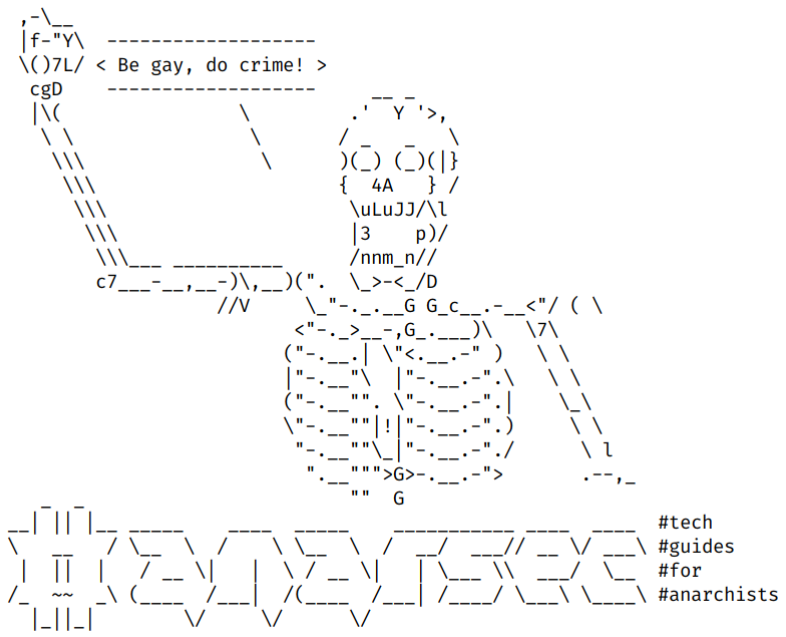
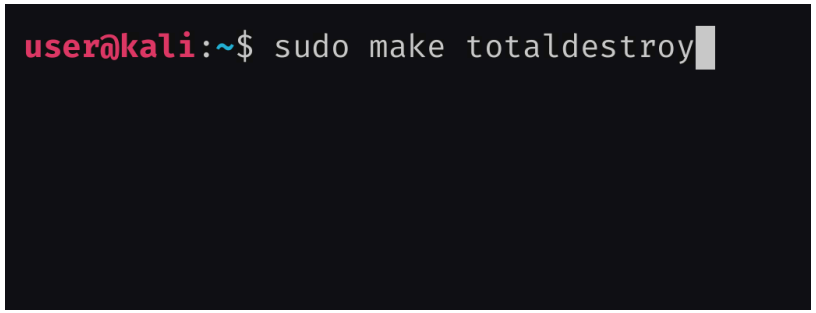
Linux Essentials

As an anarchist, someone's probably recommended that you use a Linux computer at some point. This article is intended to get you started by giving you a brief overview of what you need to know.





Series: Defensive

This version of the zine was last edited on 2024-04-21. Visit anarsec.guide to see whether it has been updated since.

The dagger symbol † on a word means that there is a glossary entry for it. Ai ferri corti.

AnarSec is a resource designed to help anarchists navigate the hostile terrain of technology — defensive guides for digital security and anonymity, as well as offensive guides for hacking. All guides are available in booklet format for printing and will be kept up to date.

Defensive

Tails

- Tails for Anarchists
- Tails Best Practices

Qubes OS

- Qubes OS for Anarchists

Phones

- Kill the Cop in Your Pocket
- GrapheneOS for Anarchists

General

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Offensive

Coming soon

Contents

As an anarchist, someone's probably recommended that you use a Linux computer at some point. This article is intended to get you started by giving you a brief overview of what you need to know.

What is Linux and Why Use It?

If you're reading this, you're probably using either Windows or macOS on your computer. These are both operating systems†, which is the system software that runs your device. They're also both "closed-source", which means that the software's "*source* code" is not available (*closed*) to the public, so it can't be audited for privacy and security. Windows and macOS computers send your data to Microsoft and Apple, and you can't trust their full-disk encryption† to protect your data if the computer is physically accessed† (like after a house raid[1]).

Linux is a set of operating systems that are open-source†, which means that the *source* code can be analyzed by anyone. Linux is the name given to the core (**kernel**) of the operating system, and many different **distributions** (or 'distros') are based on it.

Some Linux distributions you may have heard of are Debian, Ubuntu and Tails[2]. Each Linux distribution manages software differently, may use a different kernel version, etc., depending on what the specific distribution is geared towards. In fact, both Ubuntu and Tails are adaptations of the Debian distribution for being user-friendly (Ubuntu) and providing anonymity (Tails).

How Software Works

In Linux, the term for an application is a **package**. Instead of downloading applications from various sites on the Internet (as in Windows and macOS), a Linux distribution has a centralized **repository** where the software lives. The advantage of this is that

[1] notrace.how/threat-library/techniques/house-raid.html
[2] anarsec.guide/tags/tails/

Tor network

Tor[39] (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor "the King of high secure, low latency Internet anonymity" with "no contenders for the throne in waiting". The Tor network can be accessed through the Tor Browser on any operating system. The Tails† operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists[40] and Privacy Guides[41]. To understand the limitations of Tor, see the Whonix documentation[42].

[39] torproject.org/
[40] anarsec.guide/posts/tails/#tor
[41] privacyguides.org/en/advanced/tor-overview/
[42] whonix.org/wiki/Warning

the integrity of the software is verified by the distribution, and it is guaranteed to work with that distribution. It is still possible to install software from outside of a distribution's repository, but it is generally considered riskier, and verifying the integrity becomes your responsibility. Installing a package requires knowing its name, and all packages in a repository can be browsed using a web browser for both Debian[3] and Fedora[4].

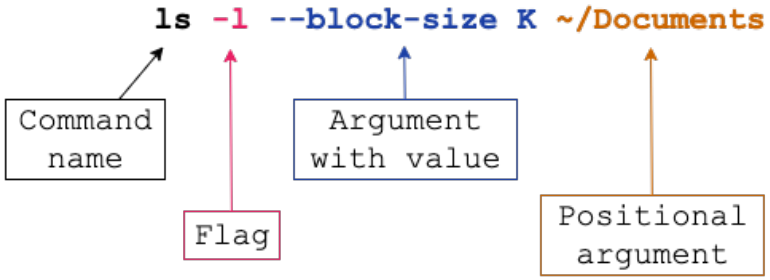
How do you actually install from a software repository? Each distribution also has a **package manager**, which is an application that installs software from a repository. Debian and other distributions based on it use the `apt` package manager. In some distributions, it is possible to install software with a Graphical User Interface (GUI) that uses the package manager in the background, such as the Synaptic Package Manager[5] in Tails.

Software Alternatives

Part of the learning curve for Linux is figuring out which open-source software to use instead of the closed-source options you are used to in Windows and macOS. For example, instead of using Microsoft Word, you might use LibreOffice. It's essential that the applications you use are open-source, but an application being open-source is not enough to consider it secure. For example, Telegram advertises itself as open-source, but its servers are not open-source and its cryptography is garbage[6]. The list of included software for Tails[7] will cover many of your needs with reputable choices, and you can also check out switching.software[8].

[3] debian.org/distrib/packages#search_packages
[4] packages.fedoraproject.org/
[5] anarsec.guide/posts/tails/#installing-additional-software
[6] buttondown.email/cryptography-dispatches/archive/cryptography-dispatches-the-most-backdoor-looking/
[7] anarsec.guide/posts/tails/#included-software
[8] switching.software/

The Command Line Interface



The dreaded command line[†]! What even is it? You are used to interacting with applications through a **Graphical User Interface (GUI)**, which means pointing and clicking with your mouse. Some applications can also be interacted with through a **Command Line Interface (CLI)**, which is textual. Many applications are available in both CLI and GUI versions. In a nutshell, the GUI is just a graphical depiction of the same things that you would do from the Command Line (CLI), designed to make it easier and more intuitive to navigate your computer.

For example, navigating the contents of your computer with the File Manager GUI is pretty standard — you click on a folder (called a *directory* in Linux), and it opens. The same navigation through the file system is also possible from the CLI.

When you open a Terminal (the CLI application), you get a *prompt*. It is called a prompt because it is prompting you to say something in a language that the Terminal understands. Prompts differ in what information is displayed, but they all end with the `$` character. You then give *commands* to the Terminal. The Terminal responds, then redisplays the prompt for the next command.

The best way to learn the basics of the command line is to interact with it. We recommend the Foundations: Linux Journey[9] "Command Line" module to learn some basic commands. The Software

[9] techlearningcollective.com/foundations/linux-journey/

Full Disk Encryption (FDE)

FDE means that the entire disk is encrypted[32] until a password is entered when the device is powered on. Not all FDE is created equal. For example, the quality of how FDE is implemented on a phone depends not only on your operating system, but also on your hardware (the model of your phone). FDE uses symmetric cryptography[32], and on Linux it typically uses the LUKS specification[32].

Open-source

The only software we can trust because the "source code" that it is written in is "open" for anyone to examine.

Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

Physical attacks

A physical attack is a situation where an adversary first gains physical access to your device through loss, theft, or confiscation. For example, your phone may be confiscated when you cross a border or are arrested. This is in contrast to a remote attack[32].

For more information, see Making Your Electronics Tamper-Evident[35], the Threat Library[36], the KickSecure documentation[37], and Defend Dissent: Protecting Your Devices[38].

[35] anarsec.guide/posts/tamper

[36] notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html

[37] kicksecure.com/wiki/Protection_Against_Physical_Attacks

[38] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/

See When to Use Tails vs. Qubes OS[29]. We do not offer "harm reduction" advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

Encrypted Messaging

See Encrypted Messaging for Anarchists[30]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[31].

Appendix: Glossary

Command Line Interface (CLI)

The "command line" is an all-text alternative to the graphical "point and click" tool that most of us are more familiar with; the Command Line Interface (CLI) allows us to do some things that a Graphical User Interface (GUI) does not. Often, either a GUI or a CLI would work, and which you use is a matter of preference. For example, in Tails†, you can verify the checksum[32] of a file using either a GUI (the GtkHash program) or a CLI command (`sha256sum`).

For more information, see Linux Essentials[33]. The Tech Learning Collective's "Foundations: Linux Journey" course on the command line[34] is our recommended introduction to using the CLI/terminal.

[28] anarsec.guide/posts/qubes/
[29] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[30] anarsec.guide/posts/e2ee/
[31] anarsec.guide/posts/tamper/
[32] anarsec.guide/glossary
[33] anarsec.guide/posts/linux/#the-command-line-interface
[34] techlearningcollective.com/foundations/linux-journey/the-shell

Distribution and Packages[10] exercise will teach you what you need to know to install software in Qubes[11].

Some commands require elevated privileges, equivalent to "Open as Administrator" in Windows. For example, installing software usually requires this privileged access. Prefixing a command with `sudo` will execute it as the administrative user, named root (note that the root user is not the same as the root directory, and the two should not be confused). A root prompt will display `#` instead of `$`. Be especially careful with any commands you run while using these elevated privileges, as you'll have the power to erase your entire hard drive or change important files. It is helpful to know that text is pasted into the Terminal with Ctrl+Shift+V (i.e. the Shift key must also be pressed).

Most Linux users will rarely need to use the CLI. If you're using Tails, you shouldn't need it at all. If you're using Qubes OS, the CLI is only needed to install software:

- This will install packages on Debian: `apt install <PACKAGE_NAME>`
- This will install packages on Fedora: `dnf install <PACKAGE_NAME>`

Additionally, the CLI is needed for the more secure installation of both Tails[12] and Qubes OS[13] to verify the download's authenticity.

If you ever need to edit a text file from the command line, you can use `nano`[14]. If you ever don't understand what a command does, try looking it up on explainshell[15].

[10] techlearningcollective.com/foundations/linux-journey/software-distribution
[11] anarsec.guide/posts/qubes/#how-to-install-software
[12] anarsec.guide/posts/tails-best/#appendix-gpg-explanation
[13] qubes-os.org/security/verifying-signatures/
[14] phoenixnap.com/kb/use-nano-text-editor-commands-linux
[15] explainshell.com/

Going Further

If you want to learn more about Linux, we'd recommend:

- The rest of the Tech Learning Collective's Foundations[16] exercises will give you a much more comprehensive foundation than what you need to use Qubes or Tails.
- Linux Fundamentals at Hack The Box Academy[17] is another interactive learning environment with a less comprehensive overview.

Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[18] for the purposes of incrimination[19] and network mapping[20]. Our goal is to obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France[21]: "So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which "private or confidential words are spoken" and must remain so, even if it's switched off, we become a potential state informer…"

You may also be interested in the Threat Library's "Digital Best Practices"[22].

[16] techlearningcollective.com/foundations/
[17] academy.hackthebox.com/course/preview/linux-fundamentals
[18] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[19] notrace.how/threat-library/tactics/incrimination.html
[20] notrace.how/threat-library/techniques/network-mapping.html
[21] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/
[22] notrace.how/threat-library/mitigations/digital-best-practices.html

Your Phone

Operating system†: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[23]. If you decide to have a phone, treat it like an "encrypted landline" and leave it at home when you are out of the house. See Kill the Cop in Your Pocket[24].

Your Computer

Operating system†: **Tails** is unparalleled for sensitive computer use (writing and sending communiques, moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network†. See Tails for Anarchists[25] and Tails Best Practices[26].

Operating system†: **Qubes OS** has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials[27]. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[28].

[23] anarsec.guide/posts/grapheneos/
[24] anarsec.guide/posts/nophones/
[25] anarsec.guide/posts/tails/
[26] anarsec.guide/posts/tails-best/
[27] anarsec.guide/posts/linux