

## Re: Difference between "nslookup" and "whois" ?

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network\\_web/2008-03/msg00364.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2008-03/msg00364.html)

---

- *From:* "VanguardLH" <V@xxxxxxxx>
  - *Date:* Tue, 25 Mar 2008 05:58:32 -0500
- 

"Ken Philips" wrote in message [news:47e8a90f\\$0\\$4858\\$9b4e6d93@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:47e8a90f$0$4858$9b4e6d93@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

What is the difference between "nslookup" and "whois" ?  
For both I enter a domain name and get an IP.

Do use both the same sources?

Can I enter in both cases domain names with a 3rd level domain name e.g.

aaa.yahoo.com

-----  
NOTE: Ken used the FollowUp-To header in an attempt to disconnect the discussion from other than his "home" newsgroup. That is rude to the visitors of the other newsgroups. If your post is on-topic to the other newsgroups, and if you choose to post to those other newsgroups, then keep your discussion in those other newsgroups; else, do NOT post there if you don't want to have your discussion seen and participated there. The newsgroups list was restored in my reply. Spammers and malcontents use the FollowUp-To header to hide replies to their posts. Only in a few newsgroups is FollowUp-To appropriate, like when posting spam samples in NANAE.

Original newsgroups:

microsoft.public.windowsxp.network\_web,microsoft.public.windowsxp.help\_and\_support

FollowUp-To: microsoft.public.windowsxp.network\_web

Restored newsgroups:

microsoft.public.windowsxp.network\_web,microsoft.public.windowsxp.help\_and\_support

-----

'nslookup' queries your DNS server to get an IP address for the IP name that you specified. Humans like to use names. Computers only use numeric addresses. Hence the purpose of DNS. 'nslookup' can also do a reverse lookup to return back from your DNS server the IP name if you enter an IP address.

'whois' looks up the domain registration. That has nothing to do with IP addresses. Domain names are registered but may not even be implemented. Not until a domain is actually implemented at a webhost provider (you or someone else) to provide a site that uses that domain name is an IP address even involved. A 'whois' only lookup won't tell you the IP address of a domain. It tells you to whom that domain is registered (the registrant) and from whom that domain is leased (the registrar). A domain doesn't have an IP address until an equivalence gets propagated through DNS servers. You get the 'nslookup' result from your DNS server to

## Re: Difference between "nslookup" and "whois" ?

get back an IP address. You get the domain registrant information from using 'whois'. Until the domain is actually implemented, it doesn't have an IP address. In fact, you need to register a domain before you can even get an IP address for it. You could, for example, register a domain and never implement it so it will never have an IP address. Some registrants deliberately register domains and then park them while hoping someone wants to buy that domain name from them (i.e., they are domain squatters). The only reason you need a domain name is to have an IP name that humans can recognize but this requires propagating your domain name and its IP address to the DNS servers worldwide (unless it is just an internally accessible site in your own company or intranet). You could always use the IP address for a site and never use an IP name. Using <http://www.dyndns.org> requires the use of a DNS server to return to your computer an IP address for the [www.intel.com](http://www.intel.com) domain that you (or a program) specified while <http://63.208.196.100> never involves a DNS server because no lookup is required as your computer already has the IP address that it needs to find that host; however, many sites will use IP names in references to the objects within their own pages or to other pages or sites and using the IP address may not provide you good access to a site.

If your 'whois' utility is returning an IP address then it is providing more than the registrant information. Depends on \*whose\* 'whois' utility you are using. A real 'whois' lookup on a domain would return the registrant information even if that domain was implemented nowhere which means it has no IP address. The 'whois' portion of your whois utility would be querying some whois provider that does the domain registration lookup for you. You'll have to find out from your utility as to who that is. If it is providing an IP address, that comes from whatever is currently assigned as your DNS server (unless it has an option to configure a specify DNS server).

I have the 'whois' utility installed from SysInternals (now owned by Microsoft). It is coded to use whois-servers.net, by default, do go hunt for the domain registration information but a command-line parameter can specify using a different whois lookup provider. It returns just the domain registration information, not the IP address for that domain (if it is actually implemented). An IP address is not part of a domain's registration information, so this utility doesn't try to list it. If you want to see if your DNS server has a lookup on that domain name then use the 'nslookup' or 'ping' commands.

Each host has a different IP address so, yes, you need to specify the hostname in an IP name lookup to get an IP address for it. You always have to specify a fully qualified hostname. Your TCP configuration may provide for some defaults in qualifying the domain(s) when trying to find a host when only its hostname is specified. A site's nameserver can be configure to point at a particular host by default if the hostname is not specified. For example, "www" is still a hostname, as in [www.dyndns.org](http://www.dyndns.org). It is not the protocol for using HTTP to that domain. It is the \*host\* on that domain. Their nameserver will return the IP address for their "www" host if it isn't specified in the URL to their domain. So entering <http://dyndns.org> will default to their "www" host (so you end up at <http://www.dyndns.org>). Not all sites provide a default host if one is not specified. For example, <http://domain.com> will result in no site found but <http://www.domain.com> will work (I can't remember a specific example of where a site forgot to provide a default host lookup when queried for an IP address but the URL only has their domain and no host specified, but I have run across sites that forget to provide a default hostname).

yahoo.com is a domain. It does not specify a host. You connect to hosts, not domains. aaa.yahoo.com is a host. It is host "aaa" on domain "yahoo.com". The "yahoo.com" domain may provide a lookup to a default host "aaa" so using just the domain results in you connecting to \*host\* "aaa".

.