Some tricks for hosts files in the system

The use of a number of support utilities such as Adblock Plus has become quite familiar to most of our users, since no one can withstand too much advertising information that is constantly displayed on access websites. they will distract the user, and greatly affect the connection speed.

The use of a number of support utilities such asAdblock Plushas become quite familiar to most of our users, since no one can withstand too much advertising information that is constantly displayed on access websites. they will distract the user, and greatly affect the connection speed. However, such a use has a very recognizable drawback, which is that they only work on installed browsers. If you want to block ads from certain domains, you should edit the hosts file of the operating system (or better of the router) to block the flow of input through the browser, so this way is often It is more effective than supporting software.

How does this process work?

To begin with, you need to consult and learn some concepts of DNS, or understand this here is an address book of the Internet. In technical terms, our computers use two ways to identify servers through the network. In the beginning, only the **/ etc / hosts file will** be used, after a period of time this file will be filled with information about host DARPA and University, then DNS will be created to search for other services for people. use.

See more articles:

1. How to reset HOSTS file on Windows operating system.
2. Go to Facebook simply and quickly by editing the HOSTS file.

Today, most operating system platforms perform the process of searching for service names via IP addresses by:

- Check the **/ etc / hosts file** first

- If you don't see it, the system will send a query about DNS

Any **hostname** information found in the hosts file will prevent subsequent query statements. On the other hand, **DNS** is particularly important in Internet security for the system. Any user can replace these parameters to 'trick' the system, connect to remote servers with **SSL** without any precautions. The security of SSL certificates is used to ensure that online trading or other operations are carried out within security and based on the **DNS** configuration of the system.

Some advantages of doing this:

- Improved Internet connection speed since file hosts on local is used in default mode, before DNS is applied.

- Not only for the browser, this approach can also be applied to iTunes client application, RealPlayer, Twitter . or any other program, regardless of UDP or TCP traffic protocols.

- Can operate on separate operating system platforms, Portable, Mac OS X, Linux or Microsoft Windows. If the system uses the **IP** protocol **- Internet Protocol** , this **/ etc / hosts file** is definitely somewhere on the operating system.

- At the same time, this can also completely prevent the tracking process from advertising servers. Applying the hosts file after customization will become extremely useful in case the user wants to completely 'exit' the monitoring of the advertising program related to the basic function of cookies.

- Can prevent malicious software sources, spyware, malware .

Exactly which file in the system should be used?

For **OS X** and **UNIX-** based **operating systems** , this file is stored in **/ etc / hosts** . On Windows, this file is frequently available at **% SystemRoot% system32drivers** (with Windows Vista or 7: **c: WindowsSystem32driversetc**).

Normally, the original host file will contain some information as follows:

127.0.0.1 localhost
127.0.1.1 my-real-hostname
:: 1 my-ipv6-addr

File hosts do not have the extension - extension, so you need to be careful before forgetting directly. The best way to ensure is to save the contents of this hosts file to a safe place (in Mac OS, open **Go> Go To Folder** and type **/ etc,** then find the **hosts** file). In fact, it is possible to create our own hosts file, thereby adding more ad server addresses to this list of restrictions. However, the simpler way is to use the hosts file available from the online community, either through searching with Google or hpHosts.

After preparing the hosts file, please copy to the directory **etc** , if you have already opened the file, copy the content starting from the line **127.0.0.1** or other IP address range. When saving, make sure you don't save the file with the extension. Another way to check the hosts file or whether the contents of the content are guaranteed or not, we only need to search for any line of information that does not begin with 127.0.0.1 or the external annotation symbol, for example. as:

egrep -v '^ 127.0.0.1 | ^ #' / etc / hosts | more

However, not all hosts files provided on the Internet are safe. In some cases, bad guys often deliberately insert domain names, distribute their malicious code into the file to deceive users, such as cnbc7.com, which looks like the CNBC TV channel but in fact it is not so. To prevent this, add this line to all hosts files on the system to prevent spyware, malware and viruses:

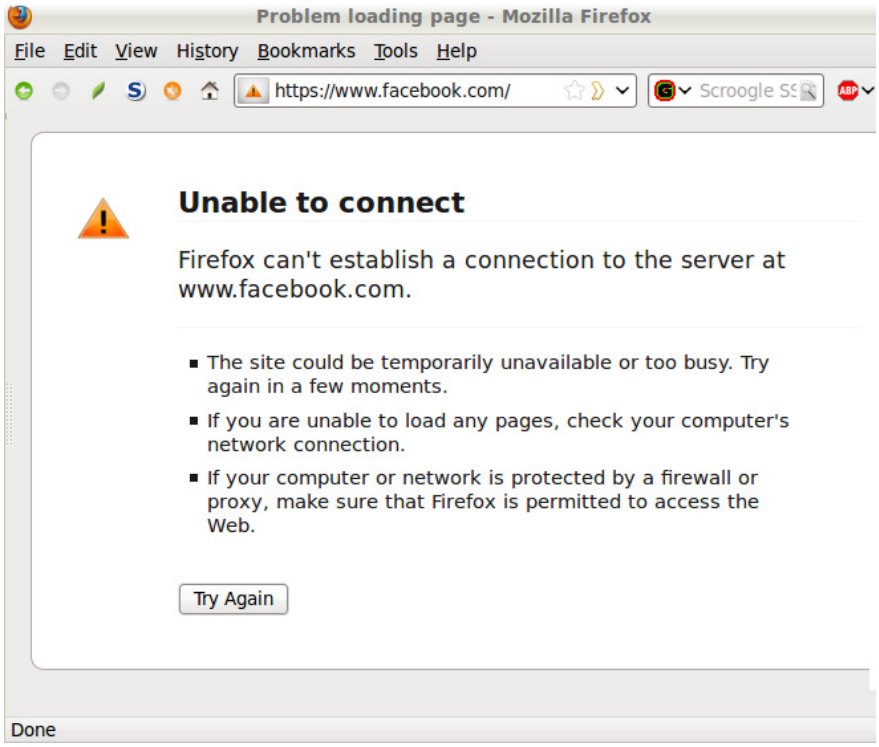
127.0.0.1 cnbc7.com

Some points to note:

Basically, the file structure of this file is exactly the same for all operating system platforms, and many users want to combine the content, the information inside with the hosts file is available online. At some point, if you want to go back to a previously blocked website, just place the comment mark in front of the server in the hosts file.

For example, if you block **facebook.com** and **www.facebook.com** , it will affect some websites or applications that have mechanisms that work through Facebook's hosting server. However, in order to minimize the potential risk, you should prepare three hosts files: hosts, hosts.noFB, hosts.FB. If you want to use it, just copy the contents of one of those 3 files into the official hosts file.

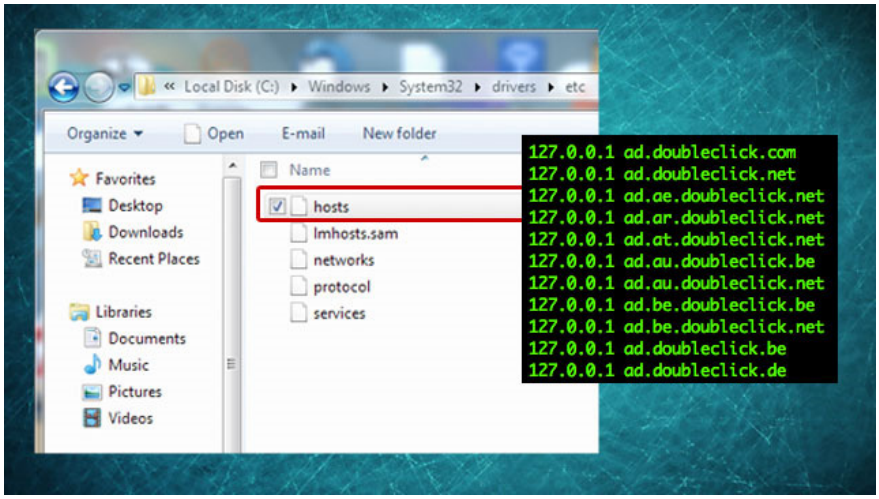
In case we block an entire website, such as **www.facebook.com** , the results displayed from the browser will look like this:



Any changes will be applied immediately, if you block a certain domain only because of the ad text, the rest of the screen will be displayed as a space, after changing the hosts file. then the rest will look like this:

127.0.0.1 localhost
127.0.1.1 my-real-hostname
:: 1 my-ipv6-addr

On some modern operating systems today, the hosts file is protected quite closely, so users must have access at the highest level - **Adminsitrator** . For some versions of **Mac OS X,** the system does not allow access and change hosts files in the usual way, please refer to these changes here.



For applications that support firewalls like Smoothwall, users will have complete control over the **/ etc / hosts file** for all devices and devices in the network. In fact, this feature proved extremely useful in managing and monitoring the system with a lot of computer components inside. In case you don't want to block content from certain websites or servers, applying the **/ etc / hosts file** may not be very reasonable. In the present time, free websites that depend largely on advertising sales will be hard to survive if we apply different ways to block advertising data, moreover you need to confirm It is clear and accurate that these are just good pieces of advertising information, which are security flaws of a **Flash-** based or **JavaScript-** based system **.** If this is the case, it is best to completely block the name. That domain or apply external support extensions. Good luck!

You finished reading the article "**Some tricks for hosts files in the system**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.