Getting your hands started with Tails

mathieu.goessens@univ-rennes1.fr contact@julielallouetgeffroy.com

http://mathieu.goessens.fr/formation

Introduction

According to its web page, https://tails.boum.org,

«Tails is a live operating system that you can start on almost any computer from a USB stick or a DVD.

It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship; all connections to the Internet are forced to go through the Tor network;
- leave no trace on the computer you are using unless you ask it explicitly;
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.»

You can read a bit more about Tails (and Tor) in the about section of the website: https://tails.boum.org/about.

This document aims to be a step-by-step tutorial which you can follow to have a quick overview of Tails, understand how it works and how it could fit your needs.

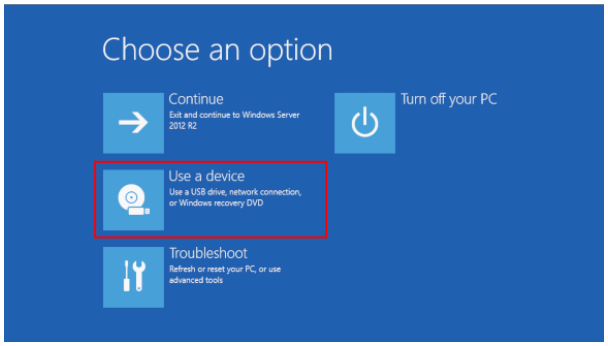
Getting started

Starting Tails

Tails is designed to run independently of your main operating system (Windows, Mac OS X. . .), in order to provide its amnesic feature and isolate what you will do with it. Thus, to start Tails, you need to shut down the computer and ask it to restart on the USB stick, instead of letting it boot to your daily operating system.

If you are on Windows,

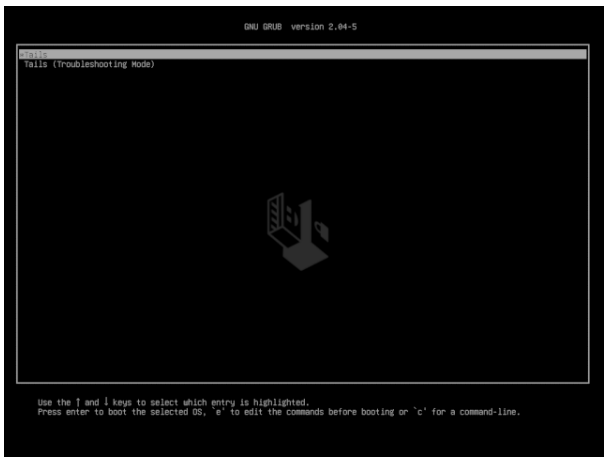
- If the computer is on, you can use, *Start* > *Power* > *Restart* **and** press the *Shift* key, when you choose restart. It should propose you a menu, where you can select to reboot on a USB Device:



If you dont have the option, or if the computer is off, you can :

- Shutdown the computer. Be sure to press the *«Shift»* key while selecting shutdown option in the start menu, or simply select the Reboot option. It will prevent the computer to boot using the *«fast boot»* or *«fast startup»* mode which would unfortunately skip USB stick detection otherwise[1].
- Then either your computer will automatically boot on the USB stick, either you may have told it to do, by pressing a specific key which may depend of your computer. To do so, follow the instructions in the Tails installation web page https://tails.boum.org/install/win/usb/#start-tails.

You should see a screen like this one (or similar, there are two versions):



If you are on Mac,

- Shutdown the computer.
- Press the *«Alt»* or *«Option»* key when the system starts (and usually emit a sound):

[1] Can be deactivated permanently either in the BIOS or in Windows settings (See https://answers.microsoft.com/en-us/windows/forum/windows8_1-performance/fast-startup-how-to-disable-if-its-causing/f9a4a2d0-104d-42dc-9946-4a2e13c0a348).

You should see a screen like this one, where you can select the USB Key instead of your hard drive (no need to set up WiFi as proposed):

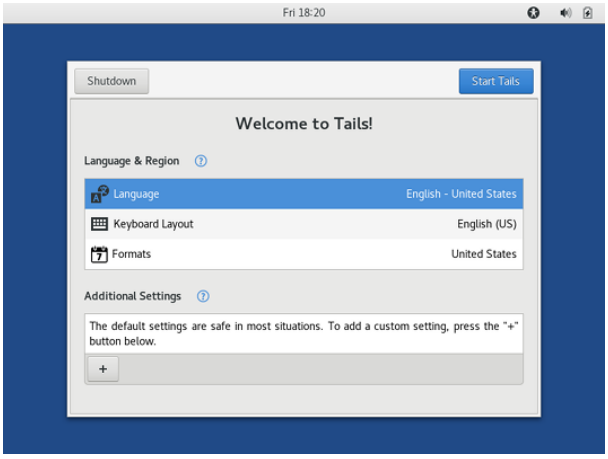
And then you should see the same boot menu as Windows.

If you see message such as “Security settings do not allow this Mac to use an external startup disk”, you will have to follow a procedure to allow your mac to boot Tails: https://tails.boum.org/install/mac/usb/#startup-security.

In both cases, the Tails should start to boot, sometimes it will print some text messages you can safely ignore, then, after a few minutes, you should see the Tails welcome screen.

Welcome screen

The Tails welcome screen allows you to select various startup options, as explained in the documentation: https://tails.boum.org/doc/first_steps/startup_options/.

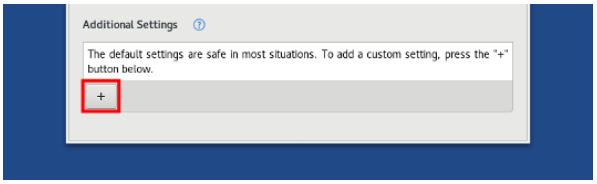


- You can start by changing your language.
- You will notice that the keyboard and format (used for dates, numbers etc) options change accordingly.
- **If you are using a specific date/number format, or a specific keyboard such as the Mac ones, you may need to change the setting accordingly** as some keys such as «@» are in different places than on PC.

In some specific situations, you may also need to perform a few changes in the *additional settings*. By default Tails also starts with the following *additional settings* set:

- No admin password is setup. This is a security measure. It prevents you from doing advanced things that are usually not required and may reduce the security and isolation provided by Tails (such as installing new software or accessing your hard drive and thus possibly leaving traces that you have been using Tails)[2].
- The connection to the Tor Network is done directly, which should work fine if the network is not filtered and may need to be changed otherwise[3]. Please remind that in any case, Tails is not designed to hide the fact that you are using Tor, **your ISP will almost always see you are using Tor**[4].
- In order to try to hide the fact **you** specifically are using Tor, Tails change the Ethernet or Mac address[5] or your computer network card. This may cause problems with some hardware (see below) or may be necessary to change if you are **connecting from a company or university network** (as some of them do not allow computers they do not know to access the Internet).
- The **Unsafe Browser**, that allows to connect to captive portals is deactivated to prevent advanced attacks, **for this workshop, we ask you to enable it**.

You can change those options, **including the unsafe browser one**, in the bottom of the welcome screen:

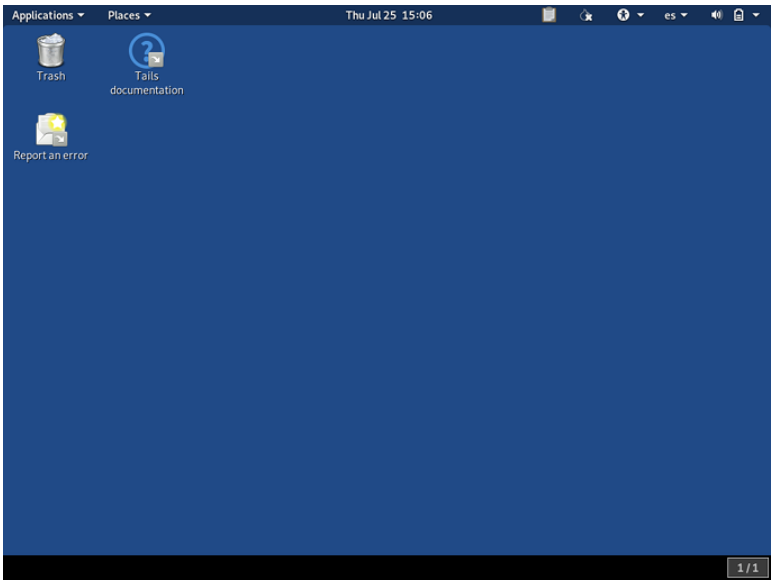


You can start Tails by selecting the start Tails button on the right top of the welcome screen. After a few 15 or 30 seconds, you should see the Tails desktop.

First hands with Tails: desktop & apps

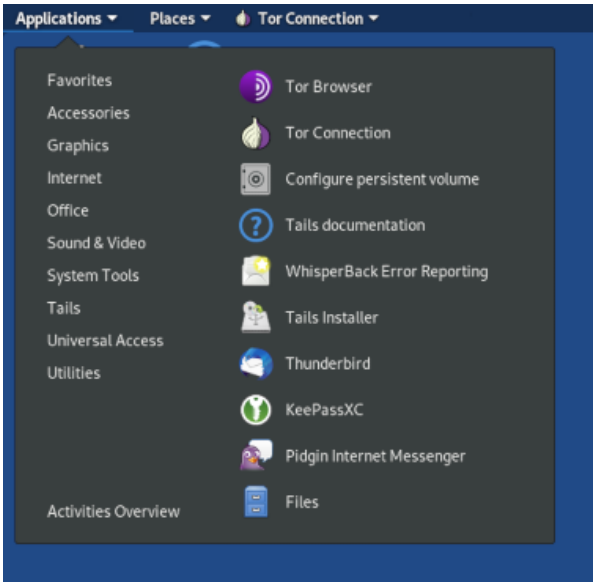
You should now see the Tails desktop which looks like this:

[2] See https://tails.boum.org/doc/first_steps/startup_options/administration_password.
[3] See https://tails.boum.org/doc/first_steps/startup_options/bridge_mode.
[4] See https://tails.boum.org/doc/about/warning/#fingerprint.
[5] See https://tails.boum.org/doc/first_steps/startup_options/mac_spoofing.



Take a bit of time to discover it:

In the top-left, you have the application menu.



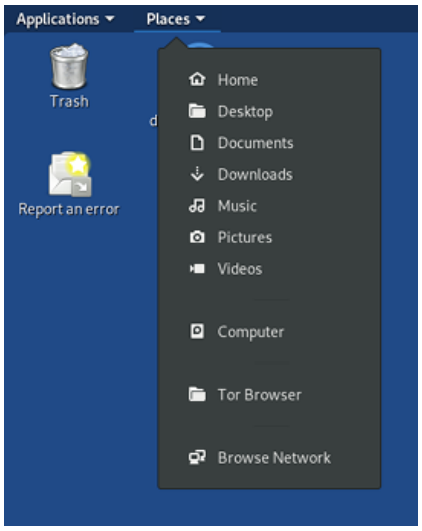
You will see here that Tails already includes numerous applications, for example:

- A few quickly accessible applications in the *«Favorites»* Menu. Including the *KeepassXC* password manager and some other tools that we will discover latter.
- In the *«Internet»* part, you have the *Tor Browser*, which allows you to browse the web anonymously but also the *Thunderbird* mail client that allows you to see your mail with an app (similar to *Microsoft Outlook* or *Apple iMail*), a chat application (*pidgin*), *Onionshare* that allows you to share files anonymously inside the Tor Network (we will use it later) and so on.
- In the *«Office»* part, you will see that Tails includes *LibreOffice* (formerly known as *OpenOffice*), allowing you to work on office documents.
- In the *«Multimedia»* part, you can find *audacity* - a simple audio editor, but also tools to burn CDs & DVDs, a simple vectorial drawing tool (*Inkscape*), a picture editing software similar to

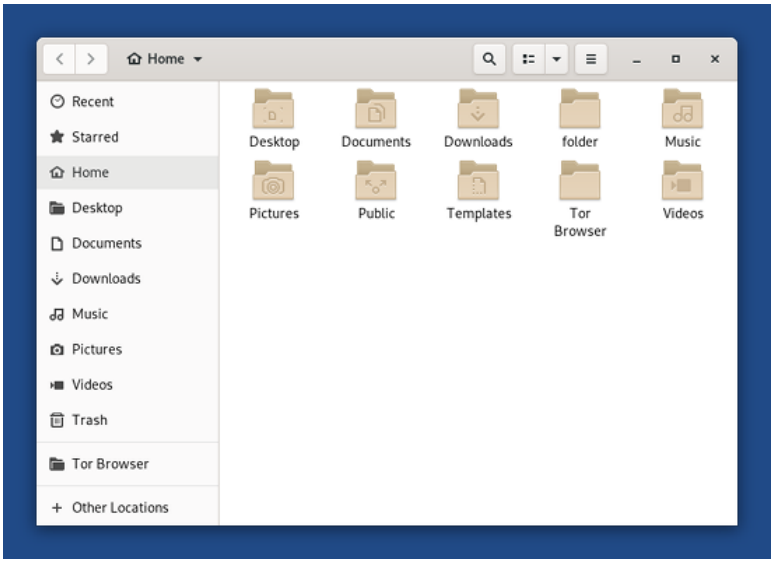
photoshop (*Gimp*) etc.

Tails is designed to provide a sufficient set of applications[6] that should cover much of your use cases, allowing you to do almost all your work within Tails, enhancing its isolation purpose. If needed, it is also possible to install other applications (if they are supported by Linux and properly integrated)[7].

You can also use the Places menu:



It will launch the file manager:

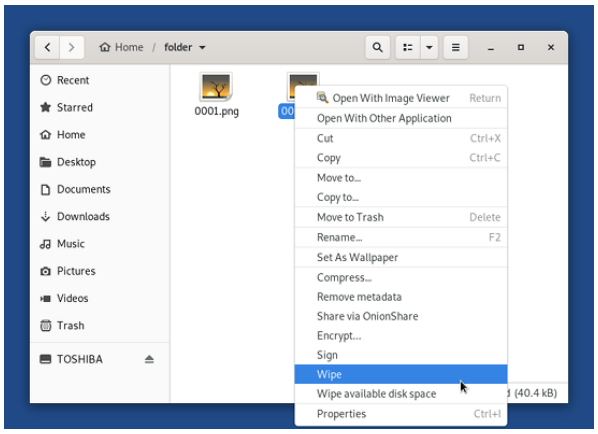


You will see that a few directories are created automatically to store your pictures etc. Please note that **all content stored here will be lost after reboot** as Tails will never save files if you don't explicitly ask for it[8] in order to leave no trace by default. We will see latter how you can save documents.

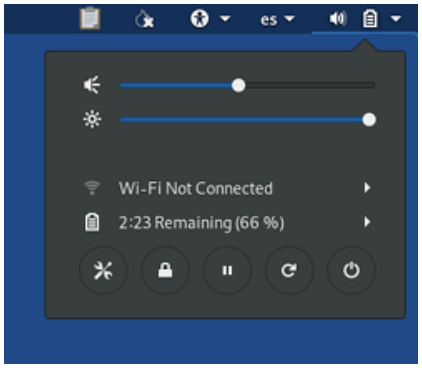
If you right-click (on a mac, click with the two fingers) on a directory or a document, you will find some classic options such as copy, new directory etc. You will also find advanced options that allow

[6] See https://tails.boum.org/doc/about/features/.
[7] See https://tails.boum.org/doc/first_steps/additional_software/
[8] See https://tails.boum.org/doc/encryption_and_privacy/your_data_wont_be_saved_unless_explicitly_asked/.

you to remove metadata[9], securely erase a document, encrypt it, or share with Onionshare. **This is an important feature of Tails: to have state-of-the-art cryptographic tools (and so on) included and easily accessible**.



On the top right corner of the screen, you will find the system menu:



You can use it to access the configuration panel, reboot, change screen brightness or sound level, or connect to a network.

Browse the Internet anonymously using the Tor Browser

Use the top right menu to connect to your WiFi Network. Once connected it may take a few seconds or minutes for Tor to setup. You may notice that the time changed, as Tails setup Time in Universal Time Zone (UTC+0), so all users are on the same Time Zone (it helps to hide their countries).

You can now browse the web using the Tor browser. You can go to classical newspapers websites such as:

- https://lemonde.fr
- https://liberation.fr
- https://lefigaro.fr

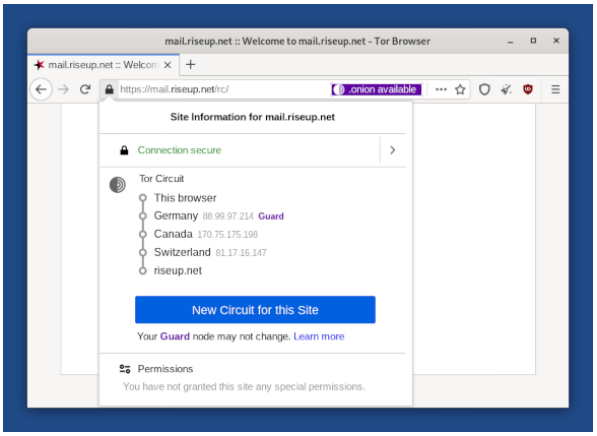
And so on.

In some websites, you may notice some text in different languages than usual. This is normal, as the Tor Browser hide your real location (IP), some websites are displaying content according to where they think

[9]Only on documents. You can try to create one (With *LibreOffice* for example) or wait a bit. We will play with that later.

you are located. For this reason, **avoid connecting to your Gmail or Facebook account**, as the fact you are connecting from different countries may be detected as a hacking tentative and **get your account blocked**, forcing you to follow recovery procedures (such as sending identity confirmation).

If you click on the top left of the address bar, you can see where your traffic goes through.



(If you don't see it, sorry, it's a bug [10], simply restarting the Tor Browser should fix it)

Try to do that for every website you have opened, you will notice for every website/tab, you are using a different path, and a different location. The first node stays the same for all along the session for security reasons[11]. You can also change the path used to connect to a given website using the *«New circuit for this site»* button. That way, a given website is unable to see that **you** are browsing it, which can be useful if you want to browse it to look for documents without revealing that **you** or your news agency is actually browsing it.

You can also connect to specific websites that are only accessible through Tor (the so-called darkweb), you can find a list here: https://huit.re/DotOnion2. Notice the URLs end with *.onion* instead of *.net*,*.org* etc (the URL's may look weird because they are in fact cryptographic identifiers).

Try to connect to a few of those websites. You may notice that there is nothing illegal here, just classical new websites that offer a direct access through Tor to increase their users security, or whistleblowing platforms (even Facebook offers a direct access to Tor users !).

If you check where you traffic goes through, you will notice that those websites use 6 hops to connect (instead of 3) and the real location of the website is hidden. That is one of the reasons Tor is widely used for whisterblowing platforms: it allows to improve user and plateform security is the same time by making both untracable [12].

Please note that Tails includes some additional security measures around the Tor Browser: it can only read and write files stored in the Tor Browser directory (and on its persistent version that we will configure latter). This is a security measure: in case the Tor Browser is compromised, it will only have access to the files stored in this directory.

Connect in public WiFi using the unsafe browser

In some specific places, such as train stations, airports, schools (*«eduspot»*), you have to open a specific web page before being able to connect to the Internet. This causes an issue with Tails as all traffic is

[10] https://redmine.tails.boum.org/code/issues/16993

[11] See https://2019.www.torproject.org/docs/faq.html#EntryGuards.

[12] It also provide nice security properties, such as build-in encryption similar to HTTPS. See https://tb-manual.torproject.org/onion-services/, https://support.torproject.org/onionservices/.

forced through the Tor network: You cannot connect to the Internet until you validate on this page, but you can not display this page as you can not connect !

For this reason there is a so-called *unsafe browser* available in Tails. It allows you to display the page you have to validate before connecting to the Internet. You can find it in *«Internet > Unsafe Browser»*, try to launch it if you like. You will notice that you will have to confirm a few times and that even the graphic and the welcome page of the Browser display warning messages informing you this browser is not anonymous and should just be used to initiate the Tor connection, and **switch back to the Tor Browser after**.

If you see an error while trying to launch it, it is because you forgot to enable it in the welcome screen. As this browser could lead users to be more exposed to attacks, or just do mistakes, it is disabled by default. There is no need to reboot, to redo the whole process, just look your colleagues screen, or skip this part, you can try it a next time.

This is also an important feature of Tails: to make it clear to users when they are doing that may reduce the protection offered by Tails.

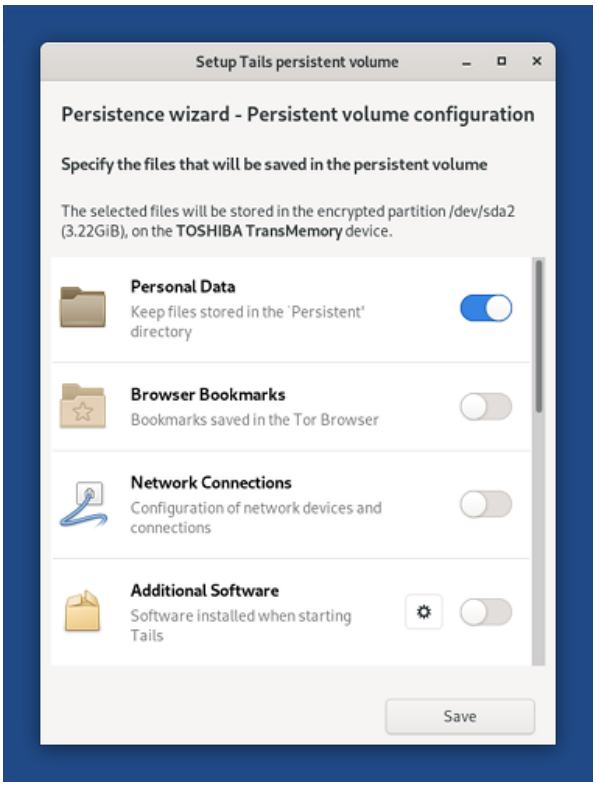
Please also note that **it is not recommended to run the *unsafe browser* and the *Tor browser* in the same time**, to prevent you to «mistake one browser for the other, which could have catastrophic consequences»[13].

Store data securely using the persistence

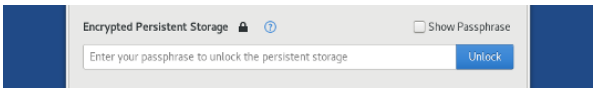
As we explained before, by default Tails is Amnesic: it leaves no trace on the computer that Tails have been used and won't save files if you don't **explicitly** ask for it. We will now see how it works.

The feature allowing you to keep files in Tails is called *«persistence»*. You can read a bit more about it in the Documentation: https://tails.boum.org/doc/first_steps/persistence/. Persistence will store data in the same USB stick as the system (the system uses 4 to 8GB). You can configure the persistence using *«Applications > Tails > Configure the persistent storage»*. There will be four steps:

[13] See https://tails.boum.org/doc/anonymous_internet/unsafe_browser/.



- In the first step you are asked to choose a passphrase that will be used to secure your data, using disk encryption. Without this passphrase or password your data will be unreadable. Generally speaking you should use a strong passphrase here, but for the sake of this workshop, better to choose a simple one, to be sure you will remind it in the next steps (experience...). You can create your own persistence with your own strong passphrase later.
- In the second step you are asked what kind of data you will want to store. By default only one option is selected: the «*Persistent*» Directory. It allows you to store directory than you put inside the *«Persistent»* Directory, thus **you have to explicitly move files inside that directory for them to be saved** across reboots. There are also other kinds of data which can be stored, you can find a list and the description in the according page of the documentation https://tails.boum.org/doc/first_steps/persistence/configure/, you may for example want to store your WiFi password to not need to retype it every time, or Thunderbird/Pidgin/PGP configuration if you are using them.
- In the last step, you are asked to **reboot the system as persistence will only be available after a reboot**. You can do it using the system menu in the top right, and following again the procedure you used to start tails.
- Once you have rebooted, you will find a new field in the welcome screen allowing to open your encrypted storage. Please note that you don't need to open it every time, using persistence when you **need** it is part of the recommendations around its use: https://tails.boum.org/doc/first_steps/persistence/warnings/



There is also a second way to store documents using Tails, simply storing them in another USB Stick. Thus if you plug back the USB stick on your computer you will clearly figure that you have been exchanging documents between Tails and another system, reducing the protection offered by Tails. If

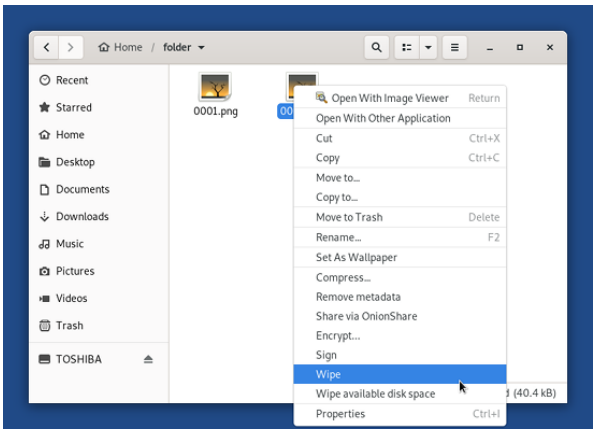
you are using it, you may be interested by two features offered by Tails: ability to securely remove files, and the ability to create or work on encrypted storage medias.

Securely remove & store files with Tails

If you are using an external drive such as a USB stick with Tails, you may be interested by the feature allowing to securely remove files from it.

Generally speaking, when you are removing a file with an Operating System, the file itself is not really removed. What is removed is the index at the beginning of the drive saying where which file is stored. That's why if you copy a 10GB file it takes minutes but is almost instaneously removed. In order to prevent people from recovering files that are removed, Tails include a feature allowing to securely remove it. Not only does it remove the file from the index, but also rewrite zeros or random data in place of the former content. You can read a bit more about it in the Tails documentation: https://tails.boum.org/doc/encryption_and_privacy/secure_deletion/

If you would like to securely remove a file/directory with Tails, you can simply right on it (on Mac, use the two fingers) and select the *«Wipe»* Option. It will be a bit longer, because the content of the file will be rewritten.



You can also wipe all the available space (if you forgot to remove a file securely). Be aware however, that for USB sticks and SSD drive, the only way to securely remove a file is to reformat it entirely. You can do it in the *«Disks»* Utility that you can launch using *«Application>System>Disks»*. Once launch simply select your drive, choose the option to format it in the menu, and in the Format Disk dialog:

- Choose to **Overwrite existing data with zeroes** in the Erase drop-down list.
- Choose **Compatible with all systems and devices (MBR/DOS)** in the Partitioning drop-down list.

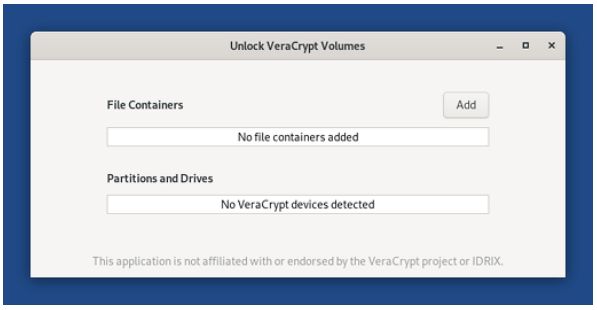
If you are looking for a similar Tool for Windows, you can use Eraser https://eraser.heidi.ie/. On Mac, you can do the same using a command line tool: https://ssd.eff.org/module/how-delete-your-data-securely-macos. You can also format the whole drive (which is better if it is a USB stick or SSD) just like on Tails, and ensuring it will do a long format.

Using the same *«Disks»* utility, you can also select the Option to format a drive only for Linux in an encrypted way. Allowing you for example to use Tails to handle your backups in a secure way. However, your backups will be only readable with Tails or other Linux such as Ubuntu. If you want to securely exchange or store files for multiple operating systems you may be more interested by the Veracrypt Integration, allowing you to open veracrypt volumes in Tails.

Exchange data securely with other systems with Veracrypt

Veracrypt https://veracrypt.fr is a disk encryption solution, allowing you to create encrypted drives or containers (and on Windows, to fully encrypt your drive). If you are using it, you may be interested to know that Tails allows to Open those Volumes and Containers (but not create them actually).

You can do it using the *«Unlock Veracrypt Volume»* Utility in *«Applications > Utilities > Unlock VeraCrypt Volumes»*.



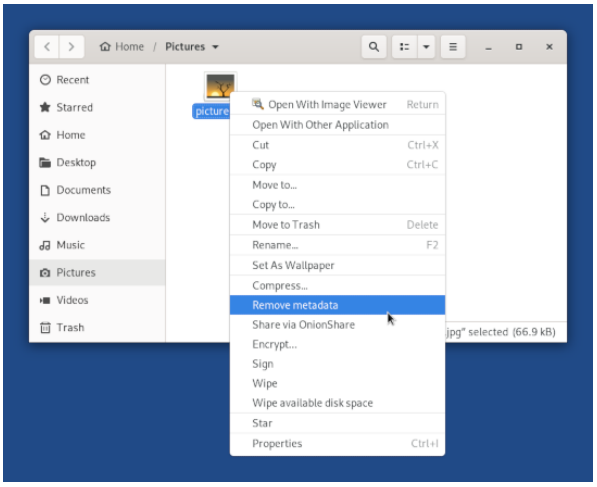
As they are numerous options for working with Veracrypt Volumes & Containers, you may be interested to give a look to the documentation if you plan to use it: https://tails.boum.org/doc/encryption_and_privacy/veracrypt/

If you are planning to exchange files between Tails and other Operating Systems, you may also be interested by the feature allowing you to remove MetaData from files.

Clean metadata using mat2

As we already discussed, if you are working on documents, they may include metadata informations such as Author, Institution, Serial Number of the software used to process them, or in case of pictures/videos, geo-location data or serial numbers of the camera used.

If you are planning to publish documents or just to export them outside of Tails, you **HAVE** to remove metadata from them. Tails includes a specialized tool allowing you to remove that metadata: mat2 for Metadata Anonymisation Tool [14]. You can use it simply by selecting *«Remove Metadata»* with a right-click (two-fingers click on Macs) on any document you want to clean.



[14] https://0xacab.org/jvoisin/mat2/.

Until recently Tails included the possibility to display metadata using mat, this functionality have been recently removed (you can only access it through command line). Until it is reintroduced in Tails, you can use the web mat version, which allows you to clean metadata but also to display them in a website.

You can use the following website:

- https://metadata.systemli.org/ from https://Systemli.org which allows to clean files up to 128MB and is also available with a .onion address: http://liqr2cbsjzxmpw6savgh274tuzl34x6cd56h7m7ceatnrokveffm66ad.onion.

This website also offer you the possibility to clean metadata outside of Tails. Be aware however of the security note on this website, **nothing prevents them from making a copy of your data when you send them for processing**, thus if you are working on sensitive data, better to handle that cleaning within Tails, which is also easier if you have multiple documents to clean and would help you to secure remove the uncleaned ones.

If you have some documents (or better, pictures) with you in a USB stick, try to

- Check for metadata is the file property window (right/two fingers-client->Properties)
- Upload them on mat2-web ; Please remind you **must** move them to the Tor Browser directory otherwise it won't have access to it
- Verify that mat display much more details and metadata than average software
- Clean them locally using mat right click/two-fingers click
- Upload the cleaned file to mat2-web
- And verify the difference.

If you are looking for the pictures on the Web, better to do it on https://flickr.com, as it is known to keep metadata, which most websites don't.

Please note however, that while trying to do its best, **mat2 offers no warranty that all metadata has been removed** thus if you are working on highly sensitive documents you **should double-check** with other tools or by asking specialists[15].

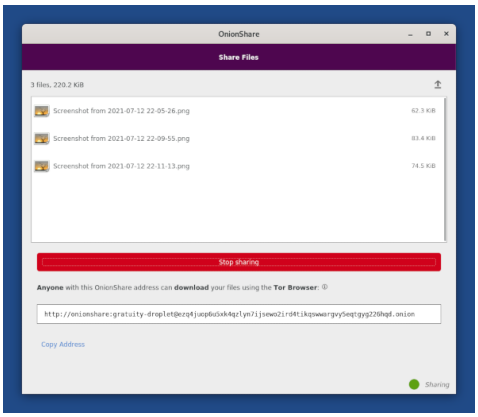
Still, mat2 is much more efficient than average software to display and clean metadata, while other software show the files as «cleaned». That is why **even if other softwares display no metadata, you should double check with mat2**, you would be surprised of the result.

Exchange data confidentially using OnionShare

If you would like to exchange documents confidentially using Tails. You can do that with *Onionshare* from https://theintercept.com Team. *Onionshare* allow you to share files **directly** with two computers **without** firstly uploading a copy to an intermediary website (like *wetransfer*). This is more secure as no intermediary will have a copy of your files, but for that the two computers need to be connected in the same time.

You can launch Onionshare using *«Application>Internet>OnionShare»* (it is also available with right-click/two-fingers click on a file) and simply select share. You will see a screen like this one:

[15] See https://0xacab.org/jvoisin/mat2/blob/master/doc/threat_model.md.



You will see that OnionShare generated a .onion link that you can share with the other person, letting them download your files, using the Tor Browser (and only with it). Yes, your computer is now part of the «darknet» and proposing files on it ! Try to exchange the link with your colleagues, you will see when they download from it. By default OnionShare only allows files to be downloaded once and stop the sharing after that. You can deactivate this behaviour using the configuration menu.

Please remind that both the Tor Browser and Onionshare are available for Windows or Mac, thus you can use it to exchange without a source without requiring her to install Tails. Tails just make them available quickly along with the other tools that allow working on the documents in a safe way, to store and remove them securely, to remove metadata etc.

Spread the word by making copies of Tails

If you like to install Tails, you can follow the install procedure from the website, https://tails.boum.org/install/. You can also make copies of Tails directly from Tails itself using «*Applications*>*Tails*>*Tails Installer*» (it will only copy the system and not the data).

If you have a USB Stick (8GB or superior)[16] with you, you can install Tails on it that way. It will use 4 to 8 GB for the system, leaving the rest of the space for data using persistence.

[16]Some sticks are known not to work with Tails https://tails.boum.org/support/known_issues/index.en.html#index1h2.

Please note that this stick will be erased and will have to be fully dedicated to Tails. If you want to reuse it for something else you have to follow a procedure to fully reset it (your system may allow you to do it, but it is likely it will only see and give you access to the system part).

- Reset procedure for Mac: https://tails.boum.org/doc/reset/mac/.
- Reset procedure for Windows: https://tails.boum.org/doc/reset/windows/.

Getting support

If you have issues with Tails, you may be interested to give a look to the support https://tails.boum.org/support/ page. It lists common issues etc. If needed, Tails is also offering a **free user support**, that is committed to help users and answer theirs questions. You can reach it by email tails-support-private@boum.org.

As said on the webpage https://tails.boum.org/support/#talk,

« We [Tails] answer requests in:

- English
- French
- Spanish
- Italian

Requests not in English might take longer to answer. Imperfect English is welcome :) »

Let's summarize with an excercise

- Download a sensitive document using the Tor Browser [17]
- Verify the metadata & Clean them.
- Store them confidentially using the persistence.
- Send them using OnionShare.
- Exchange the document with another person, group.
- Verify the metadata and clean them again, just in case (better safe than sorry).
- Store them confidentially using the persistence.
- Export them to another USB drive encrypted with gnome disk and/or,
- after encrypting the document with the right-click menu option.

[17] Looking for examples ? https://cryptome.org/2013/10/nsa-iat-tor.pdf or https://web.archive.org/web/20141230085809/https://www.spiegel.de/media/media-35535.pdf maybe cool ones (the last one may be long to load but it is worth it ... and was leaked using tails https://twitter.com/Snowden/status/1165297667490103302 ;)).

About this document

This document was wrote by contact@julielallouetgeffroy.com and mathieu.goessens@univ-rennes1.fr for journalists digital safety lessons. It is actually used as training material at IUT Lannion, Sciences Po Rennes and IJBA journalism schools in France.

Last version of this document, sources, and instructions to build your own version are available on github: https://github.com/mgoessen/tails-workshop/. Tails software and reference documentation are available on the Tails Website: https://tails.boum.org.