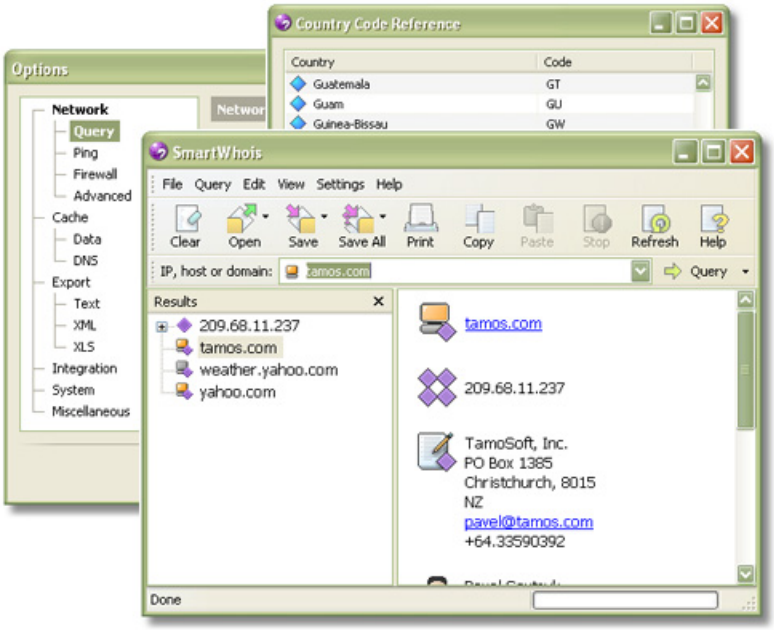
SmartWhois®
Tutorial
Domains and IP Addresses Demystified

About This Tutorial

Domains, IP addresses, host names, sites, and URLs have always been the source of many misconceptions, even amongst advanced Internet users. These notions are often misunderstood and/or confused. *What's the difference between a domain name and host name? What do those numeric IP addresses mean? How can I learn who owns a domain? Can I trace a user by IP address?*



Throughout this tutorial, we'll try to answer these and many other frequently asked questions and show you how you can use SmartWhois by TamoSoft to perform Whois look-ups.

Understanding the Basics

Domain Names, IP Addresses, Host Names, Web Sites, URLs, and Whois

Let's start with explaining the basic terms.

Domain: A domain is a logical region of the Internet. Domain names consist of one or several parts separated by periods, for example: "yahoo.com." You can refer to all of the computers that share the right-most portion of a name as being in the same domain, for example: "weather.yahoo.com" and "finance.yahoo.com" are both in the "yahoo.com" domain.

The top position in the domain hierarchy is occupied by Top Level Domains (TLDs). A TLD is the right-most portion of a domain name, and you obviously know many popular TLDs, for example: .COM, or .NET. Seven generic TLDs (.COM, .EDU, .GOV, .INT, .MIL, .NET, and .ORG) were created in 1980s, seven new TLDs were introduced in 2001 and 2002 (.BIZ, .INFO, .NAME, .PRO, .AERO, .COOP, and .MUSEUM), and, of course, there are over two hundred country-specific TLDs that consist of two letters, e.g. .CA for Canada or .DE for Germany (the complete list can be found on the IANA web site).

A second-level domain (SLD) is the next portion of a domain name (we're moving from the right to left here). For example, there are millions of second-level domains in the .COM top-level

domain zone, one of them being "yahoo.com." "Finance.yahoo.com" or "www.yahoo.com" would be a third-level domain, etc. Every existing SLD has an owner, a company, an organization, or individual and a Whois tool allows you to find the SLD owner.

IP Address: Every computer connected to the Internet is assigned a unique number known as an Internet Protocol (IP) address. This number identifies each sender or receiver of information that is sent in packets across the Internet. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 4.90.50.60 or 208.1.0.15 could be valid IP addresses.

Your computer, too, is assigned an IP address; because you can't access a web site or use any other Internet service, such as e-mail, without a valid IP address. Many IP addresses are assigned dynamically from a pool, while others are assigned on a permanent basis. Because IP addresses are usually assigned in country-based blocks, an IP address can often be used to identify the country from which a computer is connecting to the Internet.

Host Name: A host name is only an alias for the IP address. It is assigned to a computer for easy reference by humans. Take, for example, a web server, "www.lookup-ip.com." Its IP address is 66.39.117.110, but this number is not easy to remember. It's not likely that you will learn it by heart and enter it into your browser when you want to visit this web site, but www.lookup-ip.com is much easier to remember. When you enter www.lookup-ip.com into your browser, it quickly contacts the Domain Name System (DNS) server and finds out that www.lookup-ip.com translates into 66.39.117.110. From that point on, your browser uses the obtained numeric IP address to send and receive data to/from this web site. A computer connected to the Internet may or may not have a host name, but it must have an IP address.

Here are a few examples of host names: www.google.com (a web site), pop-server.austin.rr.com (a mail server), cs2416713-236.houston.rr.com (a host name assigned to a broadband Internet user), dialup134.ts521.cwt.esat.net (a host name assigned to a dial-up user).

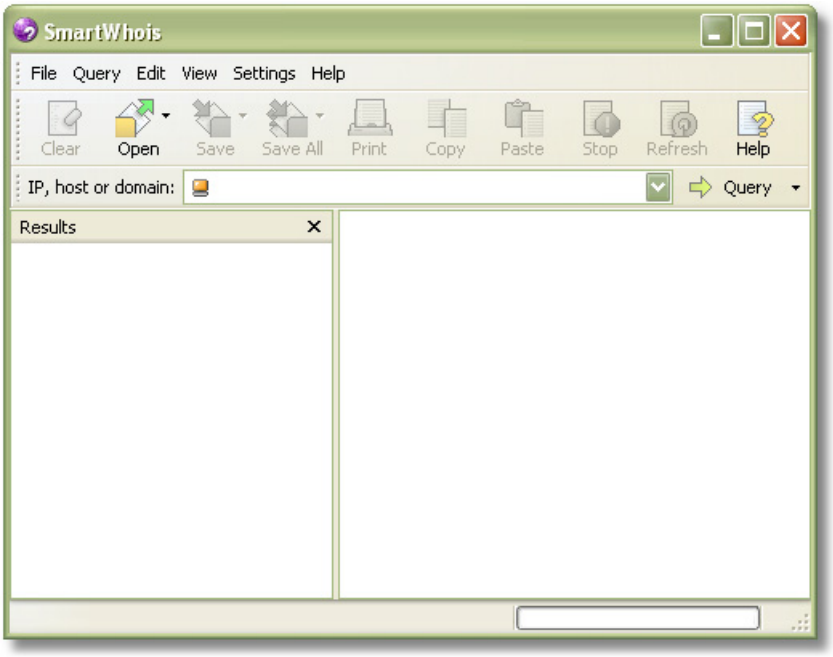
Web Site and URLs: A web site is a group of web pages stored on a particular web server. A web server is just a computer connected to the Internet that runs the software necessary for serving web pages. Typically, web servers have host names that begin with "www," e.g. "www.google.com," although this is not always the case. A Uniform Resource Locator (URL) is the address of a resource that is retrievable using on of the Internet protocols, usually Hyper Text Transfer Protocol (HTTP). An example of a URL is "http://www.google.com/about.html."

Whois: Whois is an Internet program that allows users to query a database of domains and IP addresses to retrieve information about the owners, administrators, geographic location, etc. As the name suggests, SmartWhois is a smart, feature-rich Whois utility capable of performing such queries. You will learn about what you can do with it in the next chapter.

Using SmartWhois

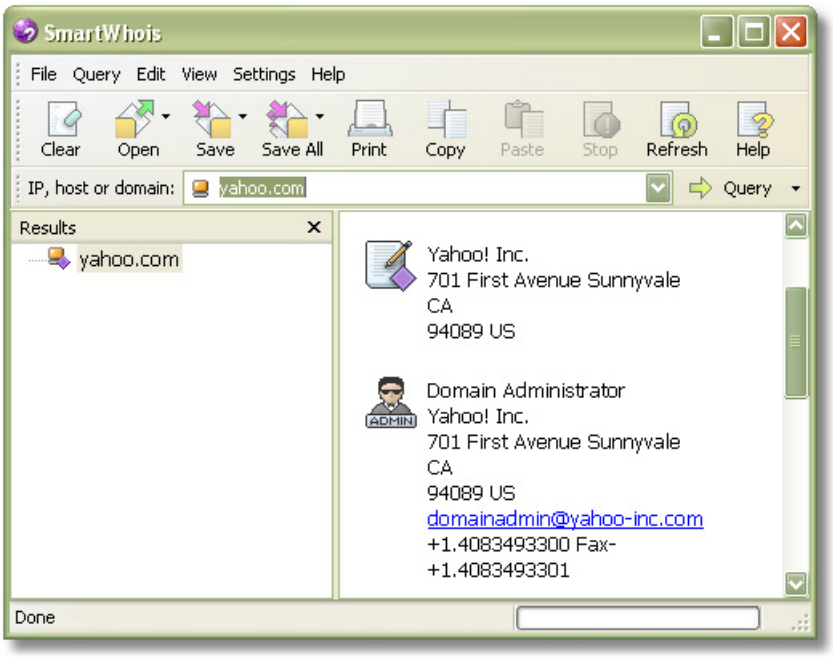
Understanding Domain and IP Address Queries

Equipped with the knowledge of the Internet terminology, we can start using SmartWhois. Download it if you haven't done so already, run the installation on your Windows 95/98/Me/NT/2000/XP/2003 system, and launch the program:

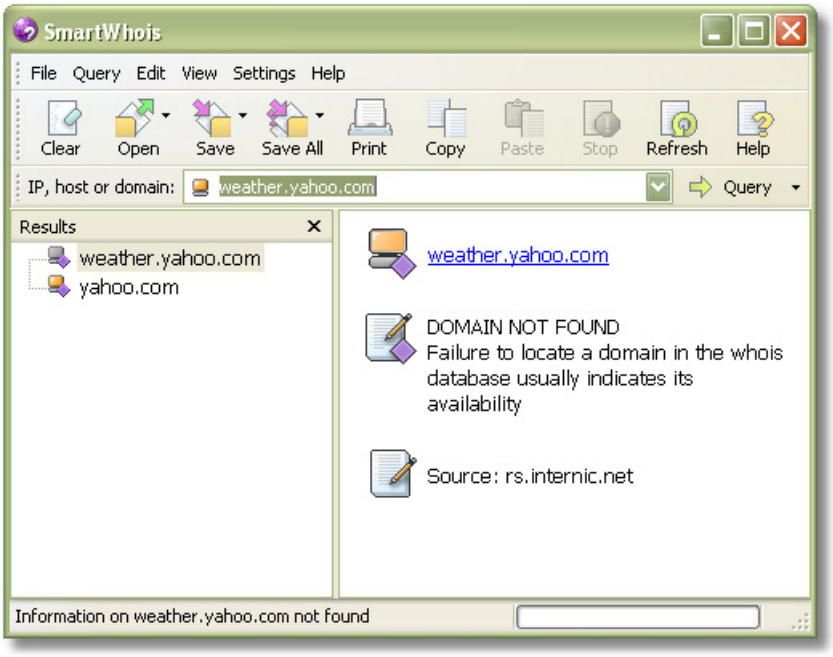


Understanding the difference between domain and IP address / host name queries is the key to successful usage of SmartWhois. When trying to find information on a particular web site, users are frequently confused about what kind of query they should perform and what they should type in the input field. So let's consider an example:

Suppose that you want to check who owns weather.yahoo.com, a popular site on weather. To find the owner of a web site, you should find out who owns the domain. In this example, the domain name is "yahoo.com." So you should type "yahoo.com" in the input field, click on the **Query** button, and select **As Domain**:



In just a few seconds, you see that "yahoo.com" belongs to Yahoo!, a California-based company. Why did we enter "yahoo.com" rather than "weather.yahoo.com"? Because "weather.yahoo.com" is not a second-level domain! Remember the previous chapter? In most of the cases, you should query **only** second-level domain names, such as "yahoo.com" rather than third-level domain names, such as "weather.yahoo.com." Actually, you can try to query "weather.yahoo.com" as a domain name:

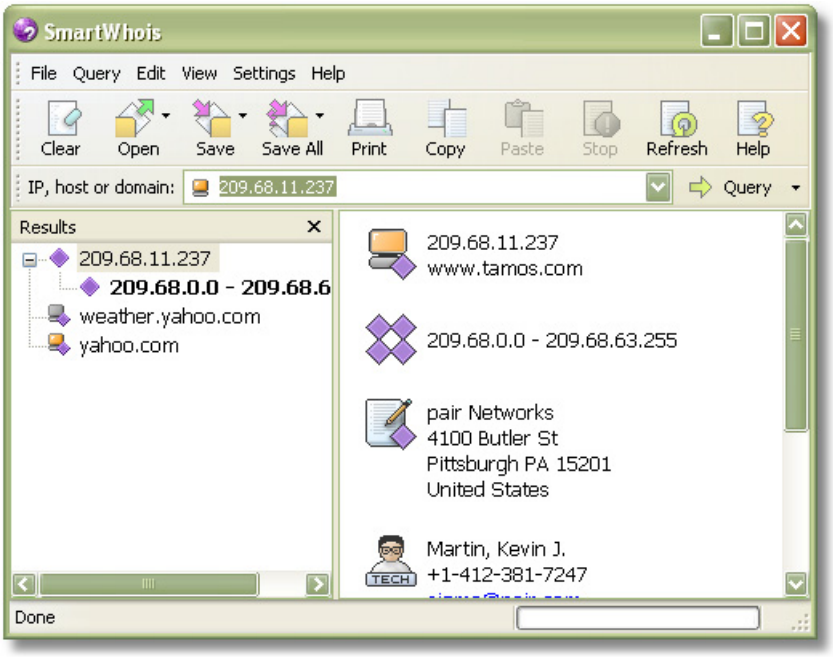


Yes, that's right, domain not found. Whois databases contain information on second-level domains only. In fact, there are a few exceptions to this rule, notably UK domains. Some countries have a domain system that is based on third-level domains, i.e. you buy a domain name with two dots already in, e.g. "jaguar.co.uk" or "bbc.co.uk." But this is rather uncommon.

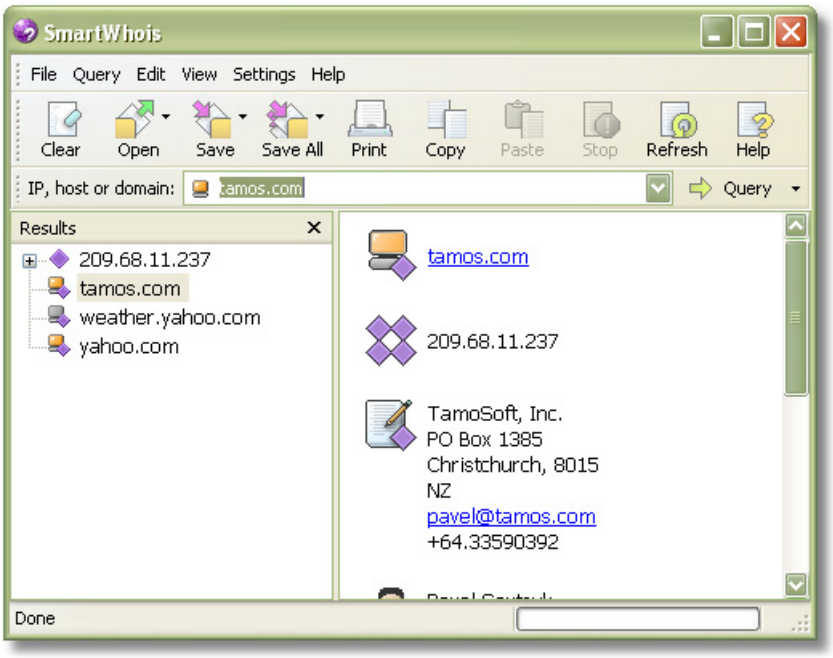
Now let's consider IP address / host name queries. Why they are grouped together? Because, technically, there is no difference between these two types of queries. As we mentioned in the first chapter, a host name is just an easy-to-remember alias for the IP address; therefore, querying a hostname and the corresponding IP address are equivalent. A host name query is just one step longer: SmartWhois needs to convert the hostname to the IP address by contacting a DNS server, and then, once the IP address for the entered hostname has been obtained, it will query one of the Whois databases for this IP address.

When does one need to perform an IP address / host name query as opposed to domain query? For example, when you need to check where a web site is hosted geographically. When you need to find out who sent you e-mail from a certain IP address. Or when you need to send a spam/abuse report to an ISP. There are many situations in which you need such information.

When you need to check an IP address or host name, just type or paste it into the entry field, click on the **Query** button, and select **As IP/Hostname**. A useful hint: You can just hit the "Enter" key :-) For domain queries, hit Enter while holding the "Ctrl" key.



We entered "www.tamos.com," and now we know that this site is located in the USA and is hosted by Pair Networks. Now, try to query "tamos.com" as a domain:



That's right; "tamos.com" belongs to TamoSoft, a New Zealand-based company. This leads us to an important observation: Domain and IP address / host name queries usually give you different results, and this is quite understandable. Query a domain to find out **who** owns it. Query a host name or IP address to find out **where** the computer with the given host name is located and **who** owns the corresponding range of IP addresses. "Tamos.com" is owned by a company based in New Zealand, but the company's web server, "www.tamos.com" (at the time of writing, this

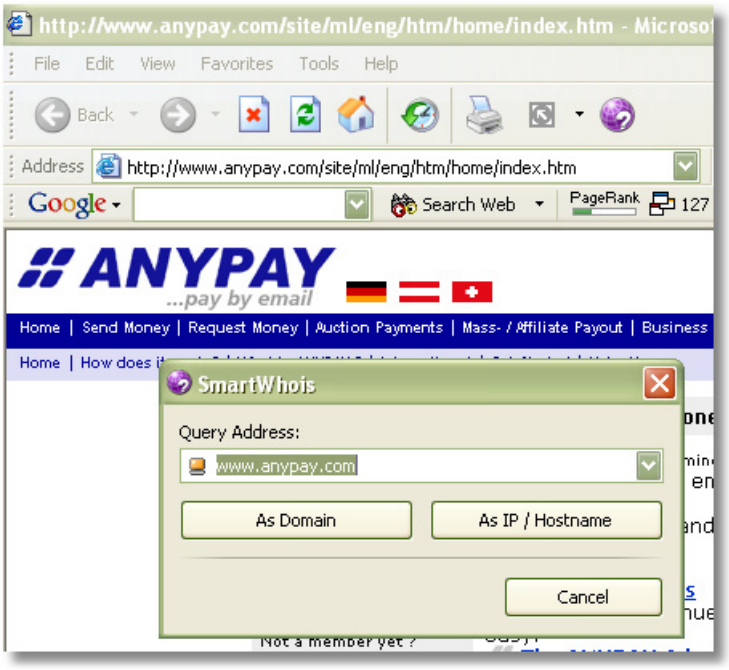
corresponds to 209.68.11.237) is located in the USA in the data center that belongs to Pair Networks.

Well, enough about the basics, let's look at a few other cool things you can do with SmartWhois.

SmartWhois and Microsoft Internet Explorer

What a Useful Button!

Have you noticed that little SmartWhois button on the Internet Explorer (IE) toolbar? If it's not there, make sure that the IE add-in is activated (in SmartWhois, click **Options => Integration => Add SmartWhois to Internet Explorer menu and toolbar**) and restart IE. Using this handy button, you can invoke SmartWhois every time you want to get more information about the web site you are visiting:



When you click on the toolbar button, the address field is pre-filled with the site address. What SmartWhois actually does is strips the URL in the IE address bar of the unnecessary parts. For example, if the current URL is "http://www.anypay.com/site/ml/eng/htm/home/index.htm," SmartWhois cuts off everything that does not constitute the site host name, "www.anypay.com." Now that we have the host name, we can perform a domain query on "anypay.com" (yes, SmartWhois will automatically cut off the unnecessary "www." part if you perform a domain query) to find out who owns this domain, or an IP address / host name query if you want to find out where the web server is hosted.

SmartWhois and Microsoft Outlook

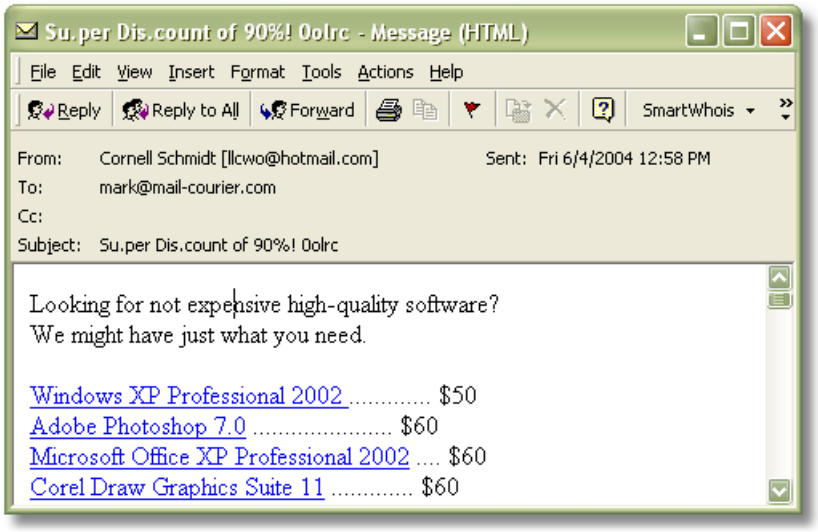
Looking at E-mail Headers

Just like in IE, you can find the SmartWhois button on the MS Outlook toolbar. If it's not there, make sure that the Outlook add-in is activated (in SmartWhois, click **Options => Integration => Install SmartWhois for MS Outlook Add-in**) and restart Outlook.

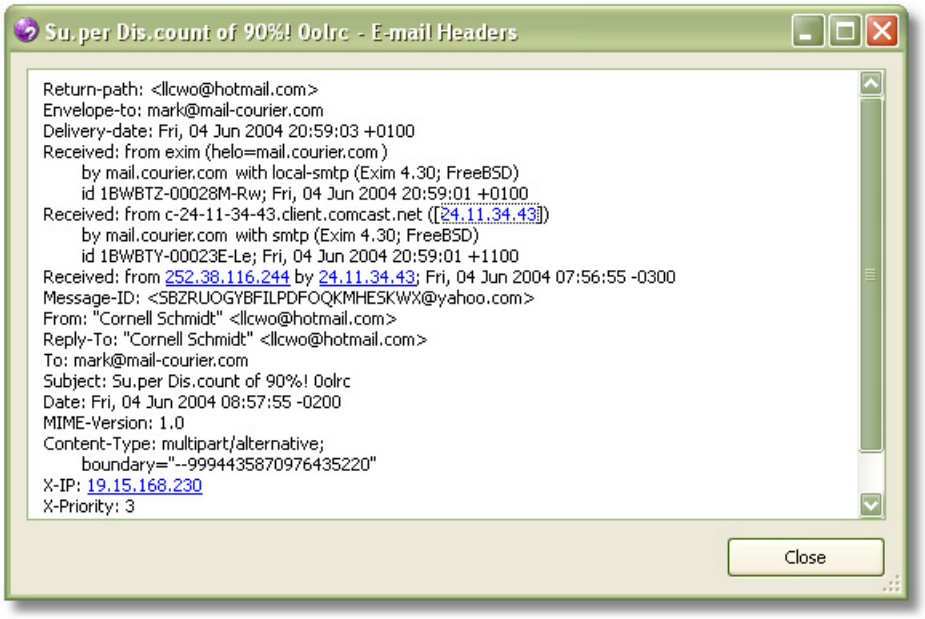
Every e-mail message that you receive includes so called "headers," that messy block of text that precedes the actual message body. Headers are included in every message, but they aren't normally displayed to the user. However, every e-mail client can be configured to show this information, and the SmartWhois add-in can help you quickly display it.

Headers contain information about the path the message took before reaching our e-mail box. Each computer that handled the message en route added something to the header, and it is this additional info we can use to help trace the message back to its source. Reading and understanding e-mail headers is not a black art, but it requires some knowledge and practice. This topic is outside the scope of this tutorial, but you can find many good articles on the Internet, for example: What Email Headers can Tell You About the Origin of Spam. Here, we'll simply show you how you can use SmartWhois to get information on the IP addresses that you can find in the headers.

Here is a typical spam message:



To look at the headers, click on the **SmartWhois** button on the toolbar and select **Pass E-mail Headers to SmartWhois**:



The IP address found in the headers are highlighted, just like hyperlinks on a web page. Clicking on any of the hyperlinks will make SmartWhois retrieve information about the selected IP address. You can also select any part of the text and query the selection as a host name or domain.

Why would anyone want to find the originating IP address of a message? Well, there could be a number of reasons. You may want to find the physical location of your correspondent (someone who claims to be staying in France might be in Italy). You may want to find to which organization the IP address in question is registered (if you got a message from customerservice@citibank.com but the message came from Nigeria, it's a good reason to think twice before submitting a web form with your account password). Or you may want to complain about spam.

Regardless of the purpose of your query, it's important to understand the limitations of the technology. It's equally important to distinguish between the myth and reality. Read more about this in the next chapter.

How Precise is the Information

Myths and Reality

You can usually get the precise information about the domain owner, as the owner's contact details are required to register a domain name. There are, of course, exceptions to this rule, because a domain may be registered using a stolen credit card and/or the owner may give fake personal information, although law in many jurisdictions prohibits this practice.

Unlike domains, IP addresses are not individualized to that extent. Usually, when you query an IP address, you get the details of the organization that owns a certain range of IP addresses. This is usually an ISP or company. Therefore, you can find out which ISP the person is using or which company he/she works for, but you can't get the name or address of the specific person who is connected to the Internet using the given IP address. The degree of precision may differ, though. An IP address may belong to a small company or ISP that owns as few as 16 IP addresses. If that's the case, you're in luck: You can find out exactly where the person is located, up to the city

district. But if you come across a huge ISP, such as AOL in the United States, all you can get is the location of the main office, and you wouldn't be able to even find out the state or province of the user, although there are other techniques that may help (e.g. the time zone or host name that often reveals the location). These are extreme examples; usually, the degree of precision is rather high.

That said, "I can get someone's address and phone number by IP his/her address" is a myth in most of the cases, at least if we consider an average "investigator." Naturally, a government agency may be capable of tracing the user by contacting the ISP and checking the connection log files. Another popular myth tells of a possibility to always find the sender's IP address in the e-mail headers. Well, that's not always the case, because it's not extremely difficult to hide one's IP address by using a proxy server (an HTTP proxy server in case of web-based e-mail services or SOCKS proxy server in case of the standard POP/SMTP e-mail clients). Again, a government agency may still trace the user.

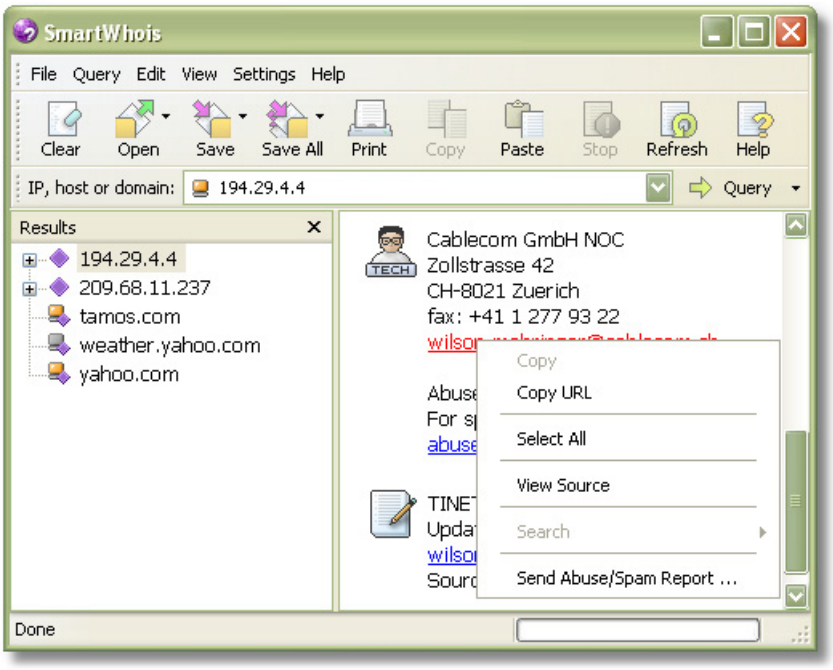
It's interesting to look at the situation from the standpoint of the user whose IP address is being queried or otherwise analyzed. Is it safe to reveal it? Do you need to hide it? The answer is not an easy one, and it's outside the scope of this tutorial. In brief, if you are looking for anonymity, you should consider implementing some measures to hide it. If you're not particularly concerned about anonymity or privacy, there are still situations where hiding your IP address might be advisable. Consider a news group posting that you made today using an alias, and another one that you made a month ago, under your real name. If you have a static IP address, searching news groups for your IP address will show all your postings, no matter what name you used. This is just one of many possible scenarios.

Anyway, back to SmartWhois …

Complaining About Spam

Just a Few Clicks

Are you sick and tired of spam? We are too, sometimes to the extent that we want to complain about a particularly persistent spammer.

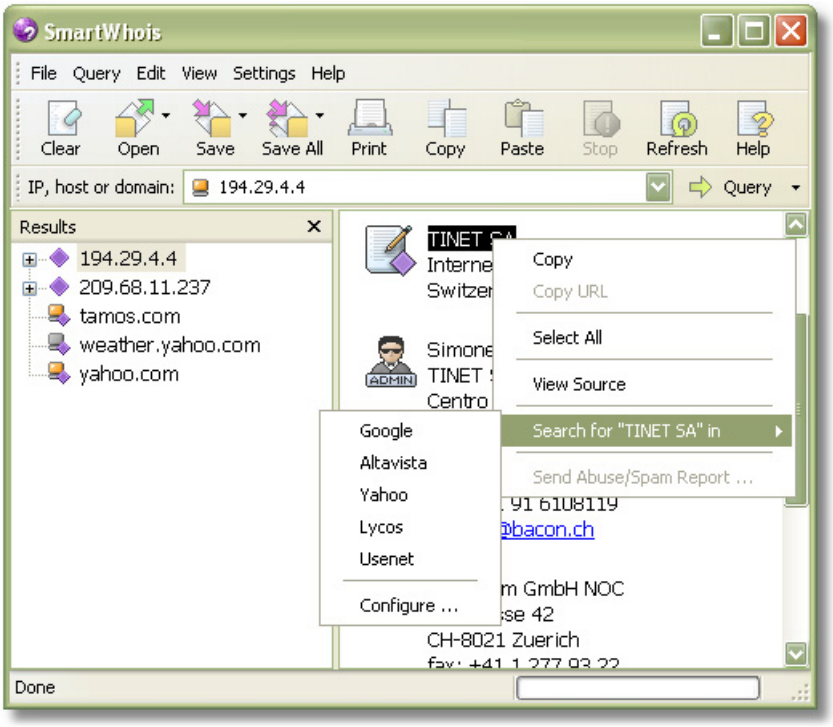


Carefully analyze the e-mail headers, find the spammer's IP address (the spammer could be using an open mail relay server or a "zombie" computer to send e-mail, but it's still good to let the ISP know), perform a SmartWhois query, locate the administrative or abuse contact, right-click on the e-mail address, and select **Send Abuse/Spam Report**. There you go, a new e-mail message will be opened in your e-mail client and pre-filled with the template. Be sure to edit the text and add the details. You can send the report in a matter of minutes!

Data Mining

Learning More Using SmartWhois as a Starting Point

SmartWhois is a great starting point for an online investigation. When you know the IP address or domain name that you want to learn more about, you can use SmartWhois for data mining. Select any part of the text in the right pane, right-click and use the **Search** command to search for the selected text using several search engines.



Examples? Sure! The "xyz.com" domain is registered by "John Doe, Ltd."? Fine, let's see what Altavista knows about John Doe, Ltd. You have received an e-mail sent from 4.4.4.4? Great, let's use Google to see what traces were left by that IP address on the Internet. Well, it's not something you can't do on your own using copy & paste commands, but it makes life easier. And you can configure this command to use any search engine.

SmartWhois for Advanced Users

Batch Processing, Exchanging Data, Custom Queries, and Other Tips

Now that we've talked about the program's core functionality, let's mention a few other useful things you can do with SmartWhois.

Some users need to query many IP addresses, host names or domains at a time. With SmartWhois, that's really easy. Click **File => Open => Batch File => As IP/Hostname List** or click **File => Open => Batch File => As Domain List** to have SmartWhois load and process a multi-line file. You can do the same using command-line arguments, which is described in the help file in detail. Command-line arguments even allow you to launch SmartWhois, have it process the list, save the results to a file and exit, all without any user interaction. There is only one thing to remember: It's a bad idea to overload Whois servers, so if your list contains a few thousand entries, there is a good chance that Whois servers will temporarily block your access to their service. You can, however, use the **Options** window to adjust the delay between the queries to reduce the server load. Be a good Netizen!

Once you've obtained the required data, there are a number of formats in which you can save the results. If you want to make a quick note of what you've just found, the easiest way is to drag-and-drop the contents of the right pane to the desktop. This will create an HTML file that you can view in your favorite browser. If you want to save many results and/or import the data into some other application, consider one of the other formats supported by SmartWhois, namely

XML, XLS, TXT, HTML, or SmartWhois native format. The latter is good when you want to load the saved file into SmartWhois and browse through the results.

Sometimes you need to perform Whois queries using extended syntax. For example, you may need to query a certain handle in a Whois database. This is not a problem: select **Query => Custom Query** to bring up a **Whois Console,** with which you are free to connect to any Whois server and send any query string.

Moving On

IP addresses, host names, and domains are an interesting part of Internet technology. We hope that this tutorial has been instrumental in understanding this technology and has provided some helpful hints on the usage of the ultimate Whois tool: SmartWhois.

Visit us today at www.tamos.com for more information, excellent technical support, instant online ordering, and more!