IP Address: Your Internet Identity

by

Russ Smith of Consumer.Net March 29, 1997

Abstract

The Internet, sometimes called the network of networks, is based upon one simple principle: transferring information from one computer to another. In order to do this each computer needs an identity which is called the "Internet Protocol address" or "IP address." It is similar to a telephone number or street address. The IP address is **personally identifiable information** that is automatically captured by another computer when any communications link is made over the Internet. This includes visiting web pages, sending or receiving e-mail, visiting newsgroups, or using a chat room. Often, a user's IP address is automatically sent to a third party when visiting a web site using banner ad networks or, under certain circumstances, opening an e-mail message. This usually occurs before there is any opportunity to review a privacy policy. The amount of information available about users from their IP addresses varies greatly depending on how they are connected to the Internet and other information that may be available. Logging the IP address is also essential in system security for tracing unauthorized use and computer break-ins. As fixed Internet connections increase, more and more users can be traced directly from their IP address. To see a demonstration of IP address tracing visit http://consumer.net/analyze/.

IP Addresses and Domain Names

Computers connected to the Internet must speak the "Internet language" called the "Internet Protocol" or simply "IP." Each computer is assigned a unique address somewhat similar to a street address or telephone number. Under the current system there are four numbers that range from 0 to 255 (Example: 206.156.18.122). Every computer, whether it functions as a web site, is being used by a web surfer, is a mail server, and/or is used for any other function, has an IP address so it can communicate across the Internet. Communication is accomplished by sending pieces of information called "packets" that include the IP address of the destination computer.

Up to this point, domain names have not yet been mentioned because they are not needed for the Internet to work! An *optional* feature of the Internet is to use domain names. With this system I can tell users to visit www.consumer.net rather than 206.156.18.122. If there are several computers in a network they can be grouped under a domain and could be given 'friendly' names for convenience such as: computer1.consumer.net, computer2.consumer.net, etc. This has the added convenience of keeping the same computer names even when the IP addresses change or if the computers move to a different physical location. Again, this naming is optional and is not always done. As a side note, the underlying IP addresses have no intrinsic value but the optional domain names can be worth thousands of dollars and have been the subject of many court cases.

The Domain Name System (often called DNS) is the system where the IP addresses are converted into names. When www.consumer.net is entered by a user into a browser a (somewhat hidden) process converts that name into 206.156.18.122. This allows the user to connect to the proper web site and usually involves a domain registration service that is funded by domain name fees.

How are IP Addresses Distributed?

Every transfer of information over the Internet must include the capture of the IP address. Some examples of automatic logging are: visiting a web site, sending or receiving e-mail, using a chat room, or reading and posting to newsgroups. A common situation that causes IP addresses to be distributed to a third party is when visiting a web site **and** that site participates in banner ad networks where the ads are served from a third party site. This third party site retrieves the IP address when it sends the ad. This information is used to measure the number of ad views and calculate click-through rates.

Transferring IP addresses to a third party can also be accomplished by sending a web page via e-mail. When the user opens the attachment (if they are connected to the Internet) the e-mailed web page could make a request to a web site anywhere on the Internet (such as requesting an image file). This transfers the user's IP address to that web site along with the date and time that the user opened the message. An Internet cookie can also be placed on the user's system at that time. Several advertisers already engage in this practice. This method could also be used to defeat anonymous e-mail.

How Can Users be Traced from their IP Addresses?

Once an IP address is captured several methods can be used to trace the user. These tools can be found at http://consumer.net/tracert.asp.

- Determine who owns the network. IP addresses are distributed in blocks to network providers or private companies. By searching IP registration databases it is possible to determine who owns an IP address block. Databases are available on the Internet for the Americas, Europe, and Asia-Pacific regions. Sophisticated computer break-ins sometimes include an attempt to erase the IP addresses captured by the log files to prevent this type of lookup.
- Perform a "reverse lookup." This converts the IP address into a computer name [Example: convert 206.156.18.122 into www.consumer.net]. This is used to determine if a computer is part of a registered Internet domain.
- Conduct a Traceroute. When information packets travel through the Internet they pass through several computers in a hierarchical fashion. Normally packets pass from the user to their Internet Service Provider (ISP) until it reaches the user's "backbone" provider. It then transfers to the destination "backbone " provider down to the ISP of the destination computer and finally to the intended recipient. It is often possible to determine an approximate physical location of an IP address in this fashion. It is also possible to determine the computer's ISP and/or network provider even if the computer itself is not part of a domain. This is usually how junk e-mail or "spam" is traced.
- Review domain registration information via the "WHOIS" databases. Domain registration information is available via the Internet by performing a WHOIS on the domain name portion of the computer name [Example: for www.consumer.net perform WHOIS CONSUMER.NET to obtain the registration information].
- Search the Internet for the IP address and/or computer name. It is often possible to find matches from users making public postings on discussion boards or from web sites that leave their log files open to the Internet. Of course, web site owners and/or banner networks could have additional non-public information based on activities at their web sites.

Generally, users who have fixed Internet connections (cable modems, private companies, etc.) have fixed IP addresses. Dial-up Internet providers usually give addresses dynamically from a pool when a user dials in to connect (such as a pool of 100 IP addresses per 800 subscribers).

Internal network procedures also affect the amount of information that can be gleaned from an IP address. If a proxy sits between the users and the Internet all of the users appear to come from one computer. In these cases, users can only traced as far as the proxy unless additional information is known. The computer names can also sometimes be used to gather additional information. One major provider's computer names usually include the nearest big city of the user. Some networks simply use the e-mail address in the computer name [Example: russ.consumer.net has e-mail address russ@consumer.net].

Ambiguities in user identification by IP address are reduced by the use of "Internet cookies." These are text files that gives users a unique identity. Cookies would essentially become unnecessary if everyone had fixed IP addresses.

Privacy Policy Implications

and CONSUMER.GOV have incorrect information concerning this issue. These policies indicate that only a domain name is captured. Some commercial web sites (such as VISA.COM) have copied this incorrect information and made it part of their own policy. Other industry privacy policy templates, such as those offered by the Direct Marketing Association and the Information Industry Association, overlook IP address collection.

A site's policy must also be coordinated with the policies of third parties that capture IP addresses from their site visitors (such as banner ad networks). Sometimes the banner ad network's policy is more import since it has the potential to track users across several sites rather than activity at a single site.