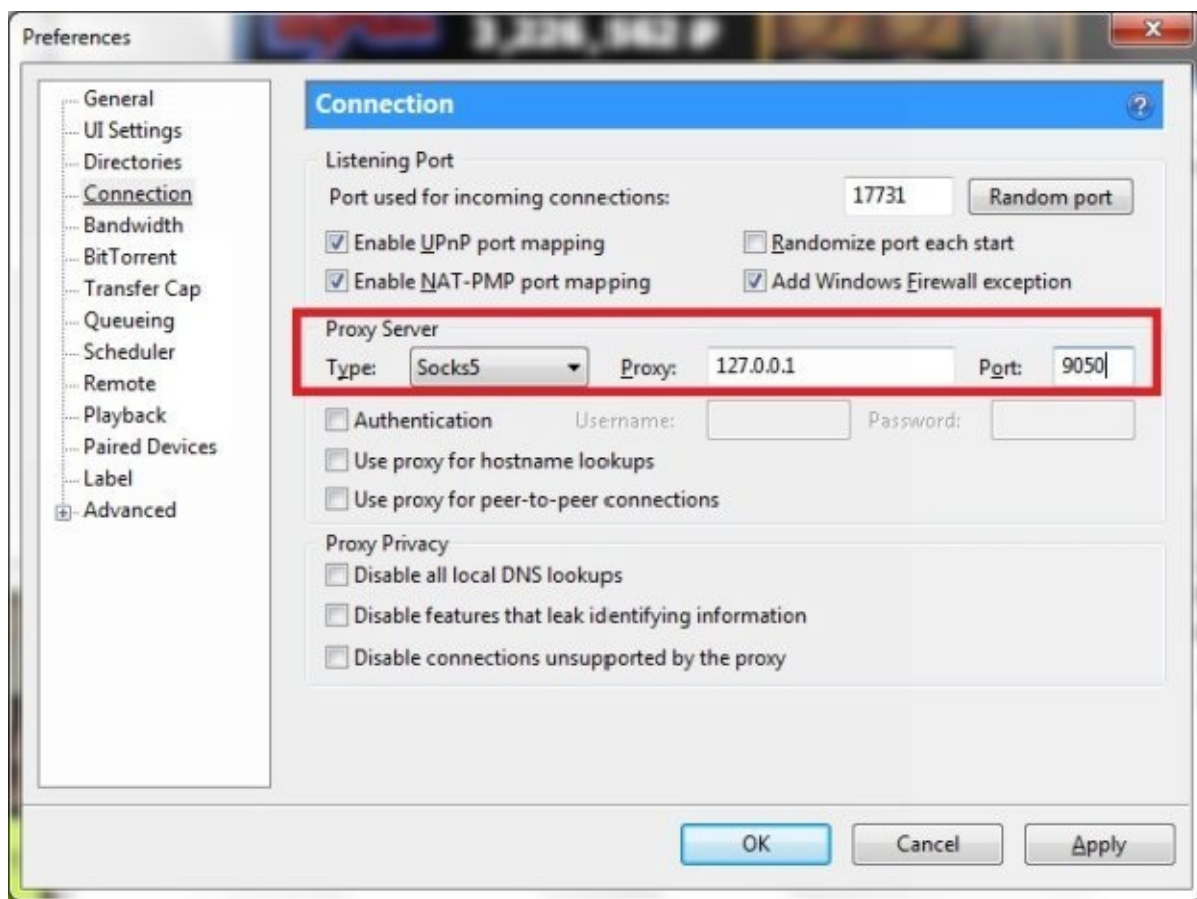


## How to “TORify” ICQ Skype, µTorrent.

The scheme is similar for ICQ and Skype: “Tools — Settings — In addition — Connections”, find the insert SOCKS5, and then write the following numerals 127.0.0.1:9050



For µTorrent you should move into “Settings-Settings of the program-Connections”. Further you should choose the settings as in the picture below.



## 7.Relay mode

Safety and efficiency of Tor network depend on the number of nodes, reliable for traffic sending. They are called relay nodes. The EFF even held Tor Challenge in order to stimulate as much users as possible for creating and configuring these nodes. As a matter of fact, article is devoted to this simple action. For work in relay mode you'll need a server, where Tor Relay will work. You can use your home PC or you can reconfigure a smart router. I offer another way – to use VPS (Virtual Private Server). Tor software is pretty modest and can easily work on VPS with minimal configuration. Memory of 256 MB or even 128 MB is enough. Disk requirements are low too: it is less than 1 GB. Price of such server per month is equal to a cup of coffee.

So, we register VPS. It should have a verified outer IP. As for me, I like your server, but there are a lot of VPS's wit Linux or \*BSD on board. As a rule, after purchasing you get a server with already installed Linux distribution. Choose anyone you like. I will show you using Debian as an example.

To start with, you should install Tor on your VPS:

```
# aptitude install tor
```

On default Tor will work in web client mode: you can use it to operate online but for anyone else it is useless. Someone else's traffic won't go through it. You must turn on Tor Relay mode.

Also you must turn on Directory Service &mdash; catalogue service, reliable for spreading information about other Tor servers. You can use undefined port for sending and for catalogue. Default configuration file offers to use port 9001 for packets retransmitting and broadcast and port 9030 for catalogue service. But we will make our server available for ports 443 and 80. These ports are usually used for www traffic.

Open /etc/tor/torrc and write in the following:

```
Nickname MyCoolNick
```

```
ContactInfo Person <somebody AT example dot com>
```

```
ORPort 443 NoListen
```

```
ORPort 9001 NoAdvertise
```

```
DirPort 80 NoListen
```

```
DirPort 9030 NoAdvertise
```

```
ExitPolicy reject *: * # no exits allowed
```

```
ExitPolicy reject6 *: * # no exits allowed
```

Under the 'Nickname' write in the name of the server. Later you'll use it for controlling server work via special services on TorProject.

In Contact Info line you can write in your contact info (in case if someone will want to contact with you). You also can leave it, then our server won't be able to let someone know, whom its owner is.

The last two lines forbid to use our server as Exit Nod of traffic. Otherwise, Tor will try to use our server for the transmission of outgoing traffic of network on external servers. Unfortunately, not everyone uses Tor with good intentions, and if traffic abandons Tor through your server, it can affect you.

In addition, the prescribed configuration compels a server to tell to other participants of network, that a server is accessible on ports 443 for sending packages and 80 for the report of information about other servers of network. Thus actually a server will wait reports on ports 9001 and 9030. In Debian

Tor by default works not from under route and such configuration allows avoiding problems with connecting to ports.

By means of iptables we will influence necessary connection between ports now.

If there are the special tools of tuning of network screen of iptables in the chosen distributive, it is possible to use it. It is simpler and more evident to do everything yourself.

We create the file of /etc/iptables.save.rules of such content:

```
# Generated by iptables-save v1.4.14 on Sat Jul 5 14:15:04 2014
```

```
*filter
```

```
:INPUT ACCEPT [0:0]
```

```
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [22:1968]
```

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A INPUT -i lo -j ACCEPT
```

```
-A INPUT -d 127.0.0.0/8 ! -i lo -j REJECT --reject-with icmp-port-unreachable
```

```
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
```

```
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

```
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

```
-A INPUT -p tcp -m tcp --dport 9001 -j ACCEPT
```

```
-A INPUT -p tcp -m tcp --dport 9030 -j ACCEPT
```

```
-A INPUT -j REJECT --reject-with icmp-port-unreachable
```

```
COMMIT
```

```
# Completed on Sat Jul 5 14:15:04 2014
```

```
# Generated by iptables-save v1.4.14 on Sat Jul 5 14:15:04 2014
```

```
*nat
```

```
:PREROUTING ACCEPT [0:0]
```

```
:INPUT ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [1:104]
```

```
:POSTROUTING ACCEPT [1:104]
```

```
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 9001
```

```
-A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 9030
```

```
COMMIT
```

```
# Completed on Sat Jul 5 14:15:04 2014
```

By this we optimize our tor server's work and access to ssh for remote administration.



It is left to prescribe loading of these rules. Usually I prescribe the start of iptables - restore in /etc/network/interfaces:

```
auto lo
```

```
iface lo inet loopback
```

```
pre-up /sbin/iptables-restore /etc/iptables.save.rules
```

On Your server the file of /etc/network/interfaces is being rewritten each time at re-starts, it is therefore possible to do hardly differently.

For example, to put loading rules of iptables in /etc/rc.local. For this purpose in EOF before exit 0 we put a line.

```
/sbin/iptables-restore /etc/iptables.save.rules
```

In conclusion we restart tor server:

```
# service tor restart
```

We check that we did everything all right. After a while after restart of file /var/log/tor/log lines must appear:

Self-testing indicates your ORPort is reachable from the outside. Excellent. Publishing server descriptor.

Tor has successfully opened a circuit. Looks like client functionality is working.

Self-testing indicates your DirPort is reachable from the outside. Excellent.

Performing bandwidth self-test...done.



In hour or two, when information will revive in a database, it is possible to call on [globe.torproject.org/](http://globe.torproject.org/) and, writing nickname of the server in the line of search, to make sure that the network of Tor was filled up by another point of redistribution of data.

Firstly through a new server traffic will not go. A course of life of Tor Relay is a theme of the separate article.

UPD: As in distributives the last version of Tor doesn't always lie, makes sense to connect special repositories.

So for Debian and Ubuntu it can be connected official repository of torproject.org. For this purpose in /etc/apt/sources.list.d/ we create the file of torproject.list of next contain:

```
deb http://deb.torproject.org/torproject.org DISTRIBUTION main
```

Where instead of DISTRIBUTION we write the version of your distribution (for example jessie or saucy) Do it

```
# gpg --keyserver keys.gnupg.net --recv 886DDD89
```

```
# gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-key add -
```

```
# apt-get update
```

```
# apt-get install tor
```

- tor
- ,vps
- ,tor relay

## 8. Adjustment and work with the Vidalia Polipo shell

There are Internet providers who forbid the use of Tor. Repeaters are required to help locked users with Tor to get an access. Since bridges are not registered in the public directories as common repeaters then provider cannot close an access to all bridges. Open addresses of bridges can be found here <https://bridges.torproject.org>. Or one can write a letter to [bridges@torproject.org](mailto:bridges@torproject.org). Indicate subject “get bridges”. Inquiry should be made only out of an account Gmail.

You should understand that the very fact of Tor installation does not anonymize computer network connections. Additional software components and adjustments are necessary. Software program Tor only controls cyphering and determines the path of software suit pass through the repeater network.

1. First of all we need virtual proxy server installed on a user's computer. Sometimes it is called “filtering proxy”. Such proxy is an intermediate between user applications for work in the Internet and Tor network.

There are two basic versions of filtering proxy server - Privoxy and Polipo.

Several years ago development engineers of Tor system recommended using Privoxy. Now they include in all assemblies only Polipo put online at [torproject.org](http://torproject.org). (?)

It is quite difficult to compare them according to their characteristics. Polipo is considered tiny – size less than 200K. All its adjustments are contained in the file `polipo.conf`. I could not find detailed literature regarding its settings. Perhaps it is not necessary.

For work with the Tor system one should use polipo proxy version not less than 1.0.4, because earlier versions do not support the work with protocol SOCKS, and as a result are not suitable for the Tor system.

Privoxy — is a free web-proxy with enhanced capabilities of filtering Internet content for the purposes of Internet users' privacy protection. The last version is 3.0.17. (2011). However Privoxy is used frequently as an intermediate between applications and software program Tor. It should be remembered that Privoxy could be a totally independent software program protecting interests of its users on the level of protocol HTTP.

Which proxy out of two one will use on his/her computer is a matter of a self-dependent decision. It is flatly not recommended to use them simultaneously since both proxy servers use the port 8118, and during combined operation problems can occur.

The simplest advice: for those who do not want to go through the hassle, it is better to use Polipo which is a part of all the last assemblies on the website [torproject.org](http://torproject.org). Those who wish to have more additional features for adjustments should download and set up Privoxy, and then during installation of assembly exclude Polipo from installation.

2. For Tor system loading and work management the software program Vidalia is used. It is frequently called graphical shell for Tor.

In the settings of Vidalia there are means to launch Tor and filtering proxy during launch of Vidalia, launch and stop Tor during operation, look through Tor network map and others. Work with the Vidalia will be discussed further more elaborately. Tor parameter settings with the help of the Vidalia shell.

When launching the software program Vidalia a sign Vidalia should appear in the form of onion. In the operating system Windows it appears in the system tray (near the watch, see the picture). In the operating system Ubuntu it appears on the taskbar. You can launch the window Vidalia by clicking a left mouse button on its sign.



On the first picture Tor is switched off, on the second – switched on.

Now when you have Tor filtering proxy server and Vidalia you can adjust applications for work with Tor or as they say “to tariff applications”.

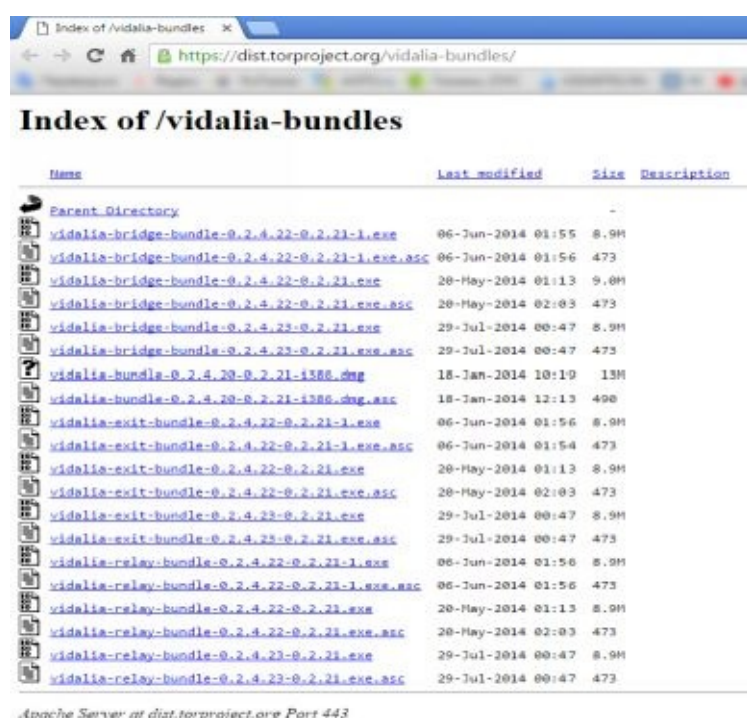
## Installation of Tor on Windows operating system – Vidalia Bundle pack

Unlike Tor Browser all the other assemblies (packs) carry out the installation of Tor and of additional components.

Components work quite the same way as in the Tor Browser, but there are some of the finer points. For instance if the browser Mozilla Firefox has not been set up then the TorButton will not be set up also. That is why it is recommended to set up Firefox before the installation of the Vidalia Bundle.

The following pictures illustrate the Vidalia Bundle installation process on Windows 7 >:

Choose the load file and save it

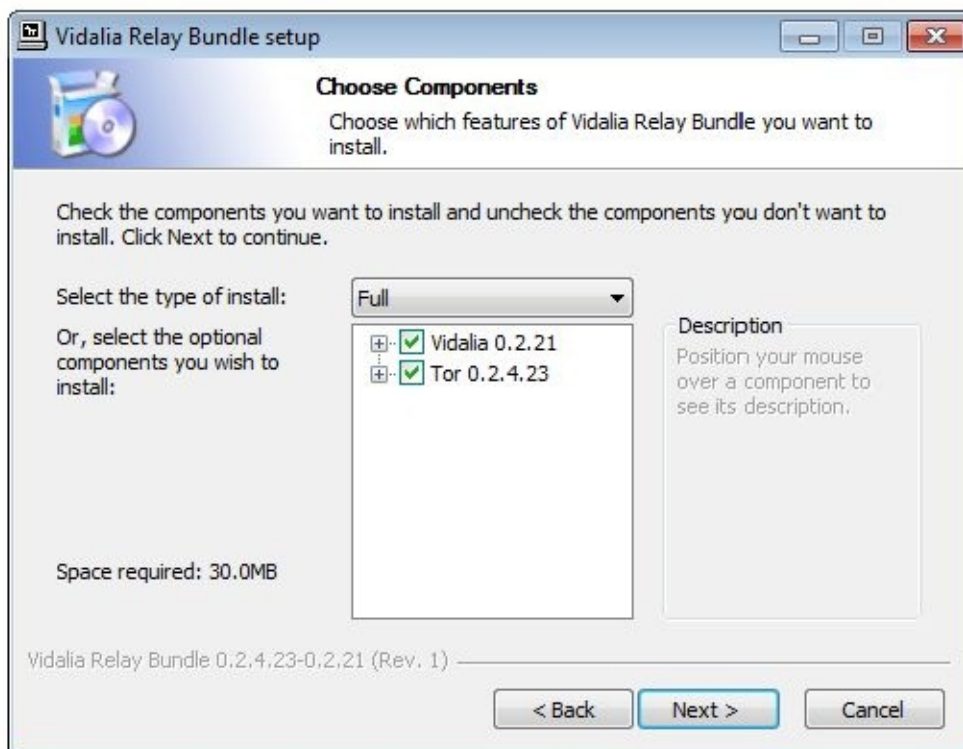


Launch the setup file



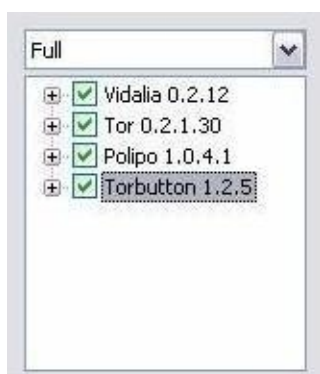
Necessary options are already marked with ticks “by default”

If a user wishes to use other configuration, for example to use filtering proxy server Privoxy or other browser for anonymous operation, ticks have to be removed from unnecessary components. At the same time the Privoxy and browser should be set up beforehand.





In the earlier versions there can be another alternative:



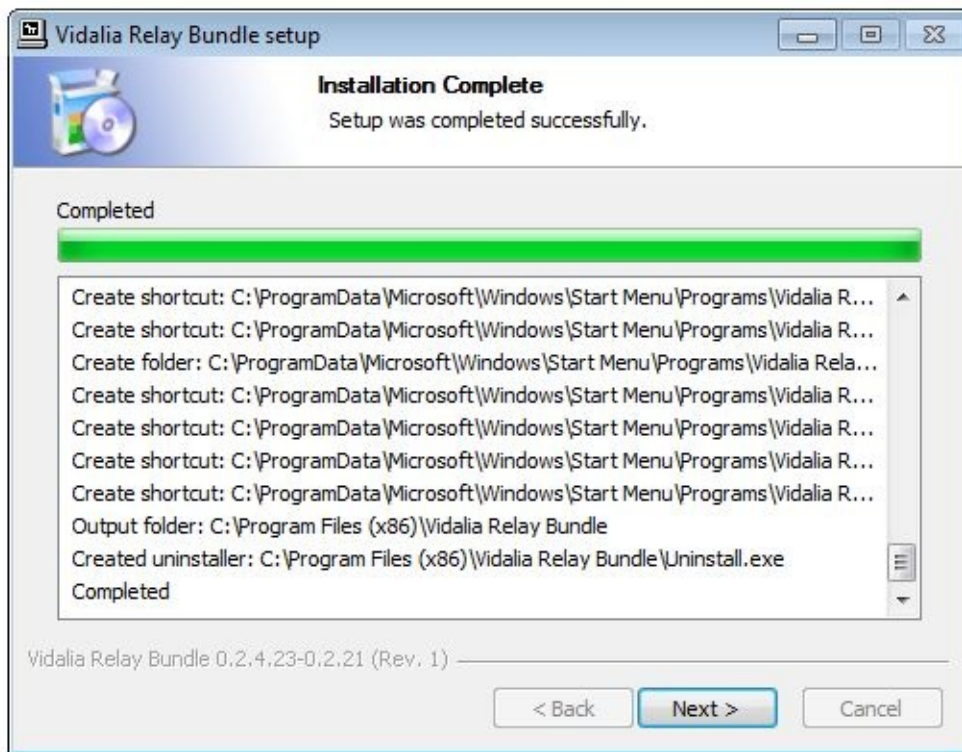
Assembling of the Vidalia Bundle for Windows contains Tor, Vidalia, Polipo, and in the earlier versions – the Torbutton (the number of versions can be seen on the pictures).

If the Firefox is not set up on a computer then the software installation program warns about that, advices to set up it and repeat installation.

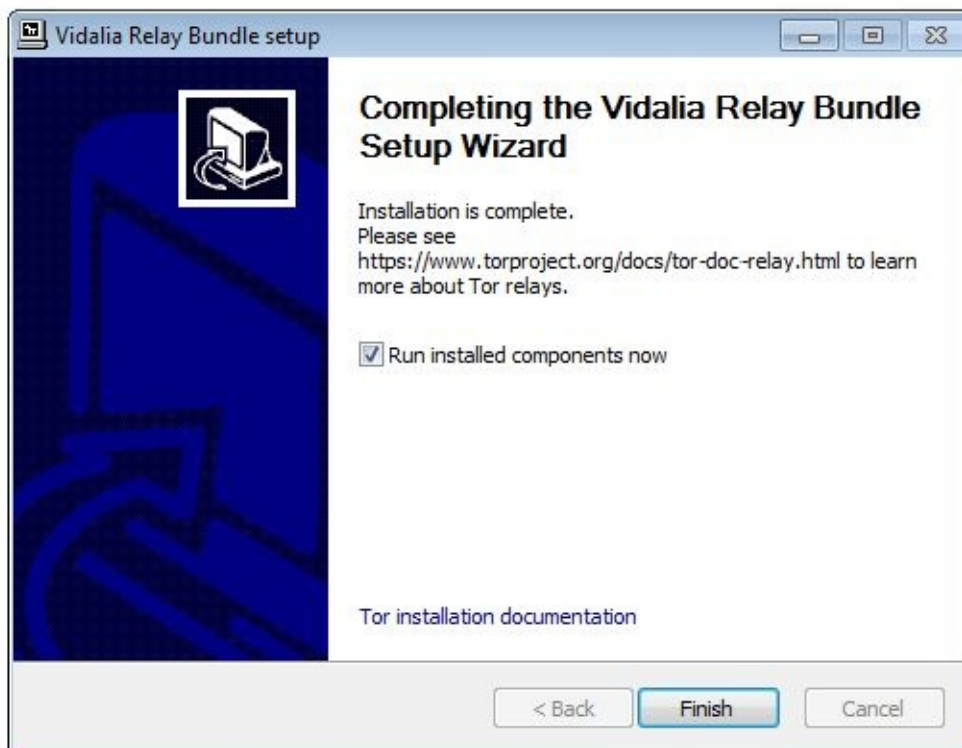
All the standard configuration components are set up by default adjusted for joint operation.

Further, choose the load directory or leave the suggested:





View of setup windows



The software program Tor is set up as a client-side program by default. It uses a built-in configuration file, and the majority of users do not need to change any settings.

## Tor parameter settings with the help of the Vidalia shell

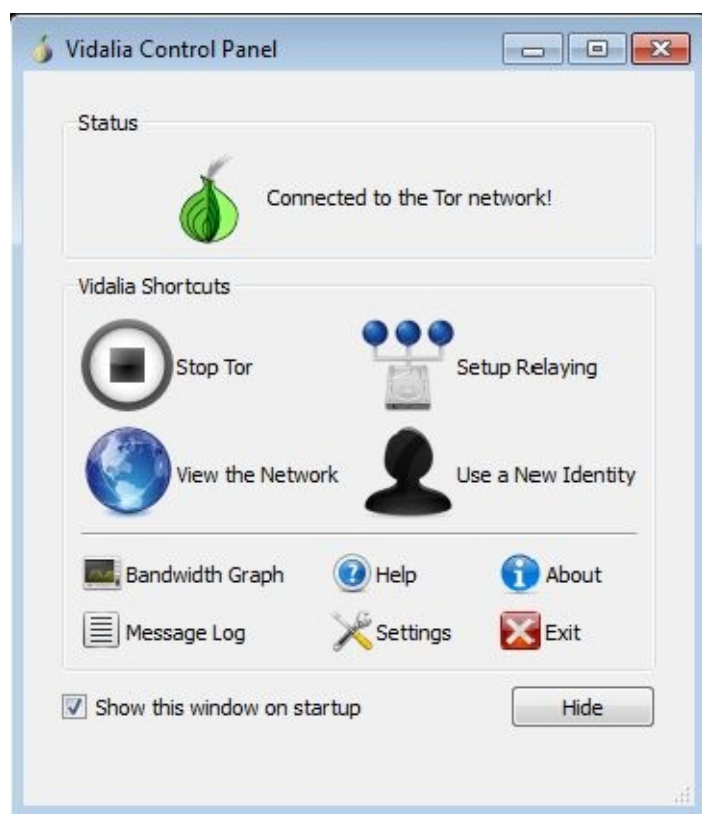
The software program Vidalia works as a graphical shell for the Tor system. It works practically on all platforms including Windows, Mac OS, Linux and others Unix systems.

If the Tor Browser assembly is used, then the Vidalia is launched with file Start Tor Browser.exe from the catalogue <TorBrowser>

If the pack Vidalia Bundle is used – you launch the file vidalia.exe from the catalogue: <installation catalogue Vidalia-bundle\Vidalia>

When launching a sign Vidalia should appear in the form of an onion. In the Ubuntu operating system it appears on the taskbar. In the Windows operating system it appears in the system tray (near the watch).

In order to launch “Vidalia Control Panel” you can click a left mouse button on its sign.



Vidalia settings are clear and comprehensible. Though we briefly enumerate them:



- Tor Launch/Stop (Start/Stop Tor)

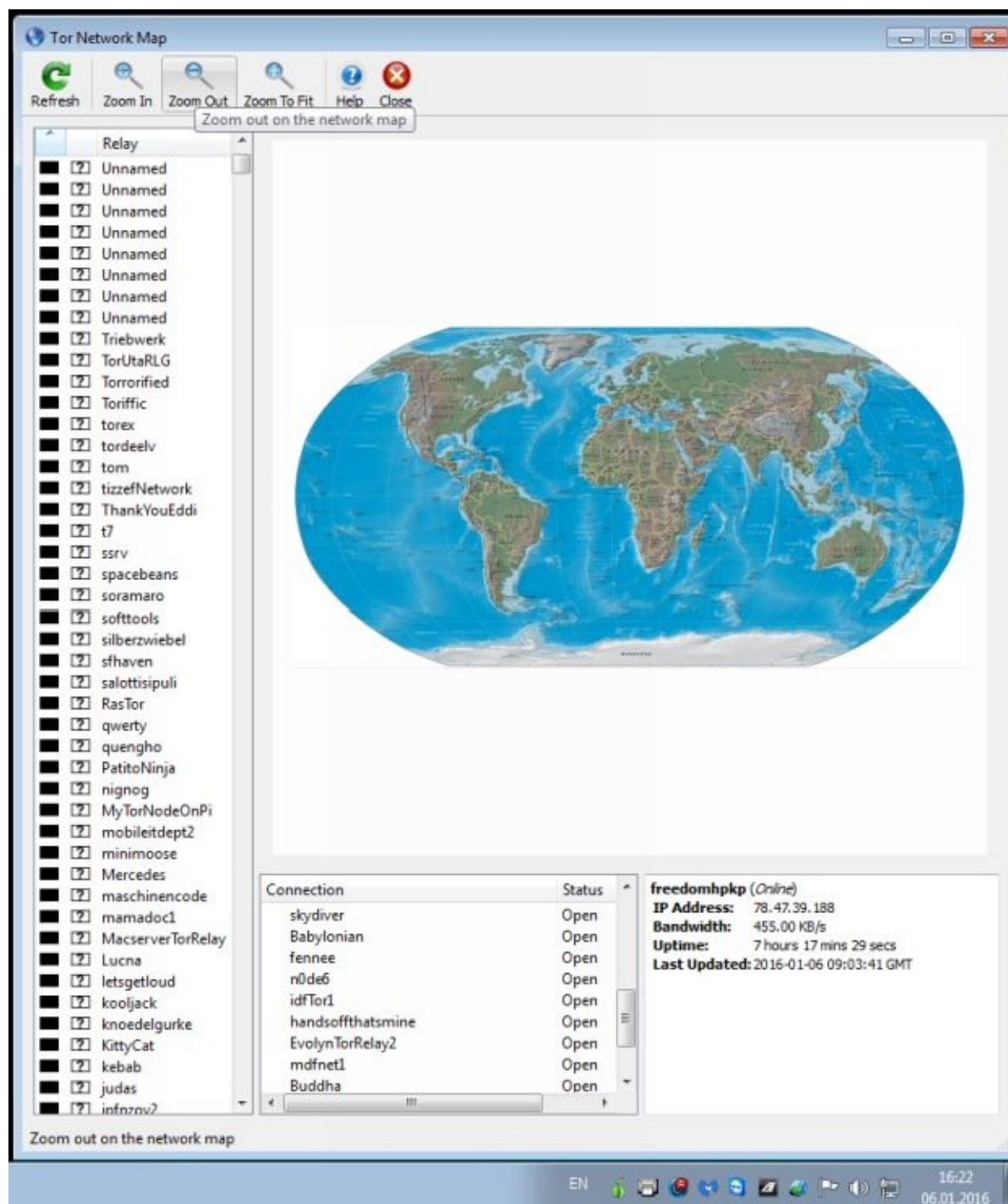


- Server settings (Sharing) establish an operating mode (client, server or bridge)



- Network overview (Network Map)

Showing Tor network map:



During Tor normal operation, circuits in use should be listed in the lower central window. At the same time in the neighboring window to the right the servers of a chosen circuit and their characteristics should be listed. In the upper window their geographical location is presented.

With the help of the network map you can choose servers according to their belonging or



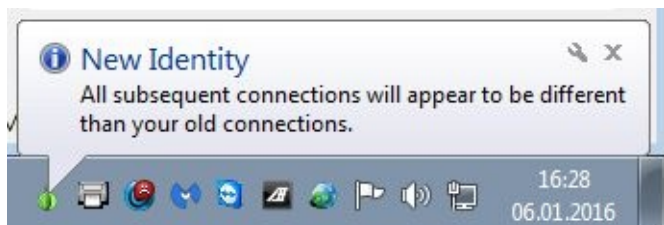


speed.



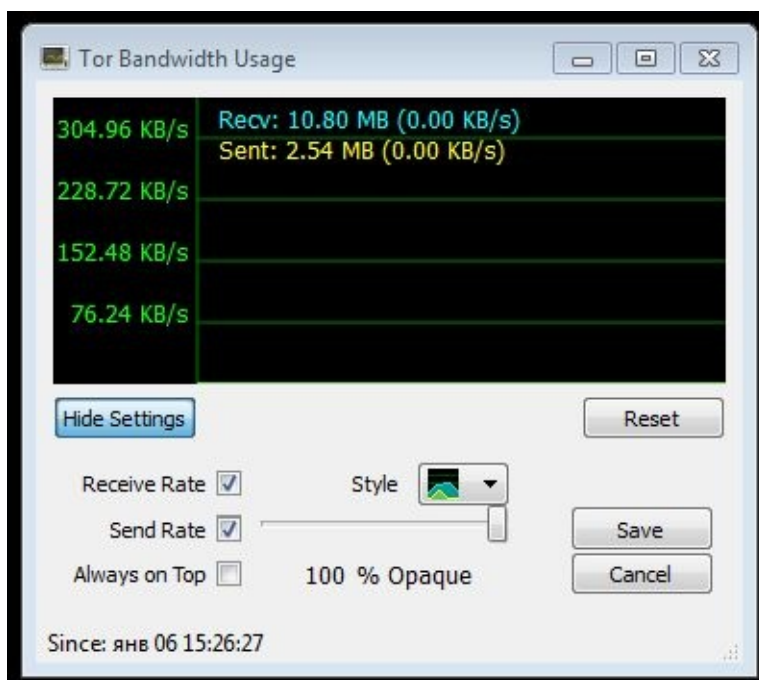
- Change the identity (New Identity). It changes Tor circuit and as a result – output IP-address.

After the successful change in tray a message will appear



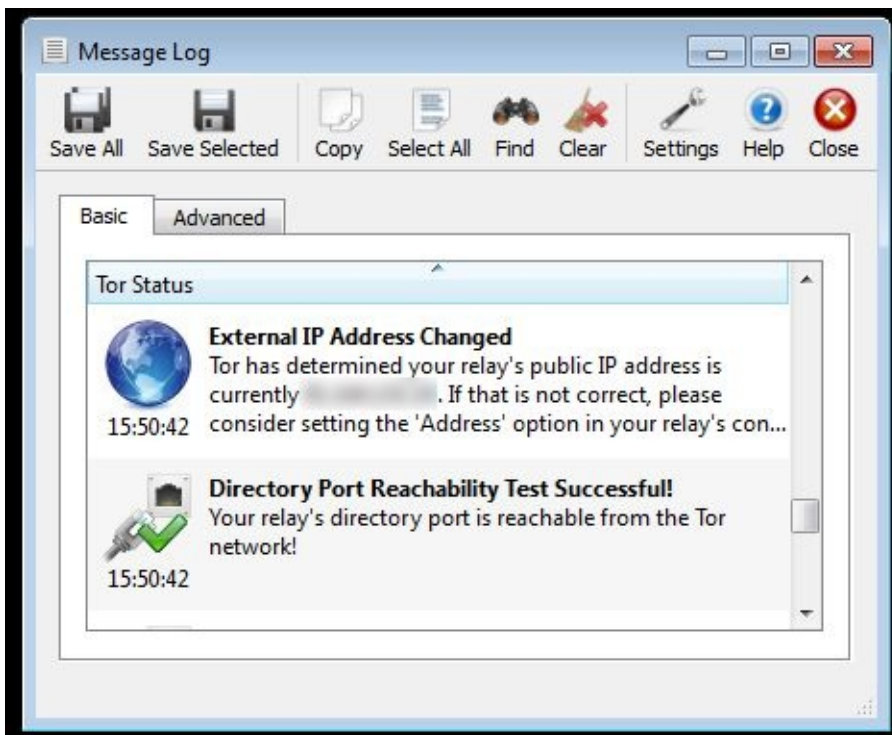
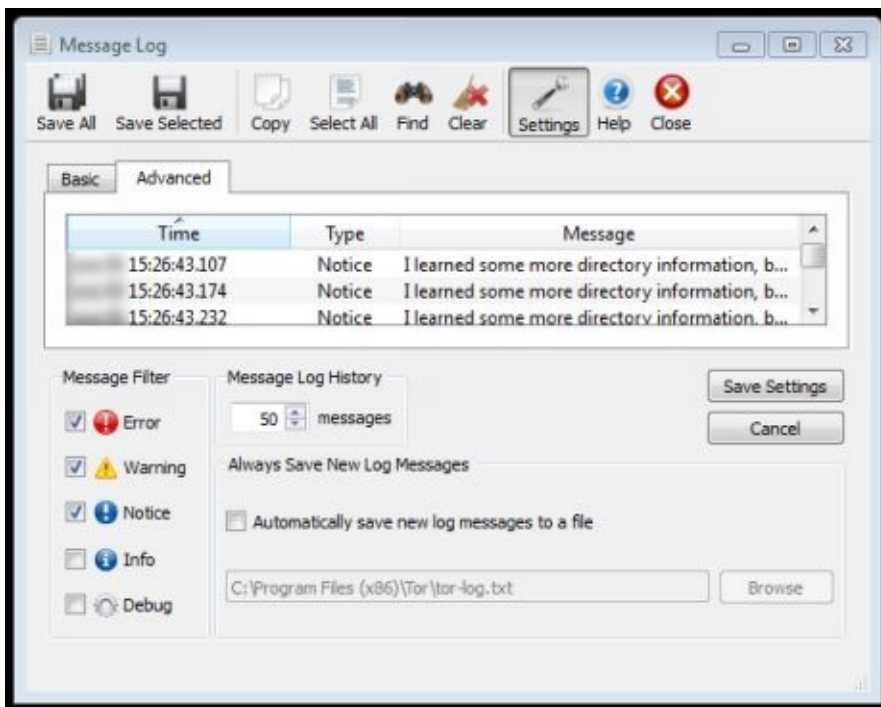
- Traffic schedule

Shows input and output traffic and Tor data rate:



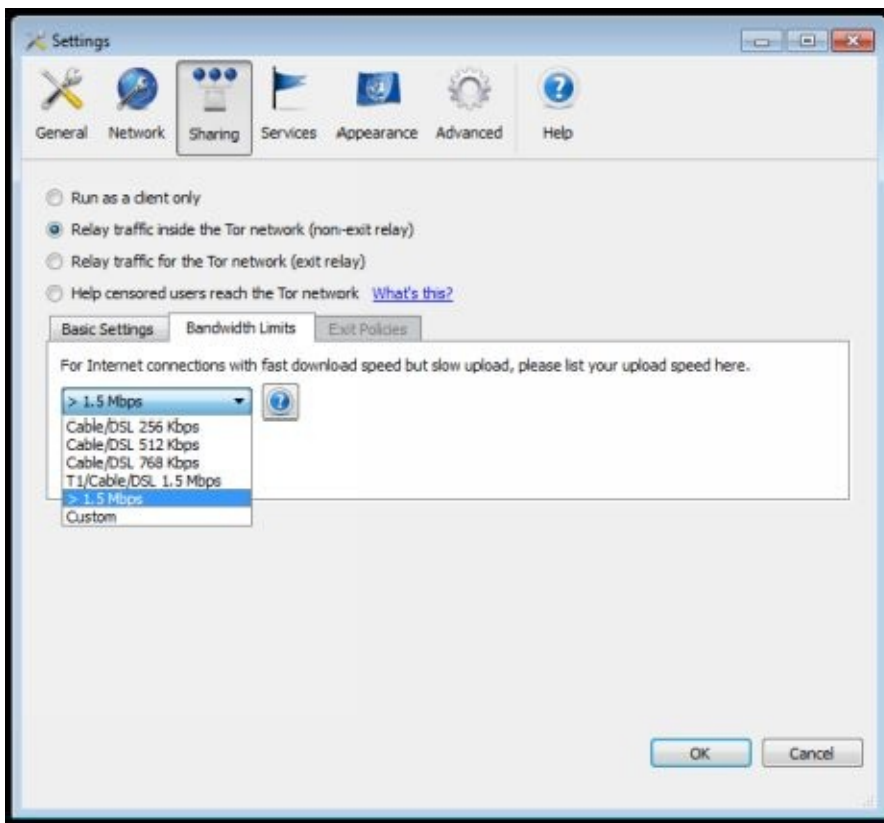


- Message Log. It allows viewing Tor operation logs:

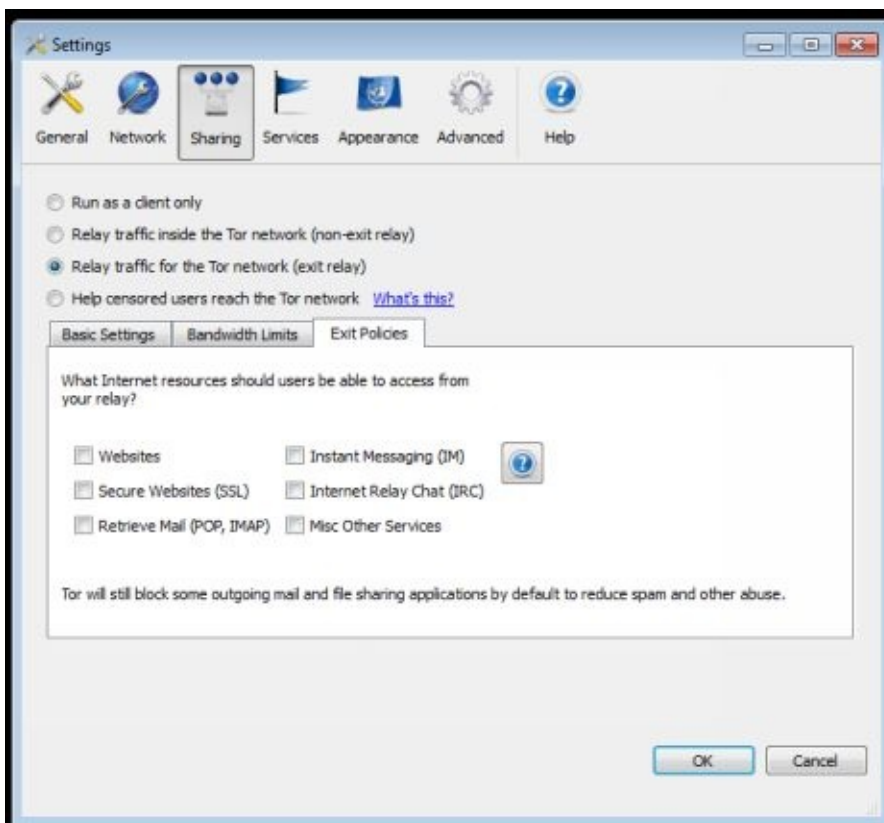




- Settings. It opens the window “Settings”:

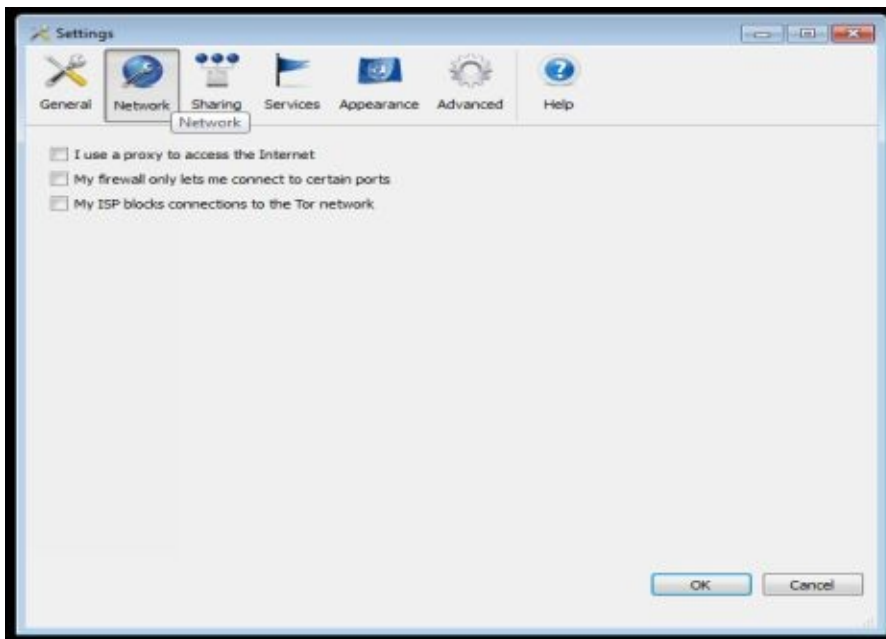


- Flap “General” allows setting up Tor components launch procedures

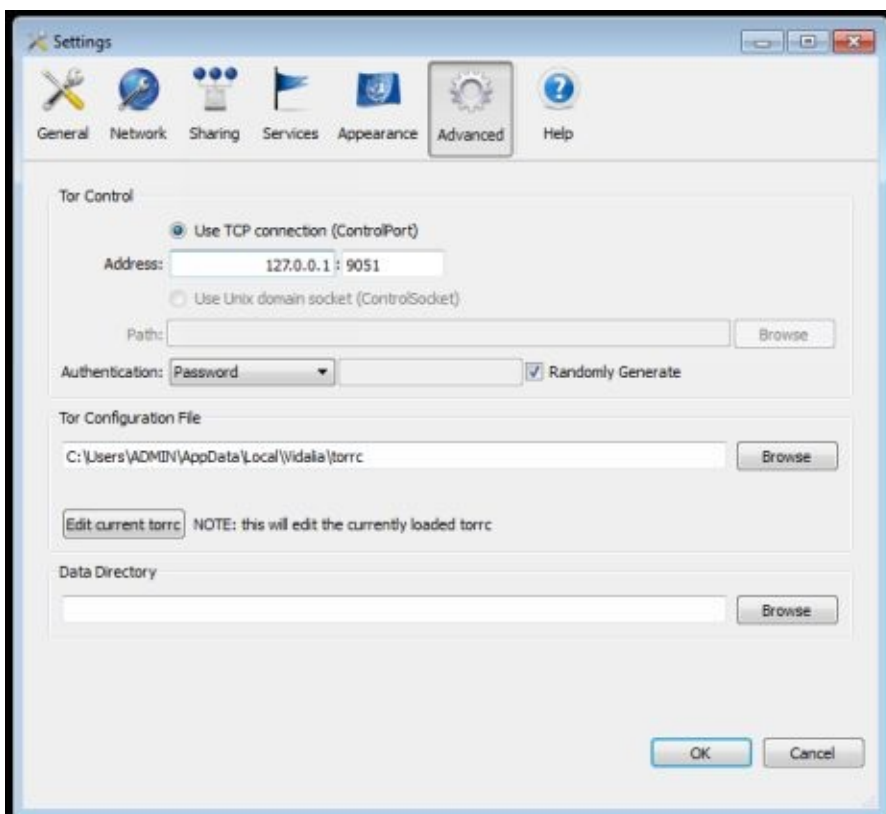




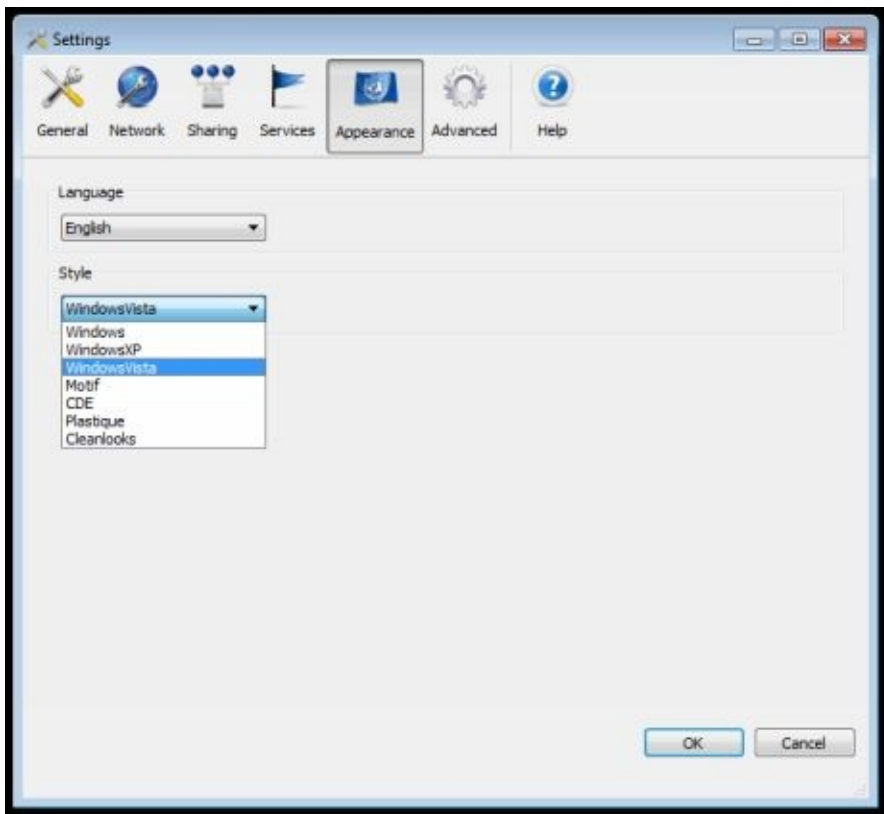
- Flap “Network” allows writing out-proxy server (“I use proxy for an access to the Internet”) or/and bridge (“My provider blocks up an access to the Tor network”) (read in the Internet – Tor blocking and how to cope with it.



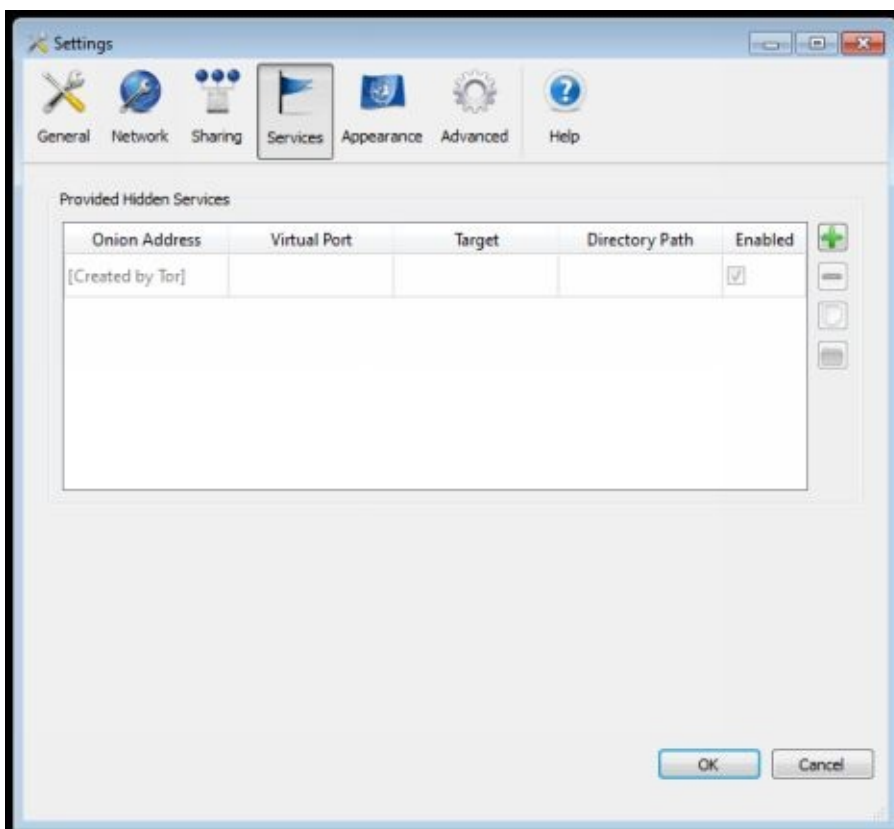
- Flap “Advanced” allows setting up (checking) parameters of TCP connection (127.0.0.1 port 9051) as well as determining (controlling) location of a torrc settings file and data catalog. Moreover, from here you can edit torrc configuration file.



-Flap “Appearance” allows changing view settings according to Your system



- Flap “Services” allows adding addresses and ports of computers in the Vidalia network.



- Flap “Help” calls the Vidalia Help Desk.

As you can see from the aforesaid with the help of the Vidalia shell you can set up and control quite a lot of Tor system parameters.

## **Tor delicate adjustment**

As a rule standard settings, which are fulfilled in the Vidalia shell, are quite enough for full value anonymous operation in the Internet. However in some cases you may require additional changes of Tor parameters.

Such changes are carried out by editing Tor configuration file and are called delicate adjustment.

Filtering proxy Polipo configuration file

Here the simplest variant of polipo.conf configuration file is listed (only not commented-out instructions).

```
### Basic configuration
proxyaddress = “127.0.0.1”
proxyport = 8118
allowedclients = 127.0.0.1
allowedports = 1-65535
proxyName = “localhost”
cacheIsShared = false
socksParentProxy = “localhost:9050”
socksProxyType = socks5
chunkHighMark = 33554432
diskCacheRoot = ””
disableLocalInterface = true
disableConfiguration = true
dnsUseGethostbyname = yes
disableVia = true
censoredHeaders = from,accept-language,x-pad,link
censorReferer = maybe
maxConnectionAge = 5m
maxConnectionRequests = 120
serverMaxSlots = 8
```

*serverSlots* = 2

*tunnelAllowedPorts* = 1-65535

Configuration file – is a common text file. It bears the name of torrc (with no extension) and is located in:

- when using Tor Browser assembly – in catalog..*<Catalog Tor Browser>\Data\Tor*
- in installation packs - *<Documents and Settings\<user>\Application Data\Vidalia*
- in Ubuntu Linux operating system – in catalog */etc/tor*

Software program Tor during loading (reloading) first of all reads configuration file and sets up operational characteristics in accordance with values of instructions in **torrc** file.

Torrc file editing can be carried out in an elementary text editor: Notepad, AkePad etc. It is desirable that before editing you save original torrc file in the same folder. For example you add to a name the extension \*.bak, \*.001 etc.

**For changes to take effect you need to reload all Tor system software!**

### **1. Fixation of output or input Tor network node**

Intercourse with Tor users shows such a nuance – by far not everyone likes constant change of their IP address.

It will be recalled that output servers in Tor constantly change in a random manner. For a user it means that his/her IP is unstable. In respect to attended resource a user at any moment can turn from an American or a Frenchman into let's say Japanese, Hindu or any other person.

Such method of approach essentially increases the level of anonymity but in certain cases is unacceptable (for instance during work with websites fixing user's session).

In Tor there is a possibility to directly indicate which server should be output. In such case IP will be constant. Tor creators do not recommend acting this way because it reduces anonymity. Here a user must decide for him/her what is more essential but I will tell you how to get rid of a constant IP change.

You will have to edit Tor configuration file, it is called “torrc” and you can get to it either through “Start” -> “Programs” -> “Vidalia Bundle” -> “Tor”, -> “torrc”, or find in the folder \Documents and Settings\user\Application Data\Vidalia orrc. Torrc – common text file, it is opened by the notepad.

For that in **torrc** write two lines:

**ExitNodes** <node name>

**StrictExitNodes** 1

Where:

Variable *ExitNodes* – indicates to use a certain server as output node

*StrictExitNodes* 1– is an indication that in case of unavailability of a chosen server you do not attempt to be linked to other server but take out a mistake.

It is allowed to write **several nodes** separated by commas or, for example, by indicating **ExitNodes {de}** – then we will get only German servers as output servers (“turn into” a German!).

You can find necessary server at: <http://torstatus.kgprog.com/> or <https://torstat.xenobite.eu/>

These are the lists of Tor network servers, you can select the required according to country, speed, traffic. Special attention must be drawn to an ability of a server to work as output.

It is clear that servers, which are not output servers, will not work in this capacity.

Choose a server and write its name (Router Name, Nickname), for instance:

ExitNodes 1000rpmLinux

StrictExitNodes 1

Safe changes in configuration file and that’s all, now IP is static. It is allowed as well to write several nicknames separated by commas (nickname1, nickname2, nickname3), in this case output servers will dynamically change but be chosen from permitted.

It is clear that network efficiency in this case depends on availability of an output server, and in case Tor stops connecting with websites, in the first place you should check if an output server have gone whack.

Similarly input node is fixed:

**EntryNodes** <node name>

**StrictEntryNodes** 1

There is another helpful setting of that kind –**TrackHostExits** fixes output node (host) for given domains what enables to save a session for those servers which check IP clients. Syntax of record is the following:

**TrackHostExits** host,.domain,...

## 2. Exclusion of suspicious nodes

To exclude doubtful nodes (for example – Russian, Ukrainian, Turkish) you have to add to **torrc** the line: **ExcludeNodes** {ru}, {ua}, {tr}

Or you can indicate a certain list of names.

Now if inquisitive guys with grey eyes in those countries hit upon an idea to make a false Tor-server and attempt to tap output data then we cannot access such server in any way.

There is a helpful feature of **torrc file**. This is commentary. Tor does not carry out a line in **torrc file** if a line begins with the sign “#”. Due to commentaries you can safe **storages** in **torrc file** and if necessary quickly switch them on by removing “#”.

## 3. Writing a proxy-server in Tor

Add the following lines at the end of Tor configuration file changing <proxy address> and <port number> (as well as <login> and <password>, if they are) into particular values of linked http or https proxy-server.

*# Force Tor to make all HTTP directory requests through this host:port (or*

*# host:80 if port is not set).*

**HttpProxy** <proxy address>:<port number>

*# A username:password pair to be used with HTTPProxy.*

**HttpProxyAuthenticator** <login>:<password>

*# Force Tor to make all TLS (SSL) connections through this host:port (or*

*# host:80 if port is not set).*

**HttpsProxy** <proxy address>:<port number>

*# A username:password pair to be used with HTTPSProxy.*

**HttpsProxyAuthenticator** <login>:<password>

After correcting and saving **torrc file** you need to restart Tor.

To check settings you can use Vidalia graphical shell or Tor-analyzer (go to <http://check.torproject.org>).

The list of several Tor instructions (settings)

**EntryNodes nickname,nickname,...**

It is a list of servers preferable for use as “input” to determine TCP/IP-connections with Tor routers nodal circuit, if it is possible.

**ExitNodes nickname,nickname,...**

It is a list of servers, which preferably take the role of closing link in Tor routers nodal circuit, if it is possible.

**ExcludeNodes nickname,nickname,...**

It is a list of nodes, which should not be used when making up nodal circuit at all.

**StrictExitNodes 0|1**If it is set up in 1, Tor will not use any kind of nodes except those which are in the list of output nodes as mediators setting up connection with target host and which are a peculiar closing link in nodes circuit.

**StrictEntryNodes 0|1**

If the value 1 is assigned to this parameter then Tor will not use any kind of nodes except those, which are present in the list of input nodes for Tor network connection.

**FascistFirewall 0|1**

If the value 1 is assigned to this parameter then Tor when setting up a connection will exclusively refer to Onion Routers which have strictly definite port numbers (with which your firewall enables to establish connection) open to carry out connection (by default: 80-th (http), 443-rd (https), see FirewallPorts). This will allow Tor, launched on your system, to work as client for firewall having strict limiting policy. Opposite statement is wrong because in this case Tor cannot fulfill the duties of a server closed by such firewall.

**FirewallPorts PORTS**

The list of ports to which your firewall allows connecting. It is used only under adjusted parameter value FascistFirewall. (by default: 80, 443) (Default: 80, 443)



## **LongLivedPorts PORTS**

The list of ports for services, which tend to establish unusually long connections (among these are mainly chats as well as interactive shells). Nodal circuits out of Tor routers, which use these ports, will contain only nodes with most high uptime (typical time of presence in network) with the purpose of decreasing the probability of nodal server disconnection from Tor network before closing of flow (by default: 21, 22, 706, 1863, 5050, 5190, 5222, 5223, 6667, 8300, 8888).

## **MapAddress address:new\_address**

When a request for indicated address comes to Tor, onion router changes address before taking up request processing. For example, if you want Tor nodes circuit to be used during connection to [www.indymedia.org](http://www.indymedia.org) with output through torserver (where torserver – is a pseudonym of server), use “MapAddress [www.indymedia.org](http://www.indymedia.org) [www.indymedia.org.torserver.exit](http://www.indymedia.org.torserver.exit)”.

## **NewCircuitPeriod NUMBER**

Every NUMBER of seconds to analyze the connection status and take a decision if a new nodal circuit formation needs to be initiated (by default: 30 seconds).

## **MaxCircuitDirtiness NUMBER**

To permit a repeated use of circuit, for the first time collected in a certain composition of its links – the biggest – NUMBER of seconds ago, but never join a new flow to a circuit which served this session during quite a long time (by default: 10 minutes).

## **NodeFamily pseudonym,pseudonym,...**

Denominated Tor servers (in a predictable manner, to increase a degree of transparency of Tor network hierarchy) unite in a “family” on the basis of general or joint administration, so you should avoid using any 2 of these nodes “related by family ties” in one and the same chain of anonymous Tor routers. Special task of option *NodeFamily* can be needed only then, when a server with this pseudonym does not report to which “family” it reckons itself, that should be proclaimed by means of indicating the parameter MyFamily in *torrc* file on the side of OR server. Multiple indications of this option are allowed.

## **RendNodes pseudonym,pseudonym,...**

The list of nodes that should be used as rendezvous points (meeting) as far as possible.

## **RendExcludeNodes pseudonym,pseudonym,...**

The list of nodes that in no circumstances should be used when choosing rendezvous points (meeting points).

## **SOCKSPort PORT**

To notify Tor that connections, which are installed by applications using SOCKS-protocol, must be bugged in this port. Zero-fill this parameter if you do not need applications establishing connections according to SOCKS-protocol by means of Tor. (Value by default: 9050).

## **SOCKSBindAddress IP[:PORT]**

To establish linkage to this address for hearing requests for connection from applications interacting according to SOCKS-protocol (by default: 127.0.0.1). You may as well indicate port (for instance, 192.168.0.1:9100), which, it is clear, should be “open” by means of corresponding firewall setting on a machine for a specified purpose. Determination of this option can be repeated many times to carry out simultaneous (“parallel”) linkage to a host of different addresses/ports.

## **SOCKSPolicy policy,policy,...**

It assigns policies of entering a given server with the purpose of limiting the circle of clients' machines, which are permitted to connect the SOCKS port. Description of these policies is introduced much as how it is done for output policies (see below).

## **TrackHostExits host,.domain,...**

For each of values in the list separated by commas Tor will trace recent connections for hosts corresponding to this value and will attempt to use one and the same output (locking) node for each of them. If an ordinary list item is anticipated by the symbol “.”, then its meaning will be treated as a corresponding to domain in general. If one of list items consists of only one “point” then it displays its “universal” correspondence to all path names. This option can turn out to be useful if You frequently establish connection with the servers which cancel all records of Your finished authentication (i.e. force You to leave and register again) during carrying out an attempt of TCP/IP-connection address modification established with one of such servers on Your new IP-address after its next change. Draw Your close attention that use of this option is disadvantageous for You, because it allows server to directly associate connection history, requested by a definite IP, with Your user account. Though basically if anyone needs to collect all the information about Your stay in server, those who wish in any case can do that by means of cookies or other means specific for exchange protocol being used.

## **TrackHostExitsExpire NUMBER**

Since servers, being output links of nodal circuit, are entitled to start work and end it at its own discretion i.e. one way or another – arbitrarily, randomly, it is desirable, that association between host and output node automatically loses its power on the expiry of some NUMBER of seconds of total network activity absence on the part of a server. By default – 1800 seconds (30 minutes).

## **Thus Tor can be quite easily configured according to current tasks.**

Existent set of Tor instructions is sufficiently big. Consideration of them all exceeds the limits of the present review. Here only several most typical variants of editing and merely a part of instructions are presented. The full list and syntax of instructions (in English) you can find on Tor development engineers' website.

Visit <https://www.torproject.org/tor-manual.html.en>

## 9. The usage on Smartphone

If you are in a country that block web sites, for example, China, maybe, you are even not able to get access to the certain web sites. Tor allows anonymously looking through a web and going round censorship on a desktop. Orbot gives Tor for Android, so you will be able to do the same using smartphone.

If you are connected to the cellular communication of data transmission or Wi - Fi - Orbot works also. Like the package of Tor Browser Bundle for the personal COMPUTER, it is connected to the network of Tor and allows anonymously looking through web pages.

If you are a dissident in such country, as Iran, it means that a government cannot find you, after placing of critical information in the Internet. Anonymity also allows avoiding censorship in the Internet and getting access to the web sites, that especially useful in such countries as China, where there is such censorship. If you are in the USA or somewhere in the world, it means that your visits of the Internet will not be related to you and kept in the arrays of databases due to PRISM or similar programs.

In the past this functionality was limited by people that used Tor on the computers. Now you can be connected to Tor on Android that allows using Tor on a mobile telephone. In addition to prevention of intercept you the provider, operator and government, there are other advantages that is given by Tor at mobile access. For example, you can use Twitter on Android via Tor.

Some authoritarian governments blocked access to Twitter, that at democratic protests you were not able to obtain information, but Twitter on Android can be set up on the use of Tor. Then Twitter will remain accessible, even if a government blocked access to him.

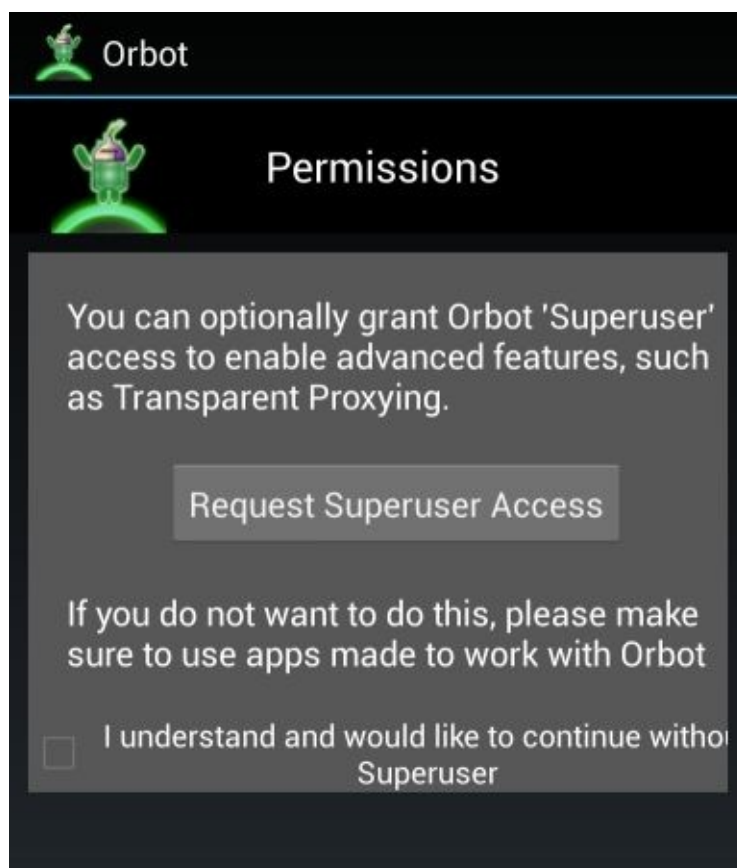


## Connecting to Tor through Orbot

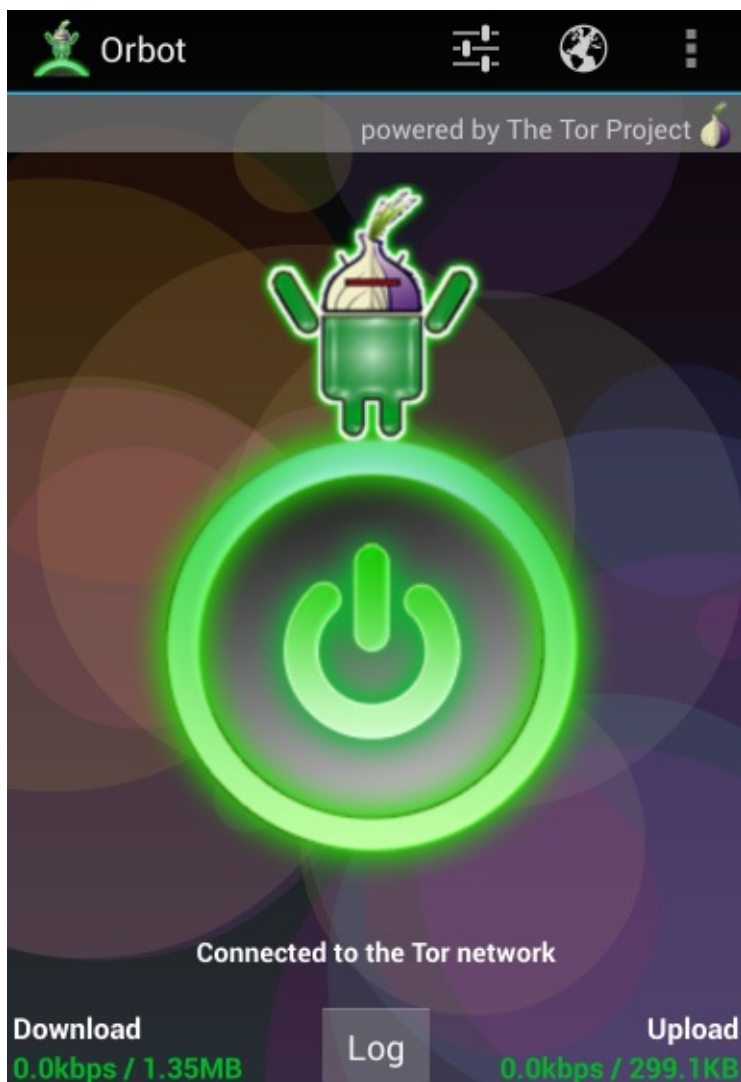
Orbot is the most essential part of puzzle. This application of Android is connected to Tor and creates local proxy that other programs can use on Your smartphone, getting permission to be connected through Tor.

To tune Orbot is easy, simply set the program, open it and pass through configuration master.

If you have access with administrative rights on the Smartphone, Orbot can function as transparent proxies. In other words, it can automatically make all network traffic to pass through Tor. If you will do this route, then keep in mind that some programs can show your real IP- address. In order to look through anonymously, you must use a browser that is created to hide IP- address. If you don't have such rights - it is well, because you can use Orbot with Orweb and other programs.



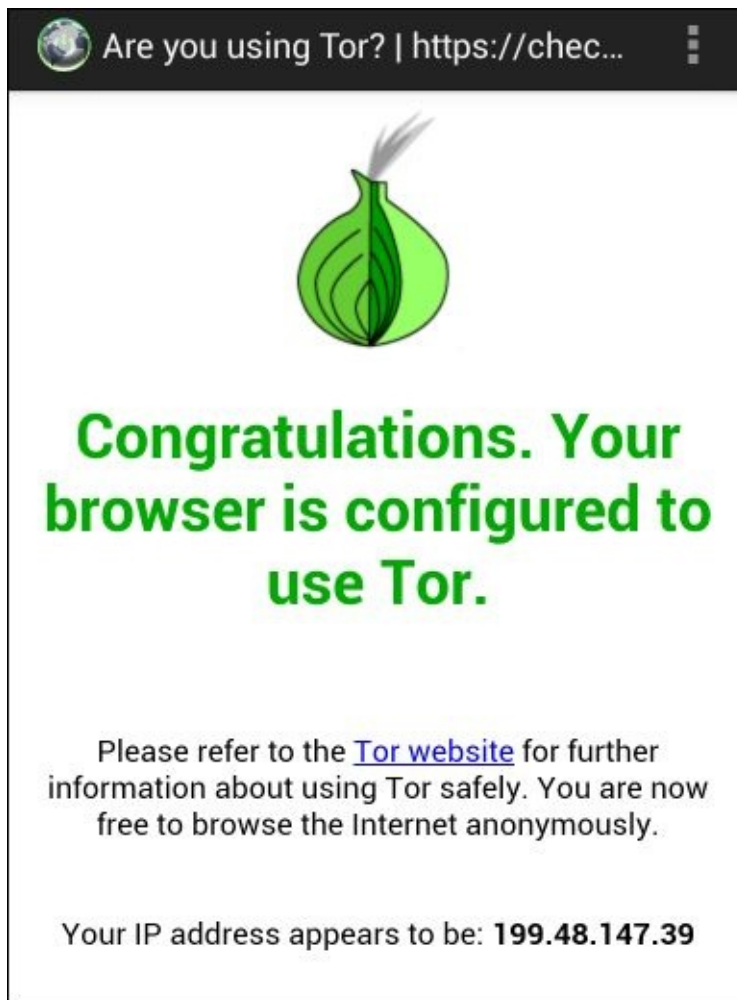
Press long on the icon of Orbot and Orbot will connect to the Tor network. An icon illuminates green during connecting to Tor.



### **Anonymous browsing via Orweb**

Since Orbot is set and start, you can use the browser of Orweb for an incognito. Orweb is well adjusted for work with Orbot and Tor. For example, Orweb does not keep history of the visited pages or other information about web-sites that you have visited. Orweb also disconnects JavaScript and flash by default, as well as Tor Browser Bundle on a desktop. JavaScript and flash in theory can be used by a web-site for determination of the real IP- address of your smartphone.

For the start of Orweb from within Orbot simply press on the icon of globe in overhead part of screen of Orbot. Orweb will be opened and will show a report that he is connected to Tor, if all works correctly. Now you can use the browser of Orweb for an incognito.

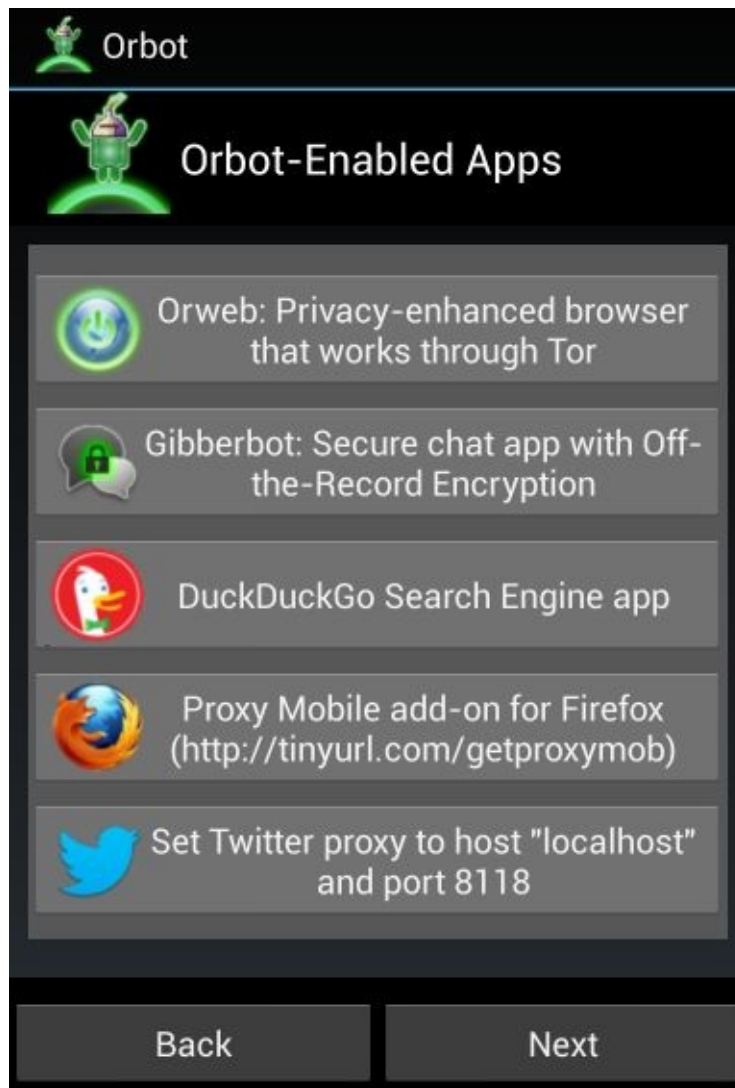


## Other programs that work with Orbot

Orbot also can be used as proxy-server for other applications. Any application that supports proxies in theory can pass the traffic through the proxies of Tor Orbot. Nevertheless, Orbot contains the list of other programs that can be adjusted on work with him. For example, you can use for the reliable communication Gibberbot, for a search through Tor is application of DuckDuckGo, to look through the Internet with Firefox for Android and by application of Proxy Mobile, or to set the proxies of Twitter on "localhost" and port 8118.

If you have access with administrative rights and you adjusted transparent proxies, then other applications must work with Orbot in theory, but more safely, if you use the programs specially tested for correct work with Tor.





Keep in mind that viewing is considerably slower when you use Tor, as usual, because the process of routing adds overhead costs. However, if you need anonymously to look over a web or go round censorship, then this decline of speed will be a small pay.

## 10. How to check Tor operation?

In order to check how Tor ensures anonymity you need to go to one of the websites, which can determine and highlight IP-address and several other data about a user. The list is put below.

In order to know your real IP-address – you can enter one of these websites except Tor. (For example checkip.com or Tor website test page - <https://check.torproject.org> etc.) Remember your IP-address and start checking.

Switch on Tor and enter a few test websites one after another.

In order to avoid a mistake IP check always should be carried out on resources, which reliably consider different nuances. That is to say, if anonymity were important, then it would not be superfluous to be verified in several places not relying upon one service.

Below are listed links to the most reliable and informative resources:

- The following website contains a set of various proxy server tests for anonymity including Java-check <http://www.stilllistener.addr.com/checkpoint1/index.shtml>

- The following website displays IP-address and (hence IP) a country of residence, as well as information about a provider: <http://www.anonymize.net/current-ID.phtml>

- <http://smart-ip.net/>- you can learn HTTP and SOCKS Proxy addresses

- <http://ip-whois.net/>, -<http://clientn.free-hideip.com/map/whatismyip.php>

<http://smart-ip.net/tools/geoip>, <http://checkip.com>, <http://torcheck.xenobite.eu/>

If none of the test websites do not highlight a real IP-address then Tor ensured your anonymity!

Thank you very much both for downloading this eBook and for reading it from the beginning to the end.

If you enjoyed this book or found it useful

**I ' d be very grateful if you ' d post a short review on Amazon**

Your post really does make a difference and I can get your feedback & make this book even better.