Regional Registries and NICs

Despite the "wild west" metaphors applied to the Internet, in one respect it is quite orderly. Domain names and IP addresses are assigned, registered, and stored in repositories around the world that are publicly accessible from anywhere. This means it is usually a simple matter to find an IP address given a domain name and vice versa. But the registries store other valuable information as well, such as who has registered the IP address, associated domain names, the network name, the registering organization name and address, and points of contact (usually system administrators), along with their phone/fax numbers and email addresses.

The **Internet Corporation for Assigned Names and Numbers (ICANN**) is the non-profit corporation that was formed to take over responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions previously performed under US-government contract by IANA, InterNIC, and other entities. While there is virtually no limit to the number of possible domain names, there are very definite limits to the number of IP addresses available, which means distribution and allocation of IP addresses is strictly controlled. IP address space is distributed hierarchically by **ICANN**, which allocates blocks of IP address space to Regional Internet Registries (**RIRs**) (more often called **Network Information Centers—NICs**). These RIRs in turn allocate blocks of IP addresses to **Local Internet Registries**. It is these local registries that assign IP addresses to **local ISPs**, who in turn allocate addresses to end users.

There are five **Regional Internet Registries:**

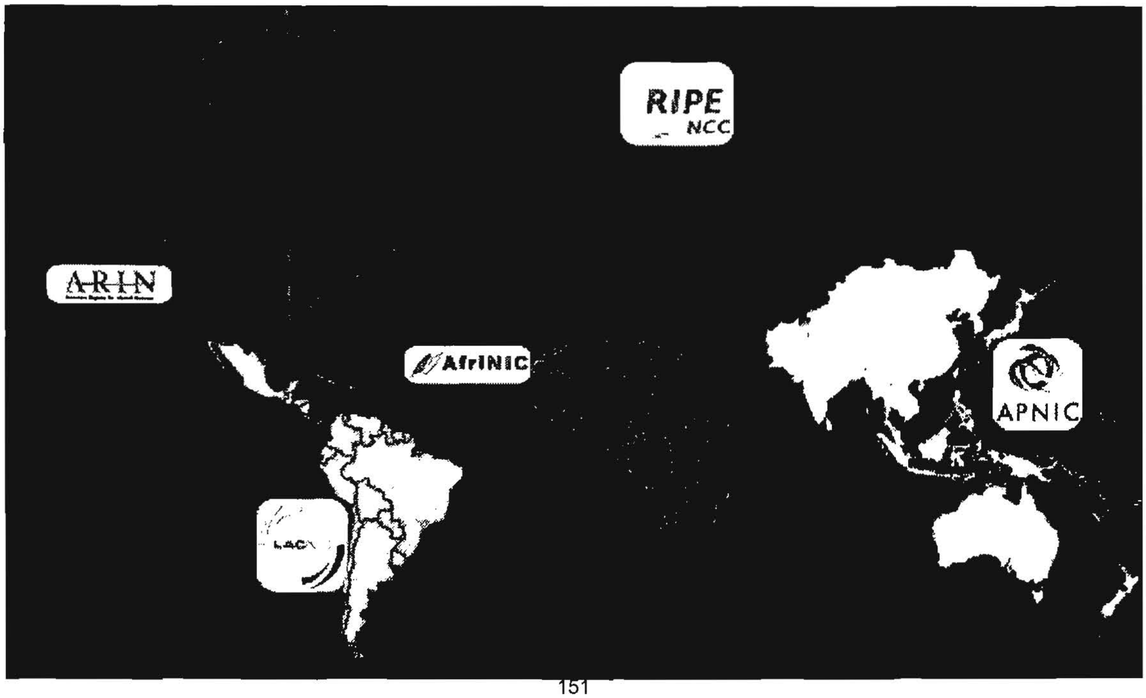
RIPE NCC for Europe and the Middle East

APNIC for the Asian/Pacific countries and

ARIN, the American Registry for Internet Numbers

LACNIC, the Latin American and Caribbean Network Information Center

AfriNIC, the African Network Information Center



[151]

ARIN took over **InterNIC's** responsibility for managing IP number assignments, though ARIN does not have the responsibility InterNIC once did for registering domain names. ARIN is modeled after RIPE and APNIC, that is, it is an independent non-profit corporation responsible for managing IP addresses for North America.

In December 2005, the new EU top-level domain opened for business. According to the European Registry of Internet Domain Names (EURid) website, "anyone based in the European Union can register a .eu domain name as long as it is available...EURid has more than 1000 accredited registrars from all over the world." At the same time as registration began, EUint opened a Whois search site for .eu domains. One indication of the popularity of the EU domain is that the Google search [site:eu] returns nearly 39 million hits.

European Registry of Internet Domain Names (EURid)
http://www.eurid.eu/en/registrant/

Complete List of Accredited EURid Registrars
http://list.eurid.eu/registrars/ListRegistrars.htm?lang=en

EURid Whois http://www.whois.eu/whois/GetDomainStatus.htm

[151] Number Resources Organization, <http://www.nro.net/about/get_resources.html> (30 January 2007).

I believe the best site for finding top-level domains and their associated Regional Internet Registry is maintained by the Number Resource Organization (NRO), which was formed by the five RIRs in 2003 "to formalise their co-operative efforts." The site includes a great deal of information about the RIRs, including a chart of each country and its associated RIR. RIPE also provides such a list.

NRO's List of Country Codes and RIRs	http://www.nro.net/about/rir-areas-rir.html
List of Country Codes and RIRs	http://www.ripe.net/info/resource-admin/rir-areas.html

ICANN and the Regional Internet Registries (aka NICs):

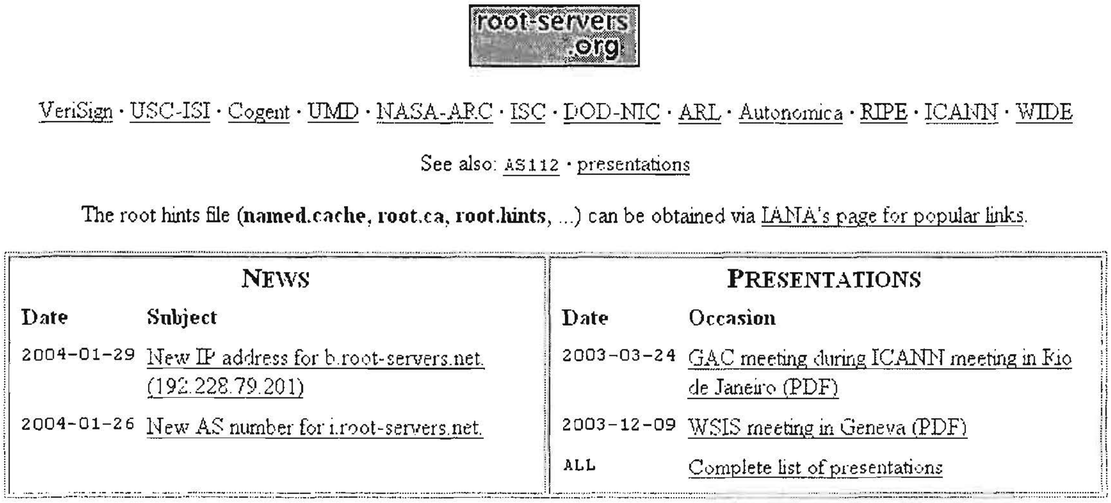
ICANN	http://www.icann.org
AfriNIC	http://www.afrinic.net/
APNIC	http://www.apnic.net
ARIN	http://www.arin.net
European Registry of Internet Domain Names (EURid)	http://www.eurid.eu/
LACNIC	http://lacnic.net/en
RIPE	http://www.ripe.net

The Ipv6 Transition

The current Internet addressing system uses IP version 4, and has for more than 20 years. However, the transition to IP version 6 (IPv6) is underway, especially in Europe and Asia.

The Internet Corporation for Assigned Names and Numbers (ICANN), the independent body that coordinates the Internet's address system, announced in July 2004 that IP version 6 (commonly written IPv6 and referred to as the "next generation" IP addressing system), has been added to the Internet's root server system. Vincent Cerf, an Internet "founding father" and a member of ICANN's board of directors, made the announcement at ICANN's annual meeting in Kuala Lumpur, Malaysia.

In practical terms, what does the addition of IPv6 mean? Today ***there are still only 13 root domain name servers that contain the master records for all Internet address mapping***.



root-servers .org

VeriSign · USC-ISI · Cogent · UMD · NASA-ARC · ISC · DOD-NIC · ARL · Autonomica · RIPE · ICANN · WIDE

See also: AS112 · presentations

The root hints file (**named.cache**, **root.ca**, **root.hints**, ...) can be obtained via IANA's page for popular links.

NEWS		PRESENTATIONS	
Date	**Subject**	**Date**	**Occasion**
2004-01-29	New IP address for b.root-servers.net. (192.228.79.201)	2003-03-24	GAC meeting during ICANN meeting in Rio de Janeiro (PDF)
2004-01-26	New AS number for i.root-servers.net.	2003-12-09	WSIS meeting in Geneva (PDF)
		ALL	Complete list of presentations

Root Servers.org http://www.root-servers.org/

This current set of rules used for Internet addresses, IPv4, became the Internet standard in 1981 and at that time it seemed as though it would provide enough addresses to last forever. But forever turned out to be a lot shorter than anyone anticipated, and the range of numbers used under the IPv4 is slowly running out; about two thirds of the 4.3 billion numbers allocated have been used. So a new set of rules, called IPv6, was created. IPv6 will increase the number of numerical addresses to 340 billion, billion, billion, billion numbers. This should be enough for the life of the Internet, in any event, regardless of how many computers, devices, or imaginary beings need to connect to it. IPv6 is also supposed to add reliability and security enhancements because of such features as built-in encryption.

I would not panic about some overnight shift from IPv4 to IPv6. Cerf said that the plan is for IPv6 to run parallel to IPv4 for about 20 years to ensure that any bugs or system errors are discovered and corrected. For more information on IPv6, see the IPv6 Information Page and read the November 2005 interview with Latif Ladid, founder of the IPv6 Forum, in which he asserts, "Overall, I would say that the show is happening in Asia, and in five years time you can expect China to be the biggest IPv6 user base in the world. By 2010 they will have two or three hundred million people using IPv6. Today the Western world will be taken by surprise. We are staying in denial."[152] IPv6 migration will happen—it's only a matter of when, not if.

Ipv6 Information Page http://www.ipv6.org/

[152] Dahna McConnachie, "IPv6 Forum Chief: The New Internet is Ready for Consumption," Computerworld, 18 November 2005, <http://www.computerworld.com.au/index.php?id=75779762> (15 November 2006).

The Shared Registration System

InterNIC, which was the original US-government sponsored domain name registry, no longer allocates IP addresses or registers domain names. Just as its IP address allocation functions were turned over to ARIN, its authority for registering the Top Level Domains (**TLD**s) .COM, .NET, .ORG and .EDU and, even more importantly, managing the vast database of registered domain names, was first assumed by **Network Solutions**.

In 1999, the **Shared Registration System** for the .COM, .NET, and .ORG domains was opened on equal terms to all accredited registrars, meaning that any company that meets ICANN's standards for accreditation is able to enter the market as a registrar and offer customers competitive domain name registration services in the . .COM, .NET, and .ORG domains.

More ***new generic top-level domains*** are being approved by ICANN all the time. Among those now in use are .BIZ, .INFO, .COOP, .AERO, .NAME, .PRO, and .MUSEUM with more on the way. For more information on these new TLDs, how to and who may register them, see the InterNIC FAQ on new top-level domains. <http://www.internic.net/faqs/new-tlds.html>

Shared Registration System (SRS) Warning!

If you look up a .com, .org, or .net domain name at the website of any SRS member (NSI, etc.), be careful! Your "domain name search will contain only technical information about the registered domain name and referral information for the registrar of the domain name. In the Shared Registration System model, registrars are responsible for maintaining Whois domain name contact information. To obtain information on the Registrant of a domain name, go to the registrar's web site listed."

What does this mean? To see the complete Whois record, you must go to the registrar's website or use a Whois browser interface that queries multiple Whois databases (more on this below).

The accuracy of the data in the Whois databases, however, is problematic. ICANN issued its first report on the accuracy of Whois database information in March 2004. The report is the first in what will be a series of annual reports on the status of complaints about Whois entries. Since ICANN instituted the Whois Data

Problem Report System (WDPRS) in September 2002 to let individual users report incorrect or incomplete domain registration information, they received over 24,000 complaints. Of those, nearly 5,000 of the complaints concerned domains containing incorrect or incomplete contact information—telephone numbers, email addresses, street addresses—for known or suspected spammers.

One problem with correcting inaccurate Whois information is that there is no real enforcement mechanism in place. Although all registrars accredited by ICANN to register domain names are required to provide "accurate and reliable contact details and promptly correct and update them during the term of the registered name registration," there is no process for following up to make sure reported inaccuracies are corrected or domain names taken away from offenders. The ICANN report claimed that "ICANN's experience has been that accredited registrars by and large do conscientiously comply with their contractual obligations by acting promptly to correct incomplete or inaccurate data that is brought to their attention." However, without stronger means of enforcing compliance, there is no way of ensuring Whois data is accurate and complete.

Whois Data Problem Report System	http://wdprs.internic.net/

Internet Myth:

You can tell a domain's country of origin by looking at its TLD.

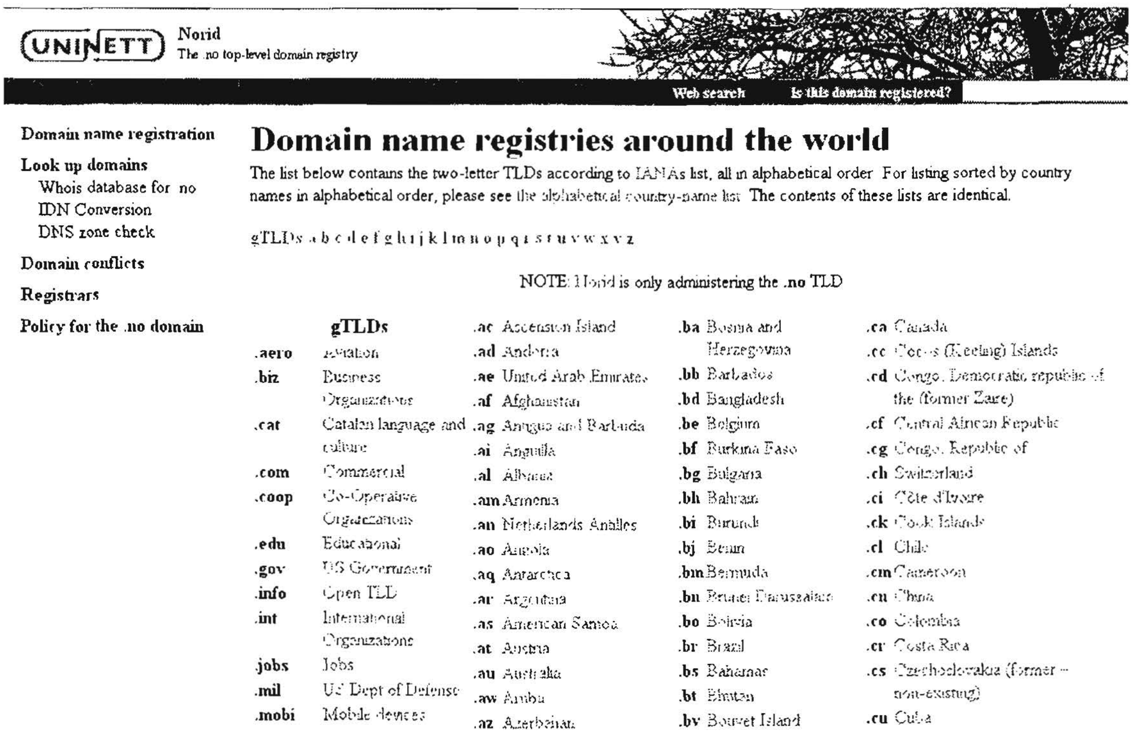
Internet Fact:

MANY foreign websites use .com, .net, and (to a lesser extent) other top-level domains, so not every foreign site will accurately reflect its country of origin by digraph. Moreover, many country registries will sell their TLD to anyone willing to pay. You cannot reliably determine country of origin by looking at a TLD.

Domain Name Registries

Every country has its own assigned top-level domain (ccTLD) in the form of a digraph: .de for Germany, .bo for Bolivia, etc. Finding the ccTLD administrator that registered a particular domain name is vital for finding all the available data registered about that name and its assigned IP address. Because local registries have the added responsibility for assigning domain names, they usually maintain separate databases that often provide more information than the regional repositories. Most national registries offer some kind of a searchable database of their registered domain names. Country-level registries are some of the best places to search for information about specific domains.

A number of websites list links to **domain name registries around the world**. All these sites present complete, up-to-date lists of **Internet country codes** (aka ccTLDs). Domain Name Registries Around the World offers both a country and digraph sort; IANA only lists the codes alphabetically by digraph.



Domain name registration

Look up domains

Whois database for .no

IDN Conversion

DNS zone check

Domain conflicts

Registrars

Policy for the .no domain

Domain name registries around the world

The list below contains the two-letter TLDs according to IANAs list, all in alphabetical order. For listing sorted by country names in alphabetical order, please see the alphabetical country-name list. The contents of these lists are identical.

gTLDs a b c d e f g h i j k l m n o p q r s t u v w x y z

NOTE: Norid is only administering the **.no** TLD

gTLDs	
.aero	Aviation
.biz	Business Organizations
.cat	Catalan language and culture
.com	Commercial
.coop	Co-Operative Organizations
.edu	Educational
.gov	US Government
.info	Open TLD
.int	International Organizations
.jobs	Jobs
.mil	US Dept of Defense
.mobi	Mobile devices

.ac	Ascension Island
.ad	Andorra
.ae	United Arab Emirates
.af	Afghanistan
.ag	Antigua and Barbuda
.ai	Anguilla
.al	Albania
.am	Armenia
.an	Netherlands Antilles
.ao	Angola
.aq	Antarctica
.ar	Argentina
.as	American Samoa
.at	Austria
.au	Australia
.aw	Aruba
.az	Azerbaijan

.ba	Bosnia and Herzegovina
.bb	Barbados
.bd	Bangladesh
.be	Belgium
.bf	Burkina Faso
.bg	Bulgaria
.bh	Bahrain
.bi	Burundi
.bj	Benin
.bm	Bermuda
.bn	Brunei Darussalam
.bo	Bolivia
.br	Brazil
.bs	Bahamas
.bt	Bhutan
.bv	Bouvet Island

.ca	Canada
.cc	Cocos (Keeling) Islands
.cd	Congo, Democratic republic of the (former Zaire)
.cf	Central African Republic
.cg	Congo, Republic of
.ch	Switzerland
.ci	Côte d'Ivoire
.ck	Cook Islands
.cl	Chile
.cm	Cameroon
.cn	China
.co	Colombia
.cr	Costa Rica
.cs	Czechoslovakia (former - non-existing)
.cu	Cuba

Domain Name Registries Around the World http://www.norid.no/domenenavnbaser/domreg.html

IANA's Contact List for TLD Administrators http://www.iana.org/root-whois/index.html

Yahoo's Computers and Internet Domain Name Registration
http://dir.yahoo.com/Computers and Internet/Internet/Domain Name Registration/→
Top Level Domains TLDs /Registry Operators/International Country Codes/

The Least You Need to Know about IPs and Domains

The Regional Internet Registries (aka NICs) are responsible solely for **IP address allocation and registration** (usually to Local Internet Registries or very large ISPs).

All five NICs (**ARIN**, **APNIC**, **AfriNIC**, **LACNIC**, and **RIPE**) maintain databases that contain formatted information about all IP addresses they have allocated or assigned, including those IP addresses its regional registries have authority to assign. **You can look up an IP number—but not a domain—at a NIC.**

"Local" registries (usually operating at country level, e.g., DENIC for Germany) register domain names and, in many cases, also allocate IP addresses.

Domain name registration for the **.com**, **.org.**, **.net**, **.biz**, **.info**, etc. TLDs has become a wide-open commercial enterprise. Anyone anywhere can register these TLDs.

Understanding Domain Name and Whois Lookup Tools

Domain names are nothing more than aliases for IP addresses; they are a convenience for human beings, who have more trouble remembering long numbers than letters, words, and names. But computers love numbers, so every time you enter a url (an address that contains the protocol, host, domain, directory, and file information), the computers that really *are* the Internet translate that name into its corresponding IP address. How do the computers know what domain name matches which IP number? **DNS**: the domain name system (or service). DNS is the Internet service that translates domain names, such as *www.amazon.com*, into IP addresses.

DNS is a huge *distributed database* residing on a network of servers. If a DNS server does not know how to translate a domain name, it will simply query another DNS server until it finds one that can translate the domain name to the correct IP address. Every server (a computer that offers services to other computers) connected to the Internet has some information about domain names; **DNS servers** keep huge lists of domain names matched with their IP addresses. Invisible to us the Internet users, the domain names are converted to their numerical addresses using the tables on DNS servers, and we get to where we want to be.

Web Tip

For a more detailed explanation of the Domain Name System/Service see:

The Domain Name Service
http://www.scit.wlv.ac.uk/~jphb/comms/dns.html

DNS and BIND, 3rd Edition, O'Reilly Online Catalog
http://www.oreilly.com/catalog/dns3/chapter/ch02.html

Fortunately, there are many freely accessible tools for accessing and analyzing the domain name system. Domain name and Whois lookup are among the most useful tools available on the Internet. Many different kinds of tools are used for gathering information about domain names and/or IP addresses. Before using these tools, it is helpful to review how domain names and IP addresses work together to make it possible for users to navigate the web and which Internet resources these tools access in order to provide information about domain names and IP addresses.

After the DNS, the Whois databases maintained by the Regional Internet Registries are the second major source of information about Internet addresses. The Whois databases contain records of IP address registrations. Searches that access the Whois databases are generally known as **network lookups** or **network Whois lookups**. In contrast to the DNS, the five Whois databases—ARIN, APNIC, AfriNIC, LACNIC, and RIPE—are *not distributed on servers across the Internet* but must be queried individually. In addition, these databases are designed to search on IP addresses, not domain names. A different type of tool should be used when searching on domain names. Unfortunately, to add to the confusion, this tool is also referred to as a Whois lookup!

In order to distinguish this third major resource from "true" Whois lookups, I will call it domain name (Whois) lookup. Domain name lookups search one or more **domain name registries**. Domain name registries are the places on the Internet where individuals and organizations go to register a name generally intended to be associated with a website, e.g., *amazon.com*. These registries include the **generic top-level domain (gTLD) registries** for .com, .net, .org, .biz, .info, and a few other gTLDs, as well as **country code top-level domain (ccTLD) registries**, e.g., .uk, .it, .ru, et al. Domain name (Whois) lookups differ from network Whois lookups in that they are primarily designed to search on a domain name instead of an IP address. All of the domain lookup tools described here can search more than one domain registry, and in some cases, will automatically search across all of them.

These are the various types of lookups that can be performed to learn more about Internet addresses.

➢ **NSLookup**—input format: either IP address or domain name

Using the DNS, a domain name is converted to its IP address (forward DNS lookup) or an IP address is converted to its host name (reverse DNS lookup).

NSLookup is a UNIX tool that allows anyone using the Internet to access the DNS and match domain names to IP addresses, or vice versa. Web interface query forms for NSLookup are very numerous. Although NSLookup doesn't do anything more than match domain names and IP addresses, this may be all you need or may give you the information you need to keep looking. For example, I have had domain names I could not match to any IP number using a Whois search. By running an NSLookup query I have found an IP number that I could then use to track down registration information about that domain.

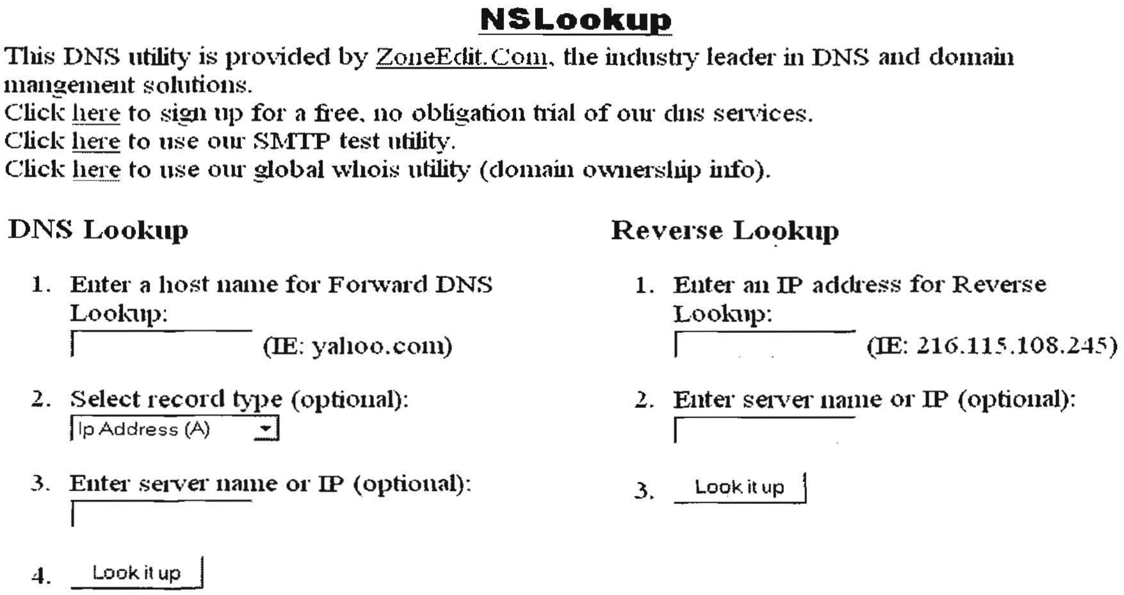
The advantage of NSLookup is that, unlike Whois requests, ***NSLookup queries can be run from anywhere*** on the Internet because the DNS data is not located in one database on one server but is distributed across a collection of intercommunicating computers, known as name servers, that translate domain names to IP addresses and vice versa.

NSLookup Tools

AnalogX	http://www.analogx.com/contents/dnsdig.htm
Check DNS	http://www.checkdns.net/quickcheck.aspx
DNS Stuff*	http://www.dnsstuff.com/
Eye-Net Consulting*	http://www.enc.com.au/itools/
Infobear	http://www.infobear.com/nslookup.shtml
Multiple NSLookup	http://www.bankes.com/nslookup.htm
SmartWhois NSLookup	http://swhois.net/
Squish DNS Lookup	http://www.squish.net/dnscheck/

A free service for DNS experts. "Given a record name, and a record type, you will receive a report detailing all possible answers. This is accomplished by traversing the DNS tree from the root examining all possible routes that a client could travel, calculating percentage probabilities on the way."

WebReference NsLookup Gateway	http://www.webreference.com/cgi-bin/nslookup.cgi
ZoneEdit NSLookup	http://www.zoneedit.com/lookup.html?ad=goto&kw=nslookup



NSLookup

This DNS utility is provided by ZoneEdit.Com, the industry leader in DNS and domain mangement solutions.
Click here to sign up for a free, no obligation trial of our dns services.
Click here to use our SMTP test utility.
Click here to use our global whois utility (domain ownership info).

DNS Lookup

1. Enter a host name for Forward DNS Lookup: (IE: yahoo.com)
2. Select record type (optional): Ip Address (A)
3. Enter server name or IP (optional):
4. Look it up

Reverse Lookup

1. Enter an IP address for Reverse Lookup: (IE: 216.115.108.245)
2. Enter server name or IP (optional):
3. Look it up

*These sites provide Ipv6 lookups in addition to Ipv4.

- **Network Whois Lookup**—input format: IP address

  IP address blocks are maintained by ARIN, RIPE, AfriNIC, LACNIC, and APNIC in separate, non-distributed databases. Formatted Whois data provides a wealth of registration information. All five Whois databases allow for advanced searches on fields other than IP address.

- **Domain Name (Whois) Lookup**—input format: domain name

  Checks a domain name against registration records based upon that domain name's TLD (.com, .uk, .ru, etc.); some automated programs can search some or all domain name registries at once.

The confusion about domain name and Whois lookups is probably in part caused by the fact that domain name registration is separate from IP address assignment. Perhaps the easiest way to understand this is to consider the following fictitious, overly simplistic example.

An imaginary Russian company named Moscow Motors wants to register two domain names: *moscowmotors.ru* and *moscowmotors.com*. But Moscow Motors only wants to use *one IP address* through its ISP, RT Communications (RTComm) Network in Moscow. The European Registry, RIPE, maintains the block of IP addresses handled by RTComm. Next, Moscow Motors goes to Network Solutions, Inc., to register its *moscowmotors.com* domain name and to RU-Center, the Russian top-level domain name registration service, to register its *moscowmotors.ru* domain name. Both domain names resolve to the same IP address registered with RIPE.

Now let's say a user runs a domain name lookup against *moscowmotors.com*. He finds the *domain name* is registered with Network Solutions, but when he tries to look up the *corresponding IP address* belonging to *moscowmotors.com,* he finds there is no network Whois record in the American Registry (ARIN) Whois database. Why? Because the ARIN Whois database only contains IP addresses assigned to it, and *moscowmotors.com* resolves to an IP address in the European (RIPE) database.

If you would like to see a real-life example of what I've just described, try the following:

1. Go to Domain Dossier (http://centralops.net/co/DomainDossier.vbs.asp) and enter the following query:
   ripe.net
   search on *domain whois record* and *network whois record*

2. Look at the IP address for *ripe.net*: 193.0.0.203

3. Look at the Domain Whois record: *ripe.net* is registered with Network Solutions, Inc.

4. Look at the Network Whois records: 193.0.0.203 is not registered in the ARIN (American) Whois database; it is registered in the RIPE (European) Whois database.

One point of this example is to warn people against making assumptions about the relationship between domain names and IP addresses, especially the generic TLDs such as .com, .net, .org, .info, .and .biz. Do not assume that a domain name in any of these generic TLDs will have an IP address registered by ARIN, the North American Registry. However, ***Local Registries (usually country-level registries) often have restrictions on who can and cannot register their top-level domains***. In these cases, IP addresses and domain names are more likely to correspond (e.g., a .ru domain almost certainly has an IP address registered in the RIPE database), but even in these cases, there are exceptions.

There are many variations in the precise type, format, quantity, and quality of the information each tool described below provides. I will explain the features of each so you can get an idea of which tool to use in which circumstance. For each tool I have listed its special features so you can quickly determine which tool is right for your specific research need.

World Network Whois Databases: AfriNIC, APNIC, ARIN, LACNIC, & RIPE

Special features: official international registrars of IP addresses; advanced search on many other fields in Whois database.

All five international registrars permit simple and advanced queries of the Whois databases via web interfaces. ***Each database must be queried separately***; however, there are third-party sites that will query all these databases at one time. Advanced search pages at each site give instructions on which fields in the Whois database can be searched. For example, all the Whois advanced searches permit lookups of network name, person (may or may not be an individual), AS (autonomous system) number, and even an associated domain, although these Whois databases should not be used for domain name lookups.

For anything and everything you ever wanted to know about Whois databases, refer to the **RIPE Database Reference Manual**. The manual's instructions also apply to the ARIN and APNIC databases.

RIPE Database Reference Manual http://www.ripe.net/ripe/docs/databaseref-manual.html

APNIC Whois lookups http://www.apnic.net/search/index.html

APNIC Whois help http://www.apnic.net/db/search/all-options.html

IP address registration for Asia-Pacific countries.

ARIN http://www.arin.net/whois/index.html

IP address registration for North America.

ARIN Whois help http://www.arin.net/tools/whois_help.html

AfriNIC Whois http://www.afrinic.net/cgi-bin/whois

AfriNIC Database User Manual http://www.afrinic.net/docs/db/afsup-dbgs200501.htm

EURid Whois http://www.whois.eu/whois/GetDomainStatus.htm

LACNIC Whois http://lacnic.net/cgi-bin/lacnic/whois

RIPE http://www.ripe.net/perl/whois/

IP address registration for Europe, North Africa, and the Middle East .

RIPE Whois help http://www.ripe.net/ripencc/pub-services/db/whois/whoishelp.html

Global Network Whois Search Tools

The following sites offer web interfaces that will either search all five regional Whois databases at once or individually.

Whois at Webhosting.info http://whois.webhosting.info/

Special features: shows hosting company name with total domains and gives reverse IP list.

Describing itself as "power whois," Web Hosting's advanced Whois service gives some additional bits of information that don't come with traditional whois lookups:

- Web Hosting Company hosting the domain name.
- Current IP Address of the domain.
- Geographical location of the IP Address.
- Reverse IP Facility - Lists all domains hosted on an IP Address.
- Domain Owner Details - Registrant, Admin Contact, etc.

MSV.DK Network Whois http://msv.dk/ms593.aspx

Special feature: searches across all registries.

Will quickly search all three main Whois databases ARIN, APNIC, and RIPE.

IP-Plus http://www.ip-plus.ch/tools/whois_set.en.html

Special feature: in addition to the main Whois databases, option to search several other country-level Network Information Centers.

Does not search all Whois databases at once; each must be searched individually from pull-down menu.

DNS411 http://dns411.com/

Special feature: "smart Whois" searches across all Whois databases automatically.

DNS411 uses the "smart Whois" search to perform universal IP address and domain names lookups. Even though the search form says to enter a domain name, it searches on IP addresses as well. In addition, DNS411 will search on second-level domain names, e.g., [amazon.co.uk], NIC Handles (unique identifiers assigned to each domain name, contact, and network records in a registrar's database), IP addresses, Autonomous System (AS) numbers, and Netblock Handles automatically across all registries. See the "tips" page for details.

Network-Tools http://network-tools.com/

Special feature: in addition to network Whois lookups, offers full range of network lookup tools on one page.

Does not search all Whois databases at once; each must be searched individually from pull-down menu. Also offers other network tools: ping, NSLookup, traceroute, DNS records, etc.

Geektools http://www.geektools.com/whois.php

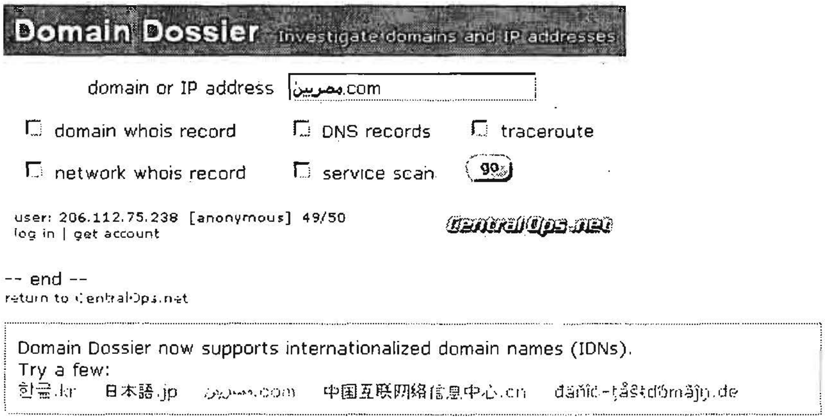
Special feature: automatic domain name/IP address search across all registries.

Geektools has long been a staple of many research toolkits by providing a fast and easy universal Whois lookup for both domain names and IP addresses. Must enter full name (domain plus TLD) or IP number (no partial searches or wildcard function).

Domain Dossier http://centralops.net/co/DomainDossier.vbs.asp

Special Features: searches across all the network Whois Registries, shows DNS records, and performs service scan from one query. Domain Dossier now supports internationalized domain names (IDNs).

Domain Dossier is one of the best lookup tools for a fast, thorough search of the three main network Whois Registries (ARIN, RIPE, APNIC). Select "network whois record" for automatic search of IP or domain name; results include canonical name, aliases, and IP addresses.



Domain Dossier Investigate domains and IP addresses

domain or IP address مصريين.com

□ domain whois record □ DNS records □ traceroute

□ network whois record □ service scan

user: 206.112.75.238 [anonymous] 49/50
log in | get account

-- end --
return to CentralOps.net

Domain Dossier now supports internationalized domain names (IDNs).
Try a few:
한글.kr 日本語.jp [illegible].com 中国互联网络信息中心.cn dänic-tåstdömäjn.de

Domain Name Whois Lookups

Each site described below either has the ability to search for domain names across all TLDs or has some sort of wildcard function when searching for domain names. **Wildcard functions** are highlighted in **red**. ***Some sites will search on second-level domain names*** (e.g., *mfa.co.jp*).

Allwhois http://www.allwhois.com/

Special features: search any TLD; full Whois output directly from appropriate database; alphabetical list of country NICs with links to websites; second-level domain name search.

Allwhois automatically queries the appropriate Whois database for registration information. The output, which appears in a small window below the query box, is directly from the Whois database without any changes. Allwhois's other useful feature is an alphabetical list of registries around the world (with the corresponding country code listed next to the country name). You can "jump to" any registry's Whois page directly from Allwhois. However, keep in mind that this list of Whois pages is not complete. For example. Saudi Arabia has a NIC with a Whois tool, but it is not on the list.

Checkdomains http://www.checkdomain.com/

Special features: universal search domain names across all TLDs at once; search on second-level domains.

Checkdomain.com will check for registrations of any domain name across all registries. Checkdomain will also search for second-level domain names, such as cars.co.uk, and provide registration information for them.

CoolWhois http://www.coolwhois.com/

Special Features: universal domain name search across all TLDs; search on second-level domains; bookmarklet can be added to the browser toolbar.

CoolWhois really is. It is a true cross-domain name search tool that automatically looks up a domain name in any TLD. An added feature of CoolWhois is a neat little bookmarklet, a piece of JavaScript that you add to your browser toolbar simply by dragging and dropping it there. Once it's there, all you have to do to perform a domain name lookup on any page you're viewing is to click on the CoolWhois bookmarklet (which looks exactly like a personal toolbar link).

DNS411 http://dns411.com

Special features: universal domain name search across all TLDs; search on second-level domains; many other unusual lookup options.

DNS411 uses the "smart Whois" search to perform universal domain names lookups. In addition, DNS411 will search on second-level domain names (e.g., *amazon.co.uk*), NIC Handles (unique identifiers assigned to each domain name, contact, and network records in a registrar's database), IP addresses, Autonomous System (AS) numbers, and Netblock Handles automatically across all registries. See the "tips" page for details.

DrWhois http://www.drwhois.com/

Special feature: universal domain name/IP address search across all TLDs.

DrWhois searches for domain names or IP addresses across all registries and will also search on second-level domain names such as [mfa.gov.ir].

Domain Dossier http://centralops.net/co/DomainDossier.vbs.asp

Special Features: searches across all the network Whois Registries, shows DNS records, and performs service scan from one query. Domain Dossier now supports internationalized domain names (IDNs).

Domain Dossier is one of the best lookup tools for a fast, thorough search of the three major network Whois Registries (ARIN, RIPE, APNIC). Domain Dossier also automatically searches the InterNIC and Open SRS domain Whois records, provides DNS records (name servers, mail exchanges, etc.), and performs a service scan, which shows the status of FTP, SMTP, HTTP, POP3, and NNTP Ports.

Domainsearch http://www.domainsearch.com/

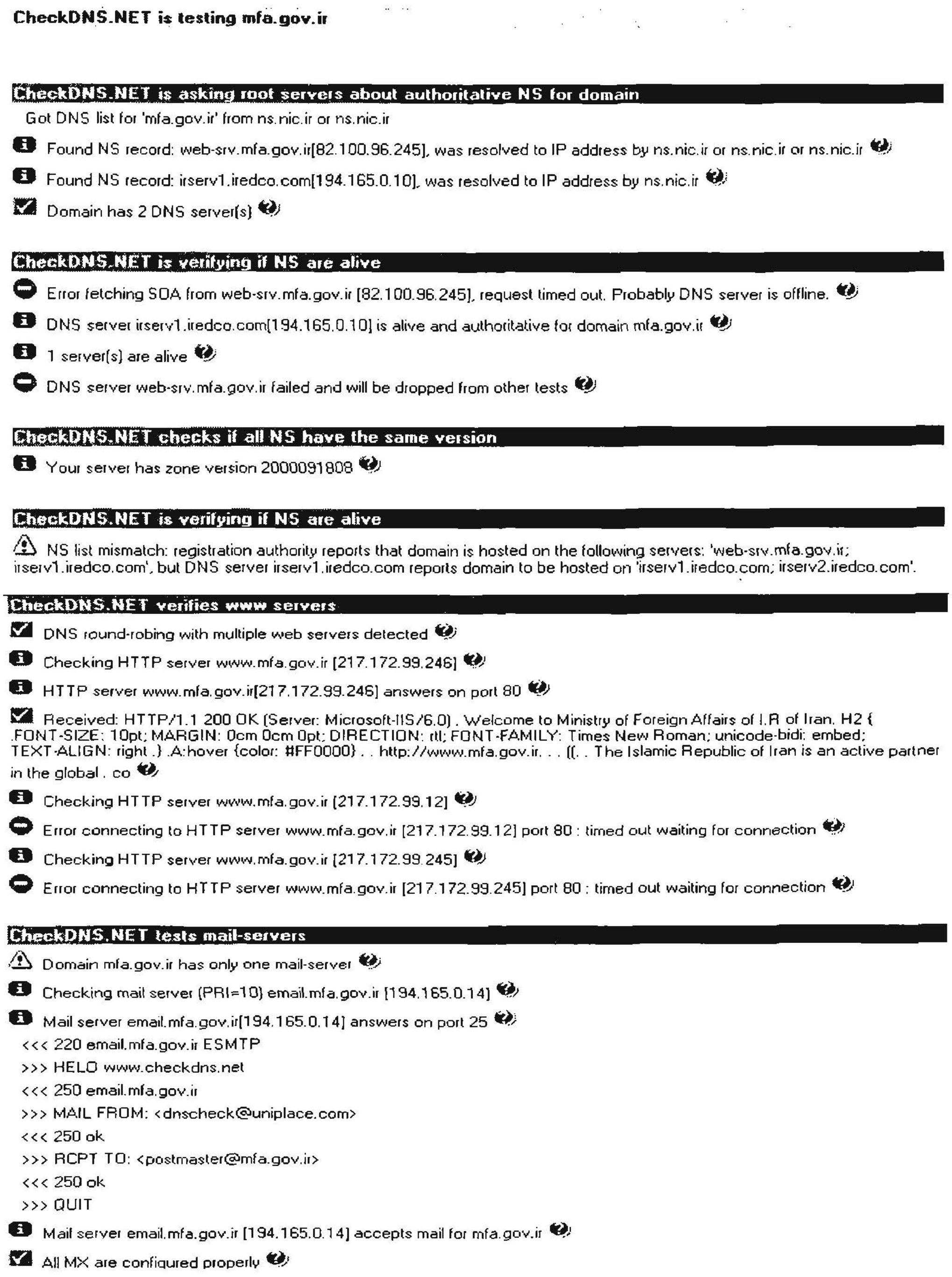
Special feature: search domain name against many combinations of TLDs, including many second-level domains.

The advantage of Domainsearch.com is that it allows you to check a domain name's registration against many available extensions at once. You enter a domain name without any extension into the search box, then select the extensions you want to search using the CTRL key for multiple selections. Domainsearch includes not only TLDs (e.g., .au) but also many second-level domains, (e.g., com.au). If a name is registered, it will appear with a small "i" inside a blue circle; clicking on the "i" brings up the Whois data for that domain name. Not all TLDs are listed as extensions.

CheckDNS http://www.checkdns.net/quickcheckdomainf.aspx

Special feature: generates the most detailed domain report available for free on the web.

CheckDNS.NET can check DNS delegation, mail and web servers for any domain. The detailed report that is generated is, I believe, unique among the various Whois tools available for free:



CheckDNS.NET is testing mfa.gov.ir

CheckDNS.NET is asking root servers about authoritative NS for domain

Got DNS list for 'mfa.gov.ir' from ns.nic.ir or ns.nic.ir

ℹ Found NS record: web-srv.mfa.gov.ir[82.100.96.245], was resolved to IP address by ns.nic.ir or ns.nic.ir or ns.nic.ir

ℹ Found NS record: irserv1.iredco.com[194.165.0.10], was resolved to IP address by ns.nic.ir

☑ Domain has 2 DNS server(s)

CheckDNS.NET is verifying if NS are alive

⊖ Error fetching SOA from web-srv.mfa.gov.ir [82.100.96.245], request timed out. Probably DNS server is offline.

ℹ DNS server irserv1.iredco.com[194.165.0.10] is alive and authoritative for domain mfa.gov.ir

ℹ 1 server(s) are alive

⊖ DNS server web-srv.mfa.gov.ir failed and will be dropped from other tests

CheckDNS.NET checks if all NS have the same version

ℹ Your server has zone version 2000091808

CheckDNS.NET is verifying if NS are alive

⚠ NS list mismatch: registration authority reports that domain is hosted on the following servers: 'web-srv.mfa.gov.ir; irserv1.iredco.com', but DNS server irserv1.iredco.com reports domain to be hosted on 'irserv1.iredco.com; irserv2.iredco.com'.

CheckDNS.NET verifies www servers

☑ DNS round-robing with multiple web servers detected

ℹ Checking HTTP server www.mfa.gov.ir [217.172.99.246]

ℹ HTTP server www.mfa.gov.ir[217.172.99.246] answers on port 80

☑ Received: HTTP/1.1 200 OK (Server: Microsoft-IIS/6.0) . Welcome to Ministry of Foreign Affairs of I.R of Iran. H2 { .FONT-SIZE: 10pt; MARGIN: 0cm 0cm 0pt; DIRECTION: rtl; FONT-FAMILY: Times New Roman; unicode-bidi: embed; TEXT-ALIGN: right .} .A:hover {color: #FF0000} . . http://www.mfa.gov.ir. . . ((. . The Islamic Republic of Iran is an active partner in the global . co

ℹ Checking HTTP server www.mfa.gov.ir [217.172.99.12]

⊖ Error connecting to HTTP server www.mfa.gov.ir [217.172.99.12] port 80 : timed out waiting for connection

ℹ Checking HTTP server www.mfa.gov.ir [217.172.99.245]

⊖ Error connecting to HTTP server www.mfa.gov.ir [217.172.99.245] port 80 : timed out waiting for connection

CheckDNS.NET tests mail-servers

⚠ Domain mfa.gov.ir has only one mail-server

ℹ Checking mail server (PRI=10) email.mfa.gov.ir [194.165.0.14]

ℹ Mail server email.mfa.gov.ir[194.165.0.14] answers on port 25

```
<<< 220 email.mfa.gov.ir ESMTP
>>> HELO www.checkdns.net
<<< 250 email.mfa.gov.ir
>>> MAIL FROM: <dnscheck@uniplace.com>
<<< 250 ok
>>> RCPT TO: <postmaster@mfa.gov.ir>
<<< 250 ok
>>> QUIT
```

ℹ Mail server email.mfa.gov.ir [194.165.0.14] accepts mail for mfa.gov.ir

☑ All MX are configured properly

Domainsurfer http://www.domainsurfer.com/

Special feature: offers some **wildcard** search capability for domain names registered in major gTLDs.

Domainsurfer offers some degree of wildcard searching. If you simply search for any domain name without a TLD extension, Domainsurfer will find all appearances of that search string regardless of where the string appears in the domain name. For example, if I search for [sonia], Domainsurfer will find *smith**sonia**n* as well as ***sonia**-net*. In order to find domain names that begin with a string, prepend a carat (^) to the string, e.g., to find *sonia-net* but not *smithsonian*, the query is [^sonia]. Only queries the .com, .org, .net, .biz, .info gTLDs.

EasyWhois http://www.easywhois.com/

Special feature: automatic universal first- and second-level Whois lookups.

Automatically searches for most gTLD and country-level domains, including second-level domains,. e.g., [amazon.co.uk] In March 2004, EasyWhois found it necessary to add a Turing number field to cut down the autobots and data mining activity. All this means is that you must enter the number in the green box before running a query.

Geektools http://www.geektools.com/whois.php

Special feature: universal domain name/IP address search across all TLDs.

Geektools has long been a staple of many analyst toolkits by providing a fast and easy universal Whois lookup for both domain names and IP addresses. Users must enter full name (domain plus TLD) or IP number (no partial searches or wildcard function). Geektools also requires users to enter the text shown below in the **Key** field before submitting a query because of autobots and data mining activity.

Namedroppers http://www.namedroppers.com/

Special feature: unusual **wildcard** option to run multiple keyword searches for domain names in the major gTLDs.

Namedroppers offers a different approach: you can enter a number of keywords to include or exclude in your search. So, a search for domain names that contain the keywords [national] and [security] and exclude the keyword association will find 153 domain names out of 29 million, including *nationalairportsecurity.com* and *internationalnetsecurity.com*. Unfortunately, Namedroppers only queries .com, .net, .org, and .edu TLDs.

Multiple DNS Lookup Engine http://www.bankes.com/nslookup.htm

Special feature: performs simple automatic network mapping.

Another invaluable web tool, the Multiple DNS Lookup Engine does something unique, as far as I know: it steps you through an entire IP address block (up or down). You either enter an IP address or a domain name and decide whether you want the lookup tool to step up or down from that address. The tool then lists the next address in the "neighborhood," associated IP or domain name, and in some cases, links to registration information. This tool is ideal for mapping a network.

Netcraft http://searchdns.netcraft.com/?host

Netcraft Search Help http://searchdns.netcraft.com/?help=yes

Special features: true **wildcard** function against all TLDs; provides information about what a site is running.

Netcraft is many researchers' favorite lookup tool because of its flexibility and power. Netcraft is designed to perform wildcard searches of domain names and it queries all TLD extensions. The simple search offers the option of searching for a domain name where the search string contains/starts with/ends with or matches a subdomain.[153] Netcraft also offers three wildcard options: * matches any number of characters; ? matches a single character; [ ] matches on specified characters. A search for [*.sc[aeio].com] returns all domains that contain *sca.com*, *sce.com*, *sci.com*, or *sco.com*. A search for sites that contain ".ir" returns sites such as www.irs.gov, whereas a search for [*.ir] finds only those sites in the Iranian domain. If you search for [*.gov.ir] Netcraft returns 11 sites, including "www.mfa.gov.ir" and "intranet.mim.gov.ir." What's more, for each hit, you have the option of seeing "what's that site running," which provides information about the operating system and web server at the site.

Whois.net http://www.whois.net/

Special feature: **wildcard** matches search string anywhere in domain name, or string anchored right or left.

Now that Whois.net searches most TLDs, it is one of the very best lookup tools on the web. As with Domainsurfer, the Whois.net keyword search will find *smith**sonian*** as well as ***sonia**-net* in its default mode. In order to find domain names that begin or end with a string, use the advanced search form, which is accessible from the ***search results' page***.

[153] As of this writing, the "site starts with" and "site ends with" options are all resolving to "site contains."

Domain Tools Whois Source http://whois.domaintools.com/

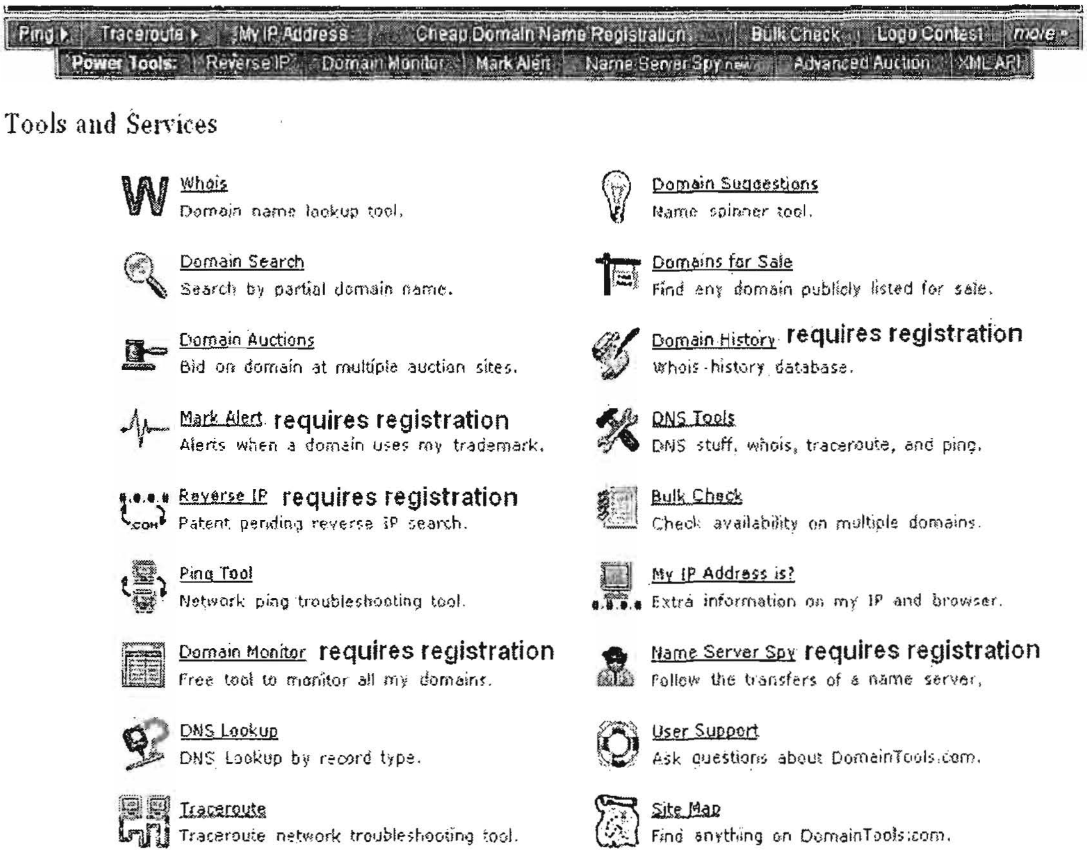
Domain Tools and Services http://www.domaintools.com/services/

Special features: option-rich search includes using **wildcards** to search for domain names; displays an image of the home page for domain records with websites.

One of the best Internet tool sites, Whois Source, was put under the umbrella of DomainTools.com. In most ways, it remains the same, but its interface is new and, I think, even nicer. The biggest and best change is the fact that ***the site now queries all top-level domains*** and not just the usual .com, .net, etc., it had queried in the past. Unfortunately, many of the tools offered require free registration (with an email address), but there are still many options available.

Another useful trick that still works is to ***type* [whois.sc/sampledomain.com] *into your browser's address bar to get the Whois records for that domain***. This is a very nice to know tip that doesn't require any special software or script.

Here is a snapshot of DomainTools.com's tools and services, and I have indicated which tools require registration. The remainder are fundamentally the same as those at the original site.



Tools and Services

Whois
Domain name lookup tool.

Domain Search
Search by partial domain name.

Domain Auctions
Bid on domain at multiple auction sites.

Mark Alert requires registration
Alerts when a domain uses my trademark.

Reverse IP requires registration
Patent pending reverse IP search.

Ping Tool
Network ping troubleshooting tool.

Domain Monitor requires registration
Free tool to monitor all my domains.

DNS Lookup
DNS Lookup by record type.

Traceroute
Traceroute network troubleshooting tool.

Domain Suggestions
Name spinner tool.

Domains for Sale
Find any domain publicly listed for sale.

Domain History requires registration
Whois-history database.

DNS Tools
DNS stuff, whois, traceroute, and ping.

Bulk Check
Check availability on multiple domains.

My IP Address is?
Extra information on my IP and browser.

Name Server Spy requires registration
Follow the transfers of a name server.

User Support
Ask questions about DomainTools.com.

Site Map
Find anything on DomainTools.com.

Domain Tools offers more features than just about any other domain name search tool. Users can search on one or more terms, using only partial word(s). It also displays an image of the home page that corresponds to the domain registration record. When you search on a domain and view the Domain Tools information, the data provided includes:

- Page information
  - website title with hyperlink to the homepage;
  - metadata description from website's own HTML meta description tag;
  - meta-keywords from website's own HTML meta keywords tag;
  - About us: link to Wikipedia article (if applicable);
  - related sites.
- Indexed Data
  - entries at Open Directory, Alexa Ranking and Trend tracking, and Y! Directory;
  - the number of listings on the site in both the Yahoo directory and DMOZ Open Directory with a link to all those listings; the directory listings show the category within the directory (e.g., History, News & Media), the title of the specific link within the domain (e.g., "History of Religions in Iran"), the description of the link, and the url itself.
  - The Alexa data shows both the site's rank for the past one and three months in terms of traffic and whether the traffic trend is up or down.
- Server Data
  - type of server on which the site runs;
  - IP address plus options for **W** (run whois lookup), **P** (ping this address), **D** (run a DNS lookup on this address), and **T** (run a traceroute to this address);
  - IP location, i.e., the physical location of the server hosting the domain (this may not always be accurate);
  - Response code[154], which indicates status of server;

[52] Joe Burns, "Server Response Codes," HTML Goodies, <http://www.htmlgoodies.com/tutors/src.html> (14 November 2006).

- Blacklist status, which indicates if a site has been blacklisted for sending spam;
- SSL cert: whether or not site has a site security certificate and when it expires;
- Website status: active, parked/redirected, on-hold, deleted, etc.

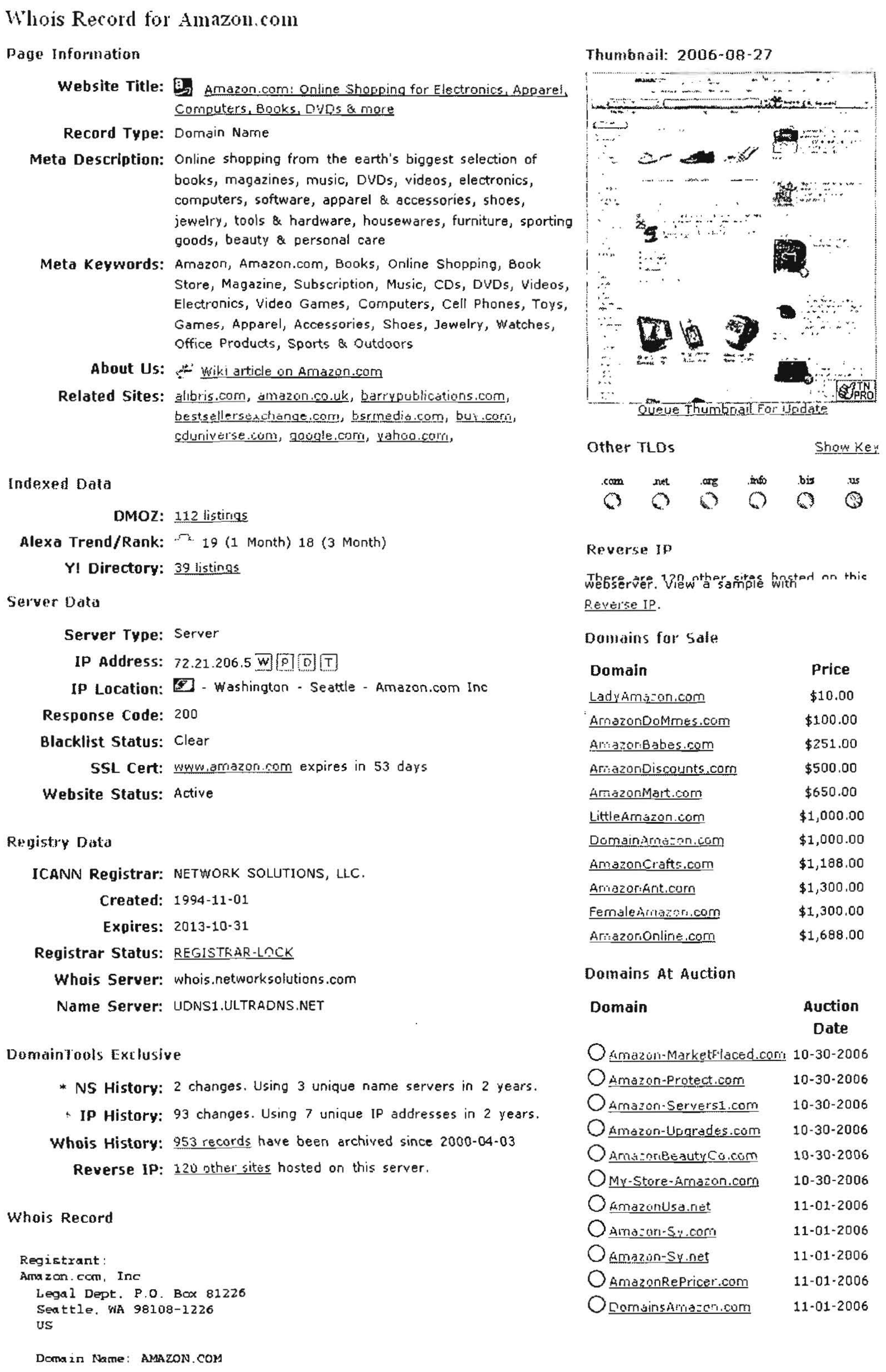
➢ Registry Data

- ICANN Registrar: the registry with which the domain name registered (e.g., Network Solutions);
- Created: date domain name was originally created;
- Expires: date domain name will expire;
- Registrar Status: the registry generally sets domain name status codes. Domain Tools provides a detailed explanation of each code;
- Whois server for the domain (where to get a full whois record);
- Name server for the domain (host that that enables the domain name to be resolved to an IP address).

➢ Domaintools Exclusive: special information provided by Domain Tools, including:

- NS history: how often the nameserver for this domain has changed;
- IP history: how often the IP address for this domain has changed;
- Whois history: historical whois lookups done by users of Domain Tools (requires registration);
- Reverse IP or the number of hosts (computers) this webserver hosts (to see them requires free registration).

➢ Whois record is displayed at the bottom of the page.



Whois Record for Amazon.com

Page Information

Website Title: Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more

Record Type: Domain Name

Meta Description: Online shopping from the earth's biggest selection of books, magazines, music, DVDs, videos, electronics, computers, software, apparel & accessories, shoes, jewelry, tools & hardware, housewares, furniture, sporting goods, beauty & personal care

Meta Keywords: Amazon, Amazon.com, Books, Online Shopping, Book Store, Magazine, Subscription, Music, CDs, DVDs, Videos, Electronics, Video Games, Computers, Cell Phones, Toys, Games, Apparel, Accessories, Shoes, Jewelry, Watches, Office Products, Sports & Outdoors

About Us: Wiki article on Amazon.com

Related Sites: alibris.com, amazon.co.uk, barrypublications.com, bestsellersexchange.com, bsrmedia.com, buy.com, cduniverse.com, google.com, yahoo.com,

Indexed Data

DMOZ: 112 listings

Alexa Trend/Rank: 19 (1 Month) 18 (3 Month)

Y! Directory: 39 listings

Server Data

Server Type: Server

IP Address: 72.21.206.5 W P D T

IP Location: - Washington - Seattle - Amazon.com Inc

Response Code: 200

Blacklist Status: Clear

SSL Cert: www.amazon.com expires in 53 days

Website Status: Active

Registry Data

ICANN Registrar: NETWORK SOLUTIONS, LLC.

Created: 1994-11-01

Expires: 2013-10-31

Registrar Status: REGISTRAR-LOCK

Whois Server: whois.networksolutions.com

Name Server: UDNS1.ULTRADNS.NET

DomainTools Exclusive

*** NS History:** 2 changes. Using 3 unique name servers in 2 years.

*** IP History:** 93 changes. Using 7 unique IP addresses in 2 years.

Whois History: 953 records have been archived since 2000-04-03

Reverse IP: 120 other sites hosted on this server.

Whois Record

```
Registrant:
Amazon.com, Inc
   Legal Dept. P.O. Box 81226
   Seattle, WA 98108-1226
   US

   Domain Name: AMAZON.COM
```

Thumbnail: 2006-08-27

Queue Thumbnail For Update

Other TLDs

Show Key

.com	.net	.org	.info	.biz	.us
○	○	○	○	○	○

Reverse IP

There are 120 other sites hosted on this webserver. View a sample with Reverse IP.

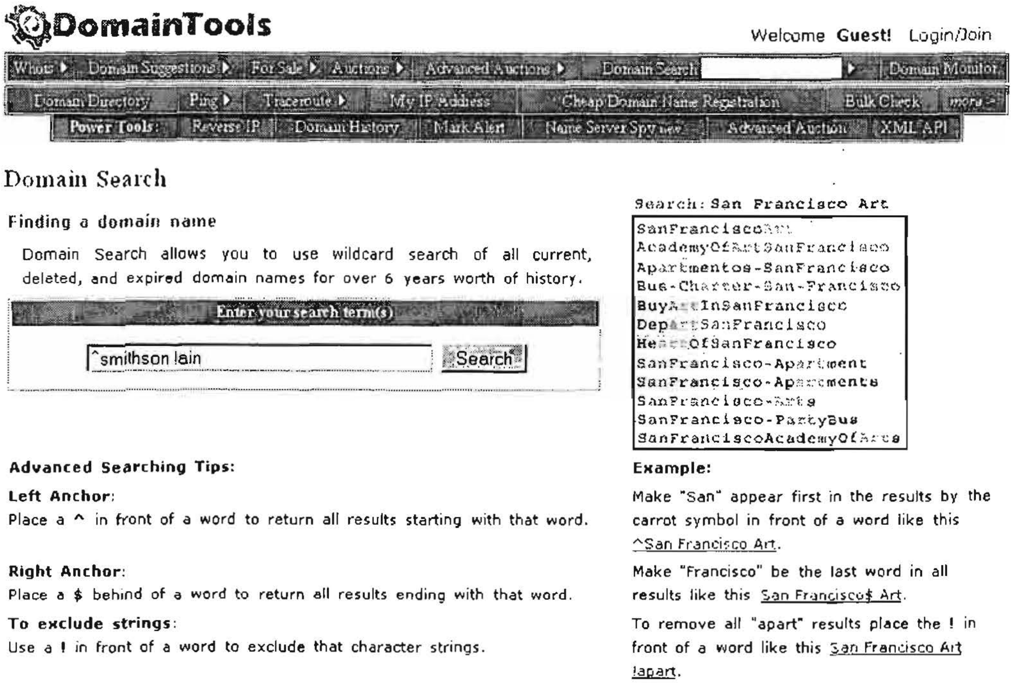
Domains for Sale

Domain	Price
LadyAmazon.com	$10.00
AmazonDoMmes.com	$100.00
AmazonBabes.com	$251.00
AmazonDiscounts.com	$500.00
AmazonMart.com	$650.00
LittleAmazon.com	$1,000.00
DomainAmazon.com	$1,000.00
AmazonCrafts.com	$1,188.00
AmazonAnt.com	$1,300.00
FemaleAmazon.com	$1,300.00
AmazonOnline.com	$1,688.00

Domains At Auction

Domain	Auction Date
○ Amazon-MarketPlaced.com	10-30-2006
○ Amazon-Protect.com	10-30-2006
○ Amazon-Servers1.com	10-30-2006
○ Amazon-Upgrades.com	10-30-2006
○ AmazonBeautyCo.com	10-30-2006
○ My-Store-Amazon.com	10-30-2006
○ AmazonUsa.net	11-01-2006
○ Amazon-Sy.com	11-01-2006
○ Amazon-Sy.net	11-01-2006
○ AmazonRePricer.com	11-01-2006
○ DomainsAmazon.com	11-01-2006

In addition, Domain Tools offers very sophisticated and somewhat confusing **wildcard** options. From the Domain Tools home page, go to More Tools and Services, then select Domain Search.



Domain Search

Finding a domain name

Domain Search allows you to use wildcard search of all current, deleted, and expired domain names for over 6 years worth of history.

^smithson !ain

Search: San Francisco Art

```
SanFranciscoArt
AcademyOfArtSanFrancisco
Apartmentos-SanFrancisco
Bus-Charter-San-Francisco
BuyArtInSanFrancisco
DepArtSanFrancisco
HeartOfSanFrancisco
SanFrancisco-Apartment
SanFrancisco-Apartments
SanFrancisco-Arts
SanFrancisco-PartyBus
SanFranciscoAcademyOfArts
```

Advanced Searching Tips:

Left Anchor:
Place a ^ in front of a word to return all results starting with that word.

Right Anchor:
Place a $ behind of a word to return all results ending with that word.

To exclude strings:
Use a ! in front of a word to exclude that character strings.

Example:

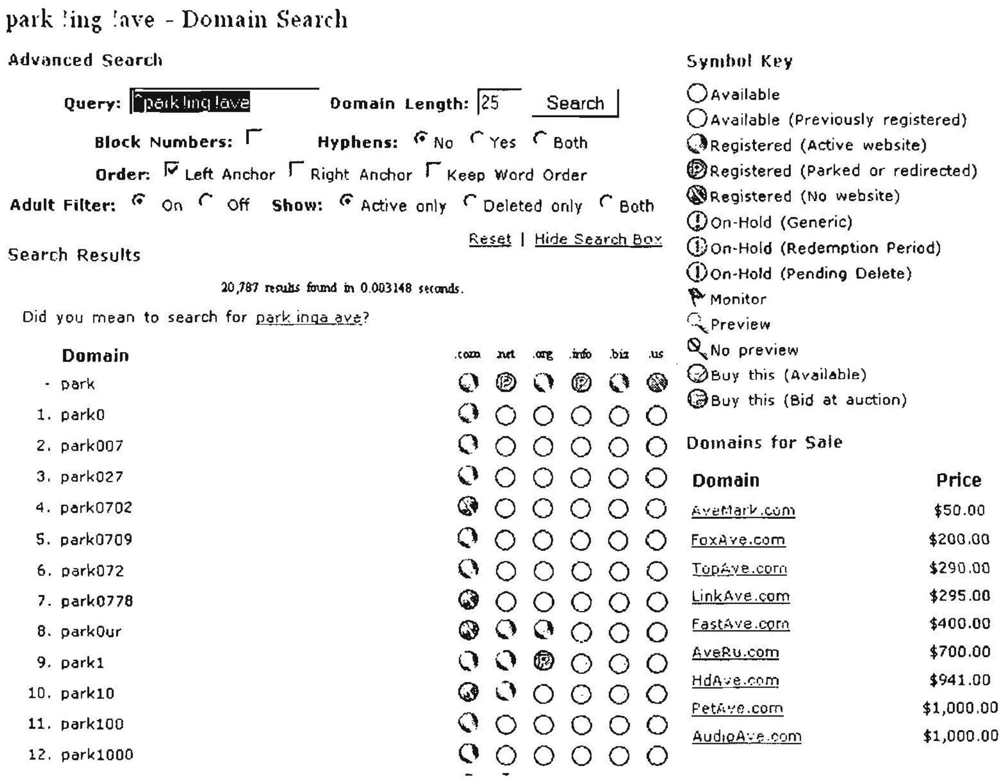
Make "San" appear first in the results by the carrot symbol in front of a word like this ^San Francisco Art.

Make "Francisco" be the last word in all results like this San Francisco$ Art.

To remove all "apart" results place the ! in front of a word like this San Francisco Art !apart.

On this page, you can use three operators to perform wildcard searches:

- A **caret (^)** serves as a Left Anchor to find all domains that **start with a series of letters**. So ^smithson will find will find not only *smithsonian* but *smithsonbrothers*.
- A **dollar sign ($)** serves as a Right Anchor to find all domains that **end with a series of letters**. So $afghan will find *absolutelyafghan* as well as *yellowpageafghan* and everything in between.
- An **exclamation point (!)** serves to **exclude a string of characters**. So [^park !ing !ave] will find domain names that start with *park* and do not include the strings *ing* or *ave* anywhere in the name, thus eliminating *parking* or *parkave* or *parkavenue* from the search. In this search I have also chosen to limit the search to 25 character names, exclude hyphenated domains, show only active domain names, and turn on the adult content filter.



park !ing !ave - Domain Search

Advanced Search

Query: park!ing!ave Domain Length: 25 Search

Block Numbers: □ Hyphens: ● No ○ Yes ○ Both

Order: ☑ Left Anchor □ Right Anchor □ Keep Word Order

Adult Filter: ● On ○ Off Show: ● Active only ○ Deleted only ○ Both

Reset | Hide Search Box

Search Results

20,787 results found in 0.003148 seconds.

Did you mean to search for park inga ave?

	Domain	.com	.net	.org	.info	.biz	.us
-	park	◐	Ⓟ	◐	Ⓟ	◐	●
1.	park0	◐	○	○	○	○	○
2.	park007	◐	○	○	○	○	○
3.	park027	◐	○	○	○	○	○
4.	park0702	●	○	○	○	○	○
5.	park0709	◐	○	○	○	○	○
6.	park072	◐	○	○	○	○	○
7.	park0778	●	○	○	○	○	○
8.	park0ur	●	◐	◐	○	○	○
9.	park1	◐	◐	Ⓟ	○	○	○
10.	park10	●	◐	○	○	○	○
11.	park100	◐	○	○	○	○	○
12.	park1000	◐	○	○	○	○	○

Symbol Key

○ Available
○ Available (Previously registered)
◐ Registered (Active website)
Ⓟ Registered (Parked or redirected)
● Registered (No website)
ⓘ On-Hold (Generic)
ⓘ On-Hold (Redemption Period)
ⓘ On-Hold (Pending Delete)
⚑ Monitor
🔍 Preview
🔍 No preview
✓ Buy this (Available)
✓ Buy this (Bid at auction)

Domains for Sale

Domain	Price
AveMark.com	$50.00
FoxAve.com	$200.00
TopAve.com	$290.00
LinkAve.com	$295.00
FastAve.com	$400.00
AveRu.com	$700.00
HdAve.com	$941.00
PetAve.com	$1,000.00
AudioAve.com	$1,000.00

In this tool, Domain Tools searches generic TLDs .com, .net, .org, .info, .biz, and .us with the status of domain names indicated by color images.

The old Whois.sc page has not actually gone away and DomainTools.com claims it will not go away. By the way, the Whois.sc page claims that the SC TLD (Seychelles) used to stand for 'source' and now stands for 'short cut.' I still think Seychelles every time I see it, though.

Whoix? http://www.whoix.com/

Whoix? Advanced Search http://www.whoix.com/advdomsearch.html

Special features: **wildcard** search on keyword across all domains; enter up to 25 domain names at one time.

From one page, users can search domains in gTLDs, domains in any country-level TLD, or second-level domain names (e.g., co.jp). In addition, Whoix has a keyword search that shows all domains that include the search term as part of their names, but only for the most popular domains. Be sure to click on the "Show who owns this domain" link for information about registered domains. Whoix's most unusual feature, however, is its option to search up to 25 domain names at a time. Results of this search show status (taken or free) and the option to view the Whois data. Home page is Yahoo-like directory devoted to domain names, trademarks, etc. Use the advanced search for options mentioned here.

Xwhois http://www.xwhois.com/

Special features: automatic universal first-, second-level Whois lookups; links to all country-level domain name registries.

Enter any domain name, including first- and second-level domain names—e.g., [bgu.ac.il]—for automatic search of correct database. Homepage includes list of all country code TLDs and links to country-level registries.

Whois the Oldest? http://www.whoisd.com/oldestcom.php

Finally, just for fun, take a look at the 100 oldest .com domains that are still registered! The very first "create date" was 15 March 1985. Try to guess the domain name ... you may be surprised.

Web Tip

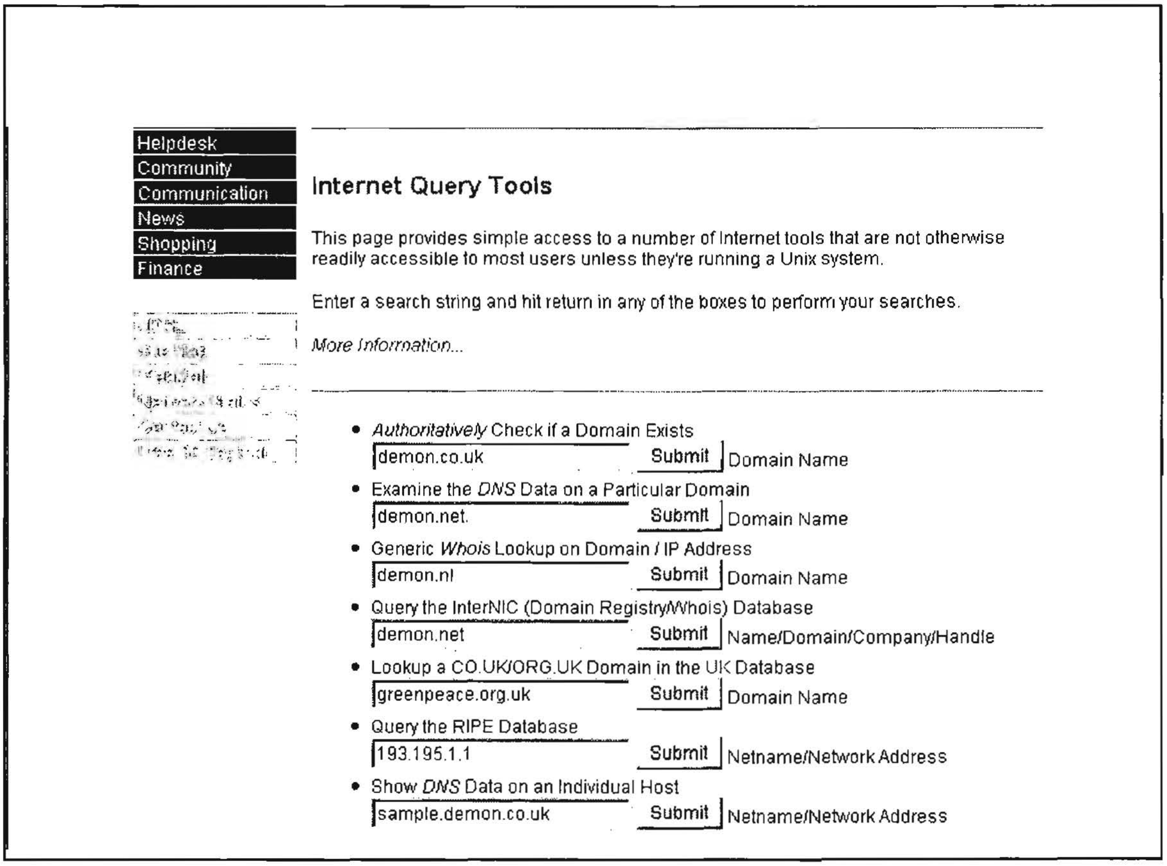
To find an almost unlimited number of downloadable tools for your PC, visit:

http://www.tucows.com/
http://download.com.com/
http://downloads-zdnet.com.com/

Many very good utility programs that will allow you to run UNIX commands, such as Whois, ping, traceroute, etc., from a PC are available for a small fee or for free. Be sure to virus scan any executable file BEFORE you install it. Also, beware of ALL SHAREWARE...it could be SPYWARE! Don't install software promiscuously.

Internet Toolkits

Some of the most useful websites are those with many **Windows-based forms** that let you run a number of different queries from one page. These are often called **Internet Tool Kits, IP Tools**, or **Nettools,** like the page at Demon.net, which gives users a range of query options as well as the opportunity to query RIPE, "InterNIC," and the UKNIC databases from one screen.



Internet Query Tools

This page provides simple access to a number of Internet tools that are not otherwise readily accessible to most users unless they're running a Unix system.

Enter a search string and hit return in any of the boxes to perform your searches.

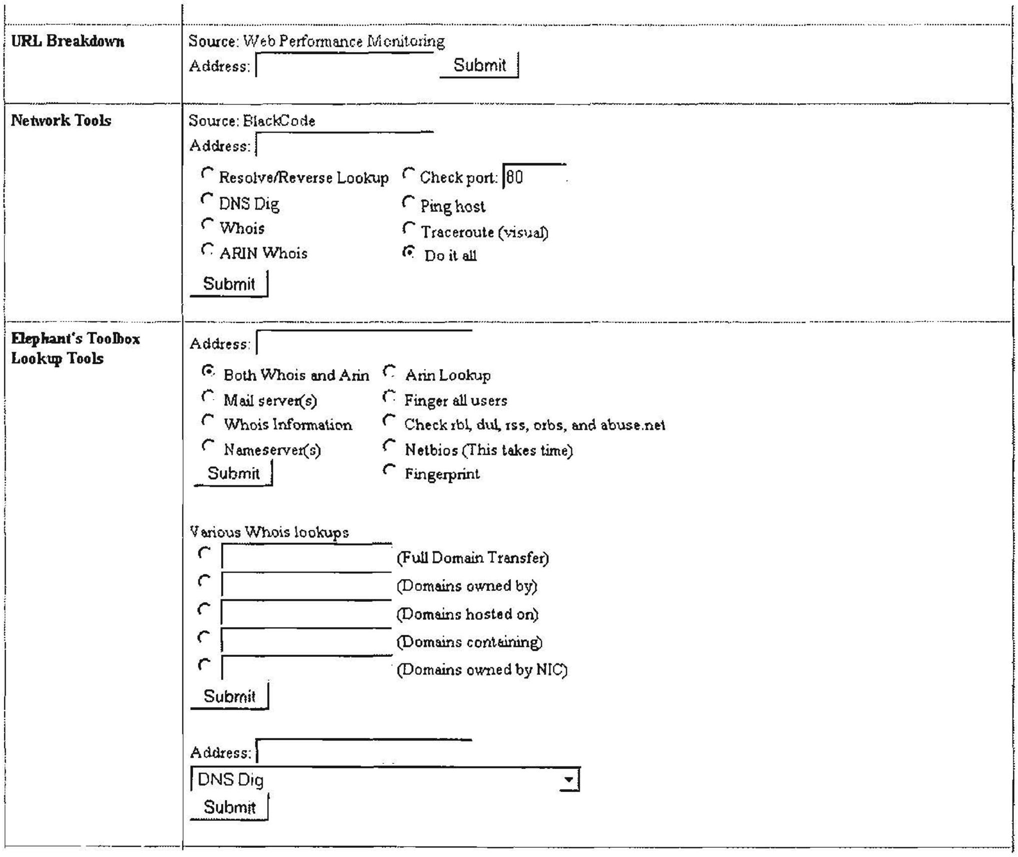
More Information...

- *Authoritatively* Check if a Domain Exists
  demon.co.uk Submit Domain Name
- Examine the *DNS* Data on a Particular Domain
  demon.net. Submit Domain Name
- Generic *Whois* Lookup on Domain / IP Address
  demon.nl Submit Domain Name
- Query the InterNIC (Domain Registry/Whois) Database
  demon.net Submit Name/Domain/Company/Handle
- Lookup a CO.UK/ORG.UK Domain in the UK Database
  greenpeace.org.uk Submit Domain Name
- Query the RIPE Database
  193.195.1.1 Submit Netname/Network Address
- Show *DNS* Data on an Individual Host
  sample.demon.co.uk Submit Netname/Network Address

Internet Query Tools http://www.demon.net/external/

RodentNet Ad Hoc IP Tools http://tatumweb.com/iptools.htm

RodentNet Ad Hoc IP Tools lets users run NSLookup, ping, traceroute, and an extremely powerful and fast IP range DNS query from one convenient menu. The IP range query will show all the IP addresses, any associated domain names, websites, and/or email addresses, as well as registration information for an entire block of addresses.

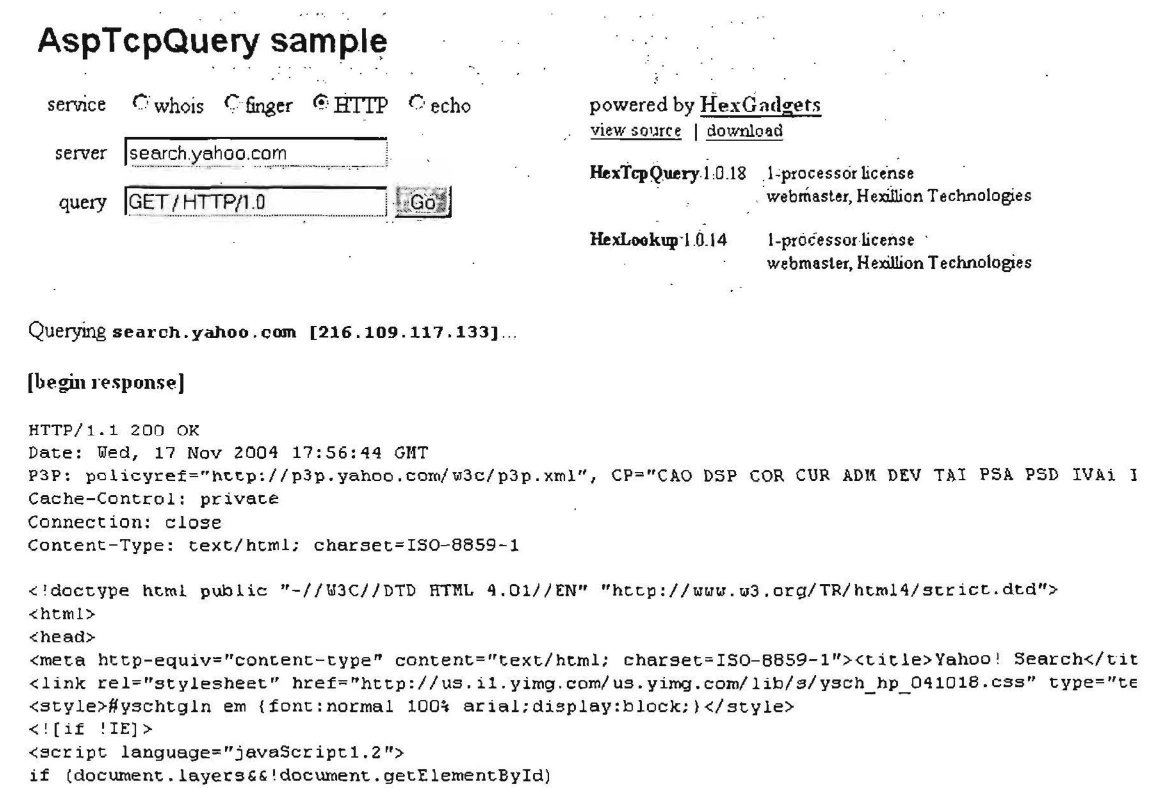


URL Breakdown	Source: Web Performance Monitoring Address: [ ] Submit
Network Tools	Source: BlackCode Address: [ ] ○ Resolve/Reverse Lookup ○ Check port: 80 ○ DNS Dig ○ Ping host ○ Whois ○ Traceroute (visual) ○ ARIN Whois ● Do it all Submit
Elephant's Toolbox Lookup Tools	Address: [ ] ● Both Whois and Arin ○ Arin Lookup ○ Mail server(s) ○ Finger all users ○ Whois Information ○ Check rbl, dul, rss, orbs, and abuse.net ○ Nameserver(s) ○ Netbios (This takes time) Submit ○ Fingerprint Various Whois lookups ○ [ ] (Full Domain Transfer) ○ [ ] (Domains owned by) ○ [ ] (Domains hosted on) ○ [ ] (Domains containing) ○ [ ] (Domains owned by NIC) Submit Address: [ ] DNS Dig ▾ Submit

The other sites listed below offer web interfaces to all the basic network tools and, in some cases, add interesting new ones.

All-Nettools.com	http://www.all-nettools.com/tools1.htm
Centralops	http://centralops.net/co/body.asp
Internet Query Tools	http://www.demon.net/external/
iTools Internet Tools	http://www.itools.com/internet/
Network-Tools	http://www.network-tools.com/
RodentNet Ad Hoc IP Tools	http://tatumweb.com/iptools.htm

Centralops Hexillion Tools includes the AspTcpQuery, which will run an HTTP GET query to retrieve the page source code data about any webpage or IP address. Here's part of the result for [search.yahoo.com]:



AspTcpQuery sample

service ○ whois ○ finger ● HTTP ○ echo

server search.yahoo.com

query GET / HTTP/1.0

powered by HexGadgets
view source | download

HexTcpQuery 1.0.18	1-processor license webmaster, Hexillion Technologies
HexLookup 1.0.14	1-processor license webmaster, Hexillion Technologies

Querying **search.yahoo.com [216.109.117.133]**...

[begin response]

```
HTTP/1.1 200 OK
Date: Wed, 17 Nov 2004 17:56:44 GMT
P3P: policyref="http://p3p.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi I
Cache-Control: private
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<!doctype html public "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1"><title>Yahoo! Search</tit
<link rel="stylesheet" href="http://us.i1.yimg.com/us.yimg.com/lib/s/ysch_hp_041018.css" type="te
<style>#yschtgln em {font:normal 100% arial;display:block;}</style>
<![if !IE]>
<script language="javaScript1.2">
if (document.layers&&!document.getElementById)
```

Central OPS TcpQuery http://www.hexillion.com/samples/AspTcpQuery.asp

How to Research a Domain Name or IP Address

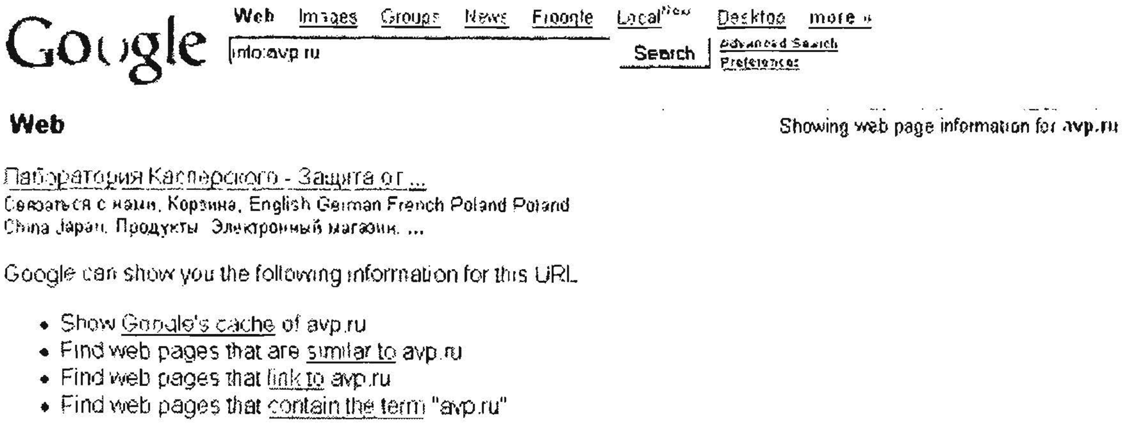
In a previous section, I discussed the differences between domain name and whois lookups. Now I am going to walk through some basic research steps to learn how to analyze who registered a domain name and/or who owns an IP address. There are a number of ways to research domain names and IP addresses and many tools on the Internet that can help provide information about a domain or IP address.

Important Caveat: despite what you may hear or read elsewhere, you cannot ascertain the location or ownership of a domain name or IP address based solely on the fact it is in one of the most commonly used top-level domains, i.e., .com, .org, or .net. Names in these domains may be registered by anyone anywhere in the world. Likewise, domains registered in specific country top-level domains, e.g., .ru, .pk, .fr, are only *presumed* to be registered by non-US entities, but there is no guarantee based on the top-level domain alone this is the case. The point is simple: all domain names must be researched, with a few exceptions. The exceptions are .mil, .gov, and .edu, all of which are, at least theoretically, restricted to US-entities. There are even some exceptions in these cases. However, you may safely assume domain names or IP addresses associated with a .mil, .gov, or .edu top-level domain are US entities.

Steps for researching a domain name and IP address:

1. Does the domain name or IP address correspond to an Internet website?

If so, the first step is to use a good search tool such as Google to find out more about the site. The *info:* command at Google will show you links to Google's cache of the page, pages that are similar to the webpage, pages that link to this site, and pages that contain the search term. For this article, I will use a high-profile Russian anti-virus company Kaspersky Labs because it has registered domain names in both the .com and .ru top-level domains.



Showing web page information for avp.ru

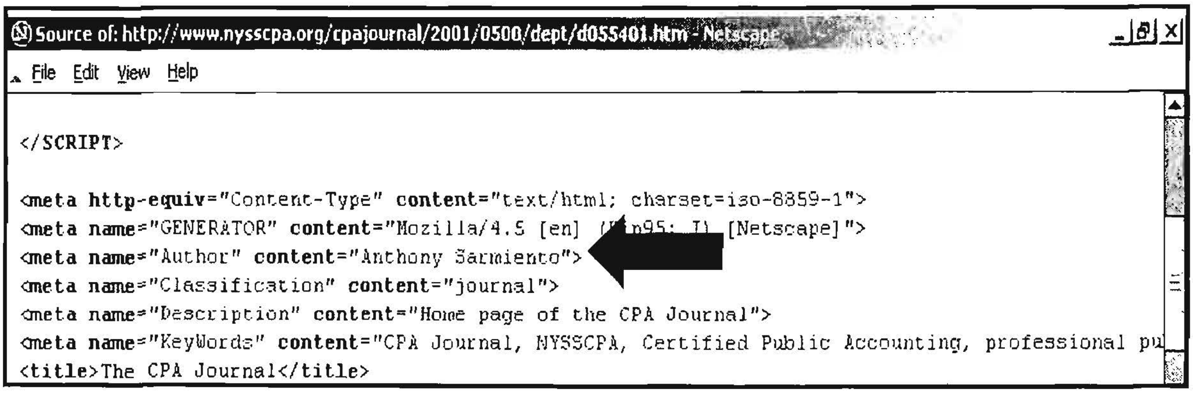
Лаборатория Касперского - Защита от ...
Связаться с нами, Корзина, English German French Poland Poland China Japan, Продукты Электронный магазин, ...

Google can show you the following information for this URL

- Show Google's cache of avp.ru
- Find web pages that are similar to avp.ru
- Find web pages that link to avp.ru
- Find web pages that contain the term "avp.ru"

The next step would be to look at the website itself. The first two pages—About Us and Contact Us—are probably the most important, but there are other good pages to examine at the site itself:

- "About Us," which often tells you a great deal about the company (who owns it, where it's located, branch offices, subsidiaries).
- Other company websites in different languages, which may provide new domain names and IP addresses, as in the case of *avp.ru*: *kaspersky.ru*, *kasperksy.com*, *kaspersky.com.cn*, etc.
- "Contact Us," which may reveal numerous email addresses, physical locations, etc.
- "Site Map," which may show more pages on the site than are obvious from the homepage.
- "Press" or "News Releases," which often have the latest news about a company's activities, including company locations, ownership, ISPs, etc.
- "Page Source," which sometimes contains information about the person or organization that created or maintains the site. To view page source in Mozilla-based browsers, View | Page Source; in Internet Explorer, View | Source. Look or search for [author] in the HTML code:

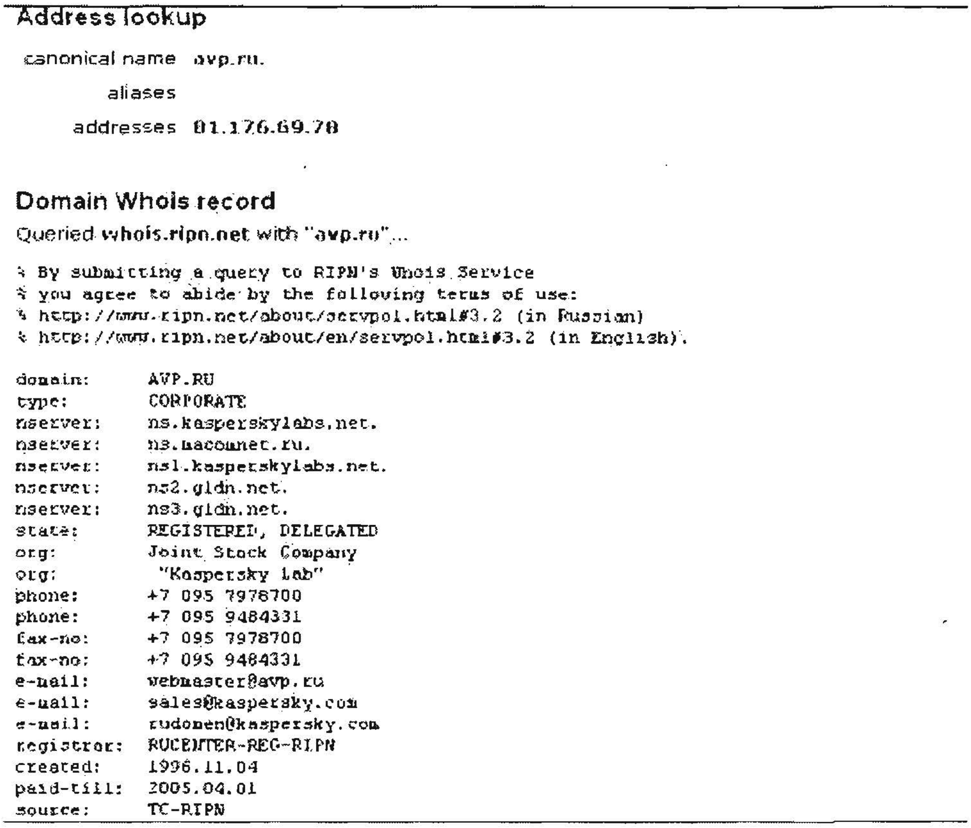

Source of: http://www.nysscpa.org/cpajournal/2001/0500/dept/d055401.htm - Netscape
File
Edit
View
Help

```
</SCRIPT>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta name="GENERATOR" content="Mozilla/4.5 [en] (Win95; I) [Netscape]">
<meta name="Author" content="Anthony Sarmiento">
<meta name="Classification" content="journal">
<meta name="Description" content="Home page of the CPA Journal">
<meta name="KeyWords" content="CPA Journal, NYSSCPA, Certified Public Accounting, professional pu
<title>The CPA Journal</title>
```

2. Who registered the domain name?

Many, many domain name and Whois lookup tools exist on the Internet to permit you to find out information about a domain name. These tools will reveal such information as the servers associated with a specific domain name. Continuing with the example of *avp.ru*, using a lookup tool such as **Domain Dossier** (http://centralops.net/co/DomainDossier.aspx), I can quickly find the domain whois records, the network whois records, and the DNS records for *avp.ru*.

The domain whois record is formatted information about the domain name *avp.ru*, in this case pulled from RIPE's Whois Service database; notice the IP address, who registered the domain (Kaspersky Labs), and the domain's registrar (RIPN, the Russian Network Information Center).



Address lookup

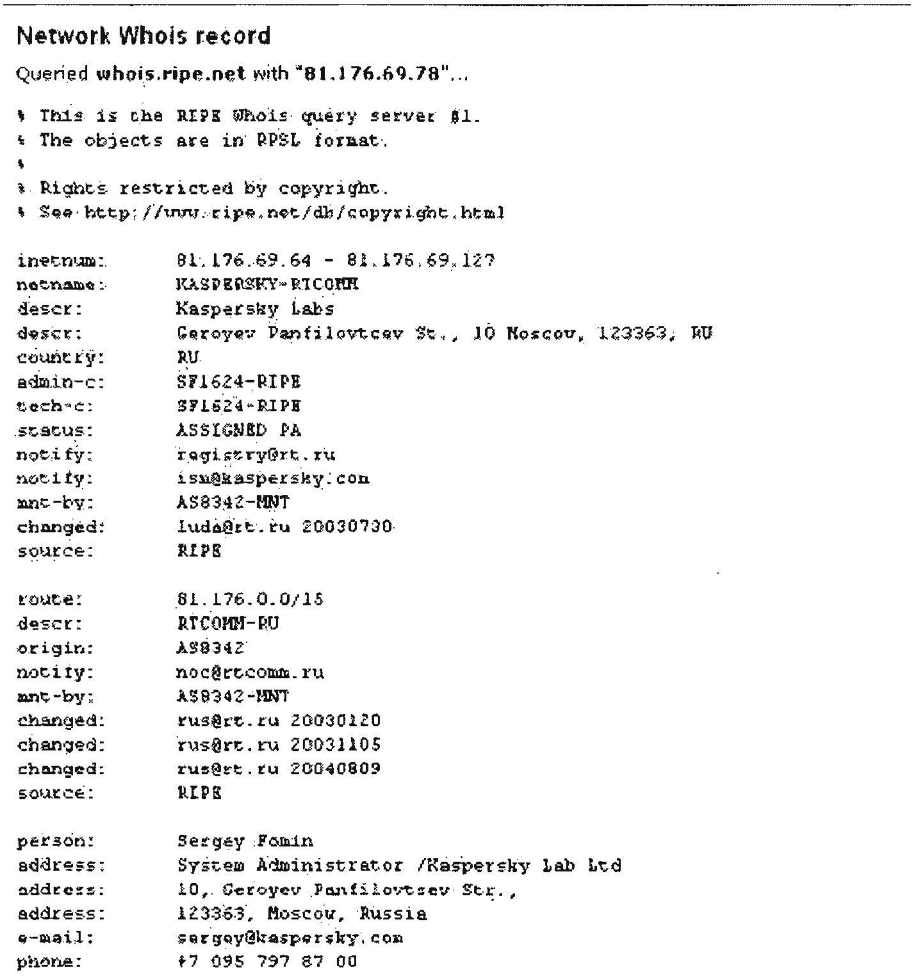
```
canonical name  avp.ru.
       aliases
     addresses  81.176.69.78
```

Domain Whois record

Queried **whois.ripn.net** with "avp.ru"...

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain:      AVP.RU
type:        CORPORATE
nserver:     ns.kasperskylabs.net.
nserver:     ns3.macomnet.ru.
nserver:     ns1.kasperskylabs.net.
nserver:     ns2.gldn.net.
nserver:     ns3.gldn.net.
state:       REGISTERED, DELEGATED
org:         Joint Stock Company
org:          "Kaspersky Lab"
phone:       +7 095 7978700
phone:       +7 095 9484331
fax-no:      +7 095 7978700
fax-no:      +7 095 9484331
e-mail:      webmaster@avp.ru
e-mail:      sales@kaspersky.com
e-mail:      rudonen@kaspersky.com
registrar:   RUCENTER-REG-RIPN
created:     1996.11.04
paid-till:   2005.04.01
source:      TC-RIPN
```

The network whois record for *avp.ru*. This is formatted information about the IP address from RIPE's database. Notice the block of IP addresses in which the IP address falls, which usually provides insight into the physical location of the servers and service providers. In this case, we can see the IP address owner (Kaspersky Labs), the Internet Service Provider (RT-COMM, a huge Russian ISP), street address, phone numbers, email addresses (interestingly, at *kasperksy.com*).

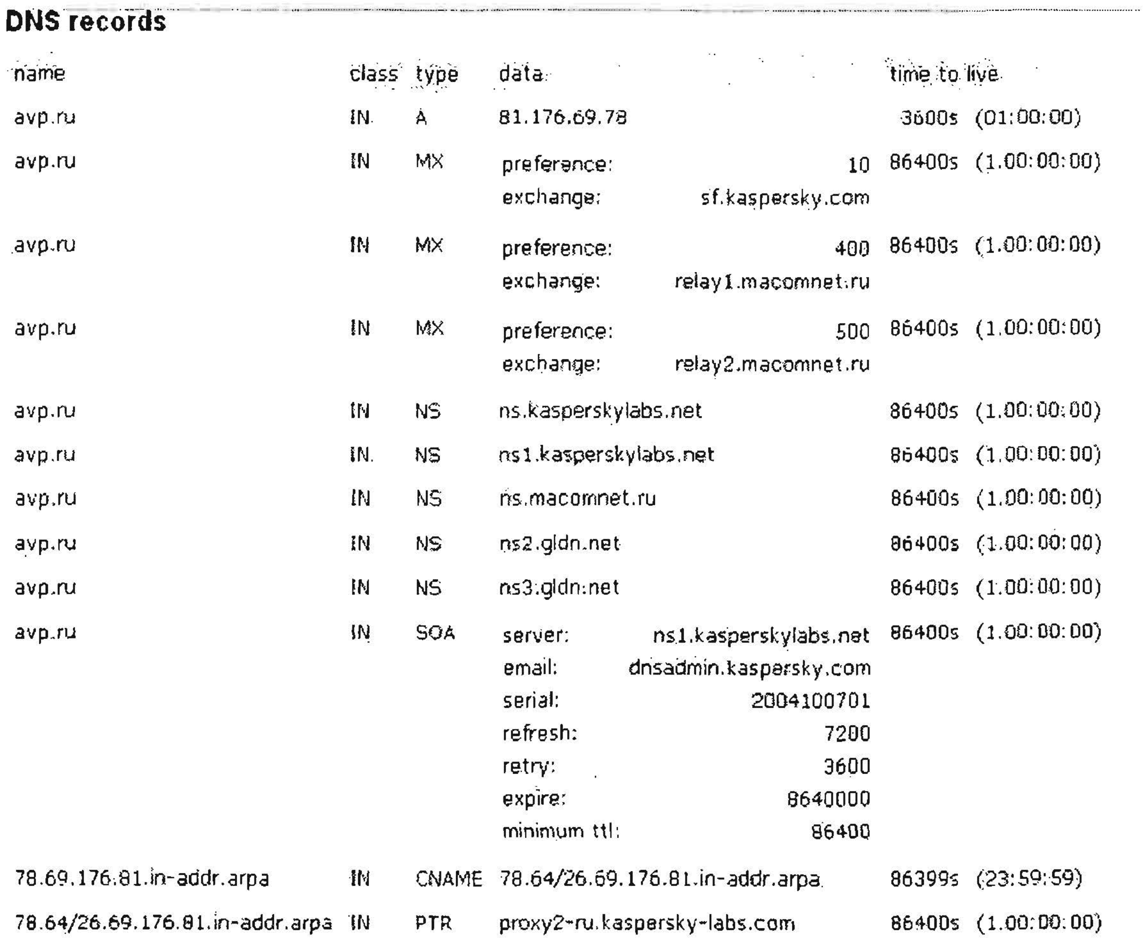


Network Whois record

Queried **whois.ripe.net** with "**81.176.69.78**"...

```
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

inetnum:      81.176.69.64 - 81.176.69.127
netname:      KASPERSKY-RTCOMM
descr:        Kaspersky Labs
descr:        Geroyev Panfilovtcev St., 10 Moscow, 123363, RU
country:      RU
admin-c:      SF1624-RIPE
tech-c:       SF1624-RIPE
status:       ASSIGNED PA
notify:       registry@rt.ru
notify:       ism@kaspersky.com
mnt-by:       AS8342-MNT
changed:      luda@rt.ru 20030730
source:       RIPE

route:        81.176.0.0/15
descr:        RTCOMM-RU
origin:       AS8342
notify:       noc@rtcomm.ru
mnt-by:       AS8342-MNT
changed:      rus@rt.ru 20030120
changed:      rus@rt.ru 20031105
changed:      rus@rt.ru 20040809
source:       RIPE

person:       Sergey Fomin
address:      System Administrator /Kaspersky Lab Ltd
address:      10, Geroyev Panfilovtsev Str.,
address:      123363, Moscow, Russia
e-mail:       sergey@kaspersky.com
phone:        +7 095 797 87 00
```

The DNS record for *avp.ru* is the formatted information about this domain name used by the Domain Name Service/System to route data, including email, over the Internet to and from this host. Notice the different server names (*kasperskylabs.net*, macomnet.*ru*, kaspersky.*com*, *kaspersky-labs.com*, *gldn.net*) associated with *avp.ru*. For example, the preferred mail exchange server for *avp.ru* is *relay1.macomnet.ru* (a Russian telecom provider).

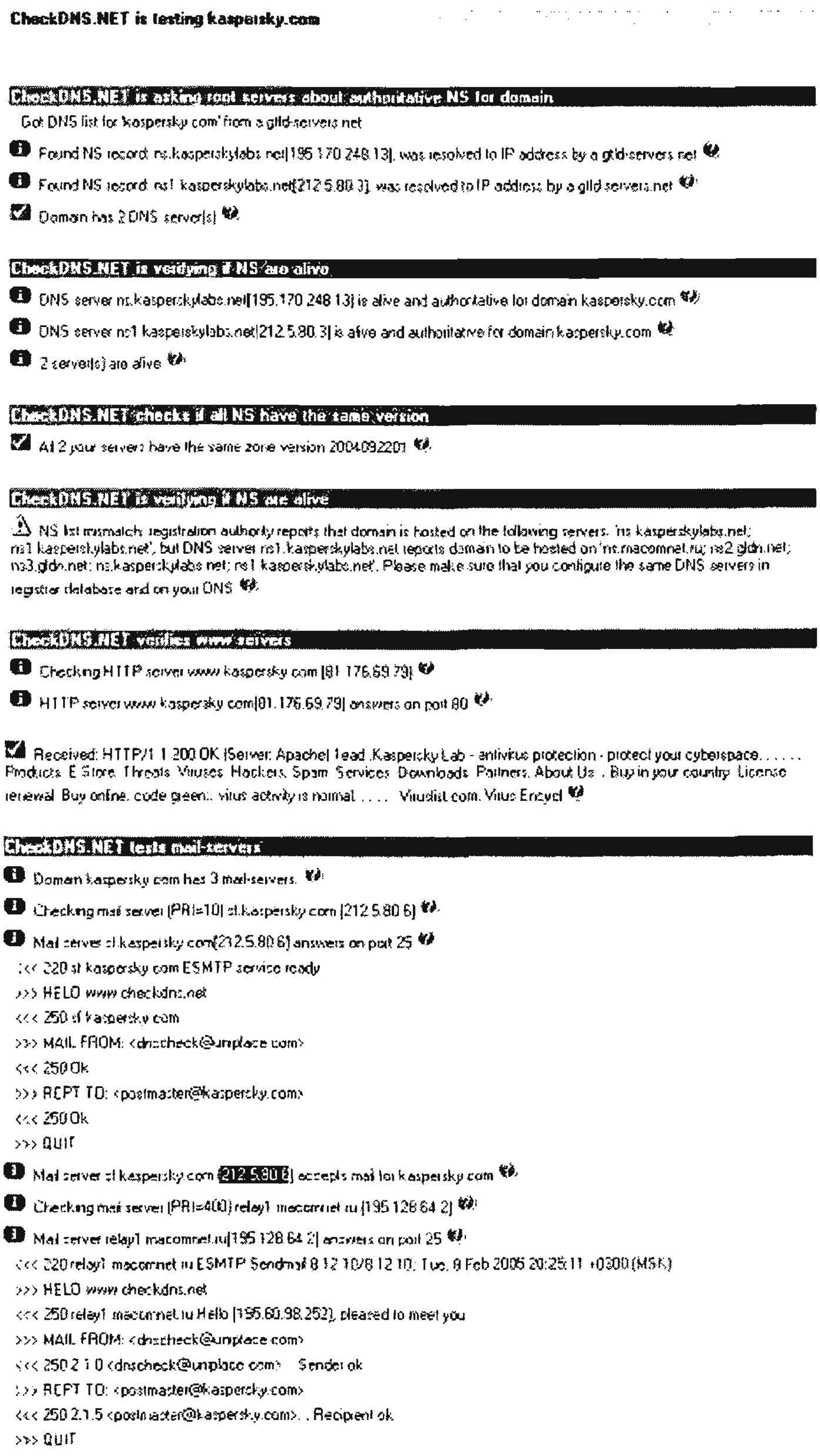


DNS records

name	class	type	data	time to live
avp.ru	IN	A	81.176.69.78	3600s (01:00:00)
avp.ru	IN	MX	preference: 10 exchange: sf.kaspersky.com	86400s (1.00:00:00)
avp.ru	IN	MX	preference: 400 exchange: relay1.macomnet.ru	86400s (1.00:00:00)
avp.ru	IN	MX	preference: 500 exchange: relay2.macomnet.ru	86400s (1.00:00:00)
avp.ru	IN	NS	ns.kasperskylabs.net	86400s (1.00:00:00)
avp.ru	IN	NS	ns1.kasperskylabs.net	86400s (1.00:00:00)
avp.ru	IN	NS	ns.macomnet.ru	86400s (1.00:00:00)
avp.ru	IN	NS	ns2.gldn.net	86400s (1.00:00:00)
avp.ru	IN	NS	ns3.gldn.net	86400s (1.00:00:00)
avp.ru	IN	SOA	server: ns1.kasperskylabs.net email: dnsadmin.kaspersky.com serial: 2004100701 refresh: 7200 retry: 3600 expire: 8640000 minimum ttl: 86400	86400s (1.00:00:00)
78.69.176.81.in-addr.arpa	IN	CNAME	78.64/26.69.176.81.in-addr.arpa	86399s (23:59:59)
78.64/26.69.176.81.in-addr.arpa	IN	PTR	proxy2-ru.kaspersky-labs.com	86400s (1.00:00:00)

3. Who registered the *.com* domain name? What can we find out about it?

Just because there are *.com* domain names associated with Kaspersky Labs does not mean they are US entities. First, let's look at the very thorough records available using CheckDNS.net .



CheckDNS.NET is testing kaspersky.com

CheckDNS.NET is asking root servers about authoritative NS for domain

Got DNS list for 'kaspersky.com' from a.gtld-servers.net

ℹ Found NS record: ns.kasperskylabs.net[195.170.248.13], was resolved to IP address by a.gtld-servers.net

ℹ Found NS record: ns1.kasperskylabs.net[212.5.80.3], was resolved to IP address by a.gtld-servers.net

☑ Domain has 2 DNS server(s)

CheckDNS.NET is verifying if NS are alive

ℹ DNS server ns.kasperskylabs.net[195.170.248.13] is alive and authoritative for domain kaspersky.com

ℹ DNS server ns1.kasperskylabs.net[212.5.80.3] is alive and authoritative for domain kaspersky.com

ℹ 2 server(s) are alive

CheckDNS.NET checks if all NS have the same version

☑ All 2 your servers have the same zone version 2004092201

CheckDNS.NET is verifying if NS are alive

⚠ NS list mismatch: registration authority reports that domain is hosted on the following servers: 'ns.kasperskylabs.net; ns1.kasperskylabs.net', but DNS server ns1.kasperskylabs.net reports domain to be hosted on 'ns.macomnet.ru; ns2.gldn.net; ns3.gldn.net; ns.kasperskylabs.net; ns1.kasperskylabs.net'. Please make sure that you configure the same DNS servers in register database and on your DNS

CheckDNS.NET verifies www servers

ℹ Checking HTTP server www.kaspersky.com [81.176.69.79]

ℹ HTTP server www.kaspersky.com[81.176.69.79] answers on port 80

☑ Received: HTTP/1.1 200 OK (Server: Apache) lead .Kaspersky Lab - antivirus protection - protect your cyberspace. . . . . . Products E Store Threats Viruses Hackers Spam Services Downloads Partners About Us . Buy in your country License renewal Buy online. code green.. virus activity is normal . . . . Viruslist.com. Virus Encycl

CheckDNS.NET tests mail-servers

ℹ Domain kaspersky.com has 3 mail-servers.

ℹ Checking mail server (PRI=10) sl.kaspersky.com [212.5.80.6]

ℹ Mail server sl.kaspersky.com[212.5.80.6] answers on port 25

```
<<< 220 sl.kaspersky.com ESMTP service ready
>>> HELO www.checkdns.net
<<< 250 sl.kaspersky.com
>>> MAIL FROM: <dnscheck@unplace.com>
<<< 250 Ok
>>> RCPT TO: <postmaster@kaspersky.com>
<<< 250 Ok
>>> QUIT
```

ℹ Mail server sl.kaspersky.com [212.5.80.6] accepts mail for kaspersky.com

ℹ Checking mail server (PRI=400) relay1.macomnet.ru [195.128.64.2]

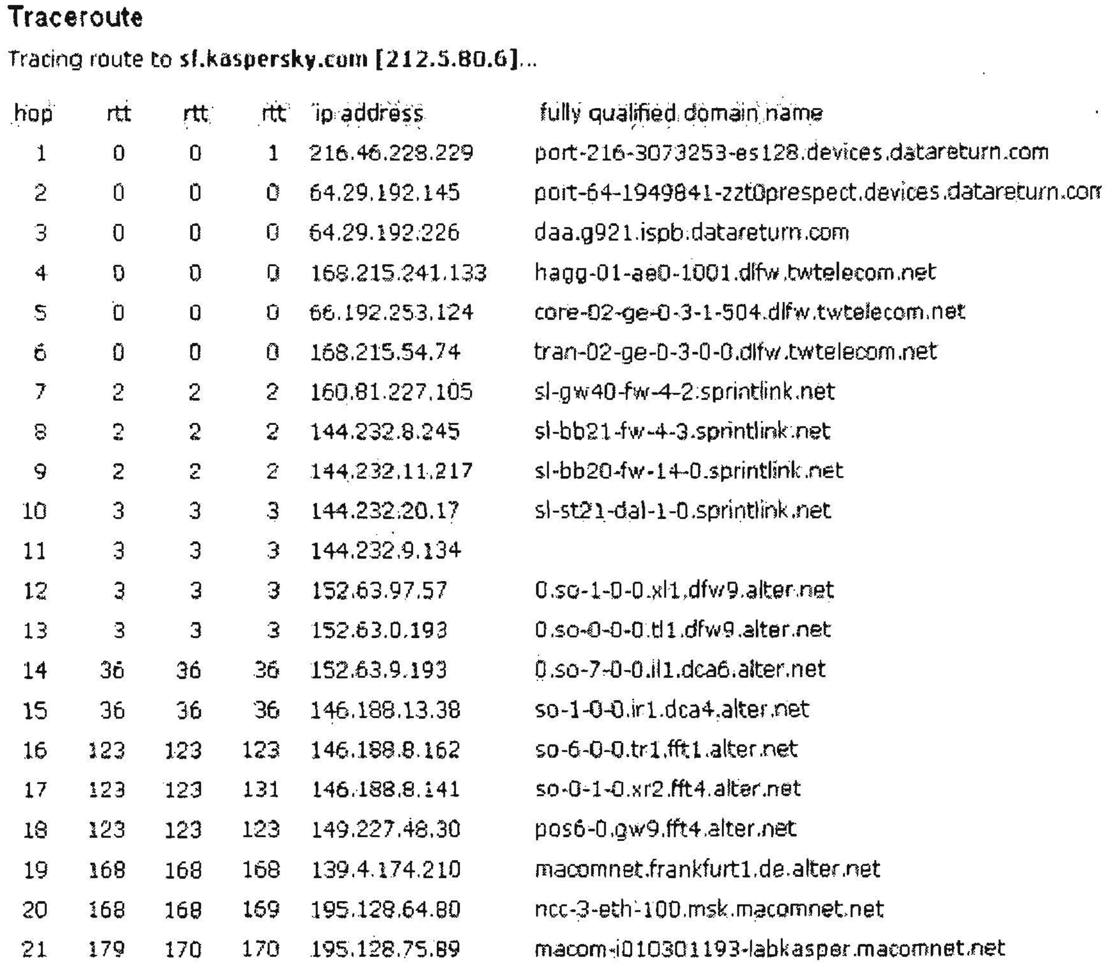
ℹ Mail server relay1.macomnet.ru[195.128.64.2] answers on port 25

```
<<< 220 relay1.macomnet.ru ESMTP Sendmail 8.12.10/8.12.10; Tue, 8 Feb 2005 20:25:11 +0300 (MSK)
>>> HELO www.checkdns.net
<<< 250 relay1.macomnet.ru Hello [195.60.98.252], pleased to meet you
>>> MAIL FROM: <dnscheck@unplace.com>
<<< 250 2.1.0 <dnscheck@unplace.com>... Sender ok
>>> RCPT TO: <postmaster@kaspersky.com>
<<< 250 2.1.5 <postmaster@kaspersky.com>... Recipient ok
>>> QUIT
```

Of special note are the two IP addresses that appear in these records as mail servers: 195.128.64.9 and 212.5.80.6. The first resolves to Macomnet in Moscow and the second to *kaspersky.com*, a domain name registered with Tucows.com. Sounds like it might be in the US.

4. Where is *kaspersky.com* or 212.5.80.6 physically located?

This is usually harder to determine because truly accurate geolocation tools are not available for free on the Internet. However, we can get some pretty good clues from the network analysis tool traceroute. Below is the traceroute to *kaspersky*.com using Domain Dossier. Notice in particular the last three hops before reaching 212.5.80.6: they are Frankfurt, Germany (frankfurt1.de.alter.net), Moscow (msk.macomnet.net), and Macomnet's address 195.128.64.9 in Moscow. Traceroute shows the name of routers along the path the data is traveling, and these routers frequently (but certainly not always) use airport codes (e.g. LON, ATL). Below, for example, *dca4.alter.net* is almost certainly in the Washington, DC, area. There is much more that can be learned from traceroutes, a topic covered in the next section.

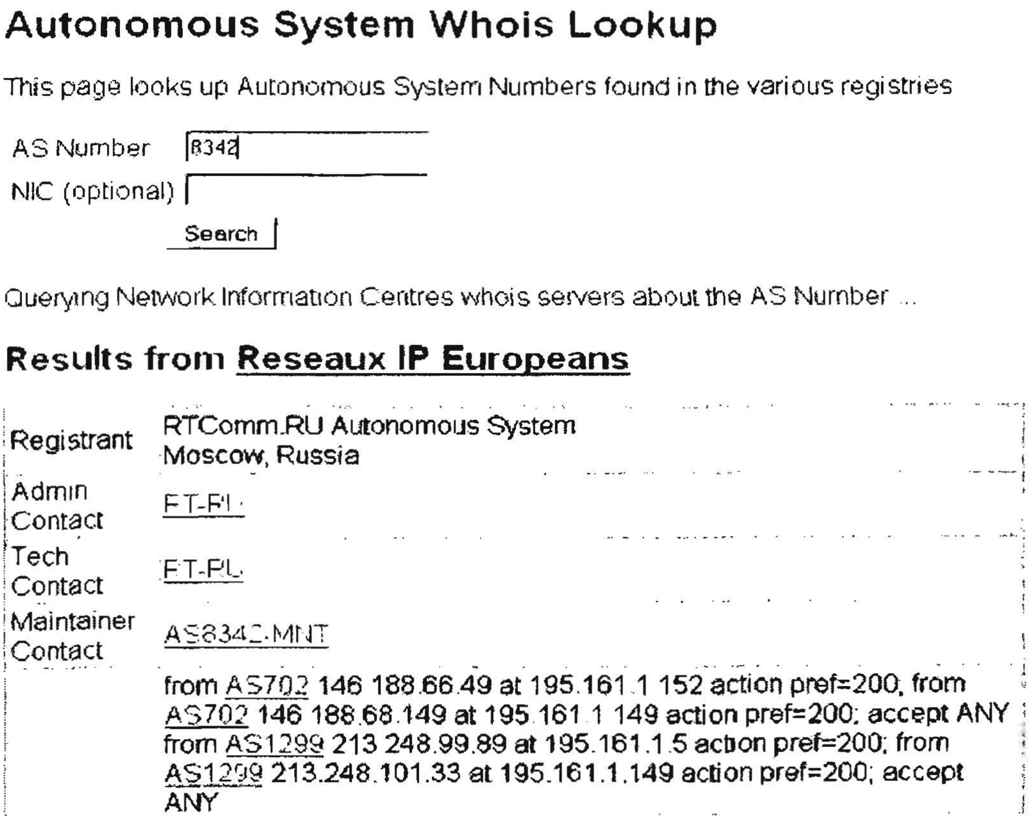


```
Traceroute

Tracing route to sl.kaspersky.com [212.5.80.6]...

hop  rtt  rtt  rtt  ip address       fully qualified domain name
  1    0    0    1  216.46.228.229   port-216-3073253-es128.devices.datareturn.com
  2    0    0    0  64.29.192.145    port-64-1949841-zzt0prespect.devices.datareturn.com
  3    0    0    0  64.29.192.226    daa.g921.ispb.datareturn.com
  4    0    0    0  168.215.241.133  hagg-01-ae0-1001.dlfw.twtelecom.net
  5    0    0    0  66.192.253.124   core-02-ge-0-3-1-504.dlfw.twtelecom.net
  6    0    0    0  168.215.54.74    tran-02-ge-0-3-0-0.dlfw.twtelecom.net
  7    2    2    2  160.81.227.105   sl-gw40-fw-4-2.sprintlink.net
  8    2    2    2  144.232.8.245    sl-bb21-fw-4-3.sprintlink.net
  9    2    2    2  144.232.11.217   sl-bb20-fw-14-0.sprintlink.net
 10    3    3    3  144.232.20.17    sl-st21-dal-1-0.sprintlink.net
 11    3    3    3  144.232.9.134
 12    3    3    3  152.63.97.57     0.so-1-0-0.xl1.dfw9.alter.net
 13    3    3    3  152.63.0.193     0.so-0-0-0.tl1.dfw9.alter.net
 14   36   36   36  152.63.9.193     0.so-7-0-0.il1.dca6.alter.net
 15   36   36   36  146.188.13.38    so-1-0-0.ir1.dca4.alter.net
 16  123  123  123  146.188.8.162    so-6-0-0.tr1.fft1.alter.net
 17  123  123  131  146.188.8.141    so-0-1-0.xr2.fft4.alter.net
 18  123  123  123  149.227.48.30    pos6-0.gw9.fft4.alter.net
 19  168  168  168  139.4.174.210    macomnet.frankfurt1.de.alter.net
 20  168  168  169  195.128.64.80    ncc-3-eth-100.msk.macomnet.net
 21  179  170  170  195.128.75.89    macom-i010301193-labkasper.macomnet.net
```

There are several geolocation tools available for free on the Internet, but no one should rely upon them alone because they may not be completely accurate. **HostIP.info** uses two sources of information to generate its geolocation tool: people identifying their city as associated with an IP address and automatic traceroutes. **Networldmap** also uses information entered by people visiting their site and has recently added links to its commercial site, **Geobytes**, which provides a more detailed report on IP address geolocation. For more details on using these tools, go to the section on Geolocating Internet Addresses.

5. What else can we learn?

Autonomous System Numbers (ASN) can help physically locate domain names and IP addresses. ASNs are unique numbers (written AS1234) associated with something called an Autonomous System (AS). An AS is an IP network with a single, clear external routing policy, which is used to exchange routing information between various Autonomous Systems. In short, each AS establishes a set of rules for how Internet traffic can travel between and among IP networks around the globe. In the case of *avp.ru/kaspersky.com*, the ASN is AS8342. Using the AS Whois Lookup tool available at Eye-Net Consulting, we see that AS8342 belongs to RT-RU, which is the Russian telecommunications giant, Rostelecom, one of the two principal shareholders of RT-COMM.



Autonomous System Whois Lookup

This page looks up Autonomous System Numbers found in the various registries

AS Number 8342

NIC (optional)

Querying Network Information Centres whois servers about the AS Number ...

Results from Reseaux IP Europeans

Registrant	RTComm.RU Autonomous System Moscow, Russia
Admin Contact	FT-RU
Tech Contact	FT-RU
Maintainer Contact	AS8342-MNT
	from AS702 146 188.66.49 at 195.161.1 152 action pref=200; from AS702 146 188.68.149 at 195 161 1 149 action pref=200; accept ANY from AS1299 213 248.99.89 at 195.161.1.5 action pref=200; from AS1299 213.248.101.33 at 195.161.1.149 action pref=200; accept ANY

Eye-Net Consulting Autonomous System Number Whois Tool
http://www.enc.com.au/itools/aut-num.php

What did we ultimately learn about *avp.ru* and its associated domain names and IP addresses? They are most likely all located inside Russia, even those in the .com and .net domains. While not every domain name or IP address is as straightforward as the example of Kaspersky Labs, the techniques and on-line tools discussed here usually can provide sufficient information to draw a pretty clear picture of who owns an IP address, who registered a domain name, and where the host computers associated with those addresses are physically located.

Confused by all the acronyms and numbers in the various DNS and Whois records? These sites provide excellent information on understanding these important records.

Paul Adams, "Ins and Outs of DNS," *Webmonkey*
http://www.webmonkey.com/webmonkey/02/31/index3a.html

DNS for Rocket Scientists http://newweb.zytrax.com/books/dns/ch1/

IBM iSeries Information Center: DNS Resource Records
http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzakk/rzakkconceptresourcerec.htm

Traceroute

Traceroute is an Internet utility that shows in real time the complete logical connection path between a local host and the remote host it is contacting, i.e., it is a tool for mapping the path from one computer to another computer's IP address while showing all the IP addresses of the routers between these two points as well as the time between each step along the way.

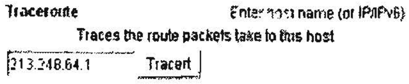
> "A traceroute utility maps the path that data packets take between two points on the Internet, showing all of the intermediate nodes traversed, along with an indication of the speed of travel. Traceroute was invented in 1988 by Van Jacobson at Lawrence Berkeley National Laboratory in the US Today a traceroute utility often comes as part of the operating system. Windows, for example, has a small utility called tracert, which is used by typing, at the MS-DOS prompt, tracert."[155]

Traceroute, which shows all the intermediate routers that packets pass through to get to their destination, was written as a network troubleshooting utility to reveal problems with routers along a specific path. It is also very useful in showing how systems on the Internet are connected to each other. While traceroute only shows logical connections, it can nonetheless help you understand possible physical connections because the Internet is not only highly redundant but also very repetitive. In other words, Internet traffic will usually take the same routes over and over again unless something, such as equipment overload or failure, interferes with it.

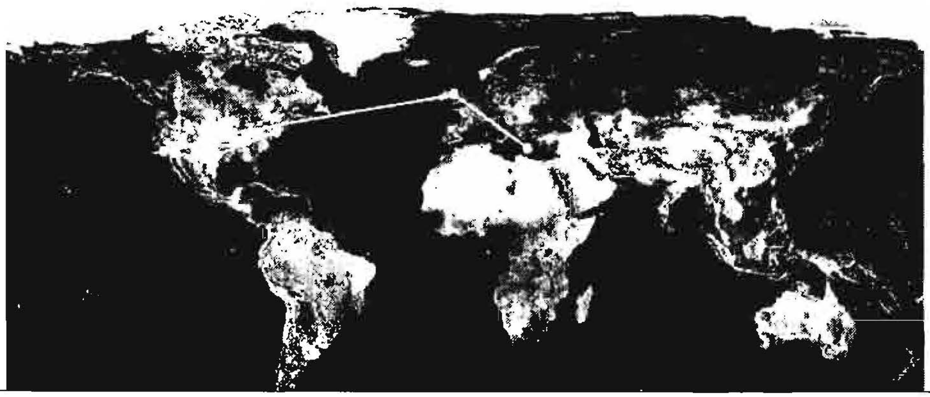
Let's take a look at a simple traceroute run using a free visual traceroute tool available at IP Address Guide:[156]

[155] Martin Dodge, "Mapping Where the Data Goes," *Internet Society*, March 2000, <http://www.isoc.org/oti/articles/0200/dodge.html> (14 November 2006).

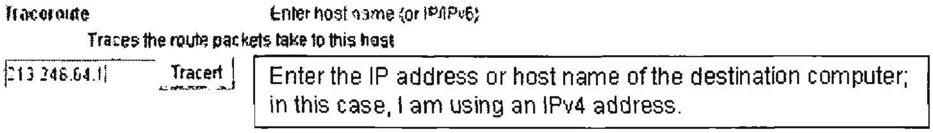
[156] The Internetipaddress.com website is currently unavailable.


Traceroute
Enter host name (or IP/IPv6)
Traces the route packets take to this host
213.248.64.1
Tracert

```
Tracing route to 213.248.64.1 over a maximum of 20 hops:

     1     0 ms     2 ms     0 ms   67.18.29.185    UNITED STATES   -   -   THEPLANET.COM INTERNET SERVICES INC
     2     0 ms     0 ms     0 ms   69.41.250.73    UNITED STATES   -   -   THEPLANET.COM INTERNET SERVICES INC
     3     0 ms     0 ms     0 ms   12.96.160.10    UNITED STATES   TEXAS   FLOWER MOUND   THEPLANET.COM INTERNET
SERVICES
     4     0 ms     0 ms     1 ms   70.85.127.74    UNITED STATES   -   -   THEPLANET.COM INTERNET SERVICES INC
     5     0 ms     0 ms     0 ms   70.85.127.5     UNITED STATES   -   -   THEPLANET.COM INTERNET SERVICES INC
     6     1 ms     1 ms     0 ms   64.210.104.57   UNITED STATES   NEW YORK   BRONX   GLOBAL CROSSING
     7    32 ms    32 ms    32 ms   67.17.67.94     UNITED STATES   CALIFORNIA   LOS ANGELES   GLOBAL CROSSING
     8    32 ms    32 ms    33 ms   208.50.13.122   UNITED STATES   ILLINOIS   MACOMB   GLOBAL CROSSING
     9    45 ms    45 ms    45 ms   213.248.80.74   UNITED KINGDOM   -   -   TELIA INTERNATIONAL CARRIER
    10   141 ms   141 ms    *       213.248.64.33   GREECE   IRAKLION (CRETE)   IRAKLEION   TELIA INTERNATIONAL
CARRIER
    11   142 ms   142 ms   142 ms   213.248.64.1    GREECE   IRAKLION (CRETE)   IRAKLEION   TELIA INTERNATIONAL
CARRIER

Traceroute complete.
```

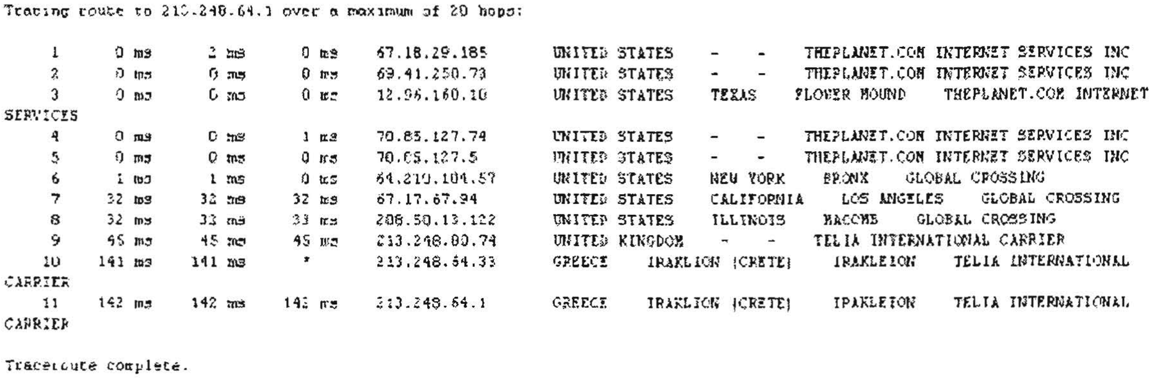


All this looks rather cryptic, but upon examination, the traceroute output is not usually very hard to read. Let's look at this traceroute step by step. We begin by entering either an IPv4 or IPv6 address or a host name, e.g., cnn.com, in the "Tracert" query box.


Traceroute
Enter host name (or IP/IPv6)
Traces the route packets take to this host
213.248.64.1
Tracert

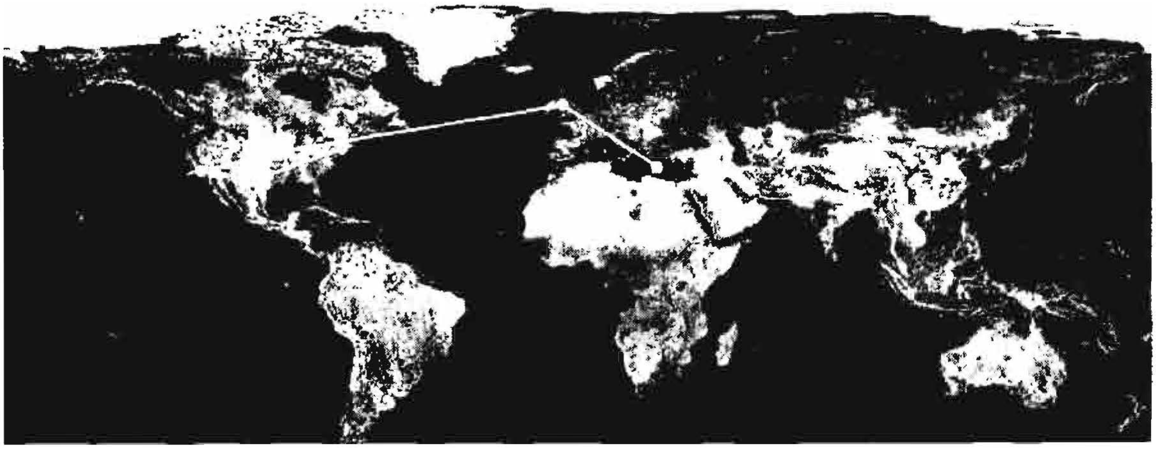
Enter the IP address or host name of the destination computer; in this case, I am using an IPv4 address.

The traceroute results should begin to appear almost instantaneously. What the readout below shows is a "road map" from the starting point of the trace, in this case, IP number 67.18.29.185, *theplanet.com* in Dallas, Texas, to the requested host 213.248.64.1, Telia International, Iraklion Crete. On the first line you see that this traceroute will allow a "maximum of 20 hops," which means the trace will show up to 20 stops of a packet as it moves from router to router before it reaches its destination. A packet is the fundamental data unit sent on the Internet or any other packet-switched network. Each line, numbered from one up to possibly 20 for this traceroute, represents a node. The node number is followed by three time measurements in milliseconds, such as line 8 with 32 ms 32 ms 33 ms. These numbers represent three different measurements of the time—known as the Round Trip Time (RTT)—it took the packet to travel from the origin IP address to that note (router) and back again. Next comes the IP address of the node, its geographical location (sometimes only a country, sometimes a country and city), and finally the domain name (THEPLANET.COM) or the name of the organization that owns that domain (e.g., TELIA INTERNATIONAL CARRIER).

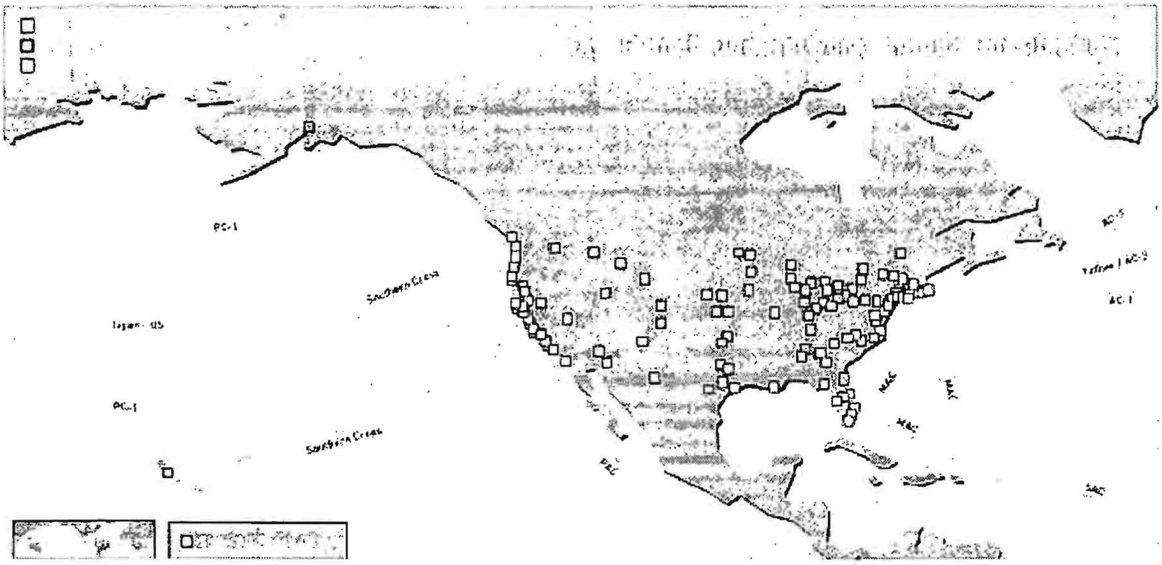


```
Tracing route to 213.248.64.1 over a maximum of 20 hops:

     1     0 ms     2 ms     0 ms    67.18.29.185      UNITED STATES    -    -    THEPLANET.COM INTERNET SERVICES INC
     2     0 ms     0 ms     0 ms    69.41.250.73      UNITED STATES    -    -    THEPLANET.COM INTERNET SERVICES INC
     3     0 ms     0 ms     0 ms    12.96.160.10      UNITED STATES   TEXAS   FLOWER MOUND    THEPLANET.COM INTERNET
SERVICES
     4     0 ms     0 ms     1 ms    70.85.127.74      UNITED STATES    -    -    THEPLANET.COM INTERNET SERVICES INC
     5     0 ms     0 ms     0 ms    70.85.127.5       UNITED STATES    -    -    THEPLANET.COM INTERNET SERVICES INC
     6     1 ms     1 ms     0 ms    64.210.104.57     UNITED STATES   NEW YORK    BRONX    GLOBAL CROSSING
     7    32 ms    32 ms    32 ms    67.17.67.94       UNITED STATES   CALIFORNIA    LOS ANGELES    GLOBAL CROSSING
     8    32 ms    33 ms    33 ms    208.50.13.122     UNITED STATES   ILLINOIS    MACOMB    GLOBAL CROSSING
     9    45 ms    45 ms    45 ms    213.248.80.74     UNITED KINGDOM    -    -    TELIA INTERNATIONAL CARRIER
    10   141 ms   141 ms     *       213.248.64.33     GREECE    IRAKLION (CRETE)    IRAKLEION    TELIA INTERNATIONAL
CARRIER
    11   142 ms   142 ms   142 ms    213.248.64.1      GREECE    IRAKLION (CRETE)    IRAKLEION    TELIA INTERNATIONAL
CARRIER

Traceroute complete.
```

Next, we can look at the visualization of the traceroute on the world map. This makes it graphically clear that packets can take very strange routes to get from point A to point B.

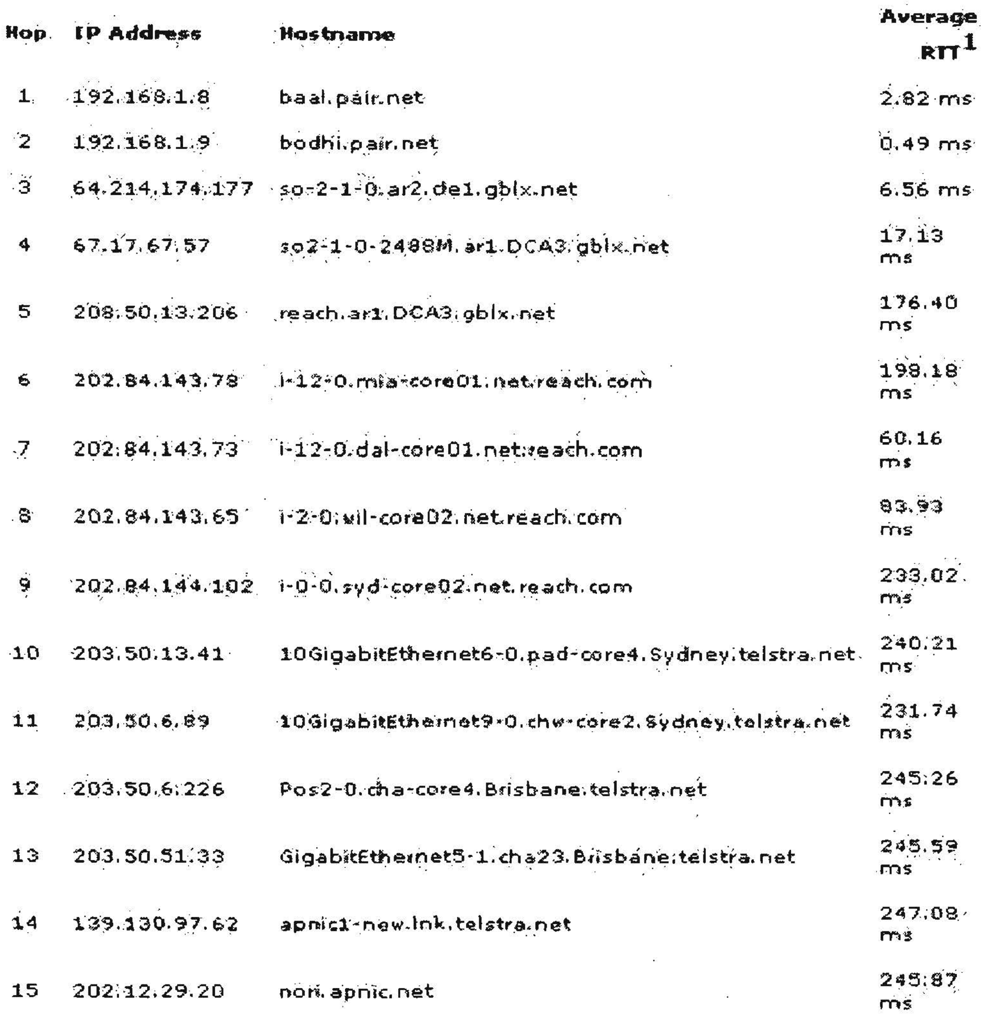


In our example, the packet travels from Texas to New York to California to Illinois before crossing the Atlantic to the UK via one of Global Crossing's three undersea cables.



Global Crossing's Interactive Network Map
http://www.globalcrossing.com/html/map05_11_05.html

Not all traceroutes look like the one above. There are many variations on the original traceroute program now available and many of them are free to use at websites. Frequently you will see a traceroute that is somewhat more cryptic than the one we just examined, but it may reveal more information about the geographical route your packet has taken. Here is a typical traceroute run at All Net Tools (http://www.all-nettools.com/toolbox)



Hop	IP Address	Hostname	Average RTT[1]
1	192.168.1.8	baal.pair.net	2.82 ms
2	192.168.1.9	bodhi.pair.net	0.49 ms
3	64.214.174.177	so-2-1-0.ar2.de1.gblx.net	6.56 ms
4	67.17.67.57	so2-1-0-2488M.ar1.DCA3.gblx.net	17.13 ms
5	208.50.13.206	reach.ar1.DCA3.gblx.net	176.40 ms
6	202.84.143.78	i-12-0.mia-core01.net.reach.com	198.18 ms
7	202.84.143.73	i-12-0.dal-core01.net.reach.com	60.16 ms
8	202.84.143.65	i-2-0.wil-core02.net.reach.com	83.93 ms
9	202.84.144.102	i-0-0.syd-core02.net.reach.com	233.02 ms
10	203.50.13.41	10GigabitEthernet6-0.pad-core4.Sydney.telstra.net	240.21 ms
11	203.50.6.89	10GigabitEthernet9-0.chw-core2.Sydney.telstra.net	231.74 ms
12	203.50.6.226	Pos2-0.cha-core4.Brisbane.telstra.net	245.26 ms
13	203.50.51.33	GigabitEthernet5-1.cha23.Brisbane.telstra.net	245.59 ms
14	139.130.97.62	apnic1-new.lnk.telstra.net	247.08 ms
15	202.12.29.20	nori.apnic.net	245.87 ms

Looking at line 4 in this example, the designation DCA3 indicates this router is in or near Washington, D.C. How do we know this? Because routers often use airport trigraphs to show their location and DCA=Washington's Reagan National Airport. A traceroute frequently provides us insights into the physical path the packet travels by indicating the locations of the routers along the way.

Following hops 4 through 7 we can see the packet moves from Washington to Miami to Dallas and then on line 8 to the mysterious *wil-core02*. What is "*wil*"? It is not an airport code but rather refers to a building, the One Wilshire Building in Los Angeles. "One Wilshire is home to virtually all of the market leaders in the telecommunications industry. The property currently houses over 120 telecom related companies including: AT&T, Cable & Wireless, China Telecom, Global Crossing, Level 3

Communications, MCI Worldcom, MFS, PacBell, Qwest Communications, Sprint, Time Warner (AOL), Verizon (GTE) and XO Communications."[157]

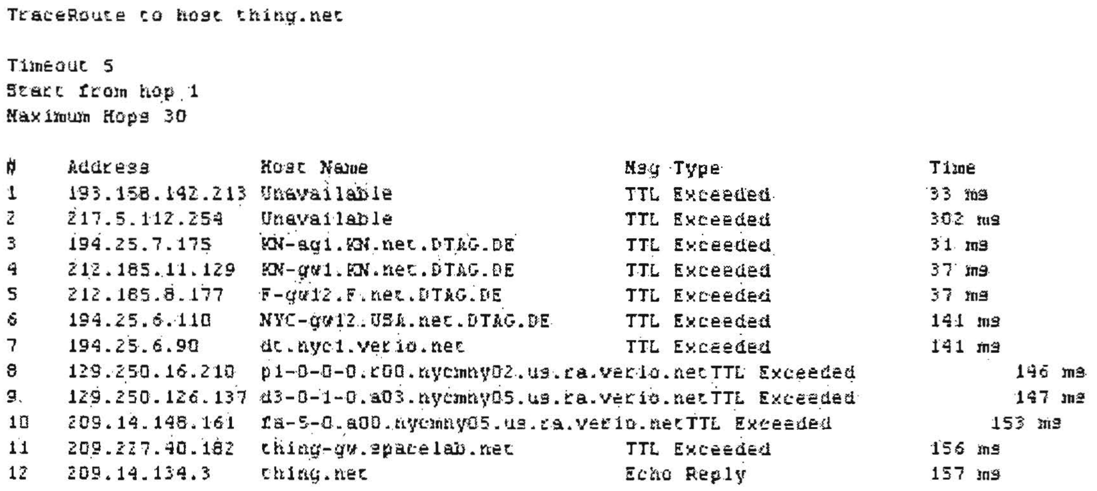
At this point note the rather dramatic increase in the RTT from 83.93 ms to 233.02 ms. The packet leaves the US and travels to Sydney, Australia, (*syd-core02*) between hops 8 and 9. In this example, *wil-core02* is the gateway router to the trans-Pacific link of the Reach network. Reach is an Asia-Pacific focused backbone provider operating a "high-speed cable network in the Asia-Pacific region. It has significant interests in all major submarine cables consortia in the Asia-Pacific region." The other indication that the packet traveled via submarine cable instead of satellite is the fact that the RTT remains relatively low. A good rule of thumb (though not by any means a guarantee) is that satellite traffic usually has a >500 ms RTT.

The packet stays on the Reach network all the way to hop 10 in Sydney where it is handed off to Telstra, Australia's largest telecommunications company. Here we see another indication of the network infrastructure: the packet is now in Telstra's 10GigabitEthernet6-0. In February 2003, Telstra activated the first 10 Gigabit Ethernet link on its Internet Direct backbone, the network that delivers broadband Internet services across Australia. The final geographical hops in this traceroute occur between hops 11 and 12 where the packet travels from Sydney to Brisbane. In fact, APNIC (the Asia Pacific Network Information Center) is located in Milton, Brisbane, Australia, the same location as the server *nori.apnic.net*. However, be cautious about geolocating a final destination server with the actual location of the organization you're researching because that organization's site may well be hosted in a separate location.

Traceroute Anomalies and Failures

Watch out for traceroute anomalies. For example, look at line 6 in this traceroute at NYC-gw12.USA.net.DTAG.DE. Despite the fact the router has a German top-level domain (DE), this router is in the US (NYC). Note also the RTT increase from 37 ms to 141 ms.

[157] "Our Building," *One Wilshire*, 2002, <http://www.onewilshire.com/our_building/index.htm> (14 November 2006).

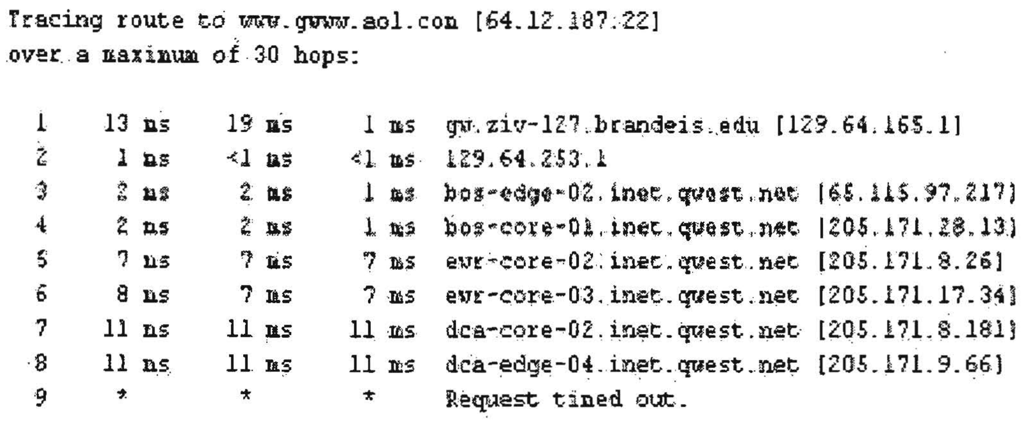


```
TraceRoute to host thing.net

Timeout 5
Start from hop 1
Maximum Hops 30

#     Address          Host Name                        Msg Type          Time
1     193.158.142.213  Unavailable                      TTL Exceeded      33 ms
2     217.5.112.254    Unavailable                      TTL Exceeded      302 ms
3     194.25.7.175     KN-ag1.KN.net.DTAG.DE            TTL Exceeded      31 ms
4     212.185.11.129   KN-gw1.KN.net.DTAG.DE            TTL Exceeded      37 ms
5     212.185.8.177    F-gw12.F.net.DTAG.DE             TTL Exceeded      37 ms
6     194.25.6.110     NYC-gw12.USA.net.DTAG.DE         TTL Exceeded      141 ms
7     194.25.6.90      dt.nyc1.verio.net                TTL Exceeded      141 ms
8     129.250.16.210   p1-0-0-0.r00.nycmny02.us.ra.verio.netTTL Exceeded        146 ms
9     129.250.126.137  d3-0-1-0.a03.nycmny05.us.ra.verio.netTTL Exceeded        147 ms
10    209.14.148.161   fa-5-0.a00.nycmny05.us.ra.verio.netTTL Exceeded        153 ms
11    209.227.40.182   thing-gw.spacelab.net            TTL Exceeded      156 ms
12    209.14.134.3     thing.net                        Echo Reply        157 ms
```

You may also run into incomplete traceroutes, usually indicated by asterisks and, sometimes, by the warning "Request timed out." There are several reasons for a traceroute to fail.

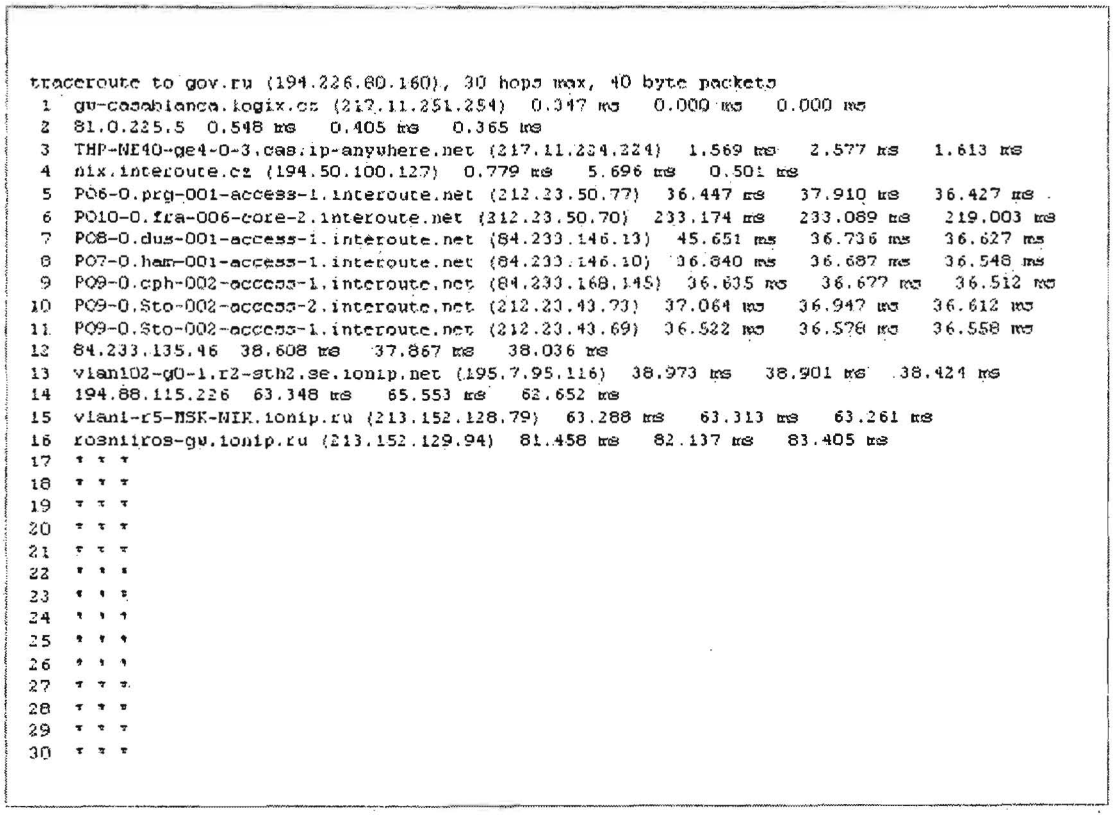
- a network problem, e.g., a server or router on the network is down (you will probably see "Request timed out"). The router immediately after the last visible one is usually the culprit.
- a server or router along the path has rejected your packet. Again, the router immediately after the last visible one is usually the culprit.
- the target host does not exist on the network because it has been disconnected, turned off, or is otherwise unreachable. You may see a !H or !N message in the traceroute.
- the traceroute may have encountered a routing loop, in which case the packet will simply bounce between two routers and never reach its destination.
- a firewall is in the route path (you may or may not see "Request timed out").
- the traceroute encounters a private IP address.
- there is packet filtering occurring somewhere along the traceroute path.

Here is a typical incomplete traceroute due to a network problem. The traceroute timed out at hop 9 because of what turned out to be an ATM router problem on the Quest network. This was determined by checking the Quest network status at the time of the interruption.



```
Tracing route to www.gwww.aol.com [64.12.187.22]
over a maximum of 30 hops:

  1    13 ms    19 ms     1 ms  gw.ziv-127.brandeis.edu [129.64.165.1]
  2     1 ms    <1 ms    <1 ms  129.64.253.1
  3     2 ms     2 ms     1 ms  bos-edge-02.inet.qwest.net [65.115.97.217]
  4     2 ms     2 ms     1 ms  bos-core-01.inet.qwest.net [205.171.28.13]
  5     7 ms     7 ms     7 ms  ewr-core-02.inet.qwest.net [205.171.8.26]
  6     8 ms     7 ms     7 ms  ewr-core-03.inet.qwest.net [205.171.17.34]
  7    11 ms    11 ms    11 ms  dca-core-02.inet.qwest.net [205.171.8.181]
  8    11 ms    11 ms    11 ms  dca-edge-04.inet.qwest.net [205.171.9.66]
  9     *        *        *     Request timed out.
```

The next example shows what is probably a firewall that caused the traceroute to fail:

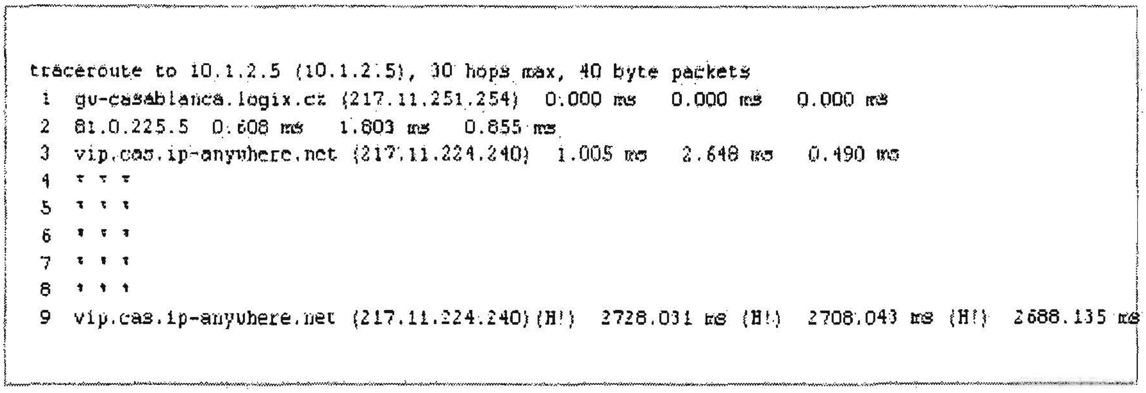


```
traceroute to gov.ru (194.226.80.160), 30 hops max, 40 byte packets
 1  gw-casablanca.logix.cz (212.11.251.254)  0.347 ms  0.000 ms  0.000 ms
 2  81.0.225.5  0.548 ms  0.405 ms  0.365 ms
 3  THP-NE40-ge4-0-3.cas.ip-anywhere.net (217.11.224.224)  1.569 ms  2.577 ms  1.613 ms
 4  nix.interoute.cz (194.50.100.127)  0.779 ms  5.696 ms  0.501 ms
 5  PO6-0.prg-001-access-1.interoute.net (212.23.50.77)  36.447 ms  37.910 ms  36.427 ms
 6  PO10-0.fra-006-core-2.interoute.net (212.23.50.70)  233.174 ms  233.089 ms  219.003 ms
 7  PO8-0.dus-001-access-1.interoute.net (84.233.146.13)  45.651 ms  36.736 ms  36.627 ms
 8  PO7-0.ham-001-access-1.interoute.net (84.233.146.10)  36.840 ms  36.687 ms  36.548 ms
 9  PO9-0.cph-002-access-1.interoute.net (84.233.168.145)  36.635 ms  36.677 ms  36.512 ms
10  PO9-0.Sto-002-access-2.interoute.net (212.23.43.73)  37.064 ms  36.947 ms  36.612 ms
11  PO9-0.Sto-002-access-1.interoute.net (212.23.43.69)  36.522 ms  36.578 ms  36.558 ms
12  84.233.135.46  38.608 ms  37.867 ms  38.036 ms
13  vlan102-g0-1.r2-sth2.se.ionip.net (195.7.95.116)  38.973 ms  38.901 ms  38.424 ms
14  194.88.115.226  63.348 ms  65.553 ms  62.652 ms
15  vlan1-r5-MSK-MIK.ionip.ru (213.152.128.79)  63.288 ms  63.313 ms  63.261 ms
16  rosniiros-gw.ionip.ru (213.152.129.94)  81.458 ms  82.137 ms  83.405 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

You may also encounter a routing loop in a traceroute. This occurs when the packet is simply bounced between two routers until the traceroute reaches its maximum number of hops. In this example, the packet was bouncing between routers at 186.40.64.94 and 186.40.64.93:

```
Tracing route to lostserver.confusion.net [186.9.17.153]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  186.217.33.1
  2    60 ms    70 ms    60 ms  rtr-2.confusion.net [186.40.64.94]
  3    70 ms    71 ms    70 ms  rtr-1.confusion.net [186.40.64.93]
  4    60 ms    70 ms    60 ms  rtr-2.confusion.net [186.40.64.94]
  5    70 ms    70 ms    70 ms  rtr-1.confusion.net [186.40.64.93]
  6    60 ms    70 ms    61 ms  rtr-2.confusion.net [186.40.64.94]
  7    70 ms    70 ms    70 ms  rtr-1.confusion.net [186.40.64.93]
  8    60 ms    70 ms    60 ms  rtr-2.confusion.net [186.40.64.94]
  9    70 ms    70 ms    70 ms  rtr-1.confusion.net [186.40.64.93]
...
...
...
Trace complete.
```

Here is what you might see in the case of an unreachable host. In this example, the traceroute attempted to reach a private IP address, but that host was not reachable on the network. Note the H! message, which is usually appears as !H.

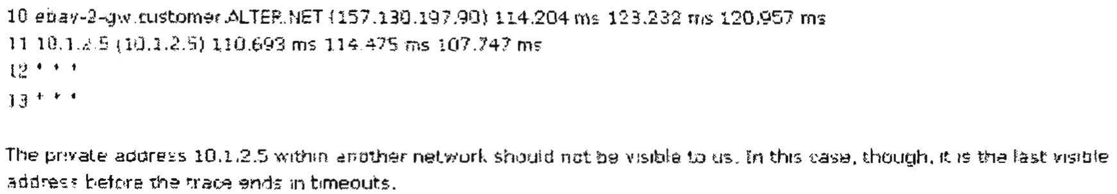


```
traceroute to 10.1.2.5 (10.1.2.5), 30 hops max, 40 byte packets
 1  gv-casablanca.logix.cz (217.11.251.254)  0.000 ms   0.000 ms   0.000 ms
 2  81.0.225.5  0.608 ms   1.803 ms   0.855 ms
 3  vip.cas.ip-anywhere.net (217.11.224.240)  1.005 ms   2.648 ms   0.490 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  vip.cas.ip-anywhere.net (217.11.224.240)(H!)  2728.031 ms (H!)  2708.043 ms (H!)  2688.135 ms
```

A private IP address will cause a traceroute to fail. Normally, you should not see these IP address blocks in a traceroute (the traceroute should time out before it reaches the private address). However, if you reach a private IP address, it is easy to spot because it belongs to a block of IPv4 addresses that are reserved for private use, meaning these address ranges are unassigned non-Internet addresses. Because they cannot be routed over the Internet, these private address are only for use on internal systems. In the following example, the traceroute should have timed out at hop 10:

- 10.*

- 172.[16-31].*
- 192.168.*



```
10 ebay-2-gw.customer.ALTER.NET (157.130.197.90) 114.204 ms 123.232 ms 120.957 ms
11 10.1.2.5 (10.1.2.5) 110.693 ms 114.475 ms 107.747 ms
12 * * *
13 * * *
```

The private address 10.1.2.5 within another network should not be visible to us. In this case, though, it is the last visible address before the trace ends in timeouts.

Traceroute Servers

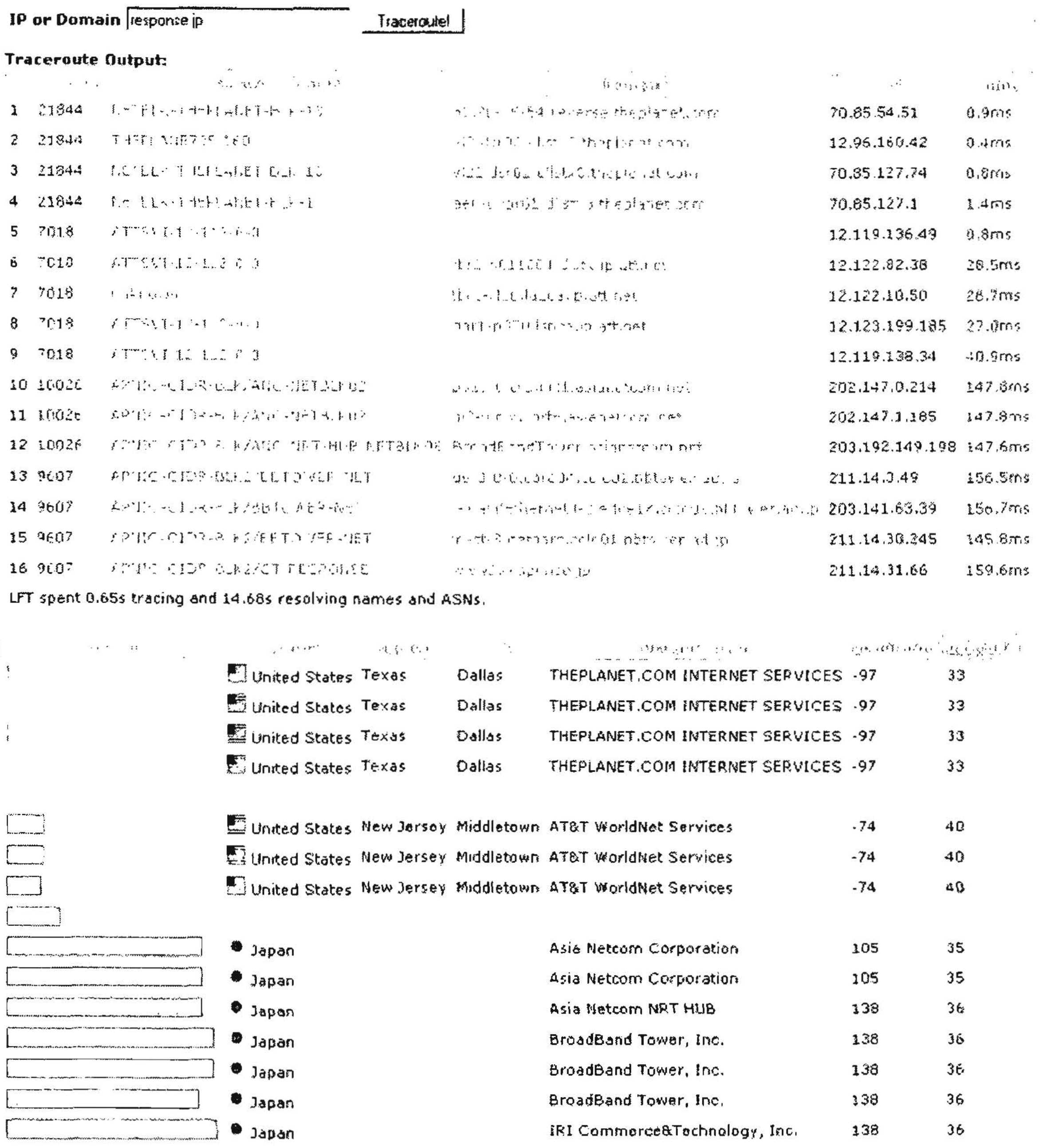
As with other Internet utilities, there are many sites that let you run a traceroute from their site to the domain or IP of your choice. Multiple Traceroute Gateway deserves a special mention because it will run a traceroute to any host or IP address from multiple starting points. The starting points can be anywhere in the world. Unfortunately, many of the traceroute starting points listed at the site no longer work, so you may have to try several to find a good one for a particular region. I recommend you not try to run too many traceroutes at once because that can be a very slow process. There are also now numerous sites offering traceroute utilities for IPv6.

The Logbud Toolkit

Logbud's set of webmaster tools is definitely worth adding to your own set of Internet toolkits. What first attracted me to it was the visual traceroute that does the following:

> **Visual Traceroute** shows geo information of the gateways it traverses: Country, Region, (State for the US), City and Network organization. The way of the trace is shown on small and big geographical maps. Also Visual Traceroute displays network names (e.g., [GNTY-NETBLK-4]) and AS (autonomous system) numbers (e.g., [AS6846]).

As you can see from this traceroute to a Japanese domain, the traceroute information from Logbud is much easier to read and understand. There is also an accompanying map, but it is not always accurate (in this case, the trace ended in New Jersey). This is certainly one of the clearest, most useful traceroute tools I have seen.



IP or Domain: response ip — Traceroute!

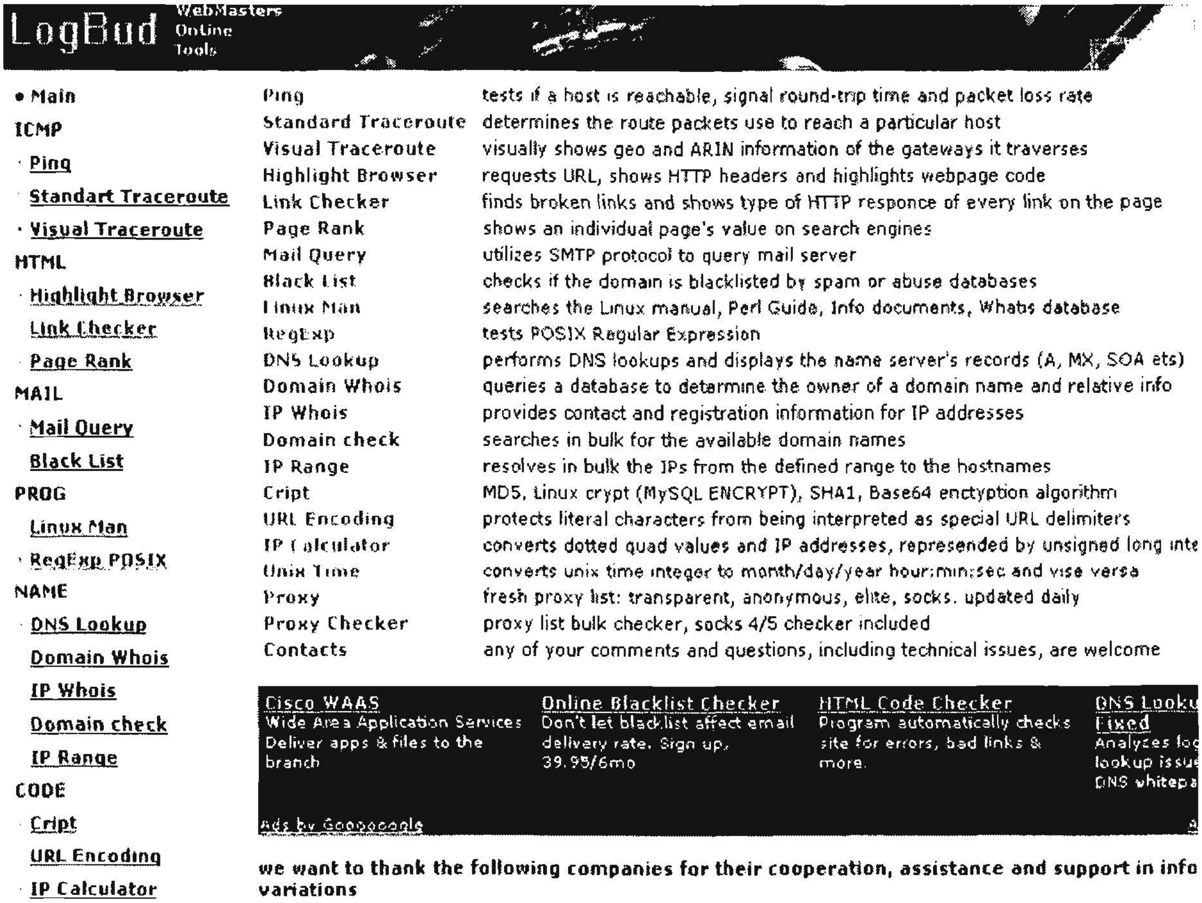
Traceroute Output:

```
 1  21844  [illegible]  [illegible]  70.85.54.51      0.9ms
 2  21844  [illegible]  [illegible]  12.96.160.42     0.4ms
 3  21844  [illegible]  [illegible]  70.85.127.74     0.8ms
 4  21844  [illegible]  [illegible]  70.85.127.1      1.4ms
 5  7018   [illegible]               12.119.136.49    0.8ms
 6  7018   [illegible]  [illegible]  12.122.82.38     28.5ms
 7  7018   [illegible]  [illegible]  12.122.10.50     28.7ms
 8  7018   [illegible]  [illegible]  12.123.199.185   27.0ms
 9  7018   [illegible]               12.119.138.34    40.9ms
10  10026  [illegible]  [illegible]  202.147.0.214    147.8ms
11  10026  [illegible]  [illegible]  202.147.1.185    147.8ms
12  10026  [illegible]  [illegible]  203.192.149.198  147.6ms
13  9607   [illegible]  [illegible]  211.14.3.49      156.5ms
14  9607   [illegible]  [illegible]  203.141.63.39    156.7ms
15  9607   [illegible]  [illegible]  211.14.30.245    145.8ms
16  9607   [illegible]  [illegible]  211.14.31.66     159.6ms
LFT spent 0.65s tracing and 14.68s resolving names and ASNs.
```

```
United States  Texas       Dallas      THEPLANET.COM INTERNET SERVICES  -97   33
United States  Texas       Dallas      THEPLANET.COM INTERNET SERVICES  -97   33
United States  Texas       Dallas      THEPLANET.COM INTERNET SERVICES  -97   33
United States  Texas       Dallas      THEPLANET.COM INTERNET SERVICES  -97   33

United States  New Jersey  Middletown  AT&T WorldNet Services           -74   40
United States  New Jersey  Middletown  AT&T WorldNet Services           -74   40
United States  New Jersey  Middletown  AT&T WorldNet Services           -74   40

● Japan                                Asia Netcom Corporation          105   35
● Japan                                Asia Netcom Corporation          105   35
● Japan                                Asia Netcom NRT HUB              138   36
● Japan                                BroadBand Tower, Inc.            138   36
● Japan                                BroadBand Tower, Inc.            138   36
● Japan                                BroadBand Tower, Inc.            138   36
● Japan                                IRI Commerce&Technology, Inc.    138   36
```

Logbud also offers a traceroute manual that has some interesting scenarios of hard to understand hops that are sometimes seen in a traceroute. It's somehow comforting when the author looks at a particular traceroute hop and comments "God only knows what's going on with [hop] 12."

Visual traceroute is only one of a number of very useful tools Logbud offers. Of special interest are those tools that help provide information about domain names and IP addresses. Note, in particular, the **IP Range query**, which does a bulk query of IP addresses in a certain range and resolves them to their host names.



Ping	tests if a host is reachable, signal round-trip time and packet loss rate
Standard Traceroute	determines the route packets use to reach a particular host
Visual Traceroute	visually shows geo and ARIN information of the gateways it traverses
Highlight Browser	requests URL, shows HTTP headers and highlights webpage code
Link Checker	finds broken links and shows type of HTTP responce of every link on the page
Page Rank	shows an individual page's value on search engines
Mail Query	utilizes SMTP protocol to query mail server
Black List	checks if the domain is blacklisted by spam or abuse databases
Linux Man	searches the Linux manual, Perl Guide, Info documents, Whatis database
RegExp	tests POSIX Regular Expression
DNS Lookup	performs DNS lookups and displays the name server's records (A, MX, SOA ets)
Domain Whois	queries a database to determine the owner of a domain name and relative info
IP Whois	provides contact and registration information for IP addresses
Domain check	searches in bulk for the available domain names
IP Range	resolves in bulk the IPs from the defined range to the hostnames
Cript	MD5, Linux crypt (MySQL ENCRYPT), SHA1, Base64 enctyption algorithm
URL Encoding	protects literal characters from being interpreted as special URL delimiters
IP Calculator	converts dotted quad values and IP addresses, represended by unsigned long inte
Unix Time	converts unix time integer to month/day/year hour:min:sec and vise versa
Proxy	fresh proxy list: transparent, anonymous, elite, socks. updated daily
Proxy Checker	proxy list bulk checker, socks 4/5 checker included
Contacts	any of your comments and questions, including technical issues, are welcome

we want to thank the following companies for their cooperation, assistance and support in info variations

The Logbud site packages a number of basic network analysis tools and provides some improved interfaces and displays to make them more useful. Highly recommended.

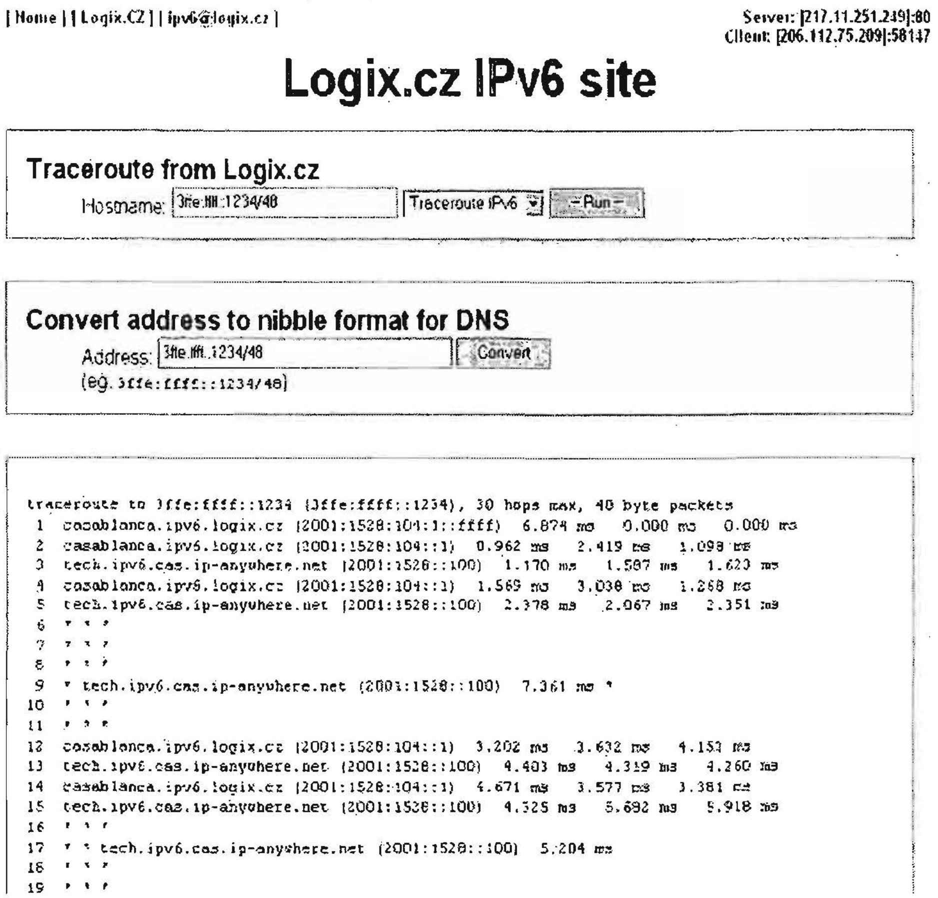
Logbud Online Tools	http://www.logbud.com/

More Traceroute Sites and Toolkits

IP Address Guide	http://www.internetipaddress.com/traceroute.aspx
All Nettools.com	http://www.all-nettools.com/toolbox
Cogentco	http://www.cogentco.com/htdocs/glass.php
Geektools Traceroute	http://www.geektools.com/traceroute.php
IP-Plus Traceroute Servers	http://www.ip-plus.ch/tools/traceroute.en.html
Multiple Traceroute Gateway	http://www.tracert.com/cgi-bin/trace.pl

New York Internet Traceroute Links	http://www.nyi.net/traceroute.html
Opus One Traceroute	http://www.opus1.com/www/traceroute.html
SixXs IPv4 and IPv6 Traceroute	http://www.sixxs.net/tools/traceroute/
Traceroute.org	http://www.traceroute.org/
Tracerouters Around the World	http://tracerouters.nielssen.com/
BGPNet IPv4 Wiki	http://www.bgp4.net/tr
BGPNet IPv6 Wiki	http://www.bgp4.net/tr6

An excellent resource for finding IPv6 traceroute sites; an example of an IPv6 traceroute is shown below:



[Home] [Logix.CZ] [ipv6@logix.cz]

Server: [217.11.251.249]:80
Client: [206.112.75.209]:58147

Logix.cz IPv6 site

Traceroute from Logix.cz

Hostname: 3ffe:ffff::1234/48 Traceroute IPv6 =Run=

Convert address to nibble format for DNS

Address: 3ffe:ffff::1234/48 Convert
(eg. 3ffe:ffff::1234/48)

```
traceroute to 3ffe:ffff::1234 (3ffe:ffff::1234), 30 hops max, 40 byte packets
 1  casablanca.ipv6.logix.cz (2001:1528:104:1::ffff)  6.874 ms   0.000 ms   0.000 ms
 2  casablanca.ipv6.logix.cz (2001:1528:104::1)  0.962 ms   2.419 ms   1.098 ms
 3  tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  1.170 ms   1.587 ms   1.623 ms
 4  casablanca.ipv6.logix.cz (2001:1528:104::1)  1.569 ms   3.038 ms   1.268 ms
 5  tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  2.378 ms   2.067 ms   2.351 ms
 6  * * *
 7  * * *
 8  * * *
 9  * tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  7.361 ms *
10  * * *
11  * * *
12  casablanca.ipv6.logix.cz (2001:1528:104::1)  3.202 ms   3.632 ms   4.153 ms
13  tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  4.403 ms   4.319 ms   4.260 ms
14  casablanca.ipv6.logix.cz (2001:1528:104::1)  4.671 ms   3.577 ms   3.381 ms
15  tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  4.325 ms   5.692 ms   5.918 ms
16  * * *
17  * * tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  5.204 ms
18  * * *
19  * * *
```

More Traceroute Tools

Learning to read and interpret traceroute data can be very frustrating and confusing in part because there is no standard way of naming routers and any number of different traceroute programs showing a variety of types of data. Here are some sites that are useful in helping to explain traceroutes.

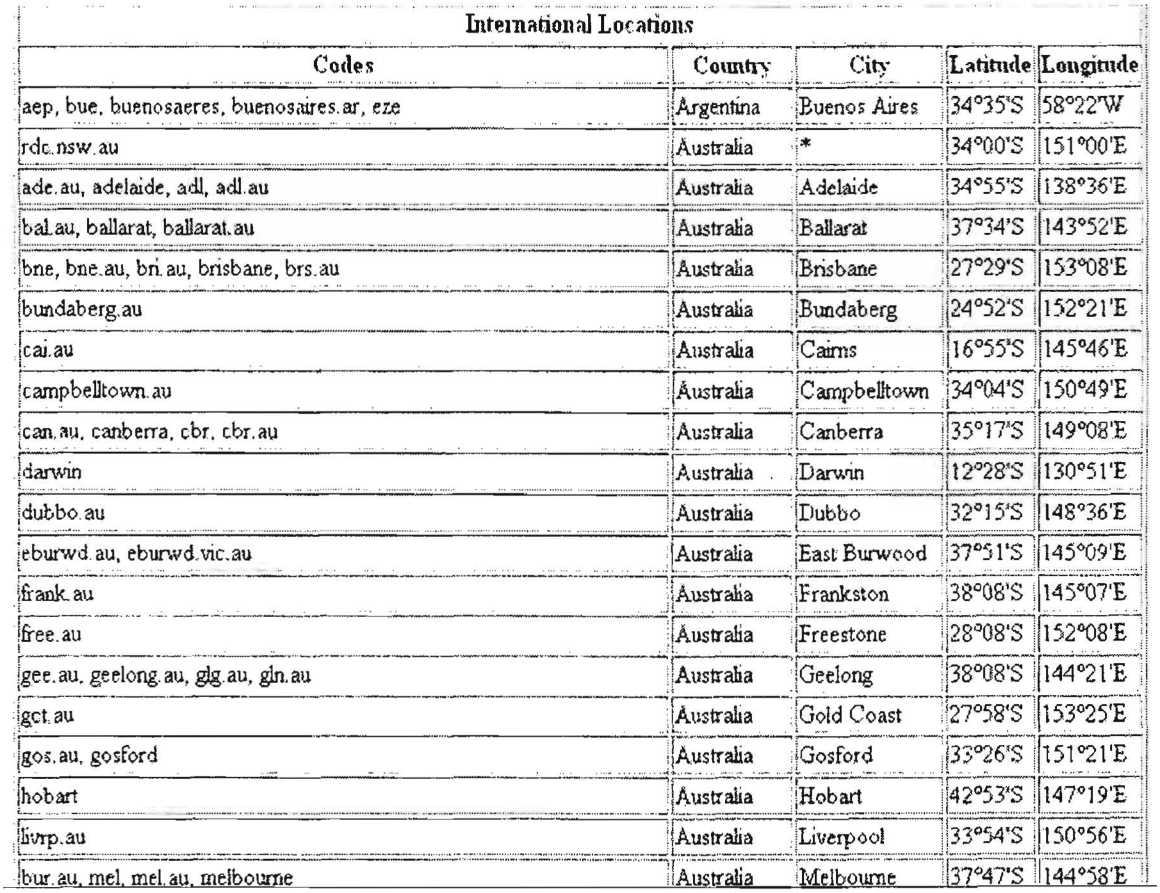
Airport and City Code Database http://www.airportcitycodes.com/aaa/CCDBFrame.html

World Airport Codes http://www.world-airport-codes.com/

Airlines of the Web Airport Codes http://flyaow.com/airportcode.htm

Sarangworld Traceroute Project Known Hostname Codes http://www.sarangworld.com/TRACEROUTE/showdb-2.php3

A huge file of codes and IP addresses seen in traceroutes translated into city names with latitudes and longitudes



International Locations

Codes	Country	City	Latitude	Longitude
aep, bue, buenosaeres, buenosaires.ar, eze	Argentina	Buenos Aires	34°35'S	58°22'W
rdc.nsw.au	Australia	*	34°00'S	151°00'E
ade.au, adelaide, adl, adl.au	Australia	Adelaide	34°55'S	138°36'E
bal.au, ballarat, ballarat.au	Australia	Ballarat	37°34'S	143°52'E
bne, bne.au, bri.au, brisbane, brs.au	Australia	Brisbane	27°29'S	153°08'E
bundaberg.au	Australia	Bundaberg	24°52'S	152°21'E
cai.au	Australia	Cairns	16°55'S	145°46'E
campbelltown.au	Australia	Campbelltown	34°04'S	150°49'E
can.au, canberra, cbr, cbr.au	Australia	Canberra	35°17'S	149°08'E
darwin	Australia	Darwin	12°28'S	130°51'E
dubbo.au	Australia	Dubbo	32°15'S	148°36'E
eburwd.au, eburwd.vic.au	Australia	East Burwood	37°51'S	145°09'E
frank.au	Australia	Frankston	38°08'S	145°07'E
free.au	Australia	Freestone	28°08'S	152°08'E
gee.au, geelong.au, glg.au, gln.au	Australia	Geelong	38°08'S	144°21'E
gct.au	Australia	Gold Coast	27°58'S	153°25'E
gos.au, gosford	Australia	Gosford	33°26'S	151°21'E
hobart	Australia	Hobart	42°53'S	147°19'E
livrp.au	Australia	Liverpool	33°54'S	150°56'E
bur.au, mel, mel.au, melbourne	Australia	Melbourne	37°47'S	144°58'E

Traceroute Articles and Tutorials

It is important to understand the value and the pitfalls of using traceroute for network analysis. While much Internet traffic is symmetric, in some cases it is not, i.e., the traffic does not travel the same way in both directions. Although traceroute can tell you whether two networks communicate directly or indirectly, ***it cannot tell you anything with certainty about the nature of their relationship***, such as who is the provider and who is the customer. For a good explanation of how traceroute works (and the some of the drawbacks of using traceroute), look at these traceroute articles and tutorials:

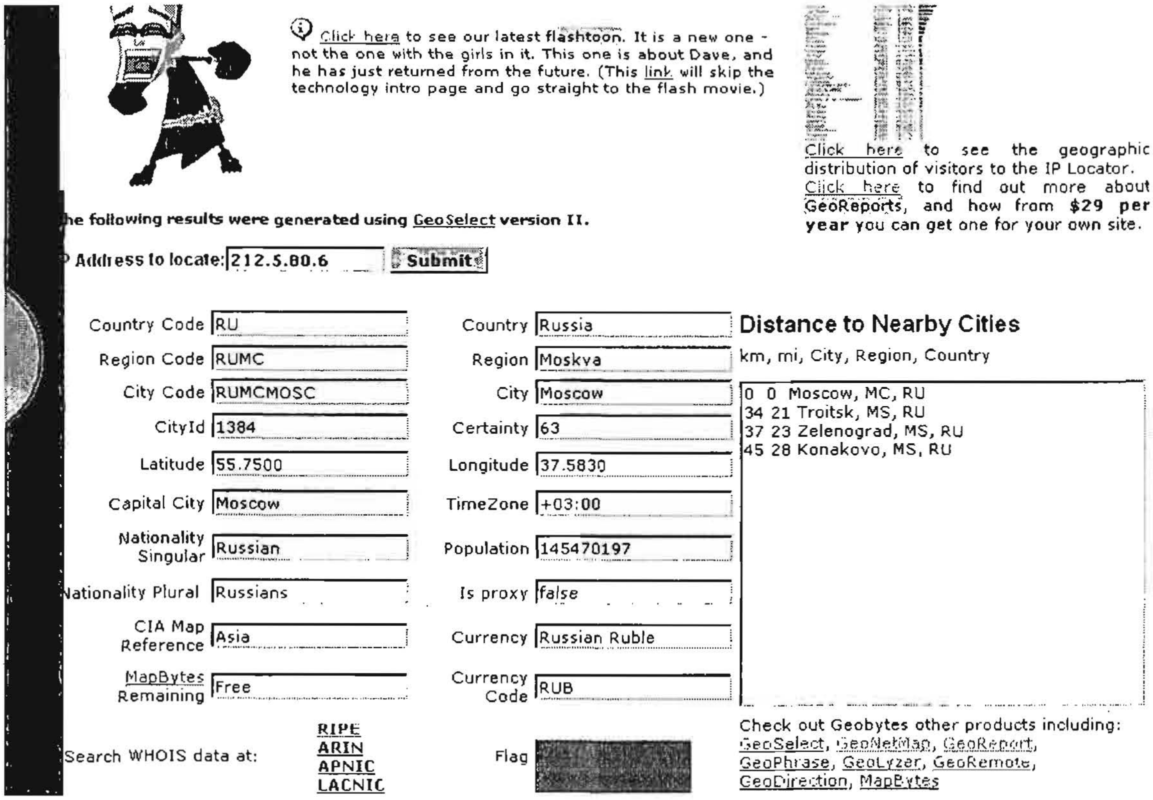
Mapping Where the Data Flows	http://www.isoc.org/oti/articles/0200/dodge.html
Traceroute Tutorial	http://www.exit109.com/~jeremy/news/providers/traceroute.html
Russ Haynal's Traceroute Overview	http://navigators.com/traceroute.html

Geolocating Internet Addresses

Geolocating Internet addresses using IP addresses has become big business and has applications for individuals as well. Why is knowing where someone is (actually, where the host computer is that he is using to connect to the Internet is physically located) important or useful? Some of the many uses of IP address geolocation include, but are not limited to:

- Tailored search results: some search engines will put local sites higher in the results' list, so if you search for "orthodontists" and you are in Boise, Idaho, local orthodontists may come up first.
- Online companies may use geolocation to tailor currency, sales tax, shipping rates, and even in some cases, prices by locality
- Automatic localization of configuration profiles (no need to reset a browser or chat software, it automatically detects where you are).
- Reducing network congestion by routing users to the closest servers that mirror the original content.
- Targeting advertising to a specific city, state, or country.
- Complying with local laws; this especially applies to online gambling, which is legal in some places and not in others.
- Controlling access; France uses geolocation to prohibit French Internet users from accessing pro-Nazi websites; China has a long, effective, and disturbing history of using geolocation to prevent access to many sites the Chinese government deems "unacceptable."

There are a number of companies, such as Quova and Digital Envoy, that sell IP geolocation/IP mapping products, but they do not give this technology away for free. However, a few websites do provide free online tools to geolocate IP addresses and/or domain names. All these tools have inherent limitations because of the ways in which they go about determining the physical location of an address. Knowing where your users are located has become increasingly important over time, whether you're a company that wants to know which products to target at a certain audience or a government seeking to control your Internet space. Therefore, because there is so much money to be made in this area, the free tools are simply not nearly as good as the ones you pay for.



Click here to see our latest flashtoon. It is a new one - not the one with the girls in it. This one is about Dave, and he has just returned from the future. (This link will skip the technology intro page and go straight to the flash movie.)

Click here to see the geographic distribution of visitors to the IP Locator.
Click here to find out more about GeoReports, and how from **$29 per year** you can get one for your own site.

he following results were generated using GeoSelect version II.

P Address to locate: 212.5.80.6

Country Code	RU	Country	Russia
Region Code	RUMC	Region	Moskva
City Code	RUMCMOSC	City	Moscow
CityId	1384	Certainty	63
Latitude	55.7500	Longitude	37.5830
Capital City	Moscow	TimeZone	+03:00
Nationality Singular	Russian	Population	145470197
Nationality Plural	Russians	Is proxy	false
CIA Map Reference	Asia	Currency	Russian Ruble
MapBytes Remaining	Free	Currency Code	RUB
Search WHOIS data at:	RIPE ARIN APNIC LACNIC	Flag	

Distance to Nearby Cities

km, mi, City, Region, Country

```
0  0  Moscow, MC, RU
34 21 Troitsk, MS, RU
37 23 Zelenograd, MS, RU
45 28 Konakovo, MS, RU
```

Check out Geobytes other products including: GeoSelect, GeoNetMap, GeoReport, GeoPhrase, GeoLyzer, GeoRemote, GeoDirection, MapBytes

Geobytes IP Locator http://www.geobytes.com/IpLocator.htm

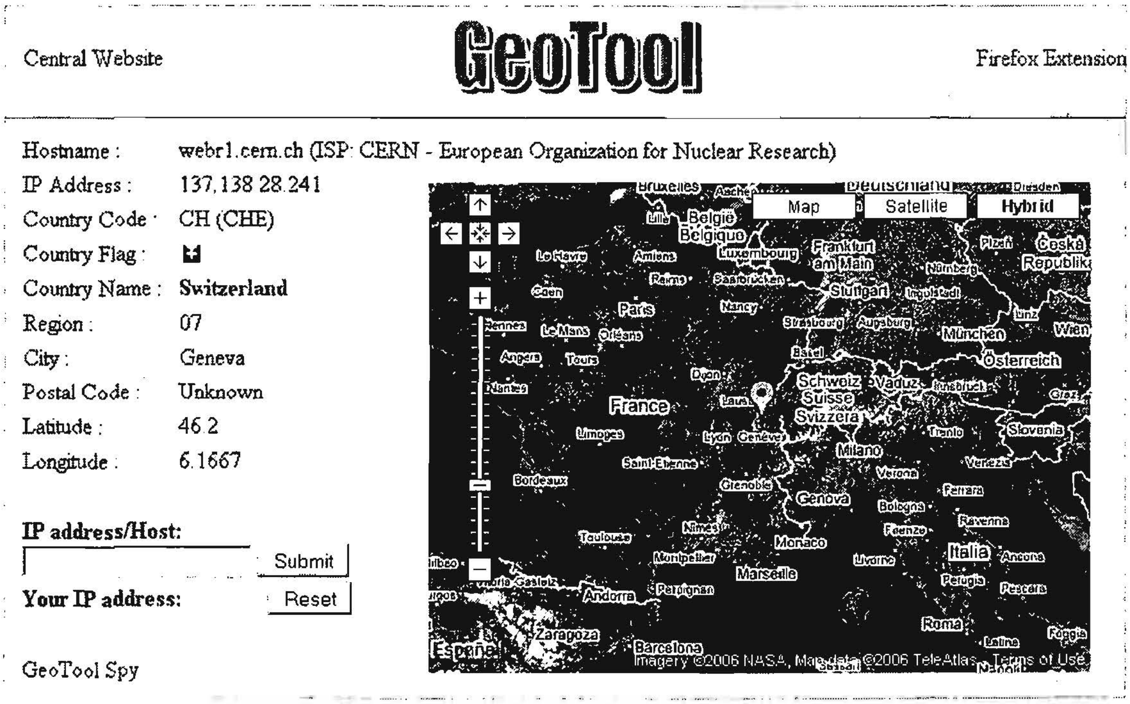
The best of the free online geolocation tools, Geobytes is the commercial version of NetWorldMap that provides a more detailed report on IP address geolocation. GeoSelect does not use any DNS reverse lookups or Whois lookups to determine location. GeoSelect uses its proprietary GeoNetMap database to determine IP location. "The purpose of the Geobytes map is to map IP Addresses to geographical locations. To achieve this we acquire seed data from a number of sources. All of these sites ask the web surfer to provide their geographic location, and this location along with the user's IP Address is forwarded to us as seed data. We then run this data through a series of algorithms which identify and extract collaborating seed points."[158] If you want to see the original site where Geobytes began collecting its data, visit NetWorldMap.

NetWorldMap http://www.networldmap.com/TryIt.htm

NetWorldMap lets users enter IP addresses, then returns information about where that server is located at the city level. It does this by gathering vast amounts of data from volunteers who, for several years, have been entering information about the physical locations of their addresses. Of course, this opens NetWorldMap up to abuse, but the information provided by volunteers is crosschecked for accuracy. The site now claims that "currently it can only locate about 97.8% of the Internet's address space," which is a vast improvement over its earlier claims. While Networldmap is far from the perfect way to geolocate addresses, it is a valuable tool.

GeoTool http://www.rleeden.no-ip.com/geotool.php

This site also uses the same free Maxmind city database and Google maps to locate and show one IP address at a time. GeoTool adds information about the IP address. Note the GeoTool Spy option: this will show who is using the tool at the moment (including you).



Hostname :	webr1.cern.ch (ISP: CERN - European Organization for Nuclear Research)
IP Address :	137.138.28.241
Country Code :	CH (CHE)
Country Flag :	
Country Name :	Switzerland
Region :	07
City :	Geneva
Postal Code :	Unknown
Latitude :	46.2
Longitude :	6.1667

IP address/Host:

Your IP address:

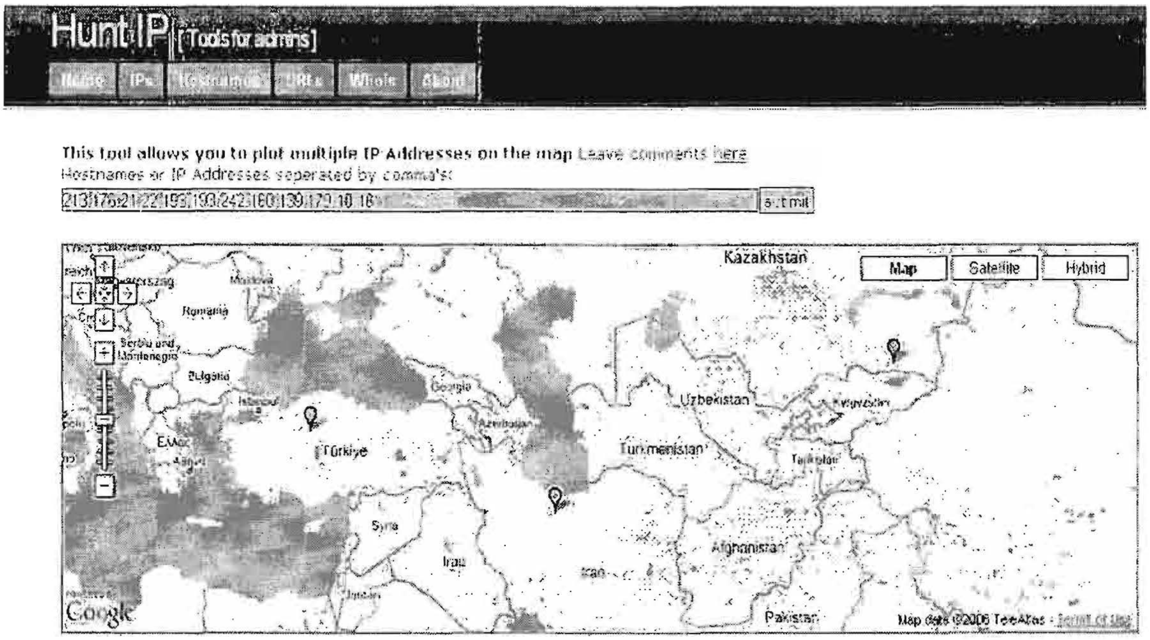
[158] Geoselect Frequently Asked Questions, Geobytes.com,<http://www.geobytes.com/FAQ.htm> (14 November 2006).

HostIP.info http://www.hostip.info/

HostIP is a community effort to build a non-commercial database of geolocated IP addresses. It uses two sources of information to generate its geolocation tool: people identifying their city as associated with an IP address and automatic traceroutes.

HuntIP http://www.huntip.com/Tools/mapips.php

HuntIP is a set of tools designed to help sysadmins do a number of things, including plot multiple IP addresses on a map. Keep in mind the caveat from the site's creator: "This site should be used as a tool for investigative purposes only. The information provided here may not be correct and should not be trusted." To perform IP geolocation, ***HuntIP uses the free GeoLite data provided by Maxmind***, which also sells more accurate IP geolocation data at its website. Because Maxmind's free site limits queries to 25 per day per incoming IP address, I expect HuntIP operates under the same restrictions. HuntIP uses a Google Map mashup to plot IP address locations. Here I have plotted three IP addresses on the Google Map image just to give you an idea of the results you might get. In each case, the IP addresses were located in the appropriate country and very close to the actual physical location within the country. If the locations had been in countries for which the Google Maps provides greater resolution, that would have been even better.



This tool allows you to plot multiple IP Addresses on the map Leave comments here

Hostnames or IP Addresses seperated by comma's:

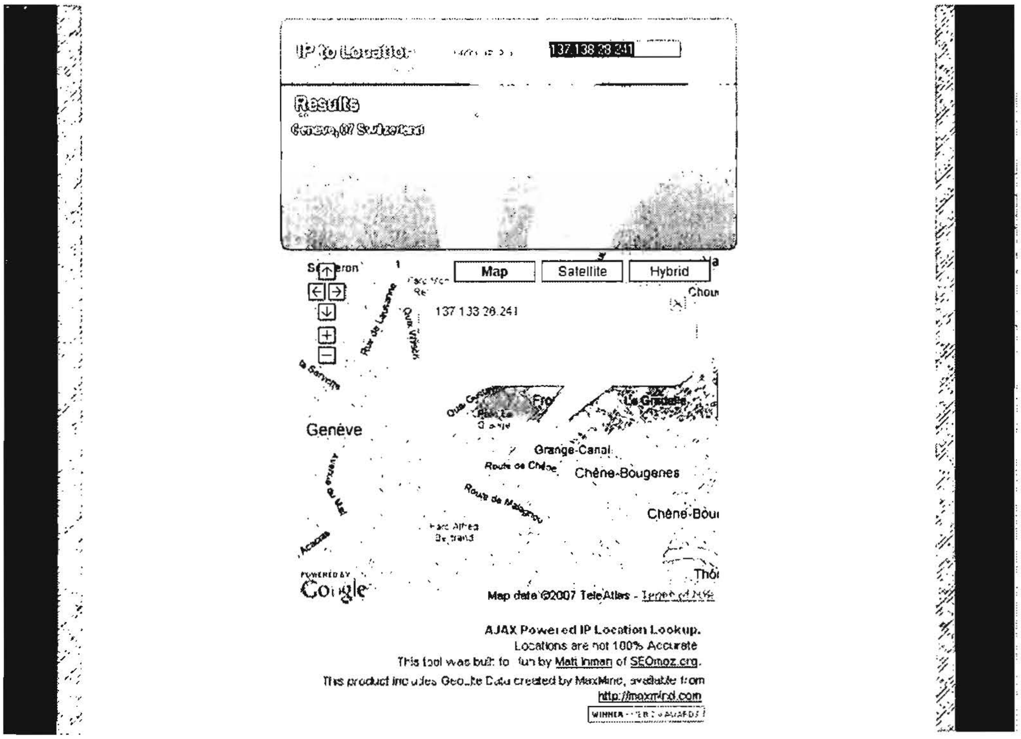
213.176.21.22,193.193.242.160,139.179.10.16

IP2Location http://www.location.com.my/free.asp

This is a very good tool, but unfortunately, users are limited to 20 free lookups per day. However, the next two sites discussed below use this same data and the searches do not appear to be cumulative, in one case, and do not appear to be limited in the other. The results offer the country, city, region, flag, and associated ISP. IP2Location gathers geolocation of IP data using its own proprietary means and claims 95% accuracy, but I can't find any independent verification of this assertion. The company is based in Malaysia.

AJAX Powered IP to Location http://www.seomoz.org/ip2loc/ip2loc.php

SEOmoz.org has a nice little tool based on MaxMind's Geolite Data that maps IP addresses to Google maps. While users must consider that the geolocations are not entirely accurate, compare this tool with the GeoTool above for the same address, and you will see that the SEOmoz application is much more detailed. The street address information below is culled from the RIPE Whois database.



IP to Location 137.138.28.241

Results

Geneva, 07 Switzerland

AJAX Powered IP Location Lookup.
Locations are not 100% Accurate
This tool was built for fun by Matt Inman of SEOmoz.org.
This product includes GeoLite Data created by MaxMind, available from http://maxmind.com

WebHosting.Info http://ip-to-country.webhosting.info/node/view/36

WebHosting.Info only resolves IP addresses to a country, but it appears to do so pretty well. I think the website says it best: "Although not 100% accurate, the IP-to-Country Database is about 98% accurate on country recognition. The main reasons for this lie in the existence of dynamic IP addresses and Internet access through proxy servers. Also, it should be noted that the IP-to-Country Database seeks to indicate the country where resources were first allocated or assigned and are not an authoritative statement of the location in which any specific resource may currently be in use. These cases are very difficult and sometimes impossible to map. However at this moment the IP-to-Country Database is by far the most accurate way to determine the location of Internet users in real-time." *[emphasis added]* Ignore the username/password boxes and look for the demo query box on the right-hand side of the page.

GeoIP Country Lookup http://www.maxmind.com/app/lookup

GeoIP City Lookup http://www.maxmind.com/app/lookup_city

GeoIP by Maxmind is a product that can be purchased; however, the Maxmind website does offer two free demonstration options, one for country lookup and one for city lookup. The country lookup is limited to 100 queries per month while the city lookup is limited to 25 lookups per day (presumably per visitor's IP address). GeoIP claims to "use a number of Internet mapping tools to identify and correct IP addresses where the end-user location does not match the ISP location on the Whois record," but they do not go into detail about exactly how they do this. They do claim they are 95 percent accurate in geolocating IP addresses.

NetGeo http://www.caida.org/tools/utilities/netgeo/

NetGeo, from the Cooperative Association for Internet Data Analysis (CAIDA), takes a completely different approach and one, frankly, that is less reliable. NetGeo correlates both IP address and Autonomous System (AS) numbers to the three major Whois databases at ARIN, APNIC, and RIPE and returns latitude/longitude data for the city, state (or province, district, etc.), and country from the text of the Whois record. The problem is, of course, that there is no guarantee that the physical location of the server is the same as the physical location registered in the Whois database. The site warns users it has not been updated and may give "wildly inaccurate" results. I believe them.

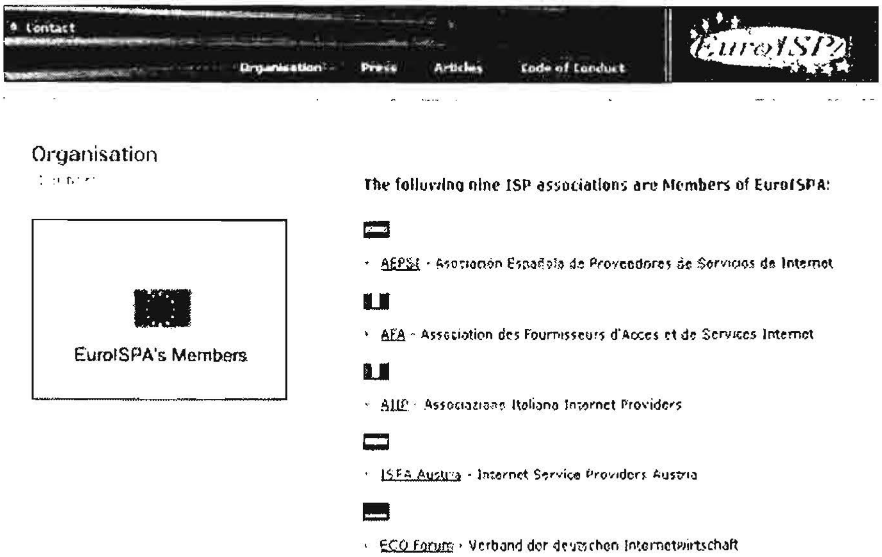
Finding ISPs & Internet Access Points

Thanks to the expansion of the Internet, it has become relatively easy to track down ISPs (Internet Service Providers) and/or Internet access points (IAPs) for any country with public Internet access. The first thing you need to understand is that ***there is no such thing as a complete list of ISPs anywhere***. Furthermore, even a cursory look at websites providing lists of ISPs are either heavily weighted toward or entirely about US ISPs. How do you go about finding ISPs in the rest of the world?

The best information about non-US ISPs, not surprisingly, requires payment, sometimes big payment. I highly recommend you check with your organization's library or other reference resource to see what premium (fee for service) resources they offer. For example, **TeleGeography's Global Internet Geography** is probably the single best source of information on ISPs around the world, but it is far from cheap. Registered users can view free samples of the report, but to view the complete provider list, read the detailed profiles on many of the providers, and see the myriad country profiles, you must have access to the complete report.

Global Internet Geography from TeleGeography
http://www.telegeography.com/products/gig/index.php

One good way to find freely available information about non-US ISPs is to look at organizations or associations, such as the European ISP Association. This page provides links to its members' sites in individual European countries, from which you can quickly dig down and find ISPs that are in turn members of that country's association.



Organisation

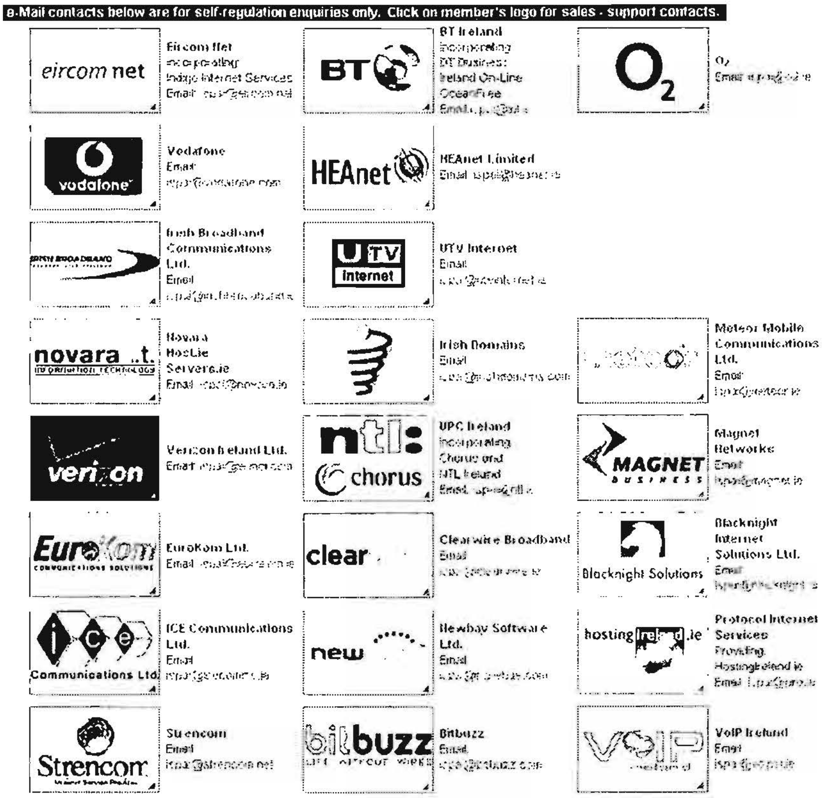
EuroISPA's Members

The following nine ISP associations are Members of EuroISPA:

- AEPSI - Asociación Española de Proveedores de Servicios de Internet
- AFA - Association des Fournisseurs d'Acces et de Services Internet
- AIIP - Associazione Italiana Internet Providers
- ISPA Austria - Internet Service Providers Austria
- ECO Forum - Verband der deutschen Internetwirtschaft

EuroISPA's Members http://www.euroispa.org/32.htm

Here are the members of the ISP Association of Ireland



e-Mail contacts below are for self-regulation enquiries only. Click on member's logo for sales - support contacts.

Eircom Net incorporating Indigo Internet Services Email [illegible]

BT Ireland incorporating BT Business: Ireland On-Line OceanFree Email [illegible]

O2 Email [illegible]

Vodafone Email [illegible]

HEAnet Limited Email [illegible]

Irish Broadband Communications Ltd. Email [illegible]

UTV Internet Email [illegible]

Novara HostIe Servers.ie Email [illegible]

Irish Domains Email [illegible]

Meteor Mobile Communications Ltd. Email [illegible]

Verizon Ireland Ltd. Email [illegible]

UPC Ireland incorporating Chorus and NTL Ireland Email [illegible]

Magnet Networks Email [illegible]

EuroKom Ltd. Email [illegible]

Clearwire Broadband Email [illegible]

Blacknight Internet Solutions Ltd. Email [illegible]

ICE Communications Ltd. Email [illegible]

Newbay Software Ltd. Email [illegible]

Protocol Internet Services Providing HostingIreland.ie Email [illegible]

Strencom Email ispa@strencom.net

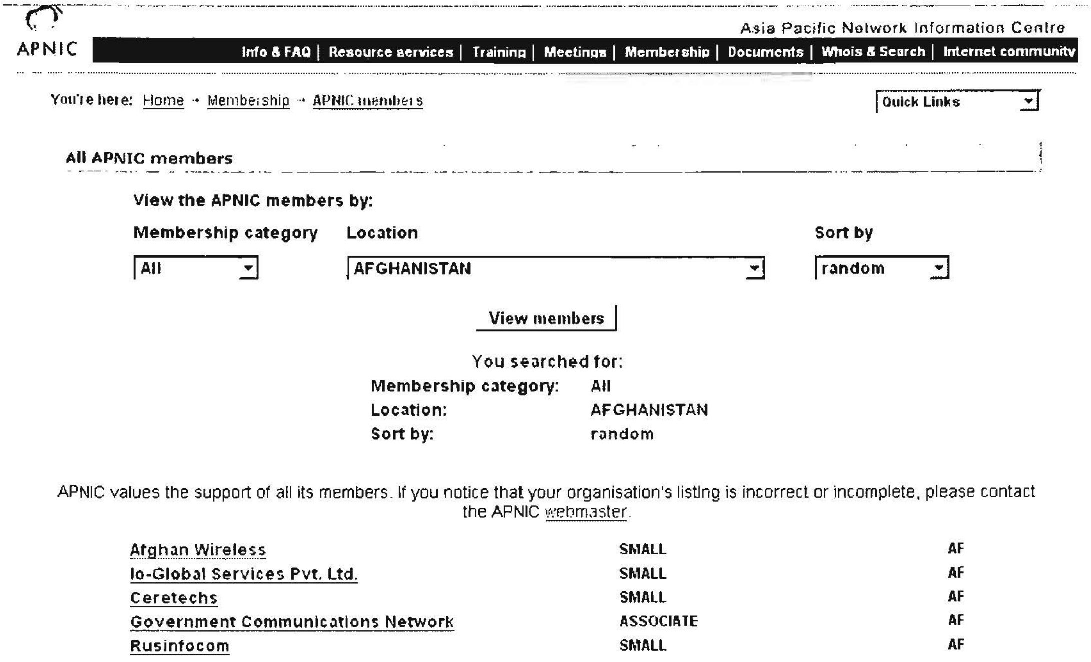
Bitbuzz Email ispa@bitbuzz.com

VoIP Ireland Email [illegible]

Other international organizations and associations that list members in their country or region include the following. Keep in mind that **Local Internet Registries** referred to at some of these sites are usually local ISPs.

Asia Pacific Network Information Center (APNIC) Membership List
http://www.apnic.net/member/current-members.html

This is an excellent way to find ISPs in the Asian Pacific region. The list is searchable by country. Below is a snapshot of the ISPs in Afghanistan that are members of APNIC.


APNIC
Asia Pacific Network Information Centre
Info & FAQ | Resource services | Training | Meetings | Membership | Documents | Whois & Search | Internet community
You're here: Home → Membership → APNIC members
Quick Links
View members

All APNIC members

View the APNIC members by:

Membership category: All

Location: AFGHANISTAN

Sort by: random

You searched for:

Membership category:	All
Location:	AFGHANISTAN
Sort by:	random

APNIC values the support of all its members. If you notice that your organisation's listing is incorrect or incomplete, please contact the APNIC webmaster.

Afghan Wireless	SMALL	AF
Io-Global Services Pvt. Ltd.	SMALL	AF
Ceretechs	SMALL	AF
Government Communications Network	ASSOCIATE	AF
Rusinfocom	SMALL	AF

RIPE NCC's Membership List (covers Europe, North Africa, and the Middle East; listed by country code) http://www.ripe.net/membership/indices/

The Internet Service Providers' Association of South Africa
http://www.ispa.org.za/about/memberlist.shtml

Africa Top Level Domains (AFTLD) Members
http://www.aftld.org/html/english/AFTLD_members.html

Internet Service Providers' Association of Nigeria http://www.ispan.org.ng/

Telecommunication Service Provider Association of Kenya (TESPOK): Kenyan ISPs
http://www.tespok.co.ke/ispa.html

Association of African Internet Service Provider Associations
http://www.afrispa.org/founding.htm

The Internet Service Providers' Association of India http://www.ispai.in/
Members are shown in a scroll near the top right of the home page.

The Internet Service Providers' Association of Bangladesh
http://www.ispabd.org/content.php?content.17

Internet Service Providers' Association of Nepal
http://www.ispan.net.np/memlist.php

The Hong Kong Internet Service Providers Association
http://www.hkispa.org.hk/memberlist.htm

Association de Fournisseurs d'Accès et de Services Internet (France)
http://www.afa-france.com/membres.html

Slovene Internet Service Provider Association
http://www.sispa.org/seznam_clani.htm

Nominet UK Internet Names Organization Members
http://www.nominet.org.uk/governance/members/list/

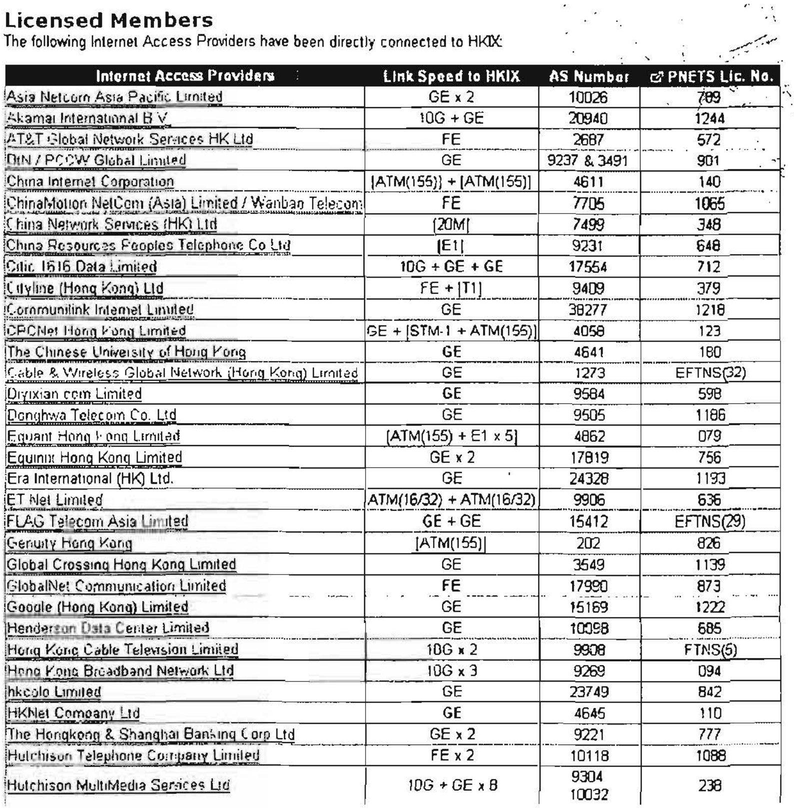
Network Access Points (or Internet Exchanges aka IXs) are also superb sources of information about local ISPs. NAPs or IXs are the junctions where Internet traffic is handed off among different Internet providers and networks. Think of them as performing the same function as airport hubs or highway cloverleaves, where travelers change from one airline or highway to another. Finding IXs is relatively easy because there are a couple of sites that provide links to virtually all the exchanges around the world. The two best free (non-registration) sites are Colosource's Internet Exchange Points and Exchange Points Around the World. If you are able to register at websites, TeleGeography's Internet Exchange Points Directory is free only to registered users.

Telegeography's Internet Exchange Points Directory [Registration Required]
http://www.telegeography.com/products/ix/index.php

Colosource's Internet Exchange Points http://www.colosource.com/ix.asp

Exchange Points Around the World http://www.ep.net/ep-main.html

It is a simple matter to use an IX directory or list to find ISPs. If I am interested in Hong Kong, from Colosource's home page, I scroll down to Asia Internet eXchanges and click on China The Hong Kong Internet eXchange (HKIX), which brings up a page with a link to "connected IAPs":



Licensed Members

The following Internet Access Providers have been directly connected to HKIX:

Internet Access Providers	Link Speed to HKIX	AS Number	PNETS Lic. No.
Asia Netcom Asia Pacific Limited	GE x 2	10026	789
Akamai International B.V.	10G + GE	20940	1244
AT&T Global Network Services HK Ltd	FE	2687	572
BtN / PCCW Global Limited	GE	9237 & 3491	901
China Internet Corporation	[ATM(155)] + [ATM(155)]	4611	140
ChinaMotion NetCom (Asia) Limited / Wanbao Telecom	FE	7705	1065
China Network Services (HK) Ltd	[20M]	7499	348
China Resources Peoples Telephone Co Ltd	[E1]	9231	648
Citic 1616 Data Limited	10G + GE + GE	17554	712
Cityline (Hong Kong) Ltd	FE + [T1]	9409	379
Communilink Internet Limited	GE	38277	1218
CPCNet Hong Kong Limited	GE + [STM-1 + ATM(155)]	4058	123
The Chinese University of Hong Kong	GE	4641	180
Cable & Wireless Global Network (Hong Kong) Limited	GE	1273	EFTNS(32)
Diyixian.com Limited	GE	9584	598
Donghwa Telecom Co. Ltd	GE	9505	1186
Equant Hong Kong Limited	[ATM(155) + E1 x 5]	4862	079
Equinix Hong Kong Limited	GE x 2	17819	756
Era International (HK) Ltd.	GE	24328	1193
ET Net Limited	ATM(16/32) + ATM(16/32)	9906	636
FLAG Telecom Asia Limited	GE + GE	15412	EFTNS(29)
Genuity Hong Kong	[ATM(155)]	202	826
Global Crossing Hong Kong Limited	GE	3549	1139
GlobalNet Communication Limited	FE	17990	873
Google (Hong Kong) Limited	GE	15169	1222
Henderson Data Center Limited	GE	10098	685
Hong Kong Cable Television Limited	10G x 2	9908	FTNS(5)
Hong Kong Broadband Network Ltd	10G x 3	9269	094
hkcolo Limited	GE	23749	842
HKNet Company Ltd	GE	4645	110
The Hongkong & Shanghai Banking Corp Ltd	GE x 2	9221	777
Hutchison Telephone Company Limited	FE x 2	10118	1088
Hutchison MultiMedia Services Ltd	10G + GE x 8	9304 10032	238

The following sites list and link to ISPs around the world, but remember that none of these sites has a complete list of all ISPs everywhere. You will need to look at some or all of these lists, as well as try country-specific resources, if you are want to find a thorough list of ISPs in a particular country. The best list of ISPs is called, not surprisingly, "The List," a site that has been around for years. Click on the highlighted country code for the best list of ISPs in most countries around the world. Other resources vary in quality depending on the country you're researching, so you will probably need to look at all of these sites.

The List http://thelist.internet.com/countrycode.html

NSRC's Connectivity Providers Database http://www.nsrc.org/networkstatus.html

Some of the information at the Network Startup Resource Center is out of date while some has recently been updated; however, the links should help you locate the major ISPs in almost any country.

International Internet Access Providers
http://www.herbison.com/herbison/iap_international_meta_list.html

Herbison's International Internet Access Providers website was last updated in April 2006. While some of the links are out of date, there is so much information at this site it is still useful.

FreedomList http://www.freedomlist.com/find.php3

Free and cheap ISPs by country; fairly well up to date.

African Internet Connectivity

Last updated 2002. http://www3.sn.apc.org/africa/af-isps.htm

Middle East Directory List of ISPs

Good resource for 16 Middle Eastern countries; some links are out of date.
http://www.middleeastdirectory.com/me-isps.htm

Major directories can be good sources for ISPs around the world, though they are only starting points and none has a really thorough list of ISPs.

Google Directory

http://directory.google.com/Top/Computers/Internet/Access_Providers/

Yahoo Directory http://dir.yahoo.com/

There are several ways to use Yahoo to find international ISPs. The best is: Business_and_Economy/Business_to_Business/Communications_and_Networking/Internet_and_World_Wide_Web/Network_Service_Providers/Internet_Service_Providers__ISPs_/
This lists ISPs for most countries and all world regions. Also, look at each individual Region and Country to see if Yahoo lists ISPs for that area or country.

Because of the lack of terrestrial broadband capacity in many locations, there is an increasing demand for broadband services via satellite in many parts of the world. These sites will help you locate satellite Internet providers.

Satellite Internet Service Providers for North & South America, Europe, Africa, Asia, Middle East http://www.satsig.net/

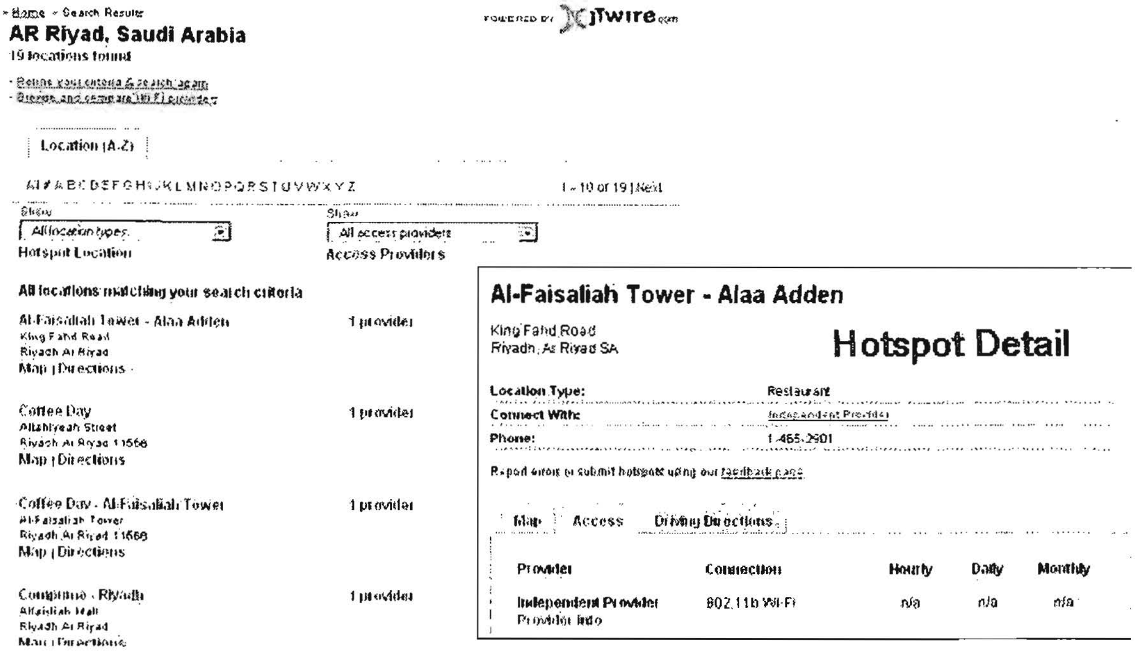
Linksat Satellite and Internet Providers (covers most of the globe)
http://www.linksat.com/

Satellite Industry Links: Satellite Service Providers (includes but is not limited to Internet service) http://www.satellite-links.co.uk/links/ssp.html

Wireless Internet access points (usually called **hotspots**) have become extremely important in recent years. Many sites have appeared to help people locate these hotspots anywhere in the world. Intel's Mobile Technology Hotspot Finder is among the best of these sites. You can search for hotspots by address, city, state, country/region, distance, business or hotspot name; location type (e.g., an airport); by service provider; or by whether they are free or commercial hotspots, or both. You can also browse hotspots by country. The number of hotspots is listed next to each country's name.

Intel's Mobile Technology Hotspot Finder

http://intel.jiwire.com/


» Home » Search Results

POWERED BY JiWire.com

AR Riyad, Saudi Arabia

19 locations found

- Refine your criteria & search again
- Browse and compare WiFi providers

Location (A-Z)

All # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

1 - 10 of 19 | Next

Show: All location types — Hotspot Location

Show: All access providers — Access Providers

All locations matching your search criteria

Al-Faisaliah Tower - Alaa Adden King Fahd Road Riyadh Ar Riyad Map | Directions	1 provider
Coffee Day Alfahliyeah Street Riyadh Ar Riyad 11566 Map | Directions	1 provider
Coffee Day - Al-Faisaliah Tower Al-Faisaliah Tower Riyadh Ar Riyad 11566 Map | Directions	1 provider
Compumo - Riyadh Alfaisliah Mall Riyadh Ar Riyad Map | Directions	1 provider

Al-Faisaliah Tower - Alaa Adden

King Fahd Road
Riyadh, Ar Riyad SA

Hotspot Detail

Location Type:	Restaurant
Connect With:	Independent Provider
Phone:	1-465-2901

Report errors or submit hotspots using our feedback page

Map | Access | Driving Directions

Provider	Connection	Hourly	Daily	Monthly
Independent Provider Provider Info	802.11b Wi-Fi	n/a	n/a	n/a

IPass's Hotspot Finder lets users look for dial-up, ISDN, PHS access points and Ethernet or Wi-Fi Internet access points in any country. For example, it found 72 hotspots in Hokkaido, Japan. Other hotspot finder websites include the following:

iPass Hotspot Finder	http://ipass.jiwire.com/
Wi-Fi Hotspot List	http://www.wi-fihotspotlist.com/
Hotspothaven	http://www.hotspothaven.com/
JiWire Global WiFi Hotspot Finder	http://www.jiwire.com/search-hotspot-locations.htm
WiFinder	http://www.wifinder.com/
WiFi411	http://www.wifi411.com/

Finally, cybercafes remain extremely popular Internet access points in many countries where it may be too expensive to have either a personal computer or an Internet connection in one's home. But they have also become popular with travelers who don't want to lug around a laptop (which is all too easy to steal). More and more people are relying on their neighborhood cybercafes as a cheap, fast, easy way to exchange email and browse the web without the inconvenience of having to carry around a laptop. There are many guides and search engines for finding cybercafes around the world, but do keep in mind that cybercafes come and go very quickly, especially in certain countries. China, for example, closed 8600 unlicensed cybercafes in 2004.

Netcafe Guide http://www.world66.com/netcafeguide

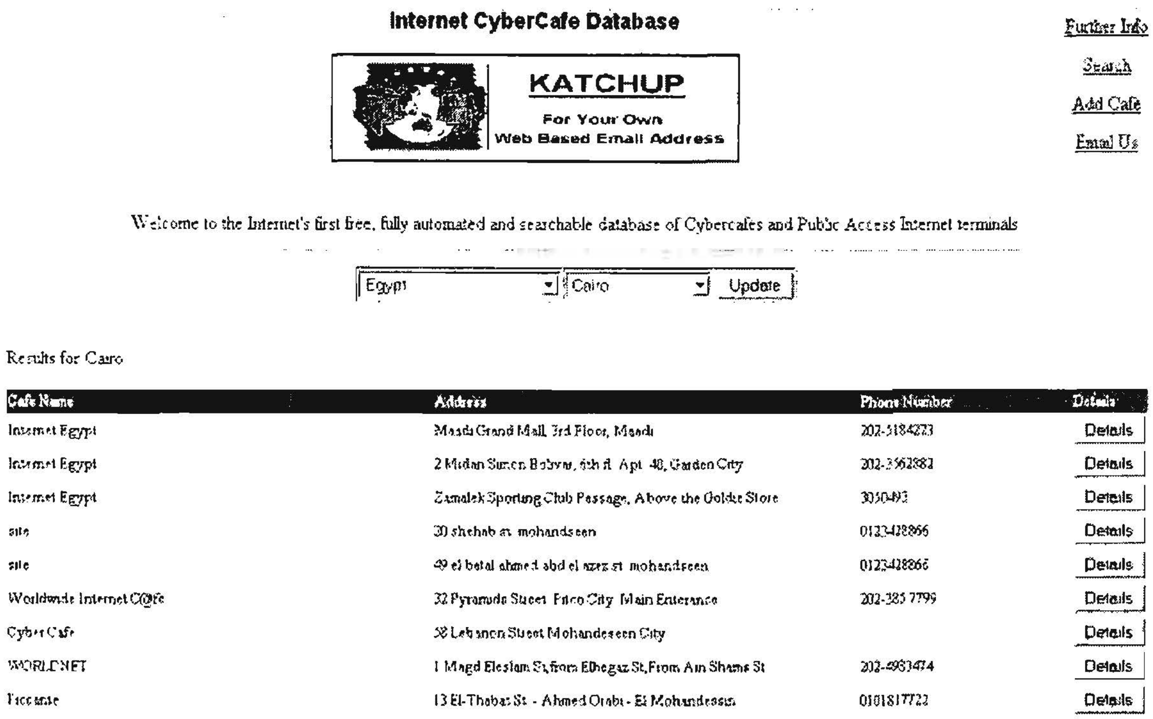
Google Directory: Cybercafes
http://directory.google.com/Top/Computers/Internet/Cybercafes/

Cybercaptive Search Engine http://cybercaptive.com/
The country search has been disabled; search by city

Indra's International Cybercafes
http://www.indranet.com/potpourri/links/cybercafeint.html

Curious Cat's Cybercafe Connections
http://www.curiouscat.com/travel/cybercafe.cfm

Internet Cybercafe Database http://cybercafe.katchup.co.nz/search.asp
A database searchable by country and city that provides results in an easy to read format.



Welcome to the Internet's first free, fully automated and searchable database of Cybercafes and Public Access Internet terminals

Egypt | Cairo

Results for Cairo

Cafe Name	Address	Phone Number	Details
Internet Egypt	Maadi Grand Mall, 3rd Floor, Maadi	202-5184273	Details
Internet Egypt	2 Midan Simon Bolivar, 6th fl. Apt. 48, Garden City	202-3562883	Details
Internet Egypt	Zamalek Sporting Club Passage, Above the Golder Store	3050493	Details
site	30 shehab st. mohandseen	0123428866	Details
site	49 el batal ahmed abd el azez st. mohandseen	0123428866	Details
Worldwide Internet C@fe	32 Pyramids Street Frico City Main Enterance	202-385 7799	Details
Cyber Cafe	58 Lebanon Street Mohandeseen City		Details
WORLDNET	1 Magd Eleslam St,from Elhegaz St,From Ain Shams St	202-4983474	Details
Ficcante	13 El-Thabat St. - Ahmed Orabi - El Mohandessin	0101817722	Details

In short, there are many resources available to help users find Internet access points and sources of all types, although there is no single resource that will do it all for you. And some types of Internet access, especially cybercafes, change so rapidly that it is especially difficult to keep up with the latest information on their locations, requiring users to refresh that data frequently.

Cybergeography, Topology, and Infrastructure

The Internet has created many new ways of seeing, understanding, and knowing the world. It has also created, in a sense, a new world unto itself, a world with its own "geography," which has come to be known as cybergeography: the configuration of the constituent parts of the Internet. The most original and informative of the websites devoted to mapping this new landscape used to be **Cybergeography**, which contains, among other things, cybermaps of many flavors: topology, census, conceptual, historical, etc. Some of these maps are very imaginative and some even display an eerie beauty. However, the site has not been updated since 2004, so it is becoming an archive instead of a library of new information.

Cybergeography Research http://www.cybergeography.org/

For a different view of the Internet, check out the **Internet Traffic Report.** "The Internet Traffic Report monitors the flow of data around the world. It then displays a value between zero and 100. Higher values indicate faster and more reliable connections." The Traffic Report uses "ping" to measure round-trip travel time along major paths on the Internet. It also measures response time, i.e., how long it takes for a piece of data to travel from point A to point B and back (round trip). The Traffic Report also provides data on packet loss, which indicates how reliable the connection is. All this data is available for major routers around the world and displayed graphically.

Internet Traffic Report http://www.internettrafficreport.com/main.htm

Yet another way of visualizing and thereby understanding the Internet is by looking at an **Internet Exchange (IX)** or **Network Access Points (NAPs)**. An IX is where networks and service providers hand off traffic to each other; they function as "hubs" for Internet traffic in very much the way certain airports serve as "switching points" for passengers. And, like airport hubs, they are very crowded, busy places. There are IXs around the world, though obviously many more in congested areas such as the US and Europe. In fact, many countries and even some regions do not have their own IXs, which means they must use exchanges in Europe, Asia, or even the US to route traffic between countries or even within one country, which leads to some very interesting routing patterns.

Internet Exchanges all have websites, and each provides a varying amount of data. The two best free metasites with links to most of the world's IXs are Exchange Point Information and Colosource:

Colosource Internet eXchange Points	http://www.colosource.com/ix.asp
Exchange Point Information	http://www.ep.net/ep-main.html

Internet Exchanges are invaluable sources of information about how major networks are connected to each other all over the world. Often IX websites will include information about **peering arrangements**. Peering is the "arrangement of traffic exchange between Internet service providers (ISPs). Larger ISPs with their own backbone networks agree to allow traffic from other large ISPs in exchange for traffic on their backbones. They also exchange traffic with smaller ISPs so that they can reach regional end points. Essentially, this is how a number of individual network owners put the Internet together."[159]

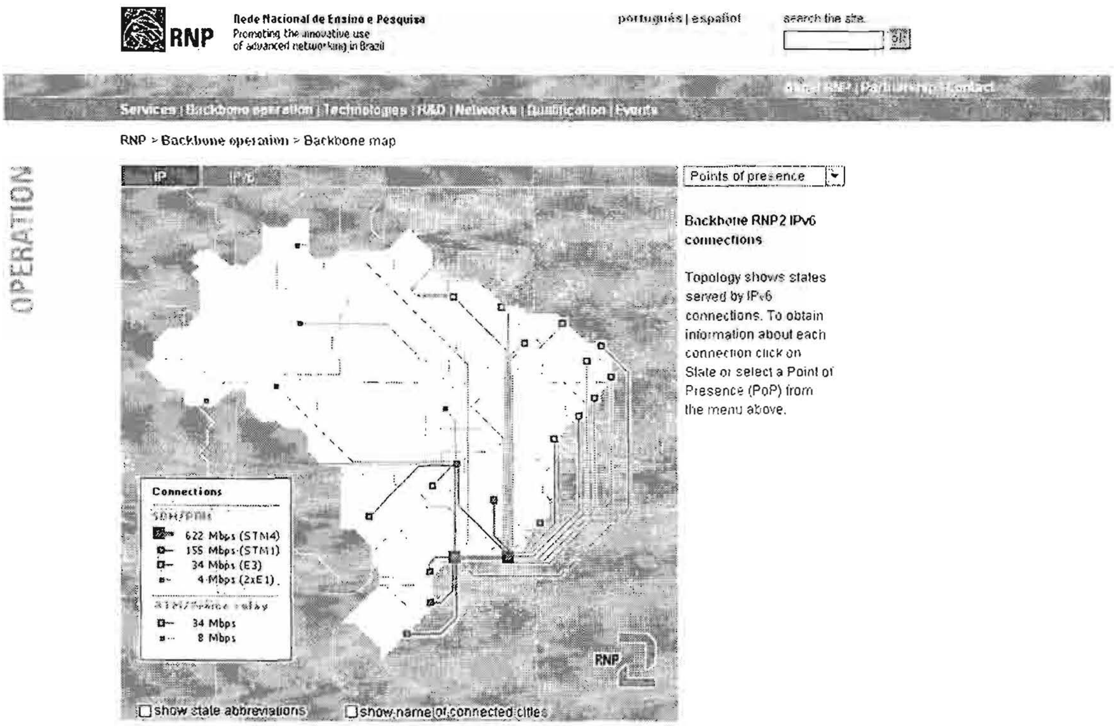
In addition to IXs, **Internet backbones**, which are central networks that connect other networks together, are high-interest segments of the Internet. Some of the best known are Worldcom/UUNET, Qwest and KPNQwest in Europe, Genuity, Sprint, AT&T, Cable & Wireless, Savvis, GlobalOne, BELNET, Telia, and Teleglobe.

Internet Backbone Networks	http://www.geog.ucl.ac.uk/casa/martin/atlas/isp_maps.html
Russ Haynal's Major Internet Backbones	http://www.navigators.com/isp.html
Boardwatch's Internet Backbone Maps	http://www.nthelp.com/maps.htm
BWM's Links to Network Maps	http://www.bandwidthmarket.com/component/option,com_weblinks/catid,74/Itemid,4/
BT Infonet's Network Maps	http://www.bt.infonet.com/services/internet/network_maps.asp

What do backbone maps typically look like? Here is the Ipv6 backbone map for the National Education and Research Network (Rede Nacional de Ensino e Pesquisa – RNP), "the Brazilian infrastructure of advanced network for collaboration and communication in the fields of teaching and research."[160] The interactive web page not only displays the topology seen here, but also includes links with details about the connectivity.

[159] "Peering," Whatis.com, <http://whatis.techtarget.com/> (14 November 2006).

[160] RNP Backbone Map, < http://www.rnp.br/en/backbone/index.php> (14 November 2006).


RNP
Rede Nacional de Ensino e Pesquisa
Promoting the innovative use of advanced networking in Brazil
português | español
search the site
ok
About RNP | Partnership | Contact
Services | Backbone operation | Technologies | R&D | Networks | Qualification | Events
RNP > Backbone operation > Backbone map
OPERATION
IP
IPv6
Points of presence
Connections
SDH/PDH
622 Mbps (STM4)
155 Mbps (STM1)
34 Mbps (E3)
4 Mbps (2xE1)
ATM/Frame relay
34 Mbps
8 Mbps
RNP 2
□ show state abbreviations
□ show name of connected cities

Backbone RNP2 IPv6 connections

Topology shows states served by IPv6 connections. To obtain information about each connection click on State or select a Point of Presence (PoP) from the menu above.

Another effort to visualize the topology of the Internet is **Mapnet**, maintained by the Cooperative Association for Internet Data Analysis (CAIDA). Their color map, which runs as a web-based Java applet, allows you to view major providers simultaneously and also to zoom into a specific world region.

Mapnet	http://www.caida.org/tools/visualization/mapnet/

Internet Privacy and Security—Making Yourself Less Vulnerable in a Dangerous World

The problems with Internet privacy and security are getting steadily worse, not better, each year as technology to collect information surreptitiously and attack computers at will steadily improves and proliferates. To make matters worse, malicious attacks are not the only or even the most common ways personal data is gathered, stored, and used. Businesses routinely collect information and, in some cases, share it without users' knowledge or consent. By now most Internet users know they are inadvertently giving out information about themselves every time they navigate the Internet. However, it is almost impossible for anyone to have a clear idea exactly what information is being unwittingly provided.

Part of the problem stems from one of the seemingly inviolable rules of progress that applies doubly so to the Internet:

More Convenience = Less Privacy

Major computer companies have recognized this trade-off for years, though rarely will they openly discuss it. In an unusual instance of candor, a Microsoft executive admitted that one of the features in Internet Explorer is a good example of this axiom. Speaking of *userdata persistence* (more on what this is later), Michael Wallent said, "this feature has a trade-off, ***like almost every other feature on the web***—in this case, between functionality and a ***minor***, potential privacy exposure."[161] [emphasis added]

[161] Paul Festa, "IE Feature Can Track Web Surfers Without Warning," *CNET News*, 11 September 2000, <http://news.cnet.com/news/0-1005-200-2751843.html> (14 November 2006).

> **"You have zero privacy anyway. Get over it."**
>
> Scott MacNealy, CEO, Sun Microsystems

Scott MacNealy's now-infamous quote,[162]—"You have zero privacy anyway. Get over it."—may no longer be an overstatement. At the very least, it should serve as a warning to Internet users to be wary of all products and services, but especially new ones that promise to do things faster, better, easier, and cheaper. There is almost always a hidden cost, often in weakened security and compromised privacy.

The costs, however, are not always so "hidden." Many are affecting the bottom line and the budgets of businesses and governments. "***Dealing with viruses, spyware, PC theft and other computer-related crimes costs U.S. businesses a staggering $67.2 billion a year***, according to the FBI. The FBI calculated the price tag by extrapolating results from a survey of 2,066 organizations. The survey...found that 1,324 respondents, or 64 percent, suffered a financial loss from computer security incidents over a 12-month period."[163] Furthermore, as both professionals and individuals become more security savvy, the ***threats become more insidious and therefore harder to detect and protect against***. The "2007 Internet Threat Outlook," a report by software maker CA, predicted that "malware brokers will continue to piece together threats such as Trojan horse viruses, worms and the many forms of spyware to hide their attacks and evade technological defenses employed by both enterprises and consumers. With the level of professionalism rising quickly among the most sophisticated virus distributors, CA predicts that zero-day exploits, drive-by malware downloads and extremely intricate phishing schemes will continue to become more dangerous and harder to detect."[164]

Especially worrisome is the proliferation of bots, the shortened version of 'robot,' which simply refers to any software designed to dig through data. For example, search engines use spider bots to crawl webpages to index them; there are shopping bots that look for the best prices for consumers; bots are at the heart of data mining, the process of finding patterns in enormous amounts of data. But "bad bots" create a virus-like infection under the remote control of a distant computer, network, or individual. This new threat exploits vulnerabilities in security subsystems

[162] Polly Sprenger, "Sun on Privacy: Get Over It," Wired, 26 January 1999, <http://www.wired.com/news/politics/0,1283,17538,00.html > (14 November 2006).

[163] Joris Evers, "Computer crime costs $67 billion, FBI says," CNET News.com, 19 January 2006, <http://news.com.com/2102-7349_3-6028946.html?tag=st.util.print> (30 January 2007).

[164] Matt Hines, "CA Predicts More Attacks on Experienced Users," eWeek via Yahoo News, 25 January 2007, <http://news.yahoo.com/s/zd/20070125/tc_zd/199597> (31 January 2007).

and often exploits normally unused ports and channels, permitting the bots to move about on the net unnoticed and undetected. There are now thousands of these bad bots (no one really knows how many) trolling the Internet connected to what is known as a "**botnet,**" a kind of underground network of malicious activity. A 2004 study concluded that "two years ago only 200 bot-virus variations existed; today [in 2004] there are about 4,000, according to F-Secure Corp."[165] The security situation is rapidly deteriorating. "David Dagon, a Georgia Institute of Technology researcher who is a co-founder of Damballa, a start-up company focusing on controlling botnets, said the consensus among scientists is that botnet programs are present on about 11 percent of the more than 650 million computers attached to the Internet."[166] None of this is new; botnets have been around for a long time. "What is new is the vastly escalating scale of the problem—and the precision with which some of the programs can scan computers for specific information, like corporate and personal data, to drain money from online bank accounts and stock brokerages."[167]

Security experts believe most spam—in fact more than 80 percent—is now sent by bots.[168] Spam is more than a nuisance. It is the most pervasive and pernicious medium for spreading all sorts of malicious software (malware). To make matters worse, simply using a preview window in an email application may be sufficient to activate scripts sent by spammers, which means many users are unwittingly contributing to the spread of spam and malware. "According to a study by network management firm Sandvine...Trojans and worms with backdoor components such as Migmaf and SoBig have turned infected Windows PCs into drones in vast networks of compromised zombie PCs. Sandvine reckons junk mails created and routed by 'spam Trojans' are clogging ISP mail servers, forcing unplanned network upgrades and stoking antagonism between large and small ISPs."[169] With more and more ISPs pulling the plug on spammers as complaints flood in, spammers are turning to these backdoor means of spreading spam because they are much more efficient, much harder to detect, and much more difficult to stop. "Making things even tougher for IT security administrators in 2007 is the fact that an increasing amount of spam will be image-based, which is more difficult to detect...image-based spam

[165] Cassell Bryan-Low, "Virus for Hire: Growing Number of Hackers Attack Web Sites for Cash," *The Wall Street Journal*, pp. A1 & A8, 30 November 2004.

[166] John Markoff, "Attack of the Zombie Computers Is Growing Threat," *The New York Times*, (registration required) 7 January 2007, <http://www.nytimes.com/2007/01/07/technology/07net.html> (16 January 2007).

[167] Markoff.

[168] Markoff.

[169] John Leyden, "Zombie PCs Spew Out 80% of Spam," The Register, 4 June 2004, <http://www.theregister.co.uk/2004/06/04/trojan_spam_study/> (14 November 2006).

accounted for more than 40% of all spam messages generated in the fourth quarter of 2006, compared with less than 5% in the first quarter of 2005."[170]

All it takes is a public willing to open spam email, especially in HTML format, or its (seemingly innocuous) attachments, and there are millions of people still doing this. Spam sent using bots is notoriously difficult to trace because it uses other people's computers to traverse the Internet and, of course, always-on broadband connections only facilitate the movement of bots and spam.

The year 2003 may be remembered in Internet history for reaching one very unfortunate milestone: there were more spam emails than legitimate emails. "In 2003, Brightmail [an anti-spam company] saw spam surpass legitimate email—growing to more than 56% of all Internet email, up from just 40% a year ago."[171] The problem continues to worsen. In 2004, statistics painted a different picture. According to [e-mail security vendor FrontBridge's] figures, spam volume increased two percent, to 87 percent of e-mail, and has continued its growth each month since May of this year [2004]."[172] December 2006 saw a new record: according to one tracking system, ***spam accounted for 94 percent*** of all email that month.[173]

Despite improvements in knowledge and education about computer security risks, too many people still know little or nothing about the vulnerabilities in the tools they use every day, and this ignorance truly is bliss to the bad people wishing to exploit those weaknesses. Therefore, the first essential step in improving your Internet security and privacy is to learn more about basic vulnerabilities, exploits, and ways to protect yourself. Many of the recommendations in this book only need to be implemented one time for the life of a computer. Some, such as keeping basic software up to date, require more diligence. However, all are examples of "good computer hygiene" that will—or should—become second nature over time.

There are new vulnerabilities disclosed literally every week, so this book cannot provide a comprehensive list of problems, flaws, and potential attacks. It can do three things:

✓ Provide general guidance on improving your Internet privacy and security.

[170] Paul McDougall, "Organized Malware Factories Threaten Internet Users, Study Says," Information Week, 30 January 2007, <http://www.informationweek.com/story/showArticle.jhtml?articleID=197001739> (31 January 2007).

[171] "Brightmail Reports on Spam Trends of 2003," Networks Unlimited, 27 February 2004, <http://www.netunlim.co.za/news/news18.htm> (link inactive as of November 2005).

[172] Sean Michael Kerner, "The Deadly Duo: Spam and Viruses." ClickZ Stats, 16 November 2004, <http://www.clickz.com/stats/sectors/email/article.php/3433141> (14 November 2006).

[173] Gregg Keizer, "Spam Sets Record, Accounts For 94% Of E-mail," InformationWeek, 10 January 2007 <http://news.yahoo.com/s/cmp/20070111/tc_cmp/196802782>, 23 January 2007.

- ✓ Describe some known problems and how to cope with them.
- ✓ Point you to some privacy-related sites that have good information about keeping a low profile and preventing malicious attacks.

Ultimately, each individual must be responsible for staying up to date with the latest news about computer vulnerabilities—*you're your own best line of defense*.

Basics for Improving Your Internet Privacy and Security

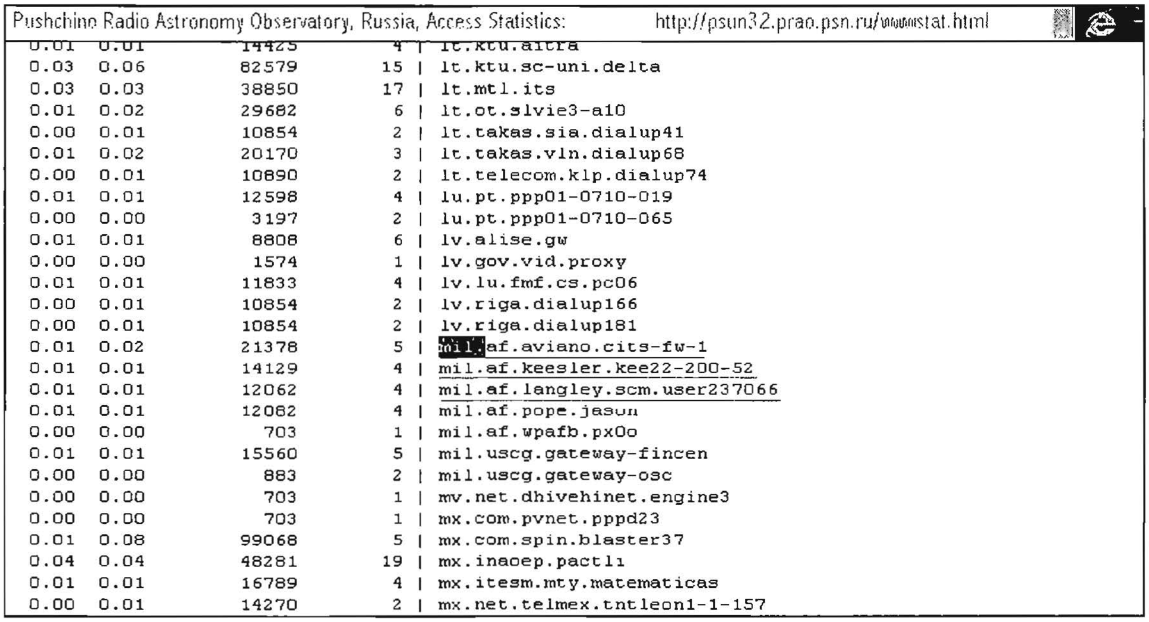
The first thing you should do is check one of the sites that lets you see what information is being unwittingly provided about you as you surf. Go to the following sites to see what is known about you as you browse and, in the case of **Shields Up!**, what can be done to your computer while you're on line. As Steve Gibson, the site's creator, explains, "Without your knowledge or explicit permission, the Windows networking technology which connects your computer to the Internet may be offering some or all of your computer's data to the entire world at this very moment!" At his site, Gibson offers very practical ways to protect yourself and your data.

Shields Up!	http://www.grc.com/
Junkbusters	http://www.junkbusters.com/cgi-bin/privacy
BrowserHawk Browser Analysis	http://www.syscape.com/showbrow.aspx
Browser Spy Browser Analysis	http://gemal.dk/browserspy/
Russ Haynal's Persona Check	http://navigators.com/cgi-bin/navigators/persona.pl
HackerWhacker Free Tools	http://whacker4.hackerwhacker.com/freetools.php especially the Browser Leakage and Quick Scan for open ports
Sygate/Symantec Online Security Services	http://scan.sygate.com/home_homeoffice/sygate/index.jsp Sygate is now owned by Symantec.

There is some, though not much, "***security through obscurity***." If you have dial-up access to the Internet through a commercial ISP, you likely will be assigned a different ("dynamic") IP address every time you log on, which means it is difficult to link you as an individual customer of a particular ISP to any specific IP number registered to that provider. Furthermore, if you use an ISP with a large geographic coverage area, it *may* be difficult to pin down your location. On the other hand, your

ISP may indicate a very specific location—say, Fairfax County, Virginia—so check your profile (how to do this later). However, just because you're using a dial-up connection doesn't mean you can become complacent. Determined malicious hackers use very sophisticated tools, such as one that automatically dials thousands of random phone numbers until it finds another modem connected to the Internet, maybe your computer modem.

The sheer size of the Internet is also an inhibiting factor in what can be tracked by network administrators. For example, take a look at a ***web statistics*** page at the Department of Pulsar Astrometry of the Pushchino Radio Astronomy Observatory in Moscow:



Pushchino Radio Astronomy Observatory, Russia, Access Statistics: http://psun32.prao.psn.ru/wwwstat.html

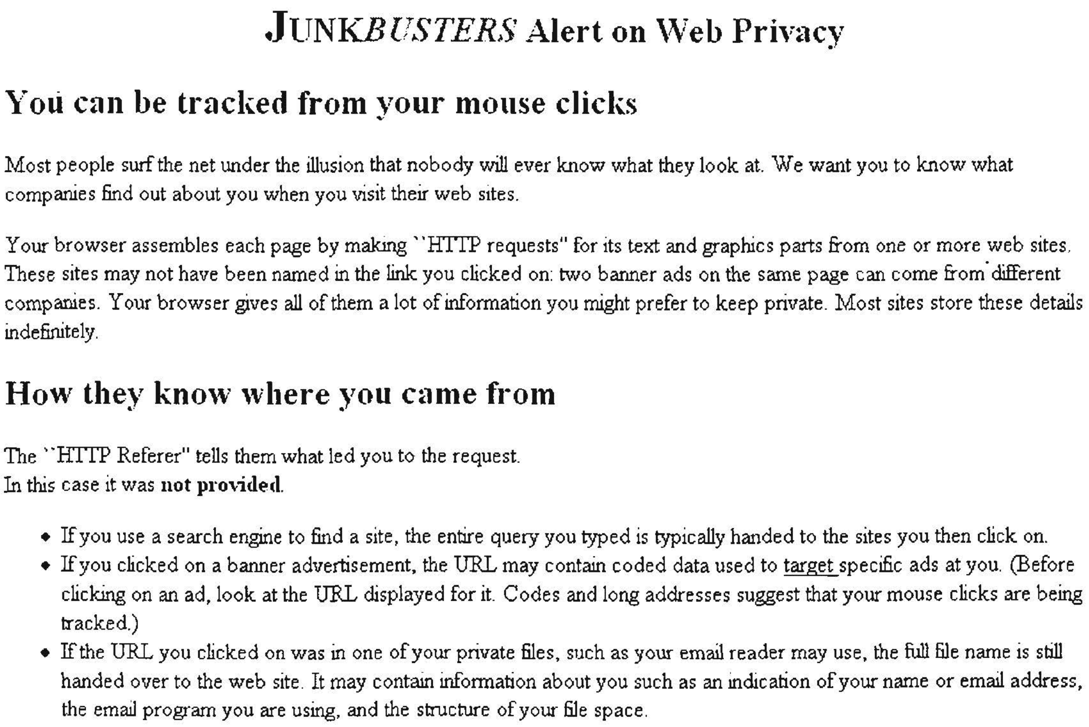
```
 0.01   0.01         14425          4 | lt.ktu.aitra
 0.03   0.06         82579         15 | lt.ktu.sc-uni.delta
 0.03   0.03         38850         17 | lt.mtl.its
 0.01   0.02         29682          6 | lt.ot.slvie3-a10
 0.00   0.01         10854          2 | lt.takas.sia.dialup41
 0.01   0.02         20170          3 | lt.takas.vln.dialup68
 0.00   0.01         10890          2 | lt.telecom.klp.dialup74
 0.01   0.01         12598          4 | lu.pt.ppp01-0710-019
 0.00   0.00          3197          2 | lu.pt.ppp01-0710-065
 0.01   0.01          8808          6 | lv.alise.gw
 0.00   0.00          1574          1 | lv.gov.vid.proxy
 0.01   0.01         11833          4 | lv.lu.fmf.cs.pc06
 0.00   0.01         10854          2 | lv.riga.dialup166
 0.00   0.01         10854          2 | lv.riga.dialup181
 0.01   0.02         21378          5 | mil.af.aviano.cits-fw-1
 0.01   0.01         14129          4 | mil.af.keesler.kee22-200-52
 0.01   0.01         12062          4 | mil.af.langley.scm.user237066
 0.01   0.01         12082          4 | mil.af.pope.jason
 0.00   0.00           703          1 | mil.af.wpafb.px0o
 0.01   0.01         15560          5 | mil.uscg.gateway-fincen
 0.00   0.00           883          2 | mil.uscg.gateway-osc
 0.00   0.00           703          1 | mv.net.dhivehinet.engine3
 0.00   0.00           703          1 | mx.com.pvnet.pppd23
 0.01   0.08         99068          5 | mx.com.spin.blaster37
 0.04   0.04         48281         19 | mx.inaoep.pactli
 0.01   0.01         16789          4 | mx.itesm.mty.matematicas
 0.00   0.01         14270          2 | mx.net.telmex.tntleon1-1-157
```

Network administrators use these statistics to glean general information about where visitors to their website are coming from, peak activity times, and which internal urls are visited most frequently. Of special interest are accesses by client domain. Most accesses at the observatory, not surprisingly, are from other computers at the site, but if you scroll down the list, many international sites, including .edu, .gov and .mil, also appear. While access to servers from commercial US accounts is generally too commonplace to provide much useful information, access from .gov or .mil accounts show up quite prominently on these statistical listings. Also, generally only older or superficial statistics tend to be available to the public; more recent statistics, which tend to be very detailed, usually require a password.

In addition to unscrupulous people trying to get into your computer, a somewhat less threatening but nonetheless worrisome possibility is that a network administrator at the website you are visiting may be able to tell the following about you:

- Who your provider is.
- Where your provider is located.
- What site you last visited.
- If you link to a site from a search engine, the query you ran.
- What browser software you are using.
- Your email address.

On the other hand, you may *not* be giving out all this information. Specifically, you should make sure your browser does not provide the "HTTP_From" or "REMOTE_USER" variables, both of which give away information about your email address and other indications of your identity. Also ensure that the "REMOTE_IDENT" variable is not being disclosed (more than likely, it is not). How do you know if you are providing these variables? Go to the **Junkbusters** site listed above and it will let you know.



JUNK*BUSTERS* Alert on Web Privacy

You can be tracked from your mouse clicks

Most people surf the net under the illusion that nobody will ever know what they look at. We want you to know what companies find out about you when you visit their web sites.

Your browser assembles each page by making ``HTTP requests" for its text and graphics parts from one or more web sites. These sites may not have been named in the link you clicked on: two banner ads on the same page can come from different companies. Your browser gives all of them a lot of information you might prefer to keep private. Most sites store these details indefinitely.

How they know where you came from

The ``HTTP Referer" tells them what led you to the request.
In this case it was **not provided**.

- If you use a search engine to find a site, the entire query you typed is typically handed to the sites you then click on.
- If you clicked on a banner advertisement, the URL may contain coded data used to target specific ads at you. (Before clicking on an ad, look at the URL displayed for it. Codes and long addresses suggest that your mouse clicks are being tracked.)
- If the URL you clicked on was in one of your private files, such as your email reader may use, the full file name is still handed over to the web site. It may contain information about you such as an indication of your name or email address, the email program you are using, and the structure of your file space.

Junkbusters http://www.junkbusters.com/cgi-bin/privacy

Increase Your Knowledge

Most computer users think they are much safer on line than they actually are according to a survey of 329 computer users by America Online and the National Cyber Security Alliance (NCSA) during 2004.[174] To conduct the survey, AOL and the NCSA sent technicians to 329 homes to inspect users' computers. Here's what the survey found:

- Four out of five users had spyware and/or adware on their computers, and most did not know this software was running on their computers.
- Nearly two-thirds had been infected by a virus at one time (and this is just the number who *knew about an infection*).
- 85 percent had anti-virus software, but more than half hadn't updated it in a week or more.
- Two-thirds of users did not have any type of firewall protection.
- Nearly three in five users did not know the difference between a firewall and antivirus software.
- 38 percent of wireless users had not bothered to encrypt their networks.

Users are endangering not only their own privacy and security, including any and all financial and personal data stored on a computer, but *they are putting everyone else at risk*. The proliferation of spyware opens the gates to intruders who can potentially gain control of individual computers. When networked together, this system of personal computers can form what is usually called a "zombie army" of PCs that can be used to attack other networks. Like it or not, each individual is responsible for his or her own computer privacy and security, so please pay attention to the basics to protect yourself and others. Here are the minimum steps you need to take:

- Keep your system patched and regularly update all security software.
- Install, routinely run, and UPDATE an anti-virus program (at least once a week).
- In general, do not open email attachments.
- Install and use firewall software and/or hardware (make sure settings are restrictive).

[174] America Online and National CyberSecurity Alliance, "AOL/NCSA Online Safety Study," Staysafeonline.org, October 2004, <http://www.staysafeonline.org/pdf/safety_study_2005.pdf> [PDF] (14 November 2006).

- Use strong passwords and change them regularly.
- Do not download and install programs indiscriminately (read user agreements).
- Install, routinely run, and update spyware software (at least one and preferably two).
- Configure your Internet browser(s) to maximize security.
- If you have a wireless network, use strong encryption.

For general information and help with personal privacy and security concerns, visit websites such as are NCSA's Stay Safe Online, CERT's Home Network Security, About's Network Security, and Microsoft's page on security and privacy for home users to learn more about vulnerabilities and how to protect yourself from many dangers on the Internet. All these sites not only warn you about the problems but also do an excellent job of telling you how to fix vulnerabilities.

About's Network Security	http://netsecurity.about.com/
CERT's Home Network Security	http://www.cert.org/tech_tips/home_networks.html
Get Safe Online	http://www.getsafeonline.org/
Microsoft Security & Privacy for Home Users	http://www.microsoft.com/athome/security/default.mspx
NSA's Security Recommendation Guides	http://www.nsa.gov/snac/
NCSA's Stay Safe Online	http://www.staysafeonline.info/
Surf the Net Safely	http://surfthenetsafely.com/

and for Macintosh users...

SecureMac.com	http://www.securemac.com/

The Perils and Pitfalls of Wireless Internet

I believe I need to interject a few comments about **wireless Internet connectivity** here. If you use wireless connections either in your home or on the road, I urge you in the strongest terms to be extremely careful with wireless connectivity. The *New York Time*'s technology columnist David Pogue wrote an interesting piece on how his eyes were opened by a stark demonstration of the insecurity of a public WiFi connection.[175] In fact, if you use WiFi without encryption, expect that anyone and everyone can read everything you read and write, and track every move you make.

You also need to be aware of the WiFi "evil twin" scenario, an attack that is remarkable both for its simplicity and its effectiveness. Here's how it works. The bad guy takes his laptop to a popular coffee shop where lots of people like to use the Internet while enjoying a cup o' joe. The bad guy has set up his computer to transmit a signal that turns his laptop into an Internet gateway or access point, one that looks and sounds remarkably legitimate. Here you come, mocha frappuccino in hand; you open your laptop, start searching for a local WiFi connection, and—bingo—in addition to that coffee shop's fee-for-service Mobile Hotspot, there is a second option Cheap & Friendly Mobile Hotspot or maybe even a Free Mobile Hotspot. If you are like most people, you might well log into the cheap or free service, assuming they are legitimate WiFi hotspots. And what happens if you do log into an evil twin WiFi access point? The bad guy will have software on his computer to capture every keystroke you make, so whatever you have entered once you've logged in, he now owns. And if you used a credit card to log into the cheap WiFi hotspot, the bad guy now has that. Even if you sent any encrypted data, such as a password, that's still probably not a problem for the bad guy because he also undoubtedly has software to break that, too.

The problem is obvious: you don't want to fall prey to this evil twin attack, but how to avoid it and still use WiFi hotspots? Here are good suggestions from PCWorld Magazine:

> "Check Your Wi-Fi Settings: Many laptops are set to constantly search and log on to the nearest hotspot. While this option might seem convenient, it does not allow you to monitor which hotspots you are logging on to and determine if they are legitimate. Turning off this option will prevent your computer from logging on to a hotspot without your knowledge.
>
> Pay Attention to Dialog Boxes: Pop-up warnings are there for a reason—to protect you. If you are lucky enough to have not clicked the "never show this again" option, make sure you read these warnings carefully before agreeing to send information.
>
> Use One of Your Credit Cards on the Web Only: Open a credit card account that is used solely for the purposes of shopping on the Web. Ideally, you should be able to access account records online so you don't have to wait for monthly statements to monitor any activity. "Be prepared to close that account on short notice if it's been compromised," says Schiller.
>
> Conduct Private Business in Private: "Maybe you don't need to move money around or check your bank statements when you are connected to a public

[175] David Pogue, "How Secure is Your WiFi Connection," Pogue's Posts, *The New York Times*, 4 January 2007, <http://pogue.blogs.nytimes.com/2007/01/04/04pogue-email/>, 16 January 2007.

> hotspot that you're not really familiar with," says Schiller. If you restrict your public surfing to Web pages you don't mind a stranger reading along with you, there is little an evil twin attacker can do to harm you."[176]

I recommend that you embark on the installation of a home wireless network with trepidation and care. Two good starting places for learning more about secure wireless networking are Tony Bradley's "Introduction to Wireless Network Security" and Brian Livingston's "Wi-Finally: Wireless Security That Actually Works."

Introduction to Wireless Network Security
http://netsecurity.about.com/od/hackertools/a/aa072004b.htm

Brian Livingston, "Wi-Finally: Wireless Security That Actually Works"
http://www.windowssecrets.com/comp/050526/ - story1

"Law #10: Technology is not a panacea."[177]

Web Tip

Virtually all Microsoft products come with all the doors open and unlocked, figuratively speaking. You must take upon yourself to find the open doors, shut them, and lock them tight.

[176] Erin Biba, "Does Your Wi-Fi Hotspot Have an Evil Twin? Identity thieves are going wireless in their quest to steal your personal info," Medill News Service, PCWorld, 15 March 2005, <http://www.pcworld.com/news/article/0,aid,120054,00.asp > (16 January 2007).

Browser Concerns

Using Internet Explorer's Privacy and Security Controls

One of the biggest underlying problems vis-à-vis Internet security is that virtually all Microsoft products,[178] including Internet Explorer, come with all the doors open and unlocked, figuratively speaking. You must take upon yourself to find the open doors, shut them, and lock them tight. The guiding principle for browser security is to place high restrictions on all web sites *by default*, while giving trusted sites only limited security restrictions. This will allow trusted sites to function with limited or no problems.

Because of the many changes occurring with Microsoft products, including the release of Internet Explorer 7 in October 2006 and the Vista operating system in January 2007, as well as the growth in popularity of the Firefox browser, I am no longer focusing on instructions for specific software. Instead, I will discuss the broad issues surrounding browser privacy and security and point you to sites where you can learn the details of securing your own particular browser and other software.

In August 2005, Microsoft released an upgrade to IE version 6 that was only available to users of Windows XP SP2. For more information on IE6 for Windows XP SP2, I recommend these sites to readers who still use IE6:

Windows XP Service Pack 2: What's New for Internet Explorer and Outlook Express
http://www.microsoft.com/windowsxp/sp2/ieoeoverview.mspx

Comparison of the Internet Explorer Security Zones in Windows XP Service Pack 2
http://surfthenetsafely.com/ieseczone5.htm

Then, on November 1, 2006, Microsoft began offering Internet Explorer 7, since renamed Windows Internet Explorer, as a high-priority update via Windows Automatic Updates. Microsoft is no longer updating its browser for any operating systems other than XP Service Pack 2, Windows Server 2003, and Windows Vista.

[177] "The Ten Immutable Laws of Security," Microsoft Security Essays, <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp > (14 November 2006).

[178] The advent of Windows XP Service Pack 2 in 2004 addressed some of these "open door" privacy and security issues, but certainly not all of them. The safest rule is never to assume any product is secure and always read the instructions on how to implement higher levels of privacy and security. A good starting place for Windows security help is Microsoft Technet Security. <http://www.microsoft.com/technet/security/default.mspx> (14 November 2006).

For help with IE7's security and privacy settings, look at the Microsoft website and these other sites, but remember, the IE browser in Windows XP is not the same as the browser that came with Vista. Microsoft offers a set of four steps to improve your online security and privacy. While it is incomplete, it is a good starting place for strengthening your Microsoft-based browser and email security.

Microsoft IE7: Dynamic Security Protection
http://www.microsoft.com/windows/products/winfamily/ie/features.mspx

Microsoft: Improve the Safety of Your Browsing and E-Mail Activities
http://www.microsoft.com/athome/security/online/browsing_safety.mspx

How to surf more safely with Internet Explorer 7
http://www.helpwithwindows.com/techfiles/ie7-surf-safe.html

Brian Livingston, Windows Secrets, IE7 Needs Tweaking for Safety
http://windowssecrets.com/comp/061026/ - story1

Diana Huggins, IE 7.0's Internet Options Privacy and Security Settings
http://www.lockergnome.com/nexus/windows/2007/01/22/ie-70s-internet-options-security-settings/
http://www.lockergnome.com/nexus/windows/2007/01/23/ie-70s-internet-options-privacy-settings-part-i/
Be sure to look at Part II as well.

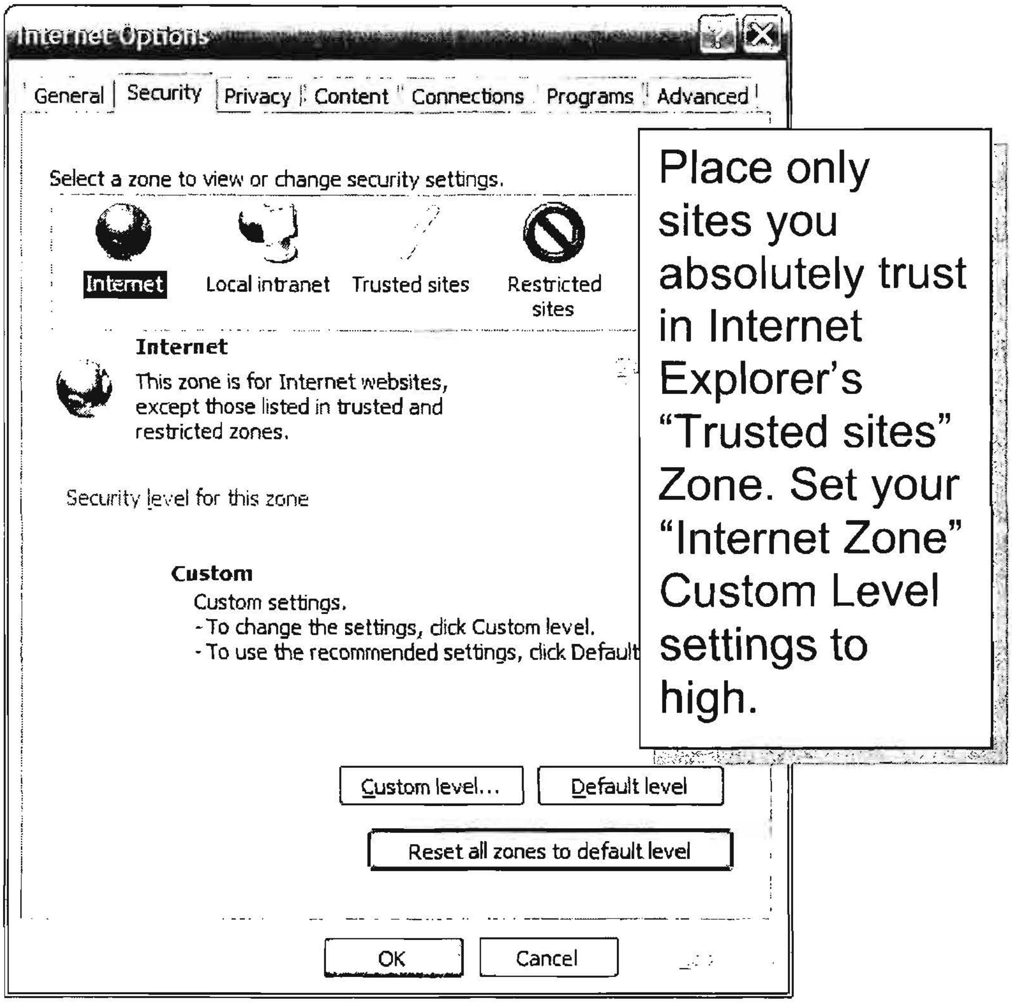
Marc Liron, Microsoft MVP on Internet Explorer 7
http://www.updatexp.com/internet-explorer-7-download.html

Deb Shinder, Tech Republic, "10 things you should know about Internet Explorer 7 Security" http://articles.techrepublic.com.com/5100-1009_11-6130844.html

Surf the Web Safely: Make IE7 Safer http://surfthenetsafely.com/ieseczone8.htm

Kim Komando's Firefox 2 and IE7's Security Settings
http://www.komando.com/tips/index.aspx?id=2523

One of Internet Explorer's best security features is its **Trusted Sites**. The Trusted Sites option is an excellent way to give some websites more privileges while keeping most sites at higher security settings. Put only sites you absolutely trust, e.g., your bank, in your "trusted sites" zone and keep all others at the highest security settings.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default

Place only sites you absolutely trust in Internet Explorer's "Trusted sites" Zone. Set your "Internet Zone" Custom Level settings to high.

While there are various differences among Microsoft Internet Explorer browser versions, these are generally accepted as safe settings for the **Internet Zone** using the **Custom Level**:

Tools | Internet Options | Security | Internet Zone | Custom Level

- ActiveX Controls and plugins
    - Download signed ActiveX controls **[Prompt or Disable]**
    - Download unsigned ActiveX controls **[Disable]**
    - Initialize and script ActiveX controls not marked as safe **[Disable]**
    - Run ActiveX controls and plug-ins **[Disable]**
    - Script ActiveX controls marked safe for scripting **[Prompt or Disable]**

- Downloads
  - File Download **[Enable]**
  - Font Download **[Prompt]**
- Microsoft VM
  - Java permissions **[High Safety]**
- Miscellaneous
  - Access data sources across domains **[Disable]**
  - Allow META REFRESH **[Enable]**
  - Display mixed content **[Prompt]**
  - Don't prompt for client certificate selection… **[Disable]**
  - Drag and drop or copy and paste files **[Enable or Prompt]**
  - Installation of desktop items **[Disable]**
  - Launching programs and files in an IFRAME **[Disable]**
  - Navigate sub-frames across different domains **[Enable or Prompt]**
  - Software channel permissions **[High Safety]**
  - Submit nonencrypted form data **[Enable]**
  - Userdata persistence **[Disable]**
- Scripting
  - Active scripting **[Disable]**
  - Allow paste operations via script **[Disable]**
  - Scripting of Java applets **[Disable]**
- User Authentication: **Automatic logon only in Intranet zone**

As a general rule, do not rely upon sliders to determine your security settings. These settings will affect your browsing. Some websites require ActiveX or scripting. If you want to run ActiveX or scripts on any website, you can either turn this feature on temporarily or add the site to the **Trusted sites zone**, though I would be very, very careful about which sites you add.

You can add Web sites by selecting the **Trusted sites** icon, and pressing the **Sites** button. The default setting only lets you add secure sites (sites using https); however, if you uncheck the **Require server verification (https:) for all sites in this zone**, you can add any site.

Web Tip

Have you suppressed popups only to continue to see them? Here's why: in Netscape, there is a default list of "exceptions" for sites whose popups are allowed. To view this list and suppress popups from these sites in Netscape 7.x, Edit | Preferences | Privacy & Security | Popup Window Controls | Suppress Popups | Exceptions | Remove All

Firefox, IE 6 for Windows XP SP2, and IE7 block all popups by default but permit users to allow popups from specific websites. Older versions of MSIE do not have a popup blocker option.

Manage ActiveX, Java, & JavaScript

Many security vulnerabilities exploit these applications and most privacy/security experts recommend disabling them. Malicious hackers can use ActiveX, Java, or JavaScript to upload files and run them on your computer when you simply visit a web page that has been cracked or created by malicious hackers. "In January 1997 members of the Hamburg-based Chaos Computer Club staged an electronic break-in on German national television. Using an ActiveX control, they made unauthorized bank transfers through Intuit's Quicken without a personal identification number. The demonstration sought to prove that executable content, particularly Microsoft's ActiveX, isn't secure."[179] In fact, *any ActiveX control downloaded over the web might be a Trojan horse or a virus.*

[179] "Preventing Possible Web Intrusions," Smartcomputing.com, Vol 8, Issue 4, April 2000, <http://www.smartcomputing.com/editorial/article.asp?article=articles%2Farchive%2Fg0804%2F37g04%2F37g04%2Easp> (14 November 2006).

More recently, malicious users have found devilishly clever ways to use ActiveX, Java, and JavaScript to hijack browsers, or to be more precise, to hijack Internet Explorer. The least innocuous form of browser hijacking involves changing the browser's home page and favorites, but most browser hijackers do a lot more, from creating endless pop-up windows to taking complete control of your browser. Browser hijacking software also usually includes some form of spyware to monitor and report your Internet activity. Worse, they are notoriously difficult to remove.

ActiveX has been implicated in the surreptitious installation of software known as drive-by downloads. **Drive-by downloads**[180] occur when a user simply visits a website or views an HTML email. These sites exploit a vulnerability in Internet Explorer's ActiveX to download, install, and run software on an unsuspecting user's computer without his knowledge or consent. This type of software can also be very difficult to remove.

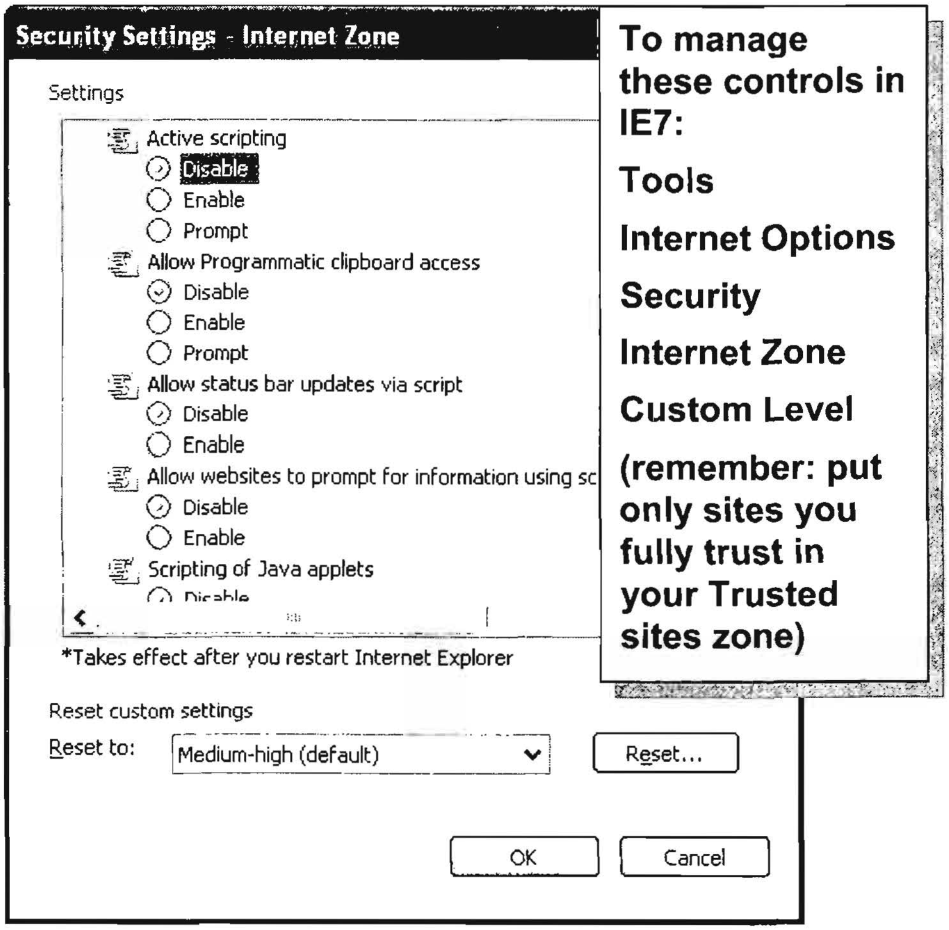
Keep in mind that, by default *active scripting is enabled by default in Internet Explorer*! The problem with simply disabling these controls is that you will encounter difficulties viewing some webpages. Experiment with turning them off or, in the case of MSIE, having your browser "Prompt" you and see what happens.

Here are recommendations for increased security settings in IE's **Internet Zone** (remember, you can put sites where you need to use these controls into your **Trusted Sites Zone**):

Tools | Internet Options | Security | Internet Zone | Custom Level

- ActiveX Controls and plugins
    - Download signed ActiveX controls **[Prompt or Disable]**
    - Download unsigned ActiveX controls **[Disable]**
    - Initialize and script ActiveX controls not marked as safe **[Disable]**
    - Run ActiveX controls and plug-ins **[Disable]**
    - Script ActiveX controls marked safe for scripting **[Prompt or Disable]**

[180] "A **drive-by download** is a program that is automatically downloaded to your computer, often without your consent or even your knowledge. Unlike a pop-up download, which asks for assent (albeit in a calculated manner likely to lead to a "yes"), a drive-by download is carried out invisibly to the user: it can be initiated by simply visiting a Web site or viewing an HTML e-mail message. Frequently, a drive-by download is installed along with another application. For example, a file sharing program might include downloads for a spyware program that tracks and reports user information for targeted marketing purposes, and an adware program that generates pop-up advertisements using that information. If your computer's security settings are lax, it may be possible for drive-by downloads to occur without any action on your part." "Drive-by Download," SearchSMB.com, <http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci887624,00.html> (14 November 2006).



Security Settings - Internet Zone

Settings

Active scripting
● Disable
○ Enable
○ Prompt

Allow Programmatic clipboard access
● Disable
○ Enable
○ Prompt

Allow status bar updates via script
● Disable
○ Enable

Allow websites to prompt for information using sc
● Disable
○ Enable

Scripting of Java applets
● Disable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

To manage these controls in IE7:

Tools

Internet Options

Security

Internet Zone

Custom Level

(remember: put only sites you fully trust in your Trusted sites zone)

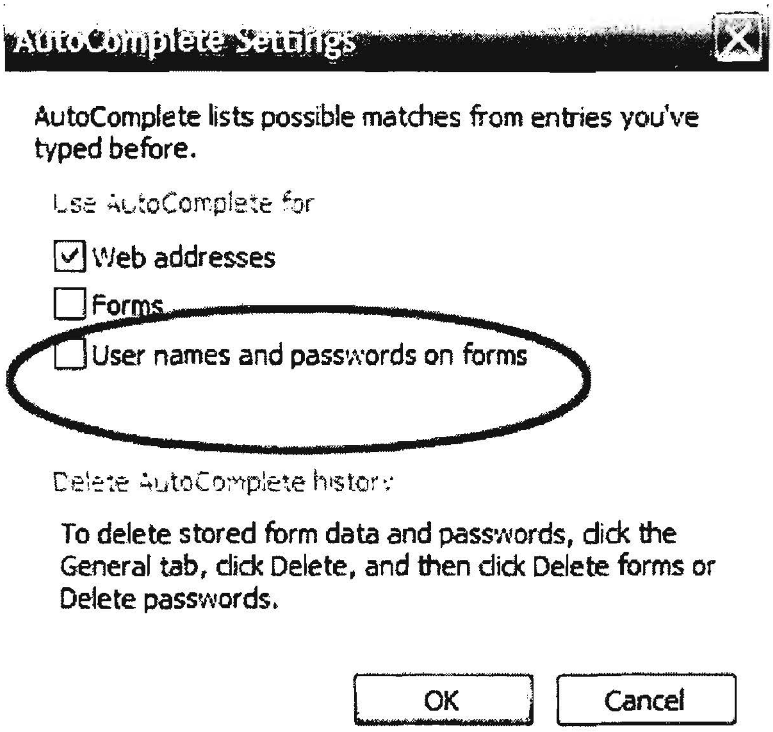
What's the best way to avoid browser hijacking and drive-by downloads? "First and foremost simply, stop using Internet Explorer. If you use Mozilla browsers (Netscape and Firefox) or Opera, you are immune to all known browser hijackers. You are immune for two reasons. First, most people use Internet Explorer, so most malicious code is custom built to exploit it. Second, Opera's and Mozilla's programmers take security very seriously and have made these browsers very secure. It is not possible to install software from a web site using these browsers without at least seeing a prompt of some sort asking permission." This is the advice of most Internet security experts.[181]

[181] Mike Helan, "Prevent Browser Hijacking," *SpywareInfo.com*, 23 March 2004 (Updated 12 January 2005), <http://www.spywareinfo.com/articles/hijacked/prevent.php> (article no longer available).

Despite changes in IE7, Microsoft's browser still relies heavily on ActiveX controls, which are often exploited by browser hijackers. In fact, *PC World* lists IE as the number one Internet threat of 2007 because of IE's "reliance on Microsoft's ActiveX technology, which allows Web sites to run executable programs on your PC via your browser."[182] Although Firefox is becoming a more tempting target for malicious hackers, IE remains the target of choice for now both because it is the most popular browser and because of its dependence on ActiveX.

Disable Autocomplete for Forms and Names/Passwords on Forms

This is another case where placing convenience ahead of security could cost you dearly. You do not want passwords or forms saved to the browser so that someone else might use them for some nefarious purpose. Passwords should not be saved unencrypted or without strong protection anywhere at any time. Many online stores will ask you if you would like to save your credit card information for future use. ***Do not allow websites to save your credit card number***. Make a habit of entering such personal and financial data each time it is needed and only for that transaction.



AutoComplete Settings

AutoComplete lists possible matches from entries you've typed before.

Use AutoComplete for

☑ Web addresses

☐ Forms

☐ User names and passwords on forms

Delete AutoComplete history

To delete stored form data and passwords, click the General tab, click Delete, and then click Delete forms or Delete passwords.

[182] Scott Spanbauer, "Thwart the Three Biggest Internet Threats of 2007," 24 January 2007, <http://www.pcworld.com/printable/article/id,128538/printable.html> (31 January 2007).

In Internet Explorer:

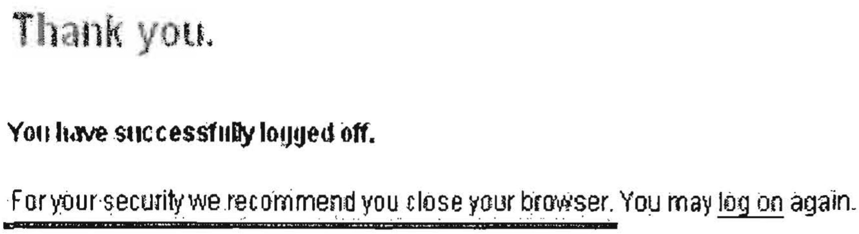
Tools | Internet Options | Content | AutoComplete Settings

Uncheck the second and third boxes (*forms* and *user names and passwords on forms*).

Be sure to Delete AutoComplete History (in IE7) or Clear Forms and Clear Passwords (in IE6) to remove any stored data.

Firefox & the "Clear Private Data" Option

One of the many nice features of Mozilla's Firefox browser is the "Clear Private Data" option. First, why did Mozilla include this option and why would you want to consider using it? A lot of websites imply this option is just for people doing things on a shared computer that they don't want others to know about, but that is an extremely narrow understanding of why it is important to remove certain personal data from your browser and computer. After logging off a secure website, especially your bank's or credit card's site, have you ever gotten a message like this?



Thank you.

You have successfully logged off.

For your security we recommend you close your browser. You may log on again.

Why is a secure site recommending you close your browser? Browsers do a very good job of keeping track of when and where you have been on the Internet and, in some cases, what you have been doing. Browsers are usually set to save or cache the pages you visit so that the next time you visit that page, you will not have to wait for the server to send the page to your browser. While this makes your surfing faster, it also causes a small but real vulnerability by creating a record of your browsing history. In the case of a site where you have entered information such as a password, a credit card number, your Social Security Number, etc., that information filled into a form on the web may remain in your cache and therefore on your computer. While it is unlikely a malicious user is going to get that information, it is not impossible. Also, if you ever use a computer that others can access, remember, they can get that information, so why not take a few steps to improve your privacy and security?

You can manually clear your browser each time you use it, and as I explained in the previous section, current versions of Internet Explorer offer an option to clear the browser cache automatically when you close the browser. However, this only addresses the cache issue. Firefox provides an easy way to delete stored information of various types either as you are working online or whenever you close your browser. The *default* setting of the "Clear private data" option in Firefox will delete:

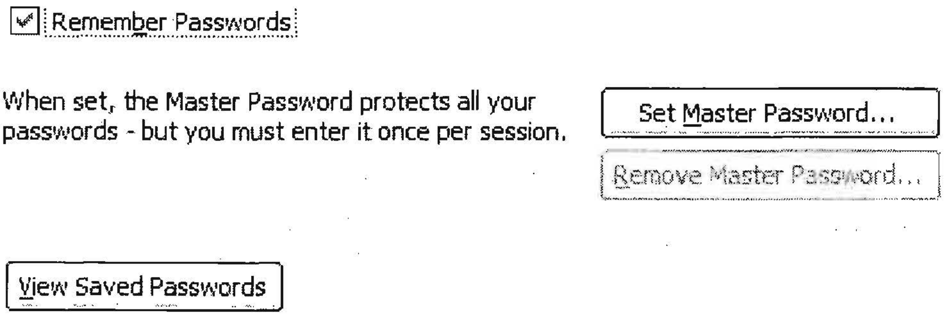
- your browsing history.
- form data (this could include credit card numbers).
- your download history, cache, and authenticated sessions (the kind of sessions likely to include passwords).

The "Clear private data" option leaves saved passwords and cookies alone unless you tell it otherwise. I doubt if many users want to preclude the use of cookies altogether; cookies placed on your computer from the originating site (that means the site you are visiting) rarely present a problem and are a genuine help in many instances (for example, cookies let you set preferences at a search engine so you don't have to reset them every time you go there). By now most people know they probably do not want third party cookies, that is, cookies placed on your computer by some uninvited third party, such as from a banner ad. You can tell Firefox (and other browsers, too) to save cookies for the originating site only and leave the "Cookies" option unchecked on the "Clear private data" form. Also keep in mind that Firefox lets you browse, search, and delete individual (or all) cookies using the "View cookies" option.

Saving passwords is a more controversial subject. My preference is not to let any browser save any of my passwords, but many experts think having Firefox manage them for you (with a very strong Master Password) is actually safer than writing them down. I disagree; most people don't break into a house in order to break into a computer. One important caveat: ***do not use the Firefox Remember passwords' option on a laptop***. That way, if someone steals your laptop and accesses the account, the thief will not have access to every saved password you have stored. It is too easy to get at the Firefox Master Password, which in turn will unlock every password saved by Firefox on that laptop.

If you want Firefox to remember your passwords, here is the safest way to do it:

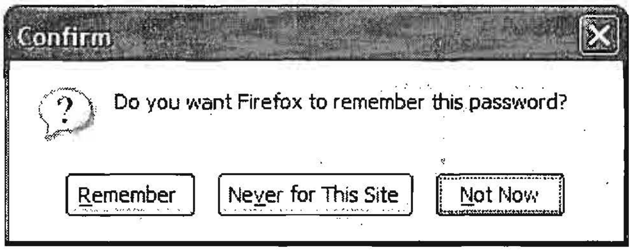
Select Tools | Options | Privacy | Passwords and check "Remember Passwords"



☑ Remember Passwords

When set, the Master Password protects all your passwords - but you must enter it once per session.

Now when you enter a password, Firefox will automatically ask you the following question:



Confirm

Do you want Firefox to remember this password?

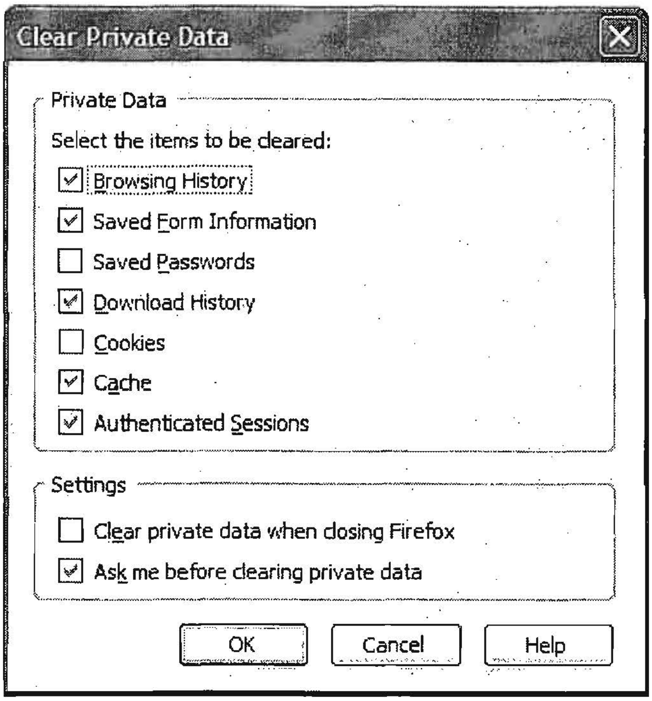
If you are going to allow Firefox to save your passwords, then I believe you must also set a Master Password (and do not forget it). Otherwise, anyone with access to your computer can view your saved passwords.[183] The Master Password will be required for your saved passwords to be loaded. Firefox will prompt you to enter it once per session when it is needed. You can also manage saved passwords and delete individual passwords by clicking the "View Saved Passwords" button. Keep in mind that the Master Password is required in order to change or remove the Master Password, which is why it is important not to forget it (of course, there are hacks for resetting it if you have forgotten it). With a Master Password in place, in principle no one can see your passwords unless he also has your Master Password. However, the Firefox Master Password is not going to stop a knowledgeable malicious hacker with full access to your computer from getting the Master Password and, indeed, all your passwords, but if someone has full file-level access to your computer, you are already in deep trouble.

Finally, I recommend using the Firefox feature that will clear your personal information automatically:

Select Tools | Options | Privacy | Settings and check "Clear private data when closing Firefox," then click OK twice.

[183] Some people have discovered, usually the hard way, that viewing someone else's Tools | Options | Privacy | View Saved Passwords | Passwords Never Saved may reveal some rather shocking facts about sites the other person has visited. This only works if Firefox is set to Remember Passwords and the user chose "Never for this site."

These are not my preferences; I like to keep my Browsing History and I have Firefox Clear private data when closing.



Private Data

Select the items to be cleared:

☑ Browsing History

☑ Saved Form Information

□ Saved Passwords

☑ Download History

□ Cookies

☑ Cache

☑ Authenticated Sessions

Settings

□ Clear private data when closing Firefox

☑ Ask me before clearing private data

You can also use the Clear Private Data option without closing the browser when you log out of a site where you entered data such as a password, credit card number, etc., (clearing Authenticated Sessions).

Select Tools | Clear Private Data or use the keystroke combination Ctrl+Shift+Del.

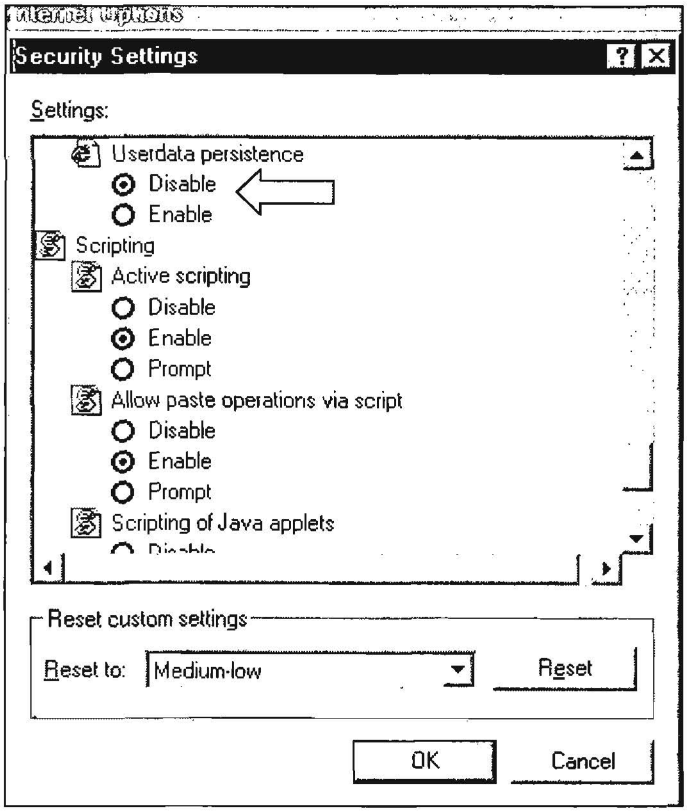
- One final comment: all these types of measures are useful and worth taking, especially since most Internet users do nothing to protect their privacy and security. But please do not be lulled into a false sense of security because a proficient malicious hacker can make hash out of all basic computer security measures.

Disable "Userdata Persistence"

Userdata Persistence is a feature in Internet Explorer that lets websites "remember" information you enter, such as search queries. Userdata persistence is an XML-based storage methodology for saving large amounts of user data. If you use Internet Explorer, have you ever come back days or weeks later and find that, as you type your query, your earlier queries suddenly appear in or below the query box? This is user data persistence at work. Many people manage cookies, but few realize they also need to disable this "feature" in MSIE. It is easy to disable: In MSIE 5 & 6:

Tools | Internet Options | Security | Custom Level | Miscellaneous

About two-thirds the way down you will see "userdata persistence." Select *Disable.*



Internet Options

Security Settings

Settings:

- Userdata persistence
  - ● Disable
  - ○ Enable
- Scripting
  - Active scripting
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Allow paste operations via script
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Scripting of Java applets

Reset custom settings

Reset to: Medium-low

You will also need to <u>*clear your cache*</u> to clean out old user data.

<u>Manage Your Cookies</u>

Cookies are the source of a great deal of discussion and consternation among Internet users. What exactly are cookies? They are text files placed on a user's hard disk (yes, your computer) by a website. Each cookie has two parts: a name and a value. The value can contain a lot of data, such as the address of the server that set the cookie, an expiration date, and (possibly) usernames and passwords. Before you panic, this data is usually encrypted, and cookies were designed so only the site that placed them on your computer in the first place could read them. This being said, nothing is 100 percent secure and it is not a good idea to accept all cookies willy-nilly.

You have many options for handling cookies. Most browsers offer the option never to accept cookies, but many sites require them and turning them all off is generally not a realistic option for most Internet users. One compromise is to accept only those cookies that are sent back to their originating server, which means you won't allow third-party cookies (this, however, will not stop cookies from pop-up windows). Blocking third-party cookies also prevents web bugs from linking together information in your email with the web sites you visit. Newer browser versions have more cookie options with promises for even greater user control in future releases. Check your browser(s) preferences/options to see what choices you have. Also check out:

To manage cookies in IE 6/7:
Tools | Internet Options | Privacy

Internet Explorer 6 and 7 have enhanced cookie management, including a ***privacy settings slider*** with six settings: Block All Cookies, High, Medium High, Medium (default level), Low, and Accept All Cookies. The default setting is Medium. You can override automatic cookie handling for all websites by clicking **Advanced** on the **Privacy** tab. You can also choose to ***always accept*** or ***always reject cookies from specific sites***. I recommend you block all cookies from sites from which you know you never want to accept a cookie, e.g., *doubleclick.net*.

Better still, get a good "cookie crumbler," that is, software designed to handle cookies automatically and intelligently. Cookie Central reviews a number of cookie management programs.

For details on handling cookies in **Internet Explorer 6/7**, I recommend Surf the Net Safely's "Advanced Cookie Management in Internet Explorer 6 and 7, <http://surfthenetsafely.com/cookie_advanced.htm>.

Firefox/Mozilla offers flexible cookie controls, and there is a very good tutorial on using Firefox's cookie management options at:

Firefox's Cookie Options
http://mozilla.gunnars.net/firefox_help_firefox_cookie_tutorial.html

Microsoft's Help Safeguard Your Privacy on the Web (for IE6, but most still applies to IE7) http://www.microsoft.com/windows/ie/using/howto/privacy/config.mspx

Cookie Central's Reviews of Cookie Management Software
http://www.cookiecentral.com/files.htm

Junkbusters Cookie Page http://www.junkbusters.com/ht/en/cookies.html

Disable or Defeat the HTTP-Referrer

The **"http referrer" variable** (often misspelled "referer"[184]) may be a serious concern. This variable lets a site you are visiting know which site you just came from (which site referred you to them). Usually, the value of the "referrer" field is the url of the page you last visited. The problem is that ***the http-referrer variable gives out more information***. If you use a search engine to find a site and then click on that site, the http-referrer will provide the ***entire query*** you used to find the site! Furthermore, it is possible that other sensitive types of information, such as username, password, email address, or even a credit card number, could be sent as part of an http-referrer variable.[185]

There are ways around this problem. Here are three solutions:

1. **Don't click on a link from a search engine**; instead right-click on the link and select Copy Link Location (Mozilla) or Copy Shortcut (IE6); paste the link in the address window, and go to the link from the new browser window. Your query will not be provided. Remember: you must copy the link to the address bar; it is ***not*** sufficient to right-click and "open in new window" or "open in new tab."

2. Use a **browser-based service** that blocks the http-referrer, such as Webwasher or Guidescope, both of which are *free to individual users*, or any number of products that can be purchased for this purpose.

Webwasher[186]
http://www.cyberguard.com/products/webwasher/webwasher_products/classic/index.html

Guidescope http://www.guidescope.com/home/

3. **Disable the http-referrer in Netscape 7 and Firefox** (you cannot do this in Internet Explorer). In the Address/Location bar, type *about:config* and find *network.http.sendRefererHeader*. This variable can be set to 0, 1, or 2:

2—default; send referrer for all requests

1—do not send referrer for images

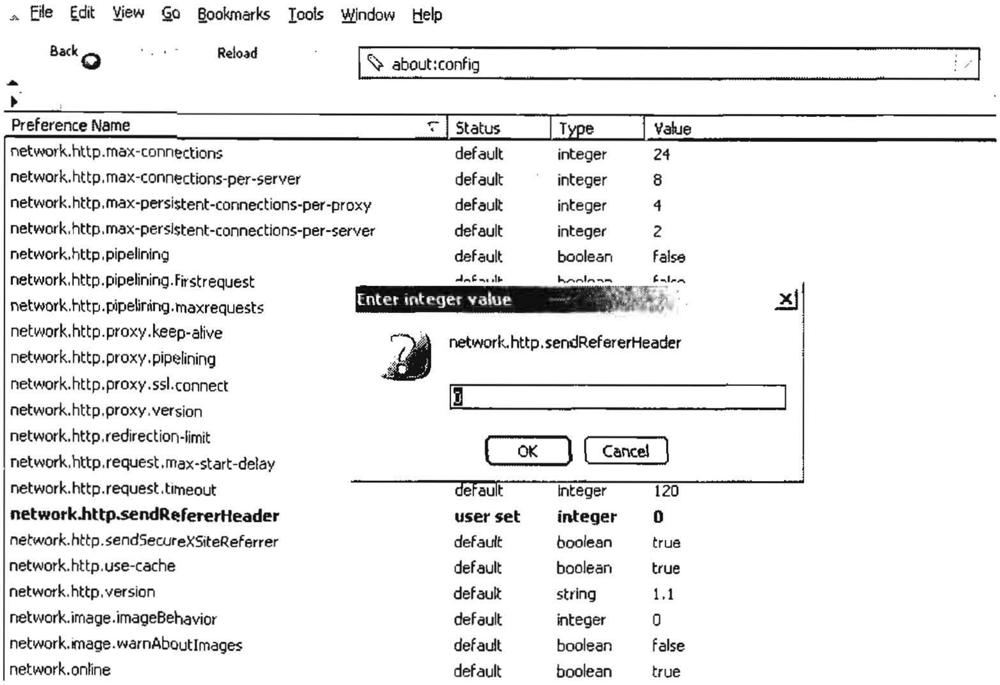
[184] The actual "referrer" code uses the incorrect spelling "referer," which may say something about the spelling skills of programmers.

[185] For an excellent overview of the legitimate use of and problems with the http-referrer, see, Lincoln D. Stein, "Referer Refresher, " *New Architect*, September 1998, <http://www.webtechniques.com/archives/1998/09/webm/> (14 November 2006).

[186] Webwasher Classic is now owned by Cyberguard and is still free, though the company does request a donation.

0—do not send referrer for anything

Open the menu by right-clicking and selecting *Modify*. Then change the numerical value from the default 2 to 0.



about:config

Preference Name	Status	Type	Value
network.http.max-connections	default	integer	24
network.http.max-connections-per-server	default	integer	8
network.http.max-persistent-connections-per-proxy	default	integer	4
network.http.max-persistent-connections-per-server	default	integer	2
network.http.pipelining	default	boolean	false
network.http.pipelining.firstrequest	default	boolean	false
network.http.pipelining.maxrequests			
network.http.proxy.keep-alive			
network.http.proxy.pipelining			
network.http.proxy.ssl.connect			
network.http.proxy.version			
network.http.redirection-limit			
network.http.request.max-start-delay			
network.http.request.timeout	default	integer	120
network.http.sendRefererHeader	**user set**	**integer**	**0**
network.http.sendSecureXSiteReferrer	default	boolean	true
network.http.use-cache	default	boolean	true
network.http.version	default	string	1.1
network.image.imageBehavior	default	integer	0
network.image.warnAboutImages	default	boolean	false
network.online	default	boolean	true

network.http.sendRefererHeader

0

Clear Your Cache

Things happen on your computer in the background as you browse the Internet, some of which can affect your privacy and security. **Caching** is the process whereby your browser tries to make your journey on the information highway faster by saving copies of webpages as you visit them. Then, if you decide to go back to a recently visited webpage, instead of having to reload the page from the Internet, your browser simply serves up the stored or "cached" copy from your computer. This is fine until you realize that the cache is a record of your web browsing and, potentially, certain information you may have entered at a website, including passwords or credit card numbers. The safest thing to do is to clear the cache each time you end an Internet session.

Internet Explorer makes this very easy to do. In fact, ***you can tell the browser to clear the cache every time you close it***. To clear the cache manually in Internet Explorer:

Tools | Internet Options | Temporary Internet Files | Delete Files

To have Internet Explorer automatically clear the cache each time you close the browser:

Tools | Internet Options | Advanced | Security | Empty Temporary Internet Folder When Browser is Closed

Delete Your History Files

Browsers keep detailed lists of everywhere you have been on the Internet for a variable length of time, depending on the settings you have chosen. These are known as history lists and many people do not like to retain them because they give anyone with access to your computer a clear picture of your browsing habits. Also, there have been a number of malicious exploits that have gained access to users' history lists, which is at the very least an invasion of privacy. You have several options for handling history files. The simplest is not to keep a history list by ***setting the number of days to keep a history list to zero***.

To manage your history file in Internet Explorer:

Tools | Internet Options | General | History | Clear History

Tools | Internet Options | General | History | Days to keep pages in history = 0

To manage your history file in Firefox:

Tools | Options | Privacy | Clear Browsing History Now

Tools | Options | Privacy | Remember Visited Pages for the last 0 days.

Set Up Different Browsers for Different Purposes

There are many ways to handle privacy and security concerns on the Internet and no one way is right for everyone. Some people have one computer (usually an old one that is not connected to any others) they use strictly for Internet browsing and shopping, while all personal and financial information is stored on other computers perhaps not even connected to the Internet at all. Another less expensive way to minimize privacy and security vulnerabilities is to set up one browser (say, Internet Explorer) to run at the highest security settings and use it for all Internet browsing. Then the other browser (say, Firefox) could be set to accept cookies, run scripts, etc., so that it could be used for such things as shopping and financial transactions. The point is to think about your personal privacy and security because the risks are real and growing.

Check Your Browser's Security

After you have made all the recommended changes to enhance your browser's privacy and security, it is a good idea to check your browser(s) for vulnerabilities. There is a free browser checkup run by a reputable company, the Belgian security firm ScanIT, which tests for system vulnerability against a range of 22 simulated attacks. The test works with any browser, including Internet Explorer, Mozilla-based browsers, and Opera. It also appears the test is not operating system dependent because it runs on Linux. Highly recommended.

ScanIt's Browser Security Check	http://www.scanit.be/bcheck