

**Quickguide to  
Anonymous Internet access with Tor,  
Circumventing P2P restrictions,  
an outlook for anonymous P2P**

**Ruediger Teichert**  
[ruediger@teichert-online.de](mailto:ruediger@teichert-online.de)

**v2.1, January 2008**

This paper contains references to copyrighted material and trademarks. All trademarks belong to their respective owners. No trademarks or owners are mentioned in this paper; however, do not assume any mentioned entity would be free of copyright or trademark because trademark or copyright are not mentioned here.

<b>1 MOTIVATION .....</b>	<b>4</b>
<b>2 ANONYMITY SERVICES .....</b>	<b>5</b>
<b>3 LEGAL RESTRICTIONS .....</b>	<b>6</b>
<b>4 WHAT CAN BE ANONYMOUS (HTTP, P2P?) .....</b>	<b>6</b>
<b>5 TOR DOWNLOAD .....</b>	<b>7</b>
<b>6 INSTALLATION.....</b>	<b>7</b>
<b>7 HANDLING .....</b>	<b>8</b>
<b>8 HOW TOR WORKS (BASICS) .....</b>	<b>9</b>
<b>9 ATTACKS AND ANONYMITY RESTRICTIONS .....</b>	<b>10</b>
<b>10 TOR AND BITTORRENT .....</b>	<b>11</b>
10.1 why?.....	11
10.2 Tor abuse.....	12
10.3 Suitable clients .....	12
10.4 Utorrent configuration / summary.....	12
<b>REFERENCES .....</b>	<b>14</b>

## 1 Motivation

### HIDE IP-ADDRESS

Computer and their networks being traceable have a lot of benefits for law enforcement. Recent examples where lacking privacy of information systems have lead to arrest of criminals resp. suspected criminals are the arrest of the so-called BTK killer in Kansas, USA, who had identified himself by sending a Microsoft Word document to the police. Word saves user and organization name, so his arrest followed swiftly [Wiki\_Rader]. Child molesters have been arrested by police-tracing software on their computers. However, even curiosity of normal citizens may lead to have the identity of these citizens tracked down by security agencies. The consequences of such a database entry are unforeseeable. Visiting a terrorist homepage out of curiosity, because it had been mentioned in the news, can nowadays lead to logging the IP address of the site visitor by security agencies. In Germany, the federal police BKA had logged the IP addresses of visitors of their website and uncovered their identity (name and address) [Slash\_BKA]. Even if the desire of security authorities to reveal identities of online users can be well understood, individuals may still have the desire to hide their identity, aiming not be mistaken for criminals by law enforcement.

In countries as the “People’s Republic of China”, visiting the “wrong” web pages is a lethal risk.

Anonymous Internet access is a solution for this problem. Tor is also aimed at users in restrictive governments as China to allow them free and uncensored access to the world wide web.

### CIRCUMVENT BLOCKS OF WEB PAGES

Some governments block access to certain websites by Firewalls. The “Great Firewall of China” is one example for this, which makes access of websites mentioning key words like Taiwan or Tibet unavailable for Chinese-based internet surfers. Tor helps accessing those “forbidden websites”, as only the communication from the target web address into the Tor network will be unencrypted. The China-based computer will receive encrypted data from within the great Tor network of Routers, so the original website can not be traced.

### CIRCUMVENTING P2P-BLOCKS

Some Internet Service Provider (ISP) or other organizations granting Internet access may try to block Peer-to-Peer (P2P) downloading not to be bothered with copyright infringements from illegal music or video downloads by customers or participants. Mostly, these organizations do not prohibit P2P download by itself in their terms of use, but rather the download of copyright protected material. Thus, downloading legal software or files, like Freeware, Shareware, GNU-licensed material or privately generated video files is usually legal. Kindly check the legal implications of your actions

and terms of use of your Internet access before applying any technologies from this guide. However, this guide contains an easy way to circumvent such restrictions in many environments by usage of Tor. It is not meant to break through a Firewall or similar to download illegal material; I used it to download a free operating system for my work even though it wouldn't work the "normal way", probably because of a Firewall.

...AND ANONYMOUS P2P ?

To counteract the massive illegal downloads of music and software, enterprises have hired Anti-P2P companies to monitor, sabotage and track down P2P-participants who are in violation of copyright laws. However, to protect their privacy, even legal P2P users may seek to hide their identity while downloading, not to avoid being submitted to supervision of organizations who may rather "shoot" (track and log a connection and sue the peers) than ask questions, as most P2P user do happen to be illegal users. There are also more and more perfectly legal downloads using P2P systems like Bittorrent. Still, the risk is very high to be subjected to bogus / sabotage data from anti-P2P organizations. Anonymous P2P would be a solution ensuring privacy. Or to say it frankly, why should anyone have an interest to reveal his or her IP address to any private companies, even if only doing legal things via P2P? However, it doesn't yet work out as it's done in this paper; but the behaviour of the Bittorrent software Utorrent in combination with Tor is analyzed. A solution may be the usage of the alternative Bittorrent client Azureus with Tor, but this is not investigated in this paper, most likely in a forthcoming one.

## 2 Anonymity services

JAP, the anonymity (anon) service of the Technical University of Dresden [JAP] in Germany is a world-wide anon service. It's still free though its on the brink of being transformed into a commercial service, as public project sponsorship has run out. It's based on David Chaum's Mix principle. It is not used in this paper.

Tor is a worldwide and now widely employed anon service, free of charge and maintained by enthusiasts using their own bandwidth, servers and money. It is used in this paper. Tor is also based on the Mix principle, applied within the "Onion routers". An Onion router is a Mix (server) of the Tor network. Tor will hide your IP address to a computer, to which you want to connect. Your computer will not get in contact directly to your target address, say [www.that-mallory-guy.com](http://www.that-mallory-guy.com) [website did not exist when I wrote this paper], but instead you will send your data packages into the Tor Onion router network, where they will be exchanged between several routers (they will be mixed), in an encrypted way (being mixed with messages of the same length; possibly these have to be created by the routers of such a system based on David Chaum's Mix principle in case of low traffic times). Finally, the server at [www.that-mallory-guy.com](http://www.that-mallory-guy.com) will only see the IP address of the Tor exit node, not the IP address of the original sender.

Even if your data packages will be encrypted while in the Tor network, they will finally reach your target computer without encryption. This is an entrance for attacks on the Tor network.

Sketch:

Sender (Client PC)-----→**TOR-network**-----→target server on Internet  
| encryption here      | *no encryption!*

### 3 Legal restrictions

Before using any technique to communicate anonymously, make sure usage of an anonymous communication system is legal in your country. Some countries rule out usage encryption of any kind for computer communication. With Tor, you do not technically use encryption by yourself and you do not deliver an encrypted data package. However, the Tor system uses encryption internally.

If you are penetrating a firewall or restrictions of your ISP to allow P2P, as shown here, make sure your action is not illegal. Do not attempt to download copyright protected software using this guide.

Be welcomed if you use it to circumvent the restrictions of a Firewall regarding P2P to download perfectly legal software, if it's okay with your ISP or company or university or whatever.

### 4 What can be anonymous (HTTP, P2P?)

Tor is meant for anonymous web browsing, so HTTP/HTTPS will be redirected within the Tor "Onion Router" network. Other applications than your Internet browser can also be used with Tor; but only if they allow a Proxy configuration (meaning: they have to be able to redirect their communication via a remote (proxy) server). For instance, the Thunderbird mail client from the Mozilla foundation has a similar configuration than the browser Firefox, the settings can be taken over to let Thunderbird run over Tor.

**IMPORTANT NOTICE:** The connection from the Tor network exit node to the email server is NOT encrypted. This means, the Tor exit node has access to unencrypted email addresses and passwords! Email passwords and addresses had been accessed and published for demonstration purposes previously [Tormail]. When redirecting email access over Tor, make sure to use SSL to avoid cleartext being sent when using email. See also here: [SSLmail].

The P2P application uTorrent (see <http://utorrent.com>) has been tested with Tor as well, but has the tendency to fall back to direct Internet connection instead of using the Tor re-route, as I found experimenting with it, which is why uTorrent only allows anonymous P2P (Bittorrent) download, if a Firewall prohibits the direct (P2P) connection. All this is discussed below. However, the P2P Bittorrent client Azureus is designed to use Tor and it may show better results (not tried out in this paper).

**IMPORTANT NOTICE:** It is against the terms of use of Tor, to send the downloaded files itself (P2P data) through the Tor network, only tracker data of Bittorrent is meant to be directed through Tor. However, this does not achieve anonymous download. Note: for the tests of this document, only few data was redirected shortly through Tor. Redirecting large amounts of data is considered out of line, as private volunteers are using private resources to keep Tor running! Tor was used rather as a prototype of an anonymous data network, to see what anonymous communication, even with large data packages as in P2P traffic, might be able to do in the future.

## 5 Tor download

You can download a bundle of the Tor client software, the Vidalia Control Panel of Tor, the Privoxy local proxy (for communication with the Tor network) and a Firefox plugin for anonymous Internet browsing here: <http://vidalia-project.net/>. Choose the right platform. Well, if you have no clue what that might be, then choose Windows ☺. In this example I am using a Windows XP Service Pack 2 system with all updates. I know the screen shots look like Vista, that is because of a Windows “theme” called “Vistamizer”, but it has nothing to do with these tests.

## 6 Installation

Installation is straight-forward; just follow the instructions on the screen and install everything. When rebooting from now on, Privoxy (the application communicating with the Tor network), the Tor client on your machine and the Vidalia control panel for Tor will be automatically started with your computer. You can identify these applications on the right hand side of your task bar next to the clock of Windows. The blue P is representing Privoxy; just let it run – you can’t do much with it directly. The little green onion stands for the Vidalia control panel, double-click on it for monitoring what Tor does.

Note: You will need the Firefox Internet browser (I used Firefox 2.0.0.8) to run Tor as described herein. Will also run with Internet Explorer, but that is not recommended. During installation, the Vidalia setup will automatically change your browser settings. When you start Firefox, you will not a Tor status field showing in red “Tor disabled” or in green “Tor enabled” in the lower right hand side of your Firefox window. Clicking on it will change between these two states! Note the browser connection changes the Vidalia installer has done to your Firefox by clicking on Tools and then on Options in the drop down menu (of the Tool menu). Make sure the Network card is selected and click on “Settings: in the Connection field. If Tor is disabled (red notice in Firefox window as described before), a direct connection to Internet will be selected (x):

*Connection Settings**(x) Direct connection to the Internet**( ) Auto-detect proxy settings for this network**( ) Manual proxy configuration:**HTTP Proxy: localhost Port: 8118**( ) Use this proxy server for all protocols**SSL Proxy: localhost Port: 8118**FTP Proxy: Port:**Gopher Proxy: Port:**SOCKS Host: localhost Port: 9050**( ) Socks v4 (x) Socks v5**No Proxy for: localhost, 127.0.0.1*

...

This means, with Tor disabled, Firefox will attempt to connect directly to the Internet and ignores all proxy settings, which is fine for most LANs. But the proxy settings suitable for Tor are already configured. As soon as you click on “Tor disabled” in the Firefox window’s right lower corner, “Tor enabled” will be shown and Tor will start working. In this case, the “Manual proxy configuration” from above will be selected automatically and the proxy configuration shown above will be active. Note: you are not using one of the Tor Onion routers directly, but the local application Privoxy instead. That’s why your proxy is localhost (communication will take place via port 8118 for HTTP and SSL (HTTPS is HTTP and SSL) and port 9050 for Socks).

If you experience difficulties to connect to the Internet at any point of time using Tor or after disabling it, please read on in the next section; this is pretty normal at this point.

## 7 Handling

Handling is very easy. If Tor is enabled, you will have your usual Internet connection and the lower right side of the Firefox window will say “Tor disabled”. Just click on it to enable Tor and the text message will change to “Tor enabled” in green.

At first usage, Tor is usually not able to establish a connection because it needs to learn about the network first. Be patient and wait a few minutes. Double-click on the green onion symbol in the lower right corner of your Firefox window to open the Vidalia control panel. Click on “Message log” to get closer information. Here, you will be notified if Tor is still in the stage of learning about connection nodes and not able to communicate yet. You will also receive warning messages here, if the anonymity appears to be compromised. For instance, usage of the P2P application uTorrent in combination with Tor will lead to a complaint, uTorrent might use an external DNS server (to resolve clear names like [www.globalforeigner.com](http://www.globalforeigner.com) into IP addresses) [instead of the anonymous Tor DNS server]. The log entry then suggests using Socks4a instead of Socks4 or Socks5 (uTorrent lets you chose between Socks4 and 5, but cannot use Socks5). This complaint comes from the fact, that uTorrent simply passes an IP address to Tor and not the clear

name URL; however this is normal behavior for uTorrent. Anonymity restrictions will be reviewed in detail below in the “Tor and Bittorrent” section. Basically you can ignore this message.

One problem has been discovered in some networks:

Problem symptom:

When you had Tor enabled (“Tor enabled” is displayed in green in the lower right corner of the Firefox window) and then disable Tor by mouse click (which leads to the red notification “Tor disabled”), no Internet connection can be established anymore. Means: As soon as you switch off Tor, no Internet connection is possible.

Cause:

When being disabled, the Tor plugin switches the Internet connection way to “Direct connection with Internet”. This is not suitable for all networks, as some networks require the setting “Auto-detect proxy settings for this network”.

Solution:

Click on Tools->Options->Advanced and in the Connection section on “Setting” to change to auto detection of proxy to resolve this problem.

## 8 How Tor works (basics)

[Tor] is a good introduction. Basically, Tor is a network consisting of several routers, the so-called (Tor-) Onion Routers. Communication between these routers will be mixed (messages of equal length will be mixed among each other) and encrypted. No sender ID of any kind is available in clear text, which provides a great deal of un-traceability of the communication. A computer with a Tor client installed will send and receive data packages into resp. from the Tor network in encrypted form. The target of the communication (for instance a website) is not part of the Tor network and will consequently receive the data packages unencrypted from the Tor exit node of this communication line. A website will know the IP address of the Tor exit node which has given data packages to it, but does not know the originator of the communication. When sending requested data, the website will send it in clear text into the Tor network, which will then encrypt and mix it again and reroute it to the originator of the communication (the computer with the Tor client). The path through the Tor network is arbitrary.

Although Tor uses encryption internally, it has to be noted that Tor finally sends data to the target (website) without encryption. Tor can be viewed as a secure communication line, within the bounds of achievable security against attacks, which starts right with your network plug (inserted into your computer) und goes all the way until the last router of the Tor network. Between this router and the target computer (website), the communication is not encrypted.

It is best to use end-to-end encryption, such as SSL, HTTPS if you want a real encrypted connection.

If the Tor Onion routers  $R_1, \dots, R_n$  are being used, the Client will encrypt the Data package in the following way ( $K_i$  with  $i$  out of  $\{1, \dots, n\}$  is the encryption key for Router  $R_i$ ):

$$\text{Encrypted Data} = K_1(K_2(K_3(\dots K_{n-1}(K_n(\text{Data}))\dots)))$$

Where Data is the original clear text.

You can really see the various encryption shells around the clear text here; like the layers of an onion.

Tor basically follows David Chaum's mix concept [ChaumMix].

## 9 Attacks and anonymity restrictions

Most importantly Tor does not encrypt communication as to the destination. Only within the Tor network, the communication will be encrypted. The "last mile" to the destination computer is not encrypted. Encryption such as HTTP/SSL shall be used to ensure secure communication to the destination computer.

Tor exit nodes, being run by attackers, have been known to search for clear text email accounts and passwords in POP3 and IMAP protocols being relayed through Tor to read email! There are whole Tor nodes out there who only accept unencrypted email data, they explicitly reject SSL email communication. One can assume the aim of their users may be to intercept email accounts. Do not attempt to redirect your email access (POP3, IMAP) through Tor without using SSL! See [Tormail] for such an attack. Note: sending email via Tor (SMTP protocol) will not work, as it is blocked to prevent spamming. See [TorFraud]: a large number of recently occurring new Tor exit nodes is located in USA and China, the latter being located in metropolitan Beijing. Government activity is suspected, which would be consistent with other activity of these governments to intercept Internet activity. Especially China has been strongly suspected of government-conducted Internet espionage including attacks on business, administration and research servers all over the world.

Also note Tor's comment on the anonymity restriction by treacherous exit nodes: [TorAnonQ].

**Conclusion: sending any unencrypted account/password information through Tor may even be a greater risk than sending it unencrypted through the normal Internet!**

Also note, applications such as Java, Javascript, Macromedia Flash and Shockwave, QuickTime, RealAudio, ActiveX controls, and VBScript are known to be able to tunnel information directly to related servers and thus break through your attempted anonymity [TorAnonQ]. Disabling these in the browser is certainly a good idea.

Internet applications such as browser will talk to DNS servers out there. DNS-servers are machines on the Internet, which will translate user-typed URLs such as [www.teichert-online.de](http://www.teichert-online.de) into an IP address (which consists of numbers). If you are attempting to use such an application anonymously, the uncontrolled communication of this application to

any DNS server is certainly undermining your anonymity, as these DNS server requests are not using the Tor network, but might be sent via their own Proxy server. See [TorWiki] on that subject.

Also, people controlling a certain number of Tor nodes are able to influence the path which data through the Tor networks takes and thus are able to undermine anonymity and may even be able to identify the sender of the data. Somebody watching both your client communication into Tor (by controlling the first Tor node you talk to) and the exit node should be able to identify, which data packages are sent from YOUR side (see [TorLook]).

Summing it up:

Q: So when I send data through Tor, is it even less secure than sending it directly through normal Internet?

A: No. But do not send account/password/email information unencrypted through Tor, as treacherous Tor exit nodes may be waiting for such unencrypted information.

Still, it will be hard or next to impossible for even a treacherous exit node to trace back who had sent the data he is intercepting. However, if the data contains your email address or your real life address, this is easy! If you are just visiting a website and do not want anybody to know what you are viewing (like being worried someone may misunderstand you watching a terrorist-supporting website out of sheer curiosity), this is usually working. If you are going through a treacherous exit node, it is able to trace that you are watching the bad website, but it cannot figure out, who you are, as your data packages came through several Tor nodes mixed and encrypted.

However, if NSA and Chinese services one day control a lot of Tor nodes, they may be able to do even that in the near future (see [TorFraud]). Having no control who is opening a new Tor node, be it an anonymity enthusiast or the Chinese secret service, is certainly a problem here.

Right now, if you are not sending passwords/user names/real names/email addresses through Tor in an unencrypted fashion and take care of anonymity breaking applications on your system (Java, ActiveX etc. as mentioned above), Tor will provide a fair degree of anonymity.

## **10 Tor and Bittorrent**

### **10.1 why?**

See chapter “motivation” as to why one may want to have anonymous P2P download. My goal was not anonymous P2P, but simply any P2P download at all. I had to download a perfectly legal free application for my work via P2P, but the company’s firewall prevented P2P, only to stop music and video download. Well, so I had the idea of relaying the download via the Tor client, which encrypts it. It worked.

Later, I became interested to review how anonymous this communication may actually be, as statements on the Internet were not too clear about my combination of the uTorrent P2P client (for the Bittorrent network) in combination with Tor.

## **10.2 Tor abuse**

Tor is maintained by private people using their own bandwidth and money. That's why it is considered to be against the Tor terms of use to redirect P2P traffic through Tor! For Bittorrent, only the tracker data (connecting to a server telling your client from where to download) may be redirected through Tor. This does not provide anonymity against a peer being maintained by a private company trying to find out what you are downloading and what's your IP address of course.

In my test, I only downloaded a very limited amount of data through Tor and only used the redirection of the P2P payload itself through Tor very occasionally, in a kind of "pumping" through the firewall, which would occasionally choke my P2P traffic. This is described later. Do NOT send huge amounts of data through Tor! Do not send the P2P payload through Tor, unless for a few seconds to get the communication started.

## **10.3 Suitable clients**

I used the Bittorrent client "uTorrent" in version 1.7.5. However, it didn't really work out to allow anonymity at first. It broke through the firewall, but tried to fall back to normal (direct) communication avoiding Tor whenever the firewall would allow it. However, using a personal firewall such as the Sunbelt (Keiro) firewall to block uTorrent would solve that problem, see more about it in my techblog (goto <http://teichert-online.de>). The Azureus client is supposed to be better suited for Tor, it even has a Tor plugin.

## **10.4 Utorrent configuration / summary**

This part about the configuration of Utorrent has been omitted here as I have now an updated article about it in my techblog. Please visit my homepage <http://teichert-online.de> and click on the link to my techblog. I made several updates to this part in my blog, so I did not want to repeat it here.

Summary: Utorrent and Tor must be judged as a solution only suitable for Firewall or P2P restrictions penetration, NOT for anonymous download.

However, running Utorrent and Tor with the firewall mostly jamming normal P2P traffic, but allowing the Tor-redirectioned P2P traffic, established a "quite" anonymous P2P download. I don't call it really anonymous, as according to Tor, the network is still experimental and should not be used for strong anonymity purposes. Also, usage of DNS servers by Utorrent may reveal the real IP address to an attacker with means of intercepting this communication. It is thus rather a "very hard to trace" P2P download, but not yet one with strong anonymity.



## References

- [Wiki\_Rader] [http://en.wikipedia.org/wiki/Dennis\\_Rader](http://en.wikipedia.org/wiki/Dennis_Rader)  
[Slash\_BKA] <http://yro.slashdot.org/article.pl?sid=07/10/03/1243247>  
[JAP] [http://anon.inf.tu-dresden.de/index\\_en.html](http://anon.inf.tu-dresden.de/index_en.html)  
[Tormail] <http://arstechnica.com/news.ars/post/20070910-security-expert-used-tor-to-collect-government-e-mail-passwords.html>  
[SSLmail]: <http://cs.its.uiowa.edu/email/ssl.shtml>  
[Tor] <http://www.iusmentis.com/society/privacy/remailers/onionrouting/>  
[ChaumMix] [http://en.wikipedia.org/wiki/Chaum\\_mixes](http://en.wikipedia.org/wiki/Chaum_mixes)  
[TorFraud] <http://www.heise-security.co.uk/news/95778>  
[ChinaHacker1]  
[http://www.spacewar.com/reports/French\\_government\\_falls\\_pre\\_y\\_to\\_cyber-attacks\\_involving\\_China\\_999.html](http://www.spacewar.com/reports/French_government_falls_pre_y_to_cyber-attacks_involving_China_999.html)  
[ChinaHacker2] <http://www.timesonline.co.uk/tol/news/world/asia/article2388375.ece>  
[TorAnonQ]:  
<http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#head-5e18f8a8f98fa9e69ffac725e96f39641bec7ac1>  
[TorWiki] [http://en.wikipedia.org/wiki/Tor\\_\(anonymity\\_network\)#DNS\\_leaks](http://en.wikipedia.org/wiki/Tor_(anonymity_network)#DNS_leaks)  
[TorLook] <http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#head-a79d22244cc04ca5472832cbcc315198b875f34c>