4

Installing a Linux Virtual Machine (VM)

In the previous chapter, we discussed what the future of the Dark Web might be. As you may know, there are various operating systems on the market. Windows, macOS, ChromeOS, and Linux are the most common (not necessarily in that order). The operating system which is the most secure, and the one which we'll be using for several chapters, is Linux.

Linux has many flavors (distros), which we'll discuss in this chapter, including how to install them (we'll talk about one, but the idea is the same for most of them).

Let's start getting our hands dirty by installing Linux, the Tor browser, and accessing the Dark Web.

In this chapter, we will cover the following topics:

- Linux Distributions
- Installing and using a Linux VM
- What else can we do with a Linux VM?

Linux Distributions

Red Hat, Fedora, Ubuntu, and CentOS are just a few of the more common Linux distributions out there that you can use for everyday use or, in the context of this book, to install the Tor browser on it and access the Deep Web.

The levels of privacy and anonymity you want to reach are the main factors in choosing an OS for Deep Web browsing. There are several security-dedicated Linux-based OSes out there, which we will discuss later in the book.

For now, let's talk a little about Linux (and what a distribution is).

Linux was developed by Linus Torvalds, a Finnish computer science student, in 1991. In those days, Unix-like systems were the craze, but they were either incompatible with most PCs, or too expensive.

Linux started as a program, specifically for use with Torvalds' personal 80386 PC, but, as time went on, it evolved into an OS.

I won't go into the details of the evolution of Linux, but I will mention several important aspects of the OS:

- First, it's free
- It's also free to distribute and share
- It's also pretty secure, stable, and reliable
- Linux is also very customizable, especially if you're a coder

Since Linux is so open, there are many different versions, each of them slightly different from the others. These versions are called distributions, or distros, for short.

Before we install a Linux distribution, the question arises—which one is the best for me?

Well, since there are so many distributions, it is a matter of preference and what you want to achieve with the OS. Some distribution have more emphasis on the desktop user interface, while others are server versions, and others still are focused on security (both defensive and offensive).

A few of the more common desktop Linux distributions are Ubuntu, Mint, Fedora, Debian, and openSUSE. Several of the common server Linux distributions are Red Hat Enterprise Linux, Ubuntu Server, CentOS, and SUSE Enterprise Linux. We will start with a *standard* Linux distribution, and as we move through the book, we will examine several of the best Linux-based OSes for accessing the Deep Web.

Before you install any OS- Linux or any other- operating system, read up about it, what its weaknesses and fortes are, and most importantly, what resources are required to install it.

Linux has several advantages over Windows and even macOS, which tend to make it more secure, but as with any technology, how you use it can also affect its security.

The first advantage is that, by default, users created in Linux do not have administrative privileges. Of course, the user can change this, but if used correctly, remaining with the default privileges is a great security advantage.

Running or installing applications requires the elevation of privileges, which means that most Malware, Trojans, Backdoors, and so on will not be able to execute on download.

The fact that the vast majority of the world uses Windows is also an advantage—most hacks are pointed to that OS, which means that there are less pointed at Linux.

In addition, the diversity of Linux distribution means that each Linux OS is slightly different, which means that hackers usually need to develop specific exploits for each one. The fact that most of the OSes are Windows means that there are less ready-made hacks out there, compared to Linux.

Since Linux is free and its source code is also freely available, countless people review its source code and find any flaws or weaknesses, fix them, and then redistribute the improved code.

The sheer number of tester-users means that, statistically, most of the security flaws (and other types of flaws) will be detected and fixed, and in a comparatively short time. With Windows, mainly Microsoft employees find these flaws, meaning that there is a much smaller group of people working to find issues, and thus fewer issues are found, before the OS is released.

I will elaborate on best practices for accessing the Deep Web in a different chapter, but in general, the most important factors you need to consider are as follows:

- Use a VPN. The VPN you choose should have the following features: be able to connect via other countries' servers, prevent IP or DNS leaks, and have a kill switch if your VPN goes down.
- Use Tor to access the Dark Web, to minimize your exposure.

Let's explain some of the terms I just mentioned:

- IP leaks occur when your browser reveals your computer's IP address, even when connected to a VPN. This can be prevented by using VPNs that are designed to prevent IP leaks.
- DNS leaks occur when your computer forwards its DNS request to your ISP's DNS server rather than through the VPN you are using.

These two types of leaks occur due to weaknesses that exist in the computer's browser or OS.

A kill switch is a mechanism built into some VPNs that disconnects the internet connection of the computer, when the VPN disconnects unexpectedly, rather than returning to the default configuration of your computer, as supplied by your ISP. Without a kill switch, your computer will switch back to the ISP connection, exposing you to the public:

- Use the Tor browser. First, you won't be able to access Deep Web sites without it. But, it's also important to minimize your risks. We'll discuss Tor in the next chapter.
- Practice basic precautions, such as never using your real name, never giving out your passwords, bank, or credit card information, and so on, while on the Deep Web.

Also, always use complex passwords or passphrases, cover your camera, and if possible, disable your microphone.

I will go into more detail in the chapter regarding best practices for accessing the Deep Web.

Installing and using a Linux VM

Here, we will be installing Ubuntu.

According to the `www.ubuntu.com` website, the required resources to install Ubuntu Desktop Edition are as follows:

- 2 GHz dual core processor
- 2 GB RAM (system memory)
- 25 GB of hard-drive space (Ubuntu can also be installed on a USB stick, memory card, or external drive)
- A monitor capable of 1024x768 screen resolution

I installed Ubuntu on a VM, but the process is the same on a PC.

For those of you that don't know what a VM is, you could say that it's a virtual computer, run by specialized software, either on your desktop or in a dedicated environment. These virtual computers are called *guests*, and they are run on a *host* OS.

I personally use VMware Workstation, but there are several out there, depending on your host OS and specific requirements.

As with most OSes, Linux can be installed from a DVD, an ISO file, or a USB flash drive. Some people even prefer running their entire OS from a USB flash drive, for enhanced security.

To install Linux from a USB flash drive, you will need software taht will make the USB stick bootable.

There are many tools you can use, and you should try several until you find one that you feel comfortable with.

I use Universal USB Installer, which is a free utility, under the GNU general public license.

To get back to our Linux installation, let's go over the general steps:

1. Obtain Linux installation media (an ISO file, for example). You can obtain one by performing a web search for any distribution you want.
2. Read the installation requirements.
3. Prepare the machine you will be installing on, either VM or physical, according to the installation requirements.
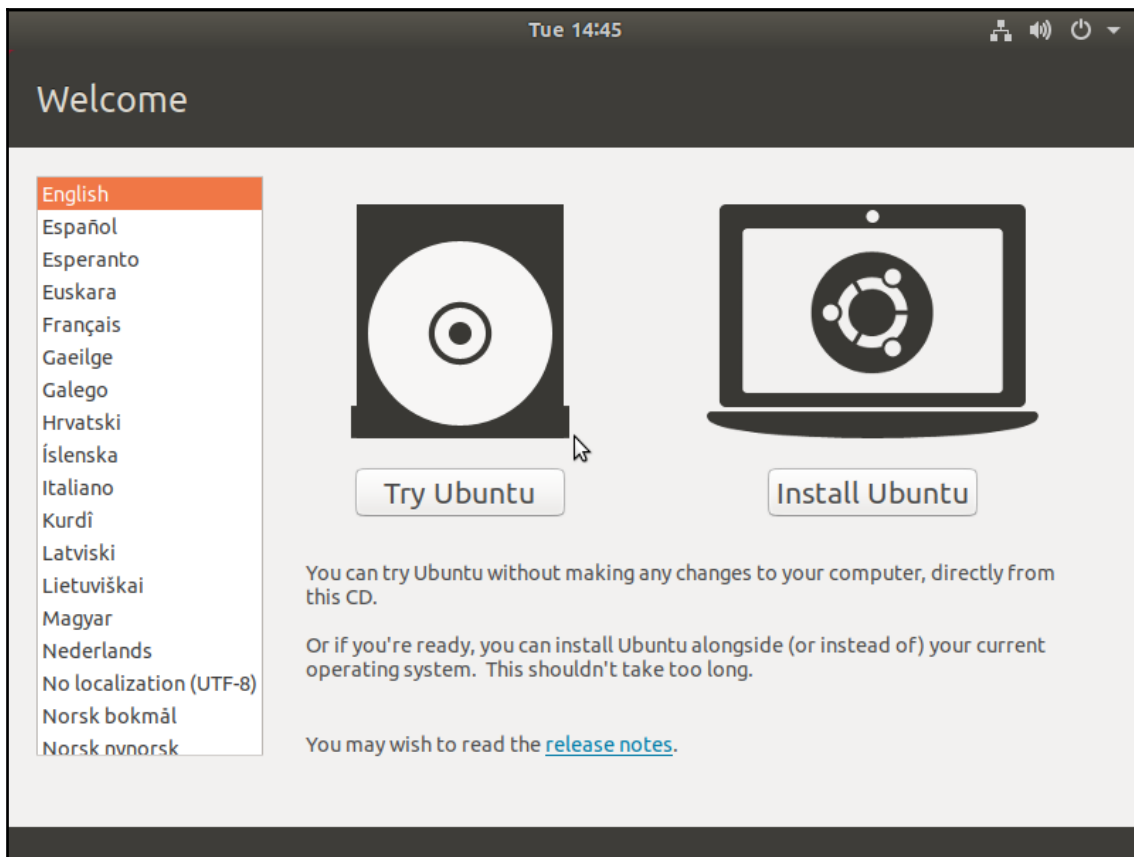4. Install from a USB flash drive, DVD, or ISO file.

Now that we have talked about the basics, let's get started.

I prepared a VM, with the required specifications, and even added more resources, to make the installed OS more efficient (and faster), as you can see here:
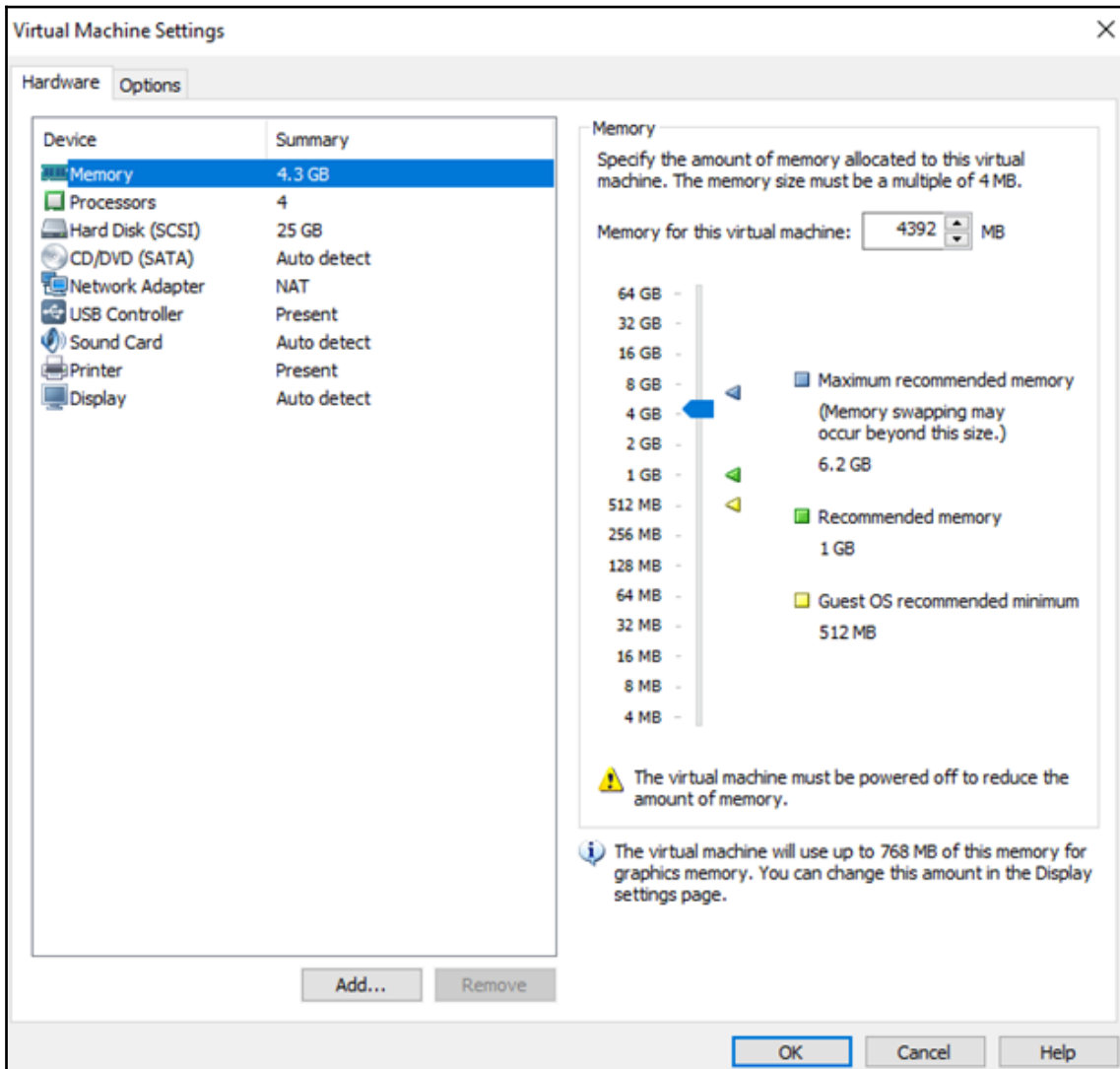
VM settings

As soon as your PC or VM boots, you will see the following on your screen:
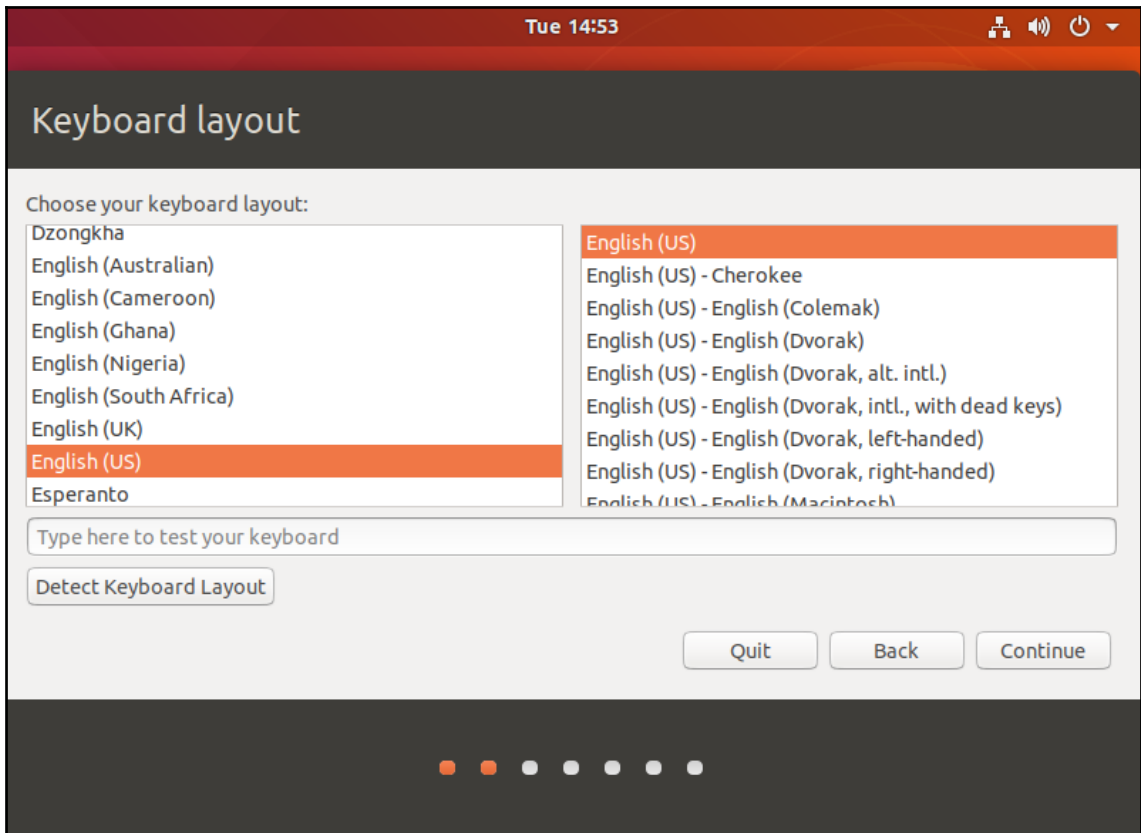

Ubuntu installation Welcome screen

Choose the language you want, and then click **Install Ubuntu**.

Another option is to boot from the CD/DVD/USB flash drive, if you click **Try Ubuntu**.

Next, you will see a screen with options for choosing your keyboard layout:

Ubuntu Keyboard layout choice screen

The next screen is for deciding whether to install the default apps and other software that you want available from the start:
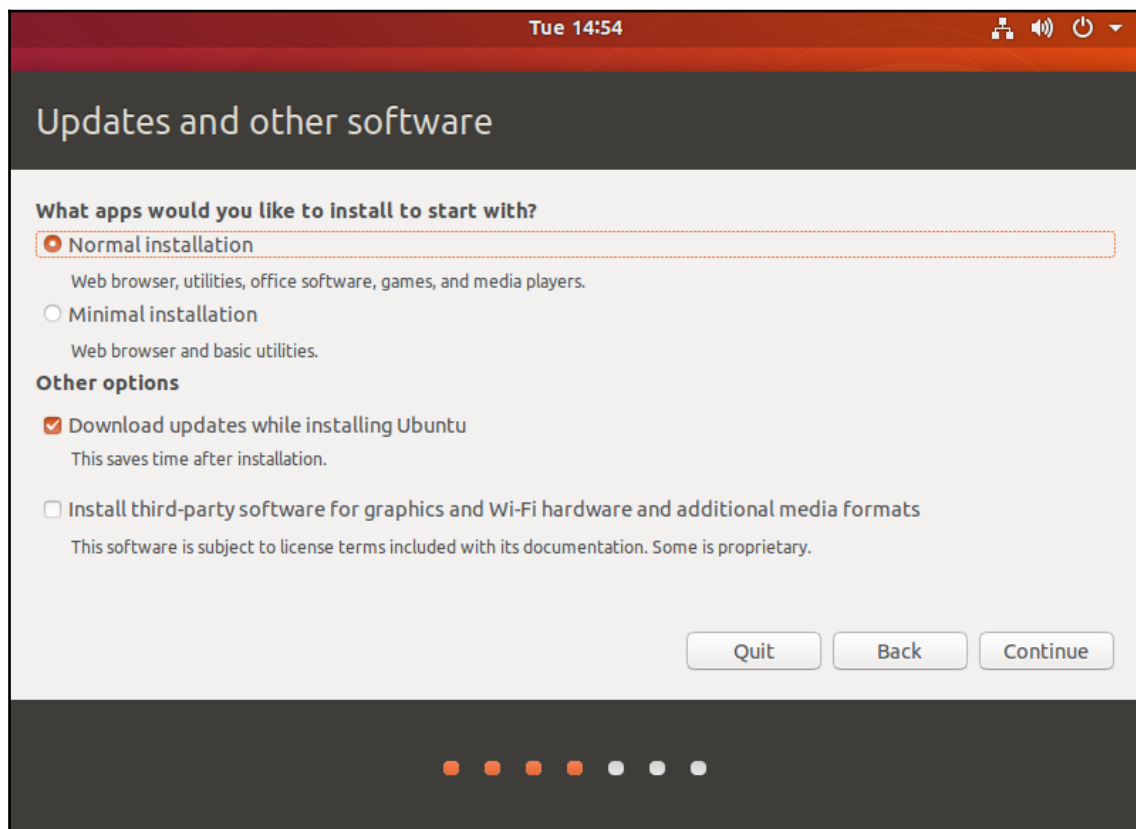
Updates and other software

The **Installation type** screen allows you to decide whether to delete any previous OSes you may have installed on the same computer, and provides the option to encrypt the new OS, and to use **Logical Volume Management** (**LVM**), for easy partition resizing and management:
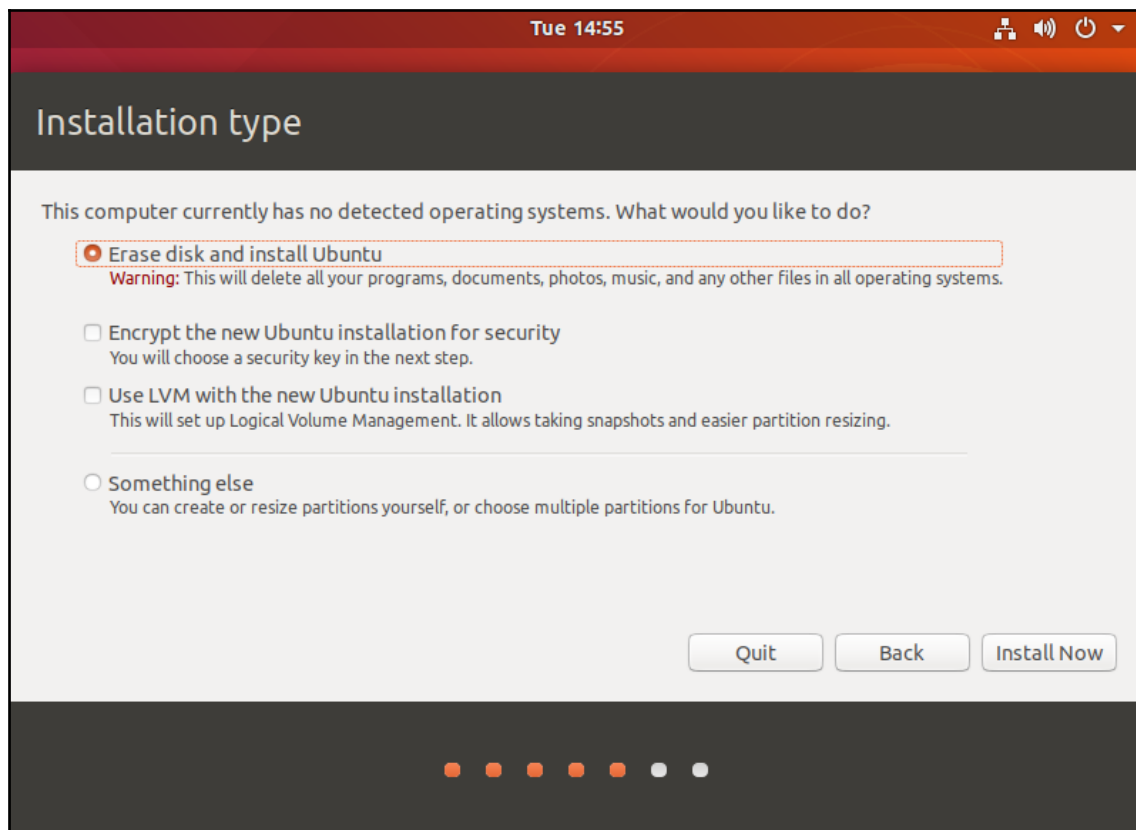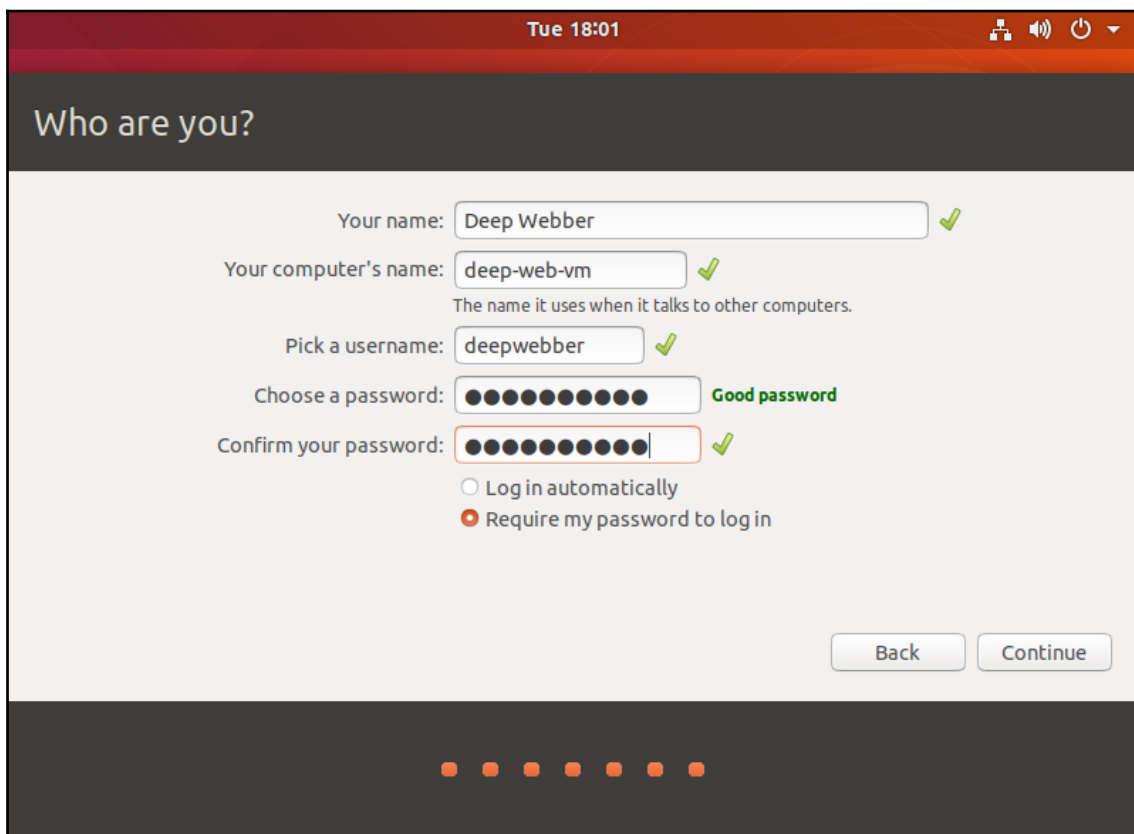
The **Where are you?** screen is basically for setting your time zone:
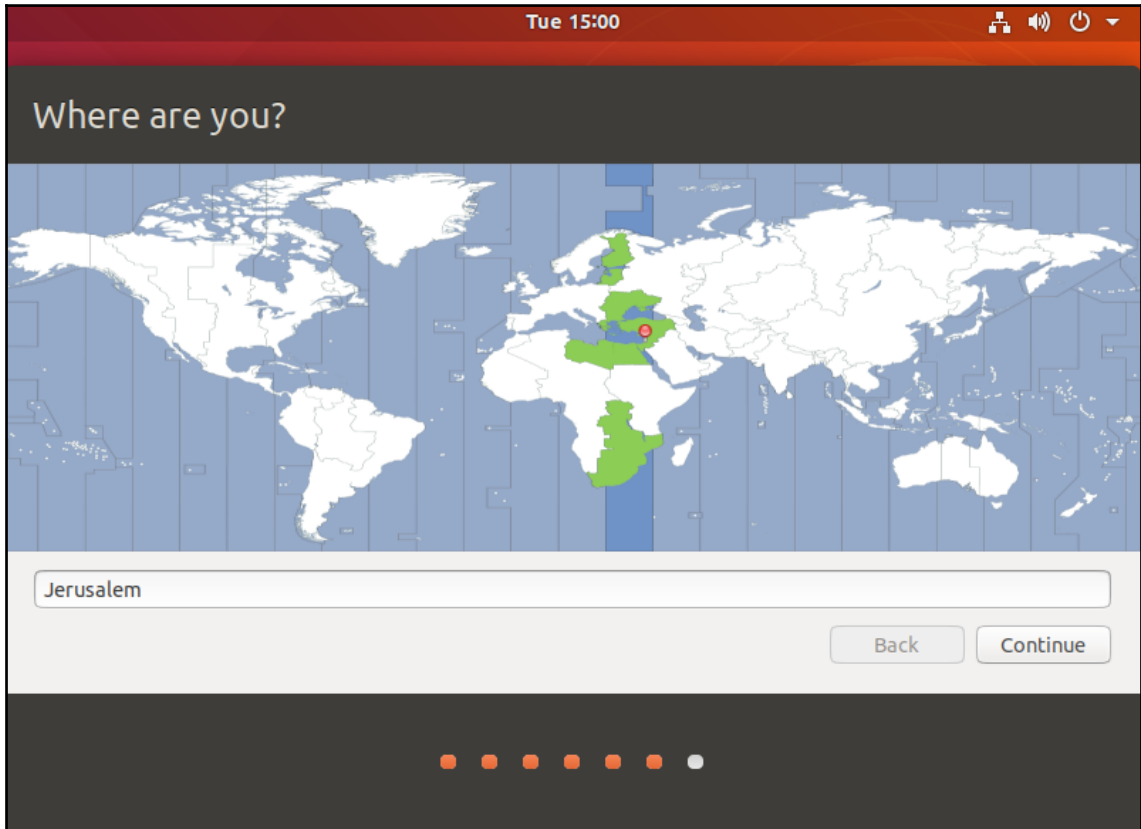
Where are you?

The **Who are you?** screen is where you provide your name (or the name that you want listed in the OS) the computer's name, a username, and a password.

Remember that you will probably use this installation to access the Deep Web. Use a handle or pseudonym in any OS you use for that purpose, for all the names you use:


Then, you'll see the installation process occur. This can take anywhere between a few minutes and an hour.

The final screen will tell you that the installation is complete, and you'll have to restart to be able to use the new installation. Do so by clicking **Restart Now**.

After the installation completes, the computer will reboot, after which, you'll reach the login screen, as displayed here:
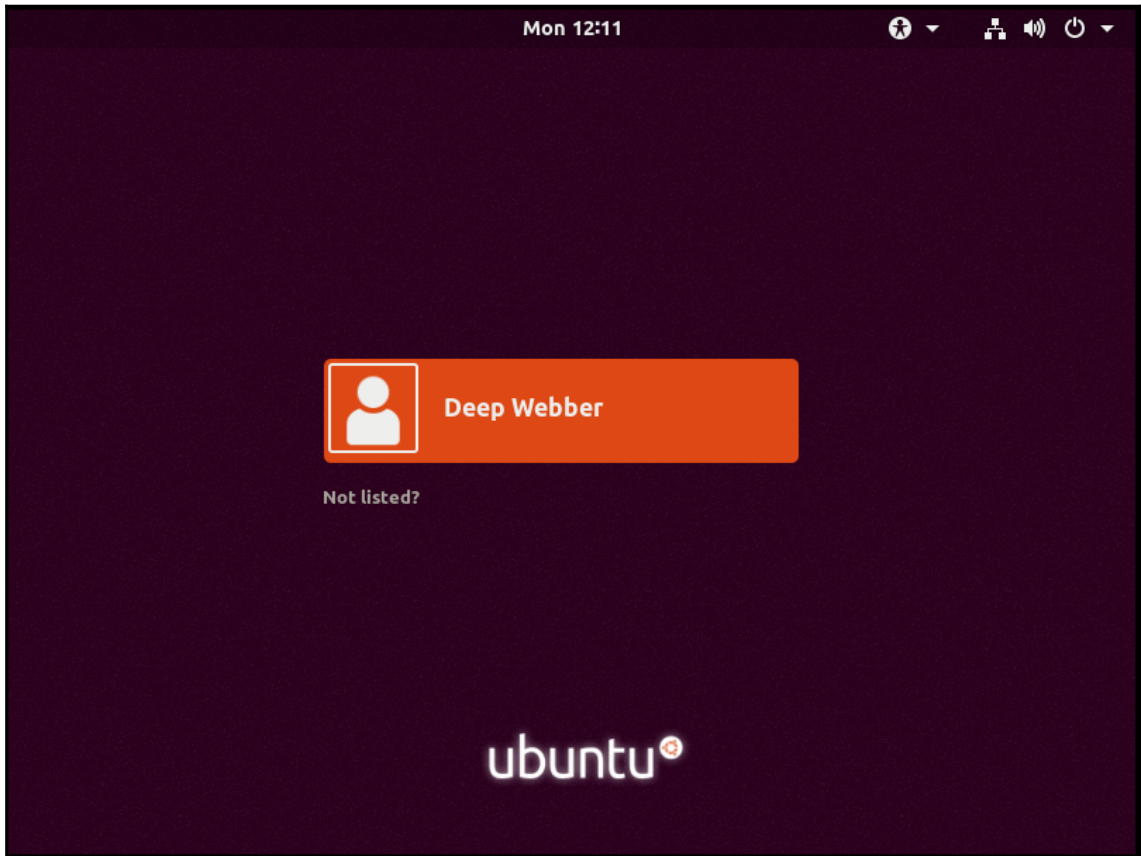
Clicking on the username will display the login box. Enter your password and click **Sign in** or press *Enter*:
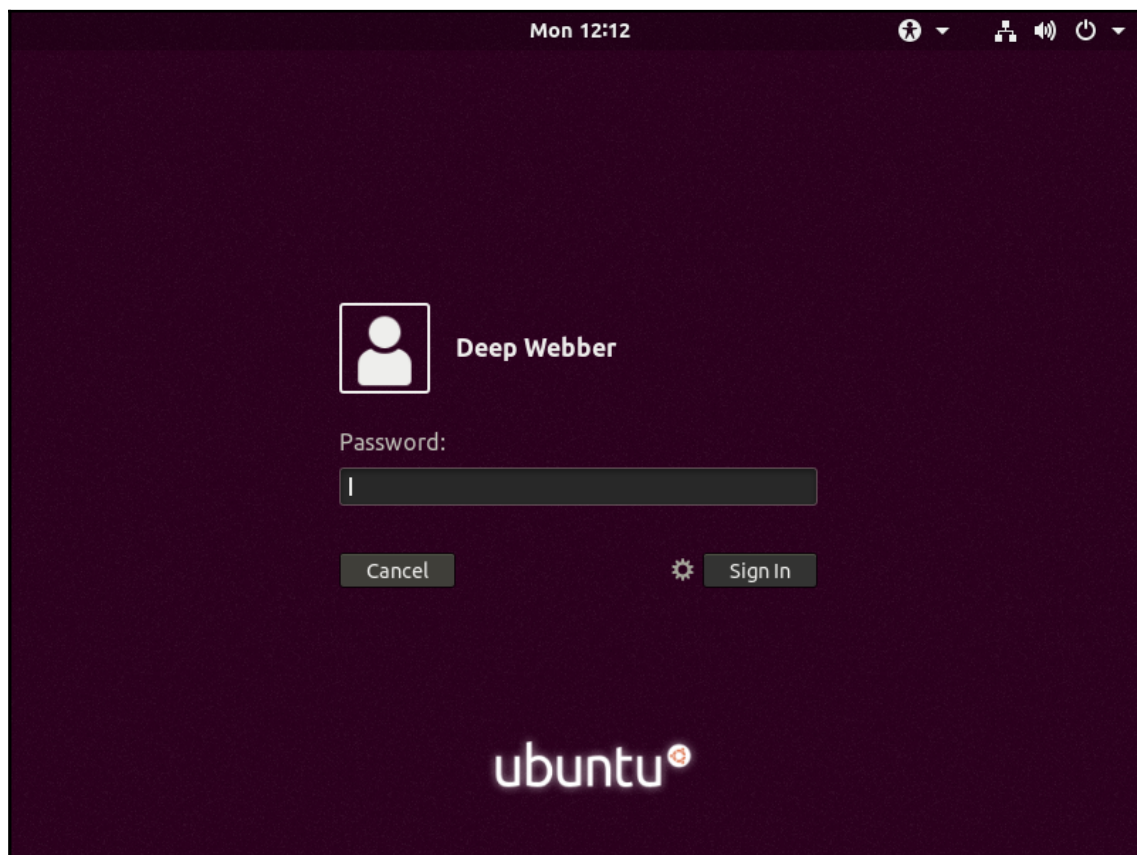
What else can we do with a Linux VM?

Now that we've installed Linux, what do we do with it?

Well, the obvious answer is install Tor browser. Yes, but that's in the next chapter. First, let's familiarize ourselves with Linux a bit.

Linux has the same basic functions as Windows—browsers, apps, OpenOffice for a productivity suite, a desktop interface, and so on, but there are so many more things you can do with Linux as an OS, from using it to run a smart home, a media center, and more.

You can completely customize Linux, by changing things such as the desktop environment, and can even customize the OS and the applications, if you're a coder, or if you develop your coding skills.

Programming is easier with Linux, with its built-in apps that can help you to read and write code. Accessing the log files of the OS, or anything you develop, is much easier with Linux, as well.

It is worth learning how the many protocols and services work, since they are so easy to install and configure in Linux.

SSH, RDP, and DNS can be installed and learned, among others.

Linux can even help you hone your proficiency using typed commands in the Terminal window. Here's where some of the real power of Linux comes into play. The ease of installing apps and configuring the OS will become apparent, after you learn the commands, such as `apt-get` and `sudo`.

You could, for example, install multiple apps or update all your installed apps, with a single command.

Running Linux from a USB flash drive

Instead of installing Linux on a computer, why not boot from a USB flash drive? What you'll actually be doing is running a temporary OS, which won't write data to the hard drive, and will *forget* whatever you did when you shut it down.

To run Ubuntu from a USB flash drive, you'll need to have a bootable live Linux USB drive, like the one you prepared for the previous chapter, to install Ubuntu on a PC.

After booting from the Linux USB drive, you'll reach the following screen:
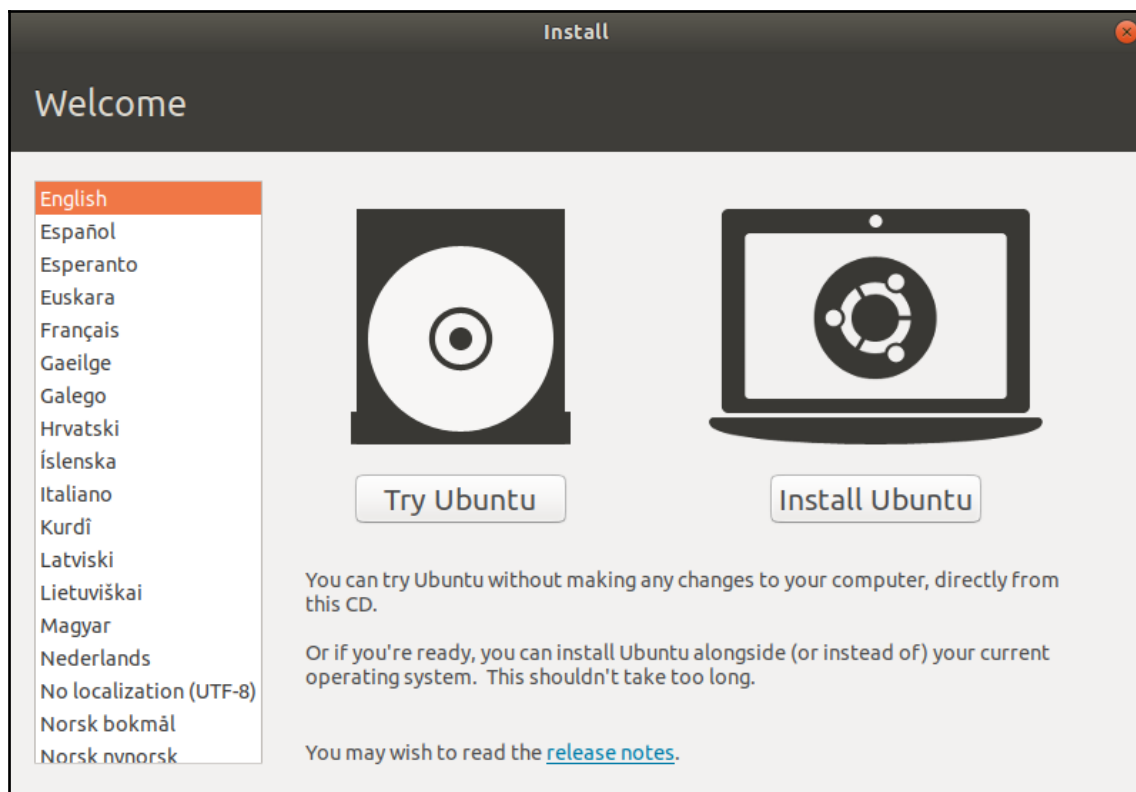
Try Ubuntu

Click **Try Ubuntu** and then Ubuntu will load without installing to the hard drive.

When you shut down the temporary OS, everything you did will be *forgotten*, providing additional security and privacy.

So, keep that in mind when deciding how to access the Dark Web. There are always multiple ways to do so, with varying levels of security. Choose what's best for you.

Summary

To sum up this chapter, Linux is a very flexible and customizable OS. With it comes a wide user base, which shares its knowledge, giving you accessible help, to perform almost anything you might want to do with it.

Play around with Linux, try out the many available distributions, and find one that is the best match for what you want to do with it. You will probably find that there is a lot of added value to it, other than using it as a simple desktop computer.

In the next chapter, we'll go over the process of installing and using the Tor browser on Linux.

Questions

1. What is Linux?
2. What is a distribution?
3. Who invented Linux?

> A. John Lin
>
> B. Linus Torvalds
>
> C. Linda Evans

Further reading

The following resources might be interesting if you'd like to delve deeper into the topics included this chapter:

- `https://www.ubuntu.com/`
- `https://www.linux.org/`
- `https://www.linuxfoundation.org/`