

TOX: ENCRYPTED P2P COMMUNICATIONS

The post-Snowdon era of justified paranoia is upon us, and it's brought its own software.

WHY DO THIS?

- Keep your private conversations safe from unwanted eavesdropping.
- Migrate your social and work contacts away from proprietary communication networks.
- Blow the whistle on illegal government activities without fear of governments intercepting the messages.

Since Edward Snowden revealed to the world the extent of government surveillance on the internet, there has been a drive to create more secure channels to let people communicate in private. Tox is an encrypted peer-to-peer chat system (with audio and video capabilities) that doesn't send your data through central servers where it could be tapped.

The lack of a central server also means that there's no company running it for a profit that could hold your data to ransom or spy on messages to target adverts

at you. It's a communications system by the people for the people.

At the moment, it's still a little rough around the edges, but it is working, and it's getting better quickly. Here at Linux Voice, we're early adopters, especially when it comes to software that encourages freedom – in every sense of the word – so we've been trying it out. We don't have an awful lot to hide, but that's not the point. Here's our six-step guide to keeping your private chats private using the *uTox* client.

Step by step: Setting up a Tox client

1 Get the software

In order to chat using the Tox network, you'll need to install some software to access it. As it's quite new, not many Linux distributions include anything useful in their repositories, so you'll need to install it manually. Tox is the protocol, and there are a few applications that can access it. There's a list of Tox clients at <https://wiki.tox.im/Binaries>. We'll use *uTox* for this tutorial, but feel free to experiment with others. They all work in roughly the same way, so you should find it easy to switch. At the moment, most clients are in quite active development, so if you find it useful, it's worth keeping an eye out to see what's useful in a few months.

To get the software, just click on the link for 32- or 64-bit to start the download (the same build should work on most distros). *uTox* is also available for Windows, so most of this tutorial can be applied to that OS as well.

The Tox wiki is also a great place to find out what's going on in the Tox world; another useful resource is the Tox subreddit at www.reddit.com/r/projecttox.

2 Installing the software

uTox comes as a **tar.xz** file. To unzip this, you'll first need to install **unxz** with your package manager. This usually comes in a package called **xz**. Once you've got it, you can extract the archive with:

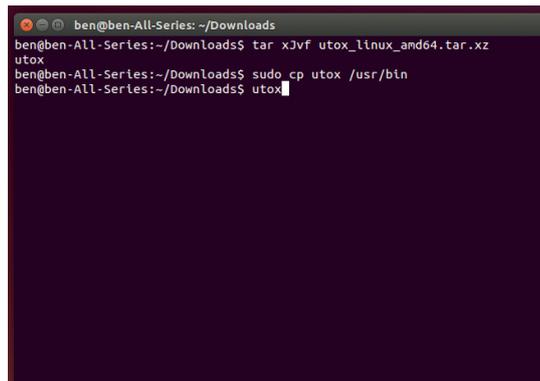
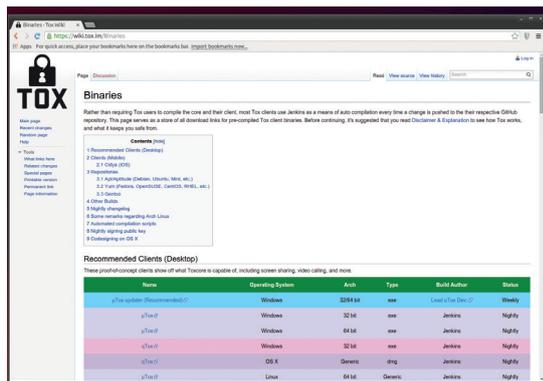
```
tar xJvf utox_linux_amd64.tar.xz
```

The **J** option signifies the **xz** compression. You may need to change the filename depending on which version you downloaded.

This should extract a single file called **utox**. It should be executable, so you can run it by entering **./utox** at the command line. However, this will only work if you're in the directory in which you decompressed the file. To make the program accessible no matter what directory you're in, like the rest of the software on your machine, you need to copy it into the appropriate directory – this is usually **/usr/bin**. To do this, enter the following in a terminal:

```
sudo cp utox /usr/bin/
```

Once this is done, you can run the software by entering **utox** (without the **./**) at the command line from anywhere.

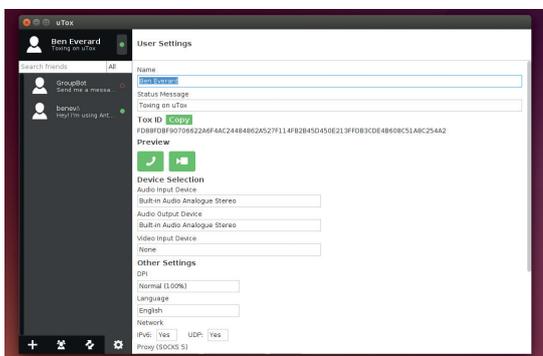


3 Creating your profile

When you first start *uTox*, it will create a new ID for you. Tox IDs are long strings of upper case letters and numbers. They're cryptographically sound, but not very nice to look at. Fortunately, you don't have to use these IDs for much, and can give yourself a name and status message. It's this name and status message that your friends will see in their lists rather than the cryptic Tox ID.

Tox IDs are cryptographic keys that you use to communicate with the other people on the Tox network. There's no central server that stores or records information, and this means that the Tox network is a little different from some other popular chat networks.

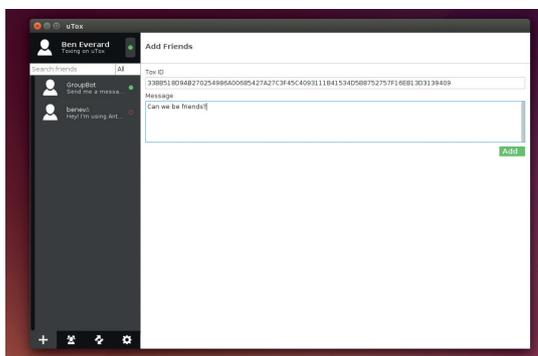
The IDs are saved in the file `~/.config/tox/tox_save`. Since there's no central server, there's no place to restore this file from, so keep it safe.



4 Adding friends

Chat networks are all about the contacts you have. Tox works on a friend-request basis. That means that if you want to communicate with someone, you first have to send them a friend request. To do this, click on the + icon in the bottom-left of *uTox*, and enter their Tox ID. You can also send them a message to let them know who you are and why you want to contact them.

If they accept your friend request, they'll be added to the friend list on the left-hand side. When they're online, a little green circle will appear by their name. You can only chat with people when they're online. This is also because there's no central server. Without a central place to store undelivered messages, there's no way to send anything to people unless they're online. By the time you read this, it may be possible to have avatars, so your friends will have different pictures displayed next to their names.

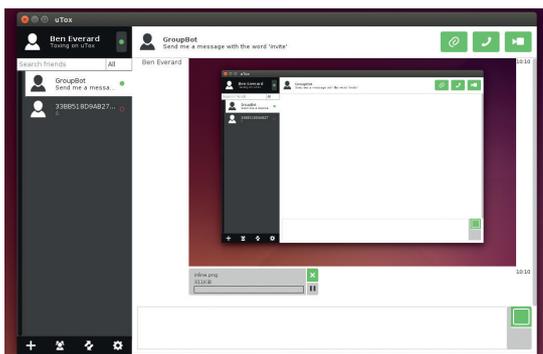


5 Extra features

Sending text between two people may have been considered sufficient for online chat software in the 90s, but now users expect a lot more. As Tox is still considered alpha quality, there is quite a bit of change in the features, and you can expect more to be released soon. However, even now there are a few features ready to use.

In the top-right corner, you should see three green icons: a paperclip, a telephone and a video camera. Unsurprisingly, these are for attaching files, making voice calls and making video calls. The odd-looking square in the bottom-right is for sending screenshots. Clicking on it will give you a cross-shaped pointer to outline the rectangle that you want to send.

Audio and video group calls are planned features for later releases, but not yet implemented.



6 Getting mobile

It's 2014, and it's no longer acceptable to have a chat platform that's not mobile. Fortunately, Tox is available for Android. You can get an APK file of the *Antox* client from the website in step 1 (it's not yet in the Play store). This can be installed on any Android device with side-loading enabled.

It's not possible to share a single Tox ID between *uTox* on your desktop and *Antox* on your mobile, and it's not clear whether it ever will be. As a general rule, you should have a separate Tox ID for each device otherwise you may end up with messages only going to one of the logged-in devices. 📱

