

# 5

## Accessing the Dark Web with Tor Browser

In the previous chapter, we installed Ubuntu Linux.

Now, we will discuss installing Tor Browser on Linux, in a few different ways, using a *standard* Linux distribution. When I say *standard*, I mean a distribution that is in common desktop use, and not a security-focused one, like the ones we will discuss in the following chapters. We'll learn how to install Tor Browser, and how to use it.

We will learn about the following topics in this chapter:

- What is Tor Browser?
- Installing Tor on Linux
- The Tor Project's recommendations on the safe use of Tor

# What is Tor Browser?

According to the Tor Project website:

*“Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.*

*The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor’s users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.”*

In other words, Tor (which is an acronym for **The Onion Router**, by the way) is a privacy focused network that hides your traffic, by routing it through multiple random servers on the Tor network.

So, instead of the packets that make up your communication with another party (person or organization), going from point A to B directly, using Tor, they will jump all over the place, between multiple servers, before reaching point B, hiding the trail.

Additionally, the packets that make up the traffic (or communication) in the Tor network are wrapped in special layers, which only show the previous server or step that the packet came from, and the next step, hiding the entire route effectively.

Tor Browser is a web browser, based on Firefox that was created for the purpose of accessing the Tor network, securely and privately.

Now, I’m going to say something that may surprise you.

Even if you use Tor, this doesn't mean that you're secure. Why is that? Because Tor Browser has software vulnerabilities, same as every other browser. It's also based on Firefox, so it inherits some of its vulnerabilities from there as well.

You can minimize attack vectors by applying common security sense, and by employing various tools to try to limit or prevent malicious activity, related to infecting Tor Browser or the host running it.

OK, let's move on to the juicy part: installing Tor on Linux.

## Installing Tor on Linux

Installing software on Linux is usually very easy. There are several ways to install Tor Browser, and as I mentioned, we'll discuss a few in this chapter.

Let's start with a *classic* installation, by accessing the Tor Project website, via a browser. The default browser that ships with Ubuntu is Firefox, which is what we'll use.

Although you might think that this would be the best way to install Tor Browser, it's actually the least secure, since the Tor Project website is continuously targeted by hackers and might have any number of security or privacy issues on it.

Instead of just downloading Tor Browser and immediately installing it (which is dangerous), you can either download the file and verify its hash (to verify that it is indeed the correct one), or you could install it through other methods, for example, via the Terminal, by using Linux commands, or from the Ubuntu Software Center.

We'll start by going over the steps to download Tor Browser from the Tor Project website:

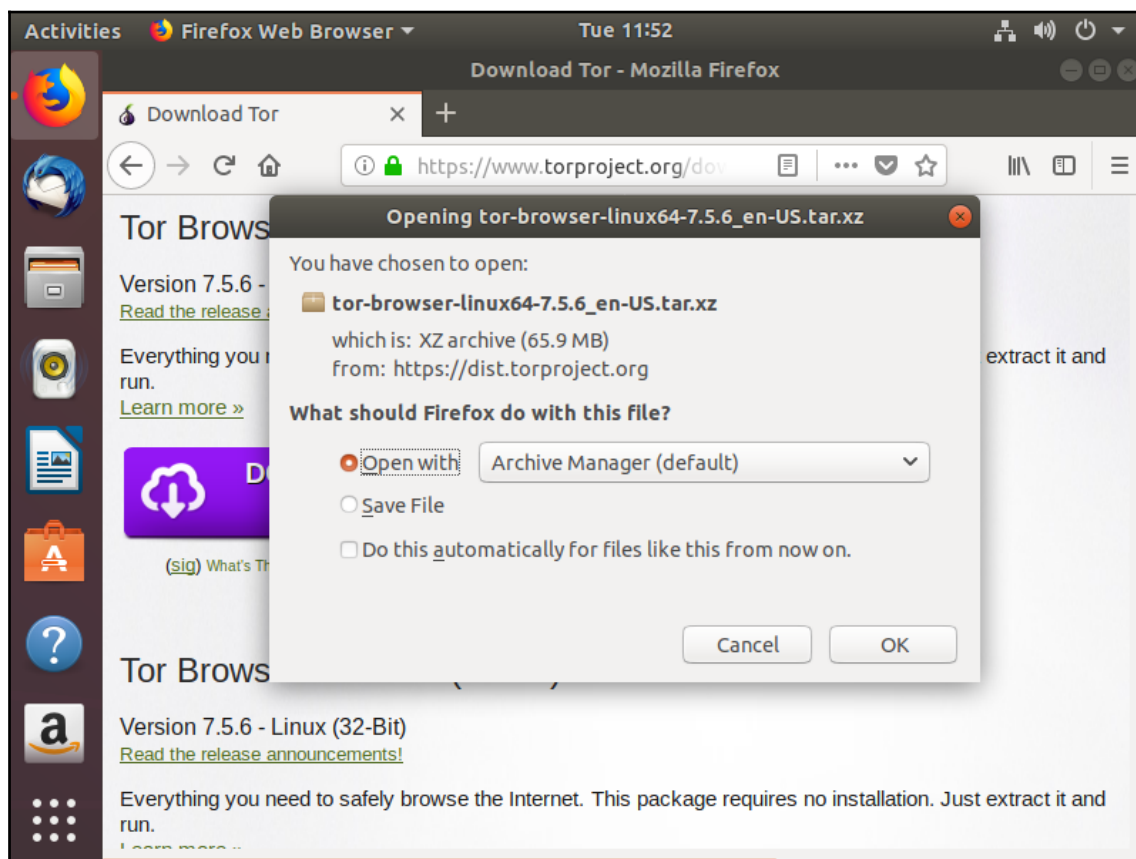
1. After booting your Linux installation, open your browser
2. Enter the following address and navigate to it: `https://www.torproject.org/download/download-easy.html.en#linux`.

Notice that the URL takes you directly to the Linux download section of the Tor Project website.

I usually prefer this direct method, rather than starting with Google (or any other search engine), searching for Tor, and then accessing the Tor Project website, since, as you may know, Google collects information about users accessing it, and the whole idea of this book is to maintain our privacy and security. Also, always verify that you're accessing the Tor Project website via HTTPS.

3. Choose the correct architecture (32 or 64 bit), and click the **Download** link.

4. You'll be able to choose what you want to do with the file—open it with Ubuntu's Archive Manager, or save it to a location on the disk:



Downloading Tor Browser

Again, the quickest way to go would be to open the compressed file, but the more secure way would be to download the file and to verify its hash, before doing anything else.

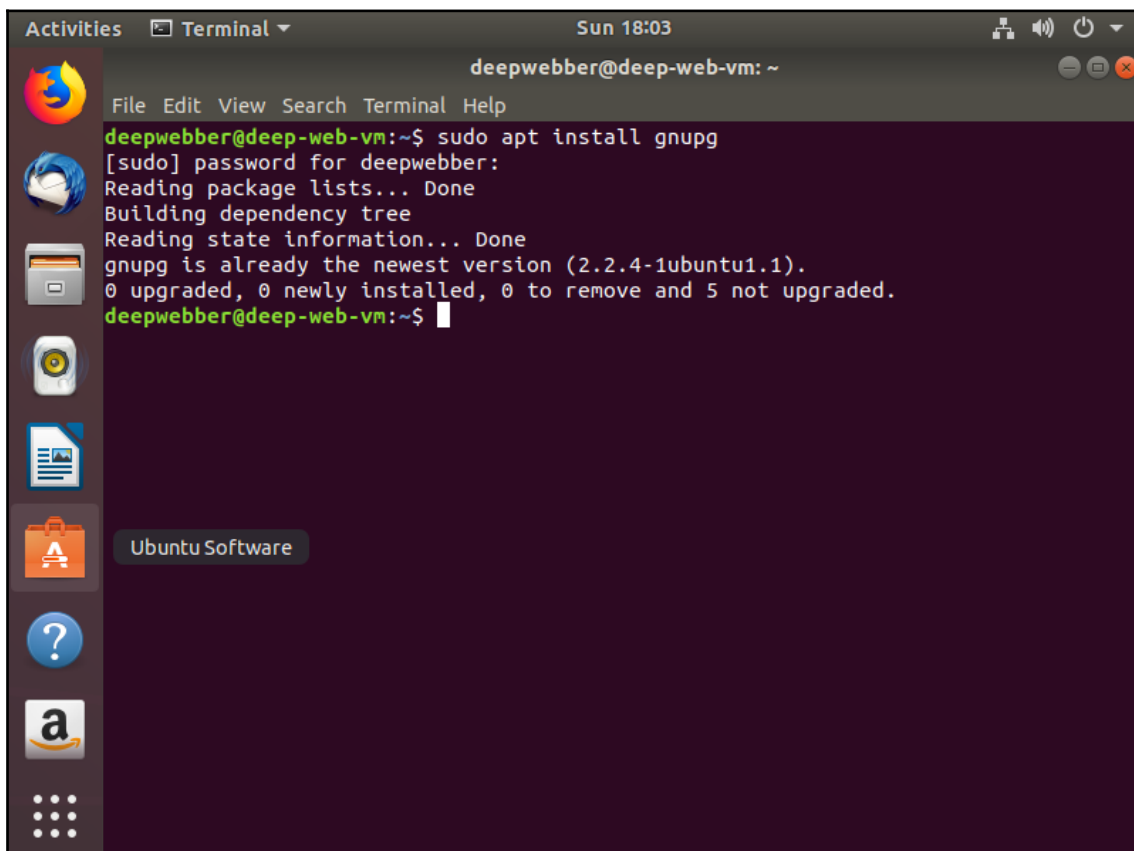
The Tor Project provides **GNU Privacy Guard (GPG)** signature files, with each version of Tor Browser. You will need to install GnuPG on your Linux OS, if it isn't there already, in order to be able to verify the hash of the browser package.

To do so, just open the Terminal and type in the following:

```
sudo apt install gnupg
```

Enter your password when required, and the installation will commence.

Most Linux installations already include `gnupg`, as can be seen in the following screenshot:

A screenshot of a terminal window titled 'Terminal' with a dark background. The prompt is 'deepwebber@deep-web-vm: ~'. The user has entered the command 'sudo apt install gnupg'. The terminal output shows the password prompt, package list reading, dependency tree building, and state information reading, all completed successfully. It then reports that 'gnupg is already the newest version (2.2.4-1ubuntu1.1)' and that '0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded'. The prompt returns to 'deepwebber@deep-web-vm:~\$'. On the left side of the terminal window, there is a vertical dock with various application icons, including Firefox, a mail client, a file manager, a disk utility, a document viewer, a software center (labeled 'Ubuntu Software'), a help icon, and an Amazon logo. The top of the window shows 'Activities', 'Terminal', and the date/time 'Sun 18:03'.

Installing GnuPG

After installing GnuPG, you need to import the key that signed the package. According to the Tor Project website, the Tor Browser import key is `0x4e2C6e8793298290`.

The Tor Project updates and changes the keys from time to time, so you can always navigate to: <https://www.torproject.org/docs/verifying-signatures.html.en> to find the current import key, if the one in the book doesn't work.

The command to import the key is as follows:

```
gpg --keyserver pool.sks-keyservers.net --recv-keys 0x4e2C6e8793298290
```

This is followed by this:

```
gpg --fingerprint 0x4e2c6e8793298290
```

This will tell you whether the key fingerprint is correct.

You should see the following:

```
deepwebber@deep-web-vm:~$ gpg --fingerprint 0x4e2c6e8793298290
pub  rsa4096 2014-12-15 [C] [expires: 2020-08-24]
    EF6E 286D DA85 EA2A 4BA7 DE68 4E2C 6E87 9329 8290
uid          [ unknown] Tor Browser Developers (signing key) <torbrowser@torproject.org>
sub  rsa4096 2016-08-24 [S] [expires: 2018-08-24]
sub  rsa4096 2018-05-26 [S] [expires: 2020-09-12]

deepwebber@deep-web-vm:~$
```

Verify key fingerprint

Now, you need to download the `.asc` file, which is found on the **Tor Browser Downloads** page, next to the relevant package of the browser (it appears as `sig`, short for signature):

Tor Browser Downloads			
To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.			
Stable Tor Browser			
Language	Microsoft Windows (7.5.6)	Apple MacOS (7.5.6)	GNU/Linux (7.5.6)
English (en-US)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
العربية (ar)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Deutsch (de)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Español (es-ES)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
فارسی (fa)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Français (fr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)

ASC file location

You can find the Tor Browser download page here: <https://www.torproject.org/projects/torbrowser.html>

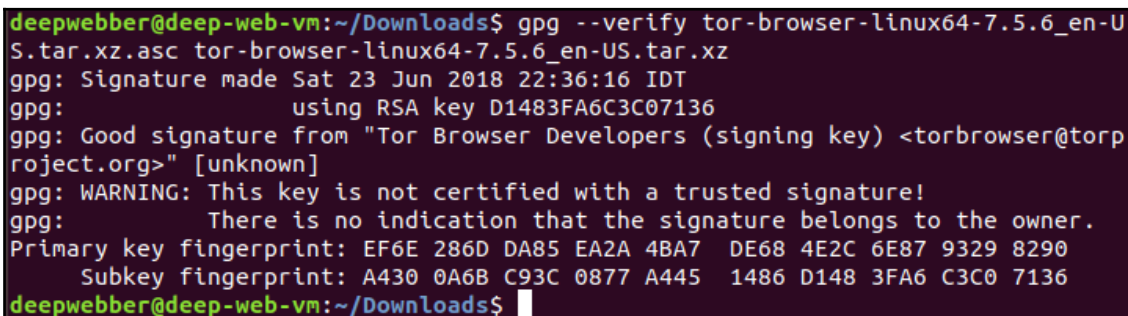
Now, you can verify the signature of the package, using the ASC file.

To do so, enter the following command in the Terminal:

```
gpg --verify tor-browser-linux64-7.5.6_en-US.tar.xz.asc tor-browser-  
linux64-7.5.6_en-US.tar.xz
```

Note the 64 that I marked in bold. If your OS is 32-bit, change the number to 32.

The result you should get is as follows:



```
deepwebber@deep-web-vm:~/Downloads$ gpg --verify tor-browser-linux64-7.5.6_en-U  
S.tar.xz.asc tor-browser-linux64-7.5.6_en-US.tar.xz  
gpg: Signature made Sat 23 Jun 2018 22:36:16 IDT  
gpg:                using RSA key D1483FA6C3C07136  
gpg: Good signature from "Tor Browser Developers (signing key) <torbrowser@torp  
roject.org>" [unknown]  
gpg: WARNING: This key is not certified with a trusted signature!  
gpg:                There is no indication that the signature belongs to the owner.  
Primary key fingerprint: EF6E 286D DA85 EA2A 4BA7  DE68 4E2C 6E87 9329 8290  
Subkey fingerprint: A430 0A6B C93C 0877 A445  1486 D148 3FA6 C3C0 7136  
deepwebber@deep-web-vm:~/Downloads$
```

Verifying the signature

After verifying the hash (signature) of the Tor Browser package, you can install it.

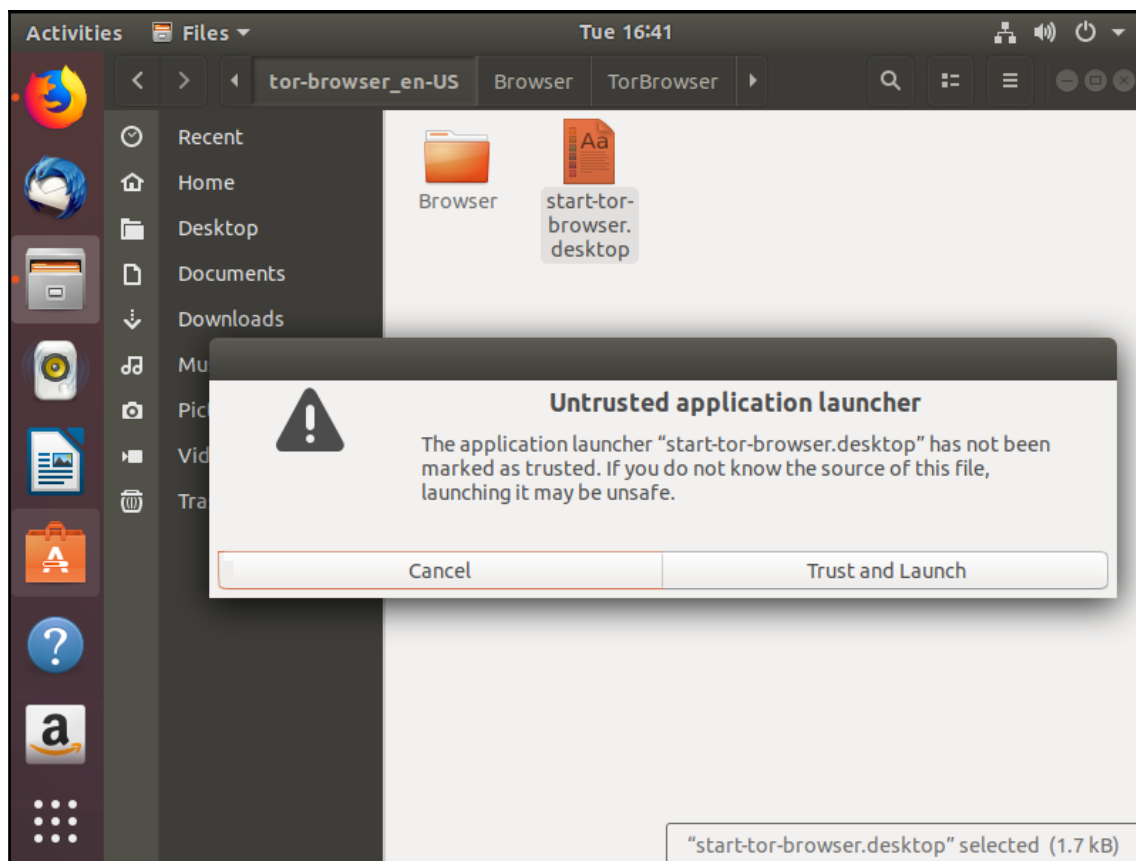
You can do so by either:

- Double-clicking the Tor Browser package file (which will open up the Archive Manager program), clicking **Extract**, and choosing the location of your choice.
- Right-clicking the file and choosing **Extract here** or **Extract to** and choosing a location.

After extracting, perform the following steps:

1. Navigate to the location you defined.
2. Double-click on the `Start-tor-browser.desktop` file to launch Tor Browser.

3. Press **Trust and Launch** in the window that appears:



Launching Tor

Notice that the filename and icon changed to **Tor Browser**.



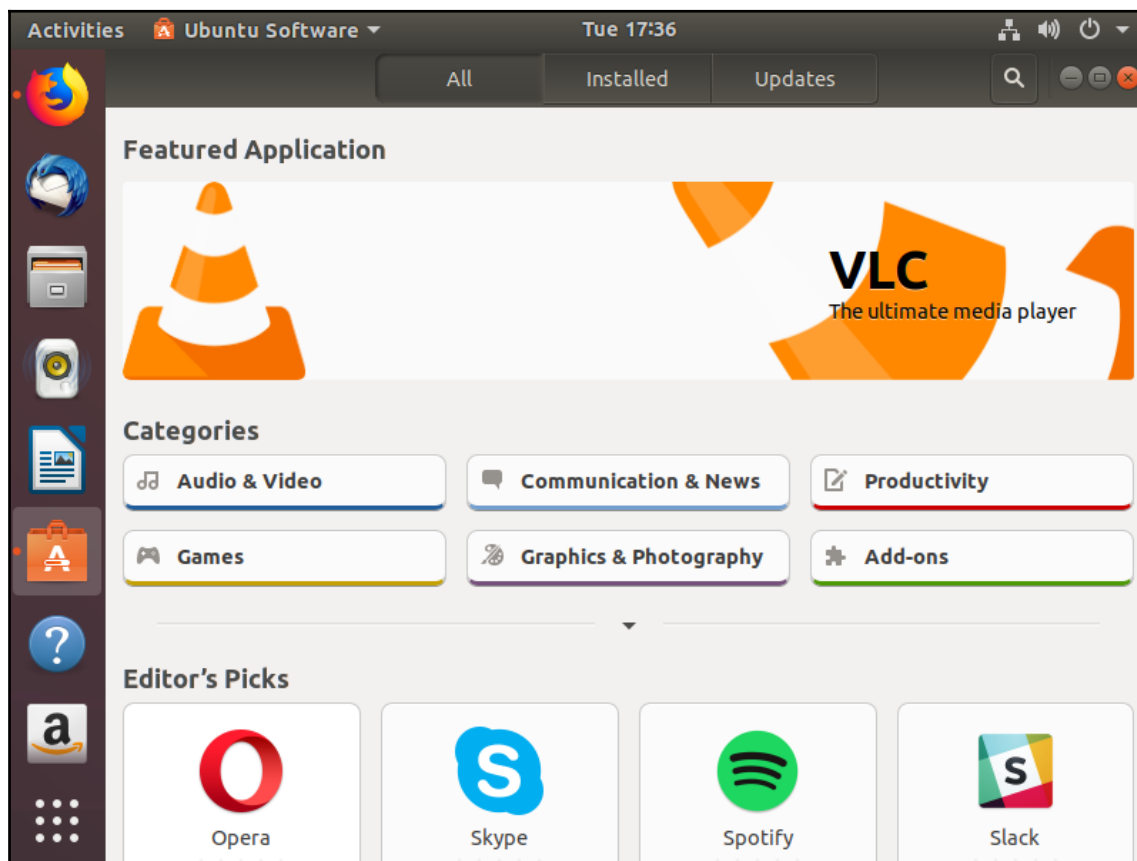
4. Press **Connect** and you will be connected to the Tor network, and will be able to browse it, using Tor Browser:



Connecting to Tor

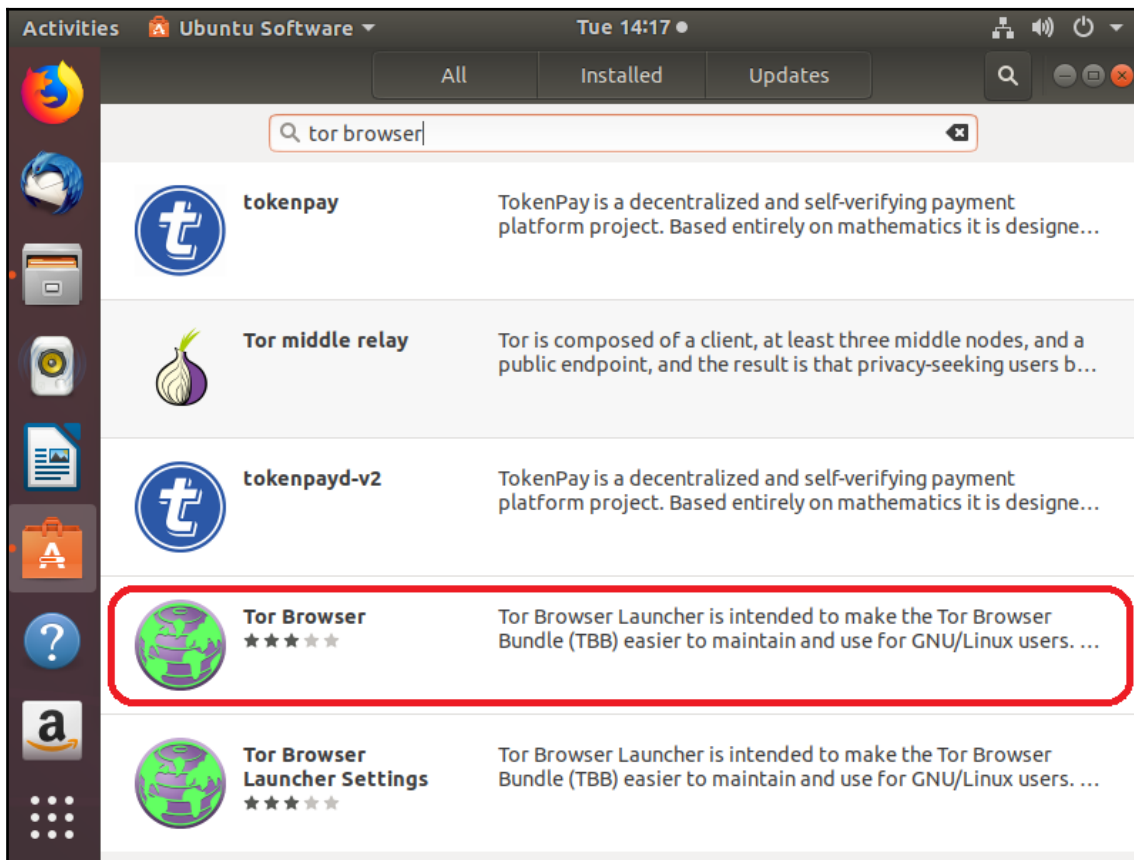
Before we discuss using Tor Browser, let's talk about alternative ways to install it, for example, by using the Ubuntu Software application.

1. Start by clicking on the Ubuntu Software icon:



Ubuntu Software

2. Search for Tor Browser, then click on the relevant result:



Tor Browser in Ubuntu Software

3. Then, click **Install**.
4. After entering your password, the installation process will start. When it ends, click **Launch** to start Tor Browser.

## Installing Tor Browser via the Terminal, from the downloaded package

Another way to install Tor is to use commands, via the Terminal.

There are several ways to do so, as follows:

1. First, download the required Tor Browser package from the website
2. Verify the download, as we discussed before, and then keep the Terminal open
3. Navigate to the location where you downloaded Tor, by entering the following command:

```
cd path/Tor_Browser_Directory
```

For example, note the following:

```
cd /downloads/tor-browser_en_US
```

4. Then, launch Tor Browser by running the following:

```
./start-tor-browser.desktop
```



Never launch Tor as root (or with the `sudo` command).

## Installing the Tor Browser entirely via the Terminal

Next, we'll discuss how to install Tor entirely via the Terminal:

1. First, launch the Terminal, as before.
2. Then, execute the following command:

```
sudo apt install torbrowser-launcher
```

This command will install Tor Browser.



We need root access to install an app, not to launch it.

3. You can then run Tor by executing the following command:

```
./start-tor-browser.desktop
```

## Tor Project recommendations on the safe use of Tor

The following is taken from the Tor Project website (<https://www.torproject.org/projects/torbrowser.html.en>), and are their recommendations on how to stay safe while using Tor.

1. Use Tor Browser.
2. Don't torrent over Tor.
3. Don't enable or install browser plugins.
4. Use HTTPS versions of websites.
5. Don't open documents downloaded through Tor while online.
6. Use bridges and/or find company.
7. Tor attempts to prevent attackers from learning what websites you browse to. But, it doesn't prevent anybody watching your traffic from detecting that you're using Tor. You can reduce this risk by using a Tor bridge relay, (<https://www.torproject.org/docs/bridges.html.en>), rather than connecting directly to the public Tor network.

But, before firing up Tor Browser, let's remember a few important things about accessing the Dark Web, or even surfing the internet, using Tor Browser. Your ISP (and thus your government or the NSA) will be able to detect you're using Tor Browser. This can draw the attention of the powers that be to yourself, and naturally, we don't want that. So, to prevent this, we need to use a **Virtual Private Network (VPN)**. To use a VPN, you need to install a VPN client on your computer.

A VPN provides additional privacy and security, while Tor Browser provides anonymity. Combined, you are as protected as you can be without extreme measures.

The question arises—which VPN should I use?

Well, there are several basic guidelines you should follow when choosing a VPN:

- First, the encryption level. 128-bit is OK, but 256-bit encryption is much better (much harder to crack).
- Also, choose a VPN that doesn't save logs, either locally or on the VPN provider's servers.

- One of the issues that many VPNs face is unexpected disconnections, which can expose your IP address to the ISP, or the world, so remember to choose one that has a kill switch (if you remember, I explained about this in *Chapter 4, Installing a Linux Virtual Machine*; it's a mechanism that disconnects the computer's internet connection, if the VPN disconnects unexpectedly).
- Choose a VPN that is designed to prevent IP and DNS leaks (operating system and browser vulnerabilities can leak, or expose, your DNS requests and IP address, if not prevented).
- Choose a VPN that provides IP addresses from other countries (and choose a country different than your own when configuring it).

There are many free and paid VPNs out there. Their installation may vary, but each will provide own instructions. Just be sure to obtain one that has the capabilities I've mentioned.

Okay, now that we've seen how we can install Tor Browser and understand that we need a VPN (and have hopefully chosen one), let's start using Tor Browser.

Start Tor Browser, using any of the options listed previously. After you reach Tor Browser's home page, you can navigate to sites on the Dark Web. These sites are in the `.onion` domain (for example, <https://darkwebsite.onion>).

You can also surf *regular* internet sites, but, they will function sluggishly, due to the routing that the Tor network performs, and the fact that cookies, scripts, add-ons, and other extensions that usually work in our regular browsers don't work in Tor Browser.

But, if used correctly (VPN + taking precautions), you can stay anonymous on the internet (and the Dark Web, of course).

Remember that Tor Browser is a web browser, like Chrome, Firefox, Edge, Internet Explorer, but much more private and anonymous, so you can perform all the same basic actions.

Here is a list of a few `.onion` sites you can start with:

- <https://www.facebookcorewwi.onion/>

Yes, it's Facebook.

Facebook provides this for use in countries that censor using it (not really for anonymity):

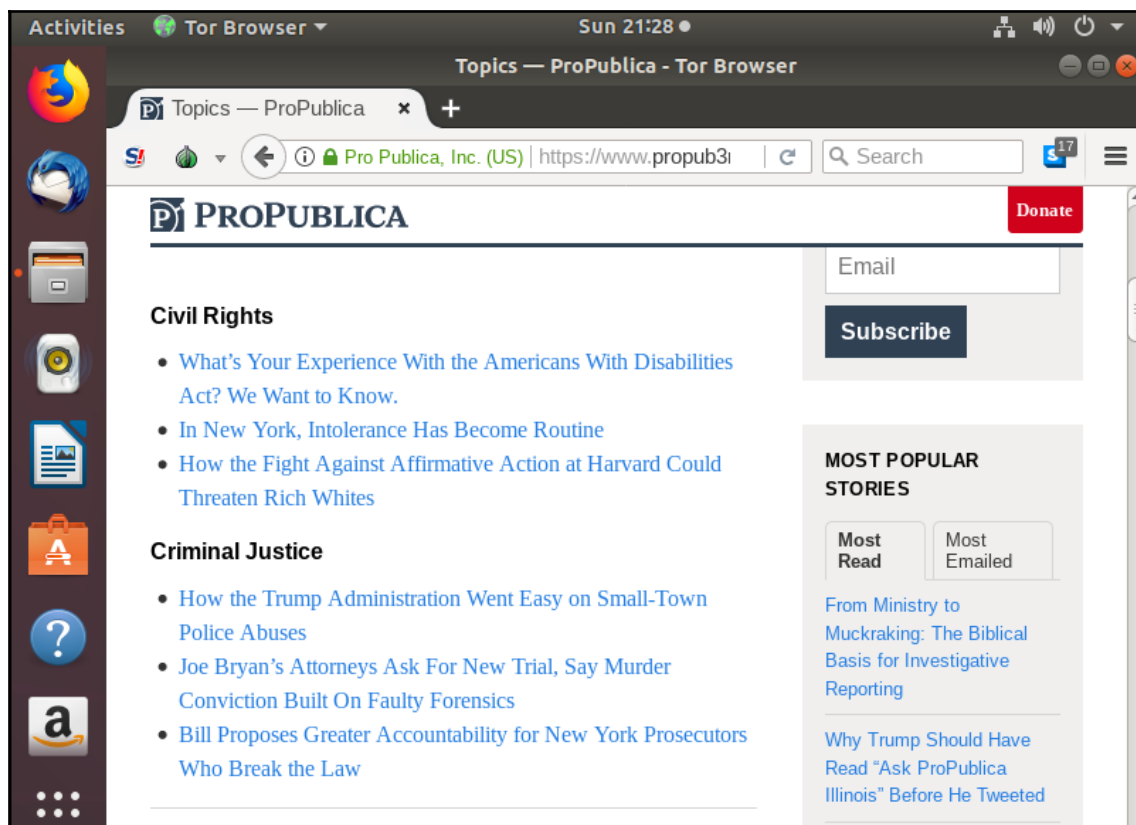
- <http://3g2upl4pq6kufc4m.onion/>

An excellent, private, alternative to Google. Search behavior and activity isn't logged, so the search experience is a little different (more like a pre-Google era search experience):

- <https://www.propub3r6espa33w.onion/>

The first online publication that won a Pulitzer prize also has a .onion domain. There, you can find many articles and information, published both anonymously and publicly, about many, many topics.

Here, you can see a screenshot of the Propublica site, as accessed via Tor Browser:



Propublica

The Hidden Wiki: think of this as Wikipedia with all stops removed. A lot of information is available at [http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\\_Page](http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)

There are also Dark Web search engines, such as the following:

- **Tor Onionland:** Search engine with close to 60,000 .onion websites and almost 5 million indexed pages. (<http://onionlandbakyt3j.onion/>)
- **Torch:** Search engine with almost 500,000 indexed .onion services. (<http://xmh57jrzrnw6insl.onion/>)
- **Not Evil:** Search engine with over 32 million .onion indexed links. (<http://hss3uro2hsxfogfq.onion/>)
- **Candle:** A basic search engine that completely ignores operators, parentheses, and quotes; just words. (<http://gjjobqjj7wyczbqie.onion.link/>)
- **Grams:** Market search engine only for finding labor, digital, and physical items you can purchase with Bitcoin and other currencies. (<http://grams7enqfy4nieo.onion/>)
- **Haystak:** Searches .onion services and claims to have more than 1.5 billion pages from almost 300,000 websites (many are already obsolete). (<http://haystakvxad7wbk5.onion/>)

Many of the sites listed may not work when you try them. This happens since their addresses change frequently. But, I listed them to help you get on your way, browsing the Deep Web. The best way to learn how to access the Dark Web is simply by doing so.

So, what are you waiting for?

## Summary

In this chapter, we talked about Tor, Tor Browser, how to install it in several ways, and how to use it.

In the next few chapters, we'll talk about several privacy- and security-focused operating systems that can be used to access the Dark Web in a safe (relatively, anyway) manner.



## Questions

1. List at least four recommendations for safe use of Tor Browser.
  - A. Use Tor Browser.
  - B. Don't torrent over Tor.
  - C. Don't enable or install browser plugins.
  - D. Use HTTPS versions of websites.
  - E. Don't open documents downloaded through Tor while online.
  - F. Use bridges and/or find company.
2. Tor Browser is based on which of the following browsers?
  - A. Chrome
  - B. Internet Explorer
  - C. Edge
  - D. Firefox
  - E. Opera
  - F. Safari
3. What is the Terminal command to start Tor Browser?

## Further reading

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

- <https://www.torproject.org/projects/torbrowser.html.en>