6
Installing Tails OS

Online privacy and security are critical. Sadly, many individuals, or groups, have less-than-honorable intentions when using the internet, the Dark Web, or any other online medium. We need to take steps to protect ourselves, and, as we've discussed previously, there are many ways to do so. One of them is by using privacy and security-oriented OSes. One of them is Tails.

In the previous chapter, we learned about Tor and how to install and use it.

In this chapter, we will learn the following topics:

- What is Tails OS?
- Tails OS installation prerequisites
- Downloading Tails OS
- Installing Tails OS

What is Tails OS?

Tails, which is short for **The Amnesic Incognito Live System**, is a Debian Linux-based, security- and privacy-focused OS, intended to be run from a USB flash drive or a DVD. As such, Tails doesn't leave any traces on the original OS installed on the PC, either in the memory or the filesystem. This, of course, helps with privacy. The Tor Project funds the development of Tails, along with Mozilla, the Freedom of the Press Foundation, and the Debian Project.

As an OS, Tails ships with several default applications, focused on security. For example, Tails uses Tor by default to connect to the internet. Its default browser is Tor Browser. All outgoing communication is routed through the Tor network, and non-anonymous connections are not allowed. It includes applications to encrypt data, a password generator, and tools to minimize the risk when connecting to the internet (all communication, including emails and instant messaging, are encrypted by default).

All in all, it's one of the most secure OSes out there.

Some of the security features supplied by Tails, by default (Tor Browser is the default browser in Tails OS), are as follows:

- **AppArmor confinement**: Enforces specific sets of rules on applications, limiting their access in the system.
- **HTTPS Encryption**: All traffic is encrypted by default.
- **HTTPS Everywhere**: Thanks to a browser extension developed by the Electronic Frontier Foundation, for Firefox, Chrome, and Opera, communication with many major websites is encrypted, providing a more secure browsing experience.
- **Torbutton**: An extension developed for Tor Browser, to enhance security and privacy, which has multiple capabilities:
    - **Protection against dangerous JavaScript**: Limits and prevents dangerous JavaScript from running.
    - **Security slider**: Feature to manage Tor Browser security setting levels.
    - **New Identity feature**: This is intended to remove session information (cache, cookies, history, and so on), closes all web connections, erases the content of the clipboard, and closes all open tabs. (Having said that, to completely remove data, restart Tails.)
    - **NoScript**: Allows complete disabling of JavaScript.

But, even with all its security, privacy, and anonymity options, Tails has weaknesses.

For example (according to the Tails website documentation), note the following:

- Tails does not protect against compromised hardware—meaning that if an attacker gains physical access to the computer you are running Tails from, it can be unsafe.
- Tails can be compromised if installed on or plugged into untrusted systems—remember that you install or run Tails from a computer with its own OS. If that computer is compromised, this can lead to disruption of Tails' protective capabilities.
- Tails does not protect against BIOS or firmware attacks—attacks that target the computer's BIOS or firmware aren't protected by Tails.
- Tor exit nodes can eavesdrop on communications—the exit node, the last node in the Tor relay network, which connects to the destination server, is not encrypted, and this allows attackers to eavesdrop and capture the communication at that point. To protect yourself, it's recommended to use end-to-end encryption.

- Tails makes it clear that you are using Tor and probably Tails—even though you're using Tails and Tor for connecting, which will make it harder to identify you, your ISP, local network admin, or destination server, can identify that you are using Tor.
- Man-in-the-middle attacks—as I mentioned previously, the traffic between the exit node and the destination server is unencrypted, which allows attackers to perform a man-in-the-middle attack, where the attacker eavesdrops on the communication.
- Confirmation attacks (also known as end-to-end correlation)—traffic entering or exiting the Tor network can be measured and analyzed, which can lead to identifying you.
- Tails doesn't encrypt your documents by default—but, Tails ships with encryption tools, just for this purpose.
- Tails doesn't clear the metadata of your documents for you and doesn't encrypt the subject and other headers of your encrypted email messages—but, Tails provides tools to anonymize your documents.
- Tor doesn't protect you from a global adversary—a global adversary has the capability to monitor all traffic in a network simultaneously. Thus, they could potentially be able to perform statistical analysis on the traffic, to identify Tor circuits and then match the communication to destination servers.
- Tails doesn't magically separate your different contextual identities—performing multiple actions in the same session is inadvisable, as Tor has a tendency to reuse the same circuits in a given session. Restarting Tails will make sure that you prevent this.
- Tails doesn't make your passwords stronger—don't use weak passwords; need I say more?
- Tails is a work in progress—as with all software in development, bugs or security flaws can occur.

Bearing all of this in mind, we can minimize our risk by following best practices and common sense.

Tails OS installation prerequisites

As with all installations of software (OSes are software), we need to verify the installation requirements before beginning.

For Tails, the hardware installation requirements are as follows:

- A 64-bit x86-64 compatible processor (except for PowerPC or ARM)
- 2 GB of RAM
- A way to boot either from a DVD or USB flash drive

There are several ways to install and use Tails, depending on the OS of the computer on which you'll be installing Tails.

The time it takes and the complexity of the installation process is also affected by the *source computer*.

Tails can be installed from Windows, Debian, Ubuntu, or Mint Linux, or almost any other Linux distros. (macOS isn't really supported, but you can always install Tails as a virtual machine in macOS.)

Although I won't go into detail for all of the possible source OSes in this book, I will outline the general processes for most of them, and provide detailed instructions for Linux (Ubuntu).

Downloading Tails OS

Let's get started by downloading Tails OS in the following OSes.

Downloading Tails OS in Windows

1. Download the Tails OS ISO file from the Tails website: `https://tails.boum.org/install/win/index.en.html`.

2. It's highly recommended to verify the downloaded file's signature.

Downloading Tails OS in Linux

1. Navigate to the Tails OS download page: `https://tails.boum.org/install/download/index.en.html#install-inc-steps-download.inline.basic-openpgp`.
2. Download the Tails OS ISO file, either directly or via a Torrent client (I personally prefer the direct download option, as torrents can be insecure).

3. For security purposes, it's a good practice to verify the ISO file. The process is similar to what I talked about previously in the book. You need to download the Tails signature, and signing key, while, or after, you download the Tails OS ISO file.
4. You can download the signing key from here: `https://tails.boum.org/tails-signing.key`.
5. And, the signature file is available here: `https://tails.boum.org/torrents/files/tails-amd64-3.8.iso.sig`.
6. Save them in the same folder where you saved the ISO file.
7. To verify the downloaded file, using OpenPGP, run the following command in the Linux Terminal:

```
gpg --no-options --keyid-format 0xlong --verify tails-
amd64-3.8.iso.sig tails-amd64-3.8.iso
```

The result should be as follows:

```
gpg: Signature made Mon 25 Jun 2018 11:14:47 AM UTC
gpg: using EDDSA key CD4D4351AFA6933F574A9AFB90B2B4BD7AED235F
gpg: Good signature from "Tails developers <tails@boum.org>" [full]
gpg: aka "Tails developers (offline long-term identity key)
<tails@boum.org>" [full]
```

8. Always verify that there is no more than five days between the signature and the latest version of the ISO file.

Installing Tails OS

Let's move on to installing Tails OS in the following OSes.

Installing Tails OS in Windows

Installing Tails directly from Windows is not currently possible, but it can be done by using two USB sticks, and installing Tails on one, and then the other, as shown in the following steps:

1. Install Tails on one of the USB sticks, the *intermediary* one, using the Universal USB Installer (I mentioned it in `Chapter 4`, *Installing a Linux Virtual Machine*).
2. In the Universal USB Installer application interface, choose to install from the Tails OS ISO file you downloaded.

3. After installing Tails OS on the first USB stick, restart your computer and boot from the USB stick. You should boot into Tails, after a few seconds.
4. Now, plug in the second USB stick, go to **Applications** | **Tails** | **Tails Installer** (in Tails OS), and install Tails on it.
5. After the installation process ends, remove the first USB stick, restart the computer, and boot from the second USB stick.

You'll boot into Tails OS.

Installing Tails OS in Red Hat, Fedora (any Linux distro that isn't Debian, Ubuntu, or Mint) for browsing the Dark Web

The process here is basically the same as with Windows (install on the first USB stick, then on the second, then run from second).

The installation of the first USB stick is done using GNOME Disks (also known as **Disks**), and then, after rebooting from it, you'll use the Tails Installer to install Tails OS on the second USB stick.

The rest of this chapter will detail how to install Tails OS via Debian, Ubuntu, or Mint Linux distros.

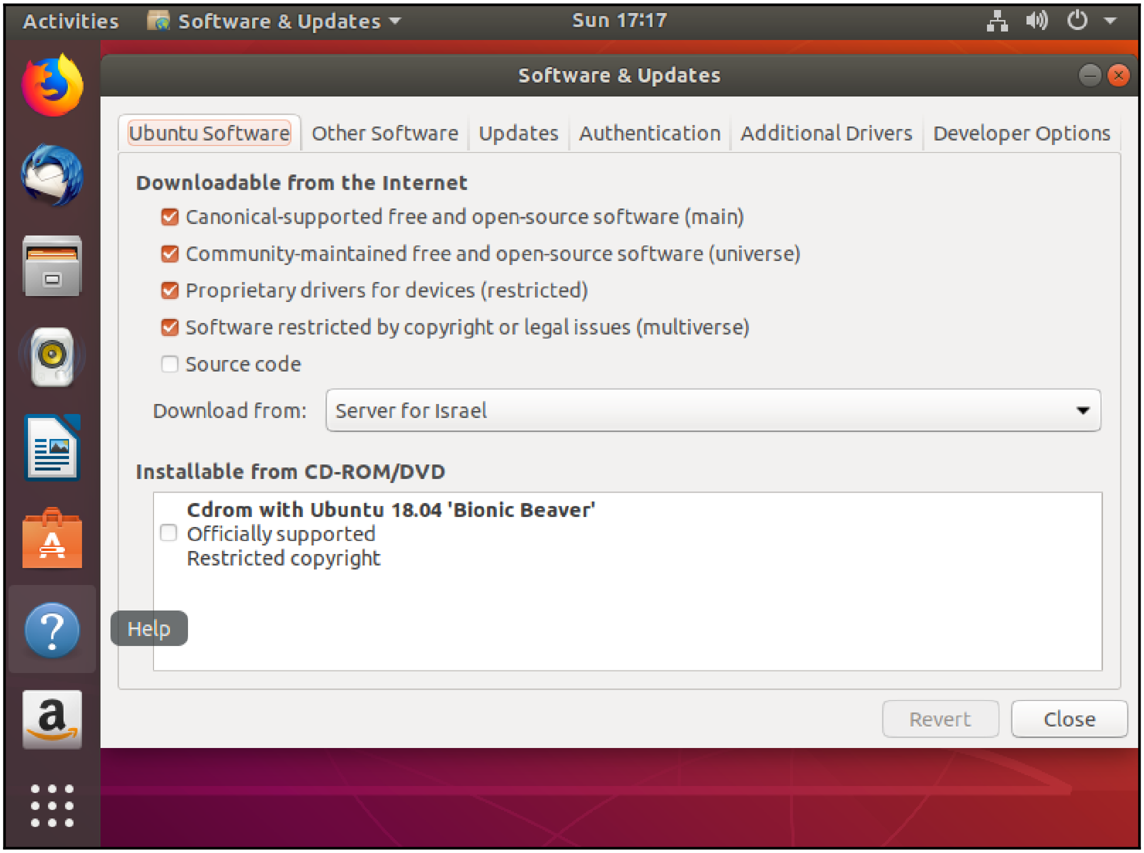
Note that the software installation requirements are as follows:

- Debian 9 and higher
- Ubuntu 16.04 and higher
- Linux Mint 18 and higher

We will start by installing Tails Installer, which, in turn, will install Tails.

To do so, perform the following actions:

1. Start software and updates in Linux.
2. Verify that the **Community-maintained free and open-source software (universe)** option is selected:



Downloadable from the Internet

☑ Canonical-supported free and open-source software (main)

☑ Community-maintained free and open-source software (universe)

☑ Proprietary drivers for devices (restricted)

☑ Software restricted by copyright or legal issues (multiverse)

□ Source code

Download from: Server for Israel

Installable from CD-ROM/DVD

□ **Cdrom with Ubuntu 18.04 'Bionic Beaver'**
Officially supported
Restricted copyright

Community-maintained free and open-source software

3. Press the **Other Software** tab, and click on the **Add...** button.
4. In the APT line field, enter the following:

```
ppa:tails-team/tails-installer
```

5. And then, press the **Add Source** button. You will see the **Authentication Required** window, so enter your password and press **Authenticate**. Then, press **Close**.
6. Then, press **Reload** and wait for the package download process to finish.
7. Open the Terminal and run the following command to install the **Tails Installer** package:

```
sudo apt install tails-installer
```

Installing Tails from the command line

You can also download and install Tails from the command line, as shown in the following steps:

1. First, download the ISO image by running the following command in the Terminal:

```
wget --continue
http://dl.amnesia.boum.org/tails/stable/tails-amd64-3.9/tails-amd64
-3.9.iso
```

Don't forget to verify the ISO file.

2. Next, install Tails Installer. Depending on your Linux distro (Debian, Ubuntu, or Mint), you'll need to run different commands in the next step, to add the required repositories.

Since we've been using Ubuntu, I'll start with the commands for it (they're the same for Mint).

There are two repositories to install—Tails PPA and universe.

A **Personal Package Archive** (**PPA**) is custom software (or custom updates), not provided in Ubuntu, by default.
The Ubuntu version release cycle is every six months, so if you want to update applications between versions, or install new ones, which don't exist in the Ubuntu Software Center, you'll probably install a PPA.

Run the following commands to add them:

```
sudo add-apt-repository universe
sudo add-apt-repository ppa:tails-team/tails-installer
```

Debian needs the `backports` repository. To add it, run the following:

```
BACKPORTS='deb http://http.debian.net/debian/ stretch-backports main'
echo $BACKPORTS | sudo tee /etc/apt/sources.list.d/stretch-backports.list
&& echo "OK"
```

Then, in any of these distros, run the following command to update your lists of packages:

```
sudo apt update
```

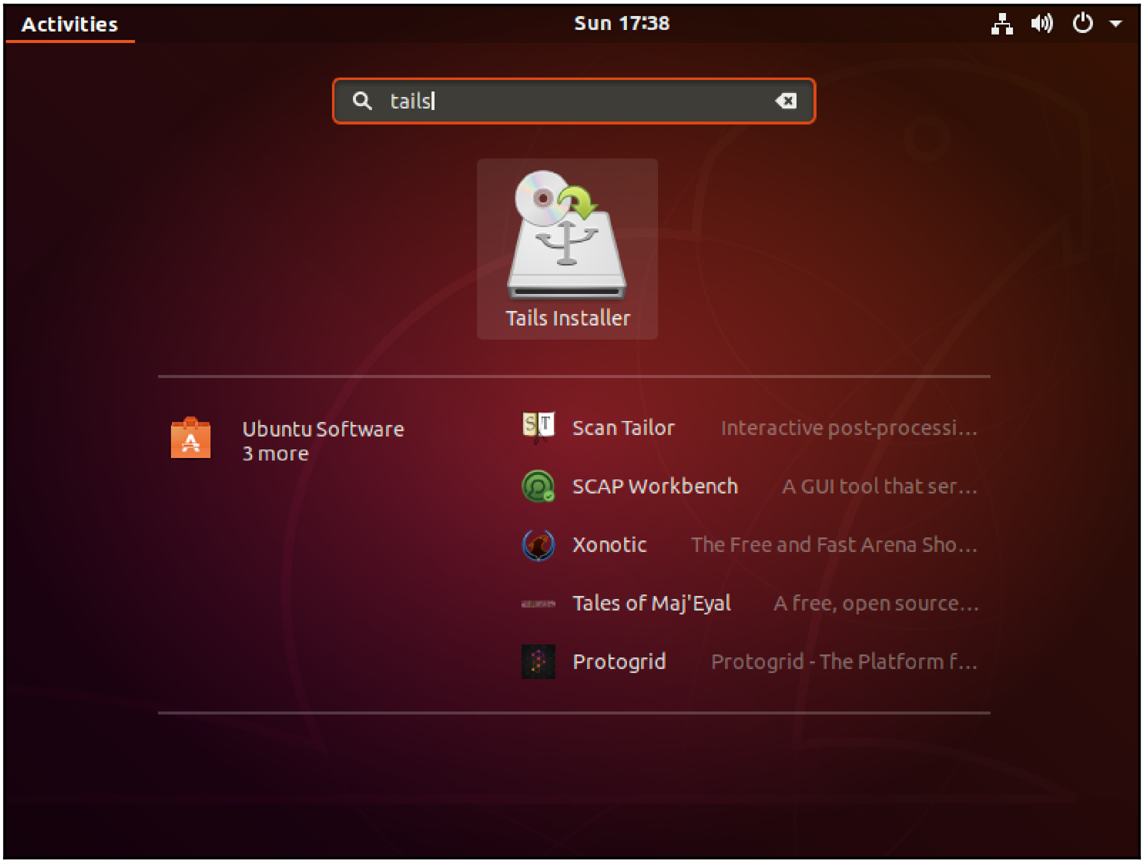
The next step will be to prepare and install Tails on the USB flash drive:

1. Connect the USB flash drive to the computer, and then start the Tails Installer from Linux.
2. You can run the following command from Terminal:

   ```
   sudo apt install tails-installer
   ```

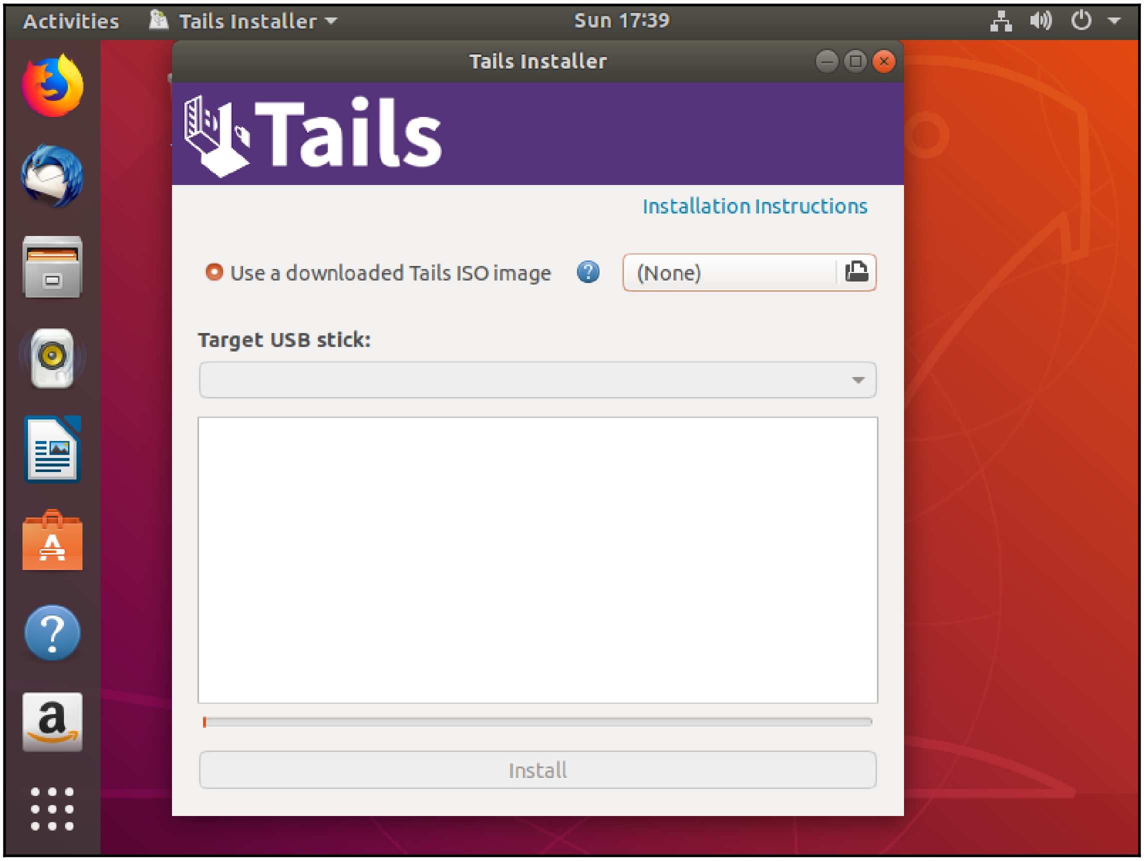
   Or, you can go to Ubuntu Software and search for Tails.

3. Press the Tails Installer icon:



Tails Installer startup

4. When Tails Installer loads, press the folder icon next to the button that displays **None**, and locate the ISO file you downloaded previously.
5. Under **Target USB stick**, choose the USB flash drive you connected to the computer, as follows:



● Use a downloaded Tails ISO image (None)

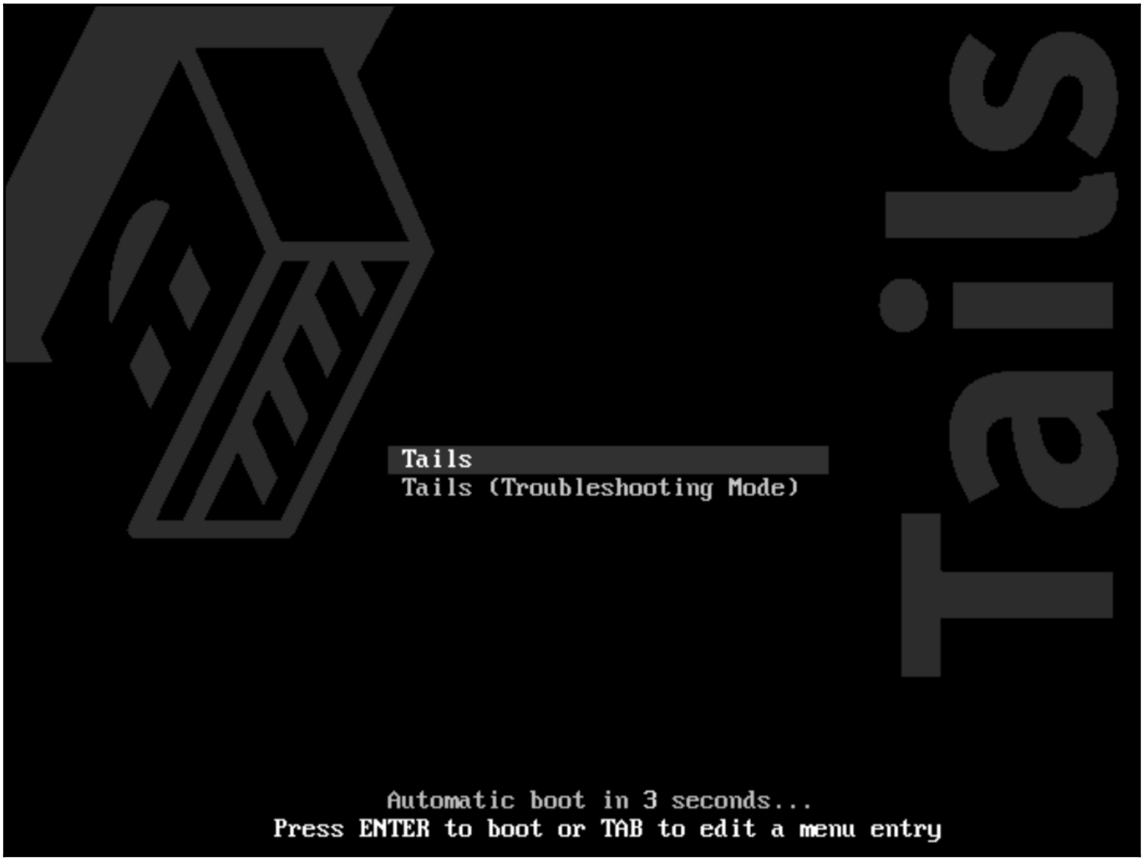
Target USB stick:

Tails Installer

6. Press **Install**, go over the displayed warning, and click **Yes** to confirm.
7. You will be asked to enter your password twice during the installation process, after which you will see an **Installation Complete** message, which you can close.

That's it. You can now boot your computer from the USB flash drive, and start Tails.

After booting from the Tails USB flash drive, you'll reach the Boot Loader Menu:



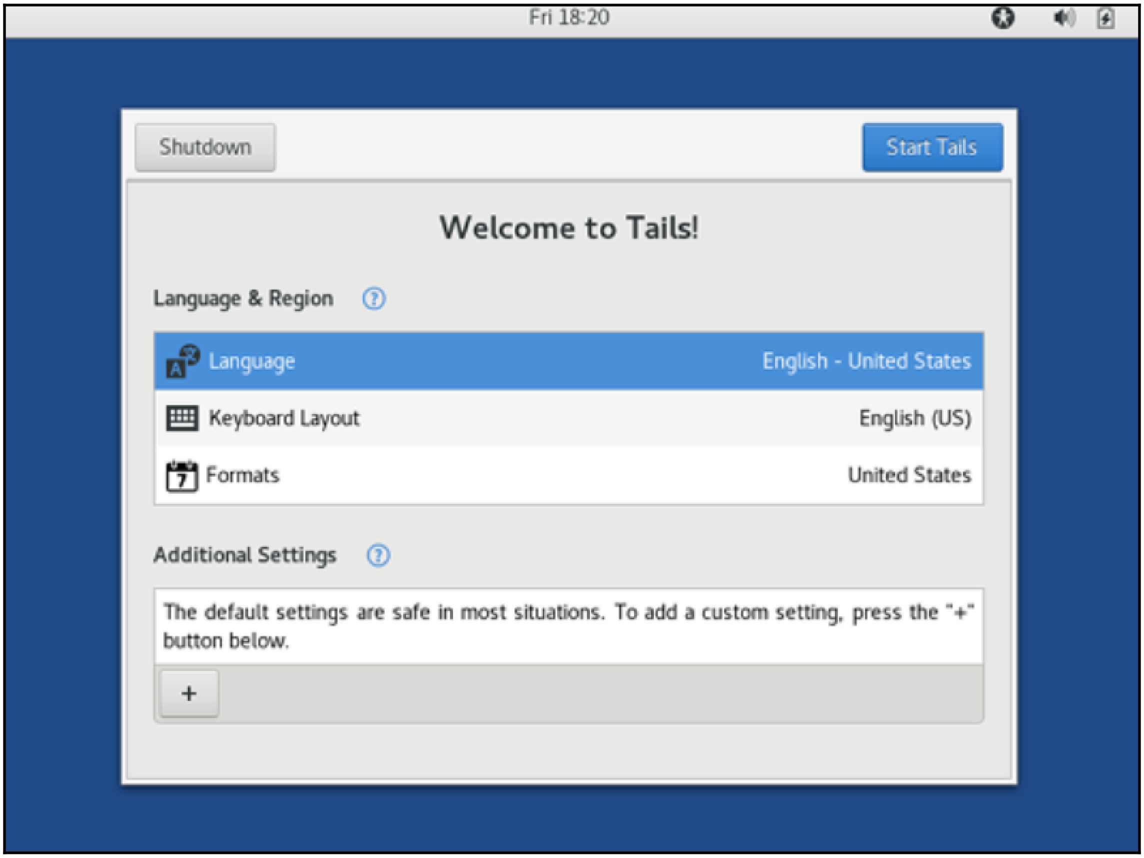
```
Tails
Tails (Troubleshooting Mode)

Automatic boot in 3 seconds...
Press ENTER to boot or TAB to edit a menu entry
```

Tails Boot Loader Menu

You can press the *Enter* key or wait until the startup process continues.

After another 30-60 seconds, the Tails Greeter screen will appear, where you can choose your language, keyboard layout, and format.

Now, press **Start Tails**:



Welcome to Tails!

Language & Region

Language English - United States

Keyboard Layout English (US)

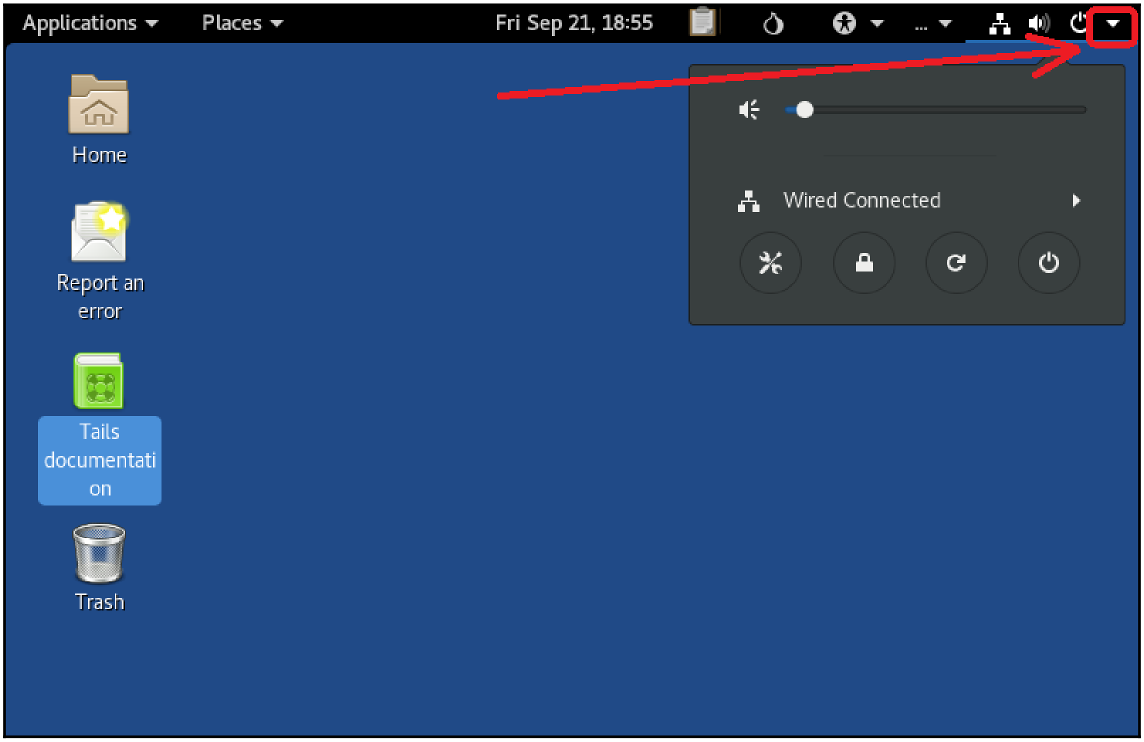
Formats United States

Additional Settings

The default settings are safe in most situations. To add a custom setting, press the "+" button below.

Tails greeter

After Tails starts, you'll reach the Tails desktop, from which you'll be able to connect to a network by going to the system menu, in the upper-right part of the screen (click the little drop-down arrow):

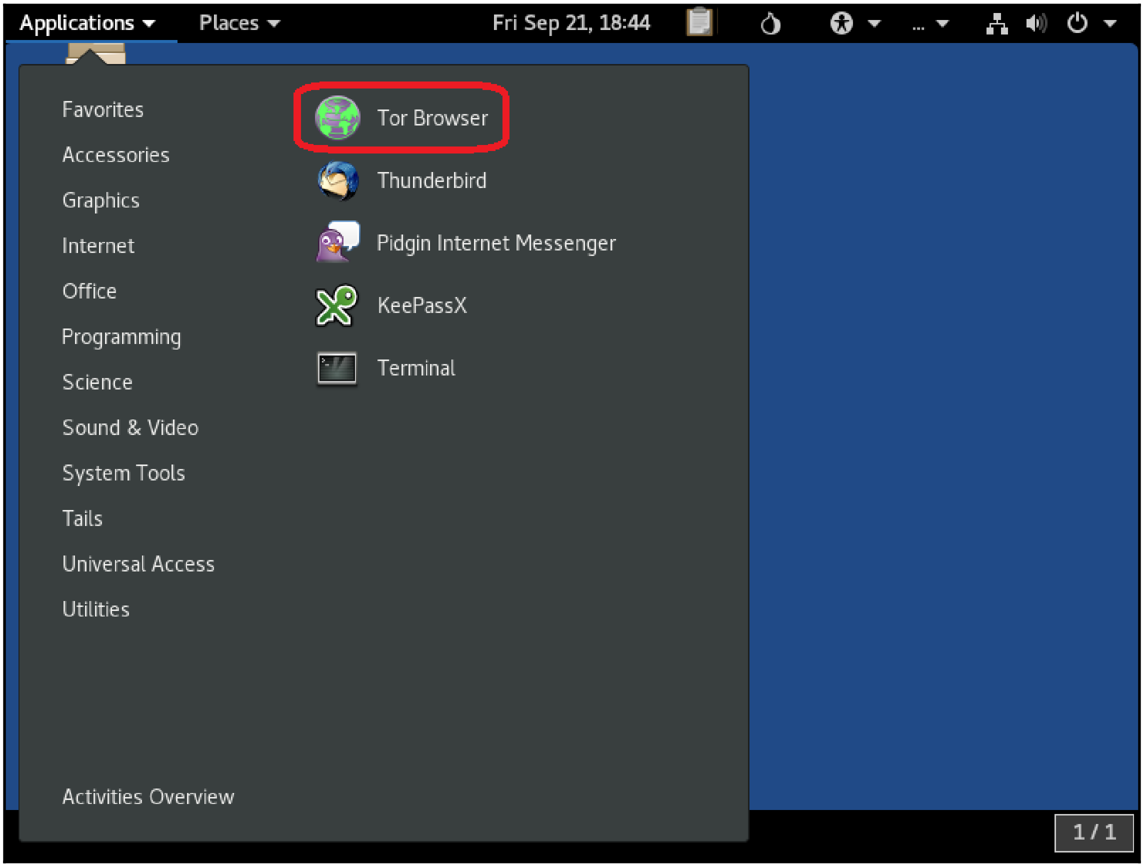


Tails System Menu

Wired connections are configured automatically; for Wi-Fi, press **Wi-Fi** (it can also display **Wi-Fi Not Connected**) and then select **Network**. Choose the required network and connect.

Now, you can run Tor Browser and surf the Deep and Surface Web much more anonymously and privately.

Using Tor Browser in Tails is similar to Linux, using the graphical user interface, rather than Terminal, as shown here:



Tor Browser in Tails

Go to the **Applications** menu, and press the Tor Browser icon.

You're done. You can now start using Tor Browser on Tails OS, to access the Dark Web.

Summary

This chapter was more hands-on and focused than previous chapters.

As we go along, I expect that your comfort with technical actions will grow, if you weren't technically proficient before reading this book, so it will get easier. But if it doesn't, you'll have the step-by-step instructions in this book.

Tails is a very privacy-focused OS that may take getting used to. If actions take more time, or work in a different manner, always remember that there's a trade-off between security/privacy and speed or comfort/ease of use.

In the next chapter, we'll continue with installations of additional OSes. After trying them out, choose the one that best fits your requirements.

Questions

1. What are the Linux software installation requirements for Tails OS?
2. What Terminal command starts the Tails Installer application?
3. What are the Tails OS hardware installation requirements?

Further reading

The following resource might be interesting if you'd like to go deeper into the subjects of this chapter:

- `https://tails.boum.org/`