Configuring the Tor network with TorK

WITHOUT A TRACE

HessenJense, photocase.com

If you're worried about eavesdroppers, connect to the Tor network with KDE's handy TorK configuration tool. **BY DANIEL GULTSCH**

The Internet is a very public place, and, whatever you use it for, you can expect that someone has an interest in watching your movements. Government agents and corporate competitors can easily monitor Internet activities.

More to the point for most users, vendors can tune in to your buying habits to scientifically determine how to sell you things. Some e-commerce sites might even vary the price of merchandise based on the region, Internet address, or past behavior of the shopper.

Tor Anonymity Network

Privacy advocates have developed several systems for users to operate anonymously on the web. One of the most popular options is the Tor anonymity network.

The Tor network [1] is a series of relays operated by volunteers that obscure the source of Internet traffic. The message bounces around inside the TOR network and emerges at an end node in a form that cannot be traced to its source.

In addition to supporting end-user tasks, such as web browsing, messaging, and email, the Tor network also provides the capacity for anonymous websites and even web forums.

Installing TorK

Despite all the benefits of the Tor network, one complication is that Tor support is often difficult to configure and use. Luckily, KDE users can use the handy TorK desktop application [2] to connect to the Tor network.

Few distributions include TorK packages. If you run openSUSE, you can use YaST to install Tor, the Privoxy web proxy, and TorK. Although Debian and Ubuntu include Tor and Privoxy, TorK might either be in *Unstable*, or available if you have release 8.04 or later.

When installing from the source code, watch out for the dependencies, which include the KDE and Qt developer packages. Apart from any dependency issues, the installation follows standard procedure. After downloading the tarball from the project website [1], unpack the ar-

How Tor Works

Tor routes encrypted traffic through a series of three servers (*nodes*). The sender wraps up three encrypted packets. The individual nodes each remove one layer of encryption and send the packet to the next node. The third node hands the fully decrypted packet over to the target. This onion skin principle gave Tor its name: The Onion Router.

The first two nodes do not know the packet's target or content. Only the last node has this information; however, the last node does not know where the packet came from.

To trace a connection, an observer would need to control all three nodes. But this is difficult to achieve, even for the authorities, if the three nodes happen to reside in different countries. When you use Tor, make sure the nodes are not all in the same country – and especially not the country where you are right now.

chive and change to the directory this step created. When you get there, build and install TorK using the standard three-command trick.

The *INSTALL* file has a detailed list of dependencies. If you want to use Remailer via TorK (see the box titled "Type III Remailers") to send anonymous email, you will also need to set up Mixminion [5]. Despite the very low version number, and its alpha status, at least the remailer client didn't appear to be too buggy. The tarball includes a *setup.py* script; start by adding execute permissions *chmod +x setup.py* and then enter *./setup.py make* to launch. When you are done, type *./setup.py install* to copy the files to the right places.

Configuring TorK

When you first launch Tork, you'll see a configuration dialog. The program will ask if you would like to connect to a local or remote Tor installation: Select *localhost*. TorK will then check to see whether the Tor daemon is running in the background. You'll need to enter the path to the Tor daemon configuration file – on Debian, Ubuntu, and (open)SUSE, this is */etc/tor/torc*.

When you click on *Modify Tor's Control File* you are prompted for the root password. Clicking *Test Tor* checks to see whether TorK is able to modify the file. If so, clicking *Next* takes you to the proxy selection dialog, where you will want to select Privoxy. Like the Tor daemon, Privoxy runs in the background on most distributions. After completing the Privoxy configuration, disable other proxies in your browser configuration.

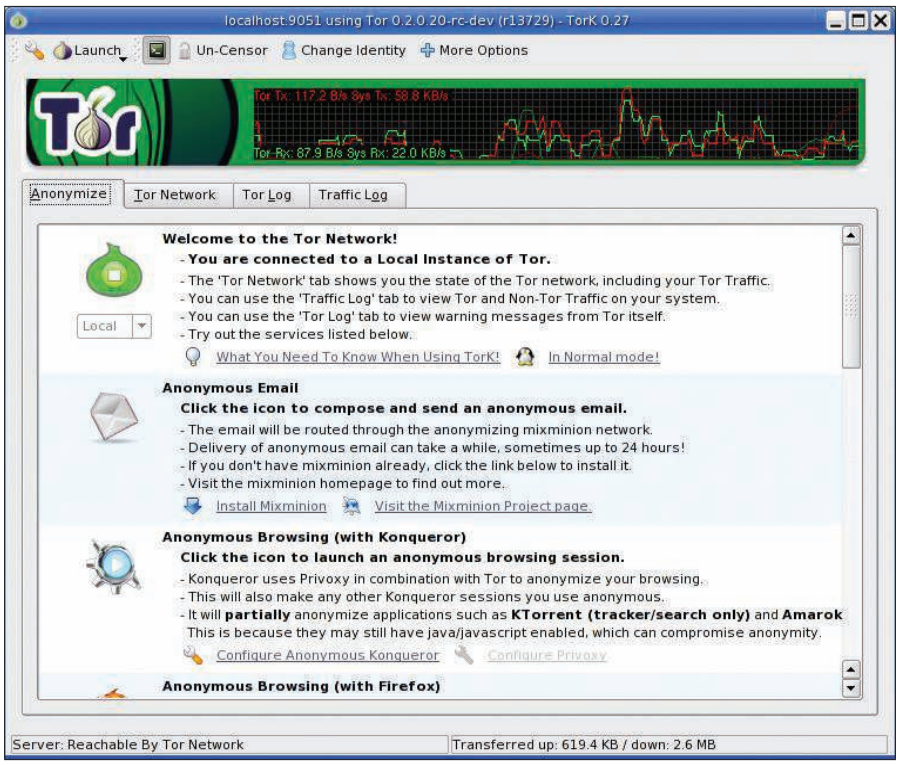

Figure 1: Click on the green onion icon to launch Tor.

Using TorK

The TorK user interface has four tabs. In the *Anonymize* tab, launch Tor by clicking on the green onion icon (Figure 1). If you use Firefox, launch the browser by clicking its icon: Firefox will now route connections via Tor. The first time you launch Firefox, it copies its settings to a new profile and reconfigures the profile to use Tor. This makes it possible to run Firefox and Tor separately; the settings and bookmarks cannot be exchanged.

If you prefer to surf the web with Konqueror, click on the icon for the KDE browser to route all future connections via Tor. By clicking the icon or closing TorK, you revert to normal use.

Incognito

The Incognito [3] Live CD, which is not part of the TorK project itself, conveniently launches TorK on any computer, including a computer in an Internet café. The easiest approach to getting TorK up and running is to use the Incognito Live CD. The 350MB ISO image [3] is only available for the x86 CPU architecture right now. Hardware detection worked fine in our lab.

On booting, Incognito gives you the option of changing the MAC address (Figure 2). If possible, you should accept this offer because it adds another layer of anonymity for your hardware. Changing the MAC address could cause problems on some networks, especially if a DHCP server is used to assign IP addresses on the basis of MAC addresses.

If you can't access the Internet after starting the Live CD, boot again – without changing the MAC address this time. In our lab, a bug bit the Live CD on some systems: Although X server would launch, it would not display. In this case, press Ctrl+Alt+F7 to toggle the screen or enter *chvt 7* at the prompt.

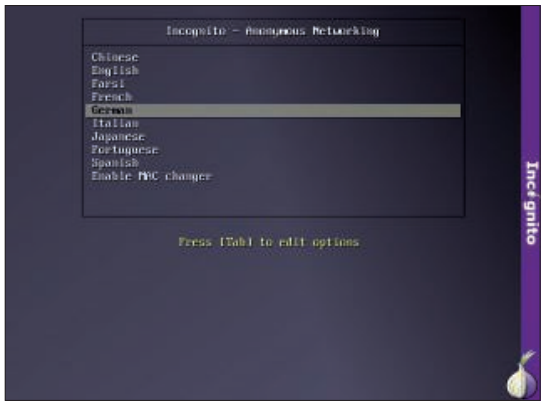

Figure 2: Experiment with accepting Incognito's offer to modify the MAC address.

When you shut down the system, Incognito ejects the Live CD and then proceeds to overwrite the RAM content, which contains a complete image of the operating system, including the websites you accessed. Theoretically, an attacker might be able to recover this data. In fact, recent research reveals that the RAM chips could be frozen with ice spray after powering off, giving a forensics expert the ability to reconstruct the data some time later [4]. If you are not worried about this, you can just switch off your PC as soon as the Incognito CD is ejected.

Also, you can launch the Pidgin instant messaging program and the Ksirc IRC client by clicking the corresponding icons. Anonymous use of the Jabber, ICQ, and MSN protocols worked in our lab, although chatting on IRC didn't always work because many IRC servers block the Tor network.

If you have installed the Mixminion anomymous mailer, you can click the mail icon to send anonymous email messages. Mixminion is very security conscious and requires you to change the permissions for both the *.mixminion* folder and the *.mixminionrc* file to avoid third parties reading them. If necessary, type *chmod 700 .mixminion* and *chmod 600 .mixminionrc* to set the permissions after the first launch.

After taking this hurdle, using Mixminion is simple: Write the email normally and send it – Mixminion automatically picks up a list of servers and sends your message.

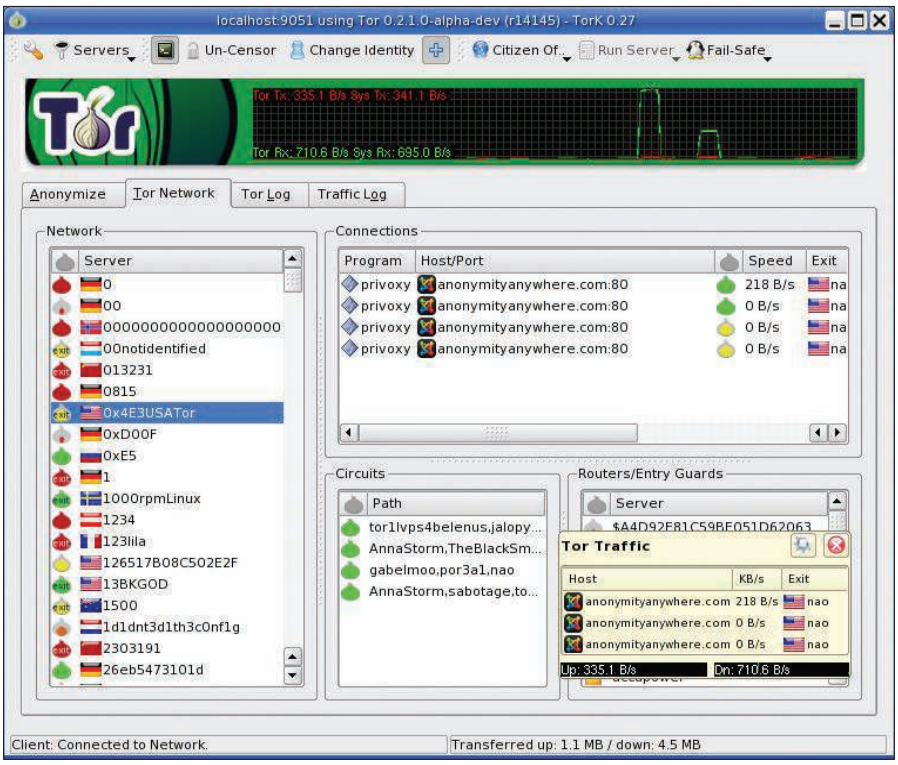

Figure 3: The Tor Network tab lets you monitor and influence active connections.

Door to Tor

Normally, Tor will select nodes itself, but if you want to influence the selection, the *Tor Network* tab lets you do so (Figure 3). The left-hand column shows you a list of all available nodes. To filter the nodes, you can use the *Servers* menu in the TorK toolbar – filter options include *Fast* and *Stable*.

The Connections section of the window takes you to a list of current connections running via Tor. TorK shows you the chain of three nodes used for each connection.

The exit node, whose IP address the recipient gets to see, is marked by the flag for its country of residence. If you want the exit node to be in a specific country, you can choose *Citizen Of...* in the toolbar. However, Tor servers are not available in all countries.

If you prefer, you can select all three nodes, rather than just the exit node. To do so, drag and drop the nodes into the Circuits window. It typically takes a couple of seconds for Tor to establish a connection to the node, and for the node to appear in the list. Also note that the third node in your chain must be an exit node; that is, it must display the word "Exit" in its Tor icon.

By default, Tor will automatically choose a chain of available nodes for each connection. If you want to specify a chain for each connection, right-click the *Connections* field and select *Let me Drag Connections to Circuits myself*. Tor will wait until you have manually dragged and dropped three nodes to set up a working chain. By right-clicking and selecting *Attach Connections to Circuits automatically*, you reset this behavior.

The *Tor Log* tab takes you to error messages and warnings. The *Traffic Log* tab stores the outgoing Tor connections for the current session and, as a cross-reference, the connections that did not use Tor.

Conclusions

Although Tor encrypts the traffic between individual nodes, the connection from the exit node to the target is unencrypted. An observer at the exit node can therefore read all your passwords if they cross the wire in cleartext. If possible, you should use an encrypted protocol such as SSL/TLS. ■

Type III Remailers

If you want to send anonymous email, you could use Tor to set up an email account with a free mail provider; but this seems slightly over the top if you will only use the service occasionally. As an alternative, you can go for a remailer. Remailers come in all shapes and sizes. The most simple type is a server that deletes the sender data from the original mail header before forwarding the message (type I).

A type III remailer splits the message into several chunks, encrypts each chunk, and sends the encrypted chunks to the target over several hops. Fragmenting the message makes it difficult to reconstruct the length of the message; however, the message can take up to 24 hours to reach its target. Thus far, only one software implementation of a type III remailer exists: Mixminion [5].

File Sharing

The idea of sharing files via Tor might sound intriguing, and the Live CD does include KTorrent, but file sharing is not what Tor is about. Because of low data transfer speeds, file sharing doesn't make much sense.

INFO

[1] The Tor network: *http://www.torproject.org/*

[2] TorK: *http://tork.sf.net*

[3] Incognito: *http://www.anonymityanywhere.com*

[4] "Cold Boot Attacks on Encryption Keys": *http://citp.princeton.edu/memory/*

[5] Mixminion: *http://mixminion.net*