## What is Torrenting?

Torrent and BitTorrent are used synonymously by many but are they actually the same thing? In reality, there is a difference between the two but they can be used interchangeably. Torrent is a file that contains metadata about the content you are about to download. On the other hand, BitTorrent is a file transfer protocol that works to breaks down large chunks of shared file into smaller pieces.

The beauty of this protocol is that you download the original file from the source and from other users as well. This makes the overall process smooth, fast, and streamlined. For instance, if you are downloading your favorite movie through a torrent, you are not only downloading the entire file from the source but also from other torrent users as well.

## How Do Torrents Work?

Torrents work is in a decentralized manner. Every user downloads and uploads the torrent file, making entire process more efficient. Here is an illustration (courtesy Wikipedia) showing how torrents work:

The figure shows seven clients (users) and one seed (the large system in the bottom). The original file is initially transferred from the seed to each client only once. The file is then transferred piece by piece between different clients. Each color represents a specific piece of the file being transferred; showcasing simultaneous upload and download.

For all torrent newbie’s, there are certain terminologies that you will come across when you use torrents. To help you out, here are some of these terminologies explained:

* **Peers:** It is a generic term used for any client (user) that is involved in file sharing in a peer-to-peer (P2P) network.
* **Swarms:** A collection of peers that are sharing (downloading & uploading) the same torrent are called swarms.
* **Seeders:** When you are downloading and simultaneously uploading a torrent, you are a seeder.
* **Leechers:**When you are only downloading but have disabled uploading, then you’re a leecher. Many trackers ban users who disable uploading. From an ethical standpoint, it is a good practice to upload the same amount that you download.
* **Indexers:**Websites that compile torrents and provides information about torrents are called indexers. They also act as a forum where you can find, share, download, or request for torrent files.
* **Trackers:** They are the servers that help to direct data packets between peers and also aid in finding other peers in the network. You can imagine them as bridges between different torrent users, helping in smooth and fast transfer of data by routing small pieces of files between each torrent downloader and uploader.
* **BitTorrent Clients:**Programs that enable file transfer using BitTorrent protocol are called BitTorrent clients. You can use them to manage your torrent files while the clients handle all the download and upload, connecting to peers, and providing you statistics about the torrent. Secondly never forget to use BitTorrent VPN for torrenting.

## Steps to Use Torrents

Using torrents is very simple and not complicated as it may sound. To demonstrate how easy it is to use torrents, follow our steps:

### Step 1: Download a Torrent Client

The first step towards using torrents is by downloading and installing a torrent client on your desired platform. There are many torrent clients that you can use. We have used uTorrent for our demonstration on Windows PC. uTorrent is also compatible on Mac and Linux operating systems and it is very easy to use; not to mention it is also free. You can also choose from other torrent clients such as BitTorrent, Deluge or Transmission.

### Step 2: Look Up & Download the Torrent File

Now that you have downloaded the torrent client, the next step is to search for the torrent and download that file. There are many torrent websites (indexers) that you can use to search for torrent files.

After you have searched and found the torrent you were looking for, download the torrent file. You can also click on the ‘magnet’ icon listed next to the download option. This way you don’t have to download the ‘.torrent’ file. Instead, you be will automatically promoted to choose a torrent client of your choice.

### Step 3: Add the Torrent File to the Client

Once you have selected the torrent client you want to use (uTorrent in our case), it’s time to add the torrent file to your BitTorrent client. Select the drive (or path) where you want to save the downloaded files. You can also choose the files you want to download via torrent and any other instructions you have for the BitTorrent client.

After you have selected the file you want to download and the path where you want to save the downloaded files, click ‘OK’ to add the torrent file. Once the file is added to the BitTorrent client, it will start downloading.

In uTorrent client, you can control certain features such as pausing the torrent, starting the download of the paused torrent files, adding more torrents using the ‘+’ sign, or deleting torrent files. You can also move torrents up or down the queue (using the arrows) to select their priority.

Torrent files at number 1 will have a higher priority than the torrent file at number 2. The uTorrent client also gives you additional information such as the peers you’re connected too, trackers, the download and upload speeds, and other information.

## Torrenting Visualized

If you evaluate the torrenting process in detail, you will know how this process starts and ends. From the image given below, you can explore four major attributes, and these are:

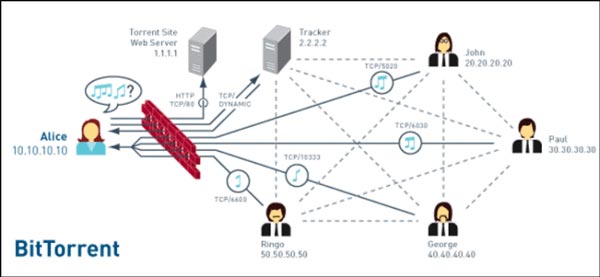
* Alice
* Torrent Site Web Server
* Tracker
* The Beatles

In this example, you are shown as Alice who wants to download files by the help of torrent network. It means you are working as seeder and a leecher trying to access the torrent site web server in the example. Now, you are able to obtain your required torrent file or magnet link. You just copy the link and open the torrent download through your torrent client.

Thus, the torrent client connects to the tracker servers and starts looking where it can place the file Alice wishes to download. Furthermore, the torrent tracker identifies John, Paul, George, and Ringo on the network. The torrent tracker recognizes all of them as the file Alice is trying to find.

After recognizing, the torrent tracker starts working with Alice’s torrent client to download the file. Now, Alice has started downloading the file from the network. She is also sharing the file with the other users. It means any file she has downloaded partially is also accessible to others.

If she has downloaded half of the file, the other users like Paul, Ringo and George can begin leeching it from her. In addition, if the other users are looking for a file that Alice already possesses. She can start seeding the file on the network. However, the file needs to be properly placed on her system.



## Streaming vs. Torrenting

Fortunately, or unfortunately, there are users who have found different ways of watching their preferred content online. This is because streamers are opting to use famous streaming services like Kodi and Popcorn Time instead of downloading the whole files from BitTorrent.

Hence, they may find themselves in the hot water of legal trouble. When it comes to online protection, you will not find much difference between streaming and torrenting.

The streaming service like Kodi uses third party add-ons that fetch content from torrents and other sources. Thus, if you stream content on Kodi, you should connect to a VPN service to safeguard your online privacy.

The same goes for Popcorn Time that has become a first choice for torrent users worldwide. The multimedia server also uses torrents to provide video content that includes TV shows and movies. As a result, you may get copyright trolls in the form of DMCA notices from copyright holders. Thus, you are bound to use a VPN when you need to watch content on Popcorn Time.

## Is Torrenting Illegal or Legal?

Now that you know **what is torrenting**, how it works and how to use a torrent, here is a question asked by many users around the world: is using torrents illegal or legal? The answer to this question depends from case to case. In certain countries, torrenting is completely legal while in others its considered illegal.

For instance, in Switzerland the use of torrents is legal as long as the material downloaded is not used to make profit. Therefore, you can download all forms of content (even copyrighted material). Similarly, in other countries such as Spain and Netherlands, torrenting is legal (to some extent). While in other regions such as Mexico, there are no laws protecting copyrights or intellectual properties; making them a safe place to for torrenting.

That said, majority of the regions frown upon the use of torrents and have deemed them as illegal. In general, torrenting is considered illegal where there are laws protecting intellectual properties and copyrights. These regions have implemented strict penalties on anyone found guilty of infringing copyrights through torrents. Users may receive warnings from ISPs, DMCA notices, fines, and even lawsuits.

## How to Perform Safe Torrenting?

When you are torrenting, one of the ways you get caught is by exposing your true location (IP address) while seeding. This is because of the way torrents work – anyone can see who and from where the file is being shared. Secondly, if your ISP logs all your internet usage activities then you can also get into trouble while using torrents.

To perform torrenting safely and securely, you should hide your IP address from copyright trolls and encrypt all your internet traffic. One of the tools for performing this task is by using a VPN for torrent. A VPN makes you anonymous by spoofing your true identity (IP address) and encrypting all your web traffic through secure protocols and encryption keys.

## Conclusion

This brings an end to our blog on torrenting. We have covered all the basis, from the fundamentals about torrents, to how they work, what terminologies you should be knowledgeable about, to how you can use torrents, and whether they are illegal or legal.

We have also highlighted how you can perform safe torrenting with the help of a VPN service. Therefore, if you are new to using torrents and don’t know where to start, then this is the perfect method for getting started.

If you have any further queries regarding torrenting or if you are facing any difficulty in using torrents, then do let us know in the comments below.

What is Wi-Fi?

A wireless network uses [radio waves](https://electronics.howstuffworks.com/radio.htm), just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

1. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

The radios used for Wi-Fi communication are very similar to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and they can convert [1s and 0s](https://computer.howstuffworks.com/bytes.htm) into radio waves and convert the radio waves back into 1s and 0s. But Wi-Fi radios have a few notable differences from other radios:

* They transmit at frequencies of 2.4 GHz or 5 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data.
* They use 802.11 networking standards, which come in several flavors:
* 802.11a transmits at 5 GHz and can move up to 54 megabits of data per second. It also uses orthogonal frequency-division multiplexing (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.
* 802.11b is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses complementary code keying (CCK) modulation to improve speeds.
* 802.11g transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.
* 802.11n is the most widely available of the standards and is backward compatible with a, b and g. It significantly improved speed and range over its predecessors. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. 802.11n can transmit up to four streams of data, each at a maximum of 150 megabits per second, but most routers only allow for two or three streams.
* 802.11ac is the newest standard as of early 2013. It has yet to be widely adopted, and is still in draft form at the Institute of Electrical and Electronics Engineers (IEEE), but devices that support it are already on the market. 802.11ac is backward compatible with 802.11n (and therefore the others, too), with n on the 2.4 GHz band and ac on the 5 GHz band. It is less prone to interference and far faster than its predecessors, pushing a maximum of 450 megabits per second on a single stream, although real-world speeds may be lower. Like 802.11n, it allows for transmission on multiple spatial streams up to eight, optionally. It is sometimes called 5G Wi-Fi because of its frequency band, sometimes Gigabit Wi-Fi because of its potential to exceed a gigabit per second on multiple streams and sometimes Very High Throughput (VHT) for the same reason.
* Other 802.11 standards focus on specific applications of wireless networks, like wide area networks (WANs) inside vehicles or technology that lets you move from one wireless network to another seamlessly.
* Wi-Fi radios can transmit on any of three frequency bands. Or, they can "frequency hop" rapidly between the different bands. Frequency hopping helps reduce interference and lets multiple devices use the same wireless connection simultaneously.

As long as they all have wireless adapters, several devices can use one router to connect to the Internet. This connection is convenient, virtually invisible and fairly reliable; however, if the router fails or if too many people try to use high-bandwidth applications at the same time, users can experience interference or lose their connections. Although newer, faster standards like 802.11ac could help with that.

A Wi-Fi hotspot is simply an area with an accessible wireless network. The term is most often used to refer to wireless networks in public areas like airports and coffee shops. Some are free, and some require fees for use, but in either case they can be handy when you are on the go. You can even create your own mobile hotspot using a cell phone or an external device that can connect to a cellular network. And you can always set up a Wi-Fi network at home.

If you want to take advantage of public Wi-Fi hotspots or your own home-based network, the first thing you'll need to do is make sure your computer has the right gear. Most new [laptops](https://computer.howstuffworks.com/laptop.htm) and many new desktop computers come with built-in wireless transmitters, and just about all mobile devices are Wi-Fi enabled. If your computer isn't already equipped, you can buy a wireless adapter that plugs into the PC card slot or [USB](https://computer.howstuffworks.com/usb.htm) port. Desktop computers can use USB adapters, or you can buy an adapter that plugs into the PCI slot inside the computer's case. Many of these adapters can use more than one 802.11 standard.

Once you've installed a wireless adapter and the drivers that allow it to operate, your computer should be able to automatically discover existing networks.

This means that when you turn your computer on in a Wi-Fi hotspot, the computer will inform you that the network exists and ask whether you want to connect to it. If you have an older computer, you may need to use a software program to detect and connect to a wireless network.

Being able to connect to the Internet in public hotspots is extremely convenient. Wireless [home networks](https://computer.howstuffworks.com/home-network.htm) are convenient as well. They allow you to easily connect multiple computers and to move them from place to place without disconnecting and reconnecting wires. In the next section, we'll look at how to create a wireless network in your home.

If you already have several computers networked in your home, you can create a wireless network with a wireless access point. If you have several computers that are not networked, or if you want to replace your [Ethernet](https://computer.howstuffworks.com/ethernet.htm) network, you'll need a wireless router. This is a single unit that contains:

1. A Port to Connect to Your [Cable](https://computer.howstuffworks.com/cable-modem.htm) or [DSL](https://computer.howstuffworks.com/dsl.htm) Modem
2. A [Router](https://computer.howstuffworks.com/router.htm)
3. An Ethernet hub
4. A [Firewall](https://computer.howstuffworks.com/firewall.htm)
5. A Wireless Access Point

A wireless router allows you to use wireless signals or Ethernet cables to connect your computers and mobile devices to one another, to a [printer](https://computer.howstuffworks.com/inkjet-printer.htm) and to the [Internet](https://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm). Most routers provide coverage for about 100 feet (30.5 meters) in all directions, although walls and doors can block the signal. If your home is very large, you can buy inexpensive range extenders or repeaters to increase your router's range.

As with wireless adapters, many routers can use more than one 802.11 standard. Normally, 802.11b routers are slightly less expensive than others, but because the standard is older, they're also slower than 802.11a, 802.11g, 802.11n and 802.11ac routers. 802.11n routers are the most common.

Once you plug in your router, it should start working at its default settings. Most routers let you use a Web interface to change your settings. You can select:

* The name of the network, known as its service set identifier (SSID) -- The default setting is usually the manufacturer's name.
* The channel that the router uses -- Most routers use channel 6 by default. If you live in an apartment and your neighbors are also using channel 6, you may experience interference. Switching to a different channel should eliminate the problem.
* Your router's security options -- Many routers use a standard, publicly available sign-on, so it's a good idea to set your own username and password.

Security is an important part of a home wireless network, as well as public Wi-Fi hotspots. If you set your router to create an open hotspot, anyone who has a wireless card will be able to use your signal. Most people would rather keep strangers out of their network, though. Doing so requires you to take a few security precautions.

It's also important to make sure your security precautions are current. The Wired Equivalency Privacy (WEP) security measure was once the standard for WAN security. The idea behind WEP was to create a wireless security platform that would make any wireless network as secure as a traditional wired network.

But hackers discovered vulnerabilities in the WEP approach, and today it's easy to find applications and programs that can compromise a WAN running WEP security. It was succeeded by the first version of Wi-Fi Protected Access (WPA), which uses Temporal Key Integrity Protocol (TKIP) encryption and is a step up from WEP but is also no longer considered secure.

To keep your network private, you can use one or both of the following methods:

* Wi-Fi Protected Access version 2 (WPA2) is the successor to WEP and WPA and is now the recommended security standard for Wi-Fi networks. It uses either TKIP or Advanced Encryption Standard (AES) encryption, depending upon what you choose at setup.

AES is considered the most secure. As with WEP and the initial WPA, WPA2 security involves signing on with a password. Public hotspots are either open or use any of the available security protocols, including WEP, so use caution when connecting away from home. Wi-Fi Protected Setup (WPS), a feature that ties a hard-coded PIN to the router and makes setup easier, apparently creates a vulnerability that can be exploited by hackers, so you may want to turn off WPS if possible or look into routers that do not have the feature.

* Media Access Control (MAC) address filtering is a little different from WEP, WPA or WPA2. It doesn't use a password to authenticate users -- it uses a computer's physical hardware. Each computer has its own unique MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. You must specify which addresses are allowed when you set up your router. If you buy a new computer or if visitors to your home want to use your network, you'll need to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can spoof a MAC address -- that is, copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

You can also change other router settings to improve security. For instance, you can set it to block WAN requests to keep the router from responding to IP requests from remote users, set a limit to the number of devices that can connect to your router and even disable remote administration so that only computers plugged directly into your router can change your network settings. You should also change the Service Set Identifier (SSID), which is your network name, to something other than the default so that hackers can't immediately tell what router you are using. And selecting a strong password never hurts.