

Installing I2P on Backtrack 5



mail : infosecpirate@gmail.com

<http://twitter.com/#!/r45c4l>

**Greetzs to my all ICW and darkc0de
brothers, d3hydr8, sinner_01, baltazar,
Beenu and all Indian Hackers.**

Introduction :

Some time back, TOR was the most favorite tool for hackers, pen testers and every one else who were concerned about there anonymity while surfing over Internet. But now the trend is changing very fast and more and more people are shifting to I2P for many reasons.

Anyways, for those who are beginners or those who have no idea about both TOR and I2P, let's start with a basic introduction of both the products. Oh yeah, how can I forget those who are very much concerned over there anonymity even for there day to day work but who are not very technically sound.

Ok, so first a little description of TOR :

According to Wikipedia : “ **TOR** or **The Onion Router** is a system intended to enable online anonymity. r t client software routes Internet traffic through a worldwide volunteer network of servers in order to conceal a user's location or from any one conducting 'network surveillance' or 'traffic analysis'. TOR basically makes it more difficult to trace internet activities including the websites you visit, instant messaging and other communication forms.”

On March 2011 The Tor Project was awarded the Free Software Foundation's 2010 Award for Project of Social Benefit.

Well this was just to present the basic overview of TOR, so let's not make it short and simple and move on to our next product 'I2P'.

Description of I2P :

According to Wikipedia I2P which is short for **Invisible Internet Project**. The purpose is building an anonymous network or more accurately a 'pseudonymous overlay network'

The network application can use to anonymously and securely send messages to each other. Possible uses include anonymous surfing, chatting, blogging and file transfer.

The application itself is called i2p router and a computer running i2p is called i2p node, whereas those, too, are often referred to as routers.

According to I2P site (www.i2p2.de) : “I2P is an anonymizing network, offering a simple layer that identify-sensitive application can use to securely communities. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.

Many applications are available that interface with I2P, including mail, peer-peer, IRC chat and others.

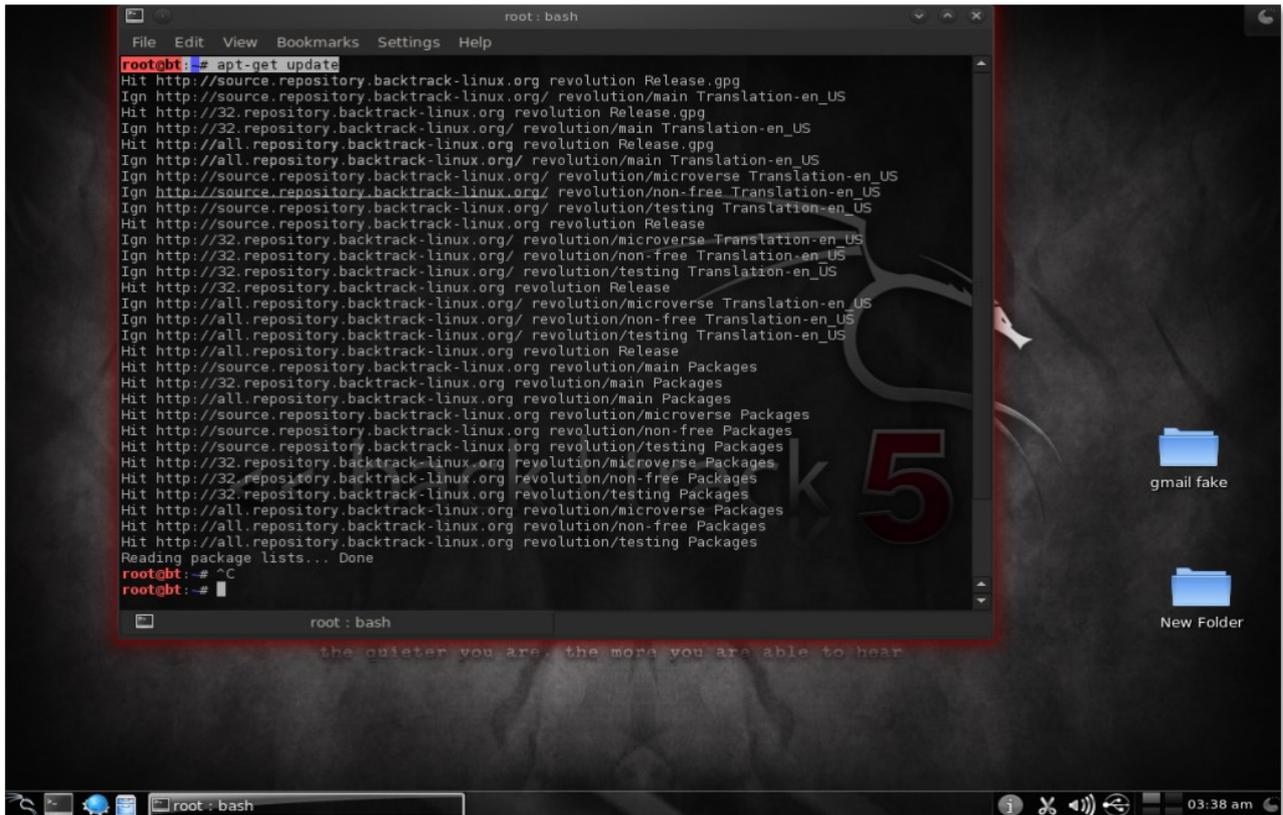
Well there is one more application “**Freenet**” (www.freenetproject.org) , but it's not a part of our discussion so we will keep it out of it, may be some other time I can write just only about this particular product.

Ok so this paper is about installing I2P on Backtrack 5 r1, so let's get back to it. I will be doing this on my BT5 r1 virtual machine because my base machine (Ubuntu 11.10 has already i2p installed).

Installing I2P :

Ok so first thing first, let's open our BT machine and do a quick 'update'

```
root@bt:~# apt-get update
```



```
root@bt:~# apt-get update
Hit http://source.repository.backtrack-linux.org/ revolution Release.gpg
Ign http://source.repository.backtrack-linux.org/ revolution/main Translation-en_US
Hit http://32.repository.backtrack-linux.org/ revolution Release.gpg
Ign http://32.repository.backtrack-linux.org/ revolution/main Translation-en_US
Hit http://all.repository.backtrack-linux.org/ revolution Release.gpg
Ign http://all.repository.backtrack-linux.org/ revolution/main Translation-en_US
Hit http://source.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
Ign http://source.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
Hit http://source.repository.backtrack-linux.org/ revolution/testing Translation-en_US
Hit http://source.repository.backtrack-linux.org/ revolution Release
Ign http://32.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
Ign http://32.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
Ign http://32.repository.backtrack-linux.org/ revolution/testing Translation-en_US
Hit http://32.repository.backtrack-linux.org/ revolution Release
Ign http://all.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
Ign http://all.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
Ign http://all.repository.backtrack-linux.org/ revolution/testing Translation-en_US
Hit http://all.repository.backtrack-linux.org/ revolution Release
Hit http://source.repository.backtrack-linux.org/ revolution/main Packages
Hit http://32.repository.backtrack-linux.org/ revolution/main Packages
Hit http://all.repository.backtrack-linux.org/ revolution/main Packages
Hit http://source.repository.backtrack-linux.org/ revolution/microverse Packages
Hit http://source.repository.backtrack-linux.org/ revolution/non-free Packages
Hit http://32.repository.backtrack-linux.org/ revolution/microverse Packages
Hit http://32.repository.backtrack-linux.org/ revolution/testing Packages
Hit http://32.repository.backtrack-linux.org/ revolution/non-free Packages
Hit http://32.repository.backtrack-linux.org/ revolution/testing Packages
Hit http://all.repository.backtrack-linux.org/ revolution/microverse Packages
Hit http://all.repository.backtrack-linux.org/ revolution/non-free Packages
Hit http://all.repository.backtrack-linux.org/ revolution/testing Packages
Reading package lists... Done
root@bt:~# ^C
root@bt:~#
```

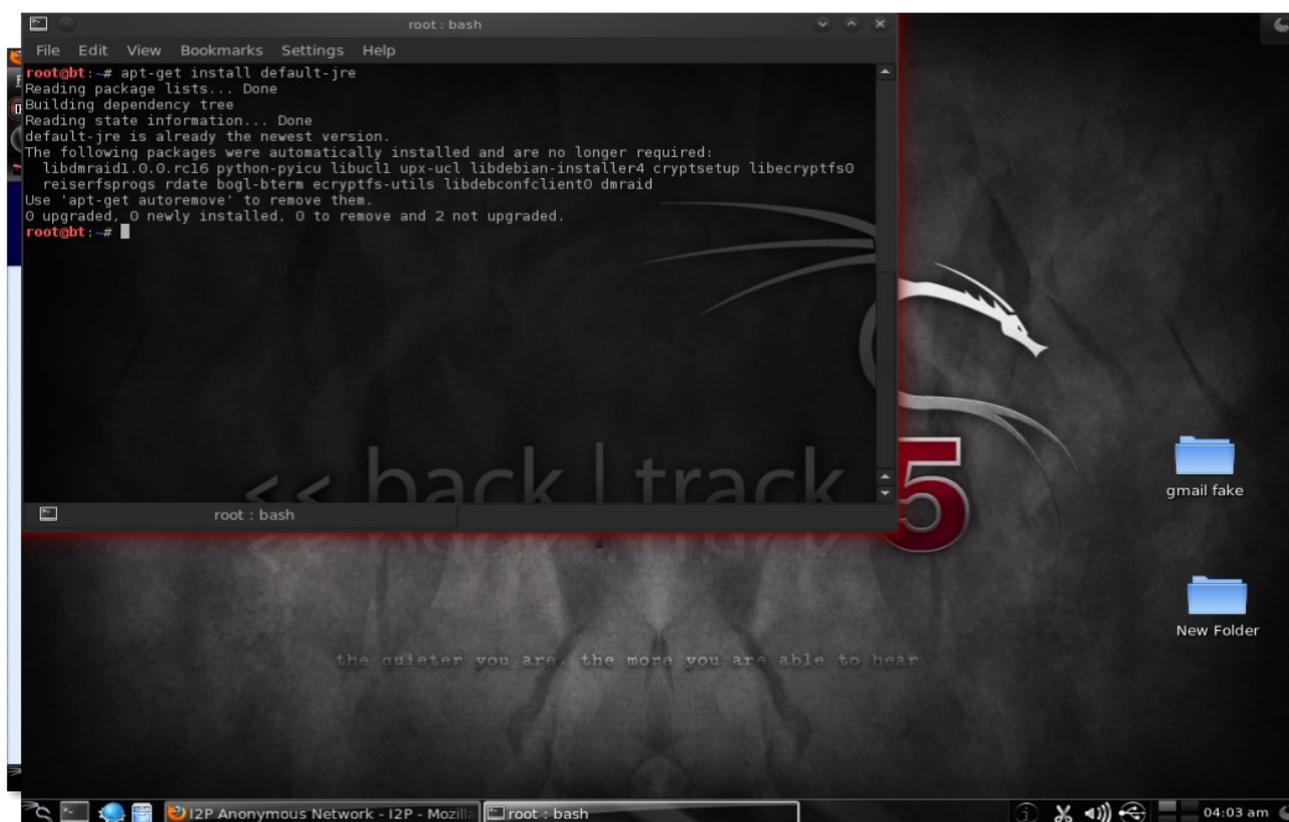
Ok, now let's open I2P site www.i2p.de

We can see there are lots of information there and also the download link of I2P.

As we are installing it on BackTrack which is based on Debian so our steps are going to be like that only.

Well first of all, before we start we need to install Java which is very simple to install, we can do it either through terminal or package manager, but I prefer doing it through CLI.

```
root@bt:~# apt-get install default-jre
```



Well in my case it is already installed, so I don't have to install it again, if this is the same case with your machine then you can move on to next step otherwise, you need to install it first.

Now let's go to the download page (www.i2p.de/download.html) of Java for the Graphical interface and follow the instructions given there.

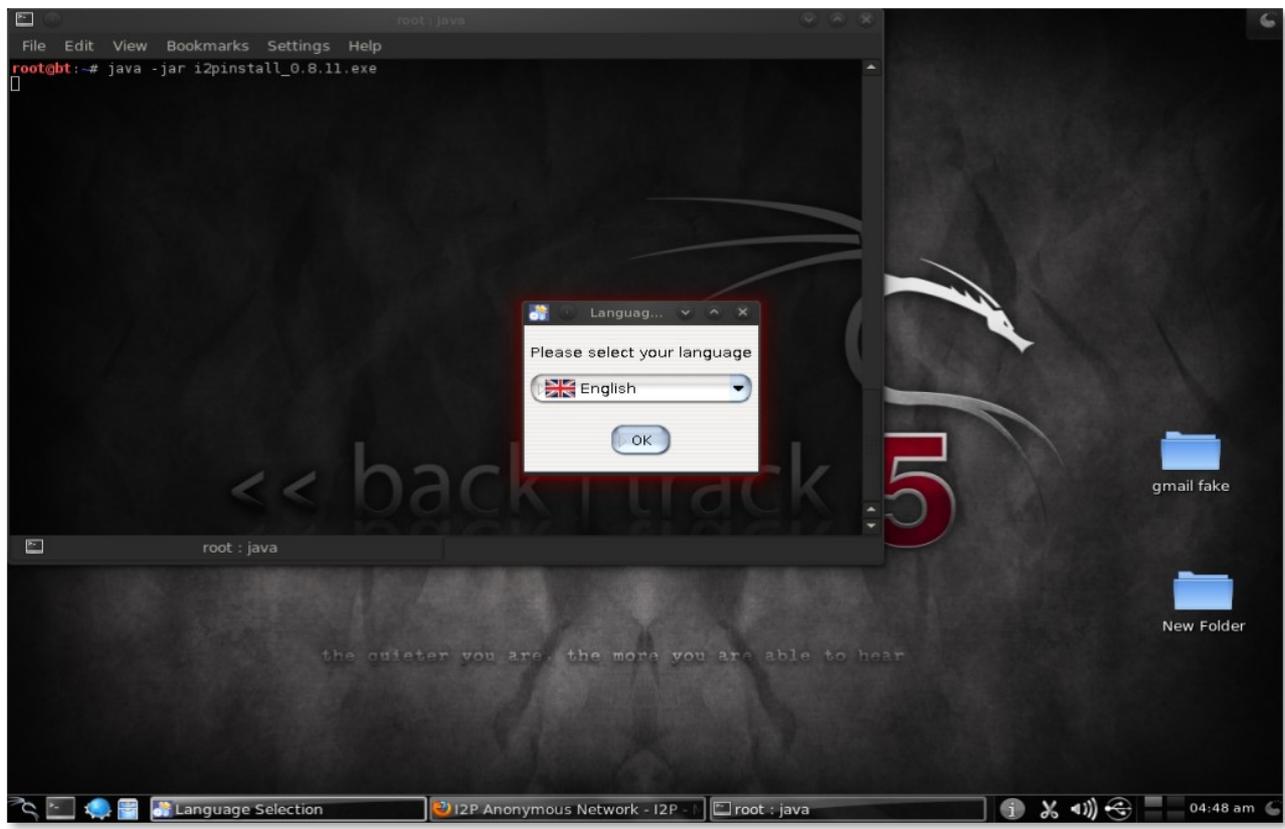
First we need to download and install the package which we are again going to do through the command line :

```
root@bt:~# wget http://mirror.i2p2.de/i2pinstall_0.8.11.exe
```

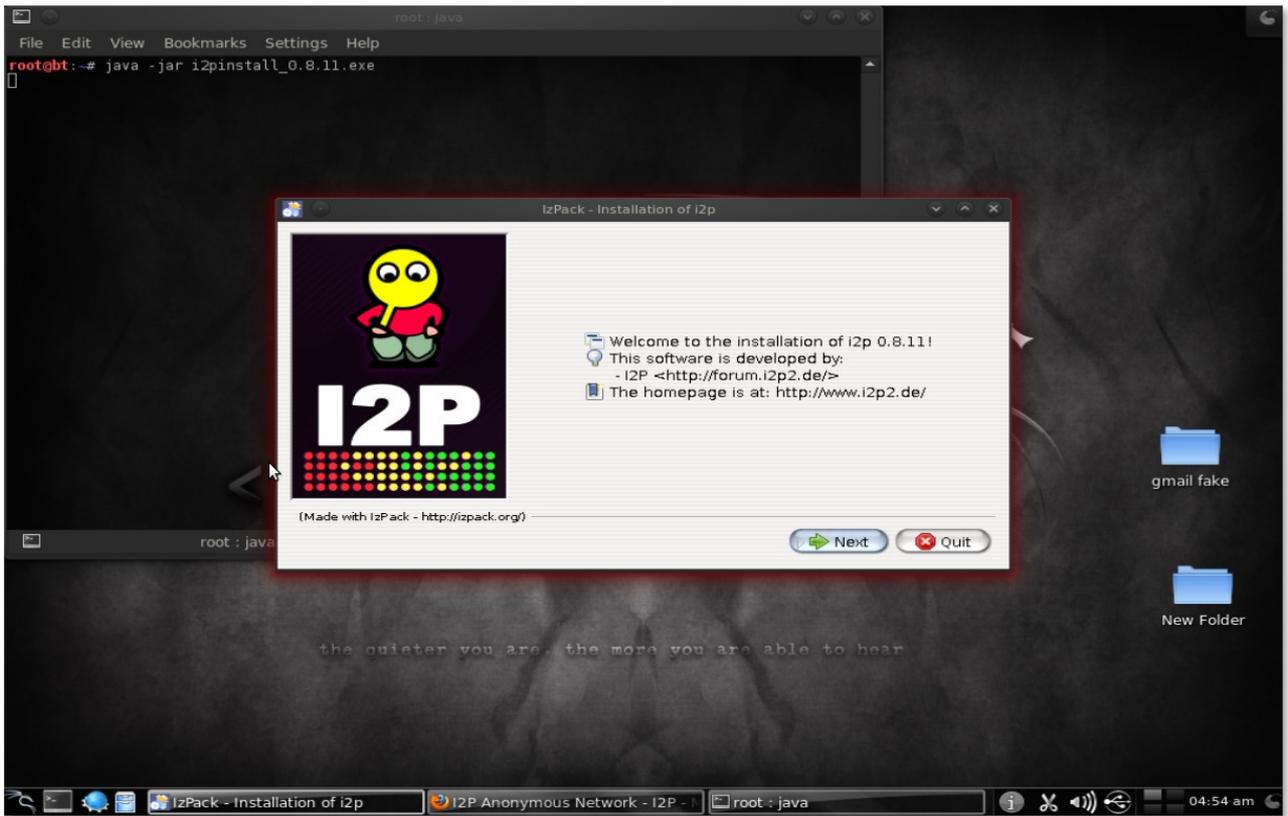


After the package is downloaded we can install it by giving the simple command

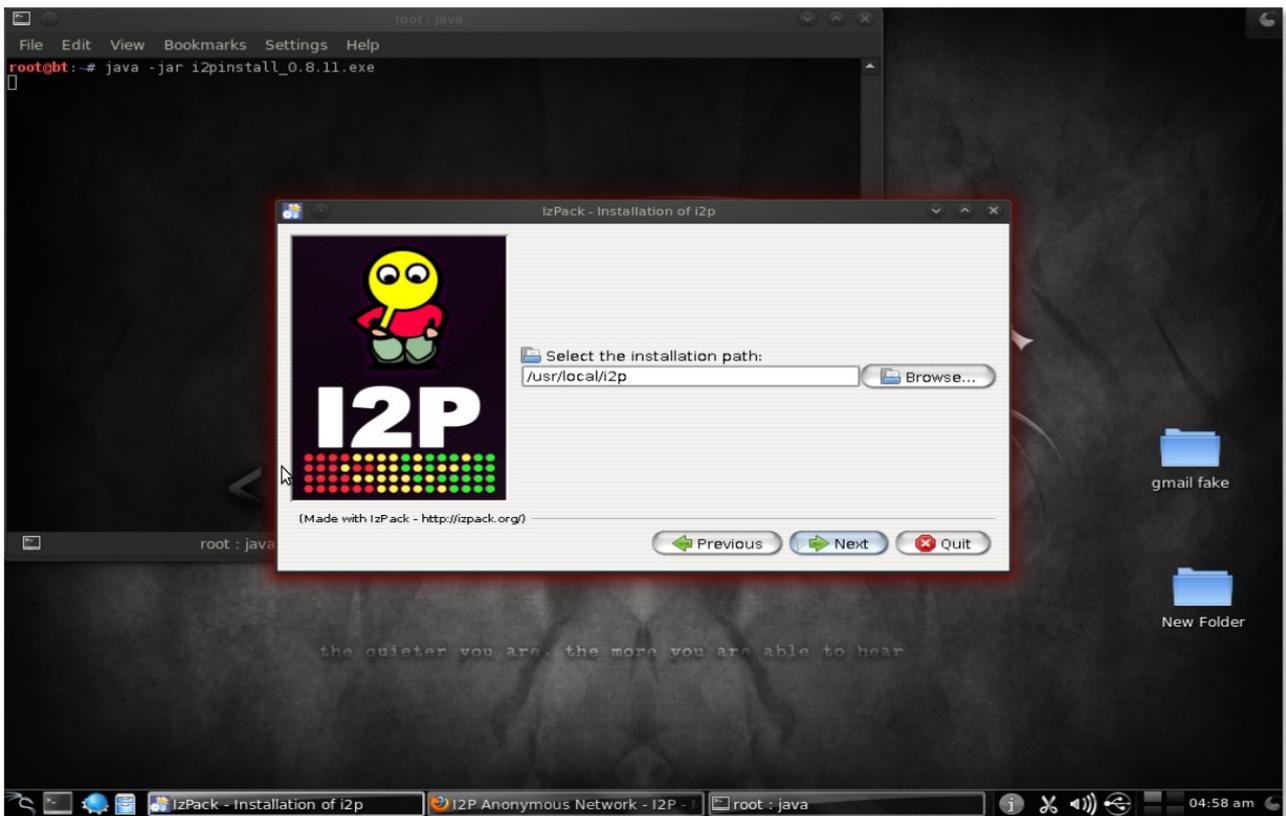
```
root@bt:~# java -jar i2pinstall_0.8.11.exe
```



It will launch the GUI installer as we can see in the above screen shot, where it's asking for the choice of language which we are going to use as English



After this when we click the 'Next' button, it will ask where to install the program.



It will be installed on the selected location





After that it will ask to read the information related to installation, now click 'Next' again and finally the installation is complete.



After the installation is done, lets go the the /usr/local/ where i2p is installed

```
root@bt:/# cd usr/local/
```

```
root@bt:/usr/local# ls
```

```
bin doc etc games i2p include info lib libexec man sbin share src var
```

Now let's go to the **i2p** directory where **i2p** router is which we need to start now.

```
root@bt:/usr/local# cd i2p/
```

```
root@bt:/usr/local/i2p# ls
```

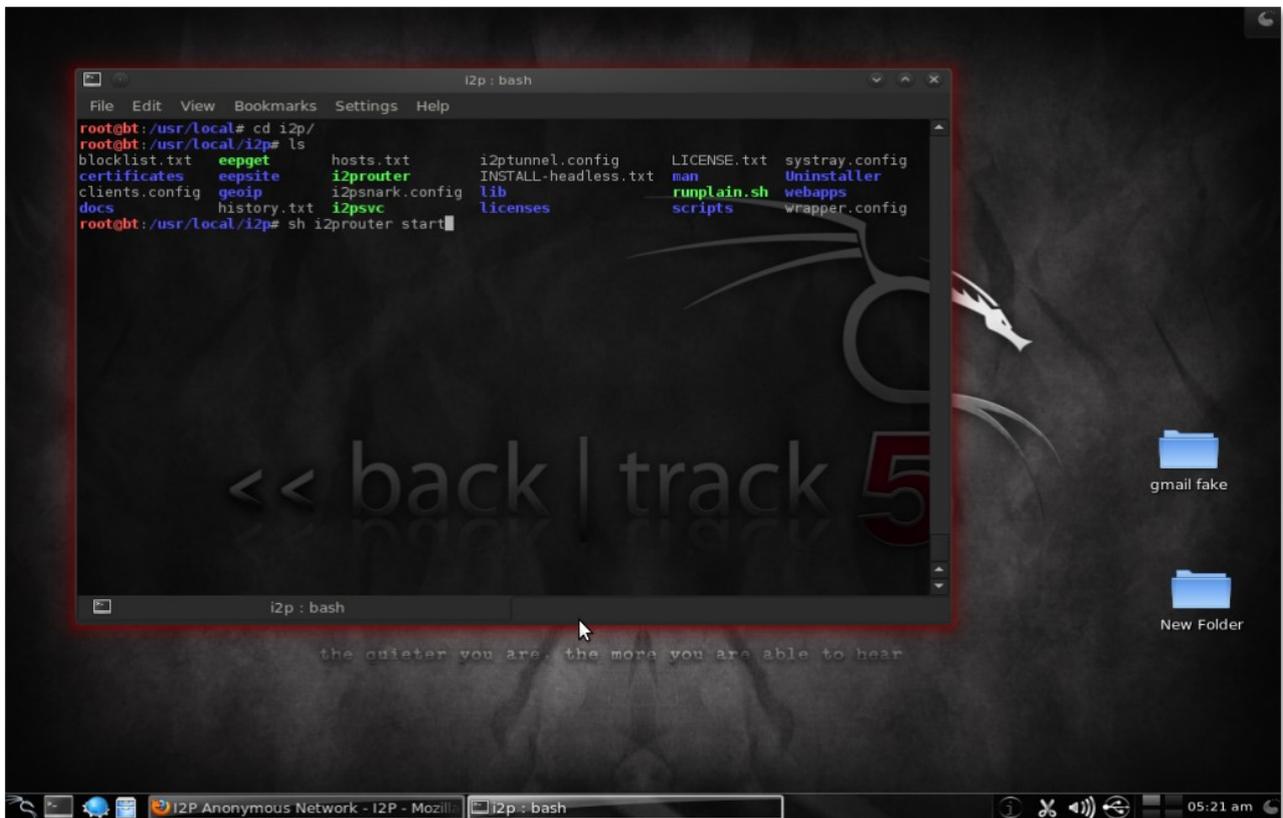
```
blocklist.txt eepget hosts.txt i2ptunnel.config LICENSE.txt systray.config
```

```
certificates eepsite i2prouter INSTALL-headless.txt man Uninstaller
```

```
clients.config geoip i2psnark.config lib runplain.sh webapps
```

```
docs history.txt i2psvc licenses scripts wrapper.config
```

```
root@bt:/usr/local/i2p# sh i2prouter start
```

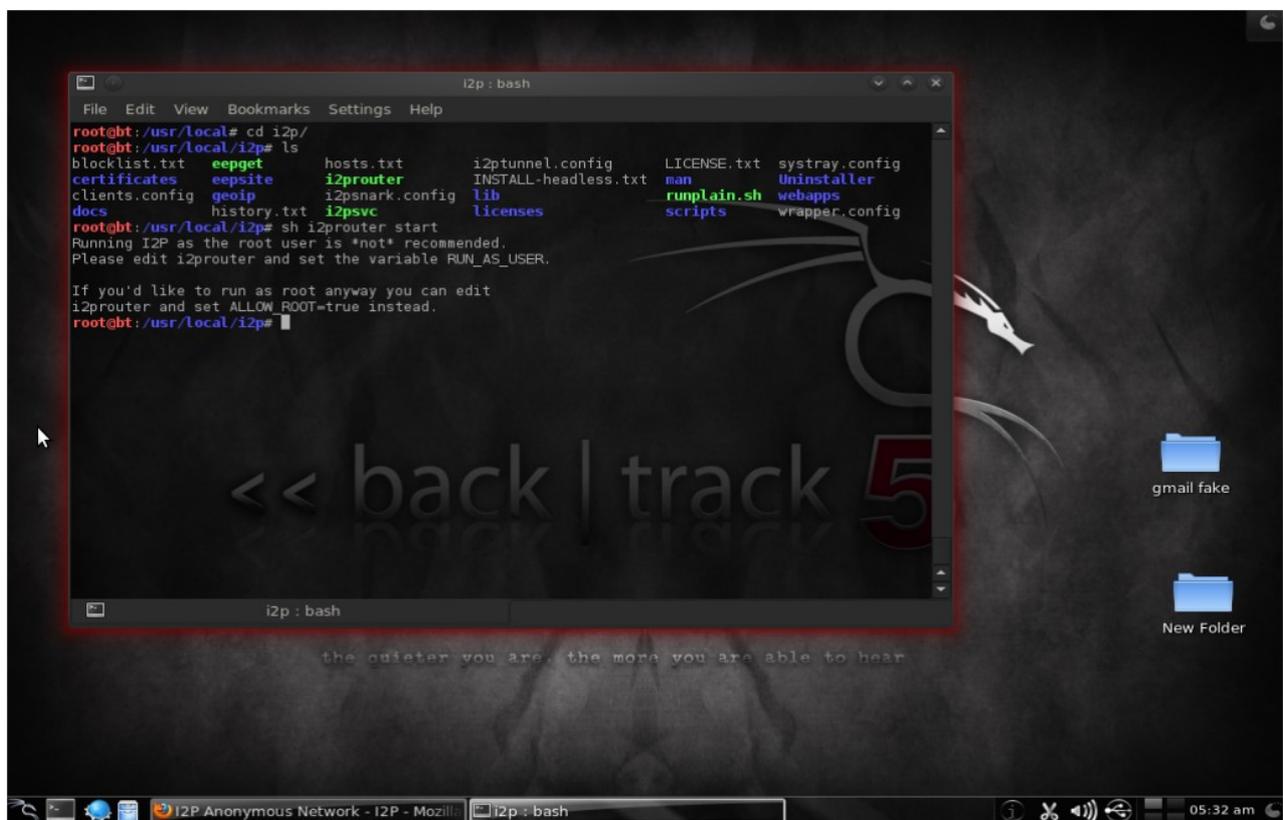


After the command is executed, and because I am already running it as root, it will show me the following message. This may not be same on your computer in case if you are not running it as root.

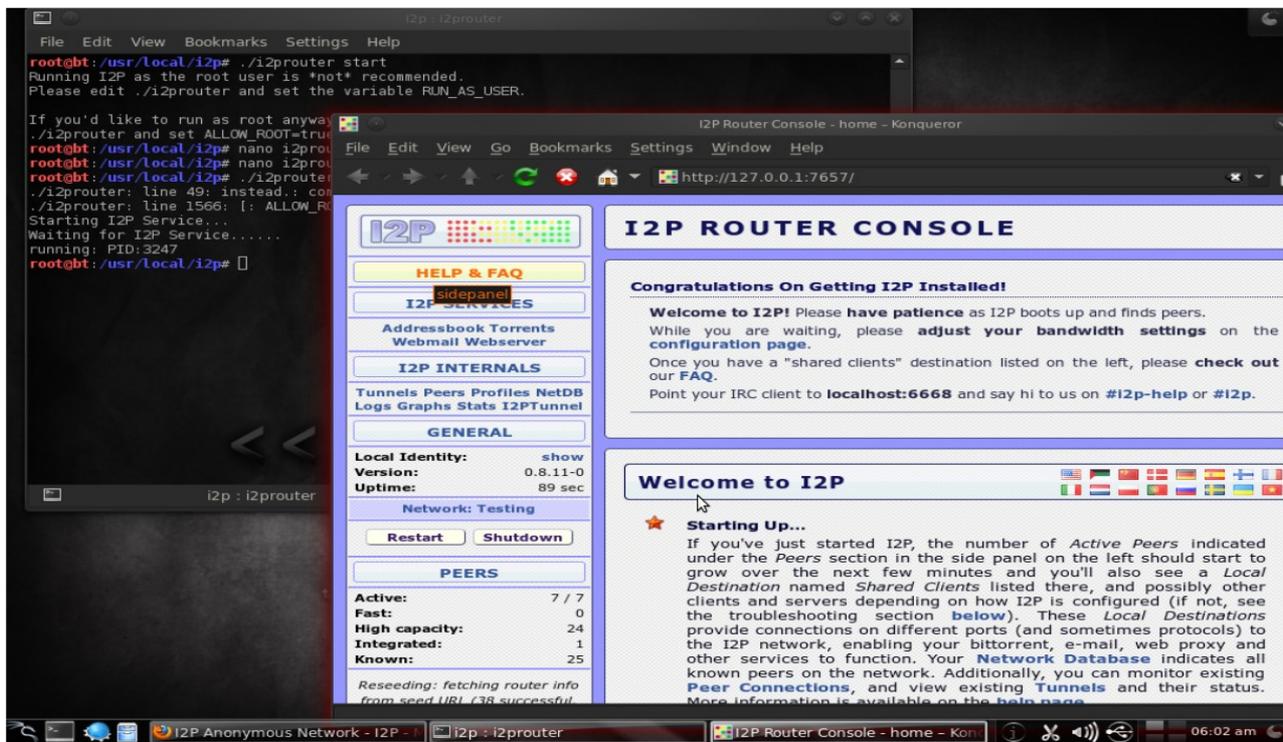
```
root@bt:/usr/local/i2p# sh i2prouter start
Running I2P as the root user is *not* recommended.
Please edit i2prouter and set the variable RUN_AS_USER.
```

If you'd like to run as root anyway you can edit i2prouter and set ALLOW_ROOT=true instead.

So what I am going to do now is edit the i2prouter and then set ALLOW_Root=true instead.



After editing the file we can finally start the **i2p** router



Well after the installation is done, we can check there are a hell lot of services which we can configure with **i2p** to remain anonymous like : Anonymous web browsing, Anonymous email, Anonymous chat with various clients like Pidgin or xchat, Anonymous file transfer and many more which we can check as soon as our **i2p** starts on <http://127.0.0.1:7657/>

The best part of **i2p** is that it's entirely web based and configuring and starting and stopping on any services are very easy as compared to TOR. We can check out about the various options by going to the '**i2p services**' page.

There are various **i2p** clients which we can configure according to our needs.

We can also Edit and Delete **i2p Client Configuration** which we can Edit and Delete as per our need, **i2p Tunnel Service** which gives information about the present connection status.

I2P Router Console - config clients - Konqueror

File Edit View Go Bookmarks Settings Window Help

http://127.0.0.1:7657/configclients

I2P CLIENT CONFIGURATION

Network | UI | Service | Update | Tunnels | Clients | Peers | Keyring | Logging | Stats | Reseeding | Advanced

Client Configuration

The Java clients listed below are started by the router and run in the same JVM.

Client	Run at Startup?	Control	Class and arguments
I2P Router Console	<input checked="" type="checkbox"/>	Edit Delete	net.i2p.router.web.RouterConsoleRunner 7657 ::1,127.0.0.1 ./webapps/
SAM application bridge	<input type="checkbox"/>	Start Edit Delete	net.i2p.sam.SAMBridge sam.keys 127.0.0.1 7656 i2cp.tcp.host=127.0.0.1 i2cp.tcp.port=7654
Application tunnels	<input checked="" type="checkbox"/>	Edit Delete	net.i2p.i2ptunnel.TunnelControllerGroup i2ptunnel.config
I2P webservice (eepsite)	<input checked="" type="checkbox"/>	Edit Delete	org.mortbay.jetty.Server "/root/.i2p/eepsite/jetty.xml"
Open Router Console in web browser at startup	<input checked="" type="checkbox"/>	Edit Delete	net.i2p.apps.systray.UrlLauncher http://127.0.0.1:7657/
BOB application bridge	<input type="checkbox"/>	Start Edit Delete	net.i2p.BOB.BOB

To change other client options, edit the file /root/.i2p/clients.config. All changes require restart to take effect.

I2P Anonymous Network - I2P - I2p : i2prouter I2P Router Console - config clien 06:18 am

I2P Router Console - tunnel summary - Konqueror

File Edit View Go Bookmarks Settings Window Help

http://127.0.0.1:7657/tunnels#TLI8

I2P TUNNEL SUMMARY

Exploratory tunnels (configure)

In/Out	Expiry	Usage	Gateway	Participant	Endpoint
↓	5 min	6 KB	N0hQ 1881593078 O	4UuC 3542305512 L	458956546
↓	3 min	31 KB	IWmX 2109415059 L	Cjj7 1765024521 L	1592566488
↑	9 min	8 KB	4137396843	IDZH 2574202549 O	G2Zs L
↑	63 sec	45 KB	1660234094	mkJR 2445288845 O	Fuqw O
↑	63 sec	36 KB	1648875019	3AzT 1057382871 O	8N2J M
↑	8 min	0 KB	2687922540	3AzT 3340431479 O	8N2J M

Lifetime bandwidth usage: 606.00 KB in, 595.00 KB out

Client tunnels for shared clients (configure)

In/Out	Expiry	Usage	Gateway	Participants	Endpoint
↓	8 min	0 KB	mkJR 3002058669 O	8bn2 3087647136 L	Cjj7 3077043171 L
↑	4 min	17 KB	1694359137	4UuC 4215486654 L	N0hQ 3695104440 O

Lifetime bandwidth usage: 41.00 KB in, 309.00 KB out

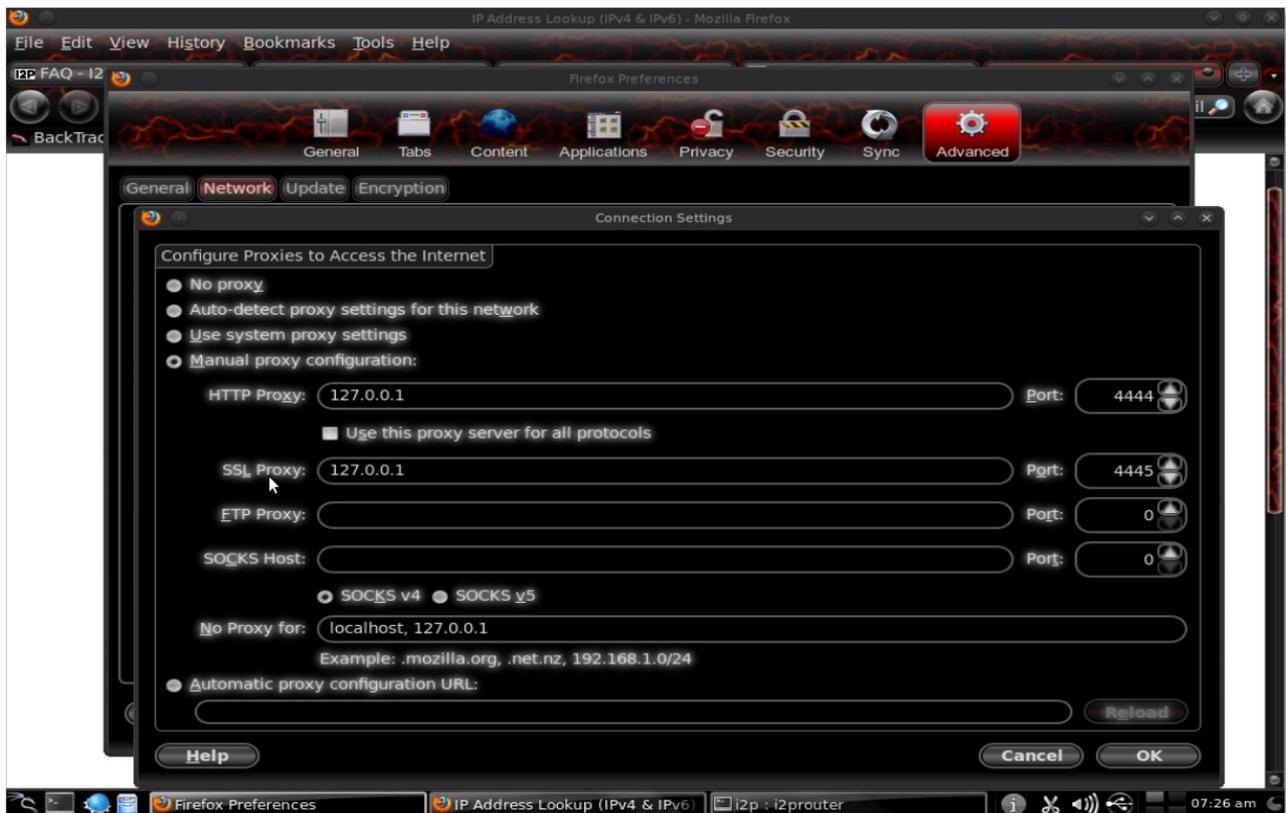
Participating tunnels

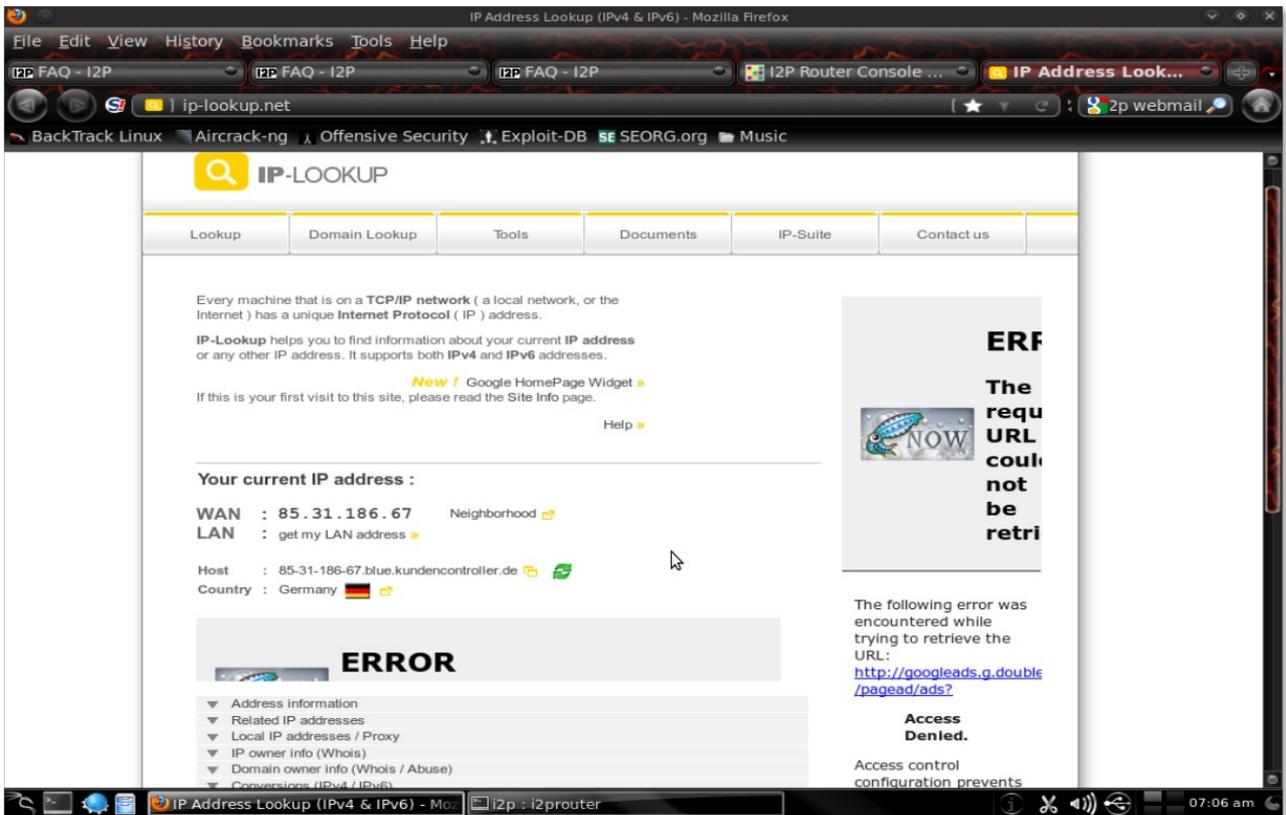
Receive on	From	Send on	To	Expiration	Usage	Rate	Role
------------	------	---------	----	------------	-------	------	------

Problem loading page - Mozilla Fi I2p : i2prouter I2P Router Console - tunnel sum 06:31 am

During all this we forgot to check the main purpose of using **i2p** and that is being anonymous. So let's look at my IP address before I configured my browser to use **i2p** and then the next IP address assigned to me when I configured my browser to use **i2p**.

So let's have a quick look that how to configure your browser according to use **i2p**. I am showing it here it for the Firefox, it's almost same for other browsers too if you know how to use proxies.





So my IP which was originally 180.215.220.200 now got changed to 85.31.186.37

Conclusion :

There are many more things which we can do with I2P but covering all those aspects will not be possible under the scope of this paper. This paper is written just to present a basic idea and features of I2P and how to install it over BackTrack 5 R1.

One more purpose of the paper was to show how easy I2P is to use and configure over TOR and the extra features.

To cover most of the features of I2P I have decided to write down a separate paper which I will be posting very soon.

For any suggestions and queries please mail me : infosecpirate@gmail.com

Reference :

www.google.com

<http://en.wikipedia.org/>

<http://www.i2p2.de/>

Share the c0de.