

THE COMPUTER CORNER

No. 141. URLs and the Hosts File

- by Stan Kaplan, WB9RQR
715 N. Dries Street
Saukville, WI 53080-1664
(262) 268-1949
skaplan@mcw.edu

Before we get into the contents of the Hosts file and how you can use it to your benefit, lets consider the topic of web addresses in general. When you wish to visit a website, lets say majorgeeks, you type in that name in your browser, or you click a shortcut to that name. Most often, you type in the URL (Uniform Resource Locator) http://www.majorgeeks.com, but just the Registered Domain Name majorgeeks.com will work all by itself (as will just majorgeeks). When you type in the URL, your machine makes a request to a server somewhere on the web (maybe thousands of miles from you) to translate the URL you typed into an IP (Internet Protocol) address. The Internet Protocol address is a unique address that computers and other smart electronic devices use to identify and communicate with each other. Once the IP address has been found by the server and sent back to your machine, you are taken to that address:

URL	IP Address
http://www.majorgeeks.com	208.101.7.150

So the URL is sort of like a name, Stan Kaplan, while the IP address is like a telephone number, (262) 268-1949. Actually, the majorgeeks IP address links to a server in Dallas owned by SoftLayer Technologies, Inc., a company that provides web services to majorgeeks. URLs are a convenient way for us humans, who understand combinations of letters as words, to link with sites that are best addressed by digital devices with numbers.

Hey, you might wonder how those four groups of numbers separated by dots can handle all of the Internet addresses in the world. Those numbers actually represent 32-bit (4 byte) values, so there are 2^{32} possible addresses, or roughly 4.3 billion. That is not enough. A shortage of such addresses is on the horizon, so a new standard, using 128 bits (16 bytes) is already in use. That will give us 2^{128} unique addresses, or about 3.4×10^{38} total. Someone computed that this would provide roughly 5,000 addresses for every square micrometer on the earth's surface, surely enough for the foreseeable future!

Now on to your HOSTS file. This is a file you can safely open and examine with the Universal Viewer program I mentioned in #140. You can use Notepad or other simple text editor, too, but use care not to edit anything – just close Notepad when you are done without saving the file. You can find the HOSTS file here, depending on the version of Windows you use. Look for a file with just the name: Hosts .. no extension.

OS	Location of HOSTS File
Vista and XP	C:\WINDOWS\SYSTEM32\DRIVERS\ETC
2000	C:\WINNT\SYSTEM32\DRIVERS\ETC
98/ME	C:\WINDOWS

The Host file can contain IP addresses and URLs, just as in the majorgeeks example I gave above. Indeed, it defines a URL as having that particular address, and if your machine has such a definition in the Hosts file, it doesn't have to go out to a server on the web to look up the address before it takes you there. It just goes right to that address. Now, that might be handy in slightly speeding up your browsing, but that is an unimportant side issue. The real value to you lies in security.

If you look at your Host file, you will see that the very first entry (after any comment lines – those preceded by the symbol #) is:

127.0.0.1 localhost

What that says – what it defines, is that the IP address 127.0.0.1 is your own machine (localhost). If you type that address into IE, you will get the message that the page cannot be found, because it looked at your own computer and did not find a webpage. If you type it into Firefox, you will be presented with a blank page. Well, now, how can that be of any value to you, security-wise?

Suppose you type in as the second line of your Hosts file:

127.0.0.1 porn.com

Now, if you ever accidentally type http://www.porn.com in your browser's address window, you will never get there. You'll get a blank screen or a "page cannot be found" message. But that is not all – it gets even better. If you are browsing on the web and you come to a page that tries to redirect you to porn.com (such redirection occurs ALL THE TIME, without your knowledge or consent), the redirection will also fail. Neato! What a tool! Now, all we need is a list of all the bad sites on the web, so we can type them into our Hosts file. THAT IS NOT NECESSARY!

It has all been done for you already. First visit http://www.mvps.org/winhelp2002/hosts.htm to read the page entitled BLOCKING UNWANTED PARASITES WITH A HOSTS FILE. I suggest you print the 5 pages for further study, so that you understand the implications of using 127.0.0.1 to help you browse the web more safely.

Next, visit majorgeeks and download and install the HostsMan (Host File Manager) program. Once installed, have the program get the very latest updates into your Hosts file, combining the efforts of several sites to cover the bulk of all the bad places on the web. It will make a backup of your old Hosts file, too. I currently have over 64,000 entries in my new Hosts file, and the file is just under 2 MB in size. The next time you boot your machine, all of those entries will be read into memory and kept there while the machine is on. Then, when you browse the web, your machine will check each URL in its memory before going out to look up the IP address so it can take you there. Any "bad guys" in your Hosts list will automatically be blocked, since the IP address points to your own machine.

This is a simple fix to block ads, banners, 3rd party cookies, 3rd party page counters, web bugs, many hijackers, data miners and other such malware from getting into your machine. Moreover, should one ever get into your machine via a non-web based source (floppy, CD, etc.), it will not be able to get out to "phone home", so long as it is included in your Hosts file. While not a substitute for antivirus and antispyware software, using the Hosts file as outlined here will certainly keep your machine safer. Do it. It is worth it. Happy Computing!