

## SECRETS OF ANONYMOUS FILE SHARING

Whether you're a privacy freak or you're actually doing something wrong, you have three choices if you want to maintain your anonymity over a file sharing network:

- Use a special firewall, such as PeerGuardian, to mask your IP address.
- Use a file sharing program that encrypts your IP address.
- Use a proxy server to strip away your IP address.

### KEEPING YOUR IP ADDRESS SECRET WITH PEERGUARDIAN

If you can't keep your IP address a secret from a file sharing network, you can keep it secret from the people most likely to be trying to track you down—if you know *their* IP addresses.

PeerGuardian (<http://www.methlabs.org>) knows those addresses; it contains a database of IP addresses that belong to various law enforcement agencies and music companies (see [Figure 6-2](#)). When someone with one of these known IP addresses tries to examine the files on various computers to determine the number and names of the songs available, PeerGuardian jumps in and blocks your IP address so they can't examine your files. PeerGuardian lets in anyone whose IP address is not in their database.



**Figure 6-2:** PeerGuardian maintains a database of suspicious IP addresses that it blocks over a file sharing network, such as those belonging to the RIAA, Warner Music, and the French Department of Defense.

### HIDING YOUR IP ADDRESS AND YOUR ACTIVITIES ON AN ENCRYPTED FILE SHARING NETWORK

Can PeerGuardian really protect you from prying eyes? Maybe, but don't count on it, because those same agencies can change their addresses or use dynamic ones. Alternatively, consider using only file sharing networks that use encryption to ensure anonymity, such as Filetopia (see [Figure 6-3](#)).



**Figure 6-3:** Filetopia gives you a choice of different encryption algorithms to mask your identity when you are connected to the Filetopia peer-to-peer network.

Such file sharing networks protect your privacy in two ways. First, instead of connecting directly to another computer to share files, networks such as MUTE reroute your connection through multiple computers. Doing this makes it nearly impossible for anyone to determine which two computers may be communicating at any given time, thus ensuring your anonymity.

Second, these networks also encrypt any files sent between computers so no one can tell what type of information people may be passing along to each other. Anonymity protects your identity while encryption protects the contents of any files that you share.

Because an anonymous file sharing network could mask the identity of blatant file sharers, the recording industry targeted Madster (formerly called Aimster), which allowed people to encrypt files and send them over instant messaging services. In court, Madster claimed that they could not block files swapped using their software because they could not tell which ones might violate copyright. However, the appeals court called this argument “willful blindness” and ordered Madster shut down anyway.

Until they shut down every possible file sharing network, though, try using one of the following:

**Freenet** <http://freenet.sourceforge.net>

**Filetopia** <http://www.filetopia.org>

**GRL ISN** <http://www.grltechnology.com>

While it’s nearly impossible to shut down a file sharing network that doesn’t route everything through a central server (which proved to be the downfall of the original Napster), organizations such as the RIAA can still try to sue the companies that produce the file sharing programs in the first place, such as Kazaa. However, that won’t happen with EarthStation 5 (<http://www.earthstation5.com>), a file sharing company located in war-torn Palestine.

To keep their users anonymous, EarthStation 5 uses encryption (which hides the contents of the files you’re sharing) and proxy servers (which masks your IP address so people can’t find you on the Internet) to ensure everyone’s identity is as secure and private as possible (see [Figure 6-4](#)).



**Figure 6-4:** EarthStation 5 offers a stealth mode to mask your IP address from any intruders.

If the authorities try to shut down EarthStation 5, they'll have to visit the less than comfortable lands inside the Palestinian territory. Between missile strikes, car bombings, and random shootings, few authorities are going to care, let alone enforce, any laws against EarthStation 5, so EarthStation 5 is likely to escape the wrath of the RIAA and other Western-based organizations for the foreseeable future.

## HIDING YOUR IP ADDRESS WITH AN ANONYMOUS PROXY SERVER

When you use file sharing networks like Morpheus or Kazaa, anyone on that network can see the IP address that identifies every computer. To avoid broadcasting your IP address to anyone who might be looking for it, try masking it by using a *proxy server*.

A proxy server acts as a middleman that (theoretically, at least) strips away your IP address. Instead of connecting to another computer directly, and thus giving away your own IP address, you connect to a proxy server, which then contacts the other computer for you. All the other computer sees is the IP address of the proxy server.

By the same token, when you connect through a proxy server and then copy files from another computer, the file you're downloading first goes to the proxy server and then to your computer. Proxy servers thus slow down file sharing programs, but they also protect your identity so that no one (except the proxy server computer) knows your IP address.

For a list of proxy servers, visit one of the following websites:

**The Proxy Connection** <http://theproxyconnection.com/httpist.html>

**Socks 5 Proxy List** <http://www.atomintersoft.com/products/alive-proxy/socks5-list>

**OpenProxies** <http://www.openproxies.com>

**ProxyKing** <http://www.proxyking.com>

**StayInvisible.com** [http://www.stayinvisible.com/index.pl/proxy\\_list](http://www.stayinvisible.com/index.pl/proxy_list)

You'll find both free and commercial proxy servers on these lists. The free ones may be slow because so many people use them, and not all of them will strip away your IP address, so if you value your time and privacy, pay to use a faster, anonymous proxy server instead.

**Note Note** Pay attention to the locations of different proxy servers. A proxy in Taiwan or Brazil probably won't care if what you're doing skirts American laws, but one in Utah or New York just might.

## Hiding behind a proxy server

Once you find a proxy server that you think you can trust, you need to configure your file sharing program to use it. Most file

sharing programs allow you to configure a proxy server to mask your IP address, although finding the specific command to do so may not be easy.

To configure Kazaa to use a proxy server, click Tools > Options, and in the Desktop Options dialog box, click the Firewall tab, as shown in [Figure 6-5](#). There you can enter the IP address of the proxy server you want to use.



**Figure 6-5:** Using a proxy server with Kazaa to mask your IP address.

## Hiding behind a wireless hotspot

For the ultimate in identity masking, log on to one of the many free wireless *hotspots* around the country. By using a public wireless Internet connection with a laptop, the only IP address anyone will see will be the one that belongs to the wireless hotspot itself, and not to your computer.

You'll find free wireless Internet access available at various parks, libraries, hotels, and restaurants in cities worldwide. Many businesses don't bother to password-protect their wireless systems, which leaves them open to visitors too.

Downloading files takes some time, so drop by with fully charged batteries -(or a power cord if you can find an outlet), and keep your screen dimmed while downloading to slow the battery drain. And bring something to read while you wait.

The following websites list where free wireless hotspots are located:

**The Wi-Fi-FreeSpot Directory** <http://www.wififreespot.com>

**FreeNetworks** <http://www.freenetworks.org>

**WiFiMaps** <http://www.wifimaps.com>

## OTHER WAYS OF HIDING YOUR IDENTITY

The precautions listed in this chapter can minimize your visibility over the Internet when you use a file sharing program. For added security, many people use file sharing networks at their job (so any file sharing activities get traced to their employer and not to any particular individual).

For even greater protection, you can turn off file sharing on your computer, as shown in [Figure 6-6](#). That means you can still copy files from other people's computers, but no one can examine, let alone copy, any files on your computer. Of course, if everyone stops sharing files to protect themselves, that essentially shuts down the file sharing networks, which is what organizations like the RIAA want everyone to do in the first place.



**Figure 6-6:** If you refuse to share files over a file sharing network, the authorities can't see if your computer contains any copyrighted files.

As another alternative, just share a handful of files and when you download new files, move them to a separate folder that you won't share with others. Now if the RIAA examines your computer, they'll think that you're not sharing enough files to make you a worthwhile target.

Another way to mask your identity is to do all your illegal file sharing activity on somebody else's computer, preferably someone you don't like. That way if the authorities do track your IP address, it will lead them directly to anyone but you. An additional way to protect yourself involves taking advantage of the way the RIAA tracks copyright violators. They don't target people copying files; they target people sharing files.

Remember, don't break the law; just creatively skirt around the legal boundaries-like any law-abiding politician would do.

Team LiB

◀ PREVIOUS    NEXT ▶